USER GUIDE

# Entuity® 16.5

## Entuity User and System Administrator Guide

*Entuity empowers service providers, systems integrators, and enterprises with network control and predictability foundational to meeting any of today's complex IT infrastructure challenges. Entuity provides a succinct suite of the most important functionality for network management – inventory, fault, and performance management – but presented in an easy to use, quick to deploy format.*

North America Headquarters
4 Mount Royal Avenue
Suite 340
Marlborough, MA 01752
Tel: +1 508 357 6344
Fax: +1 508 357 6358

EMEA Headquarters
9a Devonshire Square
London,
EC2M 4YN
Tel: +44 (0)20 7444 4800
Fax: +44 (0)20 7444 4808

## Entuity

# Contents

21 Entuity Services

22 Manage Branch Office Connectivity

## 23 Managing Performance and Asset Utilization

## 24 Monitoring Edge of Network Change

## 25 Set-up and Manage Flow Data

32 Views of the Managed Network

33 Manage View Filters

## 40 Advanced LDAP Authentication

## 41 Audit Log

## 42 Manage Entuity and Its Database

## 43 Day to Day Administration

## 49 Annotate Managed Objects

## 50 Entuity Event Handling and Integration Overview

## 51 Trap Management

## 52 Device System Logging

## 53 SNMP Trap Forwarding

## 54 Forward Events

## 55 XML Data Collection

## 56 User Defined Polling

## 69 Device Configuration Retrieval

## 70 Manage Entuity Configuration Monitor

## 71 Entuity Configuration Management

75 Entuity HA Compatibility Module

A Object States

B Connectivity Discovery Technologies

C Entuity URLs

# Figures

# Tables

# 1 Entuity Network Management Software

Entuity is an independent all-in-one network management solution that offers network staff and management full control over their converged networks. Entuity automates network management processes in a single integrated product for inventory/topology, fault/events, port, device and flow-based performance and configuration monitoring. Entuity has been highly acclaimed for its rapid deployment, ease of use, low cost of ownership, technological sophistication and openness to integration with other management systems in an enterprise.

Entuity is network management software that delivers. It delivers on the promise of proactive business resource management with a comprehensive and integrated solution that combines network performance, availability and resource management in one sleek powerful triple advantage of capability.

Entuity's fault management distinguishes between network, server and application problems using root cause analysis and prioritizes these problems based on business impact.

Entuity's performance management provides early warning of degrading performance that protects users from costly business interruptions.

Entuity's resource management builds a comprehensive inventory of network assets, their dependencies, and their physical connectivity. Resource profiles combined with fault and performance data provide an unprecedented ability to manage infrastructure in the context of the business it supports.

## Login to Entuity

You login to Entuity through a web browser using a URL with the format:

```
http://Entuityhost:port/
```

where:

- *http* can also be *https* when the Entuity server is configured to use SSL.
- *Entuityhost* is the IP address or resolved name of the Entuity server.
- *port* is the web port number defined during installation. It is not necessary to specify port if it is defined as the default http port (80) or https port (443).

Entuity displays the login screen appropriate to the device you are using to access it; from a supported tablet it is the tablet interface otherwise the standard login. There is a hyperlink from each login interface to the other.

To login to the Entuity web user interface:

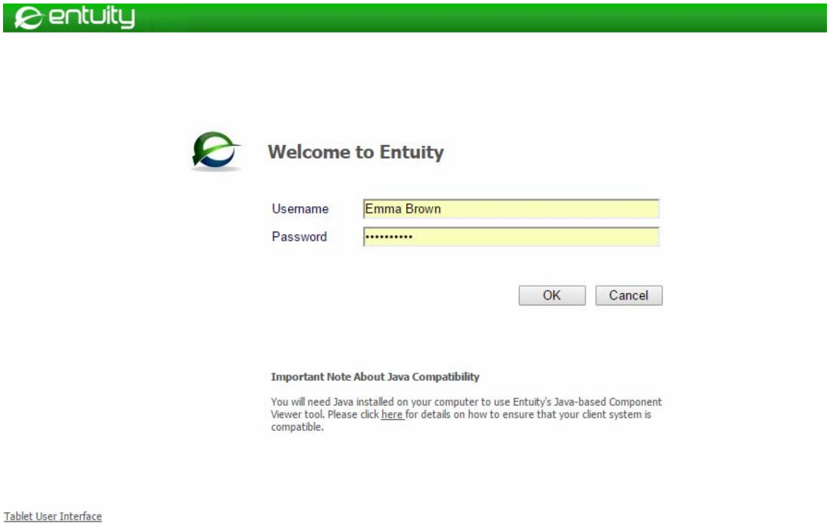
1) From a browser enter the Entuity URL. When the web server responds, it displays the Entuity login page.

   In the event of the web server failing to respond contact your System Administrator.

2) Enter your username and password. Entuity displays a brief information page showing the success of your log on operation before forwarding you to the Entuity entry page, by

default Inventory. You can also navigate to other Entuity functionality.

The user account you use to log on determines the functionality and business views to which you have access.



Welcome to Entuity

Username: Emma Brown

Password: ••••••••••

Important Note About Java Compatibility

You will need Java installed on your computer to use Entuity's Java-based Component Viewer tool. Please click here for details on how to ensure that your client system is compatible.

Tablet User Interface

Figure 1 Login to Entuity

## Entuity Interface

From the web interface you can access the main product areas of Entuity. To access an area you must have the appropriate permissions, only then are the menu options available for you to access the functionality within that area.

| Menu Item | Description |
|---|---|
| **Dashboards** | |
| Status Summary | Dashboard provides a one line performance summary of each view the user has the permission to access. |
| Service Summary | Provides a summary of viewable services, indicating service name and state with drill down capability. |
| TopN Summary | A view based report, with six sections; one section for each performance metric. Each section shows the TopN ports as measured against that section’s metric. From each section you can access more detailed graphs. |
| Device Metrics | Configurable dashboard that allows you to select the metrics to graph against selected devices. |
| Custom Dashboards | Users can run up to five user configurable dashboards, displaying data collected through Entuity or third party products (by referencing their URL). |

Table 1 Entuity Web UI Menu

| Menu Item | Description |
|---|---|
| **InSight Center** | |
| Green IT Perspective | Configurable dashboard that allows you to configure power consumption metrics and user groups, run a series of reports. |
| Network Delivery Perspective | Overview of the combined availability of services, applications, servers and infrastructure devices. |
| Service Delivery Perspective | Overview of the combined availability of services in a view. |
| Multiple/Branch Office Perspectives | Links to two Branch Office Perspectives. |
| CIO Perspective | CIO Perspective provides a high level view of service delivery. |
| Virtualization Perspective | Perspective allows visualization and evaluation of the impact of hypervisors and virtual machines in enterprise data centers. |
| User Defined Perspective | Displays either the user defined perspective template or the dashboard you have created. Contact your Entuity representative to learn more about developing perspectives. |
| **Explorer** | Provides a view based tree of the IT infrastructure objects Entuity manages. |
| **Events** | Provides access to the incidents and events raised in Entuity. |
| **Maps** | Provides access to visual representations of the network connectivity of your selected view. |
| **Charts** | Provides access to the last chart. |
| **Flows** | Provides access to flow charts through the Flow Analysis Options dialog. |
| **Reports** | Provides access to Entuity reports. |
| **Administration** | |
| Entuity Health | Overview of Entuity server health, process checking, reporting performance, database performance and detailed license checking. |
| Inventory / Topology | Provides access to:<br>■ Inventory Administration, an overview of the managed components which also provides access to inventory management functions. By default Entuity displays this page after administrators log on.<br>■ Inventory Snapshots through which you can manage snapshots used with the Inventory Change report.<br>■ ICMP Monitor through which you can set up and maintain the IP addresses Entuity uses with availability monitoring.<br>■ Physical Connections through which you can define connections between devices. |
| Events | Allows configuration of the Event Management System, event suppression and event threshold settings. |
| Flow Collector | Provides access to the Entuity Integrated Flow Analyzer configuration pages. |

Table 1 Entuity Web UI Menu

| Menu Item | Description |
|---|---|
| Data Export | Export of data from the database to a database external to Entuity. |
| User Defined Polling | Managed the configuration of User Defined Polling. |
| Account Management | Provides access to user and user group management and LDAP configuration. |
| Multi-Server Administration | Manage remote and central servers, manage license allocation and, when installed, assign flow collectors and manage SurePath servers. |
| Audit Log | Provides a central point for reviewing and analyzing actions performed on Entuity through its log files. |
| Preferences | Opens the Preferences dialog through which you can set the web interface user preferences. |
| **Help** | |
| Contents | Allows access to the Entuity help system. |
| Entuity Home | Link to the home page of the Entuity web site, http://www.entuity.com. |
| Entuity Support | Link to the Entuity Support web site, https://www.entuity-helpdesk.com, from where you can access the Entuity Help Desk.<br>Opens a page from where you can access Entuity Support details. |
| Help for this Page | A context sensitive help link from the current page. |
| About Entuity | Opens the About Entuity pop-up which details the Entuity version and its specific build number. Also included is a summary copyright statement. |

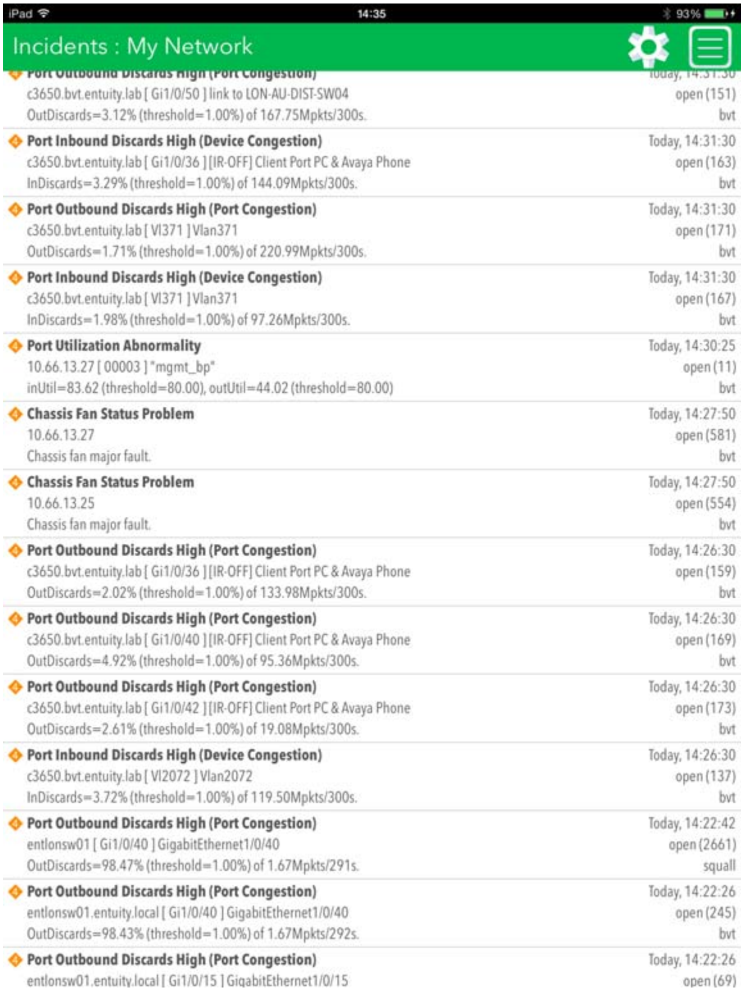
Table 1 Entuity Web UI Menu

## Tablet UI

Entuity includes multi-vendor tablet support. Entuity auto-detects whether access is from a tablet versus desktop web browser and present the appropriate interface. Tablet screens include support for popular tablet gestures.

Entuity tablet UI delivers a subset of the functionality delivered through the main interface. It includes the key features required to monitor the state of your network, comprising of:

- The Status Summary dashboard.
- Customized View, Device and Port Summary pages.
- Incident and Event Viewer.
- Reports you can configure, run and view.



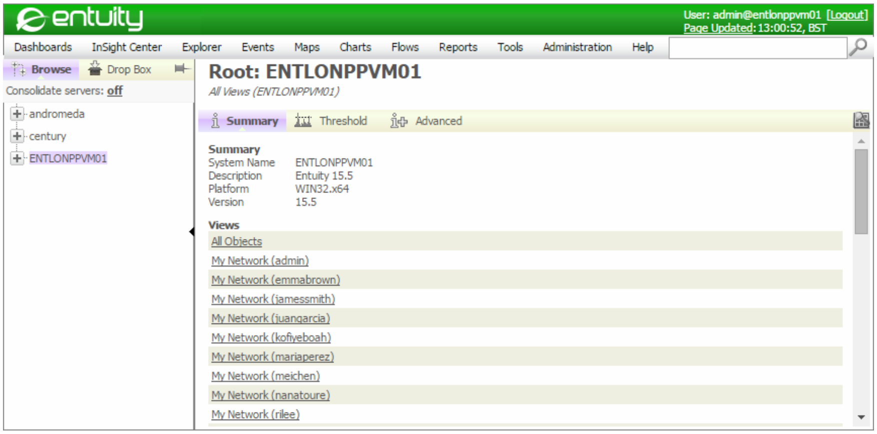
Incidents : My Network

```
Port Outbound Discards High (Port Congestion)                         Today, 14:31:30
c3650.bvt.entuity.lab [ Gi1/0/50 ] link to LON-AU-DIST-SW04                open (151)
OutDiscards=3.12% (threshold=1.00%) of 167.75Mpkts/300s.                          bvt
Port Inbound Discards High (Device Congestion)                        Today, 14:31:30
c3650.bvt.entuity.lab [ Gi1/0/36 ] [IR-OFF] Client Port PC & Avaya Phone   open (163)
InDiscards=3.29% (threshold=1.00%) of 144.09Mpkts/300s.                           bvt
Port Outbound Discards High (Port Congestion)                         Today, 14:31:30
c3650.bvt.entuity.lab [ Vl371 ] Vlan371                                    open (171)
OutDiscards=1.71% (threshold=1.00%) of 220.99Mpkts/300s.                          bvt
Port Inbound Discards High (Device Congestion)                        Today, 14:31:30
c3650.bvt.entuity.lab [ Vl371 ] Vlan371                                    open (167)
InDiscards=1.98% (threshold=1.00%) of 97.26Mpkts/300s.                            bvt
Port Utilization Abnormality                                          Today, 14:30:25
10.66.13.27 [ 00003 ] "mgmt_bp"                                             open (11)
inUtil=83.62 (threshold=80.00), outUtil=44.02 (threshold=80.00)                   bvt
Chassis Fan Status Problem                                            Today, 14:27:50
10.66.13.27                                                                open (581)
Chassis fan major fault.                                                          bvt
Chassis Fan Status Problem                                            Today, 14:27:50
10.66.13.25                                                                open (554)
Chassis fan major fault.                                                          bvt
Port Outbound Discards High (Port Congestion)                         Today, 14:26:30
c3650.bvt.entuity.lab [ Gi1/0/36 ] [IR-OFF] Client Port PC & Avaya Phone   open (159)
OutDiscards=2.02% (threshold=1.00%) of 133.98Mpkts/300s.                          bvt
Port Outbound Discards High (Port Congestion)                         Today, 14:26:30
c3650.bvt.entuity.lab [ Gi1/0/40 ] [IR-OFF] Client Port PC & Avaya Phone   open (169)
OutDiscards=4.92% (threshold=1.00%) of 95.36Mpkts/300s.                           bvt
Port Outbound Discards High (Port Congestion)                         Today, 14:26:30
c3650.bvt.entuity.lab [ Gi1/0/42 ] [IR-OFF] Client Port PC & Avaya Phone   open (173)
OutDiscards=2.61% (threshold=1.00%) of 19.08Mpkts/300s.                           bvt
Port Inbound Discards High (Device Congestion)                        Today, 14:26:30
c3650.bvt.entuity.lab [ Vl2072 ] Vlan2072                                  open (137)
InDiscards=3.72% (threshold=1.00%) of 119.50Mpkts/300s.                           bvt
Port Outbound Discards High (Port Congestion)                         Today, 14:22:42
entlonsw01 [ Gi1/0/40 ] GigabitEthernet1/0/40                             open (2661)
OutDiscards=98.47% (threshold=1.00%) of 1.67Mpkts/291s.                        squall
Port Outbound Discards High (Port Congestion)                         Today, 14:22:26
entlonsw01.entuity.local [ Gi1/0/40 ] GigabitEthernet1/0/40                open (245)
OutDiscards=98.43% (threshold=1.00%) of 1.67Mpkts/292s.                           bvt
Port Outbound Discards High (Port Congestion)                         Today, 14:22:26
entlonsw01.entuity.local [ Gi1/0/15 ] GigabitEthernet1/0/15                 open (69)
```

Figure 2 View Incidents on Tablet

## Entuity User Interface

The web User Interface (UI) provides a consistent user experience to assist your usage.



User: admin@entlonppvm01 [Logout]
Page Updated: 13:00:52, BST

Consolidate servers: off

Root: ENTLONPPVM01

*All Views (ENTLONPPVM01)*

**Summary**

| | |
|---|---|
| System Name | ENTLONPPVM01 |
| Description | Entuity 15.5 |
| Platform | WIN32.x64 |
| Version | 15.5 |

**Views**

All Objects
My Network (admin)
My Network (emmabrown)
My Network (jamessmith)
My Network (juangarcia)
My Network (kofiyeboah)
My Network (mariaperez)
My Network (meichen)
My Network (nanatoure)
My Network (rilee)

Figure 3 Entuity Server Root

The key components of the web UI are:

- Header, which includes
  - Entuity banner. If you click on the Entuity logo Entuity displays your home page.
  - `autoDiscovery` update status, this hyperlink is only available when `autoDiscovery` is in progress.
  - *User*, user name of the logged in Entuity user and the Entuity Server to which they first logged in.
  - Logout, allows you to terminate the current Entuity session.
  - Page Updated, the last time the content of the page was updated. When selecting Page Updated Entuity displays the status of all connected servers and any status messages received in the last five minutes.
- Menu bar, provides:
  - Access to the key functions of Entuity, although Entuity always checks the logged in user has the access rights to use the selected feature. Entuity displays a denied access error message when you do not have access to a feature.
  - Search, provides quick access to the search tool.
- Main panel is the area where Entuity displays network management information, e.g. maps, reports, events.
- Navigation panel is displayed on the left side of the main panel. You can click on the arrowhead to expand and hide the panel which contains two tabs:
  - Browse (default) contains the Explorer tree and shows the managed objects.
  - Drop Box is a repository for Custom Report Builder and Custom Dashboards. You can drag and drop items from the Entuity web UI for use when creating reports and dashboards.

  Navigation panel also indicates the consolidate server mode, and provides a hyperlink to the Preferences pages from where you can amend the setting.

Navigation panel is automatically displayed when you select, and Entuity displays Explorer, Events and Maps. You can also fix the panel as open by selecting the Pin icon.

## Checking Page and Server Status

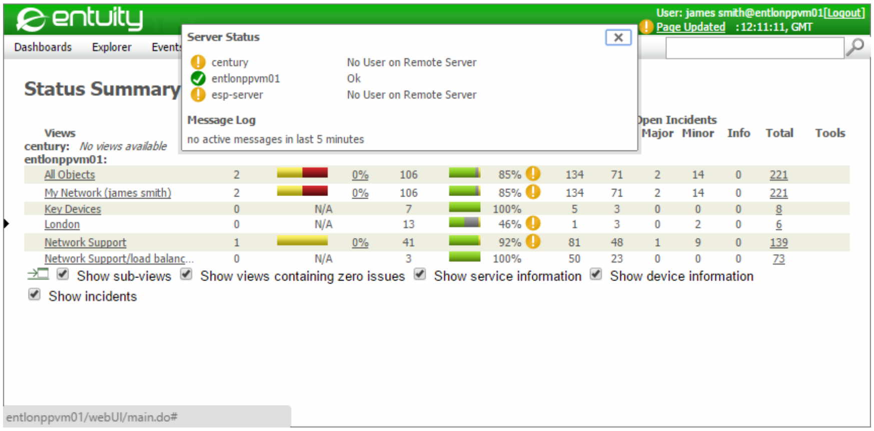
Page Updated and Page Status are indicators of the performance of your interface, however not all pages update these values. For example the event viewer is updated each time an event or incident is raised that matches the current view filter and so to for overhead reasons Entuity does not update the Page Updated state for the event viewer. Always refresh the current page if you doubt the page indicators are current.

| Attribute | Description |
|---|---|
| *Server Status* | Indicates the status of the page and Entuity servers. Entuity updates this status every time the page is updated, which by default is every five minutes. When set to:<br>■ **OK** the server is running normally. In multi-server environments the remote server considers the local server a trusted server, allowing it access.<br>■ **No Trust** the remote server may have previously allowed the local server access but has now revoked that access.<br>■ **Service Down** the server is unavailable. In multi-server environments the remote Entuity server application is down, but the server machine is responding to ping.<br>■ **Communication Failure** the remote Entuity server machine is down, i.e. not responding to ping. |
| *Message Log* | Details any messages raised in the past five minutes. |

Table 2 Page and Server Status

To check Server Status:

1) Click **Page Updated**. Entuity displays the Server Status pop-out.



entuity
User: james smith@entlonppvm01[Logout]
Page Updated :12:11:11, GMT
Dashboards
Explorer
Events
Status Summary

Server Status

| | |
|---|---|
| century | No User on Remote Server |
| entlonppvm01 | Ok |
| esp-server | No User on Remote Server |

Message Log

no active messages in last 5 minutes

| Views | | | | | | | | | Open Incidents | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Major | Minor | Info | Total | Tools |
| century: *No views available* | | | | | | | | | | | | | |
| entlonppvm01: | | | | | | | | | | | | | |
| All Objects | 2 | 🟨🟥 | 0% | 106 | 🟩 | 85% | 134 | 71 | 2 | 14 | 0 | 221 | |
| My Network (james smith) | 2 | 🟨🟥 | 0% | 106 | 🟩 | 85% | 134 | 71 | 2 | 14 | 0 | 221 | |
| Key Devices | 0 | N/A | | 7 | 🟩 | 100% | 5 | 3 | 0 | 0 | 0 | 8 | |
| London | 0 | N/A | | 13 | 🟩 | 46% | 1 | 3 | 0 | 2 | 0 | 6 | |
| Network Support | 1 | 🟨 | 0% | 41 | 🟩 | 92% | 81 | 48 | 1 | 9 | 0 | 139 | |
| Network Support/load balanc... | 0 | N/A | | 3 | 🟩 | 100% | 50 | 23 | 0 | 0 | 0 | 73 | |

☑ Show sub-views ☑ Show views containing zero issues ☑ Show service information ☑ Show device information

☑ Show incidents

Figure 4 Server Status Summary

### Browser Setup

Although Entuity works with most standard browser configurations, you must ensure that both Java and JavaScript are enabled. For example JavaScript is required to maintain session information.

Entuity requires users have installed:

- An Adobe Acrobat PDF reader to view online manuals and PDF reports.
- Telnet to use the Telnet function.
- MP4 player to play the Entuity tutorials.

You should ensure that your browser is configured to handle these applications.

The browser performance can be improved by not using web proxy servers when communicating with Entuity. This is because proxies incur delays. It is common for internal intranets to use web proxies to allow secure connection onto the external internet, but, if possible, any proxy configuration for the browser should be examined to see if exceptions which allow direct connections can be configured.

## Entuity Documentation

Entuity documentation set is aimed at all users of the product, but it is envisaged that they will principally be drawn from the following:

- Staff in the Network Operations Center (NOC), who use Entuity’s alerting capabilities to detect and fix network faults as they occur, across a wide range of situations (from routing issues to LAN cabling faults).
- Network Design Engineers, who typically focus on the performance data made available by Entuity.
- Departmental Managers, who use the above performance data to measure the performances of both the network itself and the networking staff under their control.

All users are referred to as **you** in the user documentation. Entuity documentation also identifies functionality that is only available if the user belongs to a user group with that tool permission or is only available when the user belongs to the Administrators user group.

### Documentation Resources

Entuity is supplied with user guides and reference manuals produced as PDF files, tutorial videos in the MP4 format and online help which is presented through your web browser.

You can access the help from the main Entuity menu, click:

- **Help** > **Contents** Entuity opens the home page of the help system. From this page there are links to:
  - Entuity tutorial movies.
  - Sections within the help on key features of the product.
  - The documentation page from which you can access the Entuity user guides and reference manuals which are available as PDF format files.

  - Entuity Data Dictionary. The data dictionary is useful to system administrators when developing their own Entuity configurations and scripts.
- **Help for this Page** Entuity displays the help associated with that page.

  This context sensitive help is also available from the context menu. The help context menu displays the help associated with that object, e.g. highlight an event in Event Viewer and Entuity displays help for that event.

# 2 Explore the Managed Network

You can use Explorer to navigate through the managed objects on your network. It is closely integrated with:

- Setting the context for displaying incidents and events. For example, when you highlight a device in Explorer and then click **Events** Entuity only shows incidents, and if you amend the filter events associated with that device.
- Object pages displaying the inventory and performance for the selected object, e.g. a device, port, application, CPU processor. For example, when you select a device Entuity displays an overview of the device, e.g. its name, open events, key metrics, status of its ports. You can also click through to related pages on the object, e.g. Advanced Details, Resources, Ports List.

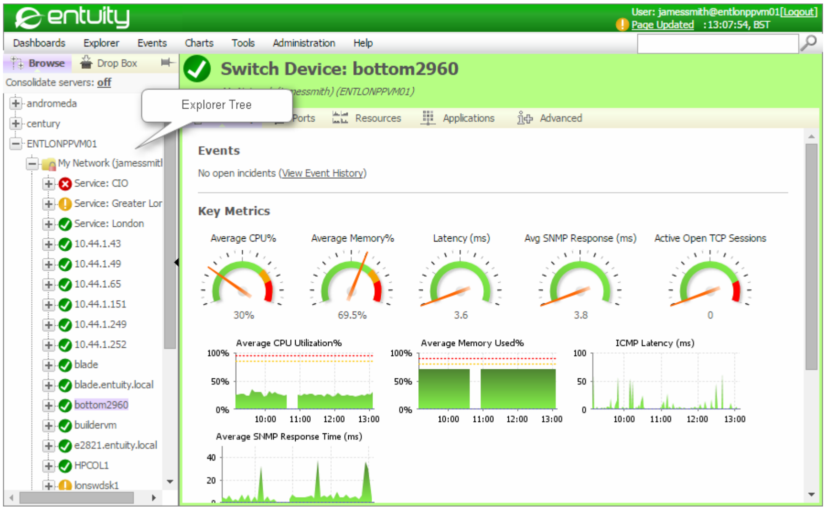


Figure 5 Explorer

## Explorer Interface

Explorer uses views to present managed devices and ports through a collapsible tree structure. In multi-server environments Entuity can present the devices and ports managed by those servers:

- Separately, so each Entuity server is listed in Explorer and below it are its views, devices and ports.
- As a consolidated whole, where the content of views with the same name on different servers is combined. Explorer does not list any Entuity servers but instead presents information as though it were managed by one server (although the managing server is clearly identified on the object summary page).

Where you are using more than one Entuity server to manage the same devices and ports, they are handled as separate objects. In consolidated mode you would see the same devices listed together.

Consolidated mode is the default state, although you can amend it through the Preferences page.

Objects in the Explorer tree have their status clearly identified through their associated icon. The tree is updated every five minutes or when traversed.

## Navigate through Explorer

You can navigate through the pages available through Explorer using the:

- Explorer tree to select the object to view, e.g. device, port.
- Tabs on the object pages to change the type of data Entuity displays on the selected object, e.g. Advanced Details, Application Details, Edit Thresholds. The type of tabs available depends upon the selected object, e.g. device, port. The current tab title and icon is highlighted in purple, the other tab names and icons are in gray.

| Icon | Tab | Description |
|---|---|---|
| i | Summary | Links to the Summary Details page of the object, e.g. device, port. |
| | Flows | From device pages links to the Entuity Integrated Flow Analyzer (IFA) page, through which you can manage the device flow collectors. From ports pages links to the Flow Details page. |
| | Ports | Available from device pages and links to the Ports List page. |
| | Resources | Available from device pages and links to the Resource List page. |
| | Applications | Available from device pages and links to the Application Details page of the device. |
| | Configuration | Available from device pages and links to the Configuration Management page of the device. |
| | Threshold | Links to the Edit Thresholds page of the object, e.g. device, port. |
| | Trace route | Available from device pages and links to the Trace route page through which you can chart the trace route history of the device. Trace route is from the Entuity server to the managed device. |
| | MIB Browser | Available from device pages and links to the MIB Browser. |
| i+ | Advanced | Links to the Advanced Details page of the object, e.g. device, port. |

Table 3 Explorer Page Icons

## Configure Columns

Throughout Entuity where data is presented through tables, for example View Summary, Audit Log, Inventory Administration pages, you often have the option of configuring which columns are displayed. These changes are saved to your customer profile and so are maintained between login sessions. Configure Columns also includes the Default Columns option which you use to revert to the original default column settings.

To configure columns:

1) Place the mouse pointer over the column heading and from the context menu select **Configure Columns**.

   You can highlight attributes and use the arrows to move columns:

   - Up, to the left on the displayed table.
   - Down, to the right on the displayed table.
   - Between the Visible and Invisible Columns to displays and hide the attributes in the table.

You can also select Default Columns to reset the table to its default state.

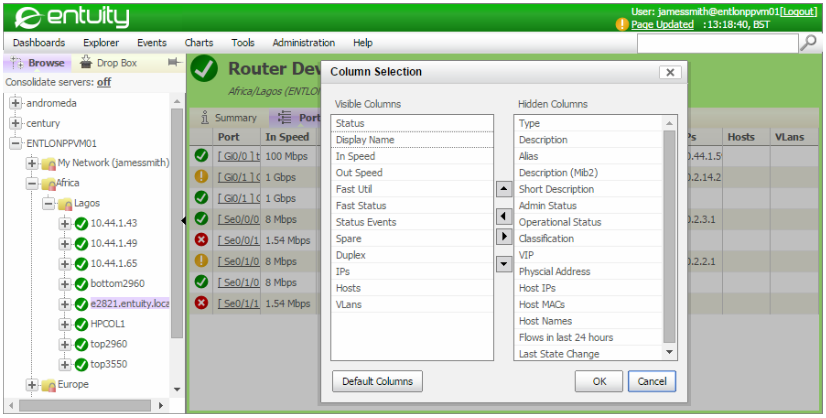


Figure 6 Configure Column Selection

## Key Metric Gauges and Charts

Entuity presents key metrics of managed objects using filled line charts and gauge graphs. From both charts you can click through to display the metric in a larger interactive chart. You can add additional metrics to interactive charts, building charts that track related metrics.

A filled line chart displays the last four hours data of a key metric. You can click on a chart to display the metric in a configurable chart.

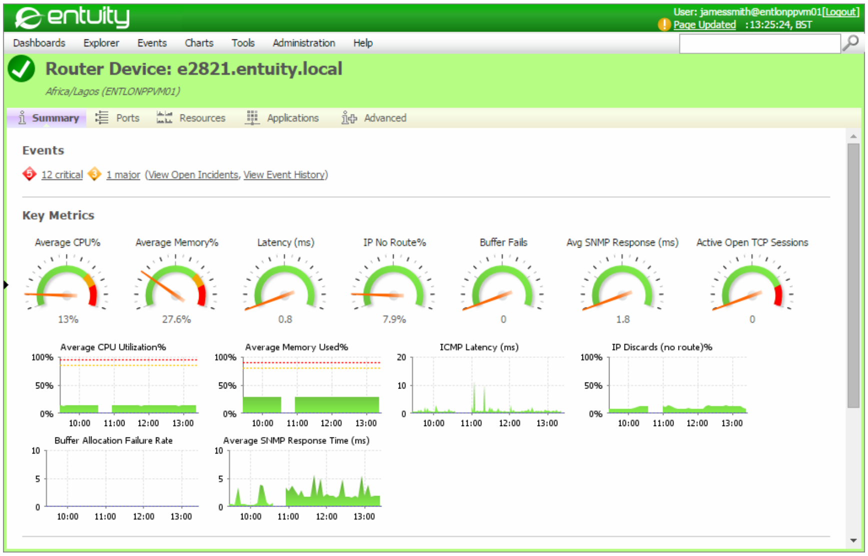


Figure 7 Key Metric Gauges and Filled Line Charts

Gauges provide an at-a-glance speedometer type view of a key metric. A label above the gauge identifies the metric, Entuity displays the last polled value of the metric below the gauge.

There are 3 types of key metric gauge graphs:

- Green only gauges are used with metrics that do not have a set threshold.
- Green and red gauges are used with metrics that have 1 set threshold.

  When gauges have set thresholds then the relative size of the red and green areas of the gauge are fixed however the relative position of the indicator does change to show the relative transgression of the threshold. When the indicator is pointing to a red area then a threshold has been crossed.

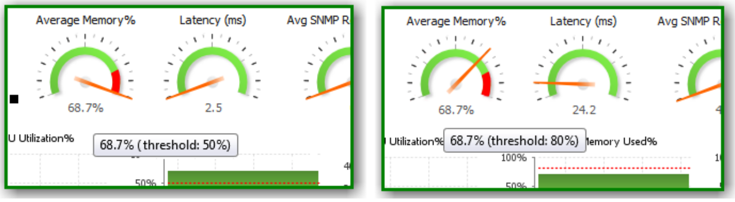


Figure 8 Same Gauge and Data with Different Threshold Levels

- Green, orange and red segmented gauges are used with metrics that have two set thresholds. Device Average CPU Usage and Device Average Memory Usage events have a two level threshold for warning and critical level events.

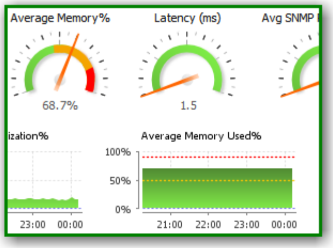


Figure 9 Gauge and Charts with 2 Set Threshold

When gauges have set thresholds then the relative size of the red area is fixed with the size of the green and orange areas of the gauge adjusted to the threshold level. When the indicator is pointing to an orange or red area then a threshold has been crossed. You can:

- View the current value of a metric and any set threshold value by passing the cursor over the data value below the graph.
- View the metric and any set threshold in the key metric charts.
- You can click on a gauge to display the metric in an interactive chart.

## Change the Display of Traffic Data

Entuity, by default, displays traffic data as utilization values. You have the option of changing the measure to by volume or rate. To amend the traffic data displays:

1) Click **Preferences**.

2) Select from *Traffic-Type* how the web UI should display traffic data, as **Utilization**, **Rate** or **Volume**.

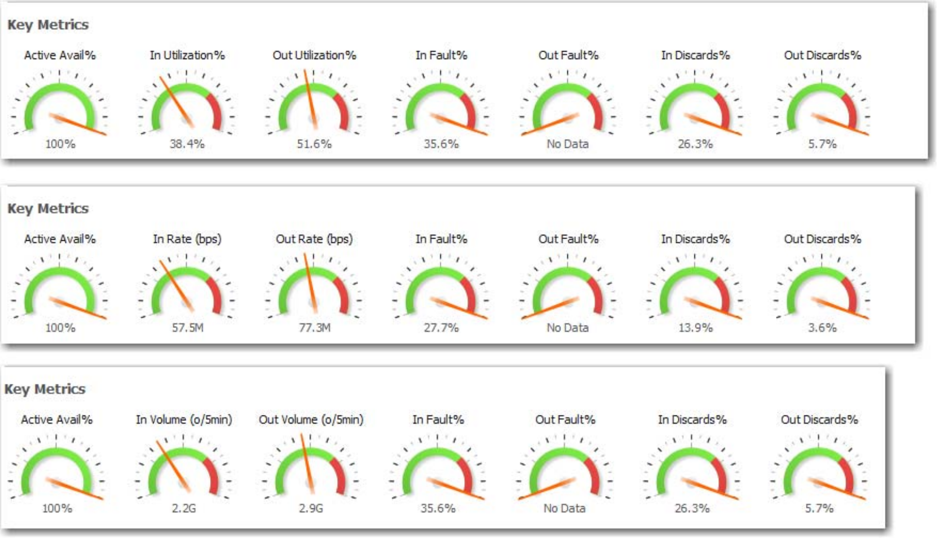


Figure 10 Three Representations of the Same Traffic Data

## Interactive Charts

You can access and graph all metrics for which Entuity maintains a history. Entuity can maintain one chart for the duration of your Entuity session, allowing you to navigate away from a chart and then return to it without losing the data streams being graphed, or any of the chart’s transient display settings, for example, zoom level, style, scaling. You can also add additional data streams to the current chart. A chart remains your current chart until you create a new chart.

You can maintain access to more than one chart in the web UI, and also maintain a chart across user sessions by assigning charts to custom dashboards. For this you require the chart URL which you can access through its **Open this chart** icon. (See *Appendix C - Entuity URLs*.)

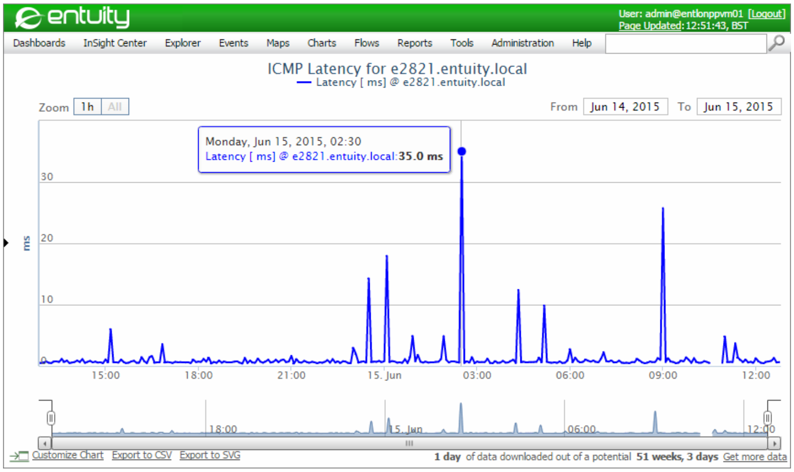

entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 12:51:43, BST
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Tools
Administration
Help
ICMP Latency for e2821.entuity.local
Latency [ ms] @ e2821.entuity.local
Zoom
1h
All
From
Jun 14, 2015
To
Jun 15, 2015
Monday, Jun 15, 2015, 02:30
Latency [ ms] @ e2821.entuity.local: 35.0 ms
ms
30
20
10
15:00
18:00
21:00
15. Jun
03:00
06:00
09:00
12:00
18:00
15. Jun
06:00
12:00
Customize Chart
Export to CSV
Export to SVG
1 day of data downloaded out of a potential 51 weeks, 3 days
Get more data

Figure 11 Active Chart

## Opening the Current Chart

To open the current chart:

1) Click **Charts**.

Entuity displays the current chart. You can amend the chart, for example drag additional data streams onto a chart from Drop Box.

When a chart is not configured Entuity displays an information message:

```
No stream attributes selected. Please select stream attributes to plot
first.
```

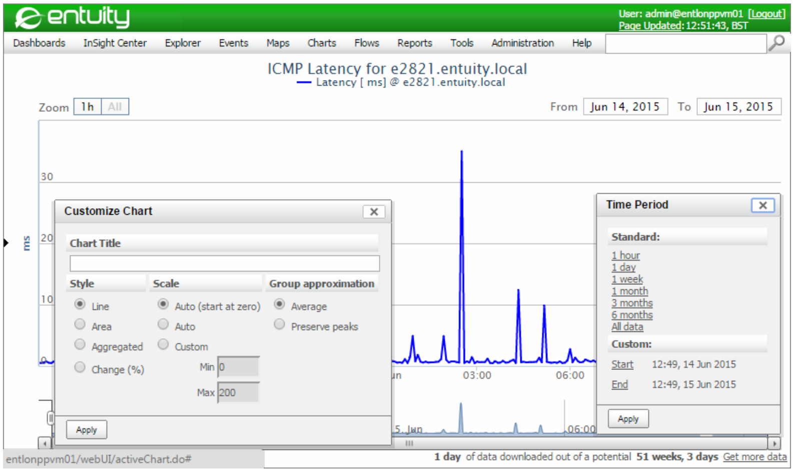
## Create a Chart

When you create a chart it automatically becomes your current chart replacing any previous chart. Entuity provides a number of methods for creating a chart:

- From the object summary pages by clicking on a gauge or filled line chart.
- By clicking on the links in the TopN dashboard page.
- By highlighting a port and from the context-menu selecting one of the options from the Graphs sub-menu.
- From a managed object’s Advanced tab, you can highlight multiple metrics and from the context-menu you can add these metrics to a new chart or add them to an existing one.

## Configure an Interactive Chart

All charts shown in the web UI include a historical timeline, to allow you to quickly and easily focus (zoom in / out) on a time frame of interest.



ICMP Latency for e2821.entuity.local

— Latency [ ms] @ e2821.entuity.local

From Jun 14, 2015 To Jun 15, 2015

Customize Chart

Chart Title

Style: ● Line ○ Area ○ Aggregated ○ Change (%)

Scale: ● Auto (start at zero) ○ Auto ○ Custom Min 0 Max 200

Group approximation: ● Average ○ Preserve peaks

Time Period

Standard: 1 hour, 1 day, 1 week, 1 month, 3 months, 6 months, All data

Custom:

Start 12:49, 14 Jun 2015

End 12:49, 15 Jun 2015

**1 day** of data downloaded out of a potential **51 weeks, 3 days** Get more data

Figure 12 Key Metric Gauge Graphs

| Feature | Description |
|---|---|
| Title | Entuity generates a default name for the chart, for example derived from the charted object and metric. You can amend the Chart Title through Customize Chart. |
| Key | Matches the line color with the managed object’s metric. You can click on an entry to show and hide the value in the chart. |
| Zoom | Entuity displays zoom levels available with the downloaded data. |
| From: / To: | Adjust the zoom level on the downloaded data. |
| Chart | Pass the mouse pointer over a point on a chart line for Entuity to display the metric type, e.g. latency, managed object source and the time the data point was taken. |
| Timeline Display | Represents the data downloaded from Entuity server, readily available for display. By default Entuity downloads one day’s worth of data. You can use the handles at each end of the timeline to set the focus of the chart. |
| Open this chart in new page | Displays the current chart in a new page. It also provides access to the chart’s URL, which you could use when including charts to custom dashboards. |
| Customize Chart | Displays the Customize Chart dialog. |
| Chart Title | You can enter a chart to replace the default chart name, although charts launched from the Advanced tab in Explorer do not have a default title. |

Table 4 Configuring Charts

| Feature | Description |
|---|---|
| Scale | The scale can be:<br>■ Auto (start at zero), the Y-axis starts at zero, but will auto scale to include the highest value on the graph.<br>■ Auto, the minimum and maximum values of the Y-axis will auto scale to include the lowest and highest values on the graph, respectively. Therefore this scale may start below or above zero.<br>■ Custom, the Y-axis scales according to the Min and Max values specified. |
| Style | The line style may be:<br>■ Line, presents each set of polled data as a separate line<br>■ Area, stacks polled datasets for the sample time<br>■ Aggregated, totals values for all polled datasets for the sample time<br>■ Change (%), where Entuity calculates the percentage change of a polled value when compared to the first sample in the chart. |
| Group Approximation | When displaying a large amount of data on a chart you can set Group Approximation to:<br>■ **Average** (default), Entuity uses a grouping algorithm to prevent the chart from becoming crowded with overlapping data points. This algorithm can lead to the loss of peak information.<br>■ **Preserve Peaks**, Entuity retains peak data points where high resolution data is available. |
| Export to CSV | Exports the current chart to CSV. |
| Attributes | Lists the attributes for export. |
| From: / To: | Adjust the report period of the chart for export. |
| Format timestamps | When:<br>■ Selected Entuity formats the date and time the data sample was taken.<br>■ Not selected Entuity presents the date and time the data sample was taken as a numeric string. |
| Format Values | When:<br>■ Selected Entuity formats the data sample values, for example limits percentage values to two decimal places and includes the percentage symbol.<br>■ Not selected Entuity exports unformatted data sample values. |
| Save as file | Sets the export to a file. |
| Show in browser | Sets the export to display the chart data in a new browser window. |
| Export to SVG | Creates an SVG file of the current chart. You can view or save the file. |
| Get more data | Displays the Time Period dialog through which you can amend the chart reporting period. |

Table 4 Configuring Charts

| Feature | Description |
|---|---|
| Standard | Select to determine how much data to download from the Entuity server to the current client. |
| Custom | Enter the start and end dates of the data polling period to set the data to download from the Entuity server to the current client. |

Table 4 Configuring Charts

## Adjust the Chart Timeline

When you open a chart it only displays data from the previous twenty-four hours. This ensures a fast download of the chart on first opening. At the bottom right of the chart Entuity displays the amount of potential data available.

You can extend the data available to the chart by selecting **Get More Data**. By default Entuity downloads data from the current time backwards, although you can request a particular period of data. On download Entuity updates the historical timeline and auto-zoom level to display all of the downloaded data.

You can adjust data displayed by using:

- The timeline at the foot of the chart, dragging its handles to zoom in
- Zoom. Entuity only displays zoom levels available with the downloaded data. The auto zoom levels offered are dependent on the amount on data downloaded to the web client, with more auto zoom levels appearing if/as more data is downloaded.

## Adding Data Streams to the Current Chart

You can build charts that have up to 10 data streams from one or more managed objects. You can add more data streams to your current chart by:

- Using Drop Box.
- Adding one or more metrics from an object’s Advanced Details page.

To develop a current chart using Drop Box:

1) Drag data streams that you want to include to the chart to drop box.
2) Click **Charts** to display the current chart.
3) Drag the required metrics from Drop Box to the chart.

To develop a current chart from an object’s Advanced Details page:

1) Navigate to the Advanced page of the managed object for which you want to graph its metrics.
2) Highlight the required metrics and from the context menu click:
   - **Show on chart**, to create a new chart that graphs the selected stream data.
   - **Add to current chart**, to add to the existing chart the selected stream data.

## Considerations for Interpreting Chart Data

Missing data points, i.e. broken lines, in charts indicate a lack of data. This may be because the Entuity server or device were down or a network issue prevented successful polling of the device. On aggregate charts Entuity may draw a line down to the nil line.

When using aggregate charts you should always use data with the same polling interval. Stream data with different polling intervals results in offset aggregation which may mislead.

## Example Peak Value Utilization

For port utilization data Entuity stores peak utilization values. Entuity charts allow you to drill down on a particular utilization stream to view its peak values.

To view and chart the peak values:

1) Create a chart containing the required port utilization data stream.

2) Within the chart click on the data stream.

   Entuity displays a new temporary chart which is a drill-down of the chosen data stream, breaking the data stream into average and peak values per sample. You can click on either line to return to the original chart.

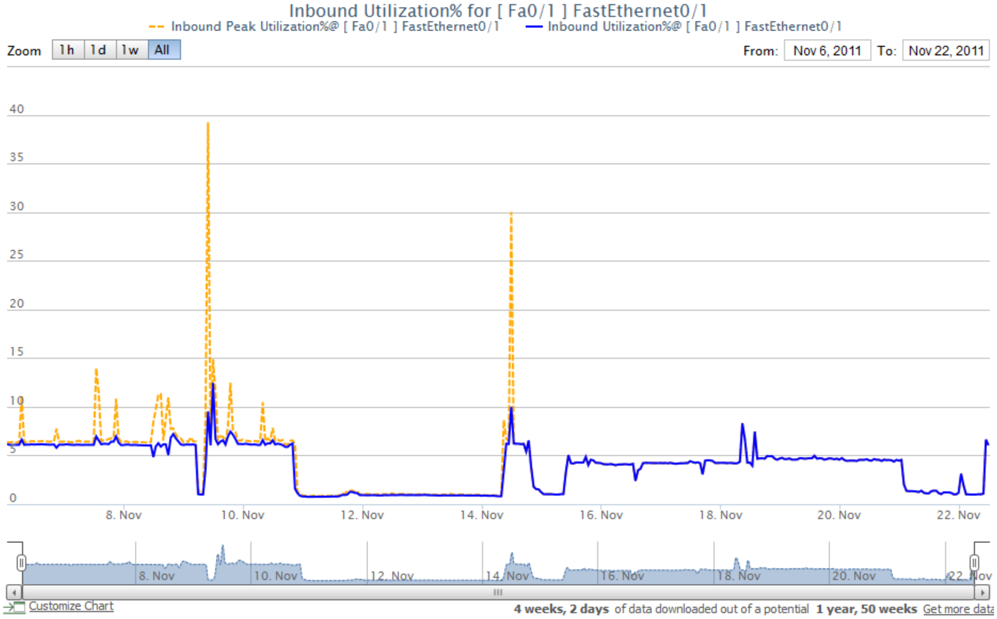


Figure 13 Peak Utilization Data Drill Down

## Example Aggregating Traffic Data

You can use the stack area charting style to quickly view the total (aggregated) value of several related data streams, for example the total in utilization across selected interfaces.

To develop a port utilization aggregate chart:

1) Navigate to the Advanced page of the first port.

2) Highlight the required *Inbound Utilization%* and from the context menu click **Show on chart**.

   Entuity creates and displays a new chart with the selected stream data.

3) Navigate to the Advanced page for each of the remaining ports, highlight *Inbound Utilization%* and from the context menu select **Add to current chart**.

4) When you have completed adding streams to the chart select from the web UI menu **Chart**, for Entuity to display the chart.

5) Select **Customize Chart** and:

   - Enter a title, e.g. Aggregated Port Utilization.
   - Select for *Style*, **Aggregated**.

6) Click **Apply** to update the chart.

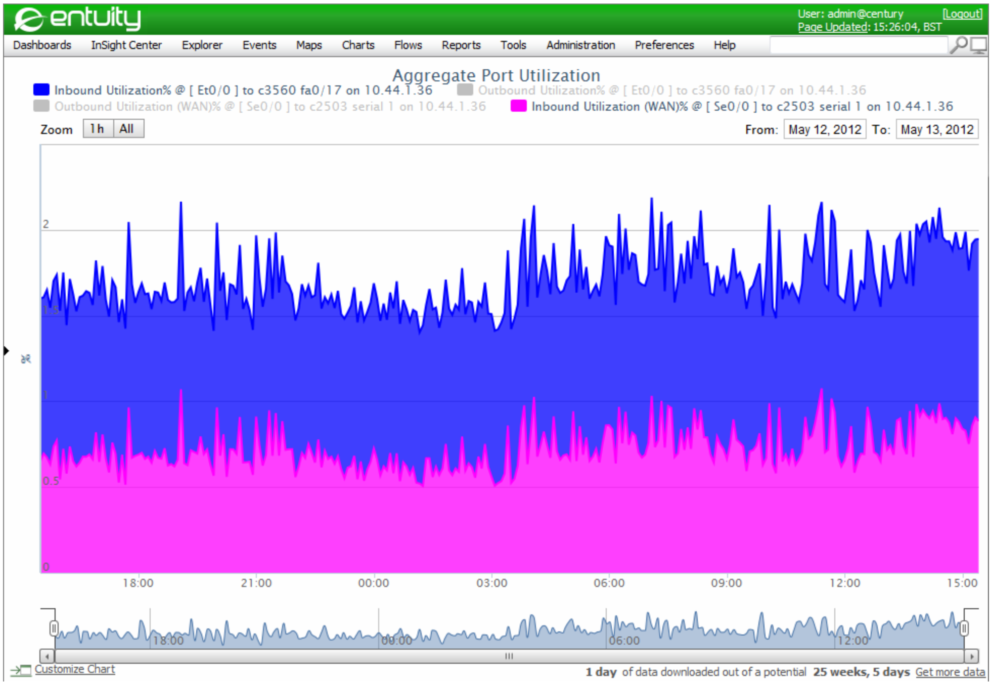

entuity
User: admin@century [Logout]
Page Updated: 15:26:04, BST
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Tools
Administration
Preferences
Help
Aggregate Port Utilization
Inbound Utilization% @ [ Et0/0 ] to c3560 fa0/17 on 10.44.1.36
Outbound Utilization% @ [ Et0/0 ] to c3560 fa0/17 on 10.44.1.36
Outbound Utilization (WAN)% @ [ Se0/0 ] to c2503 serial 1 on 10.44.1.36
Inbound Utilization (WAN)% @ [ Se0/0 ] to c2503 serial 1 on 10.44.1.36
Zoom
1h
All
From: May 12, 2012
To: May 13, 2012
2
1.5
1
0.5
0
18:00
21:00
00:00
03:00
06:00
09:00
12:00
15:00
18:00
00:00
06:00
12:00
Customize Chart
1 day of data downloaded out of a potential 25 weeks, 5 days Get more data

Figure 14 Aggregating Traffic Data

## Adding Charts to Custom Dashboards

Charts in Entuity are defined through a readily obtainable URL. All data required to display a chart is encoded in the URL, e.g. selected data streams, style, data period, zoom level, title. You can save and re-use charts by including their URL to custom dashboards. As each chart

URL is independent of any other URL you can include more than one to a custom dashboard.

A chart is included within the frame of the Entuity web UI, so its URL is not immediately visible. To recover a chart's URL:

1) From the bottom left corner of the chart:

   - Click on the **Open this chart in new page link**. Entuity opens the chart in a new page. You can copy its URL from the browser's Address bar.
   - Place the mouse pointer over the **Open this chart in new page link** icon. Depending on the browser you can now copy the URL, using options available from the browser's context menu.

   When you have copied the URL you can paste it into a custom dashboard.

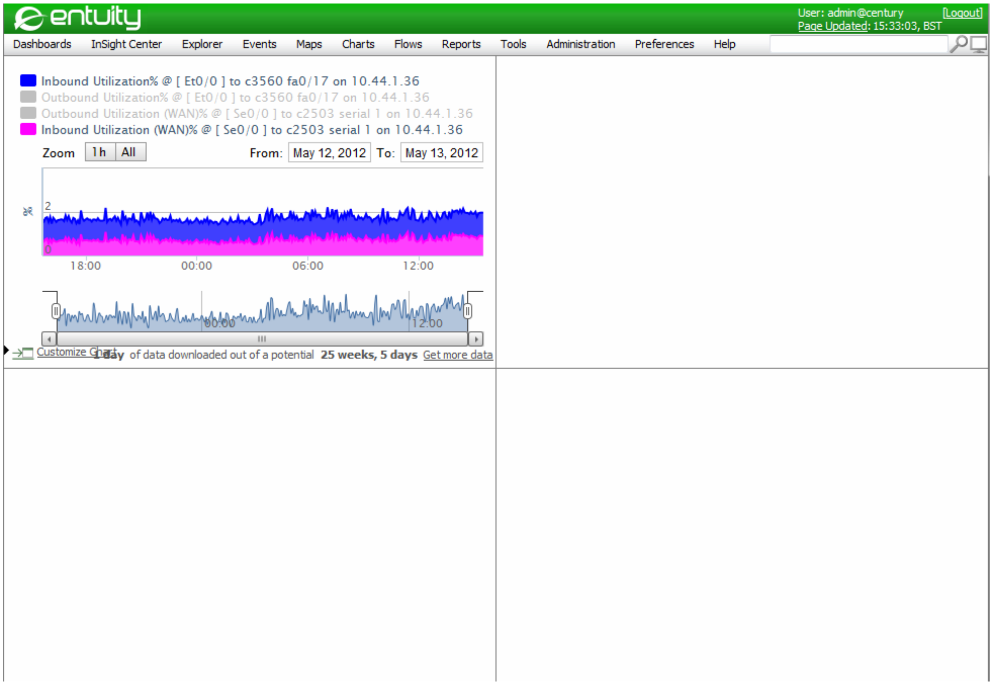

entuity
User: admin@century [Logout]
Page Updated: 15:33:03, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Preferences Help
Inbound Utilization% @ [ Et0/0 ] to c3560 fa0/17 on 10.44.1.36
Outbound Utilization% @ [ Et0/0 ] to c3560 fa0/17 on 10.44.1.36
Outbound Utilization (WAN)% @ [ Se0/0 ] to c2503 serial 1 on 10.44.1.36
Inbound Utilization (WAN)% @ [ Se0/0 ] to c2503 serial 1 on 10.44.1.36
Zoom 1h All
From: May 12, 2012 To: May 13, 2012
2
0
18:00
00:00
06:00
12:00
00:00
12:00
Customize Chart
1 day of data downloaded out of a potential 25 weeks, 5 days Get more data

Figure 15 Add a Chart to a Custom Dashboard

## Exporting Charts

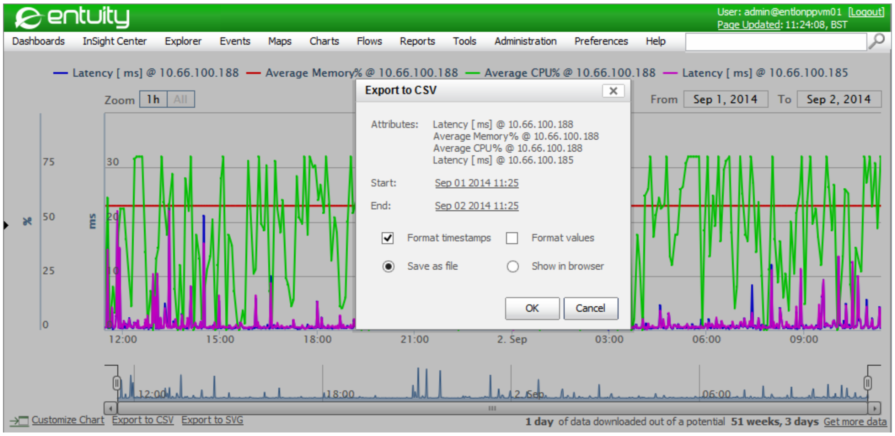
You can export the current chart to a:

- CSV file. Entuity selects the attributes in the current chart of export and through the Export to CSV dialog can amend the data format, reporting period and whether you view the data in a browser or save it to a file.
- SVG file.

To export the data in a chart to a CSV file:

1) From the bottom of the chart click on **Export to CSV**.

2) In Export to CSV specify the export configuration. (See *Configure an Interactive Chart*.)


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 11:24:08, BST
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Tools
Administration
Preferences
Help
Latency [ ms] @ 10.66.100.188
Average Memory% @ 10.66.100.188
Average CPU% @ 10.66.100.188
Latency [ ms] @ 10.66.100.185
Zoom 1h All
From Sep 1, 2014 To Sep 2, 2014
%
ms
75
50
25
0
30
20
10
12:00
15:00
18:00
21:00
2. Sep
03:00
06:00
09:00
Customize Chart
Export to CSV
Export to SVG
1 day of data downloaded out of a potential 51 weeks, 3 days Get more data

Export to CSV

Attributes: Latency [ ms] @ 10.66.100.188
Average Memory% @ 10.66.100.188
Average CPU% @ 10.66.100.188
Latency [ ms] @ 10.66.100.185

Start: Sep 01 2014 11:25

End: Sep 02 2014 11:25

☑ Format timestamps □ Format values

● Save as file ○ Show in browser

OK Cancel

Figure 16 Export Chart to CSV

# Editing Attributes

Administrators and users with the Object Editing tool permission can edit the values of scalar attributes.

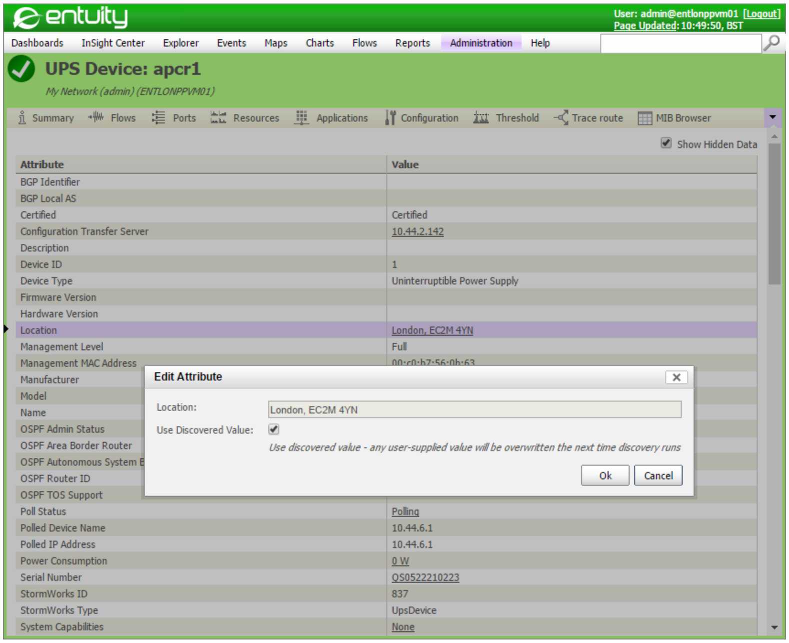
To edit the value of an attribute:

1) Navigate to the Advanced tab of the object.

   Attributes that are editable are underlined. Associations that are editable have an Edit button.

2) Click the hyperlink or Edit button, whichever is appropriate.

3) Edit the attribute value and click **OK**.



UPS Device: apcr1

*My Network (admin) (ENTLONPPVM01)*

| Attribute | Value |
|---|---|
| BGP Identifier | |
| BGP Local AS | |
| Certified | Certified |
| Configuration Transfer Server | 10.44.2.142 |
| Description | |
| Device ID | 1 |
| Device Type | Uninterruptible Power Supply |
| Firmware Version | |
| Hardware Version | |
| Location | London, EC2M 4YN |
| Management Level | Full |
| Management MAC Address | 00:c0:b7:56:0b:63 |
| Manufacturer | |
| Model | |
| Name | |
| OSPF Admin Status | |
| OSPF Area Border Router | |
| OSPF Autonomous System B | |
| OSPF Router ID | |
| OSPF TOS Support | |
| Poll Status | Polling |
| Polled Device Name | 10.44.6.1 |
| Polled IP Address | 10.44.6.1 |
| Power Consumption | 0 W |
| Serial Number | QS0522210223 |
| StormWorks ID | 837 |
| StormWorks Type | UpsDevice |
| System Capabilities | None |

Edit Attribute

Location: London, EC2M 4YN

Use Discovered Value: ☑

*Use discovered value - any user-supplied value will be overwritten the next time discovery runs*

Figure 17 Edit Attribute

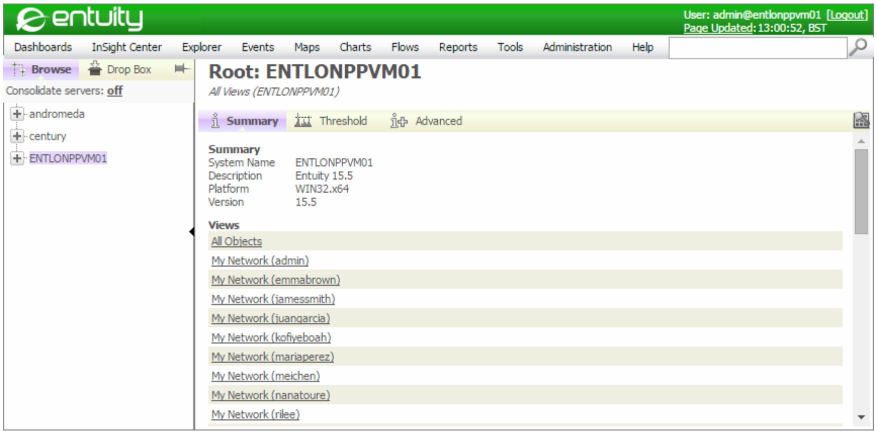
## Accessing Explorer

Explorer is available through the web UI menu. What Explorer displays when you first open it depends upon what object you had selected when you opened it. For example, when you:

- Do not select an object, e.g. you access Explorer immediately after logging into Entuity, the left pane shows available servers, the right remains blank.
- Select a device Explorer displays Device Summary Details.

To access Explorer:

1) Click **Explorer**.



Root: ENTLONPPVM01

*All Views (ENTLONPPVM01)*

Summary

| | |
|---|---|
| System Name | ENTLONPPVM01 |
| Description | Entuity 15.5 |
| Platform | WIN32.x64 |
| Version | 15.5 |

Views

All Objects
My Network (admin)
My Network (emmabrown)
My Network (jamessmith)
My Network (juangarcia)
My Network (kofiyeboah)
My Network (mariaperez)
My Network (meichen)
My Network (nanatoure)
My Network (rilee)

Figure 18 Entuity Explorer

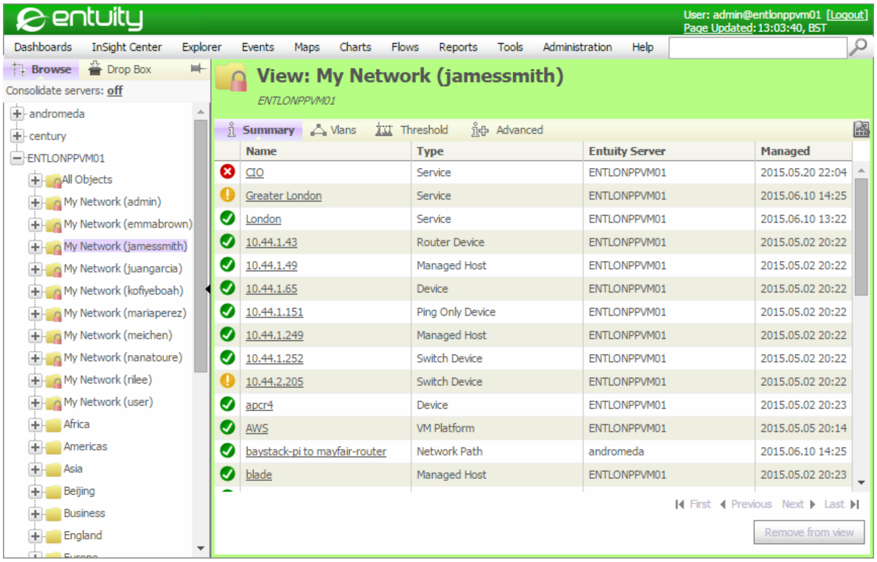
# Viewing Objects through Explorer

Using Explorer allows you to immediately view details of a selected Entuity object, for example a list of devices in a view, attributes of a device, attributes of a port.

To list devices in a view:

1) Click **Explorer**.

2) Use the Explorer pane to select the view. Entuity displays the View summary details.



View: My Network (jamessmith)

*ENTLONPPVM01*

| | Name | Type | Entuity Server | Managed |
|---|---|---|---|---|
| ✗ | CIO | Service | ENTLONPPVM01 | 2015.05.20 22:04 |
| ! | Greater London | Service | ENTLONPPVM01 | 2015.06.10 14:25 |
| ✓ | London | Service | ENTLONPPVM01 | 2015.06.10 13:22 |
| ✓ | 10.44.1.43 | Router Device | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.49 | Managed Host | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.65 | Device | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.151 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.249 | Managed Host | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.252 | Switch Device | ENTLONPPVM01 | 2015.05.02 20:22 |
| ! | 10.44.2.205 | Switch Device | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | apcr4 | Device | ENTLONPPVM01 | 2015.05.02 20:23 |
| ✓ | AWS | VM Platform | ENTLONPPVM01 | 2015.05.05 20:14 |
| ✓ | baystack-pi to mayfair-router | Network Path | andromeda | 2015.06.10 14:25 |
| ✓ | blade | Managed Host | ENTLONPPVM01 | 2015.05.02 20:23 |

Figure 19 Explorer View Summary

# Explore Entuity Server Details

You can view Entuity server details using these tabs:

- Summary, provides an overview of the server's details, e.g. its system name, installed to platform, version number, and links to its views to which you have access.
- Threshold, through which you can apply threshold settings for one or more event types at the server level.
- Advanced Details tab, includes details grouped as:
  - Attributes, repeats attributes given in Summary tab and also the internal StormWorks identifier.
  - Stream Attributes, provides a summary of events raised against the server. Event Description and Event Summary through a context menu both allow opening of a Change History dialog.
  - Associations, provides links to Services, Views, Devices, Remote Servers and Zones associated with the server to which you have access.

When you run Entuity server, and those servers are unconsolidated, Entuity server consolidation is configured through the web UI Preferences. Entuity server consolidation is configured through the web UI Preferences.

| Attribute | Description |
|---|---|
| *System Name* | Name of the Entuity server. |
| *Description* | Name and version of the Entuity software, e.g. Entuity 15.5. |
| *Platform* | Environment to which Entuity is installed, e.g. WIN32.x64, Linux.64. |
| *Version* | Internal identifier of the Entuity version, e.g. 15.5. |
| *Views* | Entuity views on the server, e.g. All Objects, London Office. Each view name is a hyperlink to a view summary. |

Table 5 Entuity Server Details in Explorer

To Click Entuity server details:

1) Click **Explorer**.

2) Use the Explorer pane to select the Entuity server. Entuity displays the server Summary tab. Also available are the:

   - Threshold tab, through which you can apply threshold settings for one or more event types at the server level. (See *Review Thresholds*.)

- Advanced Details tab, details.

# Review Thresholds

From the thresholds page you can review the current threshold settings for the selected object, for example an Entuity server, view, device, port. If you select in Explorer:

- An Entuity server then you have an extensive set of objects to set thresholds against, for example devices, ports, processes.
- A port then you have a more restricted set of objects to set thresholds against, for example ports, MPLS.
- A view then you can only set the device view reachability threshold.

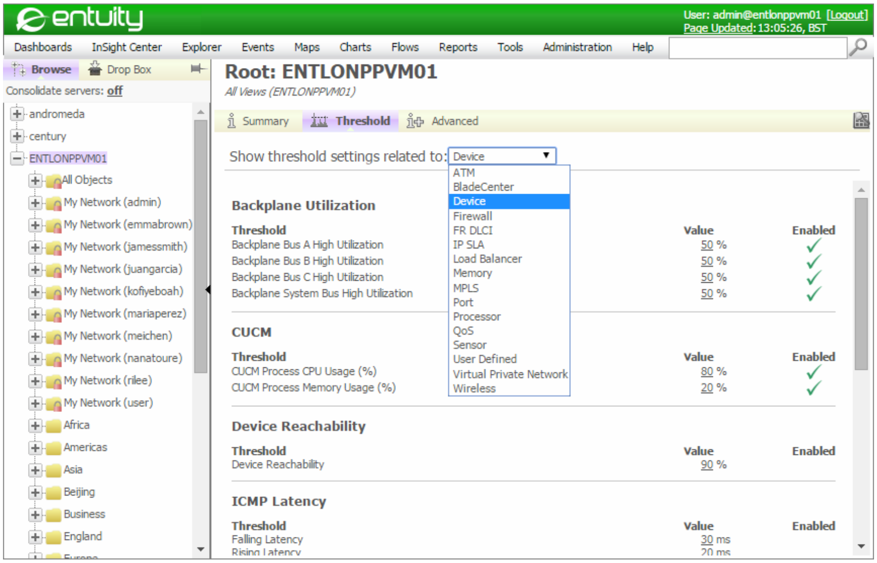
Thresholds can be set against the same object type but at different levels of the thresholds hierarchy. A value set lower in the hierarchy takes precedence over values set higher in the tree. For example if you amend a port utilization threshold at the device level it would not override any values previously set directly against individual ports.

To review threshold settings for an object:

1) Click **Explorer**.

2) Use the Explorer pane to select the object, for example an Entuity server.

3) Click **Thresholds** and from *Show thresholds settings related to* select the object type for which you want to review the threshold settings.



Root: ENTLONPPVM01

*All Views (ENTLONPPVM01)*

Show threshold settings related to: Device

**Backplane Utilization**

| Threshold | Value | Enabled |
|---|---|---|
| Backplane Bus A High Utilization | 50 % | ✓ |
| Backplane Bus B High Utilization | 50 % | ✓ |
| Backplane Bus C High Utilization | 50 % | ✓ |
| Backplane System Bus High Utilization | 50 % | ✓ |

**CUCM**

| Threshold | Value | Enabled |
|---|---|---|
| CUCM Process CPU Usage (%) | 80 % | ✓ |
| CUCM Process Memory Usage (%) | 20 % | ✓ |

**Device Reachability**

| Threshold | Value | Enabled |
|---|---|---|
| Device Reachability | 90 % | |

**ICMP Latency**

| Threshold | Value | Enabled |
|---|---|---|
| Falling Latency | 30 ms | |
| Rising Latency | 20 ms | |

Figure 20 Display Threshold Settings

## Explore Entuity Views

When you select a view in Explorer Entuity can display one of these tabs:

- Summary lists the devices, services, network paths (if you have access to a SurePath server) within the view.
- Vlans lists the VLANs within the view.

- Configuration allows you to view a summary of the configuration monitor setups of devices in the view. (See *Device Configuration by View*.)
- Thresholds allows you to view the current threshold settings, by object type, within the view. You can also amend those settings. (See *Review Thresholds*.)
- Advanced allows you to access view attributes, stream attributes and associated views.

## View Summary

Entuity Explorer details for the selected view a summary of devices in the view. The columns in the table are configurable, place the pointer over the column headings and open the context menu.

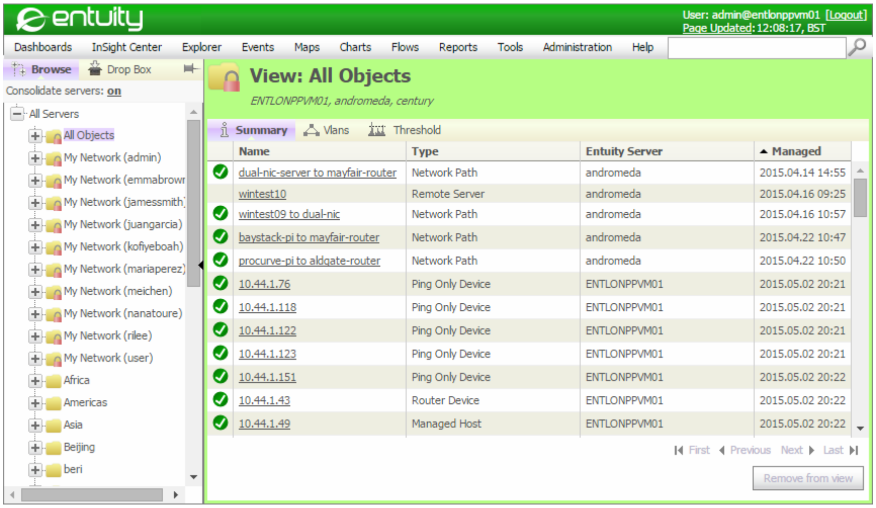
| Attribute | Description |
|---|---|
| *View Name* | Name of the Entuity view. |
| *Server name* | Name of the Entuity server, or servers when in consolidated mode in a multi-server environment. Servers to which you are currently not connected are listed in red. You can move your mouse over a server to reveal the connection failure, e.g. No Trust, Communication Failure, as a tooltip. |
| This section lists details of devices within the view. | |
| Status icon | Is set to red when the device is down, green when it is up and grey when unknown (e.g. for unmanaged devices). You can move your mouse over the icon to reveal more details on its current state as a tooltip. |
| *Device Name* | Resolved name or management IP address of the device. You can click on the name to open the Device Summary page. |
| *Type* | Entuity device type. |
| *Entuity Server* | Name of the Entuity server managing the device. |
| *Worst Event* | Event icon that indicates the severity of the open event against the device with the highest severity level. Moving the mouse over the icon reveals the event name as a tooltip. |

Table 6 Explorer Views

To list devices in a view:

1) Click **Explorer**.

2) Use the Explorer pane to select the view. Entuity displays the View summary details.



View: All Objects

*ENTLONPPVM01, andromeda, century*

| | Name | Type | Entuity Server | ▲ Managed |
|---|---|---|---|---|
| ✓ | dual-nic-server to mayfair-router | Network Path | andromeda | 2015.04.14 14:55 |
| | wintest10 | Remote Server | andromeda | 2015.04.16 09:25 |
| ✓ | wintest09 to dual-nic | Network Path | andromeda | 2015.04.16 10:57 |
| ✓ | baystack-pi to mayfair-router | Network Path | andromeda | 2015.04.22 10:47 |
| ✓ | procurve-pi to aldgate-router | Network Path | andromeda | 2015.04.22 10:50 |
| ✓ | 10.44.1.76 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:21 |
| ✓ | 10.44.1.118 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:21 |
| ✓ | 10.44.1.122 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:21 |
| ✓ | 10.44.1.123 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:21 |
| ✓ | 10.44.1.151 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.43 | Router Device | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.49 | Managed Host | ENTLONPPVM01 | 2015.05.02 20:22 |

Figure 21 Consolidated Explorer Showing All Objects View

## View VLANs

Entuity Explorer details for the selected view a summary of VLANs in the view. The columns in the table are configurable, place the pointer over the column headings and open the context menu and click **Configure Columns**. (See *Configure Columns*.)

| Attribute | Description |
|---|---|
| *View Name* | Name of the Entuity view. |
| *Server name* | Name of the Entuity server, or servers when in consolidated mode in a multi-server environment. Servers to which you are currently not connected are listed in red. You can move your mouse over a server to reveal the connection failure, e.g. No Trust, Communication Failure, as a tooltip. |
| This section lists details of VLANs within the view. | |
| VLAN | VLAN identifier, which is also a hyperlink to the VLAN’s Summary page. |
| *Entuity Server* | Name of the Entuity server managing the device. |
| *Devices* | Number of devices under management in the VLAN. |
| *Ports* | Number of ports under management in the VLAN. |

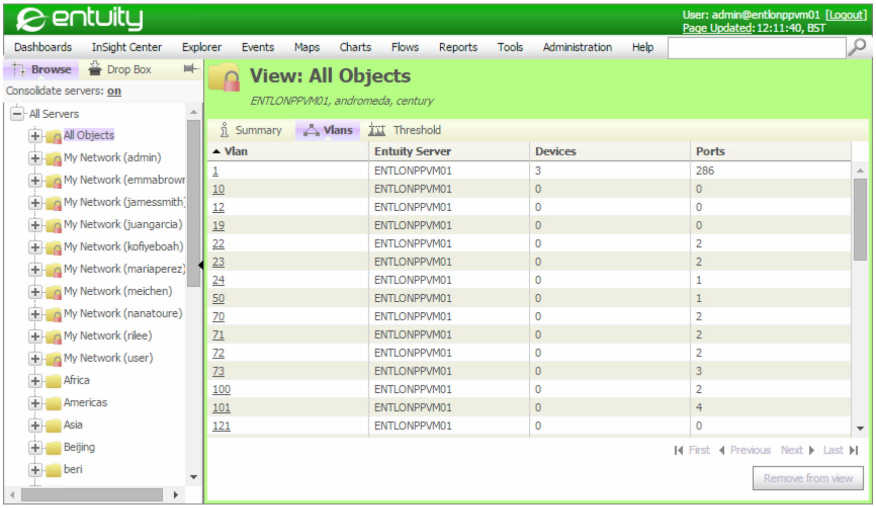
Table 7 VLANs in a View

To list VLANs in a view:

1) Click **Explorer**.

2) Use the Explorer pane to select the view. Entuity displays the View summary details.

3) Click **Vlans**.



View: All Objects

ENTLONPPVM01, andromeda, century

| Vlan | Entity Server | Devices | Ports |
|---|---|---|---|
| 1 | ENTLONPPVM01 | 3 | 286 |
| 10 | ENTLONPPVM01 | 0 | 0 |
| 12 | ENTLONPPVM01 | 0 | 0 |
| 19 | ENTLONPPVM01 | 0 | 0 |
| 22 | ENTLONPPVM01 | 0 | 2 |
| 23 | ENTLONPPVM01 | 0 | 2 |
| 24 | ENTLONPPVM01 | 0 | 1 |
| 50 | ENTLONPPVM01 | 0 | 1 |
| 70 | ENTLONPPVM01 | 0 | 2 |
| 71 | ENTLONPPVM01 | 0 | 2 |
| 72 | ENTLONPPVM01 | 0 | 2 |
| 73 | ENTLONPPVM01 | 0 | 3 |
| 100 | ENTLONPPVM01 | 0 | 2 |
| 101 | ENTLONPPVM01 | 0 | 4 |
| 121 | ENTLONPPVM01 | 0 | 0 |

Figure 22 Consolidated Explorer Showing VLANs in a View

## Viewing Device Summary through Explorer

The Device Summary page accessible through Explorer provides a summary of the selected device’s inventory and performance, with links to more detailed pages.

| Attribute | Description |
|---|---|
| Page icons | Link to other pages that display details on this device, e.g. Device Advanced Details page. (See *Navigate through Explorer*.) |
| *Device Name* | Identifies device type and resolved name/IP address, e.g. Router Device: 10.44.1.39. |
| *View(Server)* | Name of the Entuity view and server, e.g. All Objects (COMPRESSOR). |
| Events section displays the number of open events, and the severity level of the open event with the highest severity level. You can click through to open Event Viewer which displays the open events for the device. | |
| Key Metrics section includes gauge and line graphs of key metrics for the device. (See *Key Metric Gauges and Charts*.) | |
| *CPU utilization %* | Indicates the average CPU utilization over the previous polling period, expressed as a percentage of total available CPU. |
| *Average Memory %* | Indicates the average memory utilization over the previous polling period, expressed as a percentage of total available memory. |
| *ICMP Latency (ms)* | Average latency value to the device from Entuity over the polling period. |
| *IP No Route %* | Number of outbound discards expressed as a percentage of total traffic volume transmitted by the device during the polling period. |

Table 8 Device Summary Page

| Attribute | Description |
|---|---|
| *Buffer Allocation Failure Rate* | Rate of buffer allocation failures during the polling period. |
| Ports Section indicates the state of ports on the device. | |
| Port Icon | Each port is represented by an icon, its color indicating its status:<br>■ red indicates the port is administratively up but operationally down<br>■ green indicates the port is administratively and operationally up<br>■ grey indicates the port is administratively and operationally down.<br>You can click on each port to view the Port Summary page. Explorer updates to show the selected port. |
| Flow Summary Section indicates the state of flow summary collection on the device. | |
| *Description* | Provides an overview of flow data collected on the device over the previous twenty-four hours, including:<br>■ Flow packet version, e.g. NetFlow V5<br>■ Number of interfaces sending data<br>■ Average flow packet rate over the last hour<br>■ Unrecognized flow packets over the last hour. |
| General Info section provides device identifying details: | |
| *Management Level* | Level of device management, i.e. Full, Full (Mgmt Port Only), Full Management (No Ports), Basic, Ping Only |
| *Certified* | Fully managed devices can be either certified (have a vendor file created by Entuity) or uncertified (a vendor file created automatically by `proliferate`). |
| *Manufacturer* | Manufacturer name and is derived by matching the manufacturer number against the first 2500 Private Enterprise Codes compiled by the Internet Assigned Numbers Authority (http://www.iana.org/assignments/enterprise-numbers). Where the manufacturer code is not matched then the first part of the device name is taken, usually this is the manufacturer's name. |
| *Model* | Device model. |
| *Version* | Device version number. |
| *Serial Number* | Device serial number. |
| *Polled IP Address* | Management IP address Entuity uses to poll the device. |
| *Last Reboot Time* | Time of the last device reboot. |
| *Managed Since* | Date and time Entuity took the device under management. |
| *Display Name* | Name of the device as displayed in Entuity. |

Table 8 Device Summary Page

To view the device summary:

1) Click **Explorer**.

2) Use the Explorer pane to select the device. Entuity displays the Device Summary page, highlighting its tab. (See *Navigate through Explorer*.)

# Viewing Device Advanced Details

The Device Advanced Details page is for advanced users.It provides:

- Access to key details.
- Access to raw and internal attributes by clicking Show Hidden Data.
- Access to the Edit Attribute tool which is available for scalar attributes; attributes for which a change history is not retained. Clicking on the value of an attribute (it is underlined) opens the Edit Attribute tool.

The content of the Device Advanced Details page varies according to the device type and the enabled modules. This table indicates the type of available information.

| Attribute | Description |
|---|---|
| Page icons | Links to other pages that display details on this device, e.g. Device Advanced Details page. (See *Navigate through Explorer*.) |
| *Device Name* | Identifies device type and resolved name\IP address, e.g. Router Device: 10.44.1.39. |
| *View(Server)* | Name of the Entuity view and server, e.g. All Objects (COMPRESSOR). |
| *System Description* | Device description. |
| *Manufacturer* | Manufacturer name and is derived by matching the manufacturer number against the first 2500 Private Enterprise Codes compiled by the Internet Assigned Numbers Authority (http://www.iana.org/assignments/enterprise-numbers). Where the manufacturer code is not matched then the first part of the device name is taken, usually this is the manufacturer's name. |
| *Model* | Device model. |
| *Name* | Resolved name or IP address of the device. |
| *Polled IP Address* | IP address Entuity uses to poll the device. |
| *Serial Number* | Device serial number. |
| *Version* | Device version number. |
| Stream Attributes section provides latest values for port attributes for which Entuity maintains a history. | |
| *Event Description* | Description of the last event raised against the device, including event type, source and impacted details. |
| *Events Summary* | Short description of raised events. |
| Association section provides details and hyperlinks from the device to its associations. | |

Table 9 Device Advanced Details

| Attribute | Description |
|---|---|
| Association | Type of associations depend upon the device, for example:<br>■ Monitored Device, displayed when the device is a managed host.<br>■ Router Buffers<br>■ Modules<br>■ OSPF Peers<br>■ EIGRP Peers<br>■ BGP Peers<br>■ Processors Processor<br>■ Power Supplies<br>■ Ports<br>■ Memory Pools Processor. |

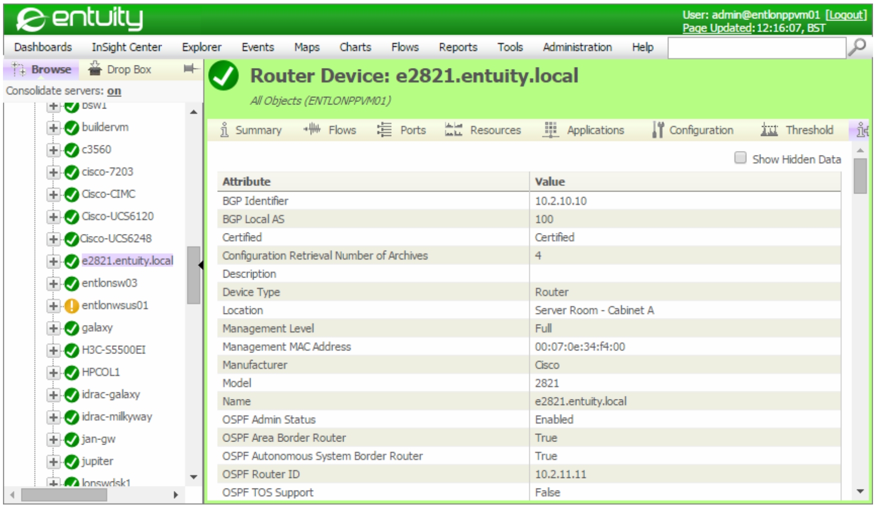
Table 9 Device Advanced Details

To view device Advanced Details:

1) Click **Explorer**.

2) Use the Explorer pane to select the device.

3) Click the Advanced Details icon. Entuity displays the Advanced Details details page, changing its tab to purple. (See *Navigate through Explorer*.)



Router Device: e2821.entuity.local

*All Objects (ENTLONPPVM01)*

| Attribute | Value |
|---|---|
| BGP Identifier | 10.2.10.10 |
| BGP Local AS | 100 |
| Certified | Certified |
| Configuration Retrieval Number of Archives | 4 |
| Description | |
| Device Type | Router |
| Location | Server Room - Cabinet A |
| Management Level | Full |
| Management MAC Address | 00:07:0e:34:f4:00 |
| Manufacturer | Cisco |
| Model | 2821 |
| Name | e2821.entuity.local |
| OSPF Admin Status | Enabled |
| OSPF Area Border Router | True |
| OSPF Autonomous System Border Router | True |
| OSPF Router ID | 10.2.11.11 |
| OSPF TOS Support | False |

Figure 23 Explorer Device Advanced Details

## Viewing Ports Associated with Devices

The Port Lists page lists the Entuity managed ports on the device. It is accessible through Explorer.

| Attribute | Description |
|---|---|
| Page icons | Links to other pages that display details on this device, e.g. Device Advanced Details page. (See *Navigate through Explorer.*) |
| *Device Name* | Identifies device type and resolved name/IP address, e.g. Router Device: 10.44.1.39. |
| *View(Server)* | The name of the Entuity view and server, e.g. All Objects (COMPRESSOR). |
| *Port* | Identifies the port, e.g. Port: [ 00028 ] Vlan1. The color of the icon indicates the port status:<br>■ red indicates the port is administratively up but operationally down<br>■ green indicates the port is administratively and operationally up<br>■ grey indicates the port is administratively and operationally down. |
| *Inbound Speed* | Inbound speed of a port operating asymmetric inbound and outbound speeds.<br>For use in Entuity your System Administrator can amend the port inbound speed. |
| *Outbound Speed* | Outbound speed of a port operating asymmetric inbound and outbound speeds.<br>For use in Entuity your System Administrator can amend the port outbound speed. |
| *Spare* | Indicates whether Entuity considers the port in use or spare |
| *IPs* | IP addresses associated with the interface. |
| *Hosts* | Lists hosts which use the interface. |
| *VLANs* | VLANs to which the interface is associated. |

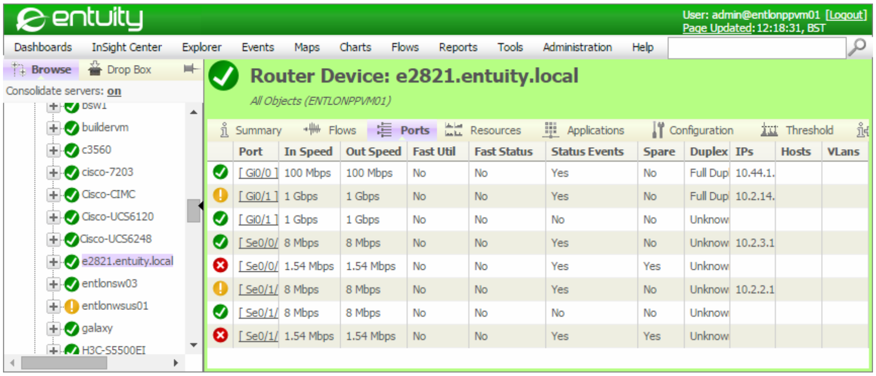
Table 10 Device Ports List

To view device ports list details:

1) From the web interface select **Explorer**.

2) Use the Explorer pane to select the device.

3) Select the Ports List icon. Entuity displays the Ports List page, changing its tab to purple. (See *Navigate through Explorer*.)



Router Device: e2821.entuity.local

*All Objects (ENTLONPPVM01)*

| | Port | In Speed | Out Speed | Fast Util | Fast Status | Status Events | Spare | Duplex | IPs | Hosts | VLans |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | [ Gi0/0 ] | 100 Mbps | 100 Mbps | No | No | Yes | No | Full Dup | 10.44.1. | | |
| ! | [ Gi0/1 ] | 1 Gbps | 1 Gbps | No | No | Yes | No | Full Dup | 10.2.14. | | |
| ✓ | [ Gi0/1 ] | 1 Gbps | 1 Gbps | No | No | No | No | Unknow | | | |
| ✓ | [ Se0/0/ | 8 Mbps | 8 Mbps | No | No | Yes | No | Unknow | 10.2.3.1 | | |
| ☒ | [ Se0/0/ | 1.54 Mbps | 1.54 Mbps | No | No | Yes | Yes | Unknow | | | |
| ! | [ Se0/1/ | 8 Mbps | 8 Mbps | No | No | Yes | No | Unknow | 10.2.2.1 | | |
| ✓ | [ Se0/1/ | 8 Mbps | 8 Mbps | No | No | No | No | Unknow | | | |
| ☒ | [ Se0/1/ | 1.54 Mbps | 1.54 Mbps | No | No | Yes | Yes | Unknow | | | |

Figure 24 Port List Details

# Viewing Device Resources

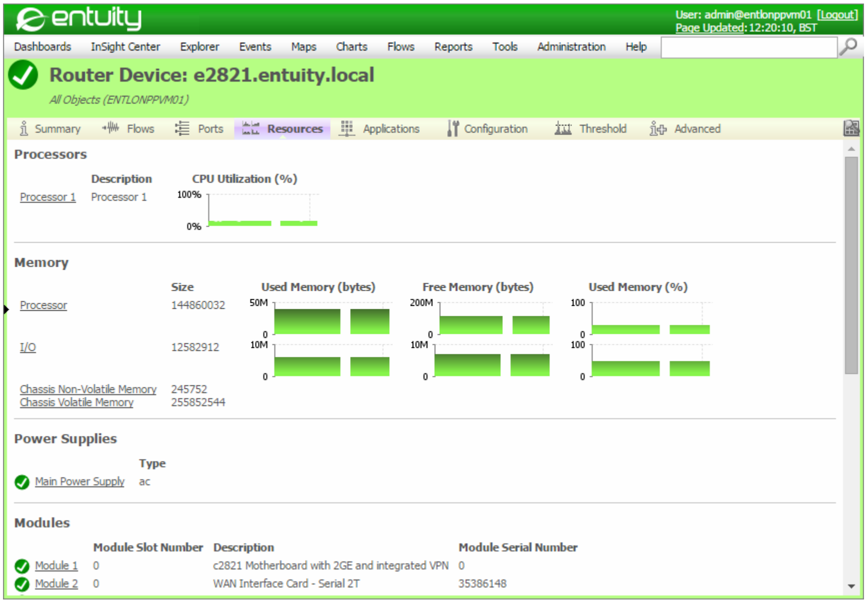
The Device Resource page accessible through Explorer provides an overview of the current state of key resources, including hyperlinks to detailed pages on those resources.

| Attribute | Description |
|---|---|
| Page icons | Links to other pages that display details on this device, e.g. Device Advanced Details page. (See *Navigate through Explorer*.) |
| *Device Name* | Identifies device type and resolved name/IP address, e.g. Router Device: 10.44.1.39. |
| *View(Server)* | The name of the Entuity view and server, e.g. All Objects (COMPRESSOR). |
| Processors section | |
| Name | Name of the processor, and includes a hyperlink to the Processor Summary page. |
| *Description* | Description of the processor, e.g. its role. |
| *CPU Utilization %* | Graphs last twenty-four hours of CPU utilization as a percentage of total utilization. You can click on the graph to view the configurable graph. |
| Memory Pools section displays details on the device memory blocks. The types of memory pool Entuity identifies include Fast, Processor, I/O, MALLOC. | |
| *Used Memory (total)* | Number of used bytes in the memory pool. |
| *Free Memory (total)* | Number of unused bytes in the memory pool. |
| *Free Memory (contiguous)* | Largest number of unused contiguous blocks in the pool. |
| Power Supplies section | |
| Icon | Power supply state icon. |

Table 11 Device Memory Pool Status

| Attribute | Description |
|---|---|
| *Name* | Name of the power supply, and includes a hyperlink to the Processor Summary page. |
| *Type* | Power supply type. |
| Modules section | |
| Icon | Module state icon. |
| *Module Name* | Name of the module, and includes a hyperlink to the Module Summary page. |
| *Module Slot Number* | Module slot number. |
| *Description* | Description of the module. |
| *Module Serial Number* | Module serial number. |
| Router Buffers section | |
| *Name* | Name of the buffer, and includes a hyperlink to the Router Buffer Summary page. |
| *Buffer Utilization%* | Buffer utilization for the last twenty-four hours expressed as a percentage of total buffer capacity. |
| Fan section | |
| Icon | Fan state icon. |
| *Fan Name* | Name of the fan, and includes a hyperlink to the Fan Summary page. |

Table 11 Device Memory Pool Status



Router Device: e2821.entuity.local

All Objects (ENTLONPPVM01)

Processors

| | Description | CPU Utilization (%) |
|---|---|---|
| Processor 1 | Processor 1 | |

Memory

| | Size | Used Memory (bytes) | Free Memory (bytes) | Used Memory (%) |
|---|---|---|---|---|
| Processor | 144860032 | | | |
| I/O | 12582912 | | | |
| Chassis Non-Volatile Memory | 245752 | | | |
| Chassis Volatile Memory | 255852544 | | | |

Power Supplies

| | Type |
|---|---|
| ✓ Main Power Supply | ac |

Modules

| | Module Slot Number | Description | Module Serial Number |
|---|---|---|---|
| ✓ Module 1 | 0 | c2821 Motherboard with 2GE and integrated VPN | 0 |
| ✓ Module 2 | 0 | WAN Interface Card - Serial 2T | 35386148 |

Figure 25 Device Resource Details

## Viewing Port Summary through Explorer

The Port Summary page accessible through Explorer provides a summary of event status, key metrics and general information on the port.

| Attribute | Description |
|---|---|
| Icons | Link to other pages that display details on this device, e.g. Port Advanced Details page. (See *Navigate through Explorer*.) |
| *Port Name* | Identifies the port, e.g. Port: [ 00028 ] Vlan1. The color of the icon indicates the port status:<br>■ red indicates the port is administratively up but operationally down<br>■ green indicates the port is administratively and operationally up<br>■ grey indicates the port is administratively and operationally down. |
| *View(Server)* | Name of the Entuity view and server, e.g. All Objects (COMPRESSOR). |
| Events section displays the number of open events, and the severity level of the open event with the highest severity level. You can click through to open Event Viewer which displays the open events for the port. | |
| Key Metrics section includes gauge and line graphs of key metrics for the port. (See *Key Metric Gauges and Charts*.) | |
| *Active Availability %* | The time both the port's Administrative and Operation statuses were up during the poll period, expressed as a percentage of the total poll period. |

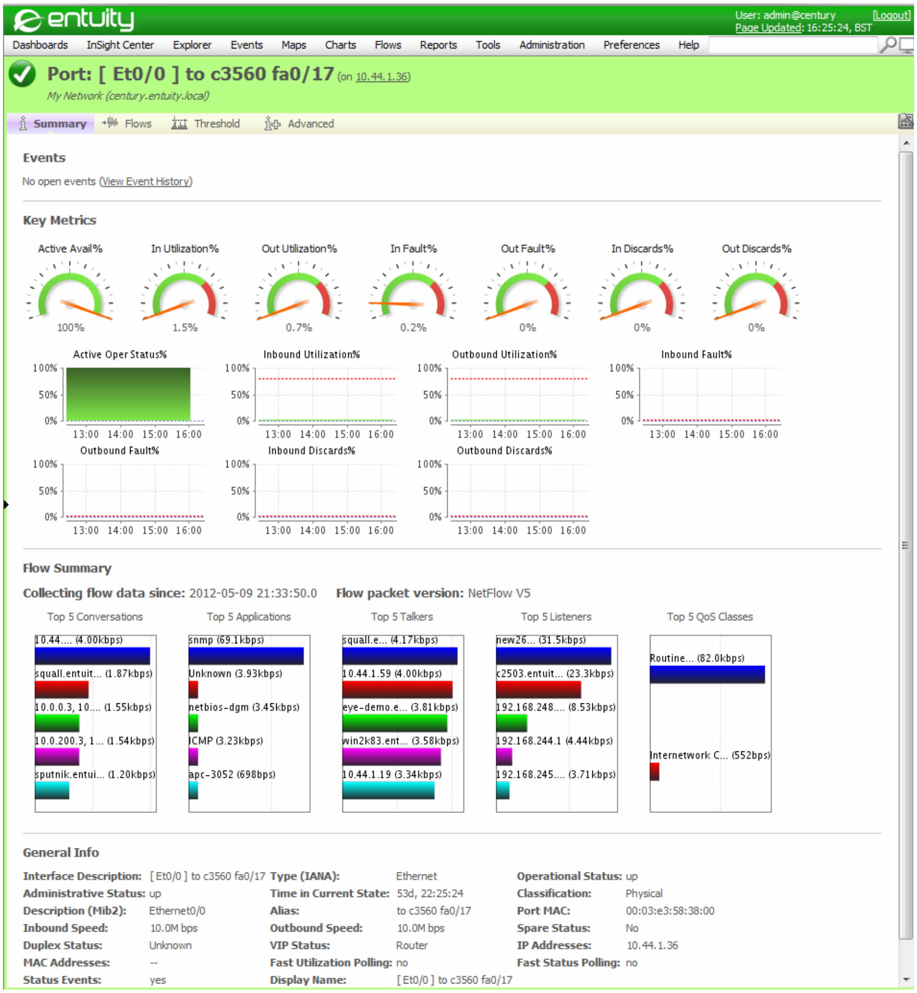
Table 12 Port Summary Page

| Attribute | Description |
|---|---|
| *Inbound Utilization %* | Utilization expressed as a percentage of actual traffic volume received against the maximum volume that can be handled by the port during the polling period. |
| *Outbound Utilization %* | Utilization expressed as a percentage of actual traffic volume transmitted during the report period against the maximum volume that can be handled by the port during the polling period. |
| *Inbound Fault %,* | The number of inbound faults expressed as a percentage of total traffic volume received by the port during the polling period. |
| *Outbound Fault %* | The number of outbound faults expressed as a percentage of total traffic volume transmitted by the port during the polling period. |
| *Inbound Discards %* | The number of inbound discards expressed as a percentage of total traffic volume received by the port during the polling period. |
| *Outbound Discards %* | The number of outbound discards expressed as a percentage of total traffic volume transmitted by the port during the polling period. |
| Flow Summary section includes graphs of key flow data for the port. | |
| *Collecting Flow Data Since* | The date and time the Entuity flow collector started collecting. |
| *Flow Packet Version* | The name and version of the flow data protocol, e.g. NetFlow5. |
| *Top N Applications* | The top applications on the interface, as measured in octets(bytes/s). The number displayed, sample interval and chart style are configurable through the chart’s Flow Details page, accessed by clicking on the chart. |
| *Top N Talkers* | The top talking hosts on the interface, measured as outbound traffic in octets(bytes/s). The number displayed, sample interval and chart style are configurable through the chart’s Flow Details page, accessed by clicking on the chart. |
| *Top N Listeners* | The top listening hosts on the interface, measured as inbound traffic in octets(bytes/s). The number displayed, sample interval and chart style are configurable through the chart’s Flow Details page, accessed by clicking on the chart. |
| *Top N QoS Classes* | The top QoS classes on the interface, as measured in octets(bytes/s). The number displayed, sample interval and chart style are configurable through the chart’s Flow Details page, accessed by clicking on the chart. |
| General Info section, provides port identifying details: | |
| *Interface Description* | Brief description of the port. It is also available through Entuity’s Topology Map. |
| *Type (IANA)* | Indicates the interface type, e.g. ethernet. |
| *Operational Status* | Current operational status, e.g. up, down. |
| *Administrative Status* | Port status as set by the system administrator. |
| *Time in Current State* | Time in its current operational state. |
| *Classification* | Indicates whether the port is a physical or virtual port. |

Table 12 Port Summary Page

| Attribute | Description |
|---|---|
| *Description (Mib2)* | Port description taken from SNMP-MIB2. |
| *Alias* | The port’s alias. |
| *Inbound Speed* | Inbound speed of a port operating asymmetric inbound and outbound speeds.<br>For use in Entuity your System Administrator can amend the port inbound speed. |
| *Outbound Speed* | Outbound speed of a port operating asymmetric inbound and outbound speeds.<br>For use in Entuity your System Administrator can amend the port outbound speed. |
| *Spare Status* | Indicates whether Entuity considers the port in use or spare. |
| *Duplex Status* | The port’s duplex status. |
| *VIP Status* | The port role, e.g. router, uplink, trunk. |
| *IP Addresses* | IP addresses associated with the port. |
| *MAC Addresses* | MAC addresses associated with the port. |

Table 12 Port Summary Page


entuity
User: admin@century [Logout]
Page Updated: 16:25:24, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Preferences Help
Summary Flows Threshold Advanced

Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)

*My Network (century.entuity.local)*

**Events**

No open events (View Event History)

**Key Metrics**

**Flow Summary**

**Collecting flow data since:** 2012-05-09 21:33:50.0 **Flow packet version:** NetFlow V5

**General Info**

| | | | | | |
|---|---|---|---|---|---|
| **Interface Description:** | [ Et0/0 ] to c3560 fa0/17 | **Type (IANA):** | Ethernet | **Operational Status:** | up |
| **Administrative Status:** | up | **Time in Current State:** | 53d, 22:25:24 | **Classification:** | Physical |
| **Description (Mib2):** | Ethernet0/0 | **Alias:** | to c3560 fa0/17 | **Port MAC:** | 00:03:e3:58:38:00 |
| **Inbound Speed:** | 10.0M bps | **Outbound Speed:** | 10.0M bps | **Spare Status:** | No |
| **Duplex Status:** | Unknown | **VIP Status:** | Router | **IP Addresses:** | 10.44.1.36 |
| **MAC Addresses:** | -- | **Fast Utilization Polling:** | no | **Fast Status Polling:** | no |
| **Status Events:** | yes | **Display Name:** | [ Et0/0 ] to c3560 fa0/17 | | |

Figure 26 Port Summary Details

## Port Advanced Details

The Port Advanced Details page is for advanced users, providing access to detailed information on the port.

The content of the Port Advanced Details page varies according to the port type and the enabled modules. This section indicates the type of available information.

| Attribute | Description |
|---|---|
| Page icons | Link to other pages that display details on this device, e.g. Port Summary page (see *Navigate through Explorer*). |
| *Port Name* | Identifies device type and resolved name\IP address, e.g. Port:  [ 00028 ] Vlan1. |
| *View(Server)* | Name of the Entuity view and server, e.g. All Objects (COMPRESSOR). |
| Attribute section, provides port identifying details: | |
| *Administrative Status* | Port status as set by the system administrator. |
| *Alias* | The port’s alias. |
| *Classification* | Indicates whether the port is a physical or virtual port. |
| *Description (Mib2)* | Port description taken from SNMP-MIB2. |
| *Device Name* | The port’s device address. |
| *Duplex Status* | The port’s duplex status. |
| *Inbound Speed* | Port’s referenced interface speed, used for example, when Entuity calculates inbound port utilization. For use in Entuity your System Administrator can amend the port interface speed |
| *Interface Description* | Brief description of the port. |
| *Operational Status* | Current operational status, e.g. up, down. |
| *Outbound Speed* | Port’s referenced interface speed, used for example, when Entuity calculates outbound port utilization. For use in Entuity your System Administrator can amend the port interface speed. |
| *Port MAC* | Port’s MAC address. |
| *Short Description* | Brief description of the port. |
| *Spare Status* | Indicates whether Entuity considers the port in use or spare. |
| *StormWorks ID* | Internal identifier of the object. |
| *Type (IANA)* | Indicates the interface type, e.g. ethernet, Prop Serial. |
| *VIP Status* | Port type, e.g. router, uplink. |
| Stream Attribute section, provides latest values for port attributes for which Entuity maintains a history: | |
| *Administrative Status* | Last polled administrative status of the port, e.g. **Up**, **Down**. |
| *CDP Local Port Name (Mib2)* | Port used in the CDP neighbor discovery. The name of the port as read from MIB2. |
| *CDP Local Port Name (ifxMib)* | Port used in the CDP neighbor discovery. The name of the port as read from MIB2. |
| *CDP Remote Device IP Address* | Device containing the port which is connected to the local port. The connection is identified through CDP neighborhood discovery. |
| *CDP Remote Port Name* | Remote port connected to the local port as identified through CDP neighbor discovery. |

Table 13 Port Advanced Details

| Attribute | Description |
|---|---|
| *Event Description* | Description of the last event raised against the port, including event type, source and impacted details. |
| *Events Summary* | Short description of raised events. |
| *IP Addresses* | IP addresses assigned to the port. |
| *Inbound Discarded Packet Rate* | The inbound discard rate of packets for which no errors were detected. Packets may be discarded to free up buffer space. |
| *Inbound Discarded Packet %* | The number of inbound packets discarded, for which no errors were detected, as a percentage of the total number of packets received during the sample period. |
| *Inbound Discards %* | The number of inbound packets discarded, for which no errors were detected, as a percentage of the total number of packets received during the sample period. |
| *Inbound Errored Packet Rate* | The inbound discard rate of packets with errors. |
| *Inbound Errored Packet %* | The number of inbound packets with errors discarded as a percentage of the total number of packets received during the sample period. |
| *Inbound Fault%* | The number of inbound packets with errors discarded as a percentage of the total number of packets received during the sample period. |
| *Inbound Non-Unicast Packet Rate* | The transmission rate of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets. |
| *Inbound Non-Unicast Packet%* | The number of inbound non-unicast (i.e. subnetwork-broadcast or subnetwork-multicast) packets expressed as a percentage of the total number of packets received during the sample period. |
| *Inbound Octet Rate* | The number of octets set for transmission during the sample period, this includes packets that were discarded or not sent but excludes packets addressed to a multicast or broadcast address at this sub-layer. |
| *Inbound Packet Rate* | The number of packets received during the sample period, this excludes packets addressed to a multicast or broadcast address at this sub-layer. |
| *Inbound Peak Rate* | Peak received rate during the sample period expressed as packets per second. |
| *Inbound Traffic* | Total inbound traffic during the sample period expressed as bits per second. |
| *Inbound Utilization (WAN) %,* | Utilization expressed as a percentage of actual traffic volume received against the maximum volume that can be handled by the port during the polling period. |
| *Inbound Interface Speed* | Inbound speed of the port.<br>For use in Entuity, system administrator's can amend the port inbound speed. |
| *Interface Type* | Interface type, e.g. Ethernet. |
| *Latest mac address count* | Count of MAC addresses identified during the last poll of the device. |

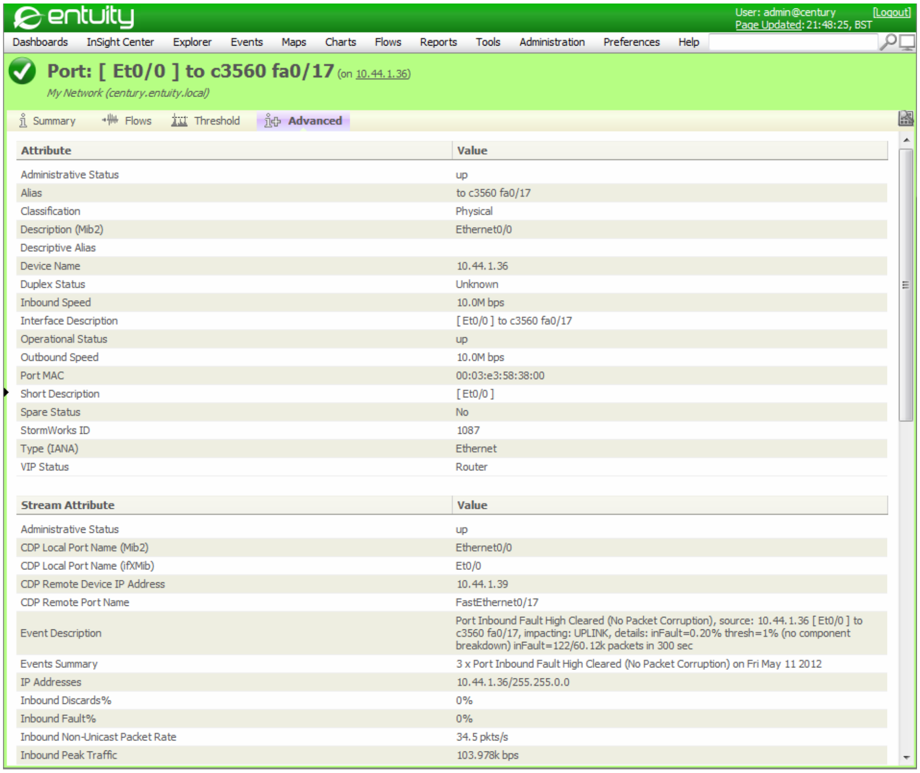
Table 13 Port Advanced Details

| Attribute | Description |
|---|---|
| *MAC Address* | List of MAC addresses associated with the device. |
| *Mac address history* | All of the MAC addresses discovered on the port. This is a change history of the MAC addresses on the port, each time the MACs on a port change Entuity retains a record of all of the MACs on the port at that time (by default Entuity retains fifty samples, although this is configurable through `entuity.cfg`). |
| *Max Packet Size* | Maximum packet size before fragmentation. |
| *Most recent mac address(es)* | Most recent MAC addresses discovered on the port. Entuity retains MAC addresses for two days after they were last polled on the device (this is a configurable setting through `entuity.cfg`). |
| *Nominal interface speed* | Interface speed polled from the port. |
| *Operational Status* | Operational status of the port. |
| *Outbound Discarded Packet Rate* | The outbound discard rate of packets for which no errors were detected. Packets may be discarded to free up buffer space. |
| *Outbound Discarded Packet %* | The number of outbound packets discarded, for which no errors were detected, as a percentage of the total number of packets transmitted during the polling period. |
| *Outbound Discards %* | The number of outbound packets discarded, for which no errors were detected, as a percentage of the total number of packets transmitted during the polling period. |
| *Outbound Errored Packet Rate* | The outbound discard rate of packets with errors. |
| *Outbound Errored Packet %* | The number of outbound packets with errors discarded as a percentage of the total number of packets transmitted during the polling period. |
| *Outbound Fault%* | The number of outbound packets with errors discarded as a percentage of the total number of packets transmitted during the polling period. |
| *Outbound Non-Unicast Packet Rate* | The transmission rate of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets. |
| *Outbound Non-Unicast Packet%* | The number of outbound non-unicast (i.e. subnetwork-broadcast or subnetwork-multicast) packets expressed as a percentage of the total number of packets transmitted during the polling period. |
| *Outbound Octet Rate* | The number of octets set for transmission during the sample period, this includes packets that were discarded or not sent but excludes packets addressed to a multicast or broadcast address at this sub-layer. |
| *Outbound Packet Rate* | The number of packets set for transmission during the sample period, this includes packets that were discarded or not sent but excludes packets addressed to a multicast or broadcast address at this sub-layer. |
| *Outbound Peak Rate* | Peak transmission rate during the sample period expressed as packets per second. |
| *Outbound Traffic* | Total outbound traffic during the sample period expressed as bits per second. |

Table 13 Port Advanced Details

| Attribute | Description |
|---|---|
| *Outbound Utilization %* | Utilization expressed as a percentage of actual traffic volume transmitted against the maximum volume that can be handled by the port during the polling period. |
| *Outbound Interface Speed* | Outbound speed of the port.<br>For use in Entuity, system administrator's can amend the port outbound speed. |
| *Outbound Utilization %* | Utilization expressed as a percentage of actual traffic volume transmitted against the maximum volume that can be handled by the port during the polling period. |
| *Port State* | Current state of the port, e.g. Up, Down. |
| *Time of Last State Change* | Date and time of the last change in *Port State.* |
| *Time in Current State* | Length of time since the last change in *Port State.* |
| **Association section provides details and hyperlinks from the device to its associations.** | |
| Association | *Access Point*<br>*Autonomous WAP Device*<br>*Device, the port's device*<br>*EIGRP Peer*<br>*HSRP Port Groups*<br>*Host MAC Addresses*<br>*IP Addresses*<br>*IPv6 Interface*<br>*Layer 3 Port Peers*<br>*MPLS Interface VRF Instances*<br>*MPLS LDP Ranges*<br>*Module*<br>*Parent MPLS LDP Label Range*<br>*Policy Maps*<br>*Vlans*<br>*Xedia Traffic Classes.* |

Table 13 Port Advanced Details



Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)

*My Network (century.entuity.local)*

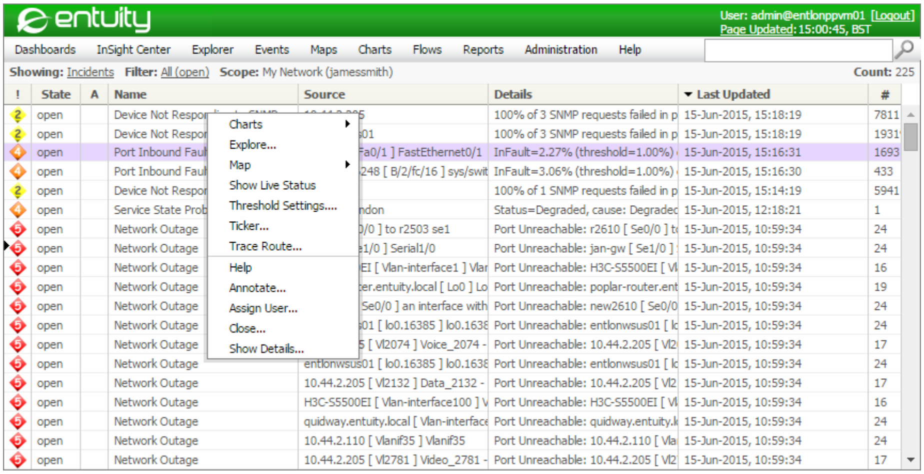
| Attribute | Value |
|---|---|
| Administrative Status | up |
| Alias | to c3560 fa0/17 |
| Classification | Physical |
| Description (Mib2) | Ethernet0/0 |
| Descriptive Alias | |
| Device Name | 10.44.1.36 |
| Duplex Status | Unknown |
| Inbound Speed | 10.0M bps |
| Interface Description | [ Et0/0 ] to c3560 fa0/17 |
| Operational Status | up |
| Outbound Speed | 10.0M bps |
| Port MAC | 00:03:e3:58:38:00 |
| Short Description | [ Et0/0 ] |
| Spare Status | No |
| StormWorks ID | 1087 |
| Type (IANA) | Ethernet |
| VIP Status | Router |

| Stream Attribute | Value |
|---|---|
| Administrative Status | up |
| CDP Local Port Name (Mib2) | Ethernet0/0 |
| CDP Local Port Name (ifXMib) | Et0/0 |
| CDP Remote Device IP Address | 10.44.1.39 |
| CDP Remote Port Name | FastEthernet0/17 |
| Event Description | Port Inbound Fault High Cleared (No Packet Corruption), source: 10.44.1.36 [ Et0/0 ] to c3560 fa0/17, impacting: UPLINK, details: inFault=0.20% thresh=1% (no component breakdown) inFault=122/60.12k packets in 300 sec |
| Events Summary | 3 x Port Inbound Fault High Cleared (No Packet Corruption) on Fri May 11 2012 |
| IP Addresses | 10.44.1.36/255.255.0.0 |
| Inbound Discards% | 0% |
| Inbound Fault% | 0% |
| Inbound Non-Unicast Packet Rate | 34.5 pkts/s |
| Inbound Peak Traffic | 103.978k bps |

Figure 27 Port Advanced Details

# 3 Event and Incident Management

Entuity incidents and events indicate the state of your network. Entuity is shipped with a default configuration, which administrators and users with the Event Administration permission can configure.



**Showing:** Incidents **Filter:** All (open) **Scope:** My Network (jamessmith) **Count:** 225

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| 2 | open | | Device Not Respor | 5 | 100% of 3 SNMP requests failed in p | 15-Jun-2015, 15:18:19 | 7811 |
| 2 | open | | Device Not Respor | 01 | 100% of 3 SNMP requests failed in p | 15-Jun-2015, 15:18:19 | 1931 |
| 4 | open | | Port Inbound Faul | Fa0/1 ] FastEthernet0/1 | InFault=2.27% (threshold=1.00%) | 15-Jun-2015, 15:16:31 | 1693 |
| 4 | open | | Port Inbound Faul | 248 [ B/2/fc/16 ] sys/swit | InFault=3.06% (threshold=1.00%) | 15-Jun-2015, 15:16:30 | 433 |
| 2 | open | | Device Not Respor | | 100% of 1 SNMP requests failed in p | 15-Jun-2015, 15:14:19 | 5941 |
| 4 | open | | Service State Prob | ndon | Status=Degraded, cause: Degradec | 15-Jun-2015, 12:18:21 | 1 |
| 5 | open | | Network Outage | 0/0 ] to r2503 se1 | Port Unreachable: r2610 [ Se0/0 ] t | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | e1/0 ] Serial1/0 | Port Unreachable: jan-gw [ Se1/0 ] | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | EI [ Vlan-interface1 ] Vlar | Port Unreachable: H3C-S5500EI [ Vl | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | | Network Outage | er.entuity.local [ Lo0 ] Lo | Port Unreachable: poplar-router.ent | 15-Jun-2015, 10:59:34 | 19 |
| 5 | open | | Network Outage | Se0/0 ] an interface with | Port Unreachable: new2610 [ Se0/0 | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | 01 [ lo0.16385 ] lo0.1638 | Port Unreachable: entlonwsus01 [ lo | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | 5 [ Vl2074 ] Voice_2074 - | Port Unreachable: 10.44.2.205 [ Vl2 | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | | Network Outage | entlonwsus01 [ lo0.16385 ] lo0.1638 | Port Unreachable: entlonwsus01 [ lo | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | 10.44.2.205 [ Vl2132 ] Data_2132 - | Port Unreachable: 10.44.2.205 [ Vl2 | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | | Network Outage | H3C-S5500EI [ Vlan-interface100 ] V | Port Unreachable: H3C-S5500EI [ Vl | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | | Network Outage | quidway.entuity.local [ Vlan-interface | Port Unreachable: quidway.entuity.l | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | 10.44.2.110 [ Vlanif35 ] Vlanif35 | Port Unreachable: 10.44.2.110 [ Vla | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | 10.44.2.205 [ Vl2781 ] Video_2781 - | Port Unreachable: 10.44.2.205 [ Vl2 | 15-Jun-2015, 10:59:34 | 17 |

Figure 28 Incidents in Event Viewer

## Event Projects

The Event Management System controls how Entuity manages incoming events, traps and syslog alerts. It is configured through an event project. Entuity includes a default project which is an appropriate starting point for your installation with more than 350 events, over 100 incidents and a default set of rules.

The default event project includes rules to:

- Handle flapping ports.
- Filter out traps from sources you have configured Entuity to discard.
- Apply N of M rules, for example for to processor utilization, port utilization, IP SLA, network outage events.

Administrators, and users with the Event Administration permission, can customize event projects, for example create new events, incidents, rules and actions.

## Events and Incidents Comparison Summary

Incidents and events have separate but related roles in managing your network.

The key differences between incidents and events are important in understanding how to best manage the information coming into Entuity:

- Incident and Event Life Cycles.

  An event indicates a particular state of an object at the time the event was raised. An incident indicates an ongoing condition on your network with its associated events providing the state updates.

  Incidents are usually removed from the system 7 days after they are expired, events are retained by default for 14 days.

- Event and Incident Severity Levels.

  Events have an associated severity level, which is configurable through the Events administration page and also through actions. Incidents inherit the highest severity level of the currently raised event. For example, if an incident is raised by an event with a severity level of Major it has a severity level of Major, if it is updated by an event with the severity level of Critical the incident also inherits the Critical severity level.

- Event and Incident Assignment.

  Incidents you can assign to users, events you cannot.

- Event and Incident Annotation.

  Incidents you can acknowledge, events you cannot.

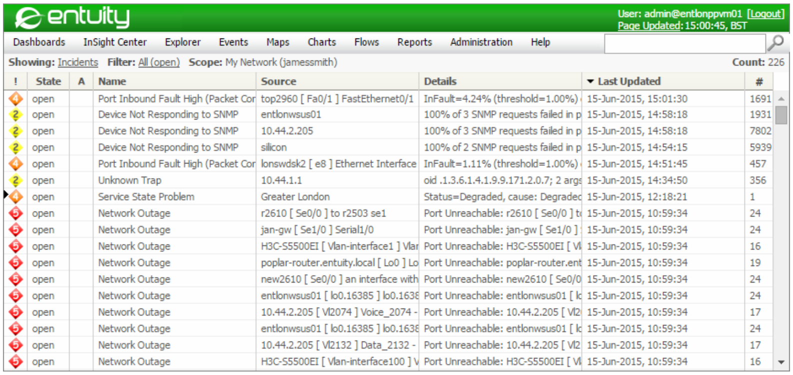
- Pre and Post Storage Processing.

  In the set up of the Event Management System you can configure processing of incoming events before they are stored in the database, and also after their storage. Processing of incidents occurs after these two event stages. This indicates that incidents are raised only after the intelligence that is built into the Event Management System has been applied, which is why incidents are the default view into the what is happening on your network.

## Viewing Events and Incidents

Incidents and events are displayed through the same viewer, by default it shows incidents and the viewer inherits the context in which it is opened. For example to open the viewer to display the open incidents raised against the managed objects in your My Network view:

1) From the Explorer tree click on your My Networks view.
2) On the menu bar click **Events.** Event Viewer displays open incidents raised in the My Networks view.



**Showing:** Incidents **Filter:** All (open) **Scope:** My Network (jamessmith) **Count:** 226

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| 4 | open | | Port Inbound Fault High (Packet Cor | top2960 [ Fa0/1 ] FastEthernet0/1 | InFault=4.24% (threshold=1.00%) | 15-Jun-2015, 15:01:30 | 1691 |
| 2 | open | | Device Not Responding to SNMP | entlonwsus01 | 100% of 3 SNMP requests failed in p | 15-Jun-2015, 14:58:18 | 1931 |
| 2 | open | | Device Not Responding to SNMP | 10.44.2.205 | 100% of 3 SNMP requests failed in p | 15-Jun-2015, 14:58:18 | 7802 |
| 2 | open | | Device Not Responding to SNMP | silicon | 100% of 2 SNMP requests failed in p | 15-Jun-2015, 14:54:15 | 5939 |
| 4 | open | | Port Inbound Fault High (Packet Cor | lonswdsk2 [ e8 ] Ethernet Interface | InFault=1.11% (threshold=1.00%) | 15-Jun-2015, 14:51:45 | 457 |
| 2 | open | | Unknown Trap | 10.44.1.1 | oid .1.3.6.1.4.1.9.9.171.2.0.7; 2 args | 15-Jun-2015, 14:34:50 | 356 |
| 4 | open | | Service State Problem | Greater London | Status=Degraded, cause: Degradec | 15-Jun-2015, 12:18:21 | 1 |
| 5 | open | | Network Outage | r2610 [ Se0/0 ] to r2503 se1 | Port Unreachable: r2610 [ Se0/0 ] t | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | jan-gw [ Se1/0 ] Serial1/0 | Port Unreachable: jan-gw [ Se1/0 ] | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | H3C-S5500EI [ Vlan-interface1 ] Vlar | Port Unreachable: H3C-S5500EI [ Vl | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | | Network Outage | poplar-router.entuity.local [ Lo0 ] Lo | Port Unreachable: poplar-router.ent | 15-Jun-2015, 10:59:34 | 19 |
| 5 | open | | Network Outage | new2610 [ Se0/0 ] an interface with | Port Unreachable: new2610 [ Se0/0 | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | entlonwsus01 [ lo0.16385 ] lo0.1638 | Port Unreachable: entlonwsus01 [ lc | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | 10.44.2.205 [ Vl2074 ] Voice_2074 - | Port Unreachable: 10.44.2.205 [ Vl2 | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | | Network Outage | entlonwsus01 [ lo0.16385 ] lo0.1638 | Port Unreachable: entlonwsus01 [ lc | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | 10.44.2.205 [ Vl2132 ] Data_2132 - | Port Unreachable: 10.44.2.205 [ Vl2 | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | | Network Outage | H3C-S5500EI [ Vlan-interface100 ] V | Port Unreachable: H3C-S5500EI [ Vl | 15-Jun-2015, 10:59:34 | 16 |

Figure 29 Event Viewer

## Control the Display of Incidents and Events

By default Event Viewer displays incidents although you can change its focus to display events. The incidents or events Entuity displays is set by a combination of:

- Those views that you have configured it to have access to, through the Preferences page.
- The context in which you open the viewer. For example if you open the viewer from a selected view, device or port in the Explorer object tree, Entuity only displays incidents for that view, device or port.
- Filters, for example by default Entuity applies the All (open) filter to the current context, displaying only open incidents.

  You can create and edit filters, and also apply different filters. For example you can create filters to only display incidents raised in the previous 2 hours or to show only the assigned events for a particular user.
- Event suppression rules. Users with the Event Suppression tool permission can create, update, monitor and delete suppression rules applied against events.

| Attribute | Description |
|---|---|
| *Severity/Color ('!')* | Color and numeric coded event severity. |
| *A* | A note icon indicates the incident has an associated annotation. |
| *Name* | Name of the incident or event, e.g. Port Utilization High. |
| *Source* | Source of the event or incident. |
| *#* | Number of times that the event has appeared since any previous age out, e.g. **3** indicates the third occurrence of the event. |

Table 14 Event Viewer Attributes

| Attribute | Description |
|---|---|
| *Impact* | Details what is impacted by the event, which might be:<br>■ Managed objects, e.g. a list of VLANs.<br>■ Internal Entuity processes.<br>■ Service(s).<br>■ The number of managed objects identified by Availability Monitor. |
| *Details* | Incident and event details vary according to what is raised, for example, for:<br>■ Packet Corruption Severe, the numbers of CRCs (Cyclic Redundancy Checks) and packets.<br>■ Entuity Server Critical Component Restarting After Failure, the name of the critical internal service, e.g. Tomcat.<br>■ Port Utilization High, details of the port utilization including actual and threshold values. |
| Last Updated | Time the event or incident was last updated. |
| *#* | Number of events raised against the incident. This include opening, updating and closing events. |

Table 14 Event Viewer Attributes

## Filter Events and Incidents

The Servers and Views tab on the Preferences dialog lists those views that you have permission to access. From this list you can select those views that you want to have available to you from the web interface. Event Viewer can potentially display all of those events within the configured views, however through event and incident filters and the application of event suppression rules you can restrict their display.

Events and incidents share the same filters, with most but not all of the options applicable to controlling the display of both events and incidents.

| Attribute | Description |
|---|---|
| *Name* | Name of the filter. It should describe the purpose of the filter. |
| *State* | Indicates the state of events and incidents that Event Viewer displays:<br>■ **all**, all states.<br>■ **open**, events and incidents that are currently open.<br>■ **closed** and expired, events and incidents that are either closed or expired. |
| *Severity* | By default set to Information and above which is equivalent to all. You can amend the event severity level to report on events of a specific severity, or a specific severity and above. |

Table 15 Edit Filter

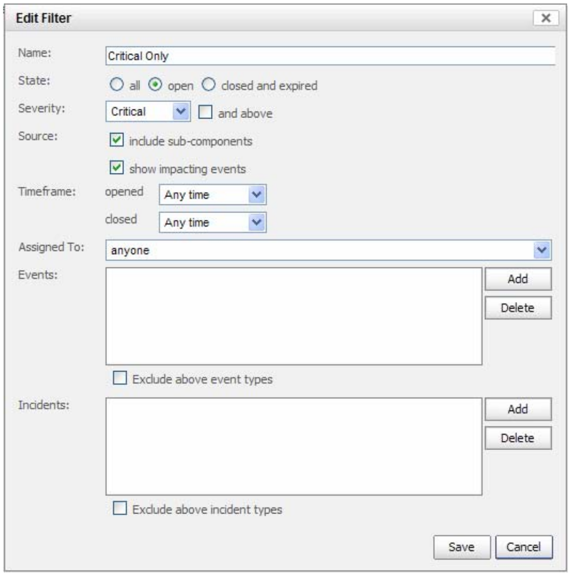
| Attribute | Description |
|---|---|
| *Source* | You can amend the scope of the Source:<br>■ Include sub-components, allows display of incidents and events from sub components of objects within the Source. For example if a device is within the filter, you can also include events and incidents from its ports.<br>■ Show impacting events allows the display of events raised on objects not within the source but impact objects within it. For example when selected you can view Network Outage events against those devices impacted by a network failure. |
| *Timeframe* | Set the opened and closed parameters of the incidents and events, by default set to no limit and now respectively. |
| *Assigned To* | Incidents can be assigned to users. Each user would have their own assignment filter with their name selected. |
| *Events* | Select events which depending on whether you select the *Exclude above event types* determines what events are displayed. |
| *Incidents* | Select incidents which depending on whether you select the *Exclude above incident types* determines what incidents are displayed. |

Table 15 Edit Filter

To create an incident and event filter:

1) Click **Events**. Event Viewer displays all open incidents with a severity level greater than Information, up to a maximum of 5000 within the current *Scope* (view).
2) If required from Explorer select the required view. When selected this changes the current *Scope* (view).

   You can concentrate the focus of Event Viewer by amending the filter displayed at the top of Event Viewer.
3) Click on the current *Filter*. Entuity displays a context menu from which you can select a filter to apply to the viewer, or create, edit or delete a filter.
4) Click **New** to create a filter.
5) Complete the filter definition and click **Save**.



Edit Filter ✕

Name: Critical Only

State: ○ all ● open ○ closed and expired

Severity: Critical ☐ and above

Source: ☑ include sub-components

☑ show impacting events

Timeframe: opened Any time

closed Any time

Assigned To: anyone

Events:

☐ Exclude above event types

Incidents:

☐ Exclude above incident types

Figure 30 Event Viewer Filter

## Event and Incident Severity Levels

Entuity events and incidents all have a severity level which indicates the seriousness to your network of the raised issue. Event severity is configurable through the Event Management System, incidents do not have an assigned severity level, instead they inherit the severity level of the event with the highest severity that is currently associated with them.

The severity symbol is a color coded diamond that holds the severity number, the greater the number the more severe the event or incident. The severity symbols are used in Entuity maps and events.

You can use the severity level within filters, for example to only view Critical events. By default Entuity's All (open) filter displays all open events and incidents; from information only and above.

| Symbol | Color | Level | Severity Description |
|---|---|---|---|
| ◆5 | Red | 5 | Critical |
| ◆4 | Orange | 4 | Severe |
| ◆3 | Amber | 3 | Major |
| ◆2 | Yellow | 2 | Minor |
| ◆1 | Green | 1 | Information only |

Table 16 Event and Incident Severity Levels

For a full listing of events and their severity levels consult the *Entuity Events Reference Manual*.

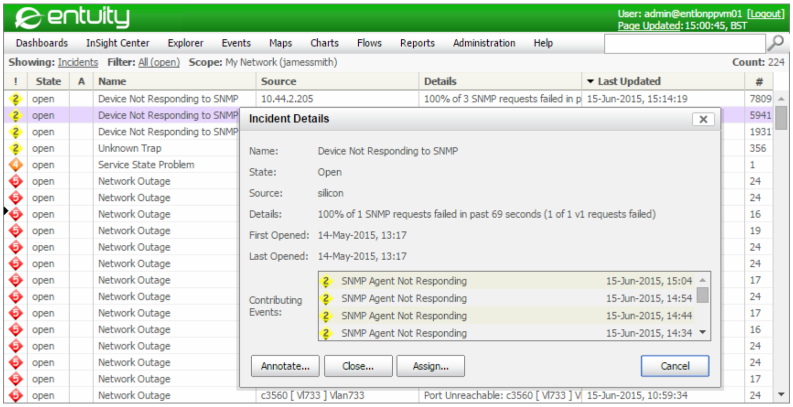
## Investigating Incidents

To investigate incidents:

1) From the Explorer tree click on your My Networks view.

2) On the menu bar click **Events.** Event Viewer displays open incidents raised in the My Networks view.

3) Highlight an incident and from the context menu click **Show Details**.



**Showing:** Incidents **Filter:** All (open) **Scope:** My Network (jamessmith) **Count:** 224

| ! | State | A | Name | Source | Details | ▼ Last Updated | # |
|---|---|---|---|---|---|---|---|
| 2 | open | | Device Not Responding to SNMP | 10.44.2.205 | 100% of 3 SNMP requests failed in p | 15-Jun-2015, 15:14:19 | 7809 |
| 2 | open | | Device Not Responding to SNMP | | | | 5941 |
| 2 | open | | Device Not Responding to SNMP | | | | 1931 |
| 2 | open | | Unknown Trap | | | | 356 |
| 4 | open | | Service State Problem | | | | 1 |
| 5 | open | | Network Outage | | | | 24 |
| 5 | open | | Network Outage | | | | 24 |
| 5 | open | | Network Outage | | | | 16 |
| 5 | open | | Network Outage | | | | 19 |
| 5 | open | | Network Outage | | | | 24 |
| 5 | open | | Network Outage | | | | 24 |
| 5 | open | | Network Outage | | | | 17 |
| 5 | open | | Network Outage | | | | 24 |
| 5 | open | | Network Outage | | | | 17 |
| 5 | open | | Network Outage | | | | 16 |
| 5 | open | | Network Outage | | | | 24 |
| 5 | open | | Network Outage | | | | 24 |
| 5 | open | | Network Outage | | | | 17 |
| 5 | open | | Network Outage | c3560 [ Vl733 ] Vlan733 | Port Unreachable: c3560 [ Vl733 ] V | 15-Jun-2015, 10:59:34 | 24 |

**Incident Details**

Name: Device Not Responding to SNMP

State: Open

Source: silicon

Details: 100% of 1 SNMP requests failed in past 69 seconds (1 of 1 v1 requests failed)

First Opened: 14-May-2015, 13:17

Last Opened: 14-May-2015, 13:17

Contributing Events:

| | | |
|---|---|---|
| 2 | SNMP Agent Not Responding | 15-Jun-2015, 15:04 |
| 2 | SNMP Agent Not Responding | 15-Jun-2015, 14:54 |
| 2 | SNMP Agent Not Responding | 15-Jun-2015, 14:44 |
| 2 | SNMP Agent Not Responding | 15-Jun-2015, 14:34 |

Figure 31 Incident Show Details

From the Incident Details dialog you can view the details already displayed in the Event Viewer columns and also:

- Contributing Events lists the events that have updated the state of the incident. You can click on an event and Entuity displays the Event Details dialog.
- User Attributes are attributes created by the system administrator within the event project.
- Assigned To is the name of the user who has the incident assigned to them
- Annotation details of the associated annotation.

You can also assign incidents to a user, close an incident and annotate an incident.

## Investigating Events

You can access events through related incidents and also by setting in Event Viewer *Showing* to Events.

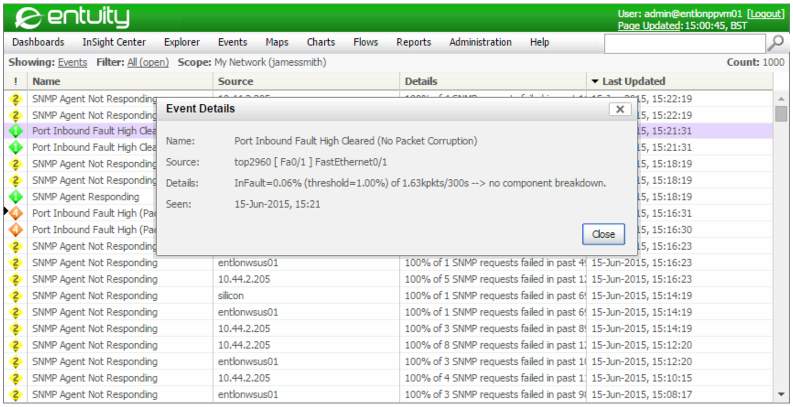
To investigate events:

1) From the Explorer tree click on your My Network view.

2) On the menu bar click **Events.** Event Viewer displays open incidents raised in the My Networks view.

3) In *Showing* click on **Incidents** and select **Events**.

4) Highlight an event and from the context menu click **Show Details**.



**Showing:** Events **Filter:** All (open) **Scope:** My Network (jamessmith) **Count:** 1000

**Event Details**

Name: Port Inbound Fault High Cleared (No Packet Corruption)

Source: top2960 [ Fa0/1 ] FastEthernet0/1

Details: InFault=0.06% (threshold=1.00%) of 1.63kpkts/300s --> no component breakdown.

Seen: 15-Jun-2015, 15:21

| ! | Name | Source | Details | Last Updated |
|---|---|---|---|---|
| 2 | SNMP Agent Not Responding | | | 15, 15:22:19 |
| 2 | SNMP Agent Not Responding | | | 15, 15:22:19 |
| 1 | Port Inbound Fault High Clea | | | 15, 15:21:31 |
| 1 | Port Inbound Fault High Clea | | | 15, 15:21:31 |
| 2 | SNMP Agent Not Responding | | | 15, 15:18:19 |
| 2 | SNMP Agent Not Responding | | | 15, 15:18:19 |
| 1 | SNMP Agent Responding | | | 15, 15:18:19 |
| 4 | Port Inbound Fault High (Pa | | | 15, 15:16:31 |
| 4 | Port Inbound Fault High (Pa | | | 15, 15:16:30 |
| 2 | SNMP Agent Not Responding | | | 15, 15:16:23 |
| 2 | SNMP Agent Not Responding | entlonwsus01 | 100% of 1 SNMP requests failed in past 4 | 15-Jun-2015, 15:16:23 |
| 2 | SNMP Agent Not Responding | 10.44.2.205 | 100% of 5 SNMP requests failed in past 1 | 15-Jun-2015, 15:16:23 |
| 2 | SNMP Agent Not Responding | silicon | 100% of 1 SNMP requests failed in past 6 | 15-Jun-2015, 15:14:19 |
| 2 | SNMP Agent Not Responding | entlonwsus01 | 100% of 1 SNMP requests failed in past 6 | 15-Jun-2015, 15:14:19 |
| 2 | SNMP Agent Not Responding | 10.44.2.205 | 100% of 3 SNMP requests failed in past 8 | 15-Jun-2015, 15:14:19 |
| 2 | SNMP Agent Not Responding | 10.44.2.205 | 100% of 8 SNMP requests failed in past 1 | 15-Jun-2015, 15:12:20 |
| 2 | SNMP Agent Not Responding | entlonwsus01 | 100% of 3 SNMP requests failed in past 1 | 15-Jun-2015, 15:12:20 |
| 2 | SNMP Agent Not Responding | 10.44.2.205 | 100% of 4 SNMP requests failed in past 1 | 15-Jun-2015, 15:10:15 |
| 2 | SNMP Agent Not Responding | entlonwsus01 | 100% of 3 SNMP requests failed in past 9 | 15-Jun-2015, 15:08:17 |

Figure 32 Event Show Details

From the Event Details dialog you can view the details already displayed in the Event Viewer columns and also:

- Impacted Objects which displays the managed objects impacted by the event.
- User Attributes are attributes created by the system administrator within the event project.
- Contributing Events, events that contribute to the raising of the event, for example where an event is only raised after a condition is applied to a contributing event.

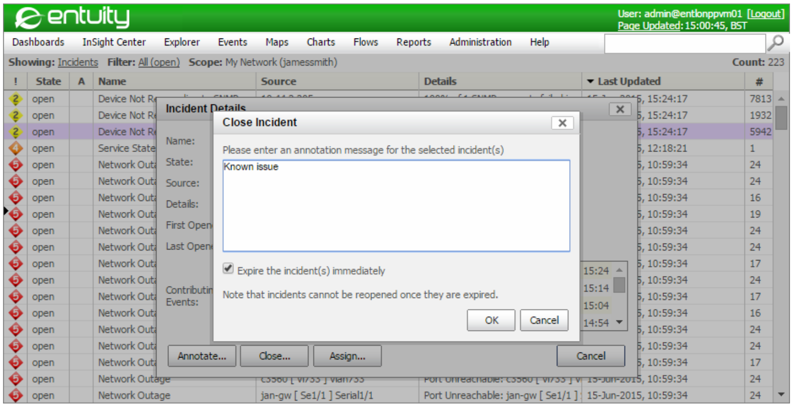
## Close Incidents

Entuity distinguishes between a closed incident, an expired incident and a deleted incident:

- Closed indicates the cause of the incident is no longer true, however if the cause recurs the incident is re-opened.
- Expired indicates that the closed incident's expiry period has completed. The incident is available for seven days for review, but if the original cause of the raising of the incident recurs the incident is not re-opened a new incident is opened.
- Deleted incident is not in the system.

There are three ways of closing incidents:

- Aging out of the incident. An incident may have a set age out. For example, by default after 3600 seconds the Device Sensor Non-Operational incident ages out and its status changes to closed.
- A closing event. For example the Device Sensor Non-Operational incident is closed when the Device Sensor Non-Operational Cleared event is raised.
- Manual Closing of the incident. From Event Viewer users can close an incident, give a reason for the closure and also immediately expire the incident.



User: admin@entlonppvm01 [Logout]
Page Updated: 15:00:45, BST

Showing: Incidents Filter: All (open) Scope: My Network (jamessmith) Count: 223

Close Incident

Please enter an annotation message for the selected incident(s)

Known issue

☑ Expire the incident(s) immediately

Note that incidents cannot be reopened once they are expired.

Figure 33 Close an Incident

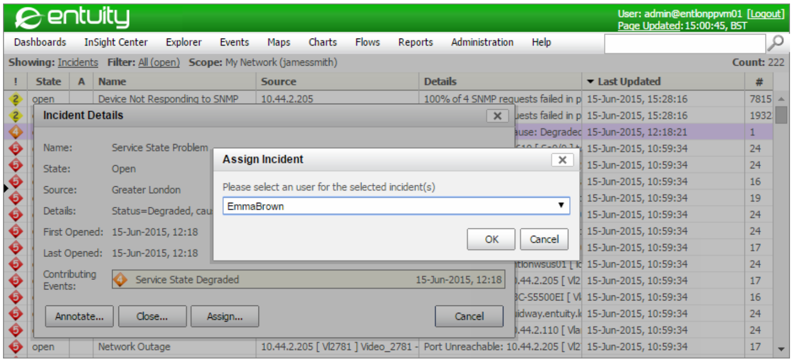
## Assign Incidents to a User

You can assign incidents to users. From Event Viewer you can assign an incident to the selected user:

1) Highlight the required incident.

2) From the context menu click **Assign**.

3) In *Assigned To* select the user, for example **JamesSmith**.



User: admin@entlonppvm01 [Logout]
Page Updated: 15:00:45, BST

Showing: Incidents Filter: All (open) Scope: My Network (jamessmith) Count: 222

Incident Details

Name: Service State Problem
State: Open
Source: Greater London
Details: Status=Degraded, cau
First Opened: 15-Jun-2015, 12:18
Last Opened: 15-Jun-2015, 12:18
Contributing Events: Service State Degraded 15-Jun-2015, 12:18

Assign Incident

Please select an user for the selected incident(s)

EmmaBrown ▼

Figure 34 Assign Incident

## How do I Find my Incident Assignments?

You can create a filter that would only permit in the view incidents assigned to the selected user.

To create a view that would include all open assignments to the user **JamesSmith**:

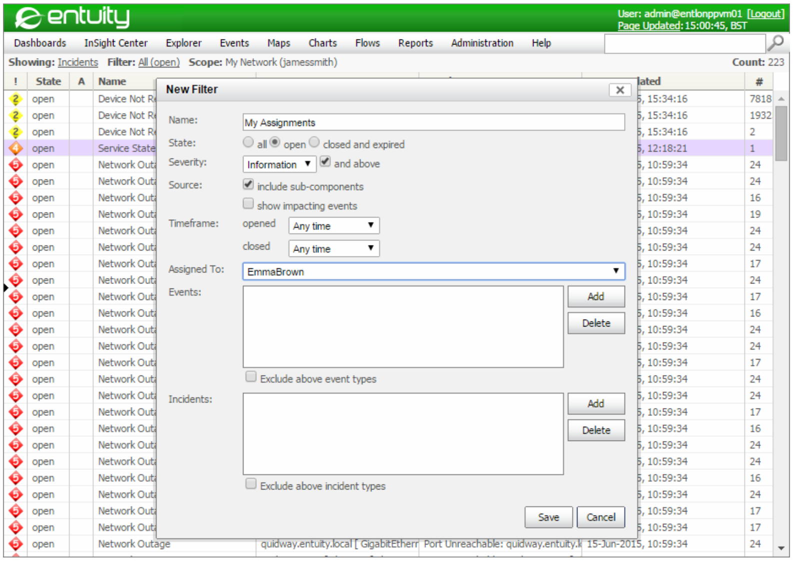
1) From Event Viewer click the filter name and select **New**.

2) In *Name* enter a meaningful name, for example My Assignments.

3) In *State* select **Open**. Entuity only includes open incidents to the view.

4) In *Assigned To* select **JamesSmith**.

5) Click **Save**.



User: admin@entlonppvm01 [Logout]
Page Updated: 15:00:45, BST

**Showing:** Incidents **Filter:** All (open) **Scope:** My Network (jamessmith) **Count:** 223

Name: My Assignments

State: ○ all ● open ○ closed and expired

Severity: Information ▼ ☑ and above

Source: ☑ include sub-components

☐ show impacting events

Timeframe: opened Any time ▼

closed Any time ▼

Assigned To: EmmaBrown ▼

Events:

☐ Exclude above event types

Incidents:

☐ Exclude above incident types

| ! | State | A | Name | | | lated | # |
|---|---|---|---|---|---|---|---|
| 2 | open | | Device Not R | | | 5, 15:34:16 | 7818 |
| 2 | open | | Device Not R | | | 5, 15:34:16 | 1932 |
| 2 | open | | Device Not R | | | 5, 15:34:16 | 2 |
| 4 | open | | Service State | | | 5, 12:18:21 | 1 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 16 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 19 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 17 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 17 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 16 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 17 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 17 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 16 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 16 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 24 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 17 |
| 5 | open | | Network Out | | | 5, 10:59:34 | 17 |
| 5 | open | | Network Outage | quidway.entuity.local [ GigabitEtherr | Port Unreachable: quidway.entuity.k | 15-Jun-2015, 10:59:34 | 24 |

Figure 35 My Assignments Filter

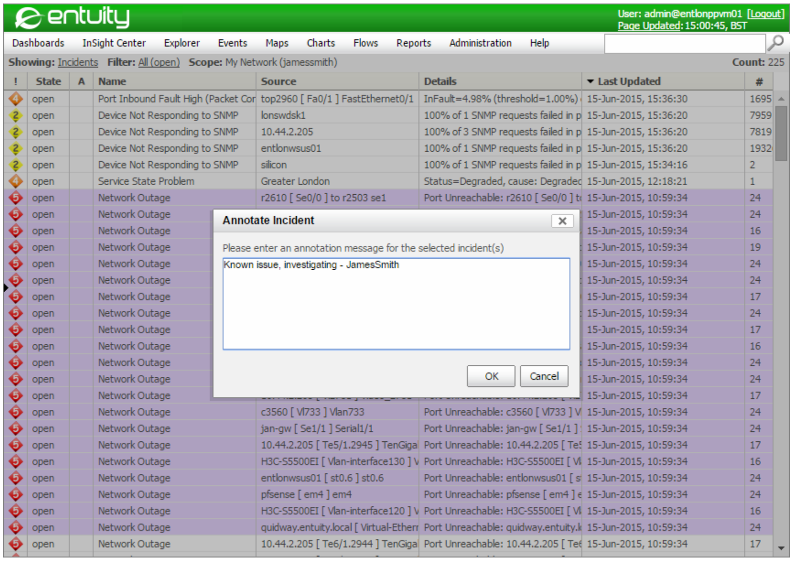
## Annotating Incidents

Annotations allow you to associate a short note to one or more selected incidents. This annotation can be viewed and updated by all users with access to the incident, the Annotation icon in the A column clearly indicates annotated incidents. Annotations can be used for any for any number of reasons, for example to indicate the action being undertaken on an issue.

From Event Viewer you can annotate incidents:

1) Highlight the required incident.

2) From the context menu click **Annotate**.



**Showing:** Incidents **Filter:** All (open) **Scope:** My Network (jamessmith) **Count:** 225

| ! | State | A | Name | Source | Details | ▼ Last Updated | # |
|---|---|---|---|---|---|---|---|
| 4 | open | | Port Inbound Fault High (Packet Cor | top2960 [ Fa0/1 ] FastEthernet0/1 | InFault=4.98% (threshold=1.00%) | 15-Jun-2015, 15:36:30 | 1695 |
| 2 | open | | Device Not Responding to SNMP | lonswdsk1 | 100% of 1 SNMP requests failed in p | 15-Jun-2015, 15:36:20 | 7959 |
| 2 | open | | Device Not Responding to SNMP | 10.44.2.205 | 100% of 3 SNMP requests failed in p | 15-Jun-2015, 15:36:20 | 7819 |
| 2 | open | | Device Not Responding to SNMP | entlonwsus01 | 100% of 1 SNMP requests failed in p | 15-Jun-2015, 15:36:20 | 1932 |
| 2 | open | | Device Not Responding to SNMP | silicon | 100% of 1 SNMP requests failed in p | 15-Jun-2015, 15:34:16 | 2 |
| 4 | open | | Service State Problem | Greater London | Status=Degraded, cause: Degradec | 15-Jun-2015, 12:18:21 | 1 |
| 5 | open | | Network Outage | r2610 [ Se0/0 ] to r2503 se1 | Port Unreachable: r2610 [ Se0/0 ] t | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 19 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | | | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | | Network Outage | c3560 [ Vl733 ] Vlan733 | Port Unreachable: c3560 [ Vl733 ] V | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | jan-gw [ Se1/1 ] Serial1/1 | Port Unreachable: jan-gw [ Se1/1 ] | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | 10.44.2.205 [ Te5/1.2945 ] TenGiga | Port Unreachable: 10.44.2.205 [ Te5 | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | | Network Outage | H3C-S5500EI [ Vlan-interface130 ] V | Port Unreachable: H3C-S5500EI [ Vl | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | | Network Outage | entlonwsus01 [ st0.6 ] st0.6 | Port Unreachable: entlonwsus01 [ s | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | pfsense [ em4 ] em4 | Port Unreachable: pfsense [ em4 ] e | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | H3C-S5500EI [ Vlan-interface120 ] V | Port Unreachable: H3C-S5500EI [ Vl | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | | Network Outage | quidway.entuity.local [ Virtual-Etherr | Port Unreachable: quidway.entuity.l | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | 10.44.2.205 [ Te6/1.2944 ] TenGiga | Port Unreachable: 10.44.2.205 [ Te6 | 15-Jun-2015, 10:59:34 | 17 |

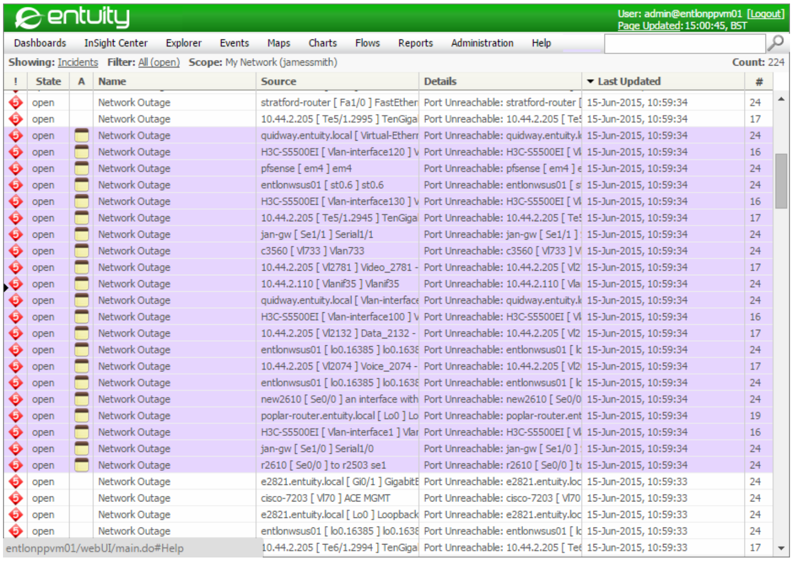
**Annotate Incident**

Please enter an annotation message for the selected incident(s)

Known issue, investigating - JamesSmith

Figure 36 Annotate Incidents

3) Enter the annotation.



**Showing:** Incidents **Filter:** All (open) **Scope:** My Network (jamessmith) **Count:** 224

| ! | State | A | Name | Source | Details | ▼ Last Updated | # |
|---|---|---|---|---|---|---|---|
| 5 | open | | Network Outage | stratford-router [ Fa1/0 ] FastEther | Port Unreachable: stratford-router [ | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | 10.44.2.205 [ Te5/1.2995 ] TenGiga | Port Unreachable: 10.44.2.205 [ Te5 | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | 🗒 | Network Outage | quidway.entuity.local [ Virtual-Etherr | Port Unreachable: quidway.entuity.l | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | H3C-S5500EI [ Vlan-interface120 ] V | Port Unreachable: H3C-S5500EI [ Vl | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | 🗒 | Network Outage | pfsense [ em4 ] em4 | Port Unreachable: pfsense [ em4 ] e | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | entlonwsus01 [ st0.6 ] st0.6 | Port Unreachable: entlonwsus01 [ s | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | H3C-S5500EI [ Vlan-interface130 ] V | Port Unreachable: H3C-S5500EI [ Vl | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | 🗒 | Network Outage | 10.44.2.205 [ Te5/1.2945 ] TenGiga | Port Unreachable: 10.44.2.205 [ Te5 | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | 🗒 | Network Outage | jan-gw [ Se1/1 ] Serial1/1 | Port Unreachable: jan-gw [ Se1/1 ] | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | c3560 [ Vl733 ] Vlan733 | Port Unreachable: c3560 [ Vl733 ] V | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | 10.44.2.205 [ Vl2781 ] Video_2781 - | Port Unreachable: 10.44.2.205 [ Vl2 | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | 🗒 | Network Outage | 10.44.2.110 [ Vlanif35 ] Vlanif35 | Port Unreachable: 10.44.2.110 [ Vla | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | quidway.entuity.local [ Vlan-interface | Port Unreachable: quidway.entuity.l | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | H3C-S5500EI [ Vlan-interface100 ] V | Port Unreachable: H3C-S5500EI [ Vl | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | 🗒 | Network Outage | 10.44.2.205 [ Vl2132 ] Data_2132 - | Port Unreachable: 10.44.2.205 [ Vl2 | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | 🗒 | Network Outage | entlonwsus01 [ lo0.16385 ] lo0.1638 | Port Unreachable: entlonwsus01 [ lo | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | 10.44.2.205 [ Vl2074 ] Voice_2074 - | Port Unreachable: 10.44.2.205 [ Vl2 | 15-Jun-2015, 10:59:34 | 17 |
| 5 | open | 🗒 | Network Outage | entlonwsus01 [ lo0.16385 ] lo0.1638 | Port Unreachable: entlonwsus01 [ lo | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | new2610 [ Se0/0 ] an interface with | Port Unreachable: new2610 [ Se0/0 | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | poplar-router.entuity.local [ Lo0 ] Lo | Port Unreachable: poplar-router.ent | 15-Jun-2015, 10:59:34 | 19 |
| 5 | open | 🗒 | Network Outage | H3C-S5500EI [ Vlan-interface1 ] Vlar | Port Unreachable: H3C-S5500EI [ Vl | 15-Jun-2015, 10:59:34 | 16 |
| 5 | open | 🗒 | Network Outage | jan-gw [ Se1/0 ] Serial1/0 | Port Unreachable: jan-gw [ Se1/0 ] | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | 🗒 | Network Outage | r2610 [ Se0/0 ] to r2503 se1 | Port Unreachable: r2610 [ Se0/0 ] t | 15-Jun-2015, 10:59:34 | 24 |
| 5 | open | | Network Outage | e2821.entuity.local [ Gi0/1 ] GigabitE | Port Unreachable: e2821.entuity.loc | 15-Jun-2015, 10:59:33 | 24 |
| 5 | open | | Network Outage | cisco-7203 [ Vl70 ] ACE MGMT | Port Unreachable: cisco-7203 [ Vl70 | 15-Jun-2015, 10:59:33 | 24 |
| 5 | open | | Network Outage | e2821.entuity.local [ Lo0 ] Loopback | Port Unreachable: e2821.entuity.loc | 15-Jun-2015, 10:59:33 | 24 |
| 5 | open | | Network Outage | entlonwsus01 [ lo0.16385 ] lo0.1638 | Port Unreachable: entlonwsus01 [ lo | 15-Jun-2015, 10:59:33 | 24 |
| | | | | 10.44.2.205 [ Te6/1.2994 ] TenGiga | Port Unreachable: 10.44.2.205 [ Te6 | 15-Jun-2015, 10:59:33 | 17 |

entlonppvm01/webUI/main.do#Help

Figure 37 Annotated Incidents

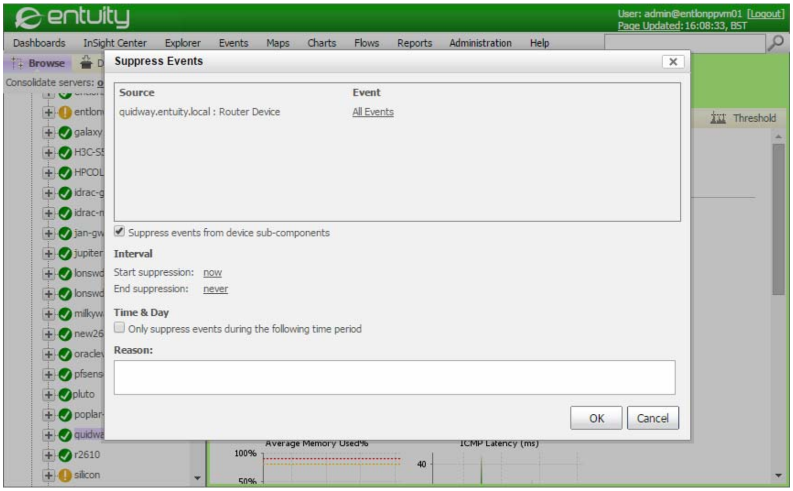
# Event Suppression

You can prevent Entuity raising events against managed objects and this would also impact on the raising of incidents associated with those events. Event suppression can be useful, for example, when a device is down for maintenance or a problem is known and you do not want Entuity to raise further events.

Entuity includes two separate event suppression mechanisms, through the:

- Event Management System system administrators, and users with the Event Administration tool permission, can define suppression rules. The suppression control available through Events Administration makes it the appropriate method for system wide or complex rules. Only system administrators can view and amend these suppression rules. (See *Rule Types and Supplied Rules*.)
- Suppress Events dialog system administrators, and users with the Event Suppression tool permission, can suppress events. System administrators can view all suppression rules, users with the tool permission can view the rules they set up and rules set up against objects to which they have access.

  Event Suppressions dialog provides a simpler interface to event suppression than the rules interface available through Events Administration, making it easier to associate suppression with managed objects which is especially true in a multi-server environment. Changes to these suppressions are also tracked by Audit Log. (See *Chapter 41 - Audit Log*.)



Suppress Events

| Source | Event |
|---|---|
| quidway.entuity.local : Router Device | All Events |

☑ Suppress events from device sub-components

Interval

Start suppression: now

End suppression: never

Time & Day

□ Only suppress events during the following time period

Reason:

Figure 38 Suppress Events Called From Explorer

Through the Suppress Events dialog you can:

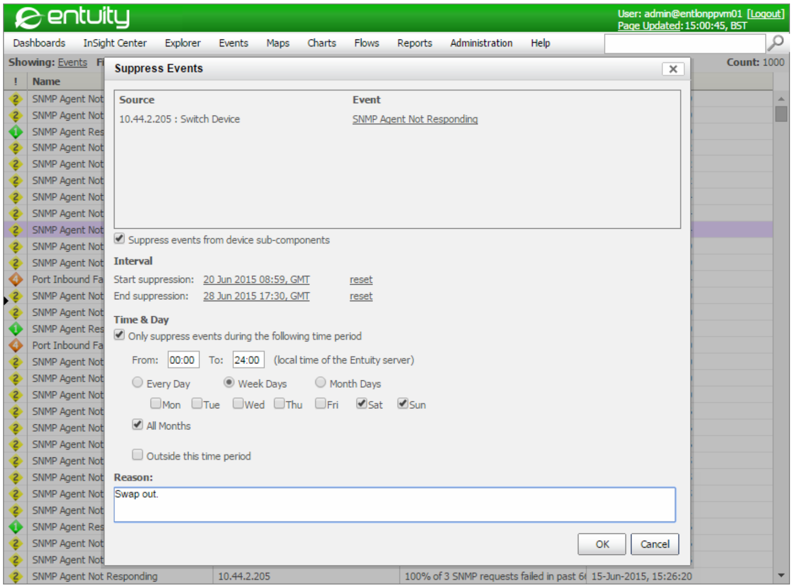
- Set the object against which to apply event suppression, and when that object is a device whether to also suppress events raised against its sub-components, e.g. ports, CPUs.
- Set for how long an event suppression rule applies.

- Set periods of the day, week and month when event suppression applies and when it does not.
- Enter the reason for event suppression.

Event suppression rules are configured through an Event Suppression dialog which you can call from a context menu by selecting:

- A raised event from Event Viewer. By default this suppresses the raising of the selected event against the managed object, for example a Network Outage event raised against the device nickel.
- A managed object from the Explorer object tree. By default this suppresses the raising of all events against the object.

You can specify suppression rules which Entuity applies against the selected managed object, or managed object - event type.



Suppress Events

| Source | Event |
|---|---|
| 10.44.2.205 : Switch Device | SNMP Agent Not Responding |

☑ Suppress events from device sub-components

Interval

Start suppression: 20 Jun 2015 08:59, GMT reset

End suppression: 28 Jun 2015 17:30, GMT reset

Time & Day

☑ Only suppress events during the following time period

From: 00:00 To: 24:00 (local time of the Entuity server)

○ Every Day ● Week Days ○ Month Days

□ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat ☑ Sun

☑ All Months

□ Outside this time period

Reason:

Swap out.

Figure 39 Suppress Events Dialog Expanded

There three components to defining Event Suppressions:

- Define the source of the event and the event types.

| Attribute | Description |
|---|---|
| *Source* | The selected source of the event to which suppression rules apply. This is fixed as the object you selected from the Explorer tree, or the source of the event you highlighted in Event Viewer. |

Table 17 Event Suppression

| Attribute | Description |
|---|---|
| *Event* | The selected event type(s) which the event suppression rules apply. You can select 1 event, a selection of events or all events. |
| *Suppress events from device sub-components* | Check the check box to prevent Entuity raising events against the sub-components of the device, for example, CPUs, ports. |
| *Reason* | Enter a meaningful description of the purpose of the rule. This description identifies the rule in the Suppression Rules page. |

Table 17 Event Suppression

- Define the suppression interval, when the suppression is active.

| Interval | Description |
|---|---|
| *Start suppression* | Date and time from when Entuity applies the suppression rule, by default now. Data and time are taken from the Entuity server. |
| *End suppression* | Date and time until when Entuity applies the suppression rule. By default set to **Never** so Entuity would always apply the rule, when amended to an expiry date which then passes Entuity would stop applying the rule but would not delete it. Data and time are taken from the Entuity server. |
| *reset* | Resets the suppression interval to its default value; *Start suppression* set to **Now** and *End suppression* to **never**. |

Table 18 Event Suppression Interval

- Define the time period.

| Time & Day | Description |
|---|---|
| *Only suppress events during the following time period* | During the defined suppression interval when:<br>■ Checked Entuity only applies the suppression rule during the defined period. On checking the box Entuity displays the Time & Day options.<br>■ Unchecked Entuity always applies the suppression rule. |
| *From / To* | The period within a day that Entuity should apply the suppression rule, by default 24 hours. |
| *Days* | The days of the week Entuity should apply the suppression rule:<br>■ Every Day (default).<br>■ Week Days, you can set particular days of the week for Entuity to apply the suppression rule.<br>■ Month Days, you can set particular days of the month, using dashes to create inclusive sets of dates, and comma delimited lists. For example to include the first, third and fifth 5 day periods in a month enter `1-5, 11-15, 21-25`. |

Table 19 Event Suppression Time

| Time & Day | Description |
|---|---|
| *All Months* | During the defined suppression interval when:<br>■ Checked (default) Entuity applies the suppression rule to all months.<br>■ Unchecked you can set particular months for Entuity to apply the suppression rule. |
| *Outside this time period* | When selected Entuity inverses when to apply the suppression rule, for example when the rule is only to be applied on Sundays, when inversed it would be applied all days apart from Sundays. |

Table 19 Event Suppression Time

## How to Suppress All Events On a Device

To suppress all events against a managed object (e.g. a router):

1) Use Explorer to find and then highlight the router.
2) From the context menu click **Suppress Events...**.

   By default Entuity creates a rule that suppresses all events on that device, and its sub-components, with a start date of now and no end date.
3) Configure the time period for which the event is suppressed, and enter a meaningful reason for why events are suppressed.
4) Click **OK**. Entuity displays a dialog indicating the success or failure of your attempt to suppress events.

   When successful you can view, edit and remove the suppression rules through the Suppression Rules page.

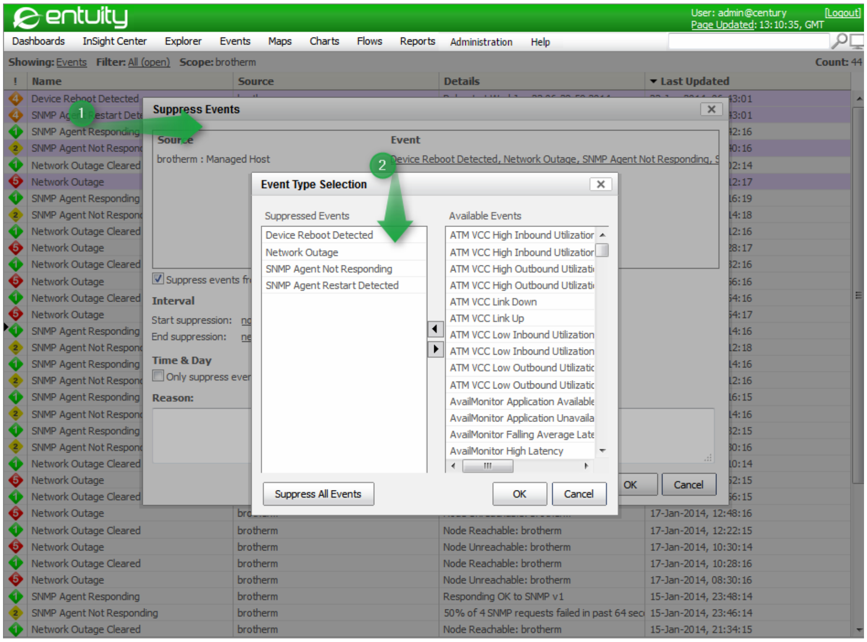
## How to Suppress Events of a Set Type on a Device

To suppress events of a set type against a managed object (e.g. a router):

1) In Explorer select the device and then Events. Event Viewer displays current incidents for the device.
2) Click **Incidents** and select **Events**.
3) In Event Viewer highlight event(s) of the type you want to suppress.
4) From the context menu click **Suppress Events**.

   By default Entuity creates a rule that suppresses events of the selected type(s) on that device, and its sub-components, with a start date of now and no end date.

   You can click on the list of selected events to view all of those selected through the Event Type Selection dialog. You also have the option of adjusting the selected events.



Showing: Events Filter: All (open) Scope: brotherm Count: 44

Suppress Events

| Source | Event |
|---|---|
| brotherm : Managed Host | Device Reboot Detected, Network Outage, SNMP Agent Not Responding, S |

☑ Suppress events fr

Interval

Start suppression: nc

End suppression: ne

Time & Day

☐ Only suppress ever

Reason:

Event Type Selection

Suppressed Events:

- Device Reboot Detected
- Network Outage
- SNMP Agent Not Responding
- SNMP Agent Restart Detected

Available Events:

- ATM VCC High Inbound Utilizatior
- ATM VCC High Inbound Utilizatior
- ATM VCC High Outbound Utilizati
- ATM VCC High Outbound Utilizati
- ATM VCC Link Down
- ATM VCC Link Up
- ATM VCC Low Inbound Utilization
- ATM VCC Low Inbound Utilization
- ATM VCC Low Outbound Utilizatic
- ATM VCC Low Outbound Utilizatic
- AvailMonitor Application Available
- AvailMonitor Application Unavaila
- AvailMonitor Falling Average Late
- AvailMonitor High Latency

| ! | Name | Source | Details | Last Updated |
|---|---|---|---|---|
| 5 | Network Outage | brotherm | Node Reachable: brotherm | 17-Jan-2014, 12:48:16 |
| 1 | Network Outage Cleared | brotherm | Node Reachable: brotherm | 17-Jan-2014, 12:22:15 |
| 5 | Network Outage | brotherm | Node Unreachable: brotherm | 17-Jan-2014, 10:30:14 |
| 1 | Network Outage Cleared | brotherm | Node Reachable: brotherm | 17-Jan-2014, 10:28:16 |
| 5 | Network Outage | brotherm | Node Unreachable: brotherm | 17-Jan-2014, 08:30:16 |
| 1 | SNMP Agent Responding | brotherm | Responding OK to SNMP v1 | 15-Jan-2014, 23:48:14 |
| 2 | SNMP Agent Not Responding | brotherm | 50% of 4 SNMP requests failed in past 64 seci | 15-Jan-2014, 23:46:14 |
| 1 | Network Outage Cleared | brotherm | Node Reachable: brotherm | 15-Jan-2014, 21:34:15 |

Figure 40 Suppress All Events for the Selected Object

5) Configure the time period for which the event is suppressed, and enter a meaningful reason for why events are suppressed.

6) Click **OK**. Entuity displays a dialog indicating the success or failure of your attempt to suppress events.

   When successful you can view, edit and remove the suppression rules through the Suppression Rules page.

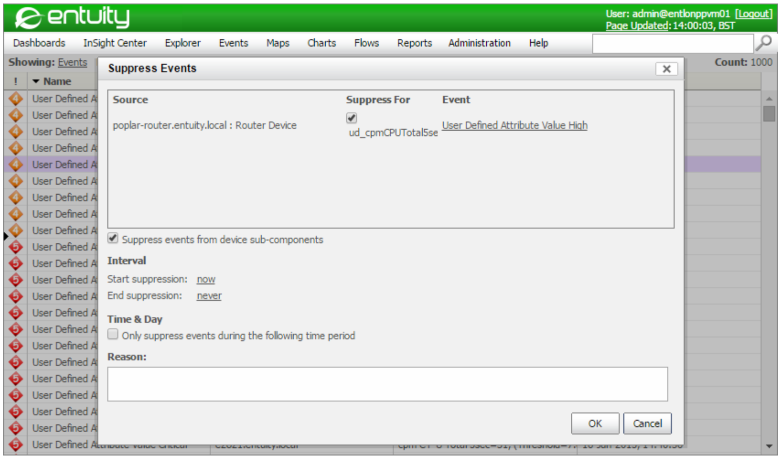
## How to Suppress Events Using Secondary Identifiers

Depending upon the event type you can prevent Entuity from raising an event using a secondary attribute. For example:

- The Network Outage event may be raised against a port but where the port has more than one address it will also include the IP address. You can then select to only suppress the event on that IP address.
- User Defined Polling uses the same event types for all user defined attributes. When an event is raised you have the option of suppressing the raising of that event type for all attributes on the managed object, or only suppressing that user defined event for the current attribute.

Through the Event Management System you can define events and incidents, with rules that raise these events when particular user defined events are raised against specified attributes

The originating events can be suppressed. In this way different attributes have their own events and incidents rather than using the standard user defined events and incidents.


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 14:00:03, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
Showing: Events
Count: 1000
! Name
User Defined A

Suppress Events

| Source | Suppress For | Event |
|---|---|---|
| poplar-router.entuity.local : Router Device | ☑ ud_cpmCPUTotal5se | User Defined Attribute Value High |

☑ Suppress events from device sub-components

Interval

Start suppression: now

End suppression: never

Time & Day

☐ Only suppress events during the following time period

Reason:

Figure 41 Event Suppression on User Defined Attribute

This example suppresses the Network Outage event for a particular IP address on a port, the port has multiple IP addresses. The Network Outage event can be raised against the same port but using different IP addresses. If you create an event suppression for Network Outage events by:

- From the Explorer navigation tree selecting the port then the event is automatically suppressed for all IP addresses on that port.
- Highlighting the raised event in the viewer then you can select to suppress the raising of the event against that IP address.

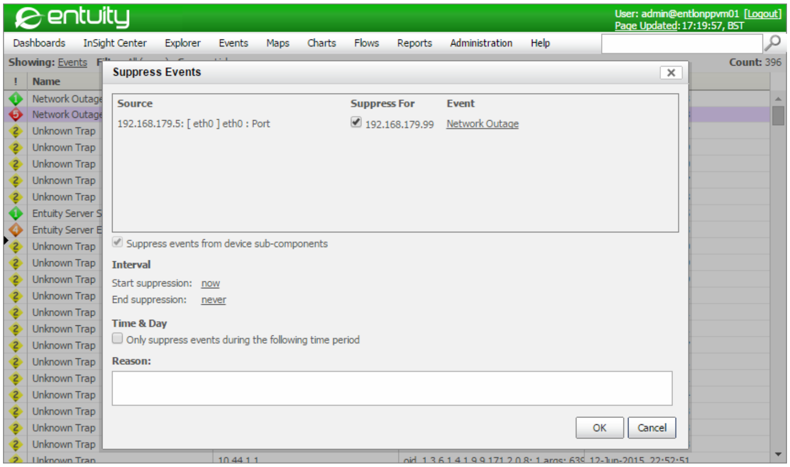
To suppress the raising of Network Outage events against an IP address:

1) In Explorer select the device and then Events. Event Viewer displays current incidents for the device.

2) Click **Incidents** and select **Events**.

3) Highlight the event and from the context-menu select **Event Suppression**.

4) Click the check box *In the Suppress For* column. If you leave the check box unchecked Entuity suppresses all Network Outage events raised against the port.



**Suppress Events**

| Source | Suppress For | Event |
|---|---|---|
| 192.168.179.5: [ eth0 ] eth0 : Port | ☑ 192.168.179.99 | Network Outage |

☑ Suppress events from device sub-components

**Interval**

Start suppression: now

End suppression: never

**Time & Day**

□ Only suppress events during the following time period

**Reason:**

Figure 42 Event Suppression by IP Address

## Manage Event Suppression Rules

Viewing, amending and deleting suppression rules is through the Event Suppressions page. System administrators can access all suppression definitions, users with the Event Suppressions tool permission can access definitions applied to objects to which they have access.

You can deactivate event suppression rules by setting an elapsed date, after which suppression rules are expired but by default are not deleted. You can delete expired rules:

- By setting *deleteExpiredEventSuppressionsPeriodSeconds* in *entuity_home*`\etc\entuity.cfg`. Entuity deletes suppression rules that are expired for the set period or longer.
- through the Event Suppressions page.

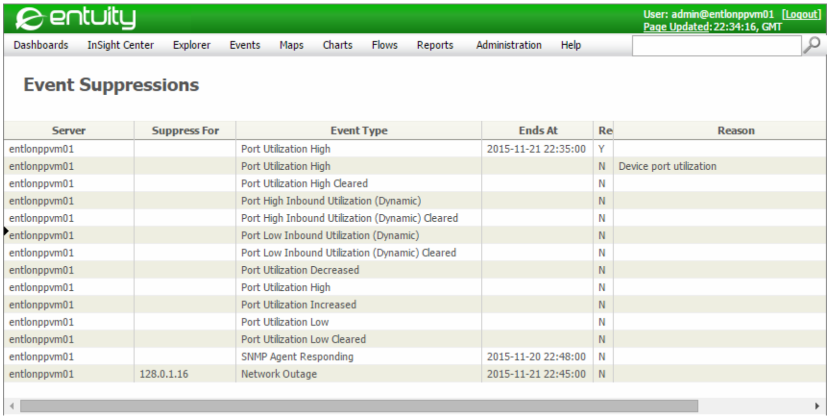
### Access Event Suppression Rules

To view suppression rules:

1) Click **Administration** > **Events** > **Suppression Rules**.

   By default Entuity shows expired suppression rules.

2) Deselect **Show expired suppressions** to only show expired rules.



Event Suppressions

| Server | Suppress For | Event Type | Ends At | Re | Reason |
|---|---|---|---|---|---|
| entlonppvm01 | | Port Utilization High | 2015-11-21 22:35:00 | Y | |
| entlonppvm01 | | Port Utilization High | | N | Device port utilization |
| entlonppvm01 | | Port Utilization High Cleared | | N | |
| entlonppvm01 | | Port High Inbound Utilization (Dynamic) | | N | |
| entlonppvm01 | | Port High Inbound Utilization (Dynamic) Cleared | | N | |
| entlonppvm01 | | Port Low Inbound Utilization (Dynamic) | | N | |
| entlonppvm01 | | Port Low Inbound Utilization (Dynamic) Cleared | | N | |
| entlonppvm01 | | Port Utilization Decreased | | N | |
| entlonppvm01 | | Port Utilization High | | N | |
| entlonppvm01 | | Port Utilization Increased | | N | |
| entlonppvm01 | | Port Utilization Low | | N | |
| entlonppvm01 | | Port Utilization Low Cleared | | N | |
| entlonppvm01 | | SNMP Agent Responding | 2015-11-20 22:48:00 | N | |
| entlonppvm01 | 128.0.1.16 | Network Outage | 2015-11-21 22:45:00 | N | |

Figure 43 Event Suppression Administration

| Attribute | Description |
|---|---|
| *Server* | Entuity Server on which the event is suppressed. |
| *Source* | The selected source of the event to which suppression rules apply. This is fixed as the object you selected from the Explorer tree, or the source of the event you highlighted in Event Viewer. |
| *Suppress For* | The attribute value on which the event is suppressed, for example IP address. |
| *Event Type* | The selected event type to which the event suppression rule applies. When creating the rule if you selected a number of event types for it to apply against, then Entuity created a separate rule for each event type; so within this table they are separately listed. |
| *Ends At* | The date and time the suppression rule applied until. When blank the suppression rule does not have an end date and so is always active. |
| Re | Recurrence indicates a Time & Day schedule is applied. |
| *Reason* | Enter a meaningful description of the purpose of the rule. This description identifies the rule in the Suppression Rules page. |
| *Last Updated By* | User name of the last person to update the suppression rule. |
| *Type* | Object type of the event against which the suppression rule is defined, e.g. Switch, Managed Host. |
| *Sub Components* | When set to:<br>■ **Y** the suppression rule also applies to subcomponents of the object type.<br>■ **N** the suppression rule only applies to the current object. |
| *Starts At* | When the rule is for a set time period Entuity displays the start time and date. |
| *Last Updated At* | When the suppression rule was last updated. |

Table 20 Event Suppressions

## Removing Event Suppression Rules

To remove suppression rules:

1) Click **Administration** > **Events** > **Suppression Rules**.
2) Highlight the rules you want to delete, allowing those events to be raised against those devices.
3) Click **Delete**. Entuity deletes the selected suppression rule(s).

### Editing Event Suppression Rules

You can amend event suppression rules, for example you may want to temporarily deactivate a rule, or change when it is applicable. You can also select multiple rules when they have the same source. You cannot change the source of the event or the event type.

To amend suppression rules:

1) Click **Administration** > **Events** > **Suppression Rules**.
2) Highlight the rule you want to amend.
3) Click **Edit**.
4) Amend the suppression rule and click **OK**. The change to the rule is immediately applied.

## Event Notifications

Event Notification allows you to configure Entuity to generate emails to send to recipients when Entuity raises events that meet the set criteria. For example, you can configure Entuity to send emails to on-call support staff when severe events are raised against key devices during out of office hours.

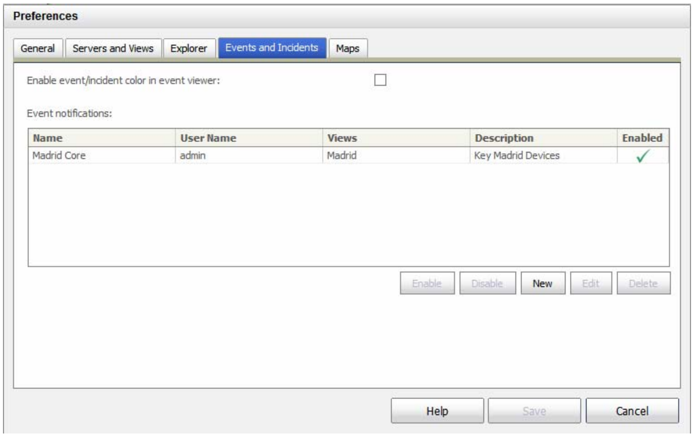
Entuity includes two notification methods:

- Through the Events and Incidents tab in the Preferences dialog.
- Using Event Management System, defining rules and/or triggers and applying the Send e-mail action.

From the Event notification section Preferences page:

- System Administrators can create event notifications, and view, amend and delete all event notifications.
- Non-system administrators with the Event Notifications tool permission can view event notification configurations assigned to their user name. They can create, suspend, amend and delete event notifications configured against their user name.
- Non-system administrators can only view the event notifications assigned to them.

For Entuity to generate emails you must have specified an SMTP server during Entuity `configure`.



Enable event/incident color in event viewer: □

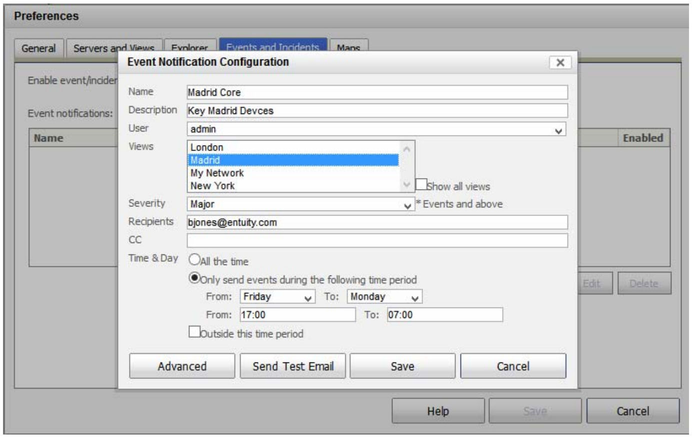
Event notifications:

| Name | User Name | Views | Description | Enabled |
|---|---|---|---|---|
| Madrid Core | admin | Madrid | Key Madrid Devices | ✓ |

Figure 44 Event Notifications

| Attribute | Description |
|---|---|
| *Name* | Unique name for the event notification. |
| *Description* | Meaningful description of the notification, e.g. its purpose. |
| *User* | Entuity user associated with the notification. |
| *Servers* | Entuity server(s) which can raise this notification. Entuity displays all of the connected servers for which you have access rights. |
| *Views* | The view(s) Entuity monitors for raising notifications. |
| *Show all views* | Displays all views, including views to which the selected *User* does not have access. |
| *Severity* | Sets the minimum severity level of events within the view that raise a notification. |
| *Recipients* | Email addresses of users you want to receive notifications. |
| *CC* | Email addresses of users you want to be copied in on notifications. |
| *Time & Day* | Specify a date and time range for the notification. |
| *Outside this time period* | When:<br>■ Selected, notifications can only be raised outside the specified *Time & Day*, e.g. when you specify office hours (8:00 to 18:00, Monday to Friday) notifications would only be sent outside of those hours.<br>■ Not selected, notifications can only be raised within the specified *Time & Day*, e.g. when you specify a weekend (18:01 to 07:59, to Friday to Monday) notifications would only be raised within those hours. |

Table 21 Configure Event Notification



Name: Madrid Core

Description: Key Madrid Devces

User: admin

Views: London, Madrid, My Network, New York

□ Show all views

Severity: Major * Events and above

Recipients: bjones@entuity.com

CC:

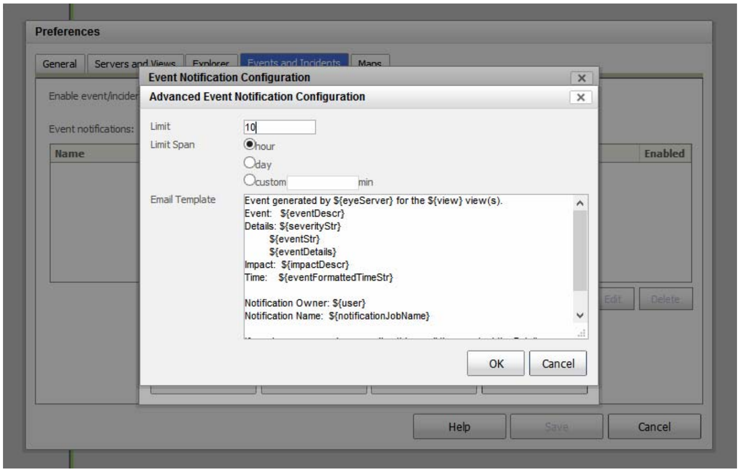
Time & Day:
○ All the time
● Only send events during the following time period
From: Friday To: Monday
From: 17:00 To: 07:00
□ Outside this time period

Figure 45 Event Notification Configuration

Notification also includes advanced options, accessible through the Advanced button on the Event Notification Configuration dialog:

- *Limit*, the maximum number of this notification that Entuity can send within a time period specified in *Limit Span*.
- *Limit Span*, the period within which *Limit* applies, i.e. hour (default), day, custom (user defined period).
- *Event Template*, is a combination of text and event variables from which the content of the notification is generated. Entuity has a default template:

```
Event generated by ${eyeServer} for the ${view} view.
Event:   ${eventDescr}
Details: ${severityStr}
         ${eventStr}
         ${eventDetails}
Impact:  ${impactDescr}
Time:    ${eventFormattedTimeStr}
Notification Owner: ${user}
Notification Name:  ${notificationJobName}
If you have any queries regarding this email then contact the Entuity
Administrator.
```



Limit: 10

Limit Span: ● hour ○ day ○ custom min

Email Template:

```
Event generated by ${eyeServer} for the ${view} view(s).
Event:   ${eventDescr}
Details: ${severityStr}
         ${eventStr}
         ${eventDetails}
Impact:  ${impactDescr}
Time:    ${eventFormattedTimeStr}

Notification Owner: ${user}
Notification Name:  ${notificationJobName}
```

Figure 46 Event Notification Advanced Configuration

## Creating Event Notifications

To configure a new event notification:

1) Click **Administration** > **Preferences**.

2) Click the Events and Incidents tab and from the Event Notification section click **New**. Entuity displays the Event Notification Configuration dialog.

3) Complete the notification select:

- **Advanced** to amend the email message, and set limits on the number of notifications within a time period.
- **Send Test Email**, to test your notification setup.
- **Save**, to save and enable the notification.

## Updating Event Notifications

To view and amend notifications:

1) Click **Administration** > **Preferences**.

2) Click the Events and Incidents tab.

   The Event Notifications section displays notifications to which your account has access, both on the local Entuity server and any connected remote servers.

3) Highlight a notification and select:

- **Edit**, Entuity opens the Event Notification Configuration dialog.
- **Disable**, Entuity deactivates the notification.
- **Enable**, Entuity activates the notification.
- **Delete**, Entuity removes the notification.

# 4 Use Dashboards to Monitor Performance

Dashboards are available for those users with the appropriate access rights. Entuity currently includes these dashboards:

- Status Summary provides a status summary for each Entuity view on the current server. In Entuity multi-server environments it can also provide a summary of the state of views on remote Entuity servers.
- Service Summary provides a summary of viewable services, indicating service name and state with drill down capability.
- TopN Summary provides a view specific dashboard measuring the status of your network against six performance metrics. For each of these measures you can access port details.
- Device Metrics allows selection of both the devices you want to monitor, and the metrics you want to use.
- Custom Dashboards allow users to develop their own dashboards, with up to five running at any one time.

## Status Summary Dashboard

Status Summary dashboard delivers an overview of network status by summarizing the state of each view to which you have access. You can further restrict the available views through your user preferences.

When you have the appropriate access rights, the dashboard includes context dependent links to Explorer, Services, the Device Status report and Event Viewer.

By default the Status Summary dashboard is the home page for users that are not members of the Administrator user group, the first page Entuity displays after successfully logging in. Also by default Entuity refreshes the page content every five minutes. You can set your own default landing page and Auto-Refresh rate through your user preferences.

| Attribute | Description |
|---|---|
| *Views* | Name of the Entuity view. You can click on it to open Explorer with the focus on that view. |
| *Services* | Number of services associated with the view. |
| *Service Status* | The segments in the colored bar indicate the current states of services within a view. When you place the mouse over a colored segment Entuity displays a breakdown of the services in that state, e.g. **75% (6/8) Up**. Entuity displays **N/A** (Not Applicable), when there are no services in the view.<br>The percentage value represents the number of services in the view with an UP state as a percentage of the total number of services in the view. You can click through to access a summary of services in the view. |
| *Devices* | Number of devices within the view. |

Table 22 Status Summary Dashboard

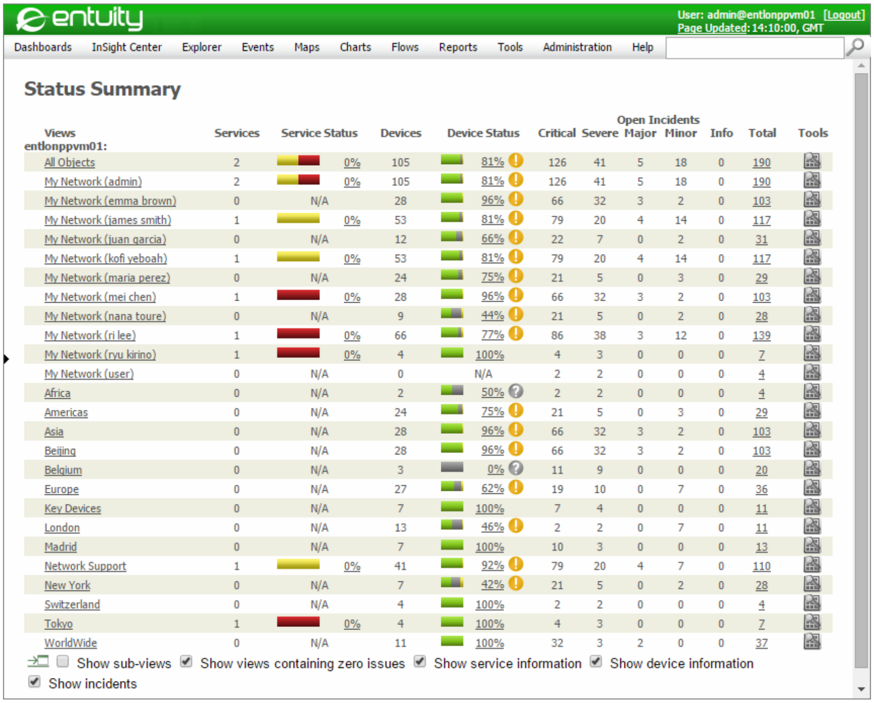
| Attribute | Description |
|---|---|
| *Device Status* | Entuity determines device state by their responses to ICMP ping and/or SNMP polling, hostname resolution and system status.<br>The segments in the colored bar indicate the current states of devices within a view. When you place the mouse over a colored segment Entuity displays a breakdown of the devices in that state, e.g. for a green segment **83.2% (119/143) Ok**.<br>The percentage value represents the number of devices within the view that are OK, as a percentage of the total number of devices in the view. You can click on the hyperlink to launch the Device Status report which shows the current state of devices.<br>The device state icon represents the worst state of a device within the view. When you rollover the icon Entuity displays a breakdown of device states within the view, for example **1 device is degraded 1 device is in unknown state**. |
| *Open Incidents* | A by incident severity breakdown of incidents raised against devices in the view. You can click on the *Total* hyperlink to view the current open incidents for the view. |
| ⇥ | Click on this icon to open the dashboard in a new browser page. Alternatively you can add the Status Summary dashboard to a custom dashboard by dragging and dropping the icon to the Dashboard Editor. |
| *Show sub-views* | When checked the dashboard displays sub-views and their states, when unchecked the dashboard only displays top-level views. |
| *Show views containing zero issues* | When checked the dashboard displays all views and their states, when unchecked the dashboard only displays views reporting problems. |
| Show service Information | When checked the dashboard displays the Services and Service Status columns, when unchecked the dashboard does not display service information. |
| *Show device information* | When checked the dashboard displays the Devices and Device Status columns, when unchecked the dashboard does not display device information. |
| *Show incidents* | When checked the dashboard displays the Open Incidents columns, when unchecked the dashboard does not display incident information. |

Table 22 Status Summary Dashboard

## Opening the Status Summary Dashboard

To access the Status Summary dashboard:

1) Click **Dashboards > Status Summary**.



User: admin@entlonppvm01 [Logout]
Page Updated: 14:10:00, GMT

Status Summary

entlonppvm01:

| Views | Services | Service Status | Devices | Device Status | Open Incidents<br>Critical | Severe | Major | Minor | Info | Total | Tools |
|---|---|---|---|---|---|---|---|---|---|---|---|
| All Objects | 2 | 0% | 105 | 81% | 126 | 41 | 5 | 18 | 0 | 190 | |
| My Network (admin) | 2 | 0% | 105 | 81% | 126 | 41 | 5 | 18 | 0 | 190 | |
| My Network (emma brown) | 0 | N/A | 28 | 96% | 66 | 32 | 3 | 2 | 0 | 103 | |
| My Network (james smith) | 1 | 0% | 53 | 81% | 79 | 20 | 4 | 14 | 0 | 117 | |
| My Network (juan garcia) | 0 | N/A | 12 | 66% | 22 | 7 | 0 | 2 | 0 | 31 | |
| My Network (kofi yeboah) | 1 | 0% | 53 | 81% | 79 | 20 | 4 | 14 | 0 | 117 | |
| My Network (maria perez) | 0 | N/A | 24 | 75% | 21 | 5 | 0 | 3 | 0 | 29 | |
| My Network (mei chen) | 1 | 0% | 28 | 96% | 66 | 32 | 3 | 2 | 0 | 103 | |
| My Network (nana toure) | 0 | N/A | 9 | 44% | 21 | 5 | 0 | 2 | 0 | 28 | |
| My Network (ri lee) | 1 | 0% | 66 | 77% | 86 | 38 | 3 | 12 | 0 | 139 | |
| My Network (ryu kirino) | 1 | 0% | 4 | 100% | 4 | 3 | 0 | 0 | 0 | 7 | |
| My Network (user) | 0 | N/A | 0 | N/A | 2 | 2 | 0 | 0 | 0 | 4 | |
| Africa | 0 | N/A | 2 | 50% | 2 | 2 | 0 | 0 | 0 | 4 | |
| Americas | 0 | N/A | 24 | 75% | 21 | 5 | 0 | 3 | 0 | 29 | |
| Asia | 0 | N/A | 28 | 96% | 66 | 32 | 3 | 2 | 0 | 103 | |
| Beijing | 0 | N/A | 28 | 96% | 66 | 32 | 3 | 2 | 0 | 103 | |
| Belgium | 0 | N/A | 3 | 0% | 11 | 9 | 0 | 0 | 0 | 20 | |
| Europe | 0 | N/A | 27 | 62% | 19 | 10 | 0 | 7 | 0 | 36 | |
| Key Devices | 0 | N/A | 7 | 100% | 7 | 4 | 0 | 0 | 0 | 11 | |
| London | 0 | N/A | 13 | 46% | 2 | 2 | 0 | 7 | 0 | 11 | |
| Madrid | 0 | N/A | 7 | 100% | 10 | 3 | 0 | 0 | 0 | 13 | |
| Network Support | 1 | 0% | 41 | 92% | 79 | 20 | 4 | 7 | 0 | 110 | |
| New York | 0 | N/A | 7 | 42% | 21 | 5 | 0 | 2 | 0 | 28 | |
| Switzerland | 0 | N/A | 4 | 100% | 2 | 2 | 0 | 0 | 0 | 4 | |
| Tokyo | 1 | 0% | 4 | 100% | 4 | 3 | 0 | 0 | 0 | 7 | |
| WorldWide | 0 | N/A | 11 | 100% | 32 | 3 | 2 | 0 | 0 | 37 | |

□ Show sub-views ☑ Show views containing zero issues ☑ Show service information ☑ Show device information
☑ Show incidents

Figure 47 Entuity Status Summary

## Checking the Reachability of Devices Within a View

1) Click **Dashboards > Status Summary**.

   For each view *Device Status* indicates the percentage of the devices within the view that respond to ping.

2) Click *Device Status* of the view you want to investigate further.

   Entuity launches the Device Status report to show the current state of devices within the view.

# Monitor Network Performance Using Port Metrics

The TopN Summary dashboard delivers a view based overview of port performance. It is useful for an immediate appraisal of the status of your network. The summary values are derived from the last three twenty minute poll roll-ups of each metric, with the exception of port utilization data which is derived from five minute polls. The dashboard is also updated every five minutes.

For the TopN Summary dashboard you can set the server, view and number of objects for each metric on which it should report.

| Attribute | Description |
|---|---|
| *Server* | Entuity server against which the dashboard is run. In multi-server environments where the server runs in:<br>■ Consolidated mode Entuity identifies the managing server of the port in the mouse over.<br>■ Unconsolidated mode you can select the server against which to run the dashboard. |
| *View* | Entuity view against which the dashboard is run. The default view is the user's My Network view. Views are selectable from the drop-down list, Entuity only displays those views the user is allowed to access. |
| *TopN* | The number of ports included to each section of the dashboard. By default this is set to five. This value also sets how many ports are displayed in the hyperlinked measurement specific dashboards. |

Table 23 TopN Summary Dashboard Configuration

Each metric is detailed in a section of the report, listing the top N ports on that measure.

For each metric, the dashboard includes a specific column for:

- *Device*, device identifier. This is also a hyperlink to the Device Summary page.
- *Port*, port number. This is also a hyperlink to the Port Summary page.
- A bar chart representation of the measure. This is also a hyperlink to a historical graph on the measure.

| Metric | Description |
|---|---|
| *Inbound Fault* | The port's inbound faults expressed as a percentage of total inbound traffic over the previous hour. |
| *Outbound Fault* | The port's outbound faults expressed as a percentage of total outbound traffic over the previous hour. |
| *Faults* | The fault metric summaries are also hyperlinks through to the Faults graph which by default displays the selected fault, inbound or outbound, for each five minute polled value, expressed as a percentage of total inbound or outbound traffic, respectively. The graph report time period is configurable, and you can also show/hide all fault metrics, i.e. Outbound Fault%, Outbound Discards%, Inbound Fault% and Inbound Discards%. |
| *Top Listeners* | The port's inbound traffic in bits per second measured over the previous hour. |
| *Top Talkers* | The port's inbound traffic in bits per second measured over the last complete hour. |
| Two traffic volume measures: The traffic volume summaries are also hyperlinks through to the Traffic Volume graph which by default displays both inbound and outbound traffic for each five minute polled value, expressed as a percentage of total inbound and outbound traffic, respectively. The graph report time period is configurable, and you can also show/hide all traffic metrics. | |
| *Inbound Utilization* | the port's inbound utilization measured over the last complete hour. |

Table 24 TopN Summary Dashboard

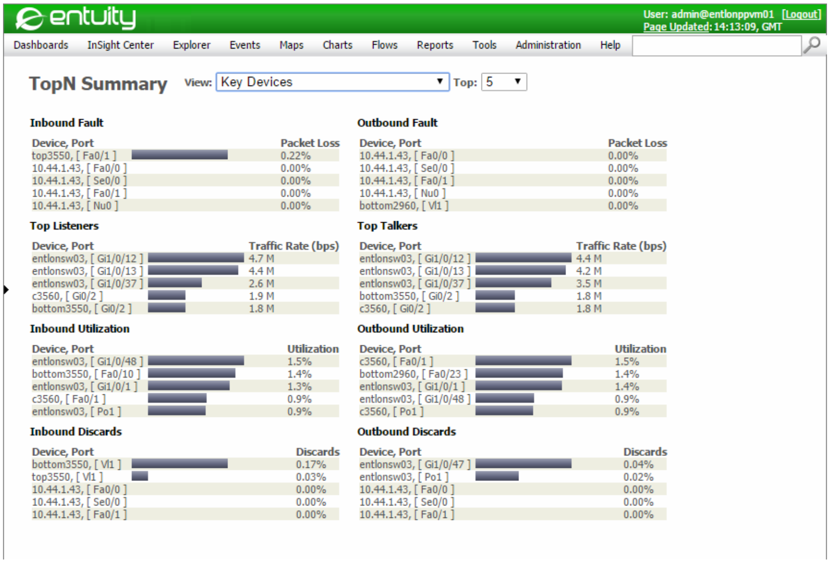
<table>
<tr><th>Metric</th><th>Description</th></tr>
<tr><td><i>Outbound Utilization</i></td><td>the port’s inbound utilization measured over the last complete hour.</td></tr>
<tr><td colspan="2">Two utilization measures: The utilization summaries are also hyperlinks through to the Utilization graph which by default displays both inbound and outbound utilization for each five minute polled value, expressed as a percentage of total inbound and outbound traffic, respectively. The graph report time period is configurable, and you can also show/hide all utilization metrics.</td></tr>
<tr><td><i>Inbound Discards</i></td><td>The number of inbound discards expressed as a percentage of total traffic volume received by the port during the last polling period.</td></tr>
<tr><td><i>Outbound Discards</i></td><td>The number of outbound discards expressed as a percentage of total traffic volume transmitted by the port during the last polling period.</td></tr>
</table>

Table 24 TopN Summary Dashboard

## Opening the TopN Summary Dashboard

To access the TopN Summary dashboard:

1) Click **Dashboards >TopN Summary**.



TopN Summary View: Key Devices Top: 5

Inbound Fault

| Device, Port | Packet Loss |
|---|---|
| top3550, [ Fa0/1 ] | 0.22% |
| 10.44.1.43, [ Fa0/0 ] | 0.00% |
| 10.44.1.43, [ Se0/0 ] | 0.00% |
| 10.44.1.43, [ Fa0/1 ] | 0.00% |
| 10.44.1.43, [ Nu0 ] | 0.00% |

Outbound Fault

| Device, Port | Packet Loss |
|---|---|
| 10.44.1.43, [ Fa0/0 ] | 0.00% |
| 10.44.1.43, [ Se0/0 ] | 0.00% |
| 10.44.1.43, [ Fa0/1 ] | 0.00% |
| 10.44.1.43, [ Nu0 ] | 0.00% |
| bottom2960, [ Vl1 ] | 0.00% |

Top Listeners

| Device, Port | Traffic Rate (bps) |
|---|---|
| entlonsw03, [ Gi1/0/12 ] | 4.7 M |
| entlonsw03, [ Gi1/0/13 ] | 4.4 M |
| entlonsw03, [ Gi1/0/37 ] | 2.6 M |
| c3560, [ Gi0/2 ] | 1.9 M |
| bottom3550, [ Gi0/2 ] | 1.8 M |

Top Talkers

| Device, Port | Traffic Rate (bps) |
|---|---|
| entlonsw03, [ Gi1/0/12 ] | 4.4 M |
| entlonsw03, [ Gi1/0/13 ] | 4.2 M |
| entlonsw03, [ Gi1/0/37 ] | 3.5 M |
| bottom3550, [ Gi0/2 ] | 1.8 M |
| c3560, [ Gi0/2 ] | 1.8 M |

Inbound Utilization

| Device, Port | Utilization |
|---|---|
| entlonsw03, [ Gi1/0/48 ] | 1.5% |
| bottom3550, [ Fa0/10 ] | 1.4% |
| entlonsw03, [ Gi1/0/1 ] | 1.3% |
| c3560, [ Fa0/1 ] | 0.9% |
| entlonsw03, [ Po1 ] | 0.9% |

Outbound Utilization

| Device, Port | Utilization |
|---|---|
| c3560, [ Fa0/1 ] | 1.5% |
| bottom2960, [ Fa0/23 ] | 1.4% |
| entlonsw03, [ Gi1/0/1 ] | 1.4% |
| entlonsw03, [ Gi1/0/48 ] | 0.9% |
| c3560, [ Po1 ] | 0.9% |

Inbound Discards

| Device, Port | Discards |
|---|---|
| bottom3550, [ Vl1 ] | 0.17% |
| top3550, [ Vl1 ] | 0.03% |
| 10.44.1.43, [ Fa0/0 ] | 0.00% |
| 10.44.1.43, [ Se0/0 ] | 0.00% |
| 10.44.1.43, [ Fa0/1 ] | 0.00% |

Outbound Discards

| Device, Port | Discards |
|---|---|
| entlonsw03, [ Gi1/0/47 ] | 0.04% |
| entlonsw03, [ Po1 ] | 0.02% |
| 10.44.1.43, [ Fa0/0 ] | 0.00% |
| 10.44.1.43, [ Se0/0 ] | 0.00% |
| 10.44.1.43, [ Fa0/1 ] | 0.00% |

Figure 48 Entuity TopN Summary Dashboard

## Investigating Port Utilization Using the TopN Summary

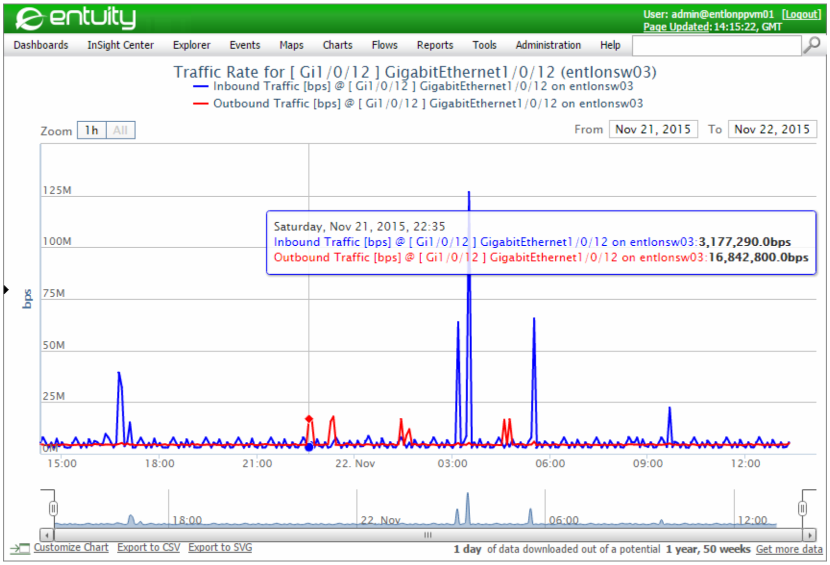
Using Entuity views you can group together key devices and ports in your network or service, and use the TopN Summary dashboard to monitor their performance. By default the dashboard displays the top 5 ports scoring highest on each metric for the past hour.

To monitor port utilization through the TopN Summary dashboard:

1) Click **Dashboards >TopN Summary**.

2) From the Inbound Utilization or Outbound Utilization section, for the port in which you are interested, select:

- Device name, to view the device information in the Device Summary page.
- Port name, to view the port information in the Port Summary page.
- Bar chart or utilization value to view the graphed history of both inbound and outbound utilization for the port.


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 14:15:22, GMT
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Tools
Administration
Help
Traffic Rate for [ Gi1/0/12 ] GigabitEthernet1/0/12 (entlonsw03)
Inbound Traffic [bps] @ [ Gi1/0/12 ] GigabitEthernet1/0/12 on entlonsw03
Outbound Traffic [bps] @ [ Gi1/0/12 ] GigabitEthernet1/0/12 on entlonsw03
Zoom
1h
All
From
Nov 21, 2015
To
Nov 22, 2015
bps
125M
100M
75M
50M
25M
0M
15:00
18:00
21:00
22. Nov
03:00
06:00
09:00
12:00
18:00
22. Nov
06:00
12:00
Customize Chart
Export to CSV
Export to SVG
1 day of data downloaded out of a potential 1 year, 50 weeks
Get more data

Saturday, Nov 21, 2015, 22:35
Inbound Traffic [bps] @ [ Gi1/0/12 ] GigabitEthernet1/0/12 on entlonsw03:**3,177,290.0bps**
Outbound Traffic [bps] @ [ Gi1/0/12 ] GigabitEthernet1/0/12 on entlonsw03:**16,842,800.0bps**

Figure 49 Graphing Utilization Data

# Monitor Operational Trends Using Device Metrics

The Device Metrics dashboard allows you to:

- View graphs for each user selected metric showing a series for each device.
- Click on a graph to display an interactive graph of that metric, which by default shows twenty-four hours of data.
- Select a reporting period, expressed as a time period back from the current time.
- Configure the selected metrics, devices and default time period.

The dashboard displays the metrics for a maximum of ten devices. This maximum is configurable through `entuity.cfg`.

The selected devices are shown with a separate graph for each metric for each device. You can set auto scaling of the Y-axis on a per metric basis. By default the dashboard auto updates at five minute intervals, which you can turn off through the Preferences settings.

| Attribute | Description |
|---|---|
| *CPU* | CPU utilization as a five minute average. |
| *Latency* | ICMP latency value. |
| *Reachability* | Derived from ICMP Ping latency data. |
| *Used Memory* | Total memory used on the device as a percentage of the total physical memory installed to it. |
| *IP Packet Discards%* | Number of received packets the device discards, as a percentage of total number of packets received by the device. |
| *IP Packet Forward%* | Number of received packets the device forwards, as a percentage of total number of packets received by the device. |
| *ICMP Redirects%* | Number of incorrectly addressed packets as a percentage of total number of packets handled by the device. |
| *ICMP TTL Exceeded%* | Number of received packets where the TTL was decremented to zero, as a percentage of total number of packets received by the device. |
| *Buffer Allocation Failure Rate* | Rate of buffer allocation failures over the reporting period. |
| *Buffer Memory Failure Rate* | Rate of buffer No Memory failures raised over the poll period. |
| *Sys Bus Util* | System bus utilization for the period. |

Table 25 Device Metrics Dashboard

## Opening the Device Metrics Dashboard

To access the Device Metrics dashboard:

1) Click **Dashboards** > **Device Metrics**.

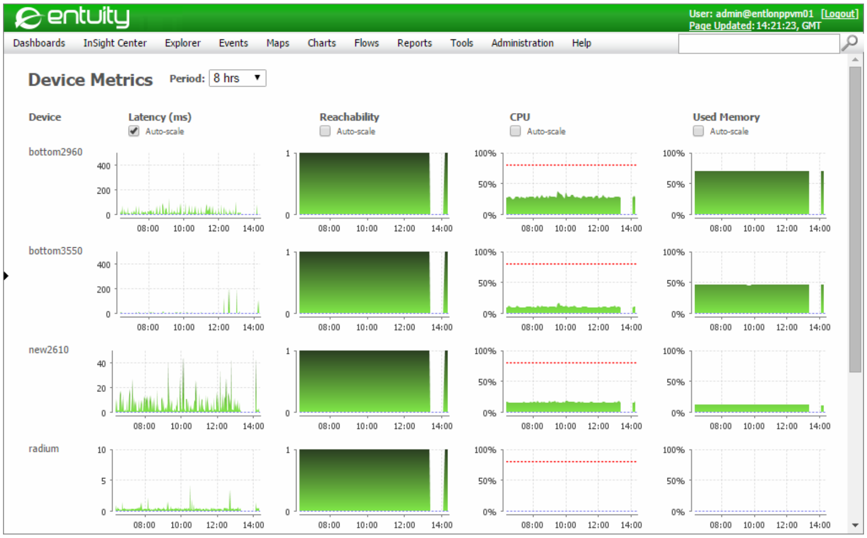


Figure 50 Device Metrics Summary

2) Click on the device metric graph you want to view over a twenty-four hour period.

Entuity displays the Device Metric Detail interactive chart.

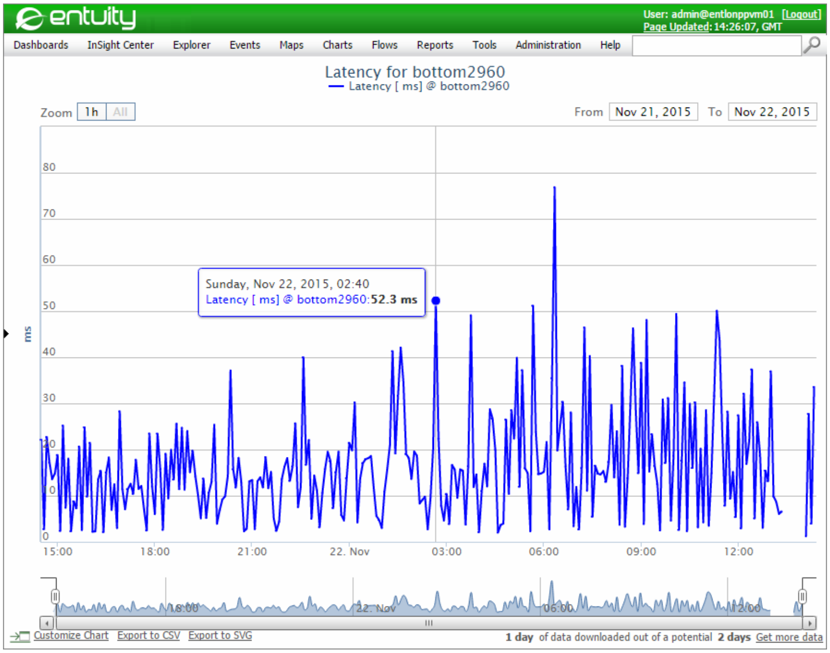

entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 14:26:07, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Latency for bottom2960
Latency [ ms] @ bottom2960
Zoom 1h All
From Nov 21, 2015 To Nov 22, 2015
Sunday, Nov 22, 2015, 02:40
Latency [ ms] @ bottom2960: 52.3 ms
ms
80
70
60
50
40
30
20
10
0
15:00
18:00
21:00
22. Nov
03:00
06:00
09:00
12:00
Customize Chart Export to CSV Export to SVG
1 day of data downloaded out of a potential 2 days Get more data

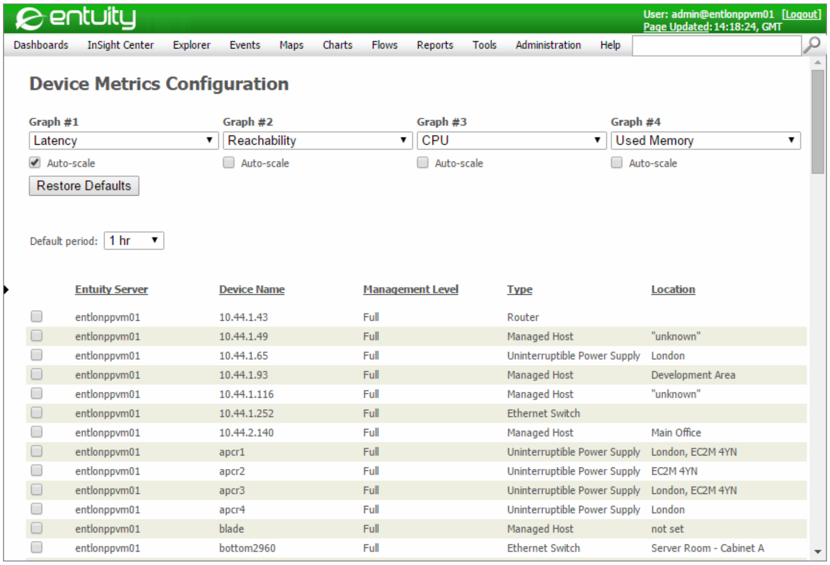
Figure 51 Device Metrics Detail Graph

## Configuring Device Metrics Dashboard

The Device Metrics dashboard is designed to display an immediate graphical summary of the current performance of your key devices. Each Entuity user with the requisite permissions can configure this dashboard to display those devices in which they are currently interested. By default you can select ten devices for display, with Entuity updating their metrics every five minutes.

To select the device and their metrics to display on the Device Metrics dashboard:

1) Click **Dashboards > Device Metrics**.
2) Select `Configure`. Entuity displays the Device Metrics Configure page, which lists all of the devices Entuity manages that the user is permitted to view.
3) Select the metrics you want to monitor for each device.
4) Check the check box of each device that you want to monitor, and click **Submit**. Entuity displays an updated Device Metrics page.



Device Metrics Configuration

Graph #1: Latency ☑ Auto-scale

Graph #2: Reachability □ Auto-scale

Graph #3: CPU □ Auto-scale

Graph #4: Used Memory □ Auto-scale

Default period: 1 hr

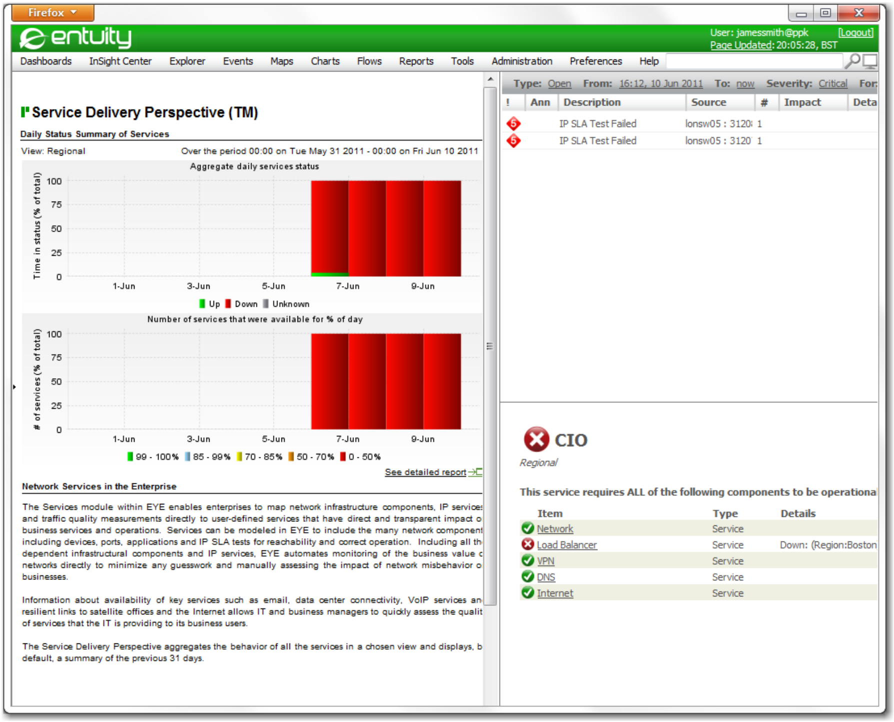
| | Entuity Server | Device Name | Management Level | Type | Location |
|---|---|---|---|---|---|
| □ | entlonppvm01 | 10.44.1.43 | Full | Router | |
| □ | entlonppvm01 | 10.44.1.49 | Full | Managed Host | "unknown" |
| □ | entlonppvm01 | 10.44.1.65 | Full | Uninterruptible Power Supply | London |
| □ | entlonppvm01 | 10.44.1.93 | Full | Managed Host | Development Area |
| □ | entlonppvm01 | 10.44.1.116 | Full | Managed Host | "unknown" |
| □ | entlonppvm01 | 10.44.1.252 | Full | Ethernet Switch | |
| □ | entlonppvm01 | 10.44.2.140 | Full | Managed Host | Main Office |
| □ | entlonppvm01 | apcr1 | Full | Uninterruptible Power Supply | London, EC2M 4YN |
| □ | entlonppvm01 | apcr2 | Full | Uninterruptible Power Supply | EC2M 4YN |
| □ | entlonppvm01 | apcr3 | Full | Uninterruptible Power Supply | London, EC2M 4YN |
| □ | entlonppvm01 | apcr4 | Full | Uninterruptible Power Supply | London |
| □ | entlonppvm01 | blade | Full | Managed Host | not set |
| □ | entlonppvm01 | bottom2960 | Full | Ethernet Switch | Server Room - Cabinet A |

Figure 52 Configuring Device Metrics

# 5 Build Custom Dashboards

With Custom Dashboards you can use the URLs that present data through the Entuity web UI, and re-use them in combinations that meet your requirements. The Dashboard Editor allows you to create dashboards that include more than one viewpoint of network data, for example filtered events, a report, flow data, key charts, that are appropriate to a specific task, e.g. monitoring delivery of key services.

Custom Dashboards allow each user to run a maximum of five Entuity dashboards, although by using the export and import tools you can have ready access to a library of dashboards. Custom dashboards are associated with the user profile, and a user with the appropriate permissions can create dashboards and assign them to other users. A user can also select a dashboard as their home page, the page Entuity displays after a user logins.



**Service Delivery Perspective (TM)**

**Daily Status Summary of Services**

View: Regional    Over the period 00:00 on Tue May 31 2011 - 00:00 on Fri Jun 10 2011

**Network Services in the Enterprise**

The Services module within EYE enables enterprises to map network infrastructure components, IP service and traffic quality measurements directly to user-defined services that have direct and transparent impact o business services and operations. Services can be modeled in EYE to include the many network componen including devices, ports, applications and IP SLA tests for reachability and correct operation. Including all th dependent infrastructural components and IP services, EYE automates monitoring of the business value c networks directly to minimize any guesswork and manually assessing the impact of network misbehavior o businesses.

Information about availability of key services such as email, data center connectivity, VoIP services an resilient links to satellite offices and the Internet allows IT and business managers to quickly assess the qualit of services that the IT is providing to its business users.

The Service Delivery Perspective aggregates the behavior of all the services in a chosen view and displays, b default, a summary of the previous 31 days.

Type: Open From: 16:12, 10 Jun 2011 To: now Severity: Critical For:

| ! | Ann | Description | Source | # | Impact | Deta |
|---|---|---|---|---|---|---|
| 5 | | IP SLA Test Failed | lonsw05 : 3120 | 1 | | |
| 5 | | IP SLA Test Failed | lonsw05 : 3120 | 1 | | |

☒ **CIO**

*Regional*

**This service requires ALL of the following components to be operationa**

| | Item | Type | Details |
|---|---|---|---|
| ✓ | Network | Service | |
| ☒ | Load Balancer | Service | Down: (Region:Boston |
| ✓ | VPN | Service | |
| ✓ | DNS | Service | |
| ✓ | Internet | Service | |

Figure 53 Custom Dashboard for Monitoring Service Delivery

## Components of Custom Dashboards

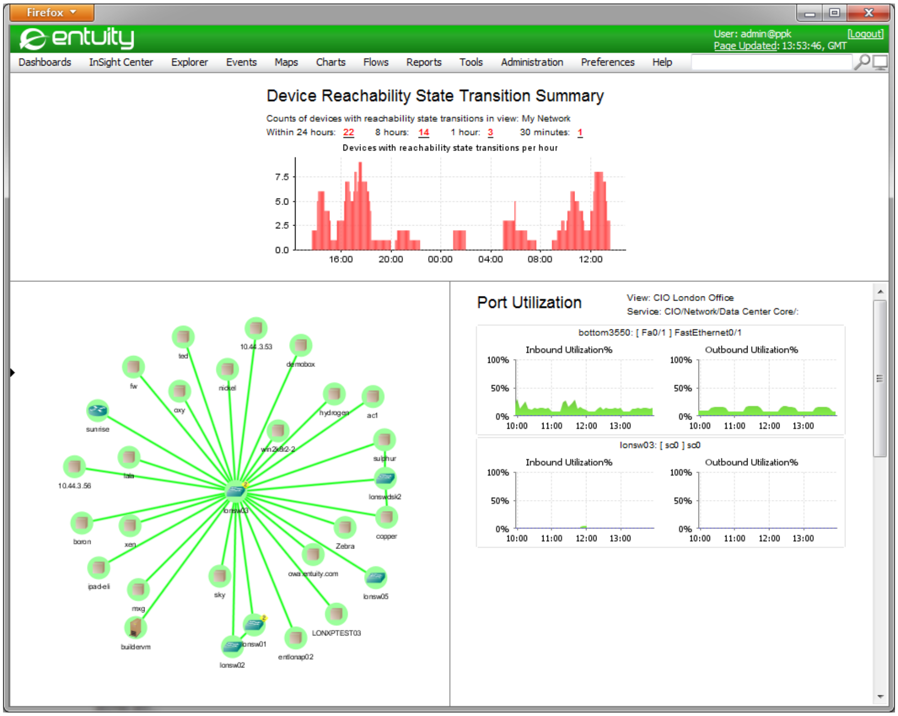
You can build custom dashboards using:

- One of seventeen layout templates. These layouts have between one and nine panes.

- Maps and charts, including Integrated Flow Analyzer charts. (See *Adding Maps to Custom Dashboards*.)
- Reports with layout configure options that you can use to better fit a dashboard panel. Entuity also includes a set of panel reports tailored for custom dashboards.
- Events and incidents.
- Other dashboards, e.g. Service Delivery Perspective.
- Auto update to automatically refresh content.

## Dashboard Panel Reports

Entuity includes a suite of dashboard optimized mini-reports that help users build richer dashboards more easily and quickly than would otherwise be possible.



Device Reachability State Transition Summary

Counts of devices with reachability state transitions in view: My Network

Within 24 hours: 22 8 hours: 14 1 hour: 3 30 minutes: 1

Devices with reachability state transitions per hour

Port Utilization

View: CIO London Office

Service: CIO/Network/Data Center Core/:

bottom3550: [ Fa0/1 ] FastEthernet0/1

Inbound Utilization% Outbound Utilization%

lonsw03: [ sc0 ] sc0

Inbound Utilization% Outbound Utilization%

Figure 54 Dashboard with a Map and Two Panel Reports

These panel reports are available from **Reports > Dashboard Panels** (see the *Reports Reference Manual*):

- Device Reachability Transitions Summary and its associated details report.
- Device Reboot Summary and its associated details report.
- Event Severity Summary and its associated details report.
- Module Change Summary and its associated details report.

- Port Operational State Transition Summary and its associated details report.
- Port Utilization Charts.
- Port Utilization Gauges.

### Dashboards and Entuity URLs

The content of a pane within a dashboard is determined by its associated URL. When you drag and drop content into a custom dashboard pane, it is the URL that the Custom Dashboard Editor displays. It is the URL that Entuity interprets to display content.

The Entuity web UI uses frames to display different types of information within the same page, each frame within the page has its own URL. There are a number of techniques for accessing these URLs:

- Use a browser’s Properties dialog to identify the source of the frame.
- Open a frame content in its own browser window and copy from its navigation bar the URL.

For interactive charts use **Open this chart,** which opens the chart in a new page with its URL available from the browser address bar.

The content of each pane of a custom dashboard is derived from a fully qualified URL, i.e. http://*entuity_server*, https://*entuity_server*. When you edit a custom dashboard you can see, and amend these URLs although they should remain fully qualified.

You should also ensure the homepage URL uses the same protocol, HTTP or HTTPS, as the Entuity server. By default browsers block mixed content to prevent unencrypted content being included in pages with encrypted content. You can change this default behavior, for example in FireFox click on the small shield in the URL bar that indicates mixed content is blocked.

For further details on URLs see *Appendix C - Entuity URLs*.

### Dashboard Performance

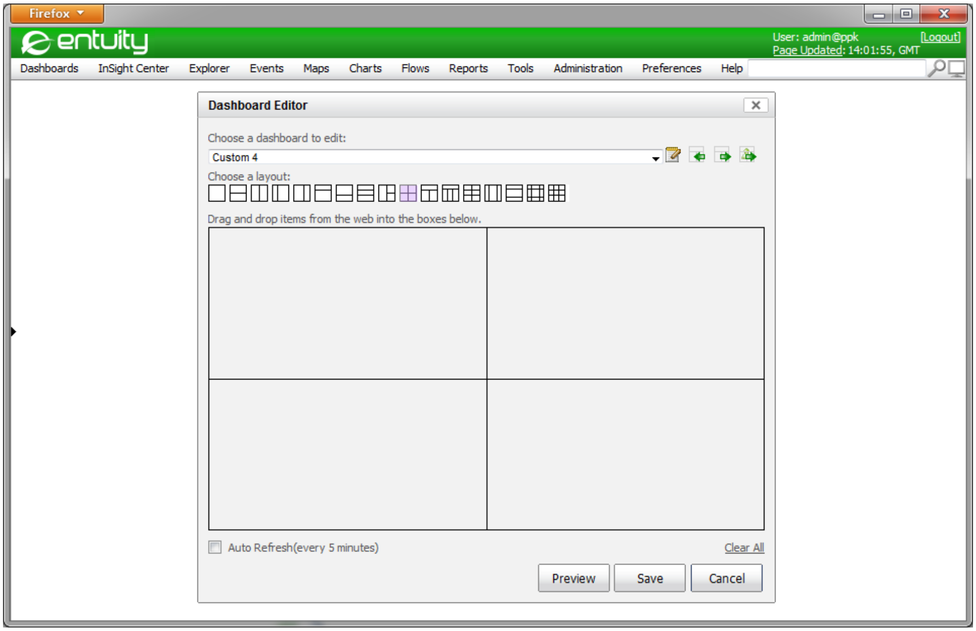
When building dashboards you should always consider the components within the panel and the resources they require. For example, if you build a dashboard with nine panels each of which contains a dashboard panel report then you are placing a high load on the caches (memory) used for those reports. For details on amending cache settings see *Appendix C - Entuity URLs*.

## Custom Dashboard Editor

Management of Custom Dashboards is through the Custom Dashboard Editor. You can create, amend, delete, import and export dashboards.

1) Click **Dashboards** > **Custom Dashboards** > **Edit**.

Entuity displays the Custom Dashboard Editor, which displays the first dashboard. For a new dashboard you are prompted to assign content, for an existing dashboard Entuity displays its current definition.



Choose a dashboard to edit: Custom 4

Choose a layout:

□ Auto Refresh(every 5 minutes)

Figure 55 Custom Dashboard Editor

## Custom Dashboard Editor Options

| Name | Description |
|---|---|
| Choose a dashboard to edit | Select the dashboard to edit. |
| Edit Name | Select to open Edit Name dialog through which you can set the dashboard name which is displayed in the Custom Dashboards menu and the Preferences page. |
| Import | Opens a File Upload dialog, allowing you to upload a saved dashboard. |
| Export | Opens a dialog which saves the dashboard as an XML file. You can edit the file with an XML editor or download it to your machine. |
| Export to users | Opens a dialog from which you can select one or more users to which to assign the dashboard. |
| Choose a layout | These templates offer a selection of layouts, with between two and nine panes, different relative pane positions and size. |
| Drag and drop panes | The pane layout changes to reflect the selected template. You can drag and drop content into the pane. |

Table 26 Custom Dashboard Editor Options

| Name | Description |
|---|---|
| Auto Refresh | Select to update the content of each pane every five minutes. When not selected, the default state, only those panes containing content with its own update mechanism refresh, e.g. Event Viewer. |
| Clear All | Select to clear the content from the panes. This change is only stored when you click **Save**. |
| Preview | Select to preview the current dashboard setup, including unsaved changes, in the main Entuity window. |
| Save | Select to save the current dashboard. |
| Cancel | Select to cancel the unsaved changes to the current dashboard. |

Table 26 Custom Dashboard Editor Options

# Creating Custom Dashboards

By default each user can run up to 5 custom dashboards at one time, this is the number available from the Custom Dashboards menu. You can make more available as it is a configurable option through *Dashboard Count* in Preferences. By default the upper limit to the number of dashboards is 20 although system administrators can amend this default through `entuity.cfg`.

To create a dashboard:

1) Click **Dashboards** > **Custom Dashboards** > **Edit**.

   Entuity displays the Dashboard Editor. The editor displays details of the first dashboard, which would be empty for a new dashboard or contains a definition for an existing dashboard.

2) Click the Edit Name icon 📝 to display the dialog through which you can specify the dashboard name.

3) Select the icon representing the required layout of your dashboard.

4) Populate the panes with the network data and presentation that you require.

   You can drag URLs into a pane. For example while the Dashboard Editor is open you can display a perspective and then drag it into a pane. You can also click on a pane and add or edit text.

   When you drag a link into a pane, any previous definition for the pane is overwritten.

5) Click **Preview** for Entuity to display the current dashboard setup.

6) Click **Save** to save the dashboard and close the editor, or **Cancel** to delete the unsaved changes to the dashboard and close the editor.

## Example Dashboard

This example dashboard includes:

- One dashboard panel report, the Port Utilization chart report ran against a sub-service. For example, this URL

  ```
  http://ppk/webUI/jasperReport.do?reportGenerationId=1353664238984&report=%2Freports%2FDashboard%2FServicePortUtilizationCharts&format=html&eyeServer=5a1b6381-0a72-495a-a1e1-62f371bf4653&view=CIO%20London%20Office&service=CIO&subservice=CIO%2FNetwork%2FData%20Center%20Core%2F%3ADegraded%2FRegion%3ASkipton%20Office&timeFrame=prev%3A1440i&secondaryTimeFrame=&primeTime=&autoRun=1
  ```

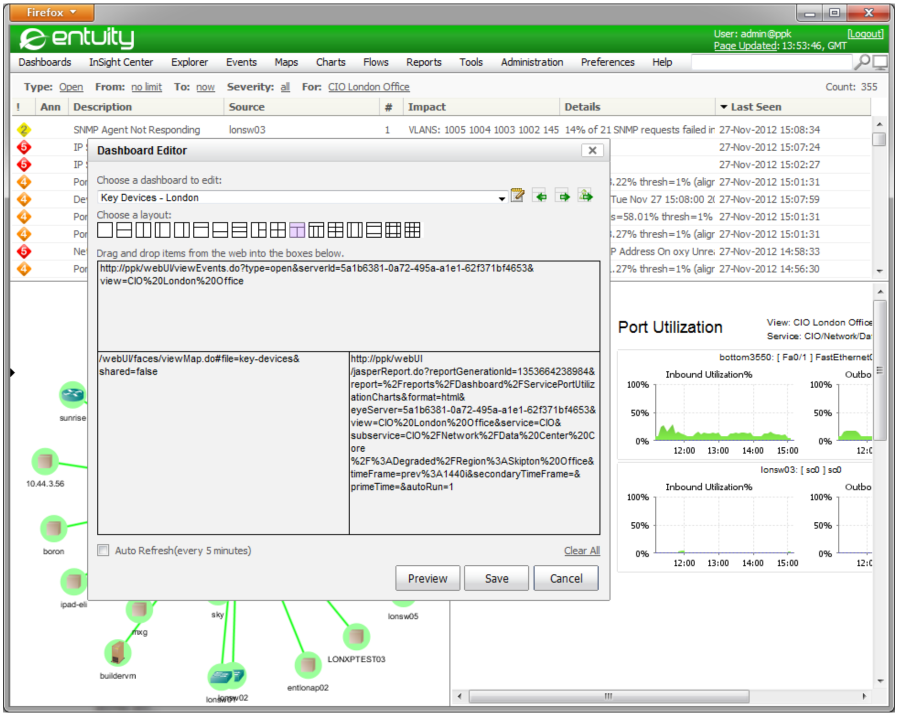
- A map. You include a map to a view by exporting the required map and then referencing the map file within the report panels URL. For example, this URL references an exported map called key-devices:

  ```
  /webUI/faces/viewMap.do#file=key-devices&shared=false
  ```

- A filtered event view. For example, this URL presents the current events for the CIO London Office view:

  ```
  http://ppk/webUI/viewEvents.do?type=open&serverId=5a1b6381-0a72-495a-a1e1-62f371bf4653&view=CIO%20London%20Office
  ```

To view methods on how to recover the URLs used within the Entuity web UI see *Appendix C - Entuity URLs*.



Type: Open From: no limit To: now Severity: all For: CIO London Office Count: 355

| ! | Ann | Description | Source | # | Impact | Details | Last Seen |
|---|---|---|---|---|---|---|---|
| 2 | | SNMP Agent Not Responding | lonsw03 | 1 | VLANS: 1005 1004 1003 1002 145 | 14% of 21 SNMP requests failed ir | 27-Nov-2012 15:08:34 |
| 5 | | IP | | | | | 27-Nov-2012 15:07:24 |
| 5 | | IP | | | | | 27-Nov-2012 15:02:27 |
| 4 | | Por | | | | .22% thresh=1% (aligr | 27-Nov-2012 15:01:31 |
| 4 | | De | | | | Tue Nov 27 15:08:00 2( | 27-Nov-2012 15:07:59 |
| 4 | | Por | | | | s=58.01% thresh=1% | 27-Nov-2012 15:01:31 |
| 4 | | Por | | | | .27% thresh=1% (aligr | 27-Nov-2012 15:01:31 |
| 5 | | Ne | | | | P Address On oxy Unre: | 27-Nov-2012 14:58:33 |
| 4 | | Por | | | | .27% thresh=1% (aligr | 27-Nov-2012 14:56:30 |

Dashboard Editor

Choose a dashboard to edit: Key Devices - London

Choose a layout:

Drag and drop items from the web into the boxes below.

```
http://ppk/webUI/viewEvents.do?type=open&serverId=5a1b6381-0a72-495a-a1e1-62f371bf4653&
view=CIO%20London%20Office
```

```
/webUI/faces/viewMap.do#file=key-devices&
shared=false
```

```
http://ppk/webUI
/jasperReport.do?reportGenerationId=1353664238984&
report=%2Freports%2FDashboard%2FServicePortUtiliz
ationCharts&format=html&
eyeServer=5a1b6381-0a72-495a-a1e1-62f371bf4653&
view=CIO%20London%20Office&service=CIO&
subservice=CIO%2FNetwork%2FData%20Center%20C
ore
%2F%3ADegraded%2FRegion%3ASkipton%20Office&
timeFrame=prev%3A1440i&secondaryTimeFrame=&
primeTime=&autoRun=1
```

☐ Auto Refresh(every 5 minutes) Clear All

Preview Save Cancel

Figure 56 Preview of Example Dashboard

To speed the development of custom dashboards you can use the Entuity web UI and have the Dashboard Editor continually displayed. To create the example dashboard:

1) Click **Dashboards** > **Custom Dashboards** > **Edit**.

2) Click the Edit Name icon to display the dialog through which you can specify the dashboard name.

3) Select the three panel grid icon representing the required layout of your dashboard.

4) Populate the top pane with the event URL.

   Click **Events** and specify the event filter and retrieve the frame's URL. For example with the Firefox browser hold down the **Shift** key and click **This Frame** > **Frame Info**.

   Paste the URL into the top pane of the dashboard.

5) Populate the left pane with the map URL referencing a saved map.

   Click **Maps** and the **Open** icon . Drag the filename of the map onto the required custom dashboard pane.

6) Populate the right pane with dashboard panel report URL.

   Click **Reports** > **Dashboard Panel Reports**. Define and run a report, use the HTML output format.

   Retrieve the report's URL. For example, position the mouse pointer over the report, with the Firefox browser hold down the **Shift** key and click **This Frame** > **Frame Info**.

7) Click **Preview** for Entuity to display the current dashboard setup.

8) Click **Save** to save the dashboard and close the editor, or **Cancel** to delete the unsaved changes to the dashboard and close the editor.

## Amending Custom Dashboards

To amend a dashboard:

1) Click **Dashboards** > **Custom Dashboards** > **Edit**.

2) Select and then amend the dashboard.

   You can change all of the components of a Custom Dashboard. When you change the layout the panes in the editor automatically adjust according to the new design. When changing to fewer panes, content of the lost panes is only deleted when you save the dashboard changes.

   You can drag and drop content between panes, as well as using cut and paste options available from the context menu.

3) Click **Preview** for Entuity to display the current dashboard setup.

4) Click **Save** to save the dashboard and close the editor, or **Cancel** to delete the unsaved changes to the dashboard and close the editor.

## Removing Custom Dashboards

Each user can have up to five custom dashboards. To create a dashboard:

1) Click **Dashboards** > **Custom Dashboards** > **Edit**.

2) Select and then amend the dashboard.

   You can change all of the components of a Custom Dashboard. When you change the layout the panes in the editor automatically adjust according to the new design. When changing to fewer panes, content of the lost panes is only deleted when you save the dashboard changes.

   You can drag and drop content between panes, as well as using cut and paste options available from the context menu.

## Assigning Custom Dashboards to Users

Entuity includes support for the assignment of custom dashboards created by an administrator to one or more other users. You can distribute dashboards through the import and export of their XML definition files (see *Exporting and Importing Custom Dashboards*), or through assignment in the web UI.

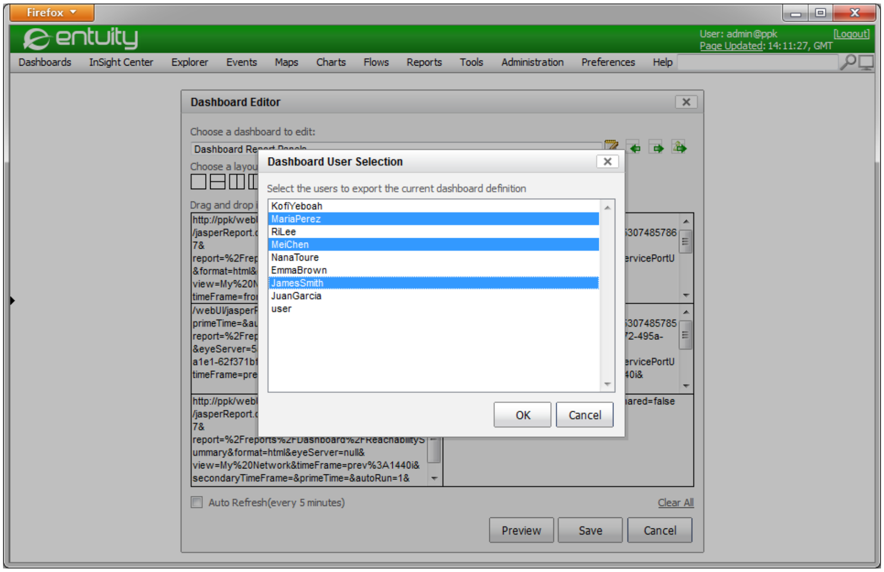
When assigning a dashboard Entuity places the dashboard in the same position in the user's list of dashboards as it is in the creator's list. For example, if the dashboard you create is the first in the drop down list of dashboards Entuity attempts to export it to the first slot in the selected users. If the slot already includes a dashboard Entuity prompts you to confirm that you want to overwrite it.

To assign a dashboard:

1) Click **Dashboards** > **Custom Dashboards** > **Edit**.

2) From *Choose a dashboard file to edit* select the dashboard you want to assign to users.

3) Click the Assign to Users icon . Entuity opens a dialog which lists the available users.



Dashboard User Selection

Select the users to export the current dashboard definition

- KofiYeboah
- MariaPerez
- RiLee
- MeiChen
- NanaToure
- EmmaBrown
- JamesSmith
- JuanGarcia
- user

Figure 57 Assign Dashboards to Users

4) Select one or more the users and click **OK**.

If a user already has a configured dashboard for that position in their drop down list of custom dashboards Entuity prompts you to confirm that you want to overwrite it.

## Exporting and Importing Custom Dashboards

Entuity allows you to export Custom Dashboard definitions to, and import them from, XML files, These XML definition files are useful when:

- Distributing dashboards between users, the XML file can be emailed to other users for their import. Alternatively you can assign dashboards to users through the web UI. (See *Assigning Custom Dashboards to Users*.)
- Developing a dashboard based on an existing one. You can export a dashboard definition and then import it to another dashboard and from their make your amendments.
- Developing dashboards and wanting to maintain a revision history of your dashboard development.
- You have a library of dashboards, import allows you to load to Entuity the currently required dashboards.
- Resetting a dashboard. If you have exported a blank dashboard definition, you can import it over an existing dashboard to reset it.

To export a dashboard:

1) Click **Dashboards** > **Custom Dashboards** > **Edit**.

2) From *Choose a dashboard file to edit* select the dashboard you want to export to an XML file.

3) Click the Export icon. Entuity opens a dialog which saves the dashboard as an XML file.

   You can edit the file with an XML editor or download it to your machine.

To import a dashboard:

1) Click **Dashboards** > **Custom Dashboards** > **Edit**.

2) From *Choose a dashboard file to edit* select the dashboard to which you want to import the saved definition. Importing a dashboard overwrites the current definition for that dashboard.

3) Select the Import icon. Entuity opens a dialog through which you browse for and then upload a dashboard saved as an XML file.

# 6 Manage Green IT Policies

Entuity's Green IT Perspective™ is a center for managing the discipline of policies that reduce the energy consumption of your network. The Green IT Perspective:

- Assists both network and general managers to reduce wasted power consumption associated with leaving desktop/notebook PCs running 24/7 where they could be safely turned off outside the working day.
- Quantifies the power savings both enterprise-wide and per department. The savings already being achieved by current equipment shutdown behavior is quantified along with the potential additional savings if all appropriate nightly shutdowns were to be performed across the board.
- Identifies trends in shutdown policy conformance by department.
- identifies those who should be targeted when looking to achieve better policy conformance and thereby higher savings.
- Quantifies the power used by the managed infrastructure devices.
- Identifies switches with high or low number/proportions of spare ports.
- Quantifies the power used by the switches per used port to evaluate power efficiency.
- Identifies servers that are lightly used and might become the target of consolidation initiatives to reduce data center power utilization.

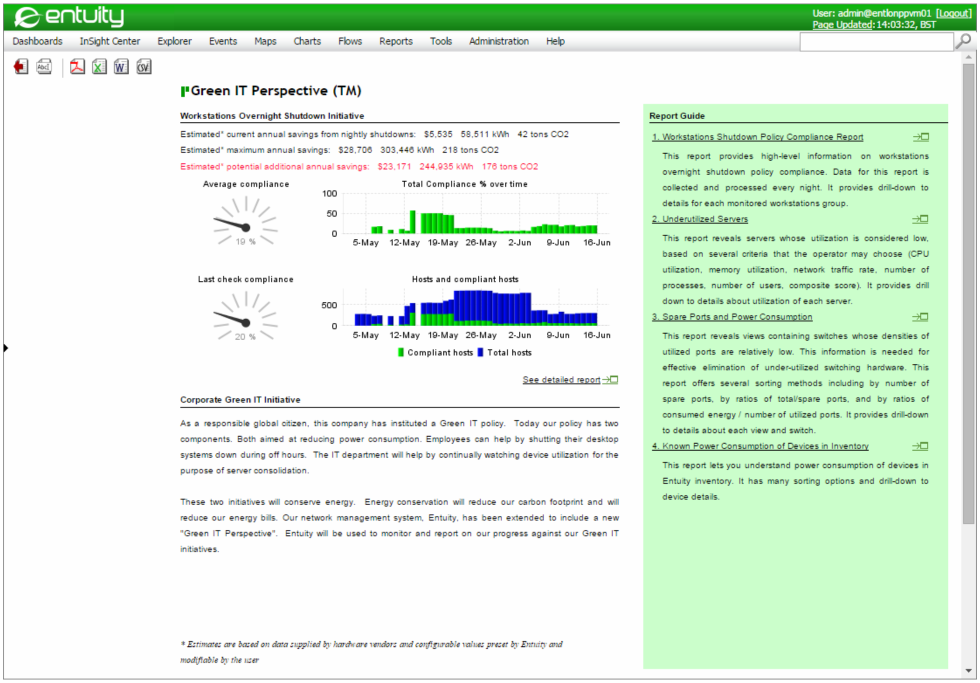
Entuity generates the information for the Green IT Perspective and its reports from data gathered against all of the objects it manages on the server, i.e. against the objects in the All Objects view. It is also through Green IT sub-folders of the All Objects view that you can configure the green IT cost parameters.

✓ Where the IP address ranges of different policy groups overlap, the policy groups can include the same workstations. If you then use these policy groups in the same compliance reports then the workstations that are in both policy groups are double-counted, skewing the reported savings.

## Accessing the Green IT Perspective

To access the Green IT Perspective dashboard:

1) Click **InSight Center > Green IT Perspective**.



Green IT Perspective (TM)

Workstations Overnight Shutdown Initiative

Estimated* current annual savings from nightly shutdowns: $5,535 58,511 kWh 42 tons CO2

Estimated* maximum annual savings: $28,706 303,446 kWh 218 tons CO2

Estimated* potential additional annual savings: $23,171 244,935 kWh 176 tons CO2

Corporate Green IT Initiative

As a responsible global citizen, this company has instituted a Green IT policy. Today our policy has two components. Both aimed at reducing power consumption. Employees can help by shutting their desktop systems down during off hours. The IT department will help by continually watching device utilization for the purpose of server consolidation.

These two initiatives will conserve energy. Energy conservation will reduce our carbon footprint and will reduce our energy bills. Our network management system, Entuity, has been extended to include a new "Green IT Perspective". Entuity will be used to monitor and report on our progress against our Green IT initiatives.

** Estimates are based on data supplied by hardware vendors and configurable values preset by Entuity and modifiable by the user*

Report Guide

1. Workstations Shutdown Policy Compliance Report

   This report provides high-level information on workstations overnight shutdown policy compliance. Data for this report is collected and processed every night. It provides drill-down to details for each monitored workstations group.

2. Underutilized Servers

   This report reveals servers whose utilization is considered low, based on several criteria that the operator may choose (CPU utilization, memory utilization, network traffic rate, number of processes, number of users, composite score). It provides drill down to details about utilization of each server.

3. Spare Ports and Power Consumption

   This report reveals views containing switches whose densities of utilized ports are relatively low. This information is needed for effective elimination of under-utilized switching hardware. This report offers several sorting methods including by number of spare ports, by ratios of total/spare ports, and by ratios of consumed energy / number of utilized ports. It provides drill-down to details about each view and switch.

4. Known Power Consumption of Devices in Inventory

   This report lets you understand power consumption of devices in Entuity inventory. It has many sorting options and drill-down to device details.

Figure 58 Entuity Green IT Perspective Dashboard

## Green IT Perspective

This perspective provides an overview of workstation overnight shutdown compliance, with access to a detailed compliance report and other Green IT Perspective reports.

| Attribute | Description |
|---|---|
| *Estimated Current annual savings from nightly shutdown* | Indicator of the benefits to your organization of the workstation overnight shutdown initiative. |
| *Estimated Maximum annual savings* | Potential savings in currency, kilowatts and CO2 if one hundred percent compliance was achieved. |
| *Estimated Potential additional annual savings* | Difference between current annual savings and maximum annual savings. The nominal power values used to derive the estimated savings values are configurable through `site_specific_nominal_power.cfg`, whilst the costing elements are configurable through the perspective's report options. |
| *Average Compliance* | Gauge provides the average compliance over the monitoring period, as a percentage of the maximum potential compliance. |
| Total Compliance % over time | Graphs compliance as a percentage of maximum potential compliance over the reporting period. |

Table 27 Green IT Perspective Dashboard

| Attribute | Description |
|---|---|
| *Last check compliance* | Gauge provides a measure of workstation shutdown compliance over the last poll (by default the previous day), as a percentage of the maximum potential compliance. |
| *Total Number of hosts and Number of compliant hosts* | Graphs total number of hosts and the number of hosts that are compliant over the reporting period. |
| *Corporate Green IT Initiative* | Text that the administrator can enter, for example to explain the corporate green policy. |
| Report Guide | Section provides access to a subset of Green IT reports:<br>■ Green IT Perspective Detail report<br>■ Workstations Shutdown Policy Compliance report<br>■ Underutilized Servers report<br>■ Spare Ports and Power Consumption report<br>■ Known Power Consumption of Devices in Inventory report.<br>All Green IT reports are available from the Reports Server repository. |

Table 27 Green IT Perspective Dashboard

## Configure Green IT Perspective

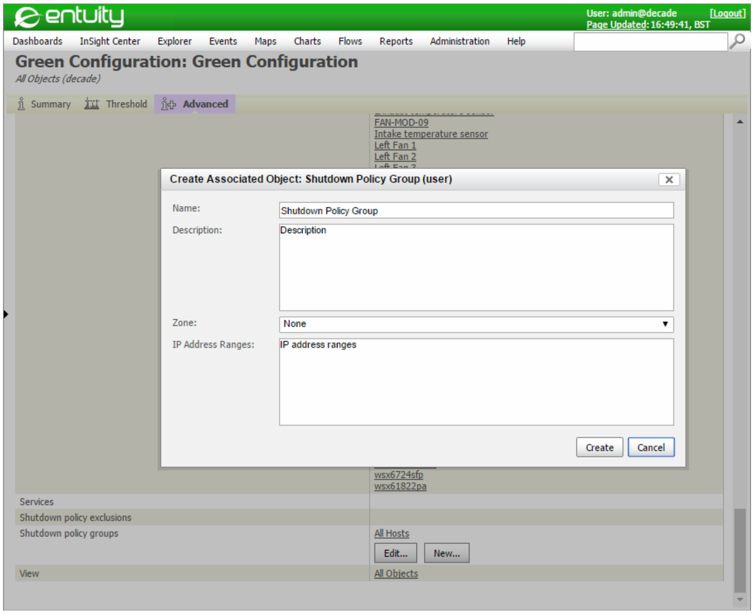
Entuity recommend you configure policy groups and their exclusions through `shutdown_policies.cfg`, where you have full add, amend and delete control. (See the *Entuity System Administrator Reference Manual*.)

These are the configurable Green IT Perspective components:

- Shutdown Policy Groups
- Shutdown Policy Exclusions
- Nominal Module Power Consumption
- Nominal Device Power Consumption
- Costing elements.

To configure Green IT set up:

1) From Explorer navigate to All Objects view Advanced tab.
2) From the Association section click the Green Configuration hyperlink.
3) Click the Advanced tab and then Show Hidden Data.
4) From the Shutdown policy groups section click New. (See *Figure 59 - Create Shutdown Policy Group*.)



Green Configuration: Green Configuration

*All Objects (decade)*

Create Associated Object: Shutdown Policy Group (user)

Name: Shutdown Policy Group

Description: Description

Zone: None

IP Address Ranges: IP address ranges

Services

Shutdown policy exclusions

Shutdown policy groups: All Hosts

View: All Objects

Figure 59 Create Shutdown Policy Group

5) Click the Advanced tab and then Show Hidden Data.

| Attribute | Description |
|---|---|
| *Name* | Name of the group displayed in reports, e.g. All Hosts, London Office. |
| *Description* | Meaningful description of the purpose of the group. |
| *Zone* | Entuity zone the policy applies to. |
| *IP Address Range* | One or more IP address ranges. Workstations with IP addresses within these ranges are included to the policy group, unless they are also included in a shutdown policy exclusion group |

Table 6-1 Associated Shutdown

## Configuring Shutdown Policy Groups

Shutdown Policy Groups allow you to group workstations that share characteristics important in developing a shutdown compliance policy, e.g. same time zone, same location.

Where the IP address ranges of different policy groups overlap, the policy groups can include the same workstations. If you then use these policy groups in the same compliance reports then the workstations that are in both policy groups are double-counted, skewing the reported savings.

Entuity recommend you configure policy groups and their exclusions through `shutdown_policies.cfg`, where you have full add, amend and delete control. (See the *Entuity System Administrator Reference Manual*.) Each shutdown policy group has its own section within this file:

```
[ShutdownPolicyGroup All Hosts]
IPAddressRange=0.0.0.0-255.255.255.255
Description=All Hosts
[ShutdownPolicyGroup London Office]
IPAddressRange=10.44.1.1-10.44.1.50, 10.44.1.60-10.44.1.90,
= 1.2.3.4-1.2.3.5, 10.44.1.98-10.44.1.123, 10.44.1.140-10.44.1.247
Description=Workstations in London Office
```

## Configuring Shutdown Policy Exclusions

Shutdown Policy Exclusion Groups allow you to identify workstations that should not be included to an exclusion policy, e.g. key servers that must be up twenty-four hours a day. Incorrect or incomplete configuration of policy exclusion groups can seriously undermine the efficacy of the compliance metrics.

For each Shutdown Policy Exclusion Group define:

- *Name*, name of the group displayed in reports, e.g. Security Cameras.
- *Description*, meaningful description of the purpose of the group, e.g. IP CCTV.
- *Minimum Address* and *Maximum Address*, are IP addresses that together define an IP range, and devices within that range are excluded from the compliance policy.

Entuity recommend you configure policy group exclusions through `shutdown_policies.cfg`, where you have full add, amend and delete control. (See the *Entuity System Administrator Reference Manual*.) Each shutdown policy exclusion has its own section within this file, for example:

```
[ShutdownPolicyExclusion London Security Cameras]
IPAddressRange=10.44.1.10-10.44.1.12
Description=IP CCTV
```

## Power and Nominal Module Power Consumption Settings

For Entuity to estimate the costs and savings of your power consumption policy, devices and modules must have within Entuity a known energy cost. Entuity supply default power consumption values for many device and module types, however you may need to add and amend power settings.

You can identify missing power settings through the Nominal Module Power Consumption and Nominal Device Power Consumption reports. You can add new settings through the `site_specific_nominal_power.cfg`.

Entuity supply two nominal power configuration files:

- `nominal_power.cfg`, contains default power consumption values for many device and module types. You cannot amend this file.
- `site_specific_nominal_power.cfg`, is included to the configuration through `nominal_power.cfg`. You can amend definitions held in `nominal_power.cfg` by redefining them here, you can also create new definitions for previously undefined devices and modules.

For details on configuring nominal power definitions see the *Entuity System Administrator Reference Manual*.

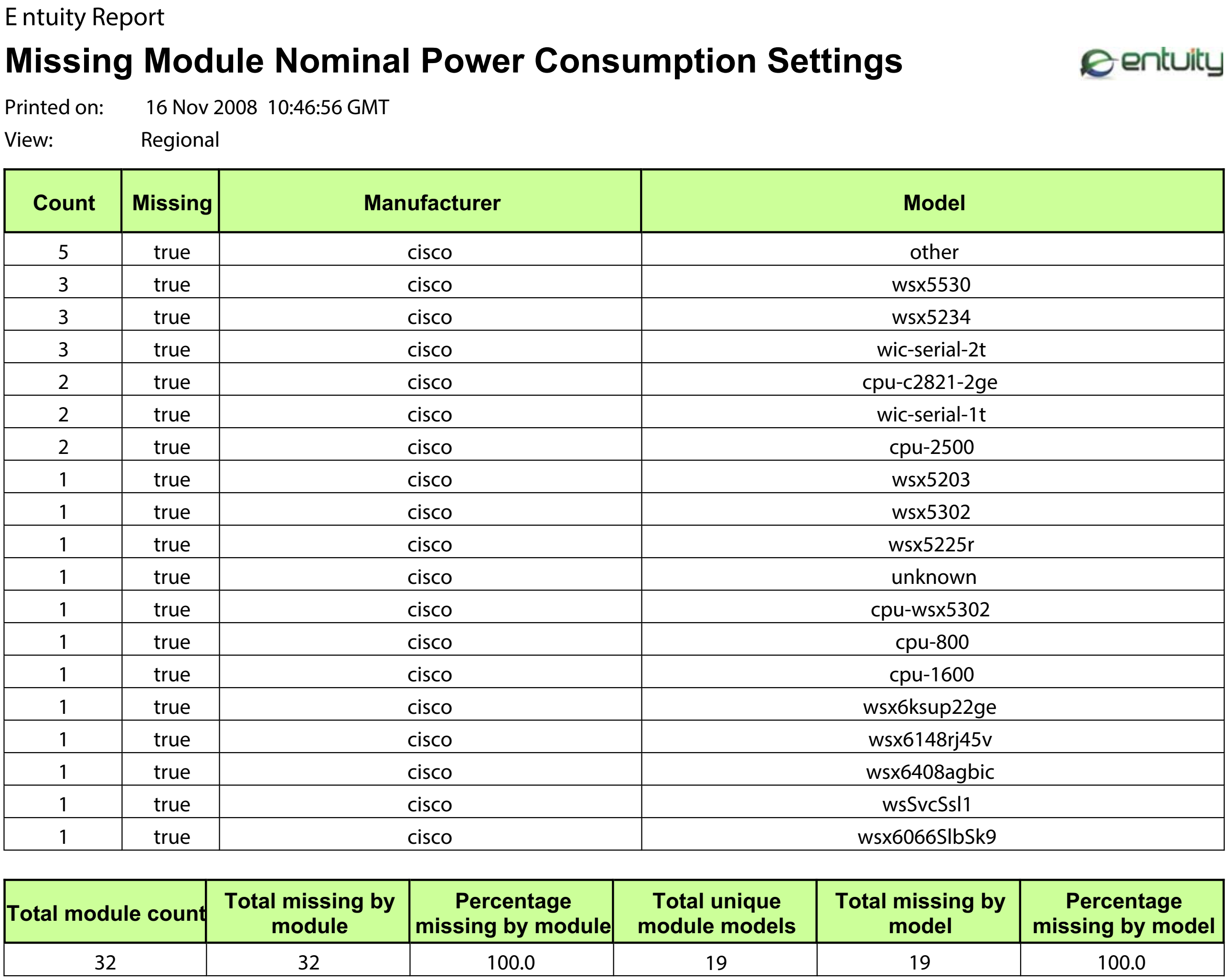
### Identifying Missing Power Consumption Settings

For each supported device and module there must be configured a power consumption estimate. These values are used when calculating annual, maximum and potential saving estimates.

Entuity includes Missing Module Power and Missing Device Module reports, which allow you to identify those module and device types for which a power consumption definition is missing.

To run the Missing Module Power report:

1) Click **Reports** > **Green Reports**.
2) Click **Missing Module Power**. Entuity generates the report. You should complete the missing nominal device power consumption values.



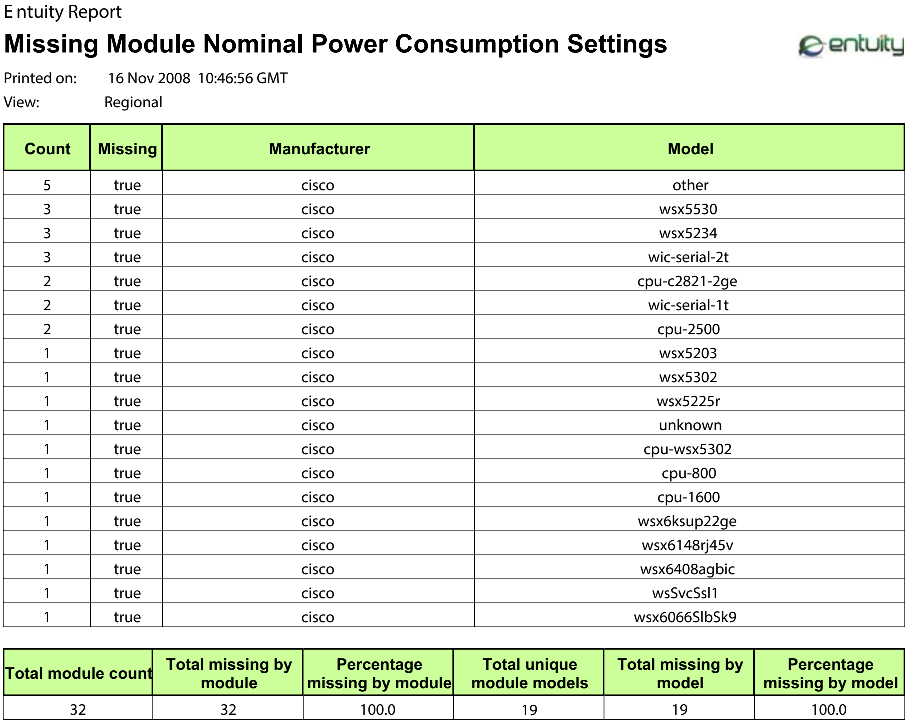
E ntuity Report

## Missing Module Nominal Power Consumption Settings

Printed on: 16 Nov 2008 10:46:56 GMT
View: Regional

| Count | Missing | Manufacturer | Model |
|---|---|---|---|
| 5 | true | cisco | other |
| 3 | true | cisco | wsx5530 |
| 3 | true | cisco | wsx5234 |
| 3 | true | cisco | wic-serial-2t |
| 2 | true | cisco | cpu-c2821-2ge |
| 2 | true | cisco | wic-serial-1t |
| 2 | true | cisco | cpu-2500 |
| 1 | true | cisco | wsx5203 |
| 1 | true | cisco | wsx5302 |
| 1 | true | cisco | wsx5225r |
| 1 | true | cisco | unknown |
| 1 | true | cisco | cpu-wsx5302 |
| 1 | true | cisco | cpu-800 |
| 1 | true | cisco | cpu-1600 |
| 1 | true | cisco | wsx6ksup22ge |
| 1 | true | cisco | wsx6148rj45v |
| 1 | true | cisco | wsx6408agbic |
| 1 | true | cisco | wsSvcSsl1 |
| 1 | true | cisco | wsx6066SlbSk9 |

| Total module count | Total missing by module | Percentage missing by module | Total unique module models | Total missing by model | Percentage missing by model |
|---|---|---|---|---|---|
| 32 | 32 | 100.0 | 19 | 19 | 100.0 |



Entuity Report

**Missing Module Nominal Power Consumption Settings**

Printed on: 16 Nov 2008 10:46:56 GMT
View: Regional

| Count | Missing | Manufacturer | Model |
|---|---|---|---|
| 5 | true | cisco | other |
| 3 | true | cisco | wsx5530 |
| 3 | true | cisco | wsx5234 |
| 3 | true | cisco | wic-serial-2t |
| 2 | true | cisco | cpu-c2821-2ge |
| 2 | true | cisco | wic-serial-1t |
| 2 | true | cisco | cpu-2500 |
| 1 | true | cisco | wsx5203 |
| 1 | true | cisco | wsx5302 |
| 1 | true | cisco | wsx5225r |
| 1 | true | cisco | unknown |
| 1 | true | cisco | cpu-wsx5302 |
| 1 | true | cisco | cpu-800 |
| 1 | true | cisco | cpu-1600 |
| 1 | true | cisco | wsx6ksup22ge |
| 1 | true | cisco | wsx6148rj45v |
| 1 | true | cisco | wsx6408agbic |
| 1 | true | cisco | wsSvcSsl1 |
| 1 | true | cisco | wsx6066SlbSk9 |

| Total module count | Total missing by module | Percentage missing by module | Total unique module models | Total missing by model | Percentage missing by model |
|---|---|---|---|---|---|
| 32 | 32 | 100.0 | 19 | 19 | 100.0 |

Figure 60 Missing Module Power Report

## Configuring Green IT Costing Elements

The values Entuity derives, for example estimated annual savings, require the setting of both power consumption and economic values. You can set these costing elements through the Green IT Perspective report options.

Entuity does not maintain a history of these settings. If you amend these settings today, and run a report that covers last week's performance it uses the current settings.

| Name | Description |
|---|---|
| *Daily excess kWh for a host* | Allows the average wasted power per host per day for hosts that are not shut off when they should be to be set. For a host that should be used for an 8 hour working day there should be 16 hours where it can be shut off. If the average consumption of hosts is 100W (a bit higher than most laptops but lower than desktops) then there would be 1600Wh (1.6kWh) of power associated with those 16 hours. |
| *Cost per kWh of Electricity,* | Cost per kilo watt hour of electricity. |
| *Currency symbol* | Identifies the currency used to display values, by default $. |

Table 7 Green IT Perspective Options

| Name | Description |
|---|---|
| *Tons of CO2 per kWh* | Tons of CO2 generated per kilo watt hour, by default 0.000718. |

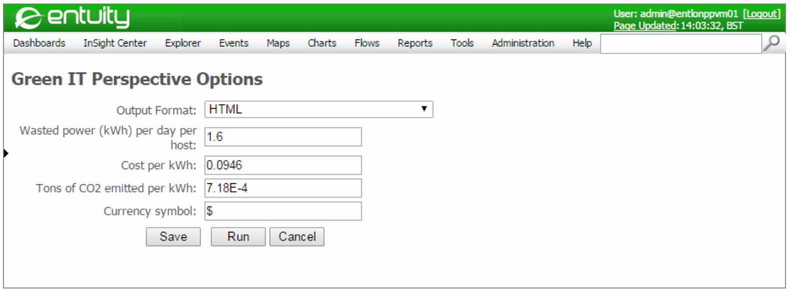
Table 7 Green IT Perspective Options

To set the Green IT Perspective costing elements:

1) Click **InSight Center >Green IT Perspective**.

2) Click the Report Options icon.

3) Configure Report Options and select **OK**.



Green IT Perspective Options

Output Format: HTML

Wasted power (kWh) per day per host: 1.6

Cost per kWh: 0.0946

Tons of CO2 emitted per kWh: 7.18E-4

Currency symbol: $

Figure 61 Green IT Perspective Report Options

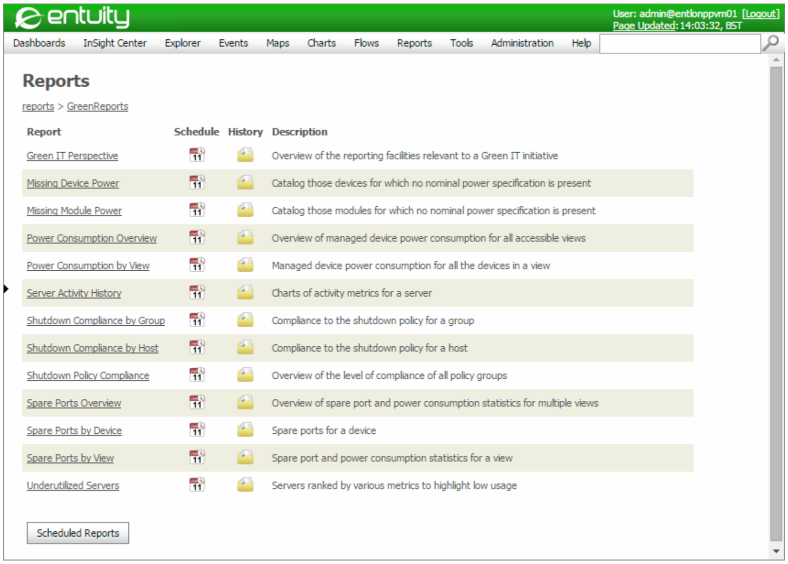
## Running Green IT Perspective Reports

The Entuity Green IT Perspective includes a set of compliance, consumption, historical and administrative reports.

The calculations underlying some of these reports are processed overnight. To avoid viewing reports with empty charts and null values, after installing the perspective you should wait twenty-four hours before running its reports.

To access the Green IT reports:

1) Click **Reports** > **Green Reports**.



Reports

reports > GreenReports

| Report | Schedule | History | Description |
|---|---|---|---|
| Green IT Perspective | 📅 | 📁 | Overview of the reporting facilities relevant to a Green IT initiative |
| Missing Device Power | 📅 | 📁 | Catalog those devices for which no nominal power specification is present |
| Missing Module Power | 📅 | 📁 | Catalog those modules for which no nominal power specification is present |
| Power Consumption Overview | 📅 | 📁 | Overview of managed device power consumption for all accessible views |
| Power Consumption by View | 📅 | 📁 | Managed device power consumption for all the devices in a view |
| Server Activity History | 📅 | 📁 | Charts of activity metrics for a server |
| Shutdown Compliance by Group | 📅 | 📁 | Compliance to the shutdown policy for a group |
| Shutdown Compliance by Host | 📅 | 📁 | Compliance to the shutdown policy for a host |
| Shutdown Policy Compliance | 📅 | 📁 | Overview of the level of compliance of all policy groups |
| Spare Ports Overview | 📅 | 📁 | Overview of spare port and power consumption statistics for multiple views |
| Spare Ports by Device | 📅 | 📁 | Spare ports for a device |
| Spare Ports by View | 📅 | 📁 | Spare port and power consumption statistics for a view |
| Underutilized Servers | 📅 | 📁 | Servers ranked by various metrics to highlight low usage |

Scheduled Reports

Figure 62 Green IT Perspective Report Repository

## Green IT Perspective Reports

Details on Green IT reports are available through the *Entuity Reports Reference Manual*.

| Report Title | Description |
|---|---|
| Shutdown Compliance Overview | This report provides an overview of shutdown compliance. |
| Shutdown Compliance by Group | This report provides an overview of shutdown compliance for the selected compliance group. |
| Shutdown Compliance by Host | This report provides an overview of shutdown compliance for the selected host. |
| Spare Ports and Power Consumption Overview | This report provides an overview of shutdown compliance, grouped by view, for the managed switches and routers. |
| Spare Ports and Power Consumption by View | This report provides an overview of spare ports and power consumption for devices within the selected view. |
| Spare Ports by Device | This report provides a breakdown of spare ports for the selected device within the selected view. |
| Underutilized Servers | Optimal utilization of servers is an important part of a successful green policy, the more servers operating at an optimal level the fewer servers that are required. |
| Server Activity History | This report provides a detailed breakdown of server performance during the reporting period. It is a useful tool when investigating server utilization. |

Table 8 Green IT Reports

| Report Title | Description |
|---|---|
| Green IT Perspective | Perspective dashboard, also available from **InSight Center > Green IT**. |
| Missing Device Power | This report identifies device types for which a power consumption definition is missing. |
| Missing Module Power | This report identifies module types for which a power consumption definition is missing. |
| Power Consumption by View | This report identifies power consumption by Entuity view, useful for example when you have views configured to meet your green IT policy. |
| Power Consumption Overview. | This report indicates device models and the state of their power consumption settings: |

Table 8 Green IT Reports

# 7 Chief Information Officer Perspective

Entuity's Chief Information Officer (CIO) Perspective provides online access to a summary dashboard showing recent business service impacts, delivering information suitable for the executive level of management. It is part of Entuity's InSight Center.

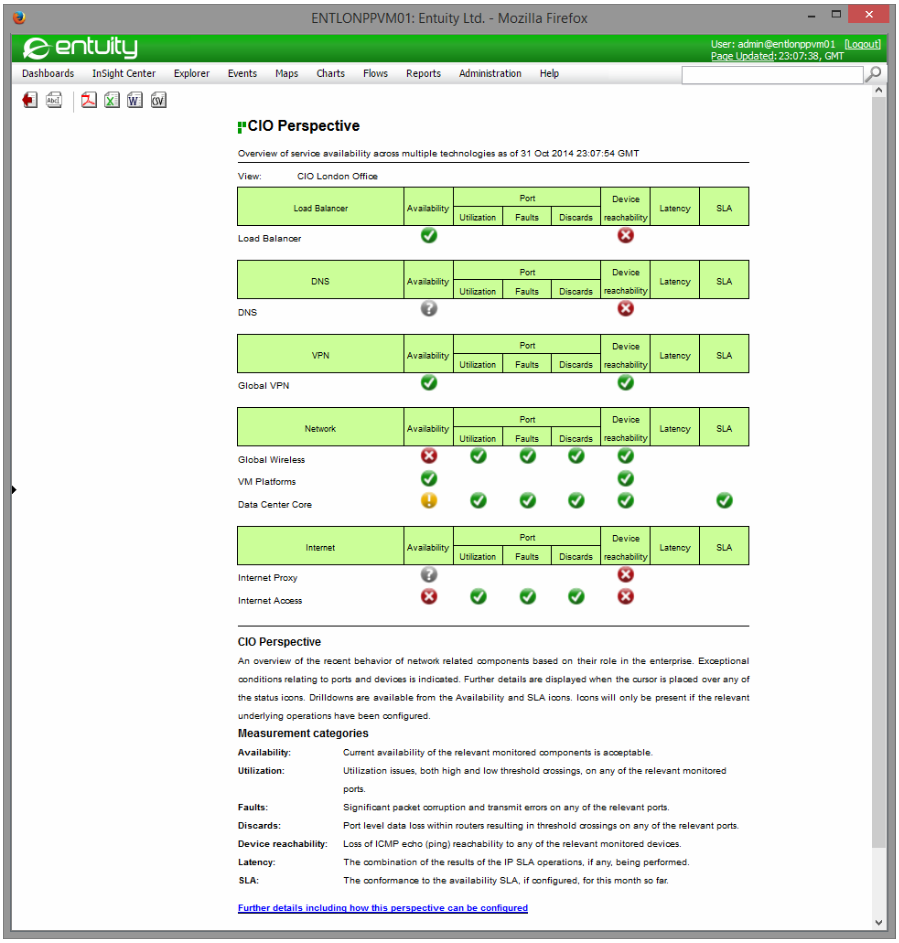
The CIO Perspective allows a high level overview of network health, identifying different categories of service. It allows an executive to rapidly determine whether there have been any recent issues that have impacted any of the business services that the company relies on. Where problems are identified it is easy to identify which parts of the company have been impacted and when that impact would have been felt. Importantly this perspective distinguishes between service impacting issues and those that can be safely accommodated through the redundant nature of the network.

The perspective has a multi-level drill down approach, whereby the top level presentation indicates whether there were any relevant issues and which business service they were related to. Each of the services and related metrics allow drilldowns that would present more details about the issues specific to the service and part of the network that were selected. This second level drilldown displays when the issues were experienced using a color ribbon presentation. A third level drilldown lists all the components being monitored for the specific service along with an indication of which one(s) was/were responsible for the issue(s).

The intended audience for this perspective is the executive level of management; managers who do not have hands-on day-to-day responsibility for the direct management of the network, its components or the other IT systems that it facilitates. Therefore the perspective's presentation includes clear descriptions of the components within services and there performance, but excludes the production of detailed line charts of changes in monitored metrics over time. The executive using the perspective can:

- Determine that there was/is an issue that is negatively impacting a relevant business service.
- Understand whether that impact is serious or is accommodated by a level of redundancy.
- See when the issues began and ended.
- See where the issues were observed in the enterprise.

Network management staff would be expected to be independently aware of problems and institute remedial actions. The executives using the facility would not be expected to be using it to marshal resources to address issues as they are observed but rather to use it to appreciate the magnitude and impact of service impacting problems to allow them to better communicate with their peers.


ENTLONPPVM01: Entuity Ltd. - Mozilla Firefox
entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 23:07:38, GMT
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Administration
Help

### CIO Perspective

Overview of service availability across multiple technologies as of 31 Oct 2014 23:07:54 GMT

View: CIO London Office

| Load Balancer | Availability | Port | | | Device reachability | Latency | SLA |
|---|---|---|---|---|---|---|---|
| | | Utilization | Faults | Discards | | | |
| Load Balancer | ✓ | | | | ✗ | | |

| DNS | Availability | Port | | | Device reachability | Latency | SLA |
|---|---|---|---|---|---|---|---|
| | | Utilization | Faults | Discards | | | |
| DNS | ? | | | | ✗ | | |

| VPN | Availability | Port | | | Device reachability | Latency | SLA |
|---|---|---|---|---|---|---|---|
| | | Utilization | Faults | Discards | | | |
| Global VPN | ✓ | | | | ✓ | | |

| Network | Availability | Port | | | Device reachability | Latency | SLA |
|---|---|---|---|---|---|---|---|
| | | Utilization | Faults | Discards | | | |
| Global Wireless | ✗ | ✓ | ✓ | ✓ | ✓ | | |
| VM Platforms | ✓ | | | | ✓ | | |
| Data Center Core | ! | ✓ | ✓ | ✓ | ✓ | | ✓ |

| Internet | Availability | Port | | | Device reachability | Latency | SLA |
|---|---|---|---|---|---|---|---|
| | | Utilization | Faults | Discards | | | |
| Internet Proxy | ? | | | | ✗ | | |
| Internet Access | ✗ | ✓ | ✓ | ✓ | ✗ | | |

**CIO Perspective**

An overview of the recent behavior of network related components based on their role in the enterprise. Exceptional conditions relating to ports and devices is indicated. Further details are displayed when the cursor is placed over any of the status icons. Drilldowns are available from the Availability and SLA icons. Icons will only be present if the relevant underlying operations have been configured.

**Measurement categories**

**Availability:** Current availability of the relevant monitored components is acceptable.

**Utilization:** Utilization issues, both high and low threshold crossings, on any of the relevant monitored ports.

**Faults:** Significant packet corruption and transmit errors on any of the relevant ports.

**Discards:** Port level data loss within routers resulting in threshold crossings on any of the relevant ports.

**Device reachability:** Loss of ICMP echo (ping) reachability to any of the relevant monitored devices.

**Latency:** The combination of the results of the IP SLA operations, if any, being performed.

**SLA:** The conformance to the availability SLA, if configured, for this month so far.

Further details including how this perspective can be configured

Figure 63 Entuity CIO Perspective Dashboard

# CIO Perspective Overview

The CIO Perspective is a report, which reports on a CIO service and its sub-services within a specified view. The perspective includes links within it that call other reports which report on those sub-services in greater detail. The CIO Perspective reports on a hierarchy of services, of which there may be four levels:

1) The parent (top level) service is always named CIO and identifies the hierarchy as one available to the CIO Perspective. Only system administrators can create this parent service.

2) The next level down of services identifies the main groupings on which you are reporting for example the type of technology. Non-system administrators can create this and subsequent levels of services.

3) At the third level sub-services may further specify the type of service delivered, and it is only at this level that you can add components to the service that are then included to the report.

4) Fourth level of the service hierarchy can identify different sites, for example offices.

The CIO Perspective suite includes a set of reports:

- CIO Perspective which provides an overview of the current health of the managed network for the selected view.
- Site Availability report which provides a breakdown of performance by site for the selected service. This report can only be called as a drilldown from a technology's availability status icon in the CIO Perspective.
- Component Availability report which provides a breakdown of performance by components for the selected service. This report can only be called as a drilldown from the Site Availability report.
- SLA Details report which is available from the Activity folder and also as a drilldown from the CIO Perspective report. By default this report displays SLA performance for the current month and predicts the SLA value for the full month, based on 100% availability for the remainder of the month.

For report and perspective details see the *Entuity Reports Reference Manual*.

## Running the CIO Perspective

To access the CIO Perspective dashboard:

1) Click **InSight Center** > **CIO Perspective**.

   As a report the CIO Perspective is also available through the Entuity reports center, click **Reports** > **CIO Perspective**, from where you can access the perspective and also a print friendly version of the same report.

2) From the Report Options you can:

   - Where you have more than 1 Entuity server run the perspective against All or a particular server.
   - Select the view against which to run the Perspective.

The perspective indicates the overall state of its monitored components through icons for each of the metrics. When you place the mouse pointer over an icon a pop-up displays details on its current status. For example, a rollover for an icon for:

- SLA indicates SLA Availability Goal, Month to date and Projected values.
- Technology Service summarizes its current state and offers a click through for a report.
- Latency performance of IP SLA operations.

For a number of the metrics you can click on a technology's icon and drilldown for more detail. When you click an:

- Availability icon, Entuity runs a Site Availability report, which provides a breakdown of performance by site for the selected service.

  For each component within this report there are hyperlinks to more details, displayed through the Component Availability report.
- SLA icon, Entuity runs a SLA Details report, which is available from the Activity folder and also as a drilldown from the CIO Perspective report. By default this report displays SLA performance for the current month and predicts the SLA value for the full month, based on 100% availability for the remainder of the month.

## Set Up Services for the CIO Perspective

The CIO Perspective is based on services configured in Entuity. You can build a hierarchy of services to reflect your network setup. The CIO Perspective comprises of a number of sections which are defined using Entuity services. Each of these sections can have a number of technologies, e.g. DNS, load balancer, Internet Access. Against each technology there are a set of available metrics that indicate its current state.

✓ Within each view you should only create one CIO service. The All Objects view and your My Network view inherit services from other views and potentially could have multiple CIO services. If a view has more than one CIO service you should not run the CIO Perspective against that view as you cannot determine which CIO service the perspective is using.

CIO Perspective services require a top level service that can only be configured by users with system administrator access rights. Non-system administrators assigned ownership of the service can then create sub-services within the CIO service, creating the hierarchy required by the perspective. A CIO service comprises of two parts, the:

- Service definition, which acts as an object to which you can associate components that make up that service. (See *Chapter 21 - Entuity Services*.)
- Components, e.g. device, ports, applications, other services, that make up the delivered service.

CIO Perspective uses these types of services:

- Standard service, for example the root service CIO is a standard service. The root service must always be called CIO and is created by a system administrator.
- Services that can report a degraded state of service in addition to reporting up and down.
- Site service, which identifies to Entuity the service as representing a region.

### Standard Services

The CIO Perspective is based on a hierarchy of services that you can build up to reflect your managed network. For CIO Perspective the root service is always called **CIO**, and therefore there can only be one CIO service in each view.

The level of service below CIO lists the main sections of the perspective used to breakdown the report. In the examples used in this section these are Network, Load Balancer, DNS, VPN and Internet.

Within these services are the technologies on which the perspective reports. In multi-server environments these technologies can be split across different Entuity servers; you can include remote sub-services, remote objects.

### Degraded State Services

You can define a state service to identify different levels of service, to identify services which are currently up but may not be operating optimally, or have lost redundancy, or be approaching a condition in which they will fail. This requires the setting of the service type to use the **At Least** operator state *Type* operator which allows you to set dual level thresholds (the second threshold represents the degraded state and is optional), for example:

- *At Least Value* level threshold would require the specified number of its components to be available for the service to be considered up.
- *Degraded* level would set the minimum number of components that could deliver a level of degraded but acceptable service delivery e.g. at least 3 components within the service are up.

These service states can be passed back to a parent service, whose name actually identifies the service delivered, e.g. Data Center Core.

You should consider setting state services *Raise Events* to false, often events raised from the parent state are more meaningful.

### Site Services

This service type identifies to Entuity that the service represents a grouping of components, logical or geographical. A site service is identified through its syntax:

```
site:ServiceName
```

where text:

- Before the colon indicates this is a site, in this case a region.
- After the colon is the service name.

In the CIO Perspective this allows a drill down to the Site Availability Report.

## CIO Perspective Metrics

The CIO Perspective includes seven measurement categories. Against each technology the perspective indicates the current state of each measurement through a status icon. When a metric is not appropriate the status icon is not displayed, e.g. where a technology does not include an IP SLA operation for measuring latency the SLA icon is not displayed. Each icon:

- Displays the current state of the technology, i.e. Down, Warning, Up.
- Includes a mouse roll-over that provides details on the metric.

- May include a hyperlink to drill down for further details, e.g. SLA Details report, Site Availability report.

Entuity does not prevent you from implementing unsupported configurations. For metrics to be valid:

- Each service within the CIO Perspective must include at least one managed object.
- When running in multi-server mode technologies of the same type must not be split across Entuity servers.
- Site services are only recognized when placed within state services.

| Metric | Description |
|---|---|
| Availability | Current availability state of the monitored component. There is a drilldown to the Site Availability report. |
| Utilization | Current port utilization state, both high and low threshold crossings, on any of the relevant monitored ports. |
| Faults | Significant packet corruption and transmit errors on any of the relevant ports. |
| Discards | Port level data loss within routers resulting in threshold crossings on any of the relevant ports. |
| Device Reachability | Loss of ICMP echo (ping) reachability to any of the relevant monitored devices. The device's of any ports included to the service are implicitly included. |
| Latency | The combination of the results of the IP SLA operations, if any, being performed. |
| SLA | A service level can be configured against the service. The icon indicates SLA performance for the current month. A mouse over shows the:<br>■ SLA Availability Goal, target SLA performance for the service.<br>■ Month to date, SLA performance for the current month.<br>■ Projected, SLA value if the service is 100% available for the remainder of the month.<br>The icon indicates the projected state of the service:<br>■ Good, indicates current and projected performance is above the set SLA value.<br>■ Warning, indicates the current service delivery is below the target, but the projected SLA value is above the target.<br>■ Failure, indicates the projected SLA value is below the target SLA value.<br>You can click on the icon to view the SLA Details report. |

Table 9 CIO Perspective Metrics

## How to Set Up a CIO Perspective

This example includes the main techniques available to you when constructing CIO Perspectives. These are the key points of the example CIO Perspective:

- A user defined view called CIO London Office.

- Components, e.g. devices, ports, IP SLA operations, placed directly into the CIO sub-services. Take this approach when you only want the component visible within the view when it is included to the service, include components directly to the view when you want them available to the view even if they are subsequently removed from the service.
- The importance of the hierarchy of services to the success of your CIO Perspective.

The CIO service can have these levels of services:

- Level 1, the root service which must be called CIO.
- Level 2, within the CIO service there are five sub services, Network, Load Balancer, VPN, DNS and Internet. These are the main headings within the CIO Perspective.

  This example concentrates on Network.
- Level 3, within the Network service there are three technologies again represented through Entuity services, i.e. Data Center Core, VM Platform, Global Wireless.

  Data Center Core uses the degraded state threshold applied to the states returned from its 3 sub-services. In this example the implication is that the data center functionality can continue with a degraded level of service if 2 out of the 3 regions are Up.

  Level 3 of the CIO service hierarchy is also the first level on which you could add components that Entuity would include to the CIO Perspective, for example adding devices to the VM Platforms service.
- Level 4 defines 3 site sub-services. These regional offices contain the components used to deliver a service to those offices, e.g. devices, applications, IP SLA operators.

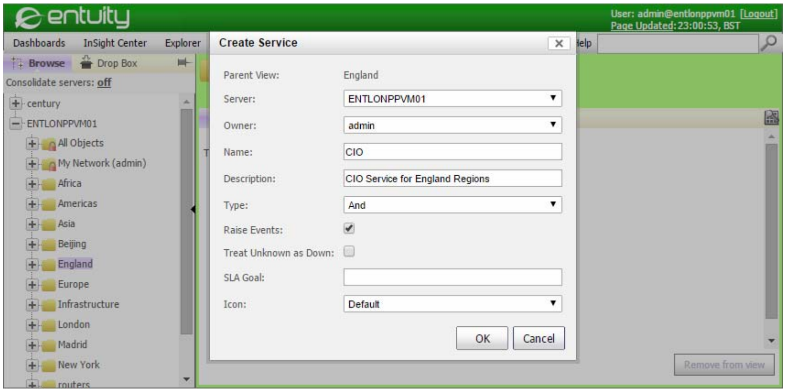
| Service | Condition | Raise Event | Type | Hierarchy Level |
|---|---|---|---|---|
| CIO | | True | Standard (root) | 1 |
| Network | | True | Standard (technology) | 2 |
| Data Center Core | OR | True | Standard (technology) | 3 |
| Region:Ilkley | | False | Site | 4 |

Table 10 Selected Example Services

## Creating CIO Perspective

To create the example CIO Perspective:

1) Create and name a view. The name should identify the purpose of the view, e.g. CIO London Office.
2) Highlight the view and from the context menu click **Create new services**.
3) Specify the root service of the perspective and name it **CIO**. This name must be uppercase. It identifies to Entuity that the service is available to the CIO Perspective.



Create Service

Parent View: England

Server: ENTLONPPVM01

Owner: admin

Name: CIO

Description: CIO Service for England Regions

Type: And

Raise Events: ☑

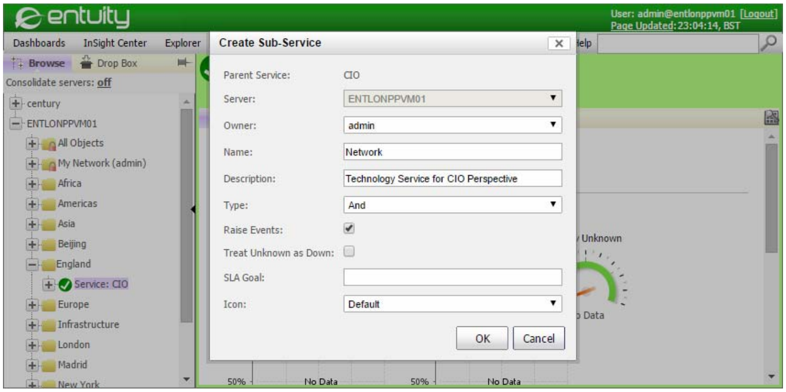
Treat Unknown as Down: ☐

SLA Goal:

Icon: Default

Figure 64 Create CIO Parent Service

4) Develop the structure of the service. Define sub-services for the perspective, these appear as the main groupings within the CIO Perspective, e.g. Network, Load Balancer, DNS.



Create Sub-Service

Parent Service: CIO

Server: ENTLONPPVM01

Owner: admin

Name: Network

Description: Technology Service for CIO Perspective

Type: And

Raise Events: ☑

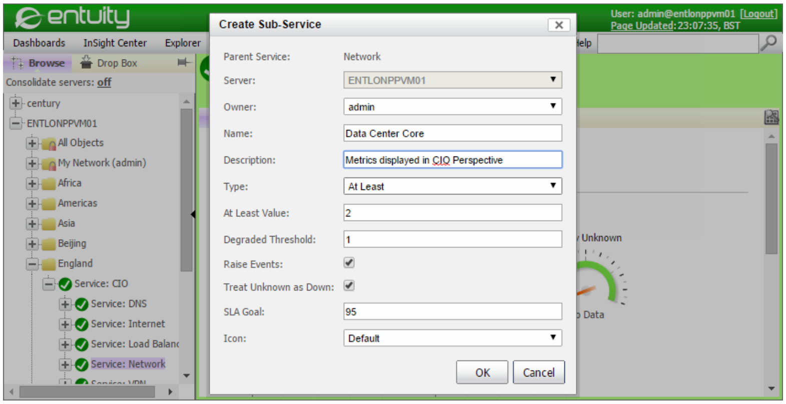
Treat Unknown as Down: ☐

SLA Goal:

Icon: Default

Figure 65 Create CIO Sub-Services

5) Define technology sub services for each grouping, for example in Network, enter Data Center Core, Global Wireless.



Create Sub-Service

Parent Service: Network

Server: ENTLONPPVM01

Owner: admin

Name: Data Center Core

Description: Metrics displayed in CIO Perspective

Type: At Least

At Least Value: 2

Degraded Threshold: 1

Raise Events: ☑

Treat Unknown as Down: ☑

SLA Goal: 95

Icon: Default

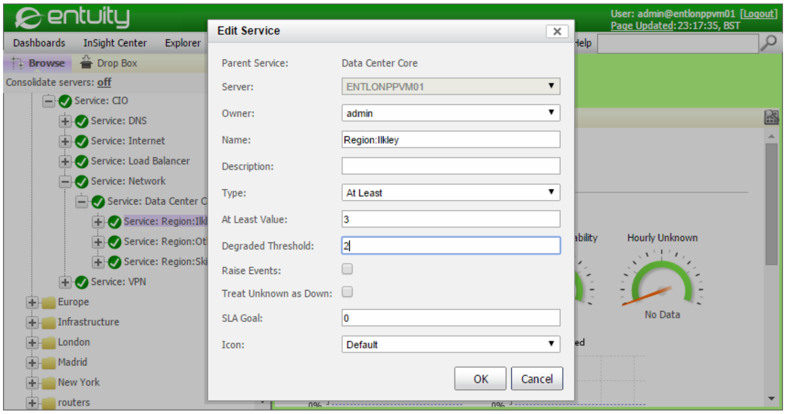
OK Cancel

Figure 66 CIO Technology Service

6) Configure the region services.

In this example Data Center Core includes state services to identify when service delivery is degrading allowing users to take action before a blackout, and also grouping of service delivery, in this case by office.

It is against the technology services that you could set SLA levels for inclusion to the perspective.



Edit Service

Parent Service: Data Center Core

Server: ENTLONPPVM01

Owner: admin

Name: Region:Ilkley

Description:

Type: At Least

At Least Value: 3

Degraded Threshold: 2

Raise Events: ☐

Treat Unknown as Down: ☐

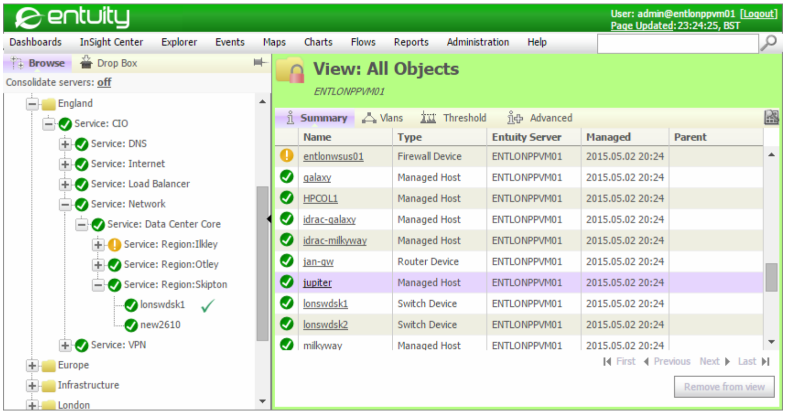
SLA Goal: 0

Icon: Default

OK Cancel

Figure 67 CIO Site Service

7) Drag and drop to the services the required devices and components. If required ports and/or IP SLA operations are configured on devices that are not in the view, then they should be dragged in to the view on their own.



| | Name | Type | Entuity Server | Managed | Parent |
|---|---|---|---|---|---|
| ! | entlonwsus01 | Firewall Device | ENTLONPPVM01 | 2015.05.02 20:24 | |
| ✓ | galaxy | Managed Host | ENTLONPPVM01 | 2015.05.02 20:24 | |
| ✓ | HPCOL1 | Managed Host | ENTLONPPVM01 | 2015.05.02 20:24 | |
| ✓ | idrac-galaxy | Managed Host | ENTLONPPVM01 | 2015.05.02 20:24 | |
| ✓ | idrac-milkyway | Managed Host | ENTLONPPVM01 | 2015.05.02 20:24 | |
| ✓ | jan-gw | Router Device | ENTLONPPVM01 | 2015.05.02 20:24 | |
| ✓ | jupiter | Managed Host | ENTLONPPVM01 | 2015.05.02 20:24 | |
| ✓ | lonswdsk1 | Switch Device | ENTLONPPVM01 | 2015.05.02 20:24 | |
| ✓ | lonswdsk2 | Switch Device | ENTLONPPVM01 | 2015.05.02 20:24 | |
| ✓ | milkyway | Managed Host | ENTLONPPVM01 | 2015.05.02 20:24 | |

Figure 68 Drag and Drop Components

# Checking on Service Status

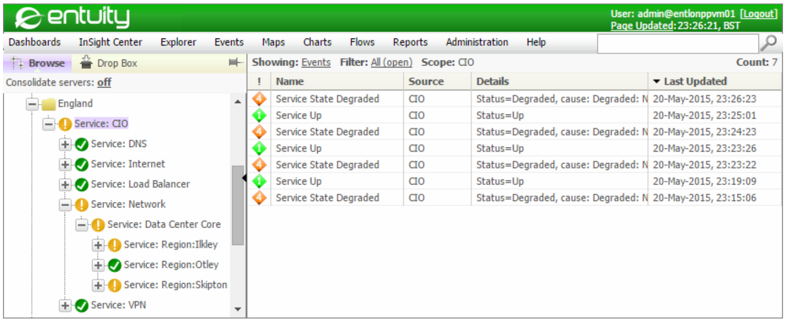
You can manage the state of your services by tracking service events and the Service State Problem incident through Event Viewer, by investigating services through dashboards and running reports.

When setting up services you should consider on which services you want Entuity to raise events. In our example three regions **Ilkley**, **Leeds** and **Skipton**, are used to pass on their state to their parent service **Data Core Center**. It is the state of the parent service which is considered important and against which you want Entuity to raise events.

Entuity includes service specific events:

- Service Down, indicates the named service is down and that the number of components failing in the service is sufficient to cause the service to fail.
- Service Degraded, indicates the named service is running in a degraded state.
- Service State Unknown, indicates the state of the named service is unknown. The state of one or more of the components in the service is unknown.
- Service Up, indicates the named service is up, its state having previously been Down or Unknown.

The state of the Service State Problem incident is determined by these events.



User: admin@entlonppvm01 [Logout]
Page Updated: 23:26:21, BST

Consolidate servers: off

- England
  - Service: CIO
    - Service: DNS
    - Service: Internet
    - Service: Load Balancer
    - Service: Network
      - Service: Data Center Core
        - Service: Region:Ilkley
        - Service: Region:Otley
        - Service: Region:Skipton
    - Service: VPN

Showing: Events Filter: All (open) Scope: CIO Count: 7

| ! | Name | Source | Details | Last Updated |
|---|---|---|---|---|
| ◆ | Service State Degraded | CIO | Status=Degraded, cause: Degraded: N | 20-May-2015, 23:26:23 |
| ◆ | Service Up | CIO | Status=Up | 20-May-2015, 23:25:01 |
| ◆ | Service State Degraded | CIO | Status=Degraded, cause: Degraded: N | 20-May-2015, 23:24:23 |
| ◆ | Service Up | CIO | Status=Up | 20-May-2015, 23:23:26 |
| ◆ | Service State Degraded | CIO | Status=Degraded, cause: Degraded: N | 20-May-2015, 23:23:22 |
| ◆ | Service Up | CIO | Status=Up | 20-May-2015, 23:19:09 |
| ◆ | Service State Degraded | CIO | Status=Degraded, cause: Degraded: N | 20-May-2015, 23:15:06 |

Figure 69 Service Events

From Event Viewer you can place your mouse pointer over the event to display a pop up dialog that provides event details, with *Details* indicating the causal component(s) of the service event.

You can also investigate service performance:

1) Click **Dashboards** > **Service Summary**.

   You can view the current status of all services and also drilldown to view service details. Depending on your Preferences settings, services are grouped by:

   - View, with Entuity listing the services in each view.
   - Alphabetically, with Entuity listing the services in alphabetic order and also including a listing of views through which the service is available.

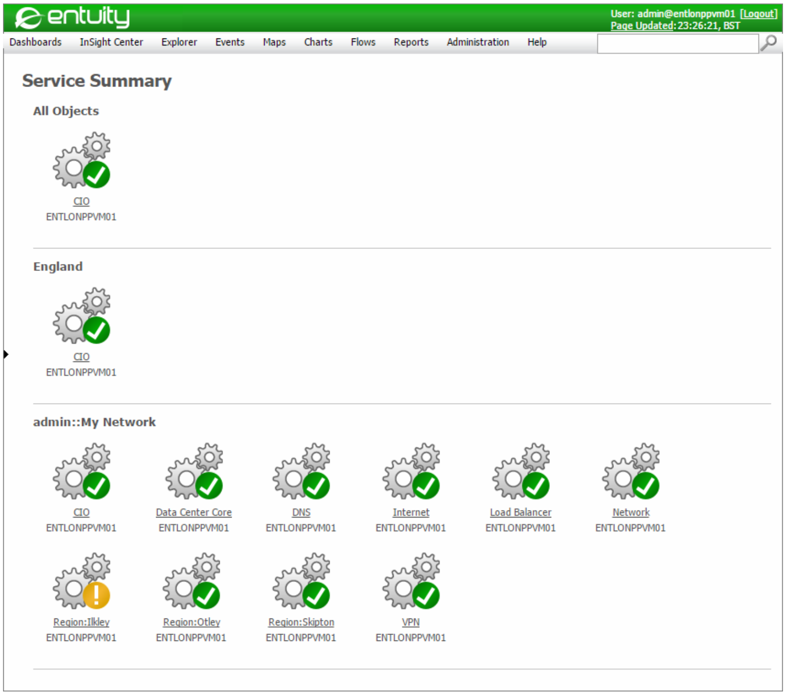
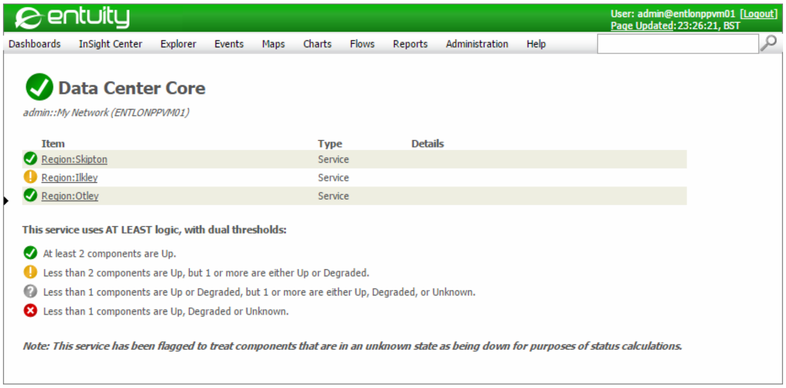


Figure 70 Service Summary Dashboard

2) For services that are in a Down or Degraded state you can place the mouse pointer over the service to view a popup that details the failing component(s).

3) Click on the required service to drill down. Entuity displays details on the service, including its components, their current state and the logic used to derive the state of the service.

   You can further drill down to investigate the cause of component failures.



✓ Data Center Core

*admin::My Network (ENTLONPPVM01)*

| | Item | Type | Details |
|---|---|---|---|
| ✓ | Region:Skipton | Service | |
| ! | Region:Ilkley | Service | |
| ✓ | Region:Otley | Service | |

**This service uses AT LEAST logic, with dual thresholds:**

✓ At least 2 components are Up.

! Less than 2 components are Up, but 1 or more are either Up or Degraded.

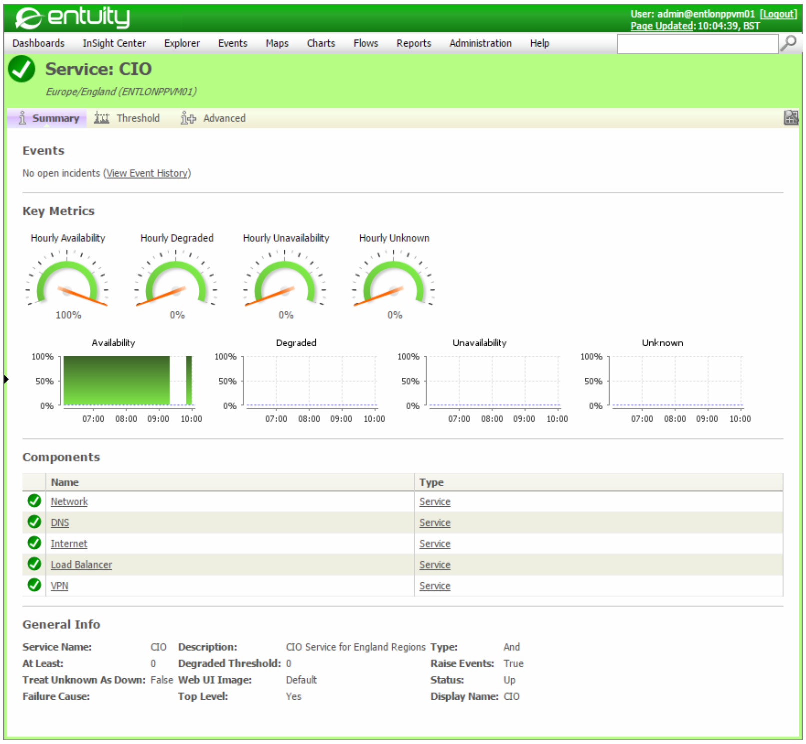
? Less than 1 components are Up or Degraded, but 1 or more are either Up, Degraded, or Unknown.

✗ Less than 1 components are Up, Degraded or Unknown.

***Note: This service has been flagged to treat components that are in an unknown state as being down for purposes of status calculations.***

Figure 71 Service Summary Component Drilldown

As a service you can view further details on CIO through the service Summary and Advanced pages. (See *Service Summary* and *Service Advanced Details*.)



✓ Service: CIO

*Europe/England (ENTLONPPVM01)*

**Events**

No open incidents (View Event History)

**Key Metrics**

**Components**

| | Name | Type |
|---|---|---|
| ✓ | Network | Service |
| ✓ | DNS | Service |
| ✓ | Internet | Service |
| ✓ | Load Balancer | Service |
| ✓ | VPN | Service |

**General Info**

| | | | | | |
|---|---|---|---|---|---|
| **Service Name:** | CIO | **Description:** | CIO Service for England Regions | **Type:** | And |
| **At Least:** | 0 | **Degraded Threshold:** | 0 | **Raise Events:** | True |
| **Treat Unknown As Down:** | False | **Web UI Image:** | Default | **Status:** | Up |
| **Failure Cause:** | | **Top Level:** | Yes | **Display Name:** | CIO |

Figure 72 CIO Service Summary

# 8 Map Device Connectivity

An Entuity map is a visual representation of the network connectivity of the selected view. If you amend a map, for example add a device, then you are also amending the view.

Maps show the:

- Devices in a view and any sub-views of that view.
- Connections of those devices, including representing any connections between sub-views.
- Device and connection status, Entuity automatically updates these states.
- Technology used when discovering those connections.

You also have the option of viewing a map with either a status or utilization overlay.

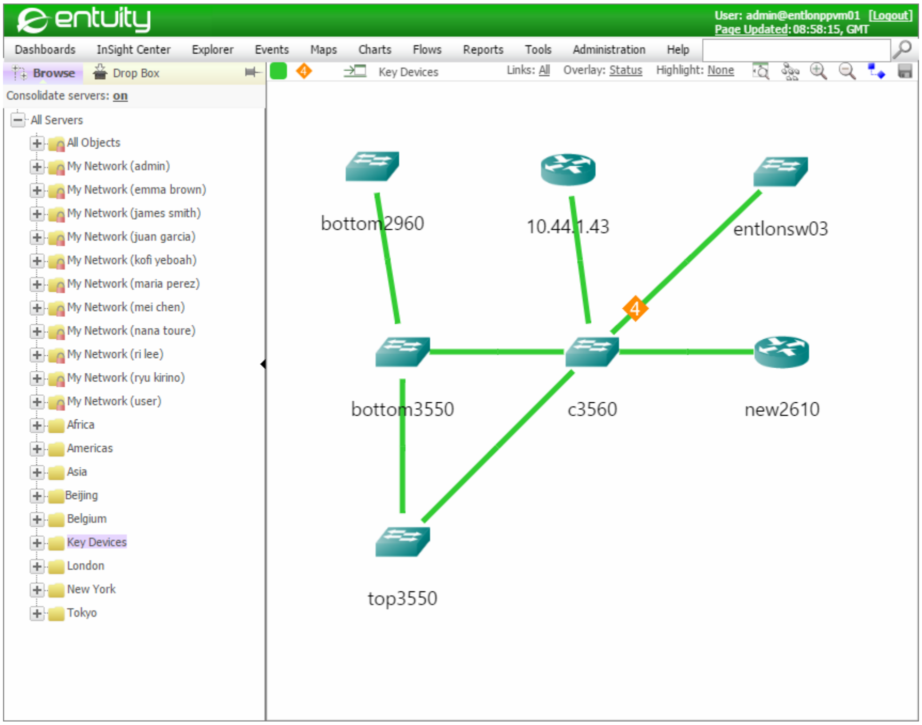


Figure 73 Entuity Maps

Entuity automatically updates the status of objects within an open map as they change. Entuity can automatically:

- Display new links between devices.
- Remove unmanaged devices from the map.

- Display new devices that meet the map filter criteria, for example a view based map where the view contains new devices since the map was uploaded.

With Entuity Maps you can:

- Control the display of link types used to identify the connectivity of the managed objects.
- Set how device and link status are presented.
- Add your own links between map objects, and associate to the link relevant objects for giving the link a meaningful state, for example the connecting ports between two devices.

You can control presentation of the map by:

- Applying a background image.
- Using the panning and resizing tools to aid navigation.
- Using layout tools, including manual and automatic mechanisms.

# Map Event Severity

Each Entuity incident type has a severity level, and the severity is color coded. Entuity maps display incident icons against devices and links that have open incidents with a severity level greater than Information. The icon severity level is derived from the associated open incident with the highest severity level.

| Symbol | Description | Color | Status Used By |
|---|---|---|---|
| 1 | Information | green | Event Viewer/Maps |
| 2 | Minor | yellow | Event Viewer/Maps |
| 3 | Major | amber | Event Viewer/Maps |
| 4 | Severe | orange | Event Viewer/Maps |
| 5 | Critical | red | Event Viewer/Maps |

Table 11 Color Coding Event Severity Status

# Determining Object and Link Status and Utilization

Entuity maps include Status and Utilization overlays. From all of the individual components on the map that could contribute to the status of an object or link, or provide utilization data, Entuity must determine the active component. Entuity also considers the Links selection, for example if you only select the Routing protocols the map will not display link utilization data.

## Utilization and State Color Coding

The following tables show the colors of nodes and links on the map, and the order of precedence for aggregation purposes, (with the first row having the highest precedence, followed by the second and so on).

Maps aggregate the components of a link and the components in a sub-map when determining the worst state to apply to that link or sub-map however:

- Devices and Ports that have a node status of Administration Down or System Uninitialized are not used when aggregating states. If for example all devices in a sub-map are in one of these states then the aggregated status means the sub-map does not have a background color (in the following table this is given as None).
- If a link has an associated port, peer, ATM VCC or FR DLCI then the status of that port, peer, ATM VCC or FR DLCI will be used. In all other cases (i.e. no port, HNIC, VMNIC and Host Connector) the port's status will be considered as Administration Down.

✓ Administration Down and System Uninitialized states are represented using blue outside of the map. The map does not use a color. This is to avoid confusion with the utilization overlay where blue is used to represent low utilization.

| Object Status | Object Color | Link Color | Description |
|---|---|---|---|
| Down | 🟥 | 🟥 | Device or Port is being polled and is down. |
| Degraded | 🟧 | 🟧 | Device or Port is being polled and is degraded. |
| Unknown | ▩ | ▩ | Device or Port is being polled, but Entuity could not determine the status, for example because:<br>■ Device unreachable but not root cause.<br>■ Port data unavailable because the device is down. |
| OK | 🟩 | 🟩 | Device or Port is being polled and is OK. |
| Administration Down | None | ⬛ | Entuity identifies an object as administration down when:<br>■ For a device Entuity polling of the device is disabled.<br>■ It is a Custom Device and is therefore not polled.<br>■ For a port it is set to administration down.<br>■ A link does not have an associated port, for example when using a physical connection. |
| System Uninitialized | None | ⬛ | Device has not yet been fully discovered by the system therefore the object does not have a background color. Port has not yet been fully discovered by the system therefore the link will be black. |

Table 12 Status Overlay

| Object Status | Utilization State | Object Color | Link Color | Description |
|---|---|---|---|---|
| OK or Degraded | Critical | 🟥 | 🟥 | Device or Port is responding and has crossed its critical utilization threshold. |
| OK or Degraded | High | 🟧 | 🟧 | Device or Port is responding and has crossed its High utilization threshold. |
| OK or Degraded | Low | 🟦 | 🟦 | Device or Port is responding and has crossed its low utilization threshold. |
| OK or Degraded | Unknown | ▒ | ▒ | Device or Port utilization could not be determined. |
| Unknown | Any | ▒ | ▒ | Device or Port utilization could not be determined. |
| Down | Any | ▒ | ▒ | Device or Port utilization could not be determined. |
| OK or Degraded | Normal | 🟩 | 🟩 | Device or Port is responding, and has not breached any utilization thresholds |
| Administration Down | Any | None | ⬛ | Entuity identifies an object as administration down when:<br>▪ For a device Entuity polling of the device is disabled.<br>▪ It is a Custom Device and is therefore not polled.<br>▪ For a port it is set to administration down.<br>▪ A link does not have an associated port, for example when using a physical connection. |
| System Uninitialized | Any | None | ⬛ | Device or Port has not yet been fully discovered by the system. |
| OK or Degraded | Null (no data returned) | None | ⬛ | Device or Port is ok but utilization data cannot be retrieved. |

Table 13 Utilization Overlay

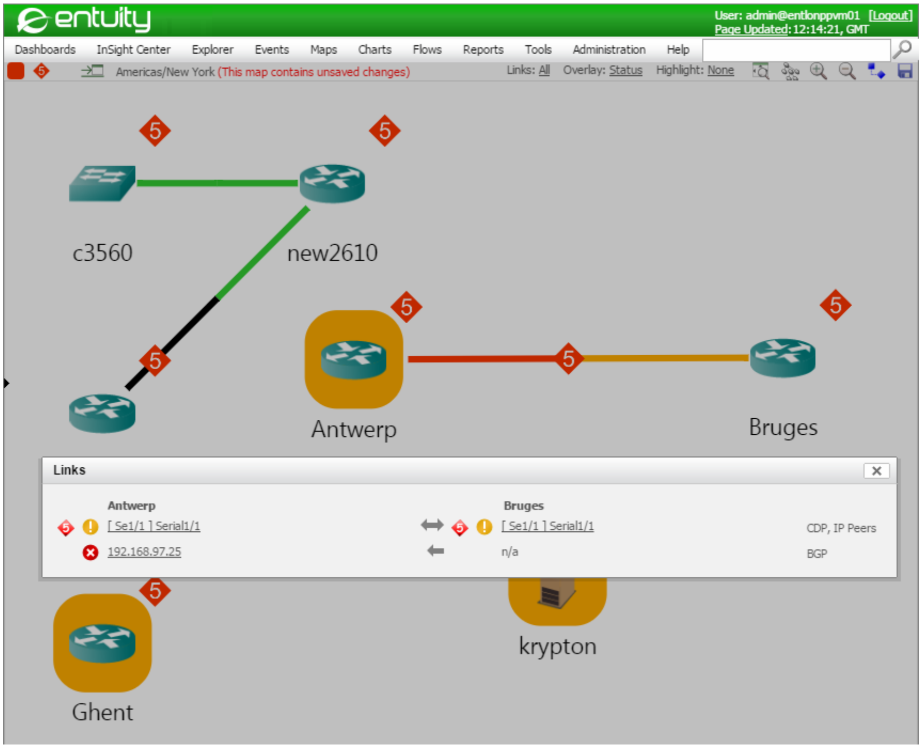
## Deriving Object Status and Utilization

Entuity uses the device status on the Status overlay. Device utilization is derived from CPU utilization.

## Deriving Link Status

Link status is taken from the two endpoints of the active link. When the two endpoints have different states then Entuity displays the two ends of the link with different colors, colors that are appropriate to the state at that end of the link. If different technologies are reporting different states the map displays the worst state of those links displayed on the map.

If a user double-clicks on the link it opens a dialog detailing the two ends of the link and the active components involved in the link, e.g. port, VNIC, BGP peer.



Links

| | Antwerp | | Bruges | |
|---|---|---|---|---|
| 5 ! | [ Se1/1 ] Serial1/1 | ↔ | 5 ! [ Se1/1 ] Serial1/1 | CDP, IP Peers |
| ✖ | 192.168.97.25 | ← | n/a | BGP |

Figure 74  Reporting the Worst State on a Link

When determining a link status on a map Entuity always uses the highest active component, for:

- Non-channel-based-wan connections there is usually only a single topology node in the link from which to derive link status, i.e. a port.
- Channelized links state is derived from the highest level of the link, for example if the link is:

  `device > port > frDlci - atmVcc < port < device`

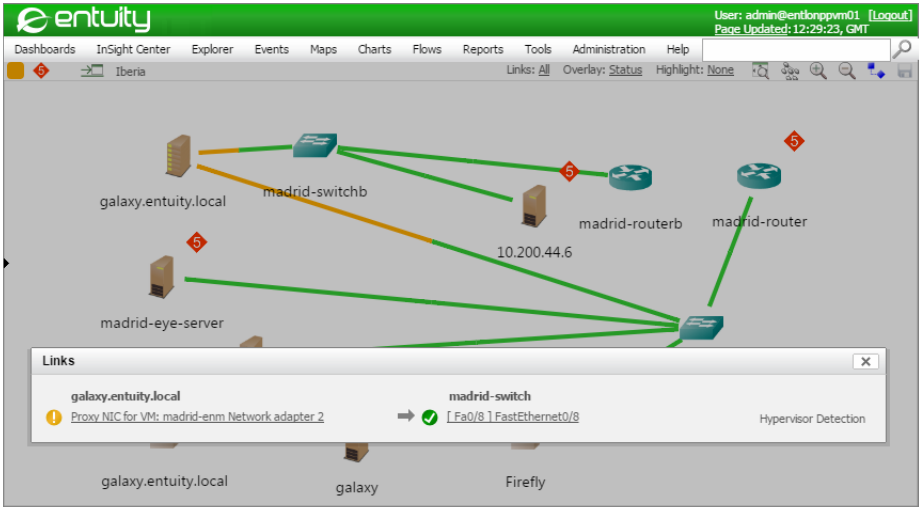
  then the active link is `frDlci- atmVcc` and the left hand side status will be that of the frDlci topology node and the right hand side will be that of the atmVcc.

Entuity maps can represent links where one endpoint will not return a state, for example:

- Switch to hypervisor (no state from the hypervisor).
- Hypervisor to managed host (no state from the hypervisor).
- Custom Device to a device (no state from the Custom Device).

Entuity maps can also represent link types that will never have a state:

- Custom Device to Custom Device (no state from the user created nodes).



Links

galaxy.entuity.local
Proxy NIC for VM: madrid-enm Network adapter 2

madrid-switch
[ Fa0/8 ] FastEthernet0/8

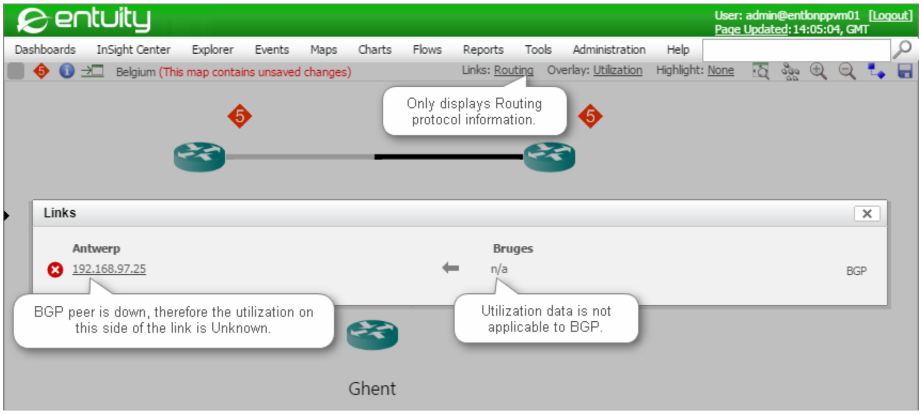
Hypervisor Detection

Figure 75 VNIC to Port Connections

## Deriving Link Utilization

Link utilization is always derived from the port involved in the link. If port utilization data is not available then the utilization link is set to Unknown (a gray line). However, if no utilization is shown for the link (a black line) this indicates the connection does not have identified ports which may be because:

- It is a physical connection to a device (rather than to an interface on the device).
- The device is a hypervisor.
- The device is a managed host.
- The map Links is set to Routing, and the routing protocols do not refer to ports. However if the peer involved in the link is down then the map does display a gray link. This indicates that the peer is unavailable.


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 14:05:04, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Belgium (This map contains unsaved changes)
Links: Routing Overlay: Utilization Highlight: None
5
Links
Antwerp
192.168.97.25
Bruges
n/a
BGP
Ghent

Only displays Routing protocol information.

BGP peer is down, therefore the utilization on this side of the link is Unknown.

Utilization data is not applicable to BGP.

Figure 76 Gray and Black Utilization States

## Maps Interface Overview

You can manage maps through controls available from context menus and the maps toolbar. Context menus display appropriate map commands and also provide access to the wider functionality available with Entuity, e.g. Explorer, Live Status, Trace Route.

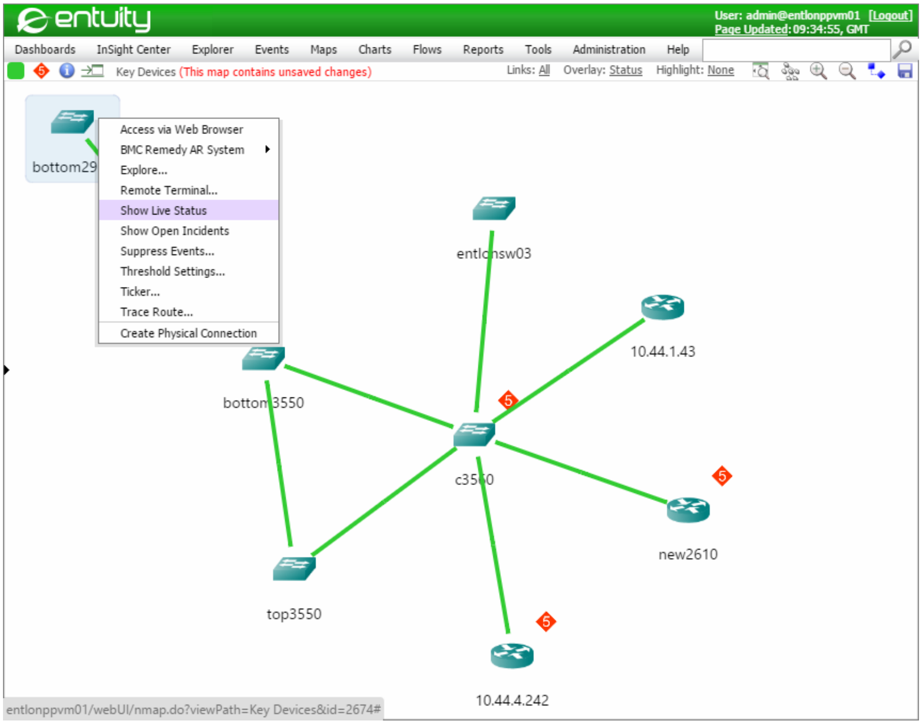

entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 09:34:55, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Key Devices (This map contains unsaved changes)
Links: All Overlay: Status Highlight: None
bottom29
Access via Web Browser
BMC Remedy AR System
Explore...
Remote Terminal...
Show Live Status
Show Open Incidents
Suppress Events...
Threshold Settings...
Ticker...
Trace Route...
Create Physical Connection
entlonsw03
10.44.1.43
bottom3550
c3560
new2610
top3550
10.44.4.242
5
entlonppvm01/webUI/nmap.do?viewPath=Key Devices&id=2674#

Figure 77 Maps Context Menu

From the Maps toolbar you have immediate access to its functionality and also its current setup, for example the name of the map view, the applied overlay, links displayed.

| Label | Description |
|---|---|
| 🟧 | Displays the worst state of a device or link in the map using the selected *Overlay* metric, i.e. Utilization or Status.<br>When the state changes the icon blinks five times. |
| 5 | Displays the severity level of the incident with the worst severity level in the map. By default this includes incidents raised against devices in the view and their ports. Through a user preference setting port incidents can be excluded.<br>When the state changes the icon blinks five times. |
| ℹ | Indicates a possible issue with the map. A mouse rollover provides a summary of any issue. You can click on the icon to display more details. |
| ⇥ | Opens the current map in a new window. You can also drag the icon to a pane in the Dashboard Editor which adds the map URL to the dashboard. |
| View Path | Identifies the full path of the map's view. A forward slash separates a sub-view from its parent view. For example Asia/Beijing indicates Beijing is a sub-view of Asia. |
| *Links* | Links control the type of link between objects included to the map, for example trace route, IP peering, BGP. |
| *Overlay* | Select the type of information displayed within the map:<br>■ **Status** displays current state for managed objects and link states derived from interfaces linking objects on the map. (See *Show Map Status Overlay*.)<br>■ **Utilization** displays utilization of the links between objects (derived from port utilization) and also the CPU utilization of devices. (See *Show Map Utilization Overlay*.) |
| *Highlight* | Select a view, service or network path (when you have a remote Entuity SurePath server) and then components that are outside of the selection are grayed out. (See *Highlight a View, Service or Network Path*.) |
| 🔍 | Click to resize the map so that all of it fits into the current map pane. |
| ⁂ | Click to display the layout options, Radial Layout and Grid Layout. |
| 🔍+ | Click to zoom into the map. You can also use your mouse wheel to zoom in. |
| 🔍− | Click to zoom out of the map. You can also use your mouse wheel to zoom out. |
| ■→◆ | Click to download the current map as a Visio (`.vdx`) document. The file is saved to the default download folder of your web browser. |
| 💾 | Click to save the current map. When you have not changed the map this icon is grayed out, when you do not have the permission to save the map it is crossed out. |

Table 14 Map Toolbar

The behavior of map select functionality:

- Select is available on the object icon and not on its background or its label.
- Selecting an object on the right-click also opens the context menu.

- Press the `Shift` key, hold down the left mouse button and then drag the mouse pointer over the map to draw a selection box. Every object inside the box is selected.
- Press the `CNTRL` key and then click on objects in the map to select a particular set of objects.
- Click on the map background to clear the current selection. You can also clear the selection by clicking an object or link that is not part of the current selection.
- If an object is selected in the tree it is also selected in the map. Selecting an object in the map would not update the tree.
- Double-click on a sub-view in a map to drill-down to the map of that sub-view. Entuity also updates the tree to select this view as a drill-down is an explicit action for opening a new view map.

## Map Progress Bar

The map progress bar is displayed at the foot of the loading map. It indicates the progress of both the loading of objects within the map and their states. This may be most noticeable when loading devices and links that are from remote Entuity servers.

## Map Icons

Entuity displays managed devices by associating the device type against a supplied icon.

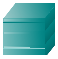
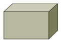
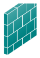
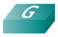
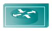
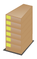
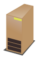
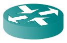
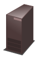
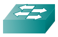
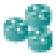
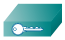
| Icon | Name | Icon | Name |
|---|---|---|---|
|  | BladeCenter |  | DeviceEx |
| | A device managed through Entuity but not SNMP polled, e.g. a Ping Only device, a VM Platform, Custom Device. |  | Firewall |
|  | Generic Device |  | Hub |
|  | Hypervisor |  | Managed Host |
|  | Router |  | Server |
|  | Switch |  | View |
| | Virtual machine, fully managed. |  | VPN Gateway |

Table 15 Map Icons

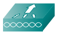
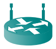
| Icon | Name | Icon | Name |
|---|---|---|---|
|  | Wireless Controller |  | Wireless Router |

Table 15 Map Icons

## Views, Security and Maps

A map is a visual representation of a view. The permissions you have on a map are the same as those you have on the view:

- Administrators have full read, save and edit permissions.
- For non-administrators, your level of access to maps is determined by the level of permission you have to the view.

All Objects and My Network views have different permissioning behavior to other views:

- All Objects view can be edited by administrators, who can assign access and edit permissions to other user groups. User groups with the edit permission, and appropriate view tool permissions, can then also assign access and the edit permission to other user groups. Members of user groups with the edit permission will be able to edit and save All Objects maps.
- My Network views by default can be edited by administrators for example to edit incident and event filters. Administrators and view owners will also be able to edit and save My Network maps.

## Map Publishers

When you open a map this sends a request to the Entuity server for information on the objects in that map. Publishers manage the request and the return of information. For each type of information available through the map Entuity creates its own publisher. Potentially each map has six types of publishers:

- Highlights
- Incidents
- Links
- Nodes
- Utilization
- Views.

Each publisher has a set of associated attributes. If one of these attributes changes this causes the publisher to update the map. If a publisher cannot return information then Entuity updates the map notification and reports the publisher that failed.

| Icon | Information Description |
|---|---|
| i | Information messages, for example in server consolidation mode some remote servers may not have the current view, or if they do the current user does not have the permission to access it. |
| ! | Error messages reporting the failure of a publisher. For example if a remote server is taken down then all of its publishers will be identified as unavailable. |

Table 16 Map Publisher Messages

If the map includes devices from remote servers then proxy publishers are created on those remote servers. All information is returned to the central server. The background color of devices and the color of connections on the map are automatically updated to show the polled status of the devices and ports no matter which server is managing them.

Entuity can report the failure of individual publishers and identify the server. If a remote server is unavailable then:

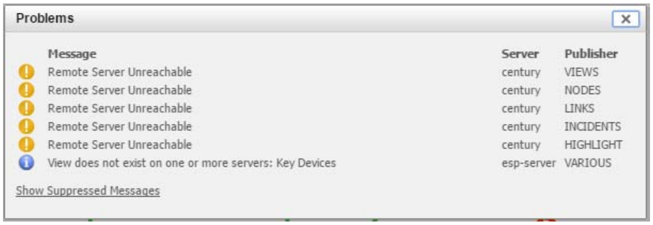
- All of its publishers will fail. The failure is identified through the map information icon.
- The state of objects on the map remains unchanged. If you refresh the map or re-open the map then the objects from the unavailable remote server are not displayed.

To check the status of the map publishers:

1) From the map click on the notification icon.

   Entuity displays a summary of the notifications.

2) Click on Show Suppressed Messages. Entuity provides a breakdown of the map messages and identifies the source Entuity server.



Problems

| | Message | Server | Publisher |
|---|---|---|---|
| ! | Remote Server Unreachable | century | VIEWS |
| ! | Remote Server Unreachable | century | NODES |
| ! | Remote Server Unreachable | century | LINKS |
| ! | Remote Server Unreachable | century | INCIDENTS |
| ! | Remote Server Unreachable | century | HIGHLIGHT |
| i | View does not exist on one or more servers: Key Devices | esp-server | VARIOUS |

Figure 78 Map Publisher Messages

## Viewing Connectivity

You can access a map by highlighting a view and then from the main menu clicking **Maps**. As Entuity opens the map it automatically updates the status of devices and links.

As more than one user can access the same view and therefore map it is possible that another user will make and save map while you are viewing it. Depending upon your permission level to the view, and your user preference setting, Entuity either automatically updates the map with changes to the map or prompts you to refresh and therefore accept the changes or reject the option to refresh and therefore retain the potential to update the view with your current map layout.

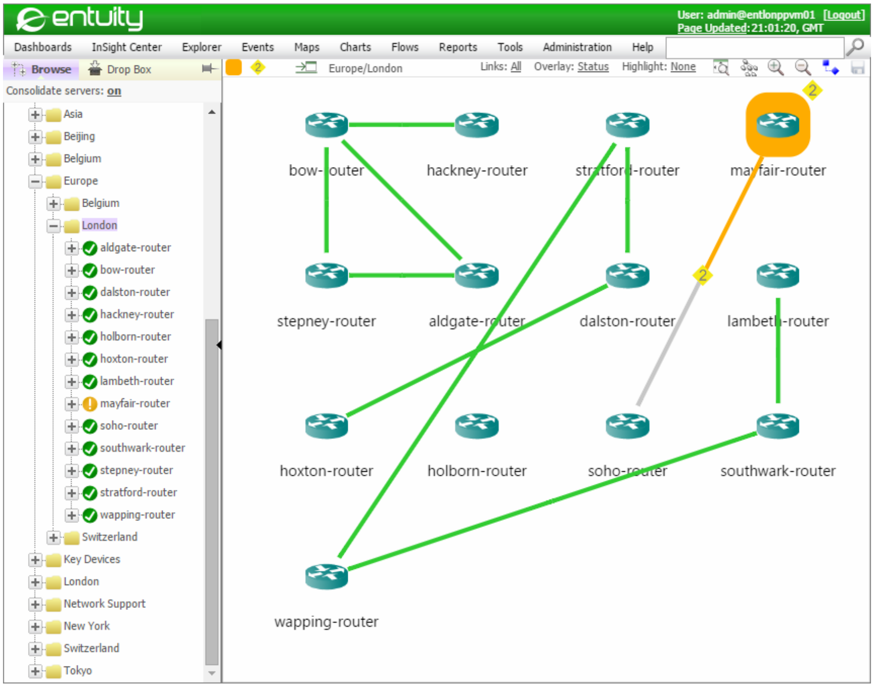


Figure 79 Mapping Views

## Set Map Link Types

Entuity network topology is the product of a number of discovery technologies. Entuity combines these technologies to provide a clear view of the network topology. When you select two or more link types to display, and they have different statuses, the map displays the worst state.

By default a new map shows all link types, a saved map shows the link types saved to it. You can control the combination of link types used on a map and this will effect the state Entuity associates with the links. It is therefore important to select link types appropriate to your purpose. For example setting map links to only use the routing technologies would not be useful if you are interested in utilization performance.

The Links setting on a higher level map also impacts how Entuity calculates the states returned to that map from its sub-views. However when you drill down from one map to a second map the second map does not inherit the settings of the first. The second map uses its own defaults; Links, Overlay and Highlight settings are set per map.

Entuity supports these link types and you can select any combination of them in a map:

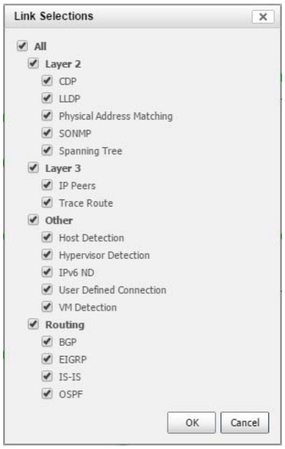
- Layer 2

  - Cisco Discovery Protocol (CDP)
  - Link Layer Discovery Protocol (LLDP)
  - Physical Address Matching
  - SynOptics Network Management Protocol (SONMP)
  - Spanning Tree
- Layer 3
  - IP Peers
  - Trace Route (ping state)
- Other
  - Host Detection
  - Hypervisor Detection
  - IPv6 ND. IPv6 ND is available in Entuity through the IPv6 module. When it is activated through `configure` Entuity discovers port IPv6 addresses on IPv6 managed devices. You can then use the IPv6 ND to show links between IPv6 devices using neighbor discovery.
  - User Defined Connection displays any user defined Physical Connections in the map.
  - VM Detection
- Routing
  - Border Gateway Protocol (BGP)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Intermediate System to Intermediate System (IS-IS)
  - Open Shortest Path First (OSPF).

  The routing protocols are available in Entuity through the Routing Protocols module. They are only available when the module is activated through `configure`.

To control the link type used to build a map:

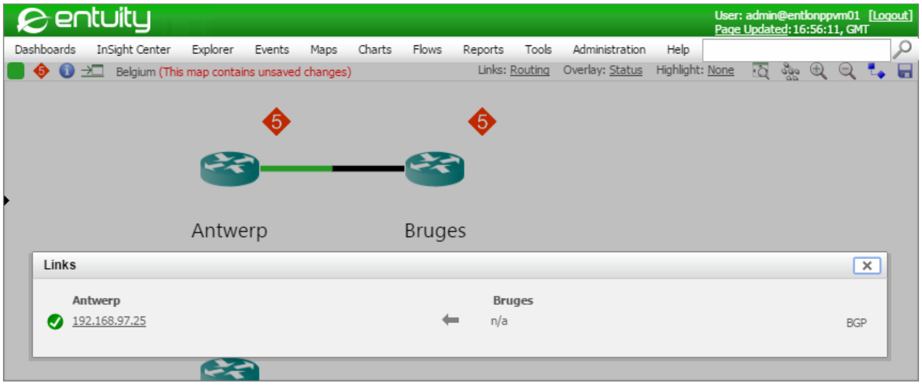
1) From the map toolbar click the Links current setting, e.g. **All**.
2) From the Link Types dialog use the check boxes to select and deselect link types.



Link Selections

- ☑ All
  - ☑ Layer 2
    - ☑ CDP
    - ☑ LLDP
    - ☑ Physical Address Matching
    - ☑ SONMP
    - ☑ Spanning Tree
  - ☑ Layer 3
    - ☑ IP Peers
    - ☑ Trace Route
  - ☑ Other
    - ☑ Host Detection
    - ☑ Hypervisor Detection
    - ☑ IPv6 ND
    - ☑ User Defined Connection
    - ☑ VM Detection
  - ☑ Routing
    - ☑ BGP
    - ☑ EIGRP
    - ☑ IS-IS
    - ☑ OSPF

Figure 80 Map Link Types



Links

| Antwerp | | Bruges | |
|---|---|---|---|
| ✓ 192.168.97.25 | ⬅ | n/a | BGP |

Figure 81 Router Links

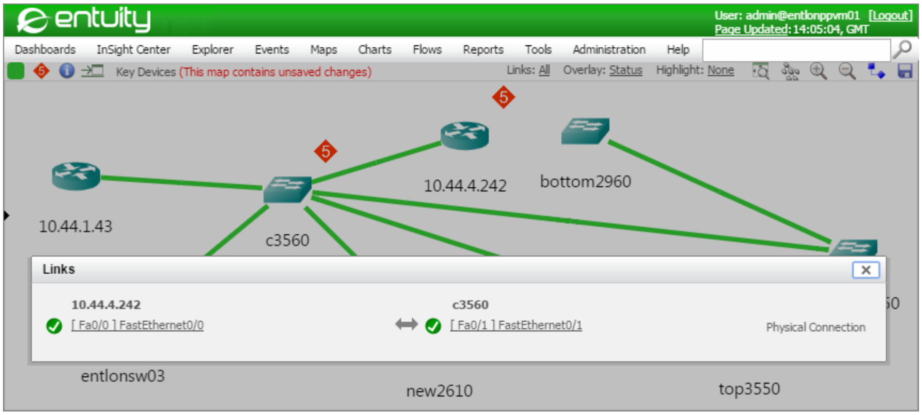
## Set Physical Connections

You might define physical connections between devices when Entuity does not automatically discover a connection between them, which may happen, for example, when:

- There is only a cable connection between devices.
- Two devices are managed by different Entuity servers.

Physical connections are unidirectional. You set source and destination devices and optionally specify the interfaces involved on one or both sides of the connection.

System administrators can create, edit and delete physical connections. All users can view the physical connection within a map if they have permission to access both the source and destination devices.



Links

| 10.44.4.242 | | c3560 | |
|---|---|---|---|
| ✓ [ Fa0/0 ] FastEthernet0/0 | ↔ | ✓ [ Fa0/1 ] FastEthernet0/1 | Physical Connection |

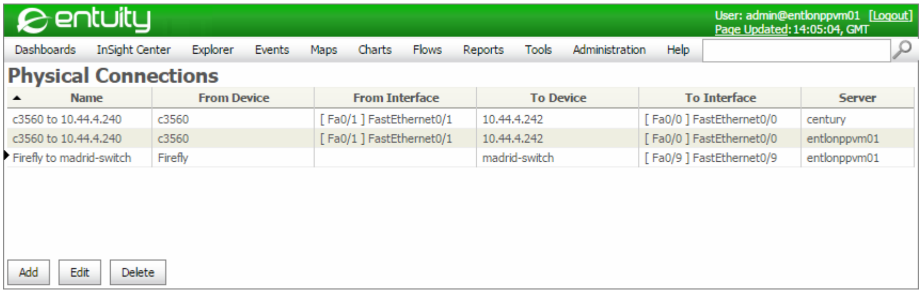
Figure 82 User Defined Physical Connections

## Viewing Configured Physical Connections

Physical Connections page displays a summary of each defined connection, you can change the connection attributes Entuity displays in the table through the **Configure Columns** context menu. From this page you can:

- View existing connections and their definitions.
- Add new connections.
- Edit connections, for example change an interface used in the connection.
- Delete connections.

You can manage connections through the Physical Connections page accessed by clicking **Administration** > **Inventory** / **Topology** > **Physical Connections**.



Physical Connections

| Name | From Device | From Interface | To Device | To Interface | Server |
|---|---|---|---|---|---|
| c3560 to 10.44.4.240 | c3560 | [ Fa0/1 ] FastEthernet0/1 | 10.44.4.242 | [ Fa0/0 ] FastEthernet0/0 | century |
| c3560 to 10.44.4.240 | c3560 | [ Fa0/1 ] FastEthernet0/1 | 10.44.4.242 | [ Fa0/0 ] FastEthernet0/0 | entlonppvm01 |
| Firefly to madrid-switch | Firefly | | madrid-switch | [ Fa0/9 ] FastEthernet0/9 | entlonppvm01 |

Figure 83 Physical Connections Listing

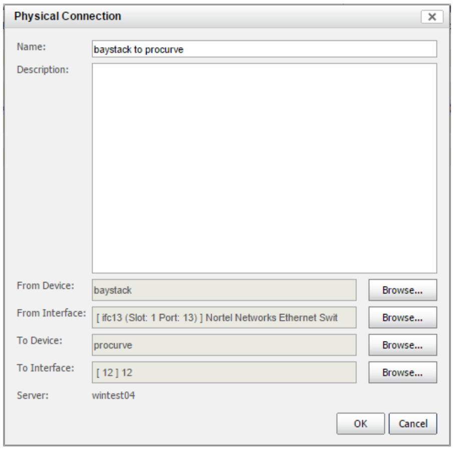
| Attributes | Description |
|---|---|
| *Enabled* | All new and updated physical connection definitions are enabled. The option to enable/disable physical connections has been removed. Unless a definition is migrated from an earlier version of Entuity this value is always Enabled. |
| *Name* | Display name of the physical connection. |
| *From Interface* | The interface on the device to which the source of the connection is associated. |
| *From Device* | The device to which the source of the connection is associated. |
| *To Interface* | The interface on the device which is the destination of the connection. |
| *To Device* | The device which is the destination of the connection. |
| *Description* | Full description of the connection, for example to describe its purpose. |
| *Created At* | Date and time the connection was created. |
| *Created By* | User who created the connection. |
| *Last Updated By* | User who most recently updated the connection. |
| *Last Updated At* | Time of the last change to the connection configuration. |
| *Server* | Entuity server on which the connection is defined. |

Table 17 Physical Connection Columns

## Adding Physical Connections

System administrators can define connections between devices, and optionally specify the interfaces on those devices. The devices can be managed by different Entuity servers.

After you define a physical connection Entuity then creates the association between the source and destination devices. This creation uses the discovery process. There will therefore be a short delay between defining a connection and for example Entuity displaying it in a map. When displayed on a map these connections will display a state.



Physical Connection

Name: baystack to procurve

Description:

From Device: baystack

From Interface: [ ifc13 (Slot: 1 Port: 13) ] Nortel Networks Ethernet Swit

To Device: procurve

To Interface: [ 12 ] 12

Server: wintest04

Figure 84 Add Physical Connections

| Attribute | Description |
|---|---|
| *Name* | Display name of the physical connection. |
| *Description* | Full description of the connection, for example to describe its purpose. |
| *From Device* | The device to which the source of the connection is associated. |
| *From Interface* | The interface on the device to which the source of the connection is associated. You can click **Browse** to open the Interface Selector and then pick the source interface of the connection. |
| *To Device* | The device which is the destination of the connection. |
| *To Interface* | The interface on the device to which is the destination of the connection. You can click **Browse** to open the Interface Selector and then pick the destination interface of the connection. |
| *Servers* | Entuity servers managing the devices and where the connection is stored. If the connection is between devices managed by different Entuity servers the connection definition is stored on both servers. The connection remains unidirectional. |

Table 18 Physical Connections

You can define a physical connection by clicking Add through the Physical Connections page, or you can select two devices on a map. With either method you define the connection details using the same Physical Connections dialog, although when called from the map the dialog will default details of the selected devices.

To create physical connections from the map:

1) Select the two devices.

   Click on the first device and holding down the `CNTRL` key click the second device.

2) From the context menu click **Create Physical Connection**.

3) Define the connection:
   - Enter a meaningful name and description.
   - Entuity defaults the source and destination devices. You can optionally specify from and to interfaces.
4) Click **Ok**.

### Deleting Physical Connections

To delete physical connections:

1) Click **Administration** > **Inventory** / **Topology** > **Physical Connections**.
2) Highlight the physical connection row.
3) Click **Delete**.

### Editing Physical Connections

To edit physical connections:

1) Click **Administration** > **Inventory** / **Topology** > **Physical Connections**.
2) Highlight the physical connection row.
3) Click **Edit**.
4) Amend the connection, for example to change the enabled state of the connection.
5) Click **OK**.

## Status and Utilization Map Overlays

Entuity maps include Status and Utilization overlays:

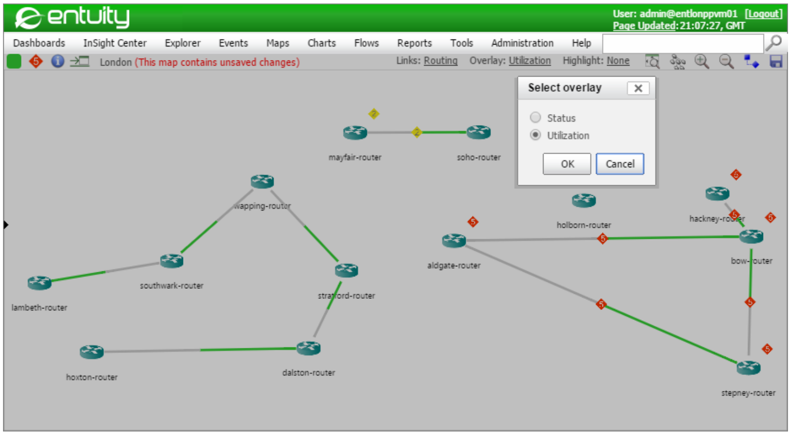
- Status overlay displays the state of the managed objects, for example for device this might be OK, Down, Unknown.

  The state of links between objects on a map is derived from the active components of the link and their state, for example ports linking devices on the map. (See *Show Map Status Overlay*.)
- Utilization displays utilization of the links between objects (derived from the active component at each end of the connection) and also the CPU utilization of devices. (See *Show Map Utilization Overlay*.)

*Overlay* indicates the map currently displayed, for example Utilization. It is also a hyperlink to the Select Overlay dialog through which you can change the map overlay type.

To change the map overlay:

1) Click on the current *Overlay* value, for example **Utilization**.
2) From the Select Overlay dialog select the overlay type and click **Ok**.



London (This map contains unsaved changes)

Links: Routing Overlay: Utilization Highlight: None

Select overlay

○ Status
● Utilization

OK Cancel

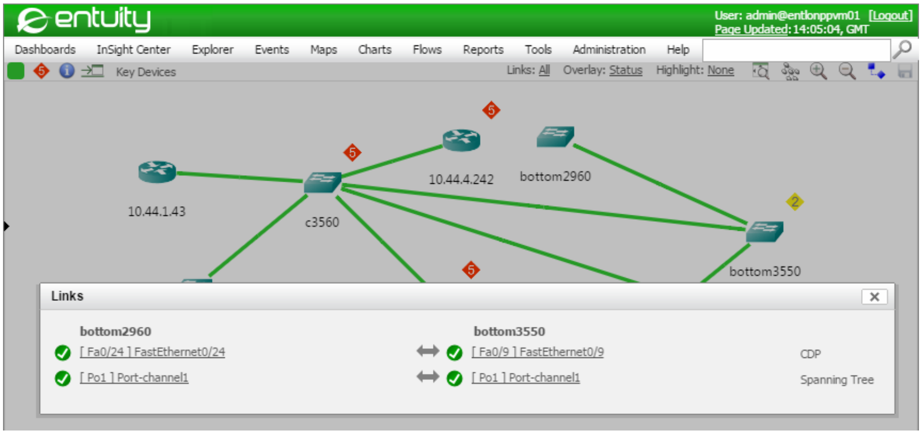
Figure 85 Select Map Overlay

## Show Map Status Overlay

Entuity Maps uses two separate status measures to indicate the health of the network:

- Event severity state is the highest severity level of the open event associated with the device or link. Entuity displays the event severity symbol on the device/link.
- Topology state is derived from the polling of the topology nodes, i.e. the state of the interfaces making the link between devices.

Both types of severity states are context dependent. Change the link type(s) displayed in the map and the displayed severity states can also change. When you pass the mouse over a link, you can open the context menu and select Details. Entuity then displays details of those enabled links including link state and event severity.


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 14:05:04, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
10.44.1.43
c3560
10.44.4.242
bottom2960
bottom3550

Key Devices

Links: All Overlay: Status Highlight: None

Links

| bottom2960 | | bottom3550 | |
|---|---|---|---|
| ✓ [ Fa0/24 ] FastEthernet0/24 | ↔ | ✓ [ Fa0/9 ] FastEthernet0/9 | CDP |
| ✓ [ Po1 ] Port-channel1 | ↔ | ✓ [ Po1 ] Port-channel1 | Spanning Tree |

Figure 86 Displayed States May Vary According to Link Type

For more information you can select a:

- Device and from its context menu select **Show Live Status**.
- Link and from its context menu select **Show Details**.

From both dialogs you can use hyperlinks to open the incident viewer in context.

## Show Map Utilization Overlay

The utilization map overlay displays link utilization data as color coded links and CPU utilization data as color coded backgrounds to devices. The overall utilization state of the map is derived from the worst utilization state returned by devices, links and sub-views and is displayed in the map toolbar. The background color of sub-views on utilization maps reflects the most severe level of utilization within that sub-view, whether it is derived from devices, links or other sub-views.

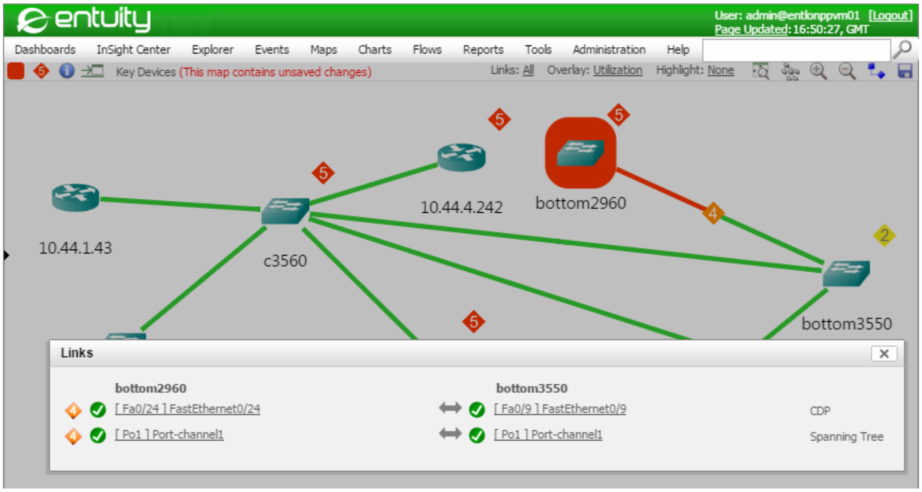
Each half of a link is color coded to reflect the utilization of that interface. Link color is derived by comparing the input and output utilization data for the ports involved in the link against the low and critical utilization thresholds for those ports. For example if a port returns inbound data that is below its low utilization threshold and outbound utilization above the high threshold then map uses the high threshold severity state, i.e. sets that interface's half of the link to red rather than blue.

Where a physical connection details the ports of the devices being connected then the link can also be drawn using utilization data. Where it is just between two devices there is no utilization data and the line will always be gray.

To view details on a utilization link:

1) Click on the link and from the context menu select **Show Details**.

   Entuity displays details of the devices and ports involved in the link. You can click on a port and Entuity displays a summary of port performance including charts on inbound and outbound utilization.



Links

| bottom2960 | bottom3550 | |
|---|---|---|
| 4 ✓ [ Fa0/24 ] FastEthernet0/24 | ↔ ✓ [ Fa0/9 ] FastEthernet0/9 | CDP |
| 4 ✓ [ Po1 ] Port-channel1 | ↔ ✓ [ Po1 ] Port-channel1 | Spanning Tree |

Figure 87 Utilization Overlay Map

# Layout Maps

When you open a new map it zooms to a level where all of the objects in the map are visible and lays them out according to the grid algorithm. When you have a large number of assets, a complex network structure or both the default presentation may not be appropriate. You can adjust the layout, by selecting one or more objects and dragging them to a new position. You can also control the view zoom and focus.

## Zoom and Pan Maps

You can control zoom and pan maps through your mouse controls:

- Rock the mouse wheel forward to zoom in the maps, and rock it backward to zoom out.
- Hold the mouse button down and drag the mouse pointer (now changed to the move pointer) in the direction you want to move the map. Release the mouse button when the map is positioned how you require.

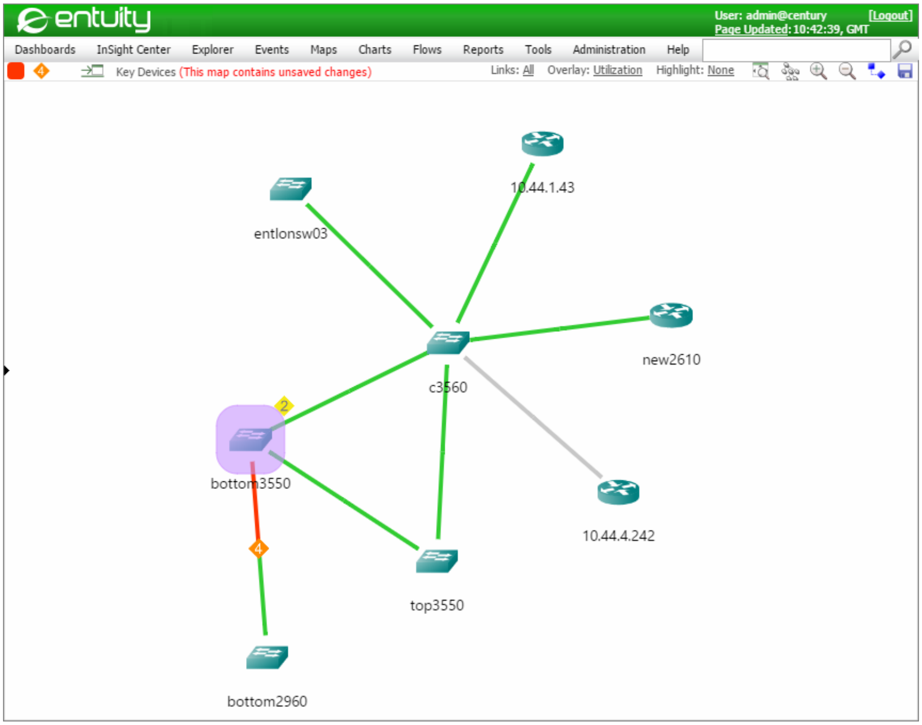
When zooming or panning within a map the camera position is now stored in the browser URL so that when using the back button or refreshing the page you are returned to the same camera position. These changes are not saved as part of the map definition.

## Map Layout Algorithms

When you create a view and first open the map Entuity lays out the objects on a grid. If you add a new device to the view Entuity displays the device in the next available space on the grid. There are two layout algorithms, Grid and Radial, and which is the most appropriate depends upon the number of objects in the view, and the structure their relationships form. When using the:

- Grid Layout Entuity lays out objects on the underlying grid, but they are slightly offset. This prevents the overlapping of long object names. The selectable grid layout is suitable for any data relationships, although most suitable for arranging a collection of isolated nodes or connected components.
- Radial Layout Entuity lays out the linked devices in a map according to a force directed layout algorithm. It calculates the layout of objects on the map around a central position stopping when the layout meets the set criteria. Select the option again and Entuity recalculates the layout starting from the new position, stopping again when it next meets the set criteria. In this way the map layout is updated. Devices that are not linked are placed at the foot of the map.

If you hold down the `SHIFT` key and click Radial Layout Entuity includes the devices not connected to other devices when calculating the layout.



User: admin@century [Logout]
Page Updated: 10:42:39, GMT

Key Devices (This map contains unsaved changes)

Links: All Overlay: Utilization Highlight: None

Figure 88 Map Radial Layout

## Adjusting the Layout

The default map layout or application of the two layout algorithms can provide a starting point from which you can improve the layout presentation by dragging objects. When you have adjusted the layout, and if you have the edit permission on the view, you can save the adjusted map. The adjusted layout will now be used by all users that open the map.

To move one object:

1) Click on it and hold down the mouse button.

2) Drag the object to its new position and release the mouse button.

To move a number of objects:

1) Hold down the `control` key and click on each object in turn.

2) While still holding down the `control` key drag the selection to its new position.

## Applying a Map Background

By default maps have a blank, white background. If you have the permission level to edit a map then you can also change its background image. The image must be in one of these file formats `PNG`, `GIF`, or `JPG`.

To add an image to a map background:

- You can drag and drop the required image onto the map from, for example, Windows Explorer.
- Click the map background and from a context menu set the image.

When users alter the zoom level of a map they also alter the zoom level of its background, ensuring the map objects maintain their position relative to their background image.

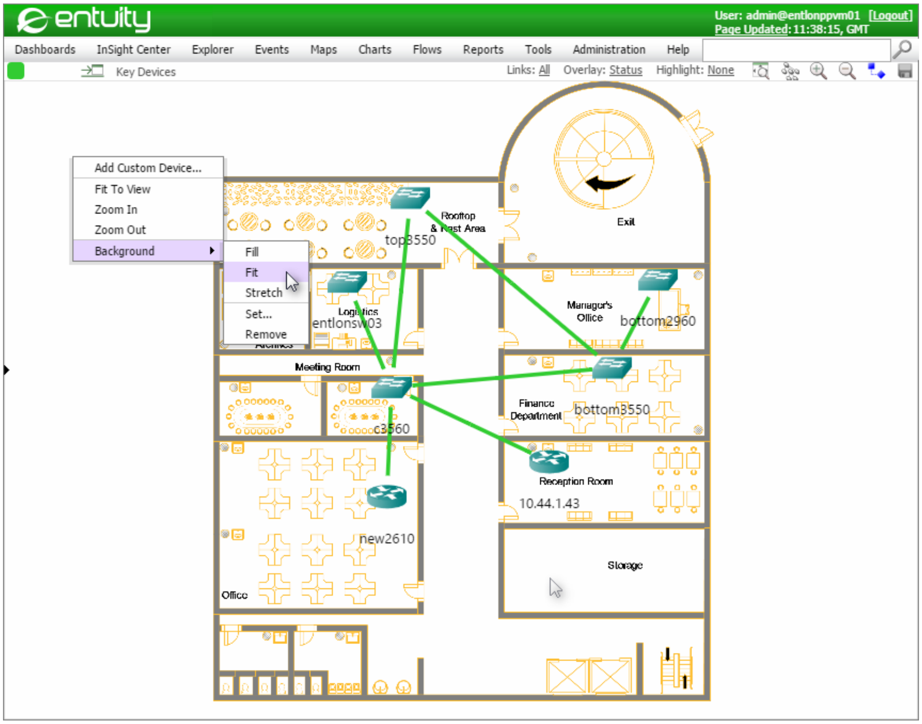


Figure 89 Set a Background Image

To amend the map background:

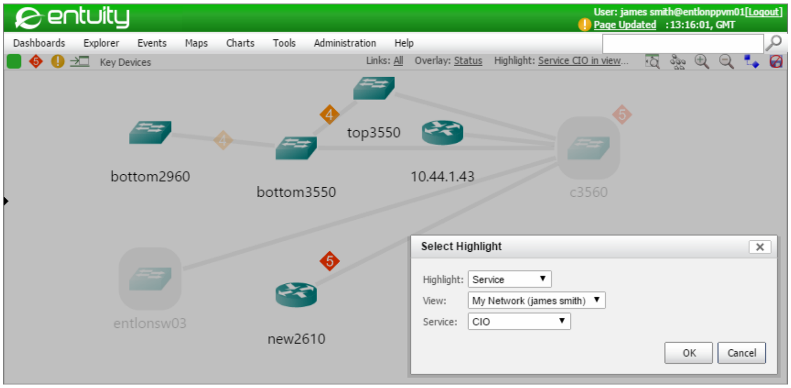
1) Click on the map background and from the context menu click **Background** and then the required background option.

| Action | Description |
|---|---|
| **Fill** | Entuity uses the image to completely fill the map background, although as the relative dimensions of the picture and map may differ the full image may not always be displayed. |
| **Fit** | Entuity displays the complete image in the map background although as the relative dimensions of the picture and map may differ on the vertical or horizontal edges of the background Entuity may display the default map background color. |
| **Remove** | Entuity removes the image from the map. If you want to replace an image you do not have to first remove the image, you can drag the new image to the map and it will replace the old image. |
| **Set** | Opens a Browse dialog through which you can load an image to the map background. |
| **Stretch** | Entuity stretches the image (adjust its aspect) to fit the map background. |

Table 19 Map Background Options

# Highlight a View, Service or Network Path

The Highlight mode allows for greater focus by graying out components that are outside of the selected service, view or network path and therefore emphasizing components within the selected view, service or path. You can save the highlight setup as part of the map definition.



Highlight: Service

View: My Network (james smith)

Service: CIO

Figure 90 Highlight Objects in Selected Service

| Highlight | Description |
|---|---|
| Network Path | This option is only available when you have a remote SurePath server. When selected Entuity lists views that contain network paths. When you select a view Entuity then displays the network paths available in the view.<br>When applied to the map Entuity highlights the devices that are in the network path and grays out devices not in the path. |
| Service | When selected Entuity lists views that contain services. When you select a view Entuity then displays the services available in the view.<br>When applied to the map Entuity highlights the devices that are in the service and grays out devices not in the service. |
| View | When selected Entuity lists all views from which you can choose the view to apply as a highlight.<br>When applied to the map Entuity highlights the devices that are in the view and grays out devices not in the view. |

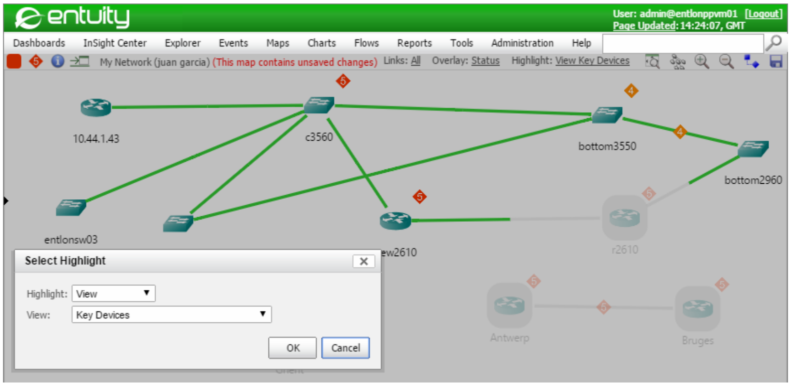
Table 20 Highlight Options

To highlight the objects within the current map that are in a particular view:

1) From the map click on the Highlight link.

2) From the dialog select **View** and then select the view from the list of available views.

3) Click **OK**. Entuity fades out the objects on the map that are not in the selected view.


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 14:24:07, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
My Network (juan garcia) (This map contains unsaved changes) Links: All Overlay: Status Highlight: View Key Devices
10.44.1.43
c3560
bottom3550
bottom2960
entlonsw03
ew2610
r2610
Antwerp
Bruges
Select Highlight
OK
Cancel

Highlight: View

View: Key Devices

Figure 91 Highlight Objects in a View

## Accessing More Information from Entuity

Each object in the map, device or link, has a status which, by default, is indicated by its status color. Maps are fully integrated with Entuity, you can access more detail on devices and links. From Maps you can access in context a:

- Device’s details, status and connectivity.
- Link’s details and status.

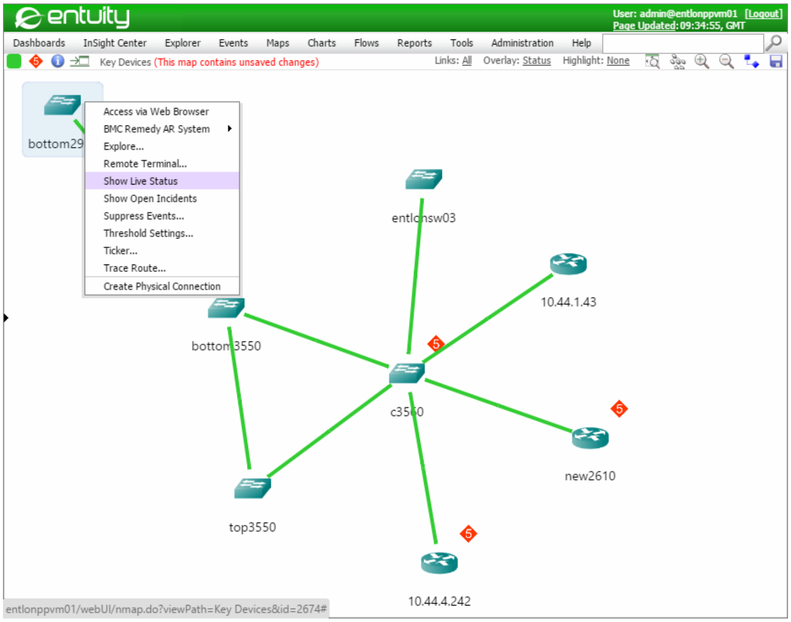
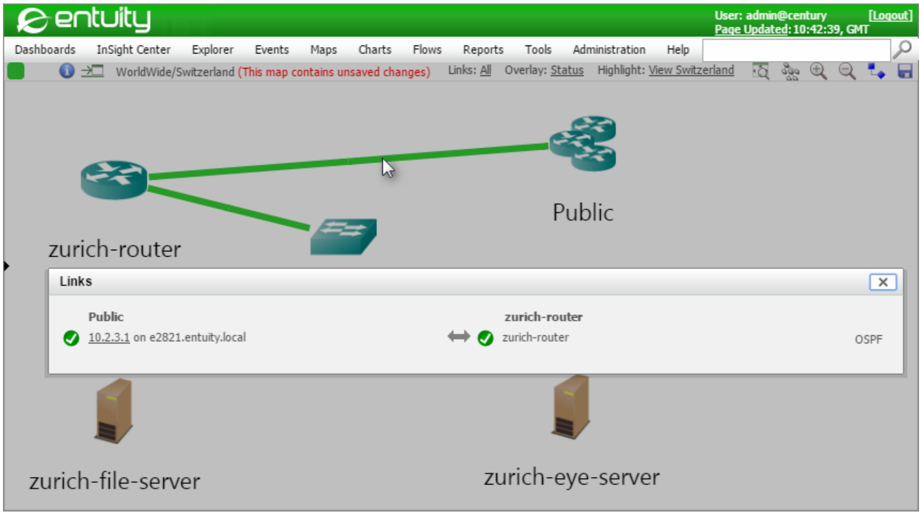

entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 09:34:55, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Key Devices (This map contains unsaved changes) Links: All Overlay: Status Highlight: None
bottom29
Access via Web Browser
BMC Remedy AR System
Explore...
Remote Terminal...
Show Live Status
Show Open Incidents
Suppress Events...
Threshold Settings...
Ticker...
Trace Route...
Create Physical Connection
entlonsw03
10.44.1.43
bottom3550
c3560
new2610
top3550
10.44.4.242
entlonppvm01/webUI/nmap.do?viewPath=Key Devices&id=2674#

Figure 92 Viewing Connectivity in Context

# Show Link Details

When you select a link on a map from the context menu you can select **Show Details.** Entuity displays the state of the link between the two devices. Where more than one link type exists between them each row in the dialog shows the state of each and also the direction of the connection. From each row you can click on the:

- State icon associated with the end of a link and open the Live Status dialog.
- Hyperlink for an object at the end of a link. Usually this would be a port and clicking on the link would display Port Summary page, but it might also be for example an OSPF peer, host connection.



| Public | | zurich-router | |
|---|---|---|---|
| ✓ 10.2.3.1 on e2821.entuity.local | ↔ | ✓ zurich-router | OSPF |

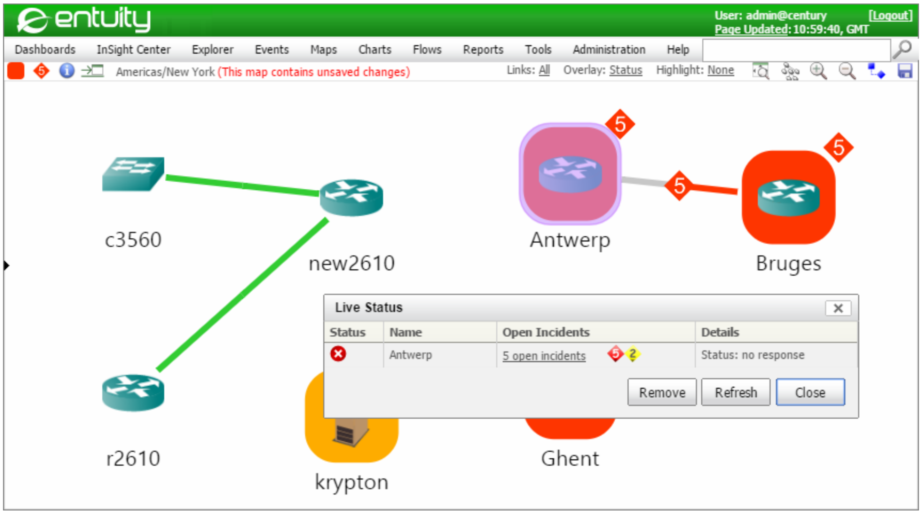
Figure 93 Map Link Details

# Managed Object Live Status

From the map you can monitor the Live Status of up to ten objects, which can be made up of any combination of devices and ports.

To view the live status of an object from a map:

1) Select the managed object and then from the context menu **Live Status**.



Live Status

| Status | Name | Open Incidents | Details |
|---|---|---|---|
| ✖ | Antwerp | 5 open incidents 5 2 | Status: no response |

Figure 94 Map Live Status

# Maps Devices and Links from Multiple Entuity Servers

When you have more than one Entuity server managing your network it is likely that you will want to see devices managed by those different servers on the same map. This is possible using the Consolidate Servers option, where views with the same name on different Entuity servers are consolidated. When this option is on, the maps are also consolidated.

Although devices managed by different Entuity servers can appear on the same map the connections between them are not automatically discovered. However you can define physical connections between devices and these connections can contain state information on the connection, and if you define the ports then also utilization data.

When setting up views on remote servers it is always important to ensure that you set up users with the appropriate access permissions. This can often mean that different users accessing the same consolidated view see different devices because they have different permissions on the remote servers. This may mean they also have conflicting map layout requirements. In this case it would be better to make a copy of the central server view and assign the original view to one user and the copy to the other.

This example uses a central consolidation server to develop a map that shows:

- Devices managed by different Entuity servers.
- Connections between devices that are managed by different Entuity servers.

To create a consolidated map with connections between devices managed by different Entuity servers:

1) Create views with the same name on each of the Entuity servers.

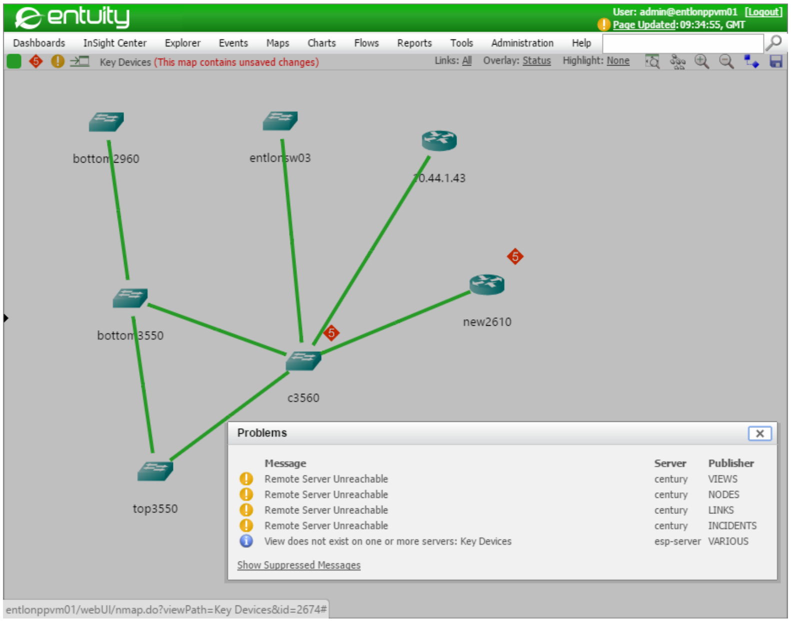
2) Ensure that you set up users to have appropriate permissions to those views on the central and remote servers.

3) From the central Entuity server set consolidate servers to on. This groups together the content of views with the same name across all connected servers.

4) Open the map.

   The central Entuity server controls the collecting of information on objects in the consolidated map from all servers. (See *Map Publishers*.)

5) A consolidated map with devices managed by different Entuity servers cannot automatically determine connections between those devices. However you can define physical connections between devices. These connection will have a status and are displayed on the map.



Problems

| | Message | Server | Publisher |
|---|---|---|---|
| ! | Remote Server Unreachable | century | VIEWS |
| ! | Remote Server Unreachable | century | NODES |
| ! | Remote Server Unreachable | century | LINKS |
| ! | Remote Server Unreachable | century | INCIDENTS |
| i | View does not exist on one or more servers: Key Devices | esp-server | VARIOUS |

Show Suppressed Messages

Figure 95 Multiple Entuity Servers

## Behavior of Maps With Multiple Entuity Servers

All map definitions are stored on the Entuity server and drawn on your client machine. When you are logged into a server that has one or more remote servers then where a map definition is stored depends upon the Consolidate servers mode. Consolidate servers mode is set to:

- **On**. When you select a view Entuity consolidates the content of all views with that name across all of the servers to which you currently have access. When you open the map it also includes all of those objects. When you save the map that definition is saved to the server to which you logged into.

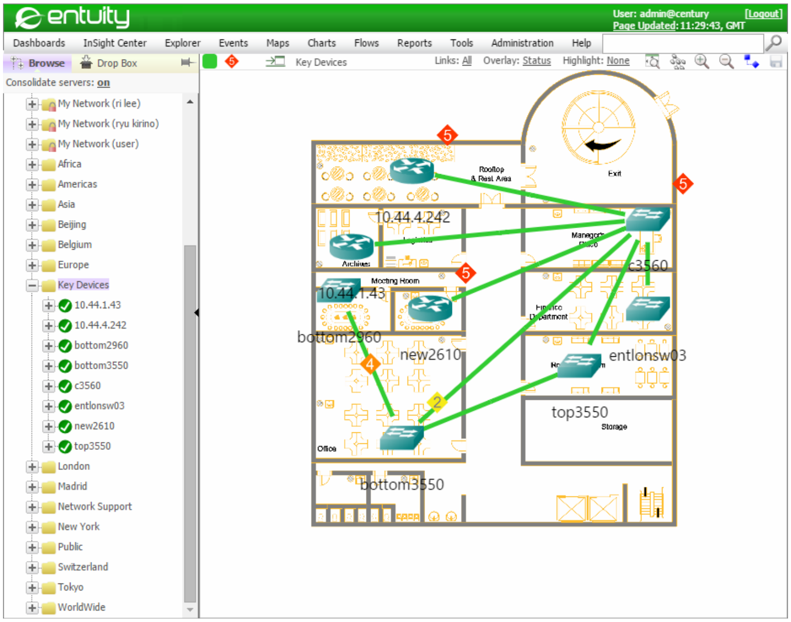


Figure 96 Consolidate Servers On

- **Off**. Entuity groups all views by their server. To select a view you first have to select a server. The content of the view is restricted to the objects on that server and the map contents are similarly restricted. When you save the map that definition is saved to the view's server.

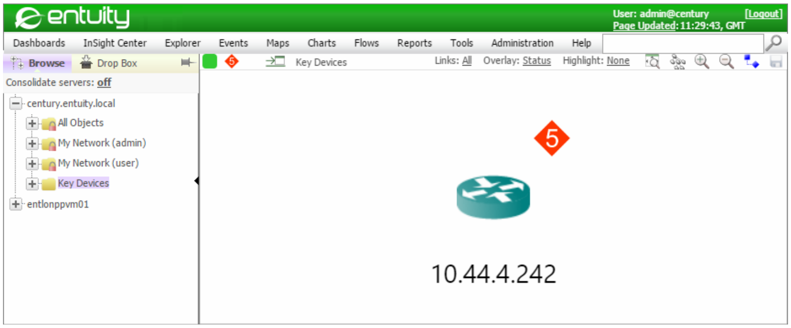


Figure 97 Consolidate Servers Off

There are therefore two map definitions and which one is saved is dependent upon whether you are using the server consolidated or unconsolidated mode. If you alternate between consolidated and unconsolidated modes then you are also alternating between map definitions, even if the selected view only exists on the server to which you are logged into.

The same consolidated map definition can at different times display different objects, for example:

- If the remote server is unavailable when you open a map Entuity cannot display those objects in the map. However if the remote server becomes available while you have the map open it will update the map with the missing objects.
- Different users have different permissions. For example two users may be able to log into the same central server and use the same view but their permissions to remote servers may be very different. In both cases Entuity would only display the network objects that they have permission to view.
- A user may alter their Servers and Views user preferences. For example if they decide not to show a particular remote server then views and objects from that server are no longer available to the map.

## Saving Maps

All map definition files are stored on the Entuity server and drawn on your web browser. The map definition that determines the position of objects on the map is only updated when users adjust the map layout and then save it. Only at this point are the layout co-ordinates for a deleted object removed or for a new object added.

Changes to the map that can be saved as part of the map definition are:

- Changes to the positional co-ordinates of nodes on the map. Co-ordinate change can be caused by repositioning nodes on the map, adding nodes to the map and removing nodes from the map.
- Changes to the map overlay.
- Changes to the active link types.
- Changes to the background image of the map.

Zooming or panning within a map is not saved to the map definition. The camera position is now stored in the browser URL so that when using the back button or refreshing the page you are returned to the same camera position.

When you make a savable change, and have the permission to save the map to one or more of these settings, Entuity displays an informational message in red informing you that the map contains unsaved changes. On leaving the map Entuity by default (see *Save Maps User Preference*) prompts you to save the map definition if you are:

- An administrator.
- The owner of the view.
- A member of a user group that has the Edit permission for the view you are amending.
- A member of a user group that has the Create View permission if the view and therefore map are new.

If you do not have the permission to save map layout changes you can still adjust the map but you cannot save those adjustments. If another user updates the map Entuity prompts you to reload the map to get the new layout but you also have the option to ignore the reload prompt.

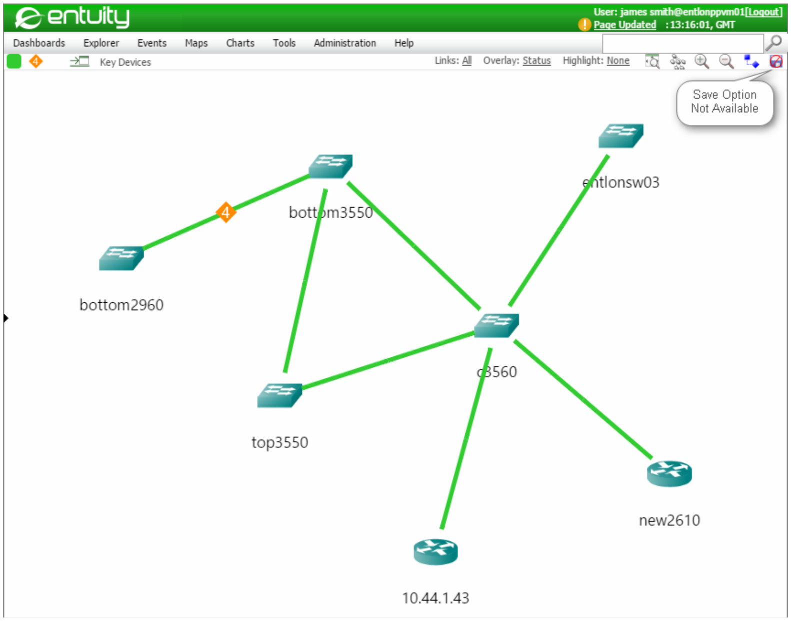


Figure 98 Save Map Option Not Available

When you edit and save a map Entuity checks if other users have updated the map since you last loaded it and if:

- There are no other changes Entuity prompts you to save your changes.
- There are changes Entuity prompts you to overwrite the map with your changes.

In both cases Entuity also allows you to cancel the save operation.

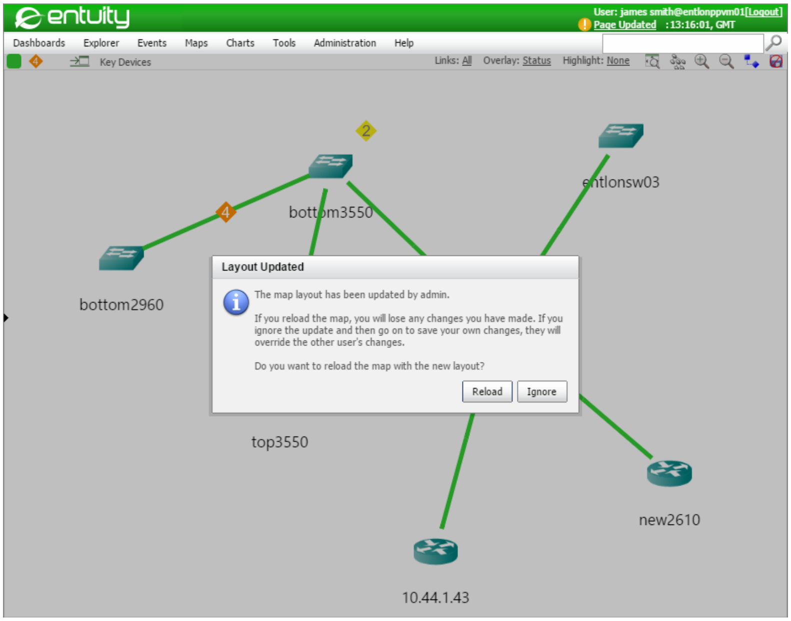
When you save the map other users that have the map open and have:

- Not made changes that could be saved to the map definition have their map automatically refreshed with the latest changes.
- Made changes that could be saved to the map definition are prompted to update their map with the latest changes. This is true regardless of whether the user has the permission to save their changes or not. The prompt includes details of who last saved the map definition.

  If the user does not update their map then their map is only retained for their current Entuity session or until they open another map. If the user has the appropriate permissions on the view they can save their current map and therefore overwrite the changes of the other user.

  When users have a conflict in how they are laying out a map, resulting in frequent overwrites of a map definition then users should consider duplicating the view. Although the views have the same content users can differently lay out the associated maps.

Entuity maps does not include an auto-save option. This prevents Entuity saving maps that you are not ready to save and in multi user environments prevents users with the same open map continually overwriting each other’s changes.



Layout Updated

The map layout has been updated by admin.

If you reload the map, you will lose any changes you have made. If you ignore the update and then go on to save your own changes, they will override the other user's changes.

Do you want to reload the map with the new layout?

Figure 99 Prompt to Reload a Map

### Save Maps User Preference

By default if you adjust a map with a change that can be saved and have the permission to do so Entuity prompts you to save the map when you navigate away from it. Through the User Preference Maps tab you can amend this user preference through the check box:

```
Show a warning message if there are unsaved changes, when navigating
away from the map
```

This option is checked by default. If it is unchecked when you navigate away from the map Entuity silently discards any changes you have made.

## Adding Maps to Custom Dashboards

You can add maps to custom dashboards. Entuity can support multiple maps being open at the same time, so one dashboard can have multiple maps.

Maps in dashboards have a restricted edit capability. You can amend the presentation of the map but the changes are only maintained for the current browser session and cannot be saved.

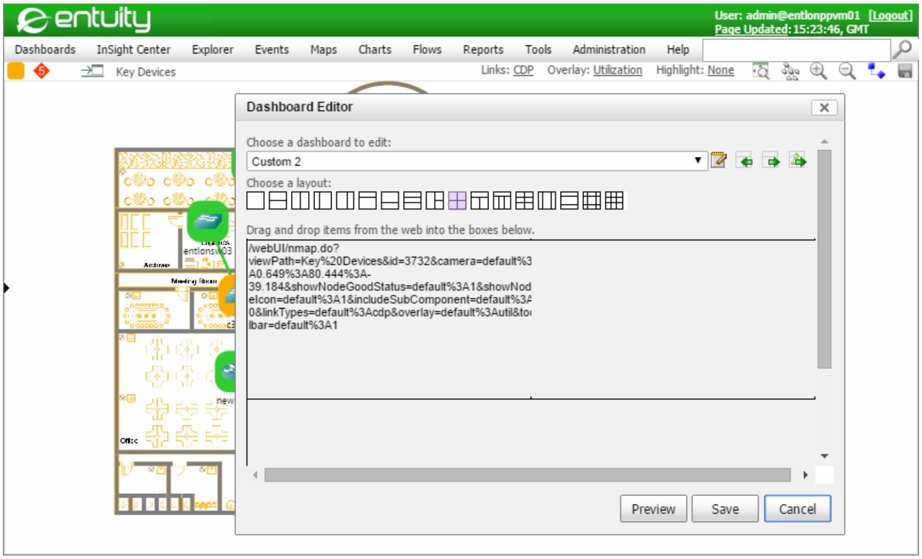
To create a dashboard and add a map to it:

1) From the map you want to add to the new dashboard click **Dashboards** > **Custom Dashboards** > **Edit**.

2) Select the dashboard layout to which you want to add the map.

3) From the map toolbar drag the map URL icon ⇥ to a pane of the custom dashboard. When you release the icon Entuity copies the map URL to the dashboard pane.

   Alternatively if you click on this icon Entuity opens the current map in a new window, from which you would be able to view and copy the map URL.



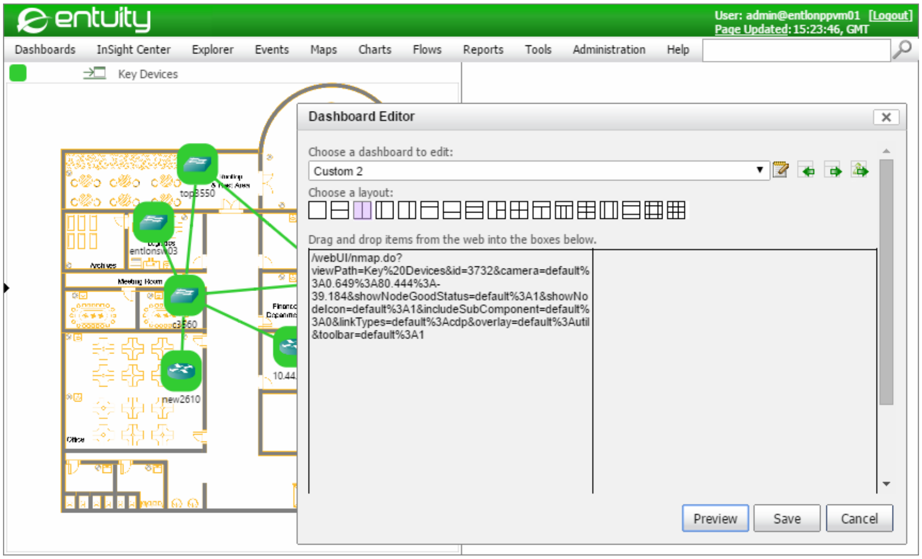
Choose a dashboard to edit: Custom 2

Choose a layout:

```
/webUI/nmap.do?
viewPath=Key%20Devices&id=3732&camera=default%3
A0.649%3A80.444%3A-
39.184&showNodeGoodStatus=default%3A1&showNod
eIcon=default%3A1&includeSubComponent=default%3A
0&linkTypes=default%3Acdp&overlay=default%3Autil&too
lbar=default%3A1
```

Figure 100 Add a Map to a Custom Dashboard

4) You can now preview, save or cancel the changes to the custom dashboard. You can also amend the URL or dashboard layout.



Choose a dashboard to edit:

Custom 2

Choose a layout:

Drag and drop items from the web into the boxes below.

```
/webUI/nmap.do?
viewPath=Key%20Devices&id=3732&camera=default%
3A0.649%3A80.444%3A-
39.184&showNodeGoodStatus=default%3A1&showNo
deIcon=default%3A1&includeSubComponent=default%
3A0&linkTypes=default%3Acdp&overlay=default%3Autil
&toolbar=default%3A1
```

Figure 101 Preview a Map in a Custom Dashboard

## Exporting Maps to Visio

Integration with Visio 2003, Visio 2007, Visio 2010 and Visio 2013 is through the vdx XML drawing file format. The layout of the network in the export file is the same as that in the currently displayed Entuity map. The exported map uses a predetermined set of network icons. Once created the vdx file can be imported to Visio.

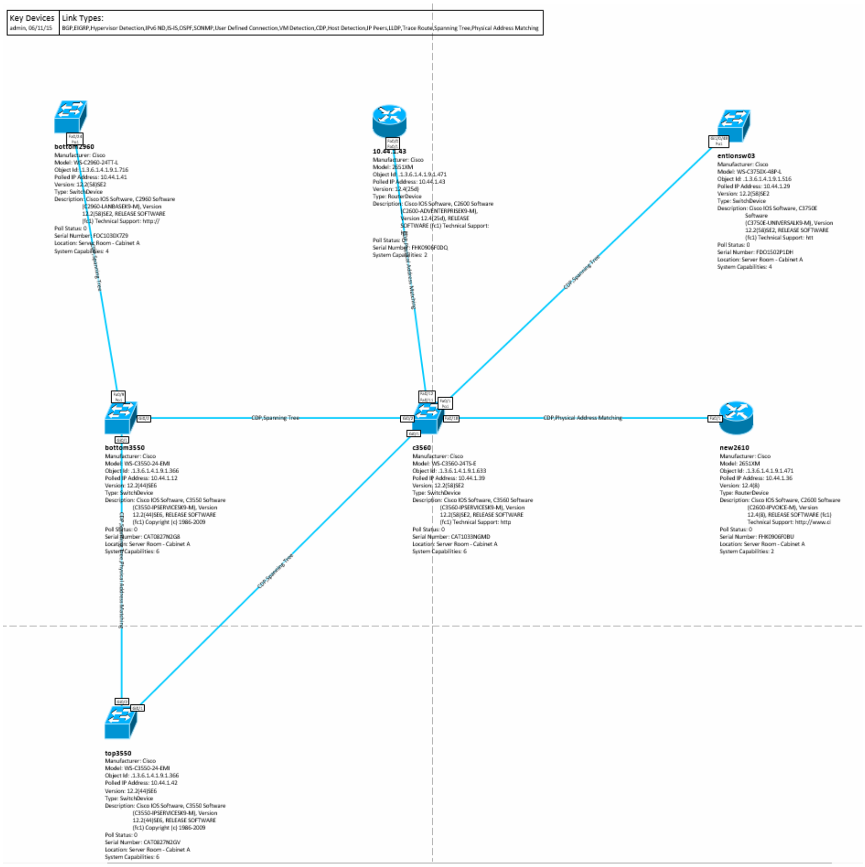
To export to the Visio VDX format:

1) Use Entuity to display the required map.

2) Layout the map.

3) Click the Visio Export icon on the toolbar.

Entuity uses the map name to generate a name for the vdx file. It exports the file to the download folder of your browser.



Key Devices
admin, 06/11/15
Link Types:
BGP,EIGRP,Hypervisor Detection,IPv6 ND,IS-IS,OSPF,SONMP,User Defined Connection,VM Detection,CDP,Host Detection,IP Peers,LLDP,Trace Route,Spanning Tree,Physical Address Matching
CDP,Spanning Tree
CDP,Physical Address Matching
CDP,Spanning Tree
CDP,Spanning Tree
CDP,Spanning Tree
CDP,Spanning Tree,Physical Address Matching
Fa0/24
Po1
Fa0/0
Fa0/1
Gi1/0/48
Po1
Fa0/9
Po1
Gi0/2
Gi0/1
Fa0/12
Fa0/11
Fa0/1
Po1
Gi0/2
Fa0/18
Gi0/1
Fa0/1
Gi0/2
Gi0/1

**bottom2960**
Manufacturer: Cisco
Model: WS-C2960-24TT-L
Object Id: .1.3.6.1.4.1.9.1.716
Polled IP Address: 10.44.1.41
Version: 12.2(58)SE2
Type: SwitchDevice
Description: Cisco IOS Software, C2960 Software
(C2960-LANBASEK9-M), Version
12.2(58)SE2, RELEASE SOFTWARE
(fc1) Technical Support: http://
Poll Status: 0
Serial Number: FOC1030X729
Location: Server Room - Cabinet A
System Capabilities: 4

**10.44.1.43**
Manufacturer: Cisco
Model: 2651XM
Object Id: .1.3.6.1.4.1.9.1.471
Polled IP Address: 10.44.1.43
Version: 12.4(25d)
Type: RouterDevice
Description: Cisco IOS Software, C2600 Software
(C2600-ADVENTERPRISEK9-M),
Version 12.4(25d), RELEASE
SOFTWARE (fc1) Technical Support:
htt
Poll Status: 0
Serial Number: FHK0906F0DQ
System Capabilities: 2

**entionsw03**
Manufacturer: Cisco
Model: WS-C3750X-48P-L
Object Id: .1.3.6.1.4.1.9.1.516
Polled IP Address: 10.44.1.29
Version: 12.2(58)SE2
Type: SwitchDevice
Description: Cisco IOS Software, C3750E
Software
(C3750E-UNIVERSALK9-M), Version
12.2(58)SE2, RELEASE SOFTWARE
(fc1) Technical Support: htt
Poll Status: 0
Serial Number: FDO1502P1DH
Location: Server Room - Cabinet A
System Capabilities: 4

**bottom3550**
Manufacturer: Cisco
Model: WS-C3550-24-EMI
Object Id: .1.3.6.1.4.1.9.1.366
Polled IP Address: 10.44.1.12
Version: 12.2(44)SE6
Type: SwitchDevice
Description: Cisco IOS Software, C3550 Software
(C3550-IPSERVICESK9-M), Version
12.2(44)SE6, RELEASE SOFTWARE
(fc1) Copyright (c) 1986-2009
Poll Status: 0
Serial Number: CAT0827N2G8
Location: Server Room - Cabinet A
System Capabilities: 6

**c3560**
Manufacturer: Cisco
Model: WS-C3560-24TS-E
Object Id: .1.3.6.1.4.1.9.1.633
Polled IP Address: 10.44.1.39
Version: 12.2(58)SE2
Type: SwitchDevice
Description: Cisco IOS Software, C3560 Software
(C3560-IPSERVICESK9-M), Version
12.2(58)SE2, RELEASE SOFTWARE
(fc1) Technical Support: http
Poll Status: 0
Serial Number: CAT1033NGMD
Location: Server Room - Cabinet A
System Capabilities: 6

**new2610**
Manufacturer: Cisco
Model: 2651XM
Object Id: .1.3.6.1.4.1.9.1.471
Polled IP Address: 10.44.1.36
Version: 12.4(8)
Type: RouterDevice
Description: Cisco IOS Software, C2600 Software
(C2600-IPVOICE-M), Version
12.4(8), RELEASE SOFTWARE (fc1)
Technical Support: http://www.ci
Poll Status: 0
Serial Number: FHK0906F0BU
Location: Server Room - Cabinet A
System Capabilities: 2

**top3550**
Manufacturer: Cisco
Model: WS-C3550-24-EMI
Object Id: .1.3.6.1.4.1.9.1.366
Polled IP Address: 10.44.1.42
Version: 12.2(44)SE6
Type: SwitchDevice
Description: Cisco IOS Software, C3550 Software
(C3550-IPSERVICESK9-M), Version
12.2(44)SE6, RELEASE SOFTWARE
(fc1) Copyright (c) 1986-2009
Poll Status: 0
Serial Number: CAT0827N2GV
Location: Server Room - Cabinet A
System Capabilities: 6

Figure 102 Map Exported to Visio

# 9 Manage the Virtual Environment

Entuity currently manages Oracle VM, Microsoft Hyper-V and VMware ESXi VM platforms, and their hypervisors, virtual machines and virtual switches. Entuity fully integrates these virtual components into its core toolset, for example:

- Hypervisors and virtual machines are represented in Entuity maps, integrated into the network through the link technologies VM Detection and Hypervisor Detection.
- Virtualization Perspective provides a suite of reports allowing for management and control of the impact of virtual components on the physical network.
- Web UI allows you to navigate between VM platforms, hypervisors, VMs and virtual switches using drilldown and presentational techniques used with other related components, e.g. between devices and ports.

## Entuity Virtualization Data

Entuity uses these device types to manage virtualization data:

- VM Platforms identify the hardware server on which hypervisors operate.
- Hypervisors hold information on the hypervisors.
- Virtual Machine identifies a virtual machine.
- vSwitch access to the virtual network. Entuity currently supports virtual switches for VMware ESXi VM platforms.

Entuity maintains the relationships between managed object types allowing you to drilldown, or up, when managing your virtual network.

You can also manage the virtual machine server as a managed host, and Entuity maintains the relationship between the host and the VM.

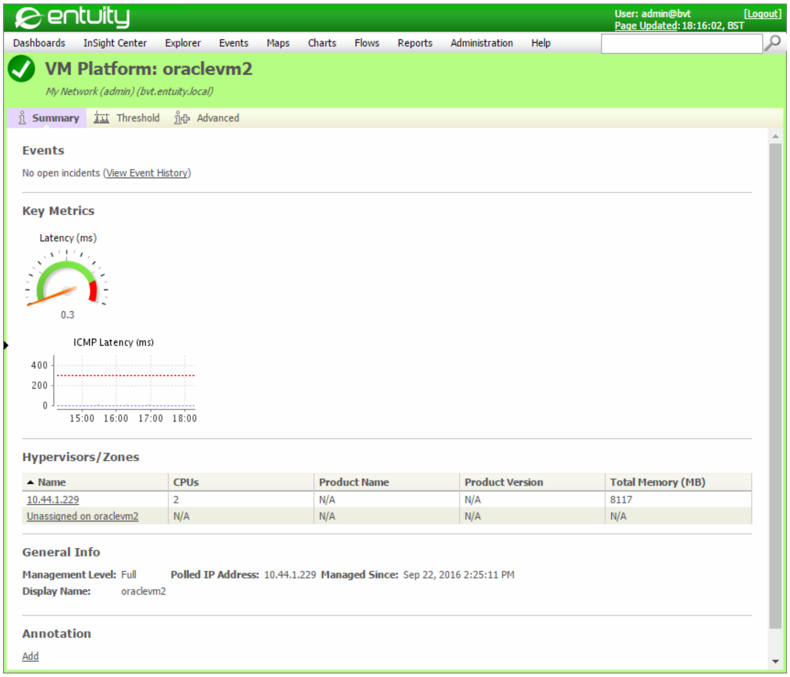
### Performing a Virtual Environment Drilldown

This example drills down from a VM Platform, to its hypervisor and then a virtual machine and finally a managed host.

To drilldown from a VM platform to a managed host:

1) Use Explorer to find the VM platform. From the Summary page you can see a summary of the platform’s events, key metrics, general information and its associated hypervisors and virtual switches.

   On Oracle VM platforms, when VMs are down Entuity categorizes them for reporting purposes as an unassigned hypervisors.



VM Platform: oraclevm2

*My Network (admin) (bvt.entuity.local)*

Events

No open incidents (View Event History)

Key Metrics

Hypervisors/Zones

| ▲ Name | CPUs | Product Name | Product Version | Total Memory (MB) |
|---|---|---|---|---|
| 10.44.1.229 | 2 | N/A | N/A | 8117 |
| Unassigned on oraclevm2 | N/A | N/A | N/A | N/A |

General Info

**Management Level:** Full **Polled IP Address:** 10.44.1.229 **Managed Since:** Sep 22, 2016 2:25:11 PM
**Display Name:** oraclevm2

Annotation

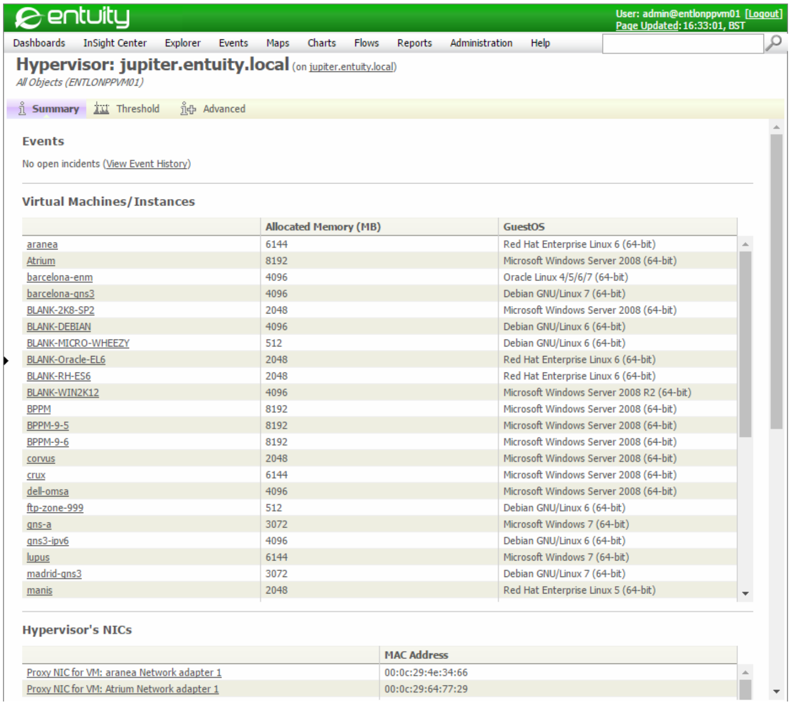
Add

Figure 103 Oracle VM Platform Summary

2) From the hypervisors section click on a hypervisor link.

Entuity displays the Hypervisor summary page:

- Alongside the title of the page is a link back to its VM Platform
- Virtual Machines section identifies each VM on the hypervisor. Each attribute, *Name*, *Allocated Memory*, *Guest O/S*, is also a link to the VM Summary page.
- Hypervisors NICs section, lists the MAC address and NIC for each VM. Entuity uses proxy NICs to as a label to identify the MAC address of the VM.



Hypervisor: jupiter.entuity.local (on jupiter.entuity.local)

*All Objects (ENTLONPPVM01)*

Events

No open incidents (View Event History)

Virtual Machines/Instances

| | Allocated Memory (MB) | GuestOS |
|---|---|---|
| aranea | 6144 | Red Hat Enterprise Linux 6 (64-bit) |
| Atrium | 8192 | Microsoft Windows Server 2008 (64-bit) |
| barcelona-enm | 4096 | Oracle Linux 4/5/6/7 (64-bit) |
| barcelona-gns3 | 4096 | Debian GNU/Linux 7 (64-bit) |
| BLANK-2K8-SP2 | 2048 | Microsoft Windows Server 2008 (64-bit) |
| BLANK-DEBIAN | 4096 | Debian GNU/Linux 6 (64-bit) |
| BLANK-MICRO-WHEEZY | 512 | Debian GNU/Linux 6 (64-bit) |
| BLANK-Oracle-EL6 | 2048 | Red Hat Enterprise Linux 6 (64-bit) |
| BLANK-RH-ES6 | 2048 | Red Hat Enterprise Linux 6 (64-bit) |
| BLANK-WIN2K12 | 4096 | Microsoft Windows Server 2008 R2 (64-bit) |
| BPPM | 8192 | Microsoft Windows Server 2008 (64-bit) |
| BPPM-9-5 | 8192 | Microsoft Windows Server 2008 (64-bit) |
| BPPM-9-6 | 8192 | Microsoft Windows Server 2008 (64-bit) |
| corvus | 2048 | Microsoft Windows Server 2008 (64-bit) |
| crux | 6144 | Microsoft Windows Server 2008 (64-bit) |
| dell-omsa | 4096 | Microsoft Windows Server 2008 (64-bit) |
| ftp-zone-999 | 512 | Debian GNU/Linux 6 (64-bit) |
| gns-a | 3072 | Microsoft Windows 7 (64-bit) |
| gns3-ipv6 | 4096 | Debian GNU/Linux 6 (64-bit) |
| lupus | 6144 | Microsoft Windows 7 (64-bit) |
| madrid-gns3 | 3072 | Debian GNU/Linux 7 (64-bit) |
| manis | 2048 | Red Hat Enterprise Linux 5 (64-bit) |

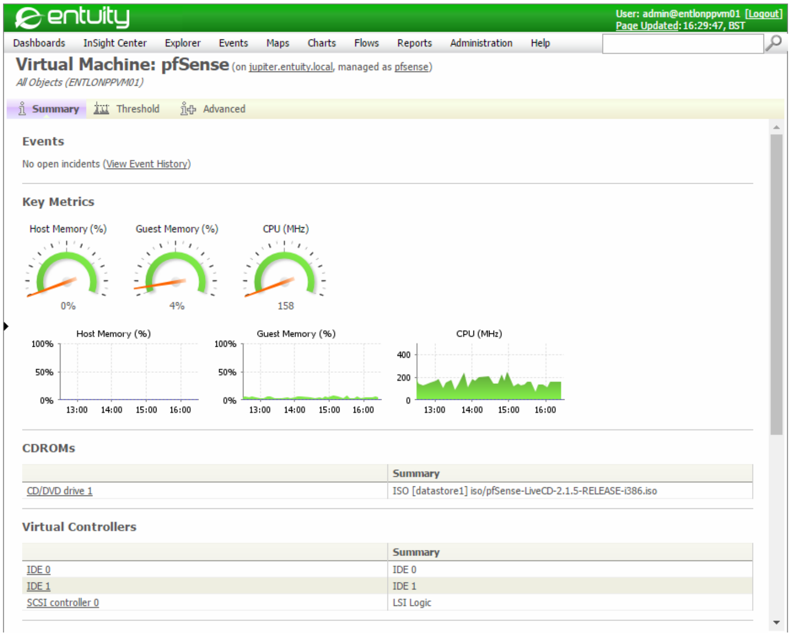
Hypervisor's NICs

| | MAC Address |
|---|---|
| Proxy NIC for VM: aranea Network adapter 1 | 00:0c:29:4e:34:66 |
| Proxy NIC for VM: Atrium Network adapter 1 | 00:0c:29:64:77:29 |

Figure 104 Hypervisor Summary

3) From the Virtual Machine section click on a VM Name.

Entuity displays the Virtual Machine summary page.



Virtual Machine: pfSense (on jupiter.entuity.local, managed as pfsense)

*All Objects (ENTLONPPVM01)*

Events

No open incidents (View Event History)

Key Metrics

CDROMs

| | Summary |
|---|---|
| CD/DVD drive 1 | ISO [datastore1] iso/pfSense-LiveCD-2.1.5-RELEASE-i386.iso |

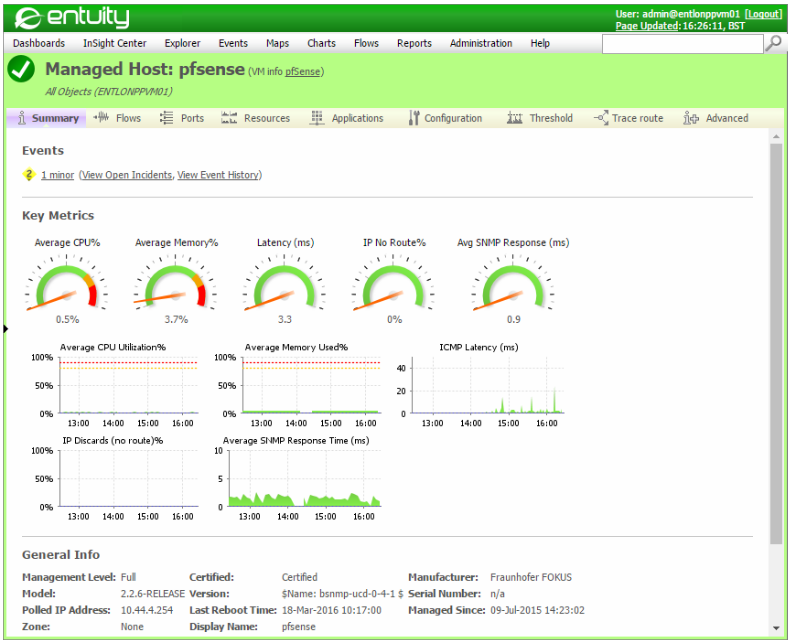
Virtual Controllers

| | Summary |
|---|---|
| IDE 0 | IDE 0 |
| IDE 1 | IDE 1 |
| SCSI controller 0 | LSI Logic |

Figure 105 Virtual Machine Summary

4) From alongside the Virtual Machine title click on the link to the managed host.

Entuity displays the Managed Host Summary page. Alongside the title of the page is a link back to its VM.



**Managed Host: pfsense** (VM info pfSense)

*All Objects (ENTLONPPVM01)*

**Events**

2 1 minor (View Open Incidents, View Event History)

**Key Metrics**

**General Info**

| | | | | | |
|---|---|---|---|---|---|
| **Management Level:** | Full | **Certified:** | Certified | **Manufacturer:** | Fraunhofer FOKUS |
| **Model:** | 2.2.6-RELEASE | **Version:** | $Name: bsnmp-ucd-0-4-1 $ | **Serial Number:** | n/a |
| **Polled IP Address:** | 10.44.4.254 | **Last Reboot Time:** | 18-Mar-2016 10:17:00 | **Managed Since:** | 09-Jul-2015 14:23:02 |
| **Zone:** | None | **Display Name:** | pfsense | | |

Figure 106 Managed Host VM Summary

## Monitoring VMware Status and Performance

Entuity collects status and performance data for VMs and hypervisors running on the VMware vCenter platform. Entuity collects data at a five minute polling frequency. This data is available through gauges and mini-charts on the Explorer Summary page for each VM and Hypervisor NICs.

Entuity includes event and incidents which alarm on:

- VMs moving, power down and powering up.
- VM high memory utilization.

| VM' Attributes | Description |
|---|---|
| *VM CPU (MHz)* | The amount of CPU used, in megahertz, during the interval. Amount of actively used virtual CPU. This is the host's view of the CPU usage, not the guest operating system view. |
| *Guest memory usage (MB)* | Guest physical memory refers to the virtual hardware memory presented to a virtual machine for its guest operating system. |
| *Host memory usage (MB)* | Machine memory is the random-access memory (RAM) that’s actually installed in the hardware that comprises the ESX server system. |
| *Power status* | Power state of the virtual machine. poweredOn or poweredOff. |

Table 9-1 VM Attributes

| NIC Attribute | Description |
|---|---|
| *Packets Tx* | Number of outbound packets transmitted by the hypervisor. |
| *Packets Rx* | Number of inbound packets received by the hypervisor. |
| *Bytes RX* | Number of inbound bytes received by the hypervisor. |
| *Bytes TX* | Number of outbound packets transmitted by the hypervisor. |

Table 9-2 Hypervisor NIC Performance Attributes

## Mapping Virtual Relationships

To map the network's virtual environment you can create a view which includes a VM managed as a managed host, a vSwitch managed as a device or a physical switch and their linked devices. For example the following map includes both physical and virtual network components:

- VM that Entuity manages as a managed host (10.44.1.220).
- vSwitch also managed as an SNMP polled device (10.44.1.98).

  A vSwitch is a type of VM, and is represented in the map with the virtual machine fully managed icon.
- VM platform (blade), which would only be linked in a map to its hypervisor (blade.entuity.local) if you added the connecting line.

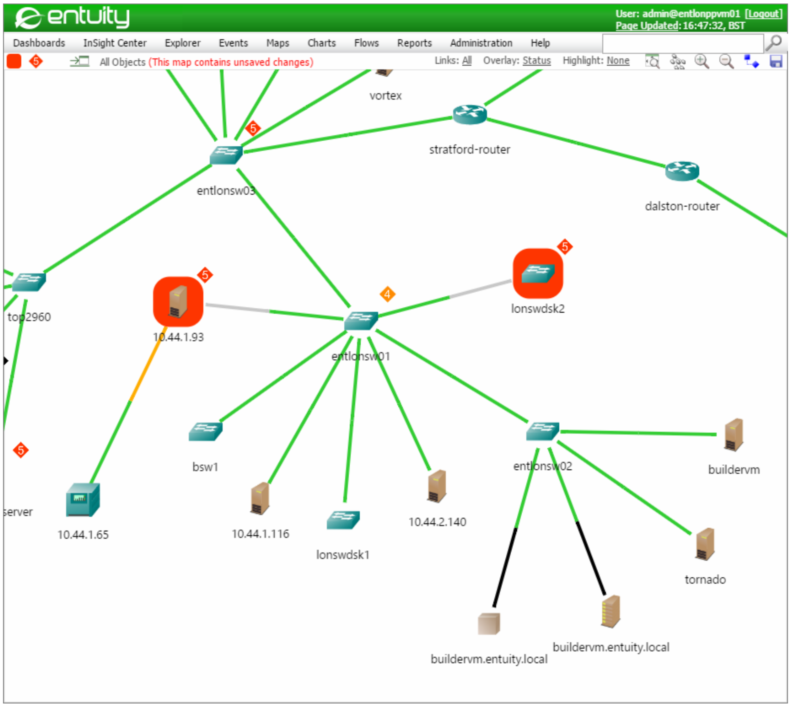
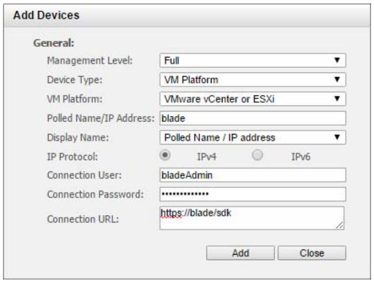


Figure 107 Physical and Virtual Network Components

## How Entuity Manages VM Platforms

Entuity manages virtual machines and hypervisors through their VM platform, The connection to the VM platform is through its SDK. Entuity can discover these devices using `autoDiscovery`, however to take them under full management you must amend their discovered attributes and enter connection details. (See the *Entuity Getting Started Guide*.)

Through the VM Platform device type Entuity currently manages Oracle VM, Microsoft Hyper-V and VMware ESXi VM Platforms.



Add Devices

General:

| | |
|---|---|
| Management Level: | Full |
| Device Type: | VM Platform |
| VM Platform: | VMware vCenter or ESXi |
| Polled Name/IP Address: | blade |
| Display Name: | Polled Name / IP address |
| IP Protocol: | ● IPv4 ○ IPv6 |
| Connection User: | bladeAdmin |
| Connection Password: | ••••••••••••• |
| Connection URL: | https://blade/sdk |

Figure 108 VM Platform Connection Attributes

After discovering VM platforms, Entuity can discover their hypervisors and virtual machines. To allow this discovery you must ensure Entuity can communicate with the platform. For example, with Microsoft Hyper-V configure its firewall to allow remote Windows Management Instrumentation (WMI) from the Entuity server.

## Managing VMware Virtual Switches

A virtual switch is the logical switching capability built into your VM platform which allows you to network your VMs in the configuration you require. Entuity currently supports virtual switches for VMware ESXi VM platforms.

Entuity has a generic virtual switch type which supports the three types of VMware vSwitch:

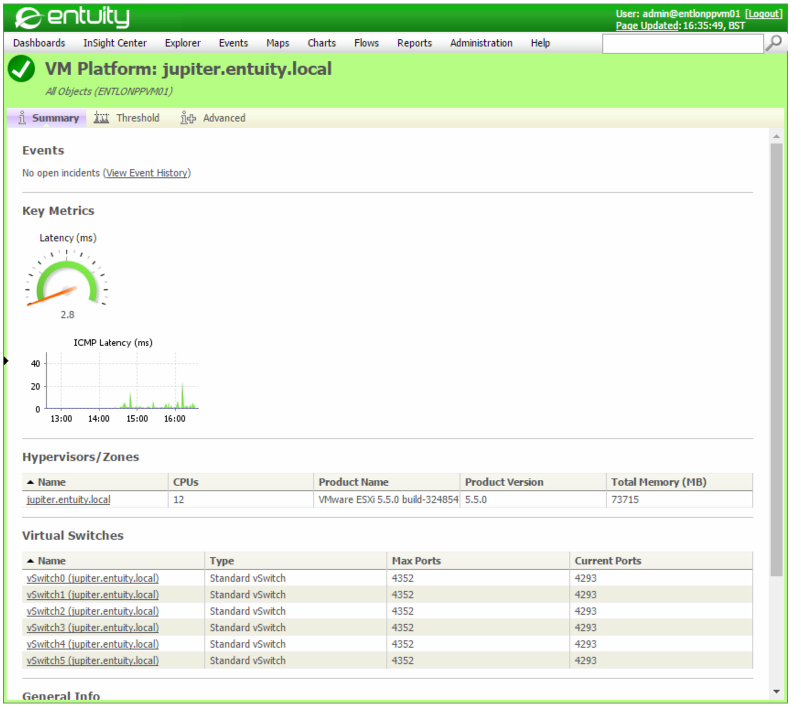
- VMware standard vSwitch, usually deployed for standalone VMware hypervisors
- VMware distributed vSwitch, a distributed vSwitch provided by VMware which, for example allows multiple hypervisors to connect to a shared distributed switch and supports vMotion, DRS
- Cisco Nexus 1000v, provides the same functionality as the VMware distributed vSwitch, but with greatly enhanced configuration options and performance operations, in effect the same functionality as a physical Nexus switch.

A virtual switch is a logical entity which comprises virtual port groups, both standard and distributed. Virtual port groups contain virtual ports, and for example their VLAN assignments, port profiles.

Virtual switch ports can connect to:

- Internal management ports (vmk ports), which can be used for hypervisor to VMware vCenter access, direct management access, dedicated vMotion links, high availability
- Uplinks which are the real physical NICs on the various hypervisors belonging to the vSwitch
- VM VNICs, these ports are connected to specific VM's virtual NICs.

  VM's can have multiple VNICs connected to different virtual switches and/or virtual switch virtual port groups (VPGs). VPGs contain virtual ports (and VLAN assignments, port profiles) and typically serve dedicated classes of traffic, e.g. application traffic, administration, vMotion traffic.



VM Platform: jupiter.entuity.local

All Objects (ENTLONPPVM01)

Events

No open incidents (View Event History)

Key Metrics

Hypervisors/Zones

| ▲ Name | CPUs | Product Name | Product Version | Total Memory (MB) |
|---|---|---|---|---|
| jupiter.entuity.local | 12 | VMware ESXi 5.5.0 build-324854 | 5.5.0 | 73715 |

Virtual Switches

| ▲ Name | Type | Max Ports | Current Ports |
|---|---|---|---|
| vSwitch0 (jupiter.entuity.local) | Standard vSwitch | 4352 | 4293 |
| vSwitch1 (jupiter.entuity.local) | Standard vSwitch | 4352 | 4293 |
| vSwitch2 (jupiter.entuity.local) | Standard vSwitch | 4352 | 4293 |
| vSwitch3 (jupiter.entuity.local) | Standard vSwitch | 4352 | 4293 |
| vSwitch4 (jupiter.entuity.local) | Standard vSwitch | 4352 | 4293 |
| vSwitch5 (jupiter.entuity.local) | Standard vSwitch | 4352 | 4293 |

General Info

Figure 109 VM Platform with vSwitches

## Finding the Physical NIC to Physical Switch Port Connection

Entuity locates the physical NIC to physical switch port connection through CDP (the VMware XML-API offers data received by its CDP listeners on each hypervisor PNIC). When the hypervisors are connected to non-Cisco switches, or CDP is blocked, or Entuity is not managing the access switch, then these connections are not displayed.

The association here allows for easy drill down from the vSwitch uplink port to the connecting access port (to allow ready access to port level statistics).

Entuity determines the location and display of hypervisors on the map using MAC location.

## Managing Cisco Nexus 1000V vSwitches

Entuity supports two methods for managing Cisco Nexus 1000V vSwitches:

- As an extension of VMware hypervisor support.
- As a separately managed device:
  - Managed as though it were a physical Cisco Nexus Switch.
  - Port level traffic volume monitoring.
  - Configuration upload, change alerting, policy violation.

- Traffic analysis using Integrated Flow Analyzer (IFA) down to the individual port.

vSwitches are not automatically discovered and SNMP polled as switch devices, you must specifically add a vSwitch as a device, for example through the Add Devices dialog accessed through **Administration** > **Inventory** / **Topology** > **Inventory** and then **Add**.

You can use both methods to manage a device and Entuity links the resultant data, from the:

- SNMP polled switch device Summary page there is a link from the virtual switch section
- vSwitch Summary page there is a link from the SNMP polled switch section.

Entuity XML Data Collection includes an implementation for collecting data from Nexus devices.

Device Access for XML Data Collection

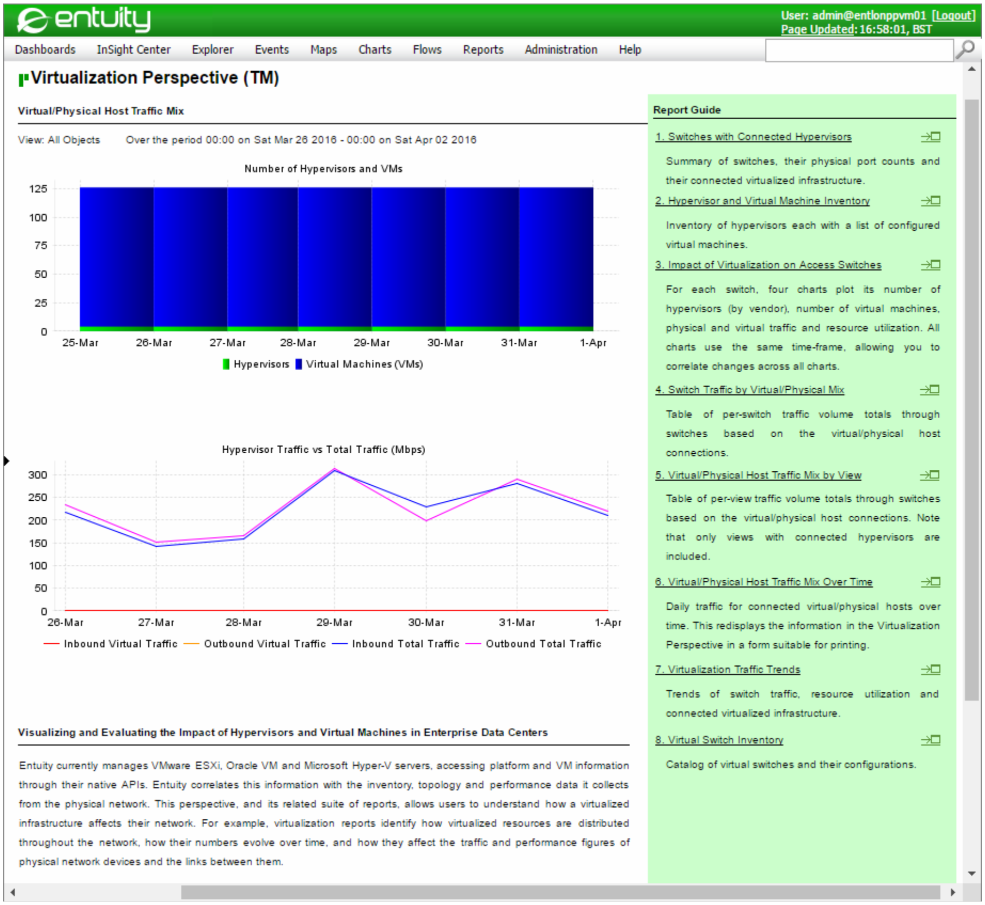
## Accessing the Virtualization Perspective

To access the Virtualization Perspective dashboard:

1) Click **InSight Center** >**Virtualization Perspective**.
2) Complete the Report Options for the perspective.

The Virtualization Perspective:

- Charts the daily number of hypervisors and VMs over the reporting period.
- Charts the both inbound and outbound traffic, both virtual and total.
- Provides links to eight reports.



**Virtualization Perspective (TM)**

**Virtual/Physical Host Traffic Mix**

View: All Objects Over the period 00:00 on Sat Mar 26 2016 - 00:00 on Sat Apr 02 2016

**Visualizing and Evaluating the Impact of Hypervisors and Virtual Machines in Enterprise Data Centers**

Entuity currently manages VMware ESXi, Oracle VM and Microsoft Hyper-V servers, accessing platform and VM information through their native APIs. Entuity correlates this information with the inventory, topology and performance data it collects from the physical network. This perspective, and its related suite of reports, allows users to understand how a virtualized infrastructure affects their network. For example, virtualization reports identify how virtualized resources are distributed throughout the network, how their numbers evolve over time, and how they affect the traffic and performance figures of physical network devices and the links between them.

**Report Guide**

1. Switches with Connected Hypervisors

   Summary of switches, their physical port counts and their connected virtualized infrastructure.

2. Hypervisor and Virtual Machine Inventory

   Inventory of hypervisors each with a list of configured virtual machines.

3. Impact of Virtualization on Access Switches

   For each switch, four charts plot its number of hypervisors (by vendor), number of virtual machines, physical and virtual traffic and resource utilization. All charts use the same time-frame, allowing you to correlate changes across all charts.

4. Switch Traffic by Virtual/Physical Mix

   Table of per-switch traffic volume totals through switches based on the virtual/physical host connections.

5. Virtual/Physical Host Traffic Mix by View

   Table of per-view traffic volume totals through switches based on the virtual/physical host connections. Note that only views with connected hypervisors are included.

6. Virtual/Physical Host Traffic Mix Over Time

   Daily traffic for connected virtual/physical hosts over time. This redisplays the information in the Virtualization Perspective in a form suitable for printing.

7. Virtualization Traffic Trends

   Trends of switch traffic, resource utilization and connected virtualized infrastructure.

8. Virtual Switch Inventory

   Catalog of virtual switches and their configurations.

Figure 110 Entuity Virtualization Perspective

# Running Virtualization Reports

Entuity currently manages VMware ESXi, Oracle VM and Microsoft Hyper-V servers, accessing platform and VM information through their native APIs. Entuity correlates this information with the inventory, topology and performance data it collects from the physical network. This perspective, and its related suite of reports, allows users to understand how a virtualized infrastructure affects their network.

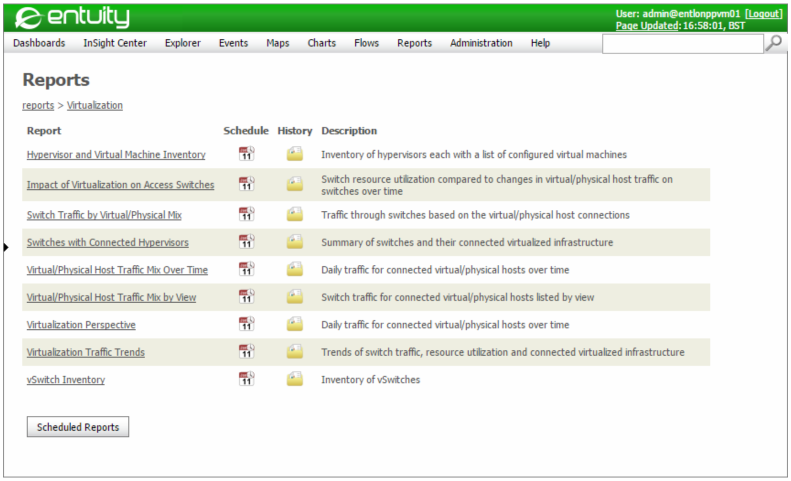
You can access virtualization reports through the:

- Virtualization Perspective. A brief description of each report and a hyperlink to its Report Options are given in its Report Guide panel.
- Reports area of the web UI where virtualization infrastructure reports are grouped together as Virtualization Reports.

To access the Virtualization Reports:

1) Click **Reports** > **View Reports**.

2) Click **Virtualization Reports**. Entuity displays all of the Virtualization Reports.



Reports

reports > Virtualization

| Report | Schedule | History | Description |
|---|---|---|---|
| Hypervisor and Virtual Machine Inventory | | | Inventory of hypervisors each with a list of configured virtual machines |
| Impact of Virtualization on Access Switches | | | Switch resource utilization compared to changes in virtual/physical host traffic on switches over time |
| Switch Traffic by Virtual/Physical Mix | | | Traffic through switches based on the virtual/physical host connections |
| Switches with Connected Hypervisors | | | Summary of switches and their connected virtualized infrastructure |
| Virtual/Physical Host Traffic Mix Over Time | | | Daily traffic for connected virtual/physical hosts over time |
| Virtual/Physical Host Traffic Mix by View | | | Switch traffic for connected virtual/physical hosts listed by view |
| Virtualization Perspective | | | Daily traffic for connected virtual/physical hosts over time |
| Virtualization Traffic Trends | | | Trends of switch traffic, resource utilization and connected virtualized infrastructure |
| vSwitch Inventory | | | Inventory of vSwitches |

Figure 111 Virtualization Reports Listing

Details on Virtualization Reports are available through the *Entuity Reports Reference Manual*.

| Report Title | Description |
|---|---|
| Hypervisor and Virtual Machine Inventory Overview | Inventory of hypervisors each with a list of configured virtual machines |
| Impact of Virtualization on Access Switches Overview | For each switch, four charts plot its number of hypervisors (by vendor), number of virtual machines, physical and virtual traffic and resource utilization. All charts use the same time-frame, allowing you to correlate changes across all charts. |
| Switch Traffic by Virtual/Physical Mix Overview | Table of per-switch traffic volume totals through switches based on the virtual/physical host connections. |
| Switches with Connected Hypervisors Overview | Summary of switches, their physical port counts and their connected virtualized infrastructure. |
| Virtual/Physical Host Traffic Mix by View Overview | Table of per-view traffic volume totals through switches based on the virtual/physical host connections. Note that only views with connected hypervisors are included. |
| Virtual/Physical Host Traffic Mix Over Time Overview | Daily traffic for connected virtual/physical hosts over time. This displays the information in the Virtualization Perspective in a form suitable for printing. |
| Virtualization Traffic Trends Overview | Trends of switch traffic, resource utilization and connected virtualized infrastructure. |

Table 10 List of Virtualization Reports

| Report Title | Description |
|---|---|
| vSwitch Inventory | Catalogs vSwitch configuration settings. |

Table 10 List of Virtualization Reports

# 10 User Preferences

Entuity user preferences allows you to view and modify the Entuity web interface. Settings apply at the user level and are maintained across user sessions, i.e. they are saved in the database. In multi-server environments with external authentication, settings apply to all servers, without external authentication settings apply only to the local server.

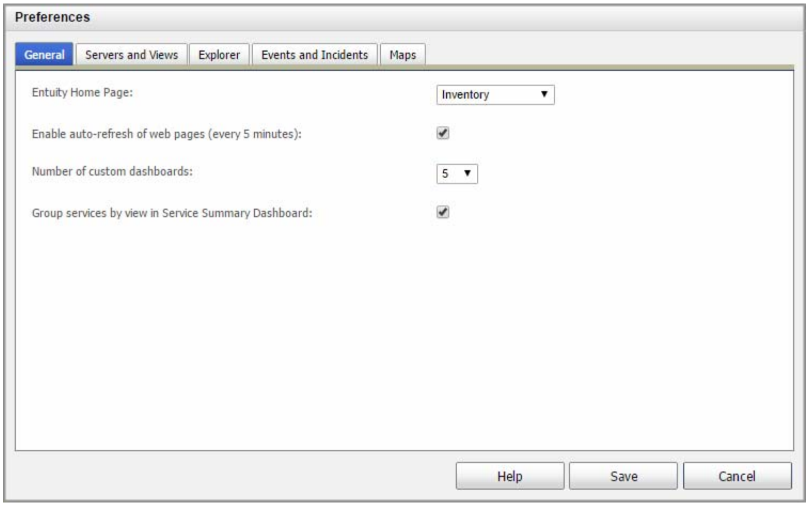
From Preferences you can configure how the web interface handles multiple Entuity servers and views, set and view event notifications, configure the interface, e.g. default page, Event Viewer display.

To personalize the Entuity interface:

1) Click **Administration** > **Preferences**.

## General Preferences

Through the General Preferences tab you can set the Entuity home page, page auto refresh state, number of permitted and how the Service Summary dashboard groups services.



Entuity Home Page: Inventory

Enable auto-refresh of web pages (every 5 minutes): ☑

Number of custom dashboards: 5

Group services by view in Service Summary Dashboard: ☑

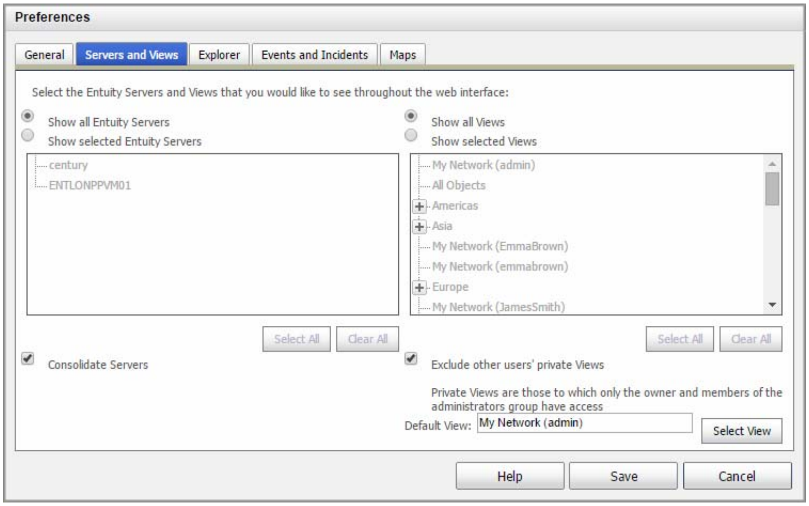
Figure 112  General Preferences

| Attribute | Description |
|---|---|
| *Entuity Home Page* | Select the page Entuity displays after logging in. You can select from:<br>■ Inventory, the factory default for members of the Administrators access group.<br>■ Status Summary, the factory default for members of the All users access group.<br>■ TopN Summary. (See *Monitor Network Performance Using Port Metrics*.)<br>■ Device Metrics. (See *Monitor Operational Trends Using Device Metrics*.)<br>■ Health Summary.<br>■ Service Summary. (See *Service Summary Dashboard*.)<br>■ Explorer.<br>■ Events.<br>■ Custom Dashboards, only available when the user has at least one custom dashboard. (See *Build Custom Dashboards*.)<br>■ User Defined URL. |
| *Enable Auto-Refresh of web pages (every 5 min)* | When Enable Auto-Refresh is:<br>■ Selected, pages within the web interface refresh every five minutes.<br>■ Not selected, pages only refresh when the Entuity server sends fresh data or the user initiates a refresh. |
| *Number of custom dashboards* | Sets the maximum number of custom dashboards that you can define and have available from the Dashboards menu. By default the maximum is 5, however by default the permitted range of values is between 1 and 20. You can amend this threshold through the `entuity.cfg` setting `webUI.customDashboardMaxCount`. |
| *Group Services by View in Service Summary Dashboard* | When Group Services by View is:<br>■ Enabled (default), the Service Summary dashboard displays services grouped by view.<br>■ Disabled, the Service Summary dashboard displays all services ordered alphabetically. For each service Entuity lists the views in which the service is available. |

Table 11 General Preferences

# Servers and Views Preferences

Through the Servers and Views tab you can tailor the display of Entuity servers and views.



Select the Entuity Servers and Views that you would like to see throughout the web interface:

● Show all Entuity Servers
○ Show selected Entuity Servers

- century
- ENTLONPPVM01

● Show all Views
○ Show selected Views

- My Network (admin)
- All Objects
- Americas
- Asia
- My Network (EmmaBrown)
- My Network (emmabrown)
- Europe
- My Network (JamesSmith)

☑ Consolidate Servers

☑ Exclude other users' private Views

Private Views are those to which only the owner and members of the administrators group have access

Default View: My Network (admin)

Figure 113 Servers and Views Preferences

| Attribute | Description |
|---|---|
| *Configuration of which remote Entuity servers are displayed in the web interface* | When you select:<br>■ **Show All Entuity Servers**, Entuity displays data from all remote Entuity servers for which their Show setting is enabled.<br>■ **Show Selected Entuity Servers**, Entuity allows you to select from the list of remote servers those that you want to view in the web interface. Only remote Entuity servers for which their Show setting is also enabled are displayed.<br>You can view, and amend, the server's show setting through the Remote Server administration page. |
| *Configuration of which views on the local Entuity servers are displayed in the web interface* | When you select:<br>■ **Show All Views**, Entuity displays all views to which the user has access.<br>■ **Show Selected Views**, Entuity allows you to select from the list of views to which you have access those views you want to access through the web interface. |
| *Consolidate Servers* | When:<br>■ Selected, the content of views with the same name on different Entuity servers are consolidated.<br>■ Not selected, the content of views with the same name on different Entuity servers are not consolidated. For example, in the Explorer object tree views are grouped by their Entuity server.<br>The current consolidate mode is indicated in the navigation panel. |

Table 12 Servers and Views Preferences

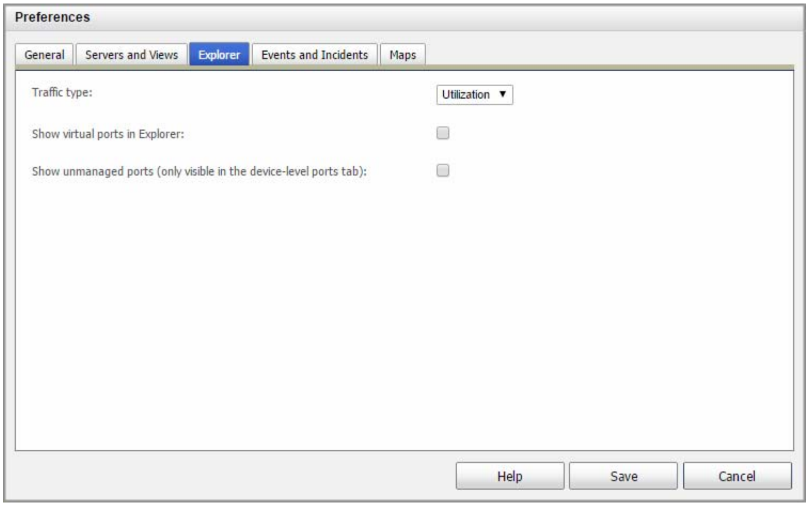
| Attribute | Description |
|---|---|
| *Exclude Other User’s Private Views* | When:<br>■ Selected, administrators only see those views to which they access through their non-administrator user groups and view ownership settings.<br>■ Not selected (default), administrators have displayed all views.<br>Private views are views to which only the owner and members of the administrators group have access. Private views are hidden to make the Explorer interface easier to manage, you might only make private views visible for the duration of a particular task.<br>This option is only available to members of the administrators user group. |
| *Default View* | Scope used by Event Viewer, by default the user’s My Network view. You can select a different view. |

Table 12 Servers and Views Preferences

When an administrator has selected **Exclude Other User’s Private Views** and then assigns view ownership to another user, if the administrator is not a member of a group that has access to that view then the administrator can longer see the view from their Explorer. The view has not disappeared, the administrator only has to change their exclusion setting to see the view again.

## Explorer Preferences

The Explorer tab controls the display of traffic data, virtual ports and unmanaged ports in the Explorer pages, e.g Summary and Advanced pages.



Preferences

Traffic type: Utilization ▼

Show virtual ports in Explorer: □

Show unmanaged ports (only visible in the device-level ports tab): □

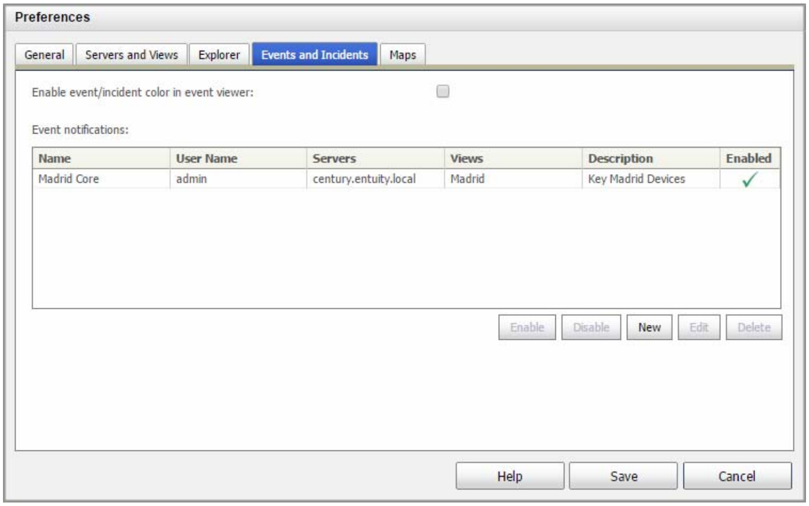
Figure 114 Explorer Preferences

| Attribute | Description |
|---|---|
| *Traffic-Type* | Sets how the web UI displays traffic data, i.e. **Utilization**, **Rate** or **Volume**. |
| *Show Virtual Ports in the Explorer* | When:<br>■ Selected, the Explorer object tree displays both physical and virtual ports.<br>■ Not selected (default), the Explorer object tree displays only physical ports. The Summary, Advanced Details and Port List pages also do not show virtual ports. |
| *Show Unmanaged Ports* | When:<br>■ Selected, Explorer displays unmanaged ports in the device's Ports tab. Unmanaged ports are not shown in the object tree.<br>■ Not selected (default), Explorer does not display unmanaged ports. |

Table 13 Explorer Preferences

# Events and Incidents Preferences

Through the Events and Incidents tab you can control the availability of event notifications and color coding of event rows in Event viewer.



Enable event/incident color in event viewer: □

Event notifications:

| Name | User Name | Servers | Views | Description | Enabled |
|---|---|---|---|---|---|
| Madrid Core | admin | century.entuity.local | Madrid | Key Madrid Devices | ✓ |

Figure 115 Events and Incidents Preferences

| Setting | Description |
|---|---|
| Event Notification | When Event Notification is:<br>■ Displays current notification settings. Entuity administrators can view all event notifications, other users can view a summary of the event notifications to which they are associated.<br>■ Allows administrators access to event notification configuration. |
| Color Event | When Color Event is:<br>■ Enabled the row of each incident and event in Event Viewer has the background color of that event’s severity level.<br>■ Not enabled (default) the background color of all incident and event rows is white. |

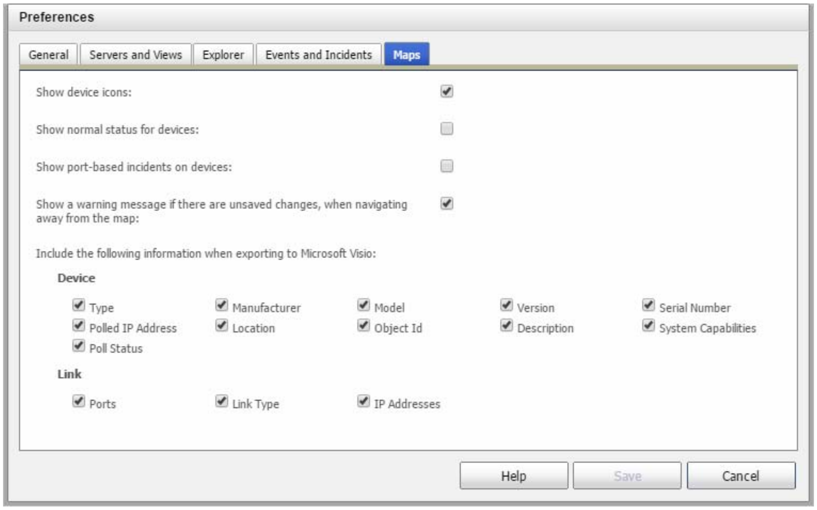
Table 14 Events and Preferences

Event Notifications

## Maps Preferences

Map user preferences allow you to configure map display and Visio export behavior. Similarly, Entuity prevents you from de-selecting both *Show Icons* and *Show Normal Status*.

Visio Export Types settings control what map information Entuity exports to Visio. Check each item that you to permit export to Visio.



Preferences

Show device icons: ☑

Show normal status for devices: □

Show port-based incidents on devices: □

Show a warning message if there are unsaved changes, when navigating away from the map: ☑

Include the following information when exporting to Microsoft Visio:

Device

☑ Type ☑ Manufacturer ☑ Model ☑ Version ☑ Serial Number
☑ Polled IP Address ☑ Location ☑ Object Id ☑ Description ☑ System Capabilities
☑ Poll Status

Link

☑ Ports ☑ Link Type ☑ IP Addresses

Figure 116 Maps Preferences

| Name | Attributes |
|---|---|
| *Show device Icons* | Device and sub-views are displayed in the map using either the appropriate icon or status disc. When Show device icon is:<br>■ Selected the map uses icons to represent devices and sub-views.<br>■ Not selected the map represents objects using a disc, the color of which indicates the object's status. Entuity also automatically selects *Show Normal Status*. |
| *Show Normal Status* | Entuity indicates the state of an object (device or sub-view) on a map by using a color coded disc as that object's background. By default Entuity only indicates objects that are not in a normal state.<br>When *Show Normal Status* is selected then Entuity also displays a color coded disc - in this case green - for those managed objects with a normal status. |
| *Show port-based incidents on devices* | When selected incidents raised against a device's ports are displayed against the device on the map. By default this option is not selected and only incidents raised against a device are indicated on the map. |
| *Show individual link status or utilization* | When selected map links indicate the status independently at each end of the link (default). When not selected map links show the worst status of either end of the link. |

Table 15 Map Preferences

| Name | Attributes |
|---|---|
| *Show a warning message if there are unsaved changes ...* | By default if you adjust a map with a change that can be saved, and you have the permission to save the map, Entuity prompts you to save the map when you navigate away from it. Deselect this checkbox when you do not want the prompt. |
| Device | Sets the device attributes exported to the Microsoft Visio `vdx` file. By default all of these device attributes are exported: *Type*, *Manufacturer*, *Model*, *Version*, *Serial Number*, *Polled IP Address*, *Location*, *Object Id*, *Description*, *System Capabilities*, *Poll Status*. |
| Link | Visio export link types: Ports, Links. |

Table 15 Map Preferences

# 11 Search the Managed Network

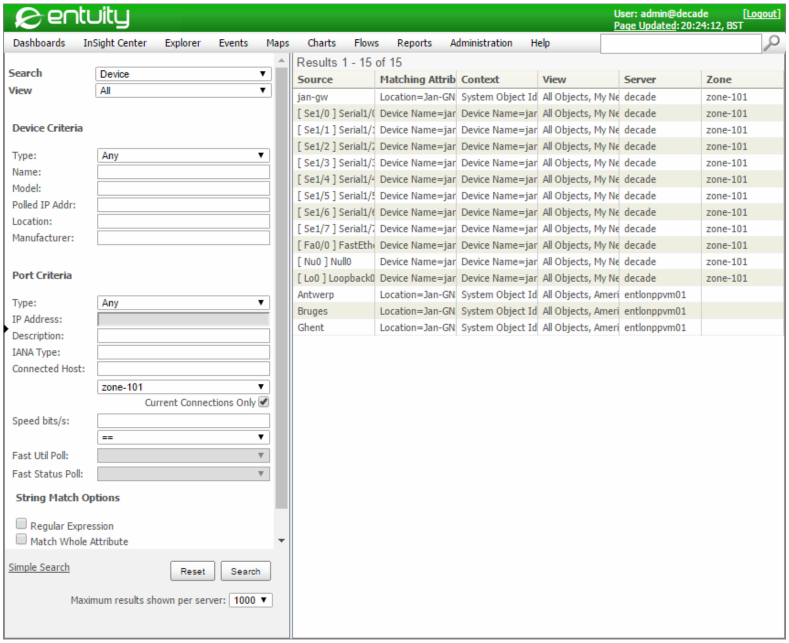
Entuity Search allows you to search for devices, ports and other managed objects across multiple Entuity servers. The search tool is accessible from all included Entuity servers through an HTML interface. Each Entuity server has its own search space so the search is performed on the remote server, and the results returned to the local server. Entuity displays the results as they are returned from each server.

Entuity Search provides:

- Searching across multiple Entuity servers as though they were one large server, with clear identification of the managing server.
- Simple and extended modes of search, with multiple search criteria support.
- Searching by zone, when multi-tenant support is configured. (See *Chapter 15 - Multi-tenant Support*.)

  Connected host searches are limited to a given zone. By default, the selected zone will be **None**. Connected host searches initiated from the quick search box in the Entuity banner always use the default **None**.
- Connected host search, for example by MAC address, IP address.
- Support for both simple and regular expressions which can be used in most text fields.
- A results page listing all matching components, with tooltips that provide more detail and context menus through which you can call more tools to investigate the results.

  When multi-tenant support is configured the details of the device zone is also returned. Configure the results column to include Zone. If a device is not assigned to a zone the column is left empty. (See *Figure 117 Multi-tenant Search*.)



Search: Device
View: All

Device Criteria

Type: Any
Name:
Model:
Polled IP Addr:
Location:
Manufacturer:

Port Criteria

Type: Any
IP Address:
Description:
IANA Type:
Connected Host:
zone-101
Current Connections Only ☑
Speed bits/s:
==
Fast Util Poll:
Fast Status Poll:

String Match Options

☐ Regular Expression
☐ Match Whole Attribute

Maximum results shown per server: 1000

Results 1 - 15 of 15

| Source | Matching Attrib | Context | View | Server | Zone |
|---|---|---|---|---|---|
| jan-gw | Location=Jan-GN | System Object Id | All Objects, My Ne | decade | zone-101 |
| [ Se1/0 ] Serial1/( | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| [ Se1/1 ] Serial1/1 | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| [ Se1/2 ] Serial1/2 | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| [ Se1/3 ] Serial1/3 | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| [ Se1/4 ] Serial1/4 | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| [ Se1/5 ] Serial1/5 | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| [ Se1/6 ] Serial1/6 | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| [ Se1/7 ] Serial1/7 | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| [ Fa0/0 ] FastEth | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| [ Nu0 ] Null0 | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| [ Lo0 ] Loopback0 | Device Name=jar | Device Name=jar | All Objects, My Ne | decade | zone-101 |
| Antwerp | Location=Jan-GN | System Object Id | All Objects, Ameri | entlonppvm01 | |
| Bruges | Location=Jan-GN | System Object Id | All Objects, Ameri | entlonppvm01 | |
| Ghent | Location=Jan-GN | System Object Id | All Objects, Ameri | entlonppvm01 | |

Figure 117 Multi-tenant Search

## What Entuity Searches

When your system administrator installs and configures Entuity, the modules they select determines what Entuity can manage and therefore the objects and attributes that Entuity can include to its search space. The default search object configuration includes, for example, Wireless, Firewall, Managed Host attributes. Entuity then maintains information on these search objects and their attributes in a search space, which it updates as they change.

| Object | Attribute |
|---|---|
| CUCM Failed Phone | CUCM Failed Phone IP Address, CUCM Failed Phone MAC Address |
| CUCM Extension | CUCM Phone Extn Number, CUCM Phone Extn IP Address |
| CUCM Phone | CUCM Phone MAC Address, CUCM Phone IP Address |
| Host IP Address | Host IP Address |
| AutonomousWap | Name, awapMac |
| BCSwitchDevice | Name |
| BladeCenterDevice | Name, ext Ethernet Interface Host Name, ext Ethernet Interface IP Address |
| All (Device) | Name, Manufacturer, Model, Version, Serial Number, Polled IP Address |
| device | Name, SNMP Community, Type, SYS OID, Description, Location |

Table 16 Default Search Objects and Attributes

| Object | Attribute |
|---|---|
| Device(Uncertified) | Name |
| HubDevice | Name |
| RouterDevice | Name |
| SSLProxyDevice | Name |
| SwitchDevice | Name, Base Bridge Address |
| VM | VM Configuration File, VM UI Name |
| frDlci | fr Dlci Index Name, fr Dlci Name, fr Dlci Type |
| ManagedHost | Name |
| module | Name, Description |
| atmPort | ifName |
| portEx | Description, Alias, Reference Speed, Short Description |
| frPort | Name |
| IPv6Address | IPv6 Address Value |
| PortIPv6Address | Port IPv6 Address String Formatted, Port IPv6 Address Type |
| PortNeighbor | Port Neighbor IP Address, Port Neighbor Physical Address |
| IPv6Interface | IPv6 Interface Identifier, IPv6 Interface Physical Address |
| llPort | Name |
| WirelessPort | Name |
| port | Name, Port Device Name, Description, Type, Speed |
| policyMap | QoS Policy Map Name |
| classMap | QoS Class Map Name |
| matchStatement | QoS match statement |
| BGPPeer | BGP Peer Remote Addr Type: OSPFPeer<br>OSPF Peer Remote Address |
| EIGRPPeer | EIGRP Peer Address |
| SystemIPLink | IP Pair Name |
| UserIPLink | User IP Link Name |
| SAAProbe | Probe Name |

Table 16 Default Search Objects and Attributes

## Running Searches

Entuity Search is available from the web interface, where you can enter the query:

- Through the Search Query pane, with the option of simple and extended search modes.
- From the menu bar’s search text field.

When you enter a search string and click on the Search icon Entuity searches for all objects within the search space testing the search string against all of the searchable attributes, for example device name, location, port description, connected hosts.

Entuity searches for connected hosts first by name/IP address and then by mac address. Mac addresses must be entered using either colon or hyphens delimiters, e.g. 00:00:00:aa:bb:cc, 00-00-00-aa-bb-cc. A connected host search does not support partial or approximate matches, and so you also cannot use regular expressions.

When you do not enter a search string but do click on the Search icon Entuity opens the Simple Search query panes where you can then enter a more specific query. (See *Running An Extended Search*.)

## Running A Simple Search

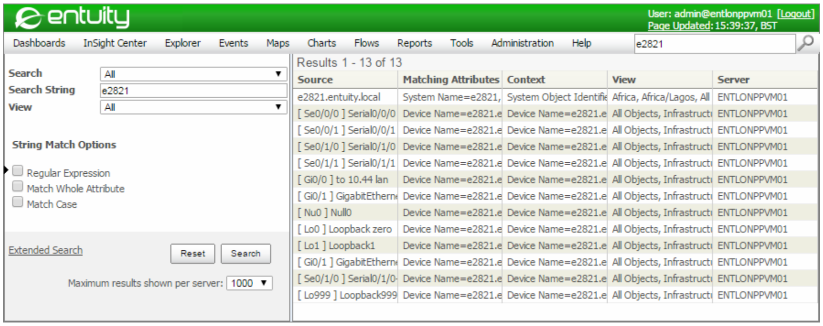
When you run a simple search Entuity applies the search string across all criteria, against both device and port searchable attributes for example device name, device model, port description, port connected hosts.

To run a quick simple search:

1) Select the magnifying glass icon from the menu bar but do not enter a query.

2) Complete the Simple Search query.

3) Click **Search**. Entuity displays results.



Search: All

Search String: e2821

View: All

☐ Regular Expression
☐ Match Whole Attribute
☐ Match Case

Maximum results shown per server: 1000

Results 1 - 13 of 13

| Source | Matching Attributes | Context | View | Server |
|---|---|---|---|---|
| e2821.entuity.local | System Name=e2821, | System Object Identifie | Africa, Africa/Lagos, All | ENTLONPPVM01 |
| [ Se0/0/0 ] Serial0/0/0 | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Se0/0/1 ] Serial0/0/1 | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Se0/1/0 ] Serial0/1/0 | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Se0/1/1 ] Serial0/1/1 | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Gi0/0 ] to 10.44 lan | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Gi0/1 ] GigabitEtherne | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Nu0 ] Null0 | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Lo0 ] Loopback zero | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Lo1 ] Loopback1 | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Gi0/1 ] GigabitEtherne | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Se0/1/0 ] Serial0/1/0- | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |
| [ Lo999 ] Loopback999 | Device Name=e2821.e | Device Name=e2821.e | All Objects, Infrastructu | ENTLONPPVM01 |

Figure 118 Running A Quick Search

## Running An Extended Search

When you run an extended search you can specify the search strings against your required device and port searchable attributes, for example device name, device model, port description, port connected hosts.

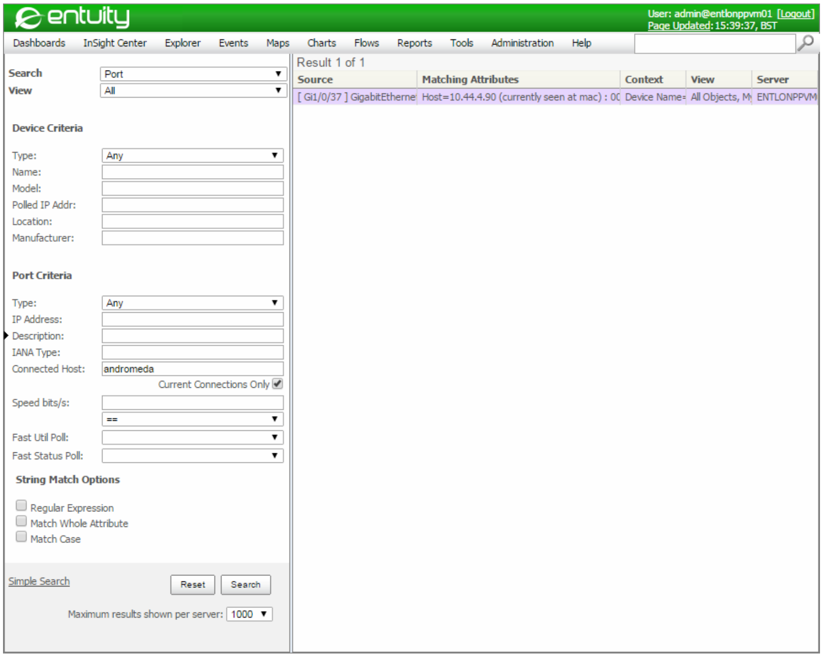
To run an extended search:

1) Select the magnifying glass icon from the menu bar but do not enter a query.

2) Click **Extended Search**. Entuity displays the Extended Search options.

3) From the Search Query pane complete your extended search query.

4) Click **Search**. Entuity displays the Search results.



Search: Port
View: All

**Device Criteria**

Type: Any
Name:
Model:
Polled IP Addr:
Location:
Manufacturer:

**Port Criteria**

Type: Any
IP Address:
Description:
IANA Type:
Connected Host: andromeda
Current Connections Only ☑
Speed bits/s:
==
Fast Util Poll:
Fast Status Poll:

**String Match Options**

□ Regular Expression
□ Match Whole Attribute
□ Match Case

Maximum results shown per server: 1000

Result 1 of 1

| Source | Matching Attributes | Context | View | Server |
|---|---|---|---|---|
| [ Gi1/0/37 ] GigabitEtherne | Host=10.44.4.90 (currently seen at mac) : 00 | Device Name= | All Objects, My | ENTLONPPVM |

Figure 119 Running A Quick Host Search

## Searching for Devices

You can execute a search for devices using as your search parameters device and/or port attributes.

To search for devices:

1) Click the Search icon from the menu bar, do not enter a search query.

   Entuity displays the Extended Search pane.

2) In *Search* select **Device**. This is the type of managed object you want to return as the search result, i.e. Device or Port.

3) In *Device Criteria* enter the device attributes to use to search for the device.

4) In *Port Criteria* enter port attributes. Search only returns details of devices with ports that match these attributes.

5) Specify *String Match Options*.

6) Select **Search**. Entuity displays the Search results.

## Searching by Interface

You can execute a search for ports using as your search parameters device and/or port attributes.

To search for ports:

1) Select the Search icon from the menu bar, do not enter a search query.

   Entuity displays the Extended Search pane.

2) In *Search* select **Port**. This is the type of managed object you want to return as the search result, i.e. Device or Port.
3) In *Device Criteria* enter device attributes. Search only returns details of ports with devices that match these attributes.
4) In *Port Criteria* enter the port attributes to search against.
5) Specify *String Match Options*.
6) Select **Search**. Entuity displays the Search results.

# Attributes of Search Queries and Results

The Entuity web interface search tool is a powerful and flexible tool for querying the management database. You can run quick, simple searches or define more complex search queries. The format of the results is the same regardless of the type of search query.

## Understanding Entuity Search Queries

You can make your search query as simple or as specific as you require. Available Search query options:

- Search, allows you to specify the type of object you want to find:
  - All, to run the query against both devices and ports
  - Device, to run the query only against devices
  - Port, to run the query only against ports.
- Search type determines the search criteria options. When search type is:
  - **Simple Search**, you enter in *Search String*, the string Entuity uses to search the database. You can amend the String Match Options to alter how Entuity handles the string.
  - **Extended Search**, you can configure highly specific search criteria for Devices and Ports, using Device Criteria and Port Criteria, respectively. (see *Understanding Extended Search Parameters*.)
- String Match Options, you can select one or more options:
  - **Regular Expression**, when selected allows development of expressions that are POSIX compliant.
  - **Match Whole Attribute**, when selected the matching attribute value on returned objects must completely match the search term.
  - **Match Case**, when selected the matching attribute value on returned objects has the same casing of the search term. By default, searches are case insensitive.
- *Maximum results shown,* the number of results Search returns.

## Understanding Extended Search Parameters

Entuity Search allows you to search for managed objects in the search space. The search page clearly identifies where you can enter your search criteria, which varies according to the searched managed object type. The search results table columns correspond to the search parameters for that managed object type.

## Using Regular Expressions

Entuity Search allows you to filter results by using regular expressions (POSIX compliant). For example to find references to:

- A device called **century** enter in *Name*:

  `century`

- All devices not called **century** enter in *Name*:

  `[^century]`

- Devices called **century** or **compressor** enter in *Name*:

  `compressor|century`

- Devices part called **cent** enter in *Name*:

  `cent+`

| Symbol | Description |
|---|---|
| \| | Boolean Or, is a vertical bar which separate alternatives. For example the pluto\|vortex return results containing either pluto or vortex. |
| [ ] | Square brackets allow you to separate and order sections of the expression. |
| . | Dot matches any single character. Within parentheses it matches its literal, dot value. |
| [^ ] | Not operator Entuity Search returns results that do not include the search string, for example searching for a device name using [^vortex] filters out device’s with vortex in their name. |
| * | Wildcard matches a string of any length of characters, including slash (/) characters. |
| ? | Wildcard matches any single character. |
| + | Wildcard matches one or more occurrences of the previous element. |
| [character set] | Wildcard matches a single character that is one of the set of characters. For example, [a-e] matches any ASCII character in the range from a to e. |
| character | Matches the entered character. |

Table 17 Sample POSIX Components

## Attributes for Searching by Device

You can execute a search for all ports of the set type where its host device attributes match the search criteria.

Entuity Search device parameters include:

- *Type*, Entuity device type, e.g. **Any**, **Ethernet Switch**, **Router**.
- *Name*, name of the managed device.
- *Address*, IP address used by Entuity to poll the device.
- *Model*, device model.
- *Location*, device location.
- *Manufacturer*, list of device manufacturers.

## Attributes for Searching by Interface

You can execute a search for all devices of the set type where certain port attributes are matched.

Entuity Search interface parameters include:

- *Type*, device interface types, e.g. **Any, Wan Port**.
- *IP Address*, IP address of the port.
- *Description*, device interface description.
- *IANA Type*, the description of the interface type, e.g. ethernet6 (for a full listing see the *Entuity System Administrator Manual*).
- *Connected Host*, resolved name, IP address or MAC address of the connected host.

  MAC addresses must be entered using either colon or hyphen delimiters, e.g. 00:00:00:aa:bb:cc, 00-00-00-aa-bb-cc.
- *Speed bit/s*, interface speed, i.e. All, 10M, 100M, 1G, 10G. When the port has asynchronous speed settings Entuity searches using only the outbound speed.

  You can select the appropriate operator from the associated drop-down list of operators.
- *Fast Util Port*, search for ports by their fast utilization polling state.
- *Fast Status Poll*, search for ports by their fast status polling state.

## Search Results

The number of results Search returns is dependent upon the value selected in *Maximum results shown per server*. Search does not sort the results, simply returning the first results that meet the search query.

Search Results display:

- *Source*, the identifier for the found object, e.g. device, port, managed host.
- *Matching Attributes*, the field on which the object matches the search criteria. The names and values of successfully matched attributes are always displayed in a Search Result.
- *Context*, details on the managed object. For example, Polled IP Address, Community String, System Object Identifier.
- *View*, Entuity business views in which the object is visible. A query that you run can only return results from views to which you have access.
- *Server*, Entuity server that manages the object. The results for a single Entuity server are displayed at one time. For multi-server searches the results page is updated with each

server's results as they arrive. You can only run searches against Entuity servers to which you have access.

When you move your mouse over a result, Search displays a tooltip that gives more information on the item in that column.

### Use Context Menus On Search Results

Context menus are also available, against those objects that have them. You can therefore select more than one item and apply the same action to all. For example, when you want to deactivate fast status polling on a subset of ports:

1) You can search for ports with fast polling enabled.
2) From the list of results highlight the port’s on which you want to deactivate polling.
3) From the context menu select **Polling** > **Fast Status Polling** > **Disable**.

# 12 Ticker - Monitoring Realtime Component Output

Ticker allows you to view real time output at the device and port level, viewing data changes as they occur. You can select to view data activity for one or more client devices or ports. For monitored:

- Ports you can select from a list of MIB variables the particular variable(s) you want to use to monitor the port. Entuity is supplied with a default number of MIB variables for use with ports.
- Devices you can assign MIB variables from MIB Browser.

By default Ticker listens for client device and port activity using port 20202, although you can amend this using `configure`. (See the *Entuity Getting Started Guide*.)

✓ To use Ticker you must have the Ticker tool permission, or be a member of the Administrator user group.

✓ The more variables you choose the greater the use of network resource, in terms of both bandwidth and CPU.

To run Ticker against a port:

1) You can:
   - From the Explorer navigation tree select a port and from the context menu select **Ticker**.
   - From a device's Ports tab select one or more ports and from the context menu select **Ticker**.
2) From Ticker's OIDs Selection dialog you can select the OIDs to apply against the selected ports (see *Select OIDs for Ticker to Monitor*).
3) Click:
   - Current Ticker Chart to add the selected variables to the chart.
   - New Ticker Chart to create a new chart.

   Through the Ticker chart you can view samples as they are collected and plotted. You can amend the original Ticker configuration and how the data is displayed.

## Select OIDs for Ticker to Monitor

After launching Ticker, you can select the POIDs for it to monitor. Even when Ticker is running you can add and remove variables to and from Ticker's monitor list.

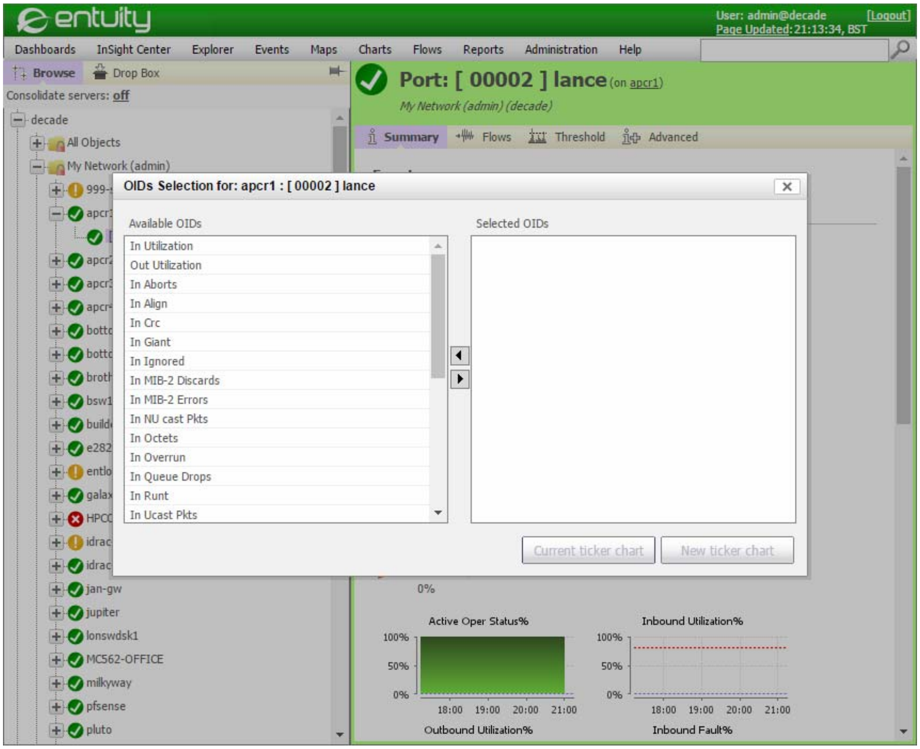


Figure 120 Select Ticker Variables

Entuity is shipped with an extensive list of OIDs that Ticker can use to monitor port activity. (See *Supplied MIB Variables for Ports*.)

OIDs Selection dialog includes two panes:

- *Available OIDs* lists all of the possible pre-supplied variables Ticker can monitor but which are not currently selected for the object.
- Selected OIDs lists all of the object’s OIDs Ticker is to monitor.

Additional OIDS can be monitored by Ticker by adding then through the MIB Browser. (See *Monitor Custom OIDs through Ticker*.)

If you terminate the Ticker session before the application is due to start ticking, then the timed capture does not take place.

## Supplied MIB Variables for Ports

Entuity provides a number of MIB variables that you can use to monitor realtime performance at the port-level. If you need additional variables you can specify them through MIB Browser. (See *Monitor Custom OIDs through Ticker*.)

The number and types of MIB variables that Ticker can monitor at the port-level are determined by the type (vendor and product) of networking equipment being polled, together with the media type(s) of the port(s) being polled. The variable selection is determined through access to the standard `bin.vendor` file. (See the *System Administrator Manual*.)

Most equipment supports only a subset of these variables, so do not expect all of these variables to be available across all equipment. Where ports are selected that are part of equipment from a variety of vendors, only those variables that are common to all of the ports may be selected.

The following tables detail the polled variables Ticker monitors. The variables are split into three types; information, performance and fault.

### Information Type Variables

This table details the MIB variables that gather information on your network that you can use to monitor its performance.

| Information Types | Description |
|---|---|
| *In NU cast Pkts* | The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets inbound to a port. |
| *In Octets* | The total number of octets received on the interface, including framing characters. |
| *In Ucast Pkts* | The number of subnetwork-unicast packets inbound to a port. |
| *Out NU cast Pkts* | The total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent. |
| *Out Octets* | The total number of octets transmitted out of the interface, including framing characters. |
| *Out Ucast Pkts* | The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent. |
| *In Utilization [%]* | Utilization is expressed as a percentage of actual traffic volume received against the maximum volume that can be handled by the port. |
| *Out Utilization [%]* | Utilization is expressed as a percentage of actual traffic volume transmitted against the maximum volume that can be handled by the port. |

Table 18 MIB Information Type Variables

### Performance Issue Variables

This table details the MIB variables that gather information on issues that can adversely affect your network's performance.

| Performance Issues | Descriptions | Possible Causes |
|---|---|---|
| *In Ignored* | Packets where no attempt to process was made. | Severe inbound congestion. Broadcast storms. |
| *In Overrun* | Receiver buffer overflowed. | Device cannot process received packets quickly enough. |
| *In Queue Drops* | Forwarding buffer overflowed | Device cannot forward inbound traffic quickly enough. |
| *Out Colln* | Collisions in packet transmission. | Line oversubscribed. |
| *Out Defer* | The number of outbound packets for which transmission was deferred. | Line oversubscribed. |
| *Out Excv Colln* | Multiple collisions in packet transmission. | Line oversubscribed. |
| *Out Mult Colln* | Packet discarded because of multiple collisions on that packet. | High network traffic. |
| *ifOutPQueueDrop* | Software buffer overflowed. | Priority queue too short or line too slow. |
| *Out Queue Drop* | Outbound buffer overflowed. | Outbound packet rate cannot be achieved by line. |
| *ifOutUnderrun* | Outbound queue emptied too quickly. | Device cannot service at line rate. |

Table 19 MIB Performance Issue Variables

## Fault Type Variables

This table details the MIB variables that gather information on errors that have occurred on your network.

| Fault Types | Descriptions | Possible Causes |
|---|---|---|
| *In Aborts* | Receiver aborted reception of packet. | Clocking problems. |
| *In Align* | Packet failed to finish on 8-bit boundary. | Synchronization error. |
| *ifInColln* | Packet caused collisions. | High network traffic. |
| *In Crc* | Packet checksum error (Cyclic Redundancy Checks). | Transmitter or line error. |
| *In Giant* | Packet above maximum allowed media size. | Transmitter or synchronization error. |
| *ifInLateColln* | Packet caused collisions outside of protocol specifications. | Transmitter error, cable fault, network too long. |

Table 20 MIB Fault Type Variables

| Fault Types | Descriptions | Possible Causes |
|---|---|---|
| *In MIB-2 Discards* | The number of inbound packets which were chosen to be discarded even though no errors had been detected. (MIB-2 variable). | Discard packets to free up buffer space. |
| *In MIB-2 Errors* | The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol (MIB-2 variable). | All network errors. |
| *In Runt* | Packet below minimum allowed media size. | Transmitter or synchronization error. |
| *In Unknown Proto* | The number of packets received via the interface which were discarded because of an unknown or unsupported protocol. | Unknown or unsupported protocol. |
| *Out Abort* | Receiver aborted transmission of packet. | Clocking problems. |
| *ifOutBabl* | Packet above maximum allowed media size. | Transmitter or synchronization error. |
| *Out CarLoss* | Carrier loss. | Line error or loss. |
| *Out Late Colln* | Packet caused collision outside of protocol specifications. | Transmitter error, cable fault, network too long. |
| *Out MIB-2 Discards* | The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. (MIB-2 variable). | Discard packets to free up buffer space. |
| *Out MIB-2 Errors* | The number of outbound packets that could not be transmitted because of errors. (MIB-2 variable). | All network errors. |
| *Out SQE Test* | Unable to determine if packet caused collision. | Transmitter or line error. |
| *ifProcessErr* | Not implemented in this release. | |

Table 20 MIB Fault Type Variables

## Customize Ticker Chart

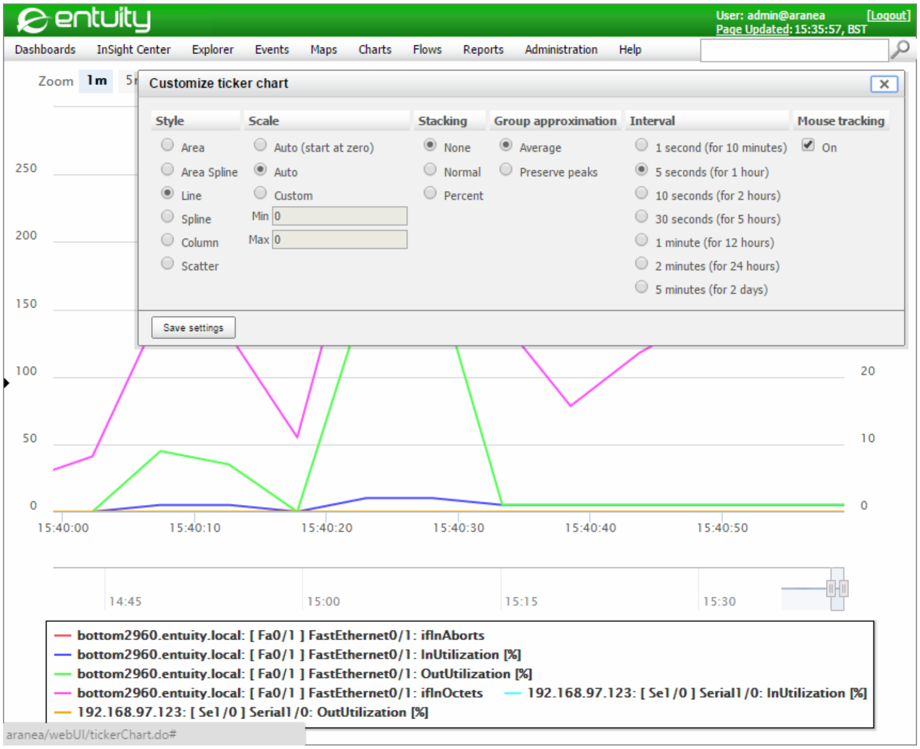
From the Customize Ticker chart popup you can amend how the data is displayed.

You can open the Customize chart popup:

1) From the Ticker chart click the Customize icon 🔧 .

| Attribute | Description |
|---|---|
| Style | Chart Type. |
| Scale | Sets the scale of the Y axis. |
| Stacking | Stacks variable values. |
| Group Approximation | Set to:<br>■ **Average** of a group of polls.<br>■ **Preserve peaks** to render a chart with preserve peaks when data-points get grouped. Effectively taking the maximum from a group. This may happen when the chart width is small comparing to the number of points that needs to be plotted. |
| Interval | Polling interval. |
| Mouse Tracking | Set to On Entuity displays information on that time point on the chart. |

Table 12-1Customize Ticker Chart



Customize ticker chart

| Style | Scale | Stacking | Group approximation | Interval | Mouse tracking |
|---|---|---|---|---|---|
| ○ Area | ○ Auto (start at zero) | ● None | ● Average | ○ 1 second (for 10 minutes) | ☑ On |
| ○ Area Spline | ● Auto | ○ Normal | ○ Preserve peaks | ● 5 seconds (for 1 hour) | |
| ● Line | ○ Custom | ○ Percent | | ○ 10 seconds (for 2 hours) | |
| ○ Spline | Min 0 | | | ○ 30 seconds (for 5 hours) | |
| ○ Column | Max 0 | | | ○ 1 minute (for 12 hours) | |
| ○ Scatter | | | | ○ 2 minutes (for 24 hours) | |
| | | | | ○ 5 minutes (for 2 days) | |

Save settings

User: admin@aranea [Logout]
Page Updated: 15:35:57, BST

aranea/webUI/tickerChart.do#

entuity
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Administration
Help
Zoom
1m
250
200
150
100
50
0
20
10
0
15:40:00
15:40:10
15:40:20
15:40:30
15:40:40
15:40:50
14:45
15:00
15:15
15:30
bottom2960.entuity.local: [ Fa0/1 ] FastEthernet0/1: ifInAborts
bottom2960.entuity.local: [ Fa0/1 ] FastEthernet0/1: InUtilization [%]
bottom2960.entuity.local: [ Fa0/1 ] FastEthernet0/1: OutUtilization [%]
bottom2960.entuity.local: [ Fa0/1 ] FastEthernet0/1: ifInOctets
192.168.97.123: [ Se1/0 ] Serial1/0: InUtilization [%]
192.168.97.123: [ Se1/0 ] Serial1/0: OutUtilization [%]

Figure 121 Customize Ticker Graph

## Using Ticker Charts

Once the main Ticker window is launched and Ticker has started collecting samples you can generate graphs from that data. Ticker allows you to generate graphs for any number of rows (i.e. ports or devices), and/or any number of columns (e.g a number of variables across a number of devices or ports).

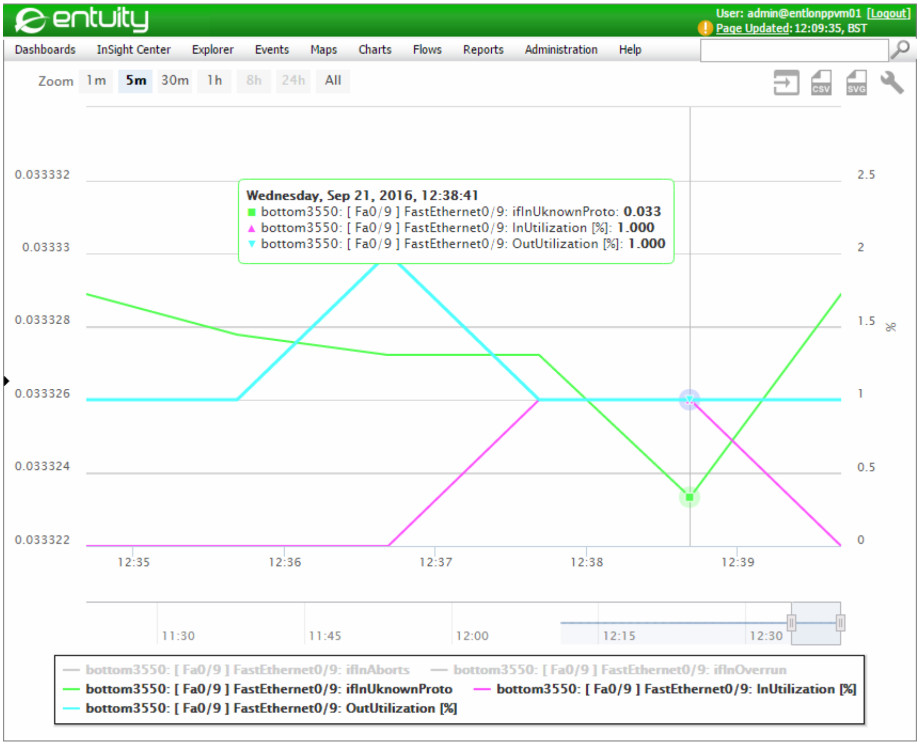
The generated graph displays the data displayed in the Ticker window, i.e. it shows the latest values in the specified data display mode. The link between the graph and the data in Ticker is maintained. In Ticker if you amend the display mode, e.g. display a variable's maximum values instead of minimum that change is also shown in the graph. Similarly, if you open a graph while Ticker is still collecting data, Ticker updates the graph as each new sample is taken.

To generate a Ticker graph:

1) Highlight the values for which you want to generate the graph.

2) Click Ticker Graph. Entuity opens a new window that contains the graph.

3) When you move your mouse, Entuity changes the details displayed in the grey box to reflect the position of your cursor on the graph.



User: admin@entlonppvm01 [Logout]
Page Updated: 12:09:35, BST

Wednesday, Sep 21, 2016, 12:38:41
🟩 bottom3550: [ Fa0/9 ] FastEthernet0/9: ifInUknownProto: **0.033**
▲ bottom3550: [ Fa0/9 ] FastEthernet0/9: InUtilization [%]: **1.000**
▼ bottom3550: [ Fa0/9 ] FastEthernet0/9: OutUtilization [%]: **1.000**

entuity
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Administration
Help
Zoom
1m
5m
30m
1h
8h
24h
All
0.033332
0.03333
0.033328
0.033326
0.033324
0.033322
2.5
2
1.5
1
0.5
0
12:35
12:36
12:37
12:38
12:39
11:30
11:45
12:00
12:15
12:30
bottom3550: [ Fa0/9 ] FastEthernet0/9: ifInAborts
bottom3550: [ Fa0/9 ] FastEthernet0/9: ifInOverrun
bottom3550: [ Fa0/9 ] FastEthernet0/9: ifInUknownProto
bottom3550: [ Fa0/9 ] FastEthernet0/9: InUtilization [%]
bottom3550: [ Fa0/9 ] FastEthernet0/9: OutUtilization [%]

Figure 122 Ticker Realtime Graph

By default all variables are plotted as a line chart, but data can also be plotted as a bar chart.

You can control which variables are displayed on the chart:

1) From the Key you can see that each variable is color coded.

2) Click on the attribute to remove the variable’s data from the chart. This also grays out the attribute in the Key.

3) To redisplay a hidden variable in the chart show click on the grayed out Key description.

## Open Chart in new Browser Window

You can open the current chart in a new window of the browser:

1) From the Ticker chart click New Window icon ⇥ .

## Exporting Ticker Sampled Data

You can export data from the Ticker chart to CSV and SVG format files:

1) From the Ticker chart click:

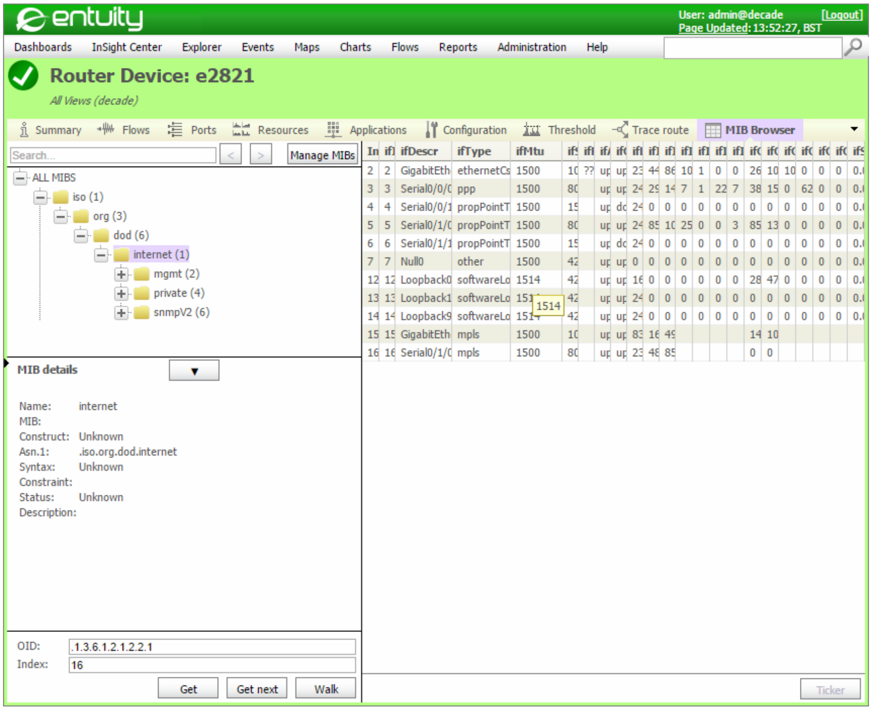
- CSV icon CSV to download the chart data to the browser Download folder.
- SVG icon SVG to download the chart as a SVG file to the browser Download folder.

# 13 MIB Browser

MIB Browser is available as a tab in Explorer for devices Entuity manages using SNMP. MIB Browser is not available for Ping-only, VM Platforms and Custom device types. Administrators and users with the MIB Browser permission have access to the MIB Browser.

MIB Browser:

- Has a user-editable *Index* allowing you to specify the index at which to start browsing the MIB. The **Get Next** and **Walk** functions update the index to reflect the last item they returned.
- Has a Walk button which:
  - Effectively performs multiple Get Next operations on the selected OID(s) starting from the current specified index, until it reaches the end of the table, or for the next 100 rows, whichever comes sooner. The results are scrollable.
  - Erases the current results and re-populates the results table. The *index* updates with the index of the last item returned (Get Next acts the same way).
- Ticker button clears the current ticker chart, adds the selected OIDs to Ticker and displays the chart.
- Identifies OIDs in the results table that can be used with Ticker. The icon is placed in the column header.
- Ticker button is only available when the selected OID can be used with Ticker.
- Has a collapsible details panel, showing the details of the OID currently selected in the MIB tree.
- Has branches in the MIB tree, with a single child, will be automatically collapsed to save space.
- Will display No MIBs loaded when no MIBs are loaded.



Name: internet
MIB:
Construct: Unknown
Asn.1: .iso.org.dod.internet
Syntax: Unknown
Constraint:
Status: Unknown
Description:

OID: .1.3.6.1.2.1.2.2.1
Index: 16

| In | ifI | ifDescr | ifType | ifMtu | ifS | ifI | ifA | ifO | ifI | ifI | ifI | ifI | ifI | ifI | ifI | ifO | ifO | ifO | ifO | ifO | ifO | ifS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 2 | GigabitEth | ethernetCs | 1500 | 10 | ?? | up | up | 23 | 44 | 86 | 10 | 1 | 0 | 0 | 26 | 10 | 10 | 0 | 0 | 0 | 0.0 |
| 3 | 3 | Serial0/0/0 | ppp | 1500 | 80 | | up | up | 24 | 29 | 14 | 7 | 1 | 22 | 7 | 38 | 15 | 0 | 62 | 0 | 0 | 0.0 |
| 4 | 4 | Serial0/0/1 | propPointT | 1500 | 15 | | up | dc | 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0 |
| 5 | 5 | Serial0/1/0 | propPointT | 1500 | 80 | | up | up | 24 | 85 | 10 | 25 | 0 | 0 | 3 | 85 | 13 | 0 | 0 | 0 | 0 | 0.0 |
| 6 | 6 | Serial0/1/1 | propPointT | 1500 | 15 | | up | dc | 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0 |
| 7 | 7 | Null0 | other | 1500 | 42 | | up | up | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0 |
| 12 | 12 | Loopback0 | softwareLo | 1514 | 42 | | up | up | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 28 | 47 | 0 | 0 | 0 | 0 | 0.0 |
| 13 | 13 | Loopback1 | softwareLo | 151 | 42 | | up | up | 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0 |
| 14 | 14 | Loopback9 | softwareLo | 1514 | 42 | | up | up | 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.0 |
| 15 | 15 | GigabitEth | mpls | 1500 | 10 | | up | up | 83 | 16 | 49 | | | | | 14 | 10 | | | | | |
| 16 | 16 | Serial0/1/0 | mpls | 1500 | 80 | | up | up | 23 | 48 | 85 | | | | | 0 | 0 | | | | | |

Figure 123 MIB Browser

OIDs in the MIB browser's results pane have a context menu, with two options:

- **Show on chart** replaces the current ticker chart with the selected oid(s). This is the same as clicking the Ticker button.
- **Add to current chart** adds the selected OIDs to the current ticker chart.

All SNMP requests made by the MIB browser are sent using the management IP address, zone, and SNMP settings of the selected device, as specified via the Inventory Administration page.

## Monitor Custom OIDs through Ticker

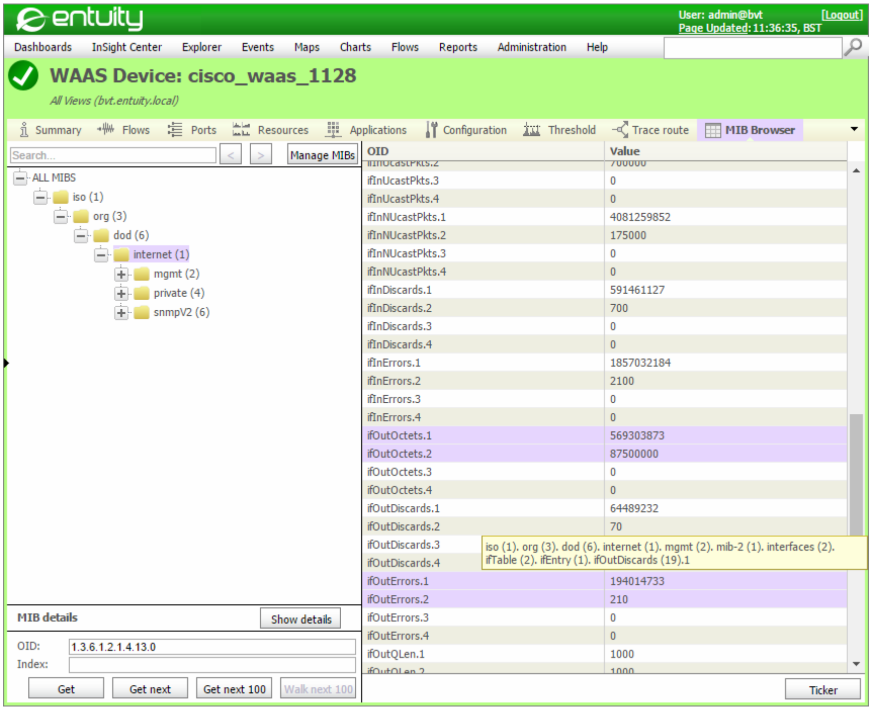
Through MIB Browser you can select OIDs to use to monitor the performance of a device. The realtime value of these OIDs can be charted through Ticker.

To use MIB Browser and Ticker to chart device OIDs:

1) From Explorer navigate to the MIB Browser tab of the device.

2) Use MIB Browser to interrogate the device.

3) Select the required OIDs.



WAAS Device: cisco_waas_1128

*All Views (bvt.entuity.local)*

OID: 1.3.6.1.2.1.4.13.0

Index:

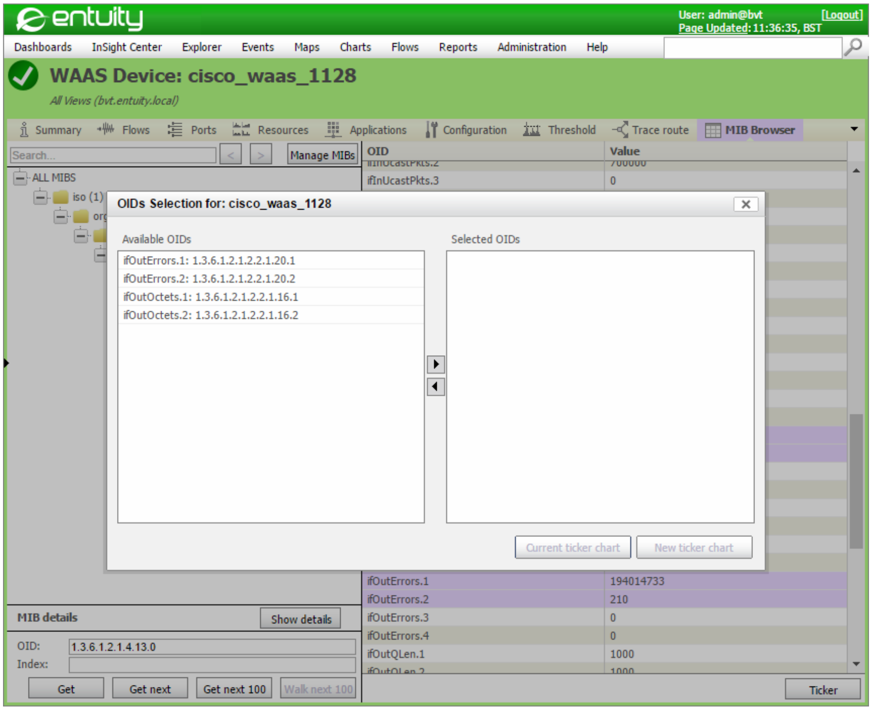
| OID | Value |
|---|---|
| ifInUcastPkts.2 | 700000 |
| ifInUcastPkts.3 | 0 |
| ifInUcastPkts.4 | 0 |
| ifInNUcastPkts.1 | 4081259852 |
| ifInNUcastPkts.2 | 175000 |
| ifInNUcastPkts.3 | 0 |
| ifInNUcastPkts.4 | 0 |
| ifInDiscards.1 | 591461127 |
| ifInDiscards.2 | 700 |
| ifInDiscards.3 | 0 |
| ifInDiscards.4 | 0 |
| ifInErrors.1 | 1857032184 |
| ifInErrors.2 | 2100 |
| ifInErrors.3 | 0 |
| ifInErrors.4 | 0 |
| ifOutOctets.1 | 569303873 |
| ifOutOctets.2 | 87500000 |
| ifOutOctets.3 | 0 |
| ifOutOctets.4 | 0 |
| ifOutDiscards.1 | 64489232 |
| ifOutDiscards.2 | 70 |
| ifOutDiscards.3 | |
| ifOutDiscards.4 | |
| ifOutErrors.1 | 194014733 |
| ifOutErrors.2 | 210 |
| ifOutErrors.3 | 0 |
| ifOutErrors.4 | 0 |
| ifOutQLen.1 | 1000 |
| ifOutQLen.2 | 1000 |

iso (1). org (3). dod (6). internet (1). mgmt (2). mib-2 (1). interfaces (2). ifTable (2). ifEntry (1). ifOutDiscards (19).1

Figure 124 Use MIB Browser to define OIDs for Ticker

4) Click **Ticker**.

5) Move the OIDs from the Available OIDs panel to the Selected OIDS panel.



Available OIDs:

- ifOutErrors.1: 1.3.6.1.2.1.2.2.1.20.1
- ifOutErrors.2: 1.3.6.1.2.1.2.2.1.20.2
- ifOutOctets.1: 1.3.6.1.2.1.2.2.1.16.1
- ifOutOctets.2: 1.3.6.1.2.1.2.2.1.16.2

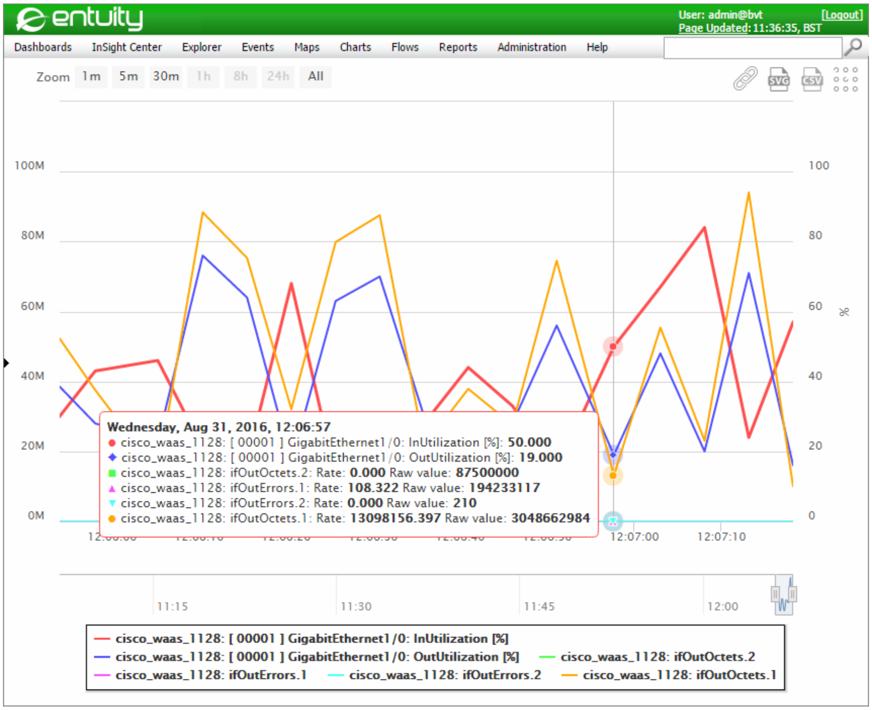
OID: 1.3.6.1.2.1.4.13.0

| OID | Value |
|---|---|
| ifInUcastPkts.2 | 700000 |
| ifInUcastPkts.3 | 0 |
| ifOutErrors.1 | 194014733 |
| ifOutErrors.2 | 210 |
| ifOutErrors.3 | 0 |
| ifOutErrors.4 | 0 |
| ifOutQLen.1 | 1000 |
| ifOutQLen.2 | 1000 |

Figure 125 MIB Browser

6) Click:

- **Current ticker chart** to add the OIDs to the current chart. This also removes the current history of that chart. All OIDs charted on a graph start from the same point in time.
- **New Ticker chart** to delete any existing ticker chart and create a new chart which only contains the currently selected OIDs.



**Wednesday, Aug 31, 2016, 12:06:57**

- ● cisco_waas_1128: [ 00001 ] GigabitEthernet1/0: InUtilization [%]: **50.000**
- ◆ cisco_waas_1128: [ 00001 ] GigabitEthernet1/0: OutUtilization [%]: **19.000**
- ■ cisco_waas_1128: ifOutOctets.2: Rate: **0.000** Raw value: **87500000**
- ▲ cisco_waas_1128: ifOutErrors.1: Rate: **108.322** Raw value: **194233117**
- ▼ cisco_waas_1128: ifOutErrors.2: Rate: **0.000** Raw value: **210**
- ● cisco_waas_1128: ifOutOctets.1: Rate: **13098156.397** Raw value: **3048662984**

— cisco_waas_1128: [ 00001 ] GigabitEthernet1/0: InUtilization [%]
— cisco_waas_1128: [ 00001 ] GigabitEthernet1/0: OutUtilization [%] — cisco_waas_1128: ifOutOctets.2
— cisco_waas_1128: ifOutErrors.1 — cisco_waas_1128: ifOutErrors.2 — cisco_waas_1128: ifOutOctets.1

Figure 126 Ticker Chart includes Standard and MIB Browser Origin OIDs

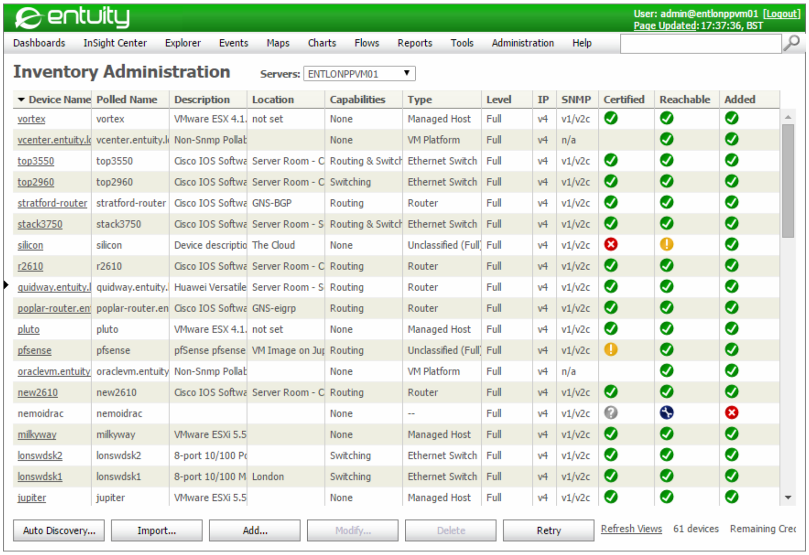
# 14 Inventory Administration

Precise, reliable inventory is the cornerstone of network management. There are three stages to Entuity fully managing a device:

1) Taking the device under management. Managing which devices are managed by an Entuity server is through the Inventory Administration page.

2) Discovering the objects associated with a managed object, for example CPUs, ports, power supply units. This identifies to Entuity the objects to poll.

3) Polling the device. Entuity gathers detailed device specifics down to the serial number, IOS versions and more. Data gathering methods include: SNMP polling, SYSLOG events, SNMP traps, ping, TCP port probing, ping-only availability monitoring and network flows.



User: admin@entlonppvm01 [Logout]
Page Updated: 17:37:36, BST

Inventory Administration

Servers: ENTLONPPVM01

| Device Name | Polled Name | Description | Location | Capabilities | Type | Level | IP | SNMP | Certified | Reachable | Added |
|---|---|---|---|---|---|---|---|---|---|---|---|
| vortex | vortex | VMware ESX 4.1. | not set | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| vcenter.entuity.lo | vcenter.entuity.l | Non-Snmp Pollab |  | None | VM Platform | Full | v4 | n/a |  | ✓ | ✓ |
| top3550 | top3550 | Cisco IOS Softwa | Server Room - C | Routing & Switch | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| top2960 | top2960 | Cisco IOS Softwa | Server Room - C | Switching | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| stratford-router | stratford-router | Cisco IOS Softwa | GNS-BGP | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| stack3750 | stack3750 | Cisco IOS Softwa | Server Room - S | Routing & Switch | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| silicon | silicon | Device descriptio | The Cloud | None | Unclassified (Full) | Full | v4 | v1/v2c | ✗ | ! | ✓ |
| r2610 | r2610 | Cisco IOS Softwa | Server Room - C | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| quidway.entuity.l | quidway.entuity. | Huawei Versatile | Server Room - S | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| poplar-router.en | poplar-router.en | Cisco IOS Softwa | GNS-eigrp | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| pluto | pluto | VMware ESX 4.1. | not set | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| pfsense | pfsense | pfSense pfsense | VM Image on Jup | Routing | Unclassified (Full) | Full | v4 | v1/v2c | ! | ✓ | ✓ |
| oraclevm.entuity | oraclevm.entuity | Non-Snmp Pollab |  | None | VM Platform | Full | v4 | n/a |  | ✓ | ✓ |
| new2610 | new2610 | Cisco IOS Softwa | Server Room - C | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| nemoidrac | nemoidrac |  |  | None | -- | Full | v4 | v1/v2c | ? | 🔧 | ✗ |
| milkyway | milkyway | VMware ESXi 5.5 |  | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| lonswdsk2 | lonswdsk2 | 8-port 10/100 Po |  | Switching | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| lonswdsk1 | lonswdsk1 | 8-port 10/100 M | London | Switching | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| jupiter | jupiter | VMware ESXi 5.5 |  | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |

61 devices Remaining Cre

Figure 127 Inventory Administration

Through the Inventory Administration page you can control which devices the Entuity server manages and have an overview of their current management status. By default only members of the Administrators user group have access to the Inventory Administration page, it is also their home page, however members of other user groups can be assigned inventory administration permissions.

You can place devices under Entuity management from the Inventory Administration page using one or more of these methods:

- Auto Discovery, where you enter parameters used by `autoDiscovery` to configure how `proliferate` finds devices on your network. As well as manually running `autoDiscovery` when you know you have devices to manage, you can also configure `autoDiscovery` to continually scan your network so that you always have an up-to-date, detailed inventory of network assets. (See *Adding Devices Using Auto Discovery*.)

- Import, to import a device (seed) file that lists devices together with their connection parameters. (See *Importing Devices Using a Device File*.)
- Add, to add individual devices to Entuity. This approach is most useful when only adding a few devices or when adding VM Platforms (VM Platforms have a different connection configuration to other device types). (See *Adding a Single Device*.)

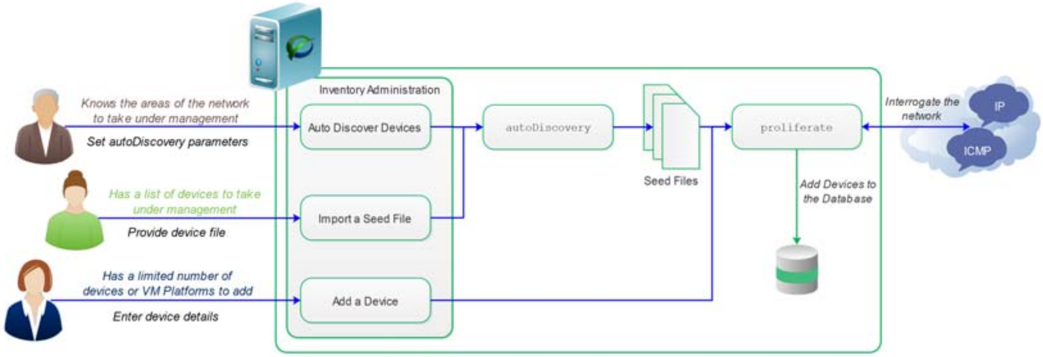

Knows the areas of the network to take under management
Set autoDiscovery parameters
Has a list of devices to take under management
Provide device file
Has a limited number of devices or VM Platforms to add
Enter device details
Inventory Administration
Auto Discover Devices
Import a Seed File
Add a Device
autoDiscovery
Seed Files
proliferate
Add Devices to the Database
Interrogate the network
IP
ICMP

Figure 128 Methods Available to Add Devices

When using Import and Auto Discovery you have the option of reviewing the discovered devices, inventory candidates, before adding them to Entuity. You can therefore select which candidate devices to add, you can also amend the management level of a device, change its device type.

After adding devices to Entuity you still can subsequently add, amend and delete managed objects from the Entuity inventory.

## Overview of Device Management

Every device under Entuity management is managed according to its management level, which is set when the device is added to Entuity. A device's default management level is partly determined by its device type. Entuity recognizes a device type through its sysOID, using it to associate the device with a device support dataset definition. These device support dataset definitions are defined in vendor files.

Each managed device has a licensing cost. (See the *Entuity Getting Started Guide*.)

### Device Preparation

For Entuity to manage most device types their management interface must be available to ICMP ping. For Entuity to collect SNMP data a device's SNMP agent must be correctly configured, allowing Entuity to collect appropriate data using read-only access permission.

✓ VM Platforms are not managed through SNMP polling but through different types of connection sets. The Amazon Web Services (AWS) VM Platform is not available to ICMP Ping.

Out of the box Entuity offers a wide range of managed device data models, these device support datasets are delivered through vendor files. Device support datasets define the attributes of each managed element, its device type, its possible dependencies in relation to other elements of the network, and the specific details to retrieve for each element. This comprehensive library streamlines modeling and ultimately shows exactly what you own, where it is deployed and how it is connected.

Current inventory information is available for use in different areas of Entuity, e.g. maintaining the network's topology maps, showing the interconnectivity of devices and enabling dependable root cause analysis.

## Device Management Levels

Entuity manages devices using one of the management levels. The management interface of all devices under Entuity management must be available to ICMP Ping. Entuity uses ping information to calculate reachability and latency information for the device. When the management interface has ping disabled Entuity reports latency and reachability as Unknown.

| Level | Description |
|---|---|
| **Full** | Entuity fully manages the device and all of its interfaces. |
| **Full (Mgmt Port Only)** | Entuity fully manages the device but only manages the management interface. |
| **Full Management (No Ports)** | Entuity fully manages the device but does not maintain any port level information. |
| **Basic** | Entuity collects only basic system information and the full IP address table via SNMP. This management level is used when Entuity does not have the appropriate vendor file, cannot generate an appropriate file or you only want the device placed under basic management. |
| **Ping Only** | Entuity does not collect SNMP data for these devices, it only reports whether these devices respond to ICMP ping. |
| **None** | Entuity does not manage the device. None is only available with the Custom Device device type, which is used to represent devices in Entuity that are not managed by Entuity. |

Table 13 Device Management Levels

✓ When `autoDiscovery` finds VMs and their hypervisors which have SNMP installed Entuity assigns them a device type of Managed Host and management level of Full. After adding the the device to Entuity you should modify the device type to VM Platform and specify its connection details.

Management level is set when adding the device. You can subsequently modify it through the Modify dialog available from the Inventory Administration.

### Certified Device Management

Fully managed devices can have a certified status of certified or uncertified.

A certified device is one where the device has an associated device support dataset created by Entuity Support. This definition is stored in `bin.vendor`. A certified device support dataset ensures the device MIB is appropriately interrogated by Entuity and that the device is assigned the appropriate Entuity device type.

An uncertified device is one where `proliferate` has automatically created a device vendor file that contains the device support dataset. When the device is similar to a device for which Entuity has a certified device support dataset, the new vendor file may be a very good fit.

Entuity can create vendor files when you first take a device under management. However every time you run `configure` Entuity re-checks devices and their associated vendor files and if a vendor file is missing Entuity creates an uncertified version. A vendor file may be missing, for example because the device has been replaced with a newer model but details such as the hostname, IP address and SNMP community were retained. Entuity continues managing and polling the device.

An uncertified vendor file does not have an associated device type, you would have to manually assign it. (See *Modifying Attributes of Discovered Devices*.) An uncertified vendor is an interim solution:

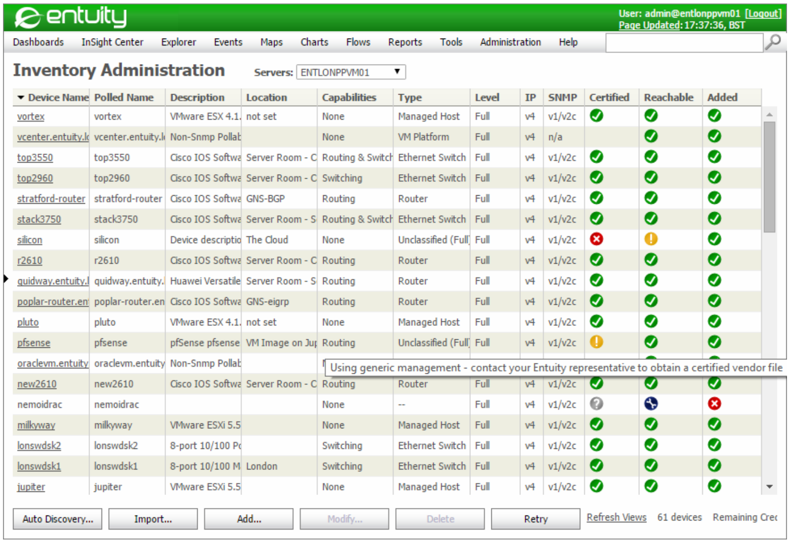
1) You should provide an SNMP walk of the device to your Entuity representative and request a certified vendor file.

2) When you receive the vendor file copy it to the *entuity_home*`\etc` and *entuity_home*`\etc\exotica` folders.

3) When you run next `configure` Entuity updates the device support dataset used with devices with that sysOID.

Entuity regularly updates `bin.vendor` with new device support datasets. If `bin.vendor` includes a device support dataset that was originally supplied in its own vendor file then during `configure` that vendor file is removed from the *entuity_home*`\etc` folder. The exception is with exotica vendor files, these files remain in place as they are used to override the default device dataset applied to a sysOID.

You can view the certified status of a device through the Inventory Administration page, Explorer device General Info section.



Inventory Administration

Servers: ENTLONPPVM01

| Device Name | Polled Name | Description | Location | Capabilities | Type | Level | IP | SNMP | Certified | Reachable | Added |
|---|---|---|---|---|---|---|---|---|---|---|---|
| vortex | vortex | VMware ESX 4.1. | not set | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| vcenter.entuity.l | vcenter.entuity.l | Non-Snmp Pollab |  | None | VM Platform | Full | v4 | n/a |  | ✓ | ✓ |
| top3550 | top3550 | Cisco IOS Softwa | Server Room - C | Routing & Switch | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| top2960 | top2960 | Cisco IOS Softwa | Server Room - C | Switching | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| stratford-router | stratford-router | Cisco IOS Softwa | GNS-BGP | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| stack3750 | stack3750 | Cisco IOS Softwa | Server Room - S | Routing & Switch | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| silicon | silicon | Device descriptio | The Cloud | None | Unclassified (Full) | Full | v4 | v1/v2c | ✗ | ! | ✓ |
| r2610 | r2610 | Cisco IOS Softwa | Server Room - C | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| quidway.entuity.l | quidway.entuity.l | Huawei Versatile | Server Room - S | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| poplar-router.ent | poplar-router.en | Cisco IOS Softwa | GNS-eigrp | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| pluto | pluto | VMware ESX 4.1. | not set | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| pfsense | pfsense | pfSense pfsense | VM Image on Jup | Routing | Unclassified (Full) | Full | v4 | v1/v2c | ! | ✓ | ✓ |
| oraclevm.entuity | oraclevm.entuity | Non-Snmp Pollab |  |  |  |  |  |  |  |  |  |
| new2610 | new2610 | Cisco IOS Softwa | Server Room - C | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| nemoidrac | nemoidrac |  |  | None | -- | Full | v4 | v1/v2c | ? | 🔧 | ✗ |
| milkyway | milkyway | VMware ESXi 5.5 |  | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| lonswdsk2 | lonswdsk2 | 8-port 10/100 Po |  | Switching | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| lonswdsk1 | lonswdsk1 | 8-port 10/100 M | London | Switching | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| jupiter | jupiter | VMware ESXi 5.5 |  | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |

Using generic management - contact your Entuity representative to obtain a certified vendor file

61 devices Remaining Crec

Figure 129 Generic Device Support

## Device Type Management

Entuity uses device type to identify the type of information that should be collected from a managed object, and then how that object and its information should be presented in Entuity. For example the type of information collected for a load balancer has significant differences to the type of information collected for a VM platform, although there will be some attributes common to both.

For those managed devices that Entuity cannot identify as a known device type, Entuity sets their device type to **Unclassified**. Basic and Ping Only devices are always considered Unclassified, Entuity also sets uncertified fully managed devices to device type Unclassified.

You can view the device type of a device through the Inventory Administration page and its Explorer Advanced tab. You can manually assign these devices an appropriate device type when adding them to Entuity or by modifying their attributes.

| Device Type | Description |
|---|---|
| Auto | An option available when adding a device. This instructs Entuity to associate an appropriate device type to the device using its vendor database. |
| Autonomous WAP | Enables the collection of additional wireless information for devices supporting the IP-MB, IF-MIB and the IEEE802.11-MIB. |
| Base Station | Satellite Base Station device. |
| Blade Center | Enables additional support for IBM and HP Blade Center devices. |
| Custom Device | Can be used to represent devices not managed by Entuity. It is used with the None management level. |

Table 14 Entuity Device Types

| Device Type | Description |
|---|---|
| Ethernet Switch | Allows collection of standard network information. |
| Firewall | Enables collection of additional Firewall information for |
| Load Balancer | Enable support for A10, Cisco, Citrix, F5 and Radware Alteon Load Balancers |
| Managed Host | Enables support for the HOST-RESOURCES-MIB (RFC 2790). |
| Matrix Switch | Enables the collection of max installable ports for the Apcon Matrix Switches |
| Multiplexer | Allows the classification of multiplexer devices, there are no additional attributes. |
| PoE Midspan Injector | Collects PoE information on Cisco-PAE-MIB (RFC 3621). |
| Router | Allows the collection of standard router metrics. |
| SSL Proxy | Enables the collection of the proxy service certificate expiration time interval from the CISCO-SSL-PROXY-MIB. |
| Uninterruptible Power Supply | Allows the device to be classified as an UPS. |
| VM Platform | Enables support for VMware, Oracle and Amazon Virtualized Platforms. |
| VPN | Supports the Cisco-IPsec-Flow-Monitor-MIB, Juniper-IVE-MIB and Shiva-VPN-System-MIB. |
| Wide Area Application Service | Adds support for Cisco's Actona-Actastor-MIB. |
| Wireless Controller | Supports the Cisco's Airespace-wireless-mib, Juniper's Trapeze-Network-Root-mib, Aruba's WLSX-Switch-MIB and Cisco-LWAP-wireless-LAN-MIB. |

Table 14 Entuity Device Types

## Custom Device Type

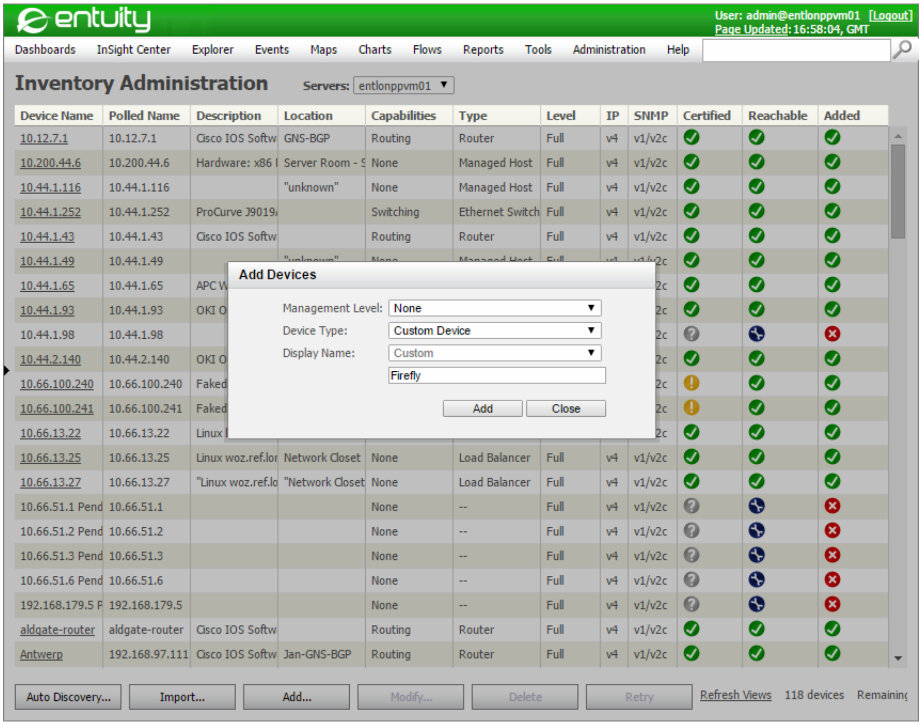
You can use the Custom Device device type to represent devices that Entuity is not managing but you want represented within Entuity. Entuity does not poll the device and therefore cannot verify the validity of a device definition. You can therefore define arbitrary Custom Devices however you should remember a Custom Device is part of your device inventory; it can be added to views, appear on maps, is part of inventory reports.

Custom Devices:

- Can be added from:
  - The Inventory Administration page by clicking **Add** and using the Add Devices dialog.
  - A map and from its context menu by clicking **Add Custom Device** and using the Add Devices dialog.
- Are not polled. On a map they do not have a background color.
- Do not have an IP address.
- Do not cost a device license credit but they are part of the main network inventory.

| Attribute | Description |
|---|---|
| *Device Type* | Custom Device. |
| *Management Level* | None. |
| *Icon* | Custom device icon. |
| *Display Name* | Custom. |

Table 15 Custom Device Attributes



Inventory Administration

Servers: entlonppvm01

| Device Name | Polled Name | Description | Location | Capabilities | Type | Level | IP | SNMP | Certified | Reachable | Added |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.12.7.1 | 10.12.7.1 | Cisco IOS Softw | GNS-BGP | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.200.44.6 | 10.200.44.6 | Hardware: x86 I | Server Room - S | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.44.1.116 | 10.44.1.116 | | "unknown" | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.44.1.252 | 10.44.1.252 | ProCurve J9019/ | | Switching | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.44.1.43 | 10.44.1.43 | Cisco IOS Softw | | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.44.1.49 | 10.44.1.49 | | "unknown" | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.44.1.65 | 10.44.1.65 | APC W | | | | | | 2c | ✓ | ✓ | ✓ |
| 10.44.1.93 | 10.44.1.93 | OKI O | | | | | | 2c | ✓ | ✓ | ✓ |
| 10.44.1.98 | 10.44.1.98 | | | | | | | 2c | ? | ● | ✗ |
| 10.44.2.140 | 10.44.2.140 | OKI O | | | | | | 2c | ✓ | ✓ | ✓ |
| 10.66.100.240 | 10.66.100.240 | Faked | | | | | | 2c | ! | ✓ | ✓ |
| 10.66.100.241 | 10.66.100.241 | Faked | | | | | | 2c | ! | ✓ | ✓ |
| 10.66.13.22 | 10.66.13.22 | Linux l | | | | | | 2c | ✓ | ✓ | ✓ |
| 10.66.13.25 | 10.66.13.25 | Linux woz.ref.lor | Network Closet | None | Load Balancer | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.66.13.27 | 10.66.13.27 | "Linux woz.ref.lo | "Network Closet | None | Load Balancer | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.66.51.1 Pend | 10.66.51.1 | | | None | -- | Full | v4 | v1/v2c | ? | ● | ✗ |
| 10.66.51.2 Pend | 10.66.51.2 | | | None | -- | Full | v4 | v1/v2c | ? | ● | ✗ |
| 10.66.51.3 Pend | 10.66.51.3 | | | None | -- | Full | v4 | v1/v2c | ? | ● | ✗ |
| 10.66.51.6 Pend | 10.66.51.6 | | | None | -- | Full | v4 | v1/v2c | ? | ● | ✗ |
| 192.168.179.5 F | 192.168.179.5 | | | None | -- | Full | v4 | v1/v2c | ? | ● | ✗ |
| aldgate-router | aldgate-router | Cisco IOS Softw | | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| Antwerp | 192.168.97.111 | Cisco IOS Softw | Jan-GNS-BGP | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |

Add Devices

Management Level: None

Device Type: Custom Device

Display Name: Custom

Firefly

118 devices Remaining

Figure 130 Add A Custom Device

## IPv4 and IPv6 Device Management

IPv4 is the most widely deployed internet protocol. It is available on the majority of devices Entuity manages and when available Entuity Support recommend you manage those devices through their IPv4 management address. IPv4 management is the default option and provides access to the full Entuity management tool-set. However for devices with IPv6 support you can instruct Entuity to manage them through their IPv6 management address. Management of IPv6 devices is fully integrated within Entuity although there are differences, for example:

- When taking devices under management `autoDiscovery` is IPv4 specific; the large number of addresses possible with IPv6 mean it is more appropriate to individually add IPv6 devices to Entuity or import them through a device file.
- How Entuity determines device availability when:
  - All IP addresses on the device are IPv4 Entuity uses the availability, or otherwise, of all IPv4 addresses.
  - All IP addresses on the device are IPv6 Entuity uses the availability, or otherwise, of the management IPv6 address only.
  - There is a mix of IPv4 and IPv6 addresses on the device Entuity uses the availability, or otherwise, of all of the IPv4 addresses and the management IPv6 address.
- IPv6 managed devices that also have IPv4 deployed and accessible to Entuity return a greater depth of data, for example on port availability and can also work with application monitoring and, where there is IPv4 access back to the Entuity server, the Configuration Monitor module.

When using Configuration Manager with only IPv6 devices then during `configure` you can set *Transfer Server IP Address* to the IPv6 IP address of the Entuity server.

- Trap handling of IPv6 addresses in general, and especially in relation to third party integrations may require more customizations than handling traps with IPv4 addresses.
- You should activate the IPv6 module. The module extends support to:
  - Finding port IPv6 addresses, for both IPv4 and IPv6 managed devices.
  - Utilize the IPv6 Neighbor Discovery (ND) protocol, with Maps including the IPv6 ND link type.

### Inventory Management Permissions

Administrators have full access to Entuity inventory management tools. For non-administrators, your level of access to these tools is determined by the level of permissions assigned to the user groups of which you are a member. There are three sets of permissions:

- Auto Discovery Administration, permits you to run `autoDiscovery` from the Inventory Administration page, you must also have the Inventory Administration permission.
- Inventory Administration, allows access to the functionality available through the Inventory Administration menu, e.g. View Devices, Add Devices, Delete Devices.
- Inventory Snapshots Administration, allows you to take snapshots of the selected view’s inventory, which are used with the Inventory Change report.

Administrators set tool permissions through the Account Management page.

## Entuity Device Connection Attributes

Entuity has two forms of connect definitions it can call on when connecting to managed devices. Entuity manages:

- The majority of its devices through SNMP using a standard set of attributes. (See *Attributes Entuity Uses to Manage Devices*.)
- Virtual machines through their VM platform SDK, and this requires a particular set of connection specifications. (See *Attributes Entuity Uses to Manage VM Platforms*.)

## Attributes Entuity Uses to Manage Devices

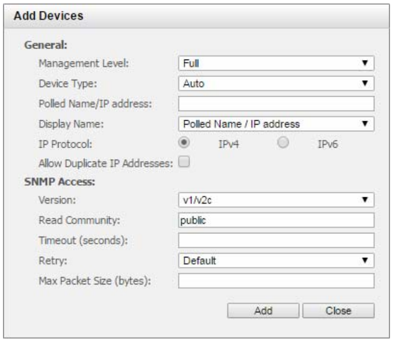
Entuity manages the majority of its devices through SNMP using a standard set of attributes. Devices managed through Ping Only only use a subset of these attributes, i.e. *IP Protocol*, *Device Type*, *Management Level*.

| Name | Description |
|---|---|
| *Management Level* | The default level of device management, i.e. **Full**, **Full (Mgmt Port Only)**, **Full Management (No Ports)**, **Basic**, **Ping Only**. |
| *Device Type* | The particular device or **Auto** for Auto Discovery to determine the device type. |
| *Polled Name/IP address* | The device name (which must be resolvable on the Entuity server) or IP address Entuity uses to poll the device. |
| *Display Name* | Device name Entuity displays within the product. (See *Device Display Name*.) |
| *IP Protocol* | IP version of the device, i.e. IPv4 (default) or IPv6. |
| *SNMP Access* | |
| *Allow Duplicate IP Addresses* | Select to permit the addition of a device with the same IP address as one already managed. |
| *Version* | SNMP version enabled on the device, i.e. SNMP v1/v2c, SNMP v2c, SNMP v3. |
| *Read Community* | SNMP read community string, by default **Public**. |
| *Write Community* | SNMP write community string. It is only set through the Modify Device dialog available from the Inventory Administration page. You can select multiple devices and set the same community string for all of them.<br>Write community strings are used with the Entuity IP SLA IOS Module. |
| *Timeout (sec)* | SNMP timeout time in seconds. |
| *Retry* | Number of SNMP retries. |

Table 16 Attributes Used to Manage Devices

| Name | Description |
|---|---|
| *Max Packet Size (bytes)* | To allow greater control over the maximum SNMP packet size Entuity uses when polling devices.The maximum size of SNMP PDUs can be limited on a per-device basis to accommodate SNMP agents with abnormally low PDU size limitations.<br>By default the maximum SNMP PDU size is 1408bytes, configurable through `entuity.cfg`. For some devices this is too large and causes polling to fail. Entuity includes a new configuration file, `snmpMaxPDUOverrides.cfg`, which contains a list of sysOids each with their own PDU size. These settings are automatically applied to all matching devices. You can amend and extend the shipped settings through a site specific file.<br>Individual devices can have their maximum SNMP PDU size limit set via the web UI.<br>Control over the maximum SNMP packet size is particularly relevant when managing Cisco ASA devices. |
| *CLI Access* | Command Line Access (CLI) credentials are set directly against each device. They are set through the Modify Device dialog available from the Inventory Administration page. You can select multiple devices and set the same credentials for all of them. |
| *Method* | Access method either SSH or Telnet. |
| *Port* | Port used to connect to the device. |
| *Username* | User account used to access the device. |
| *Password1* | User account password. |
| *Password2* | User account password. |

Table 16 Attributes Used to Manage Devices



Add Devices

General:

Management Level: Full ▾

Device Type: Auto ▾

Polled Name/IP address:

Display Name: Polled Name / IP address ▾

IP Protocol: ● IPv4 ○ IPv6

Allow Duplicate IP Addresses: □

SNMP Access:

Version: v1/v2c ▾

Read Community: public

Timeout (seconds):

Retry: Default ▾

Max Packet Size (bytes):

Figure 131 Add Devices to Entuity

## Attributes Entuity Uses to Manage VM Platforms

Through the VM Platform device type Entuity currently manages:

- Oracle VM.

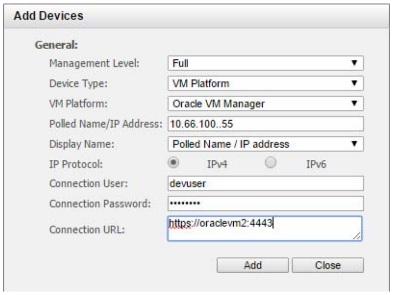
- Microsoft Hyper-V.
- VMware vCenter which also allows monitoring of that vCenter’s hypervisors and virtual machines. Although not the preferred method you can also manage the hypervisor through the VMware ESXi.
- Amazon Web Services (AWS).

The management of these virtual machines is through their VM platform SDK. Apart from AWS Entuity can discover these devices using `autoDiscovery` but it identifies them as Ping Only devices. To take these devices under full management you must modify their discovered attributes and specify their connection details. (See *Modifying Attributes of Discovered Devices*.)

There are product specific requirements:

- AWS is not discoverable by `autoDiscovery` as it is not available to either ICMP Ping or SNMP polling. AWS connection attributes include an access key and secret access key.
- Entuity manages Microsoft Hyper-V servers by remote Windows Management Instrumentation (WMI), therefore only Entuity servers installed to Windows can manage Microsoft Hyper-V servers.
- For Oracle VMs you have to specify security credentials. (See *Adding Oracle VM Managers to Entuity*.)

After discovering VM platforms, Entuity can discover their hypervisors and virtual machines. To allow this discovery you must ensure Entuity can communicate with the platform. For example, with Microsoft Hyper-V configure its firewall to allow remote Windows Management Instrumentation (WMI) from the Entuity server.



Add Devices

General:

Management Level: Full
Device Type: VM Platform
VM Platform: Oracle VM Manager
Polled Name/IP Address: 10.66.100..55
Display Name: Polled Name / IP address
IP Protocol: ● IPv4 ○ IPv6
Connection User: devuser
Connection Password: ••••••••
Connection URL: https://oraclevm2:4443

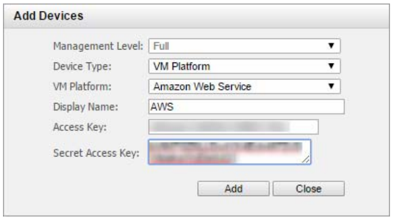
Figure 132 Entuity Add VM Platform

| Name | Description |
|---|---|
| *Device Type* | Assigned device type in Entuity, **VM Platform**. |
| *VM Platform* | VM Platform of the device, i.e. VMware vCenter / ESXi, Oracle VM Manager, Microsoft Hyper-V. |
| *IP Protocol* | Version of the IP Entuity uses when managing the device, i.e. IPv4, IPv6. |

Table 17 Attributes for VM Platform Discovery

| Name | Description |
|---|---|
| *Polled Name/IP address* | The device name (which must be resolvable on the Entuity server) or IP address Entuity uses to poll the device. |
| *Display Name* | Device name Entuity displays within the product. (See *Device Display Name*.) |
| *Connection User* | Valid username of the account Entuity uses to connect to the VM platform. |
| *Connection Passwd* | Valid password for connection user account. |
| *Connection URL* | URL Entuity uses when connecting to the VM's web API to manage the device. Ensure your URL does specify the VM platform's SDK, e.g. `https://blade/sdk`. |

Table 17 Attributes for VM Platform Discovery



Add Devices

Management Level: Full

Device Type: VM Platform

VM Platform: Amazon Web Service

Display Name: AWS

Access Key: [redacted]

Secret Access Key: [redacted]

Figure 133 Entuity Add AWS VM Platform

| Name | Description |
|---|---|
| *Device Type* | Assigned device type in Entuity, **VM Platform**. |
| *VM Platform* | VM Platform of the device, i.e. Amazon Web Services. |
| *Display Name* | Name of the AWS VM Platform. |
| *Access Key* | Access key identifier. |
| *Secret Access Key* | Secret access key.<br>*Access Key* and *Secret Access Key* together are the security credentials used to:<br>■ Check the sender of the API request.<br>■ Determine if the user making request has the required permission level. |

Table 18 Attributes for AWS VM Platform Discovery

## Device Display Name

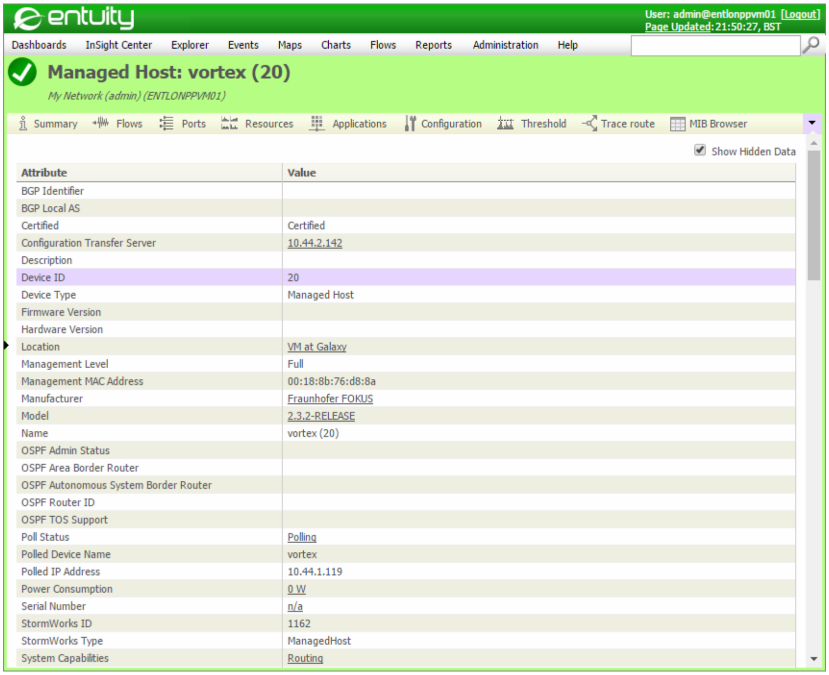
The device name Entuity displays within the product is separate from the identifier Entuity uses to poll the device. You can select from:

- **Polled Name/IP address** Entuity displays the identifier it uses to poll the device, for example as set in *Polled Name/IP address*.

- **System Name**, the administrator assigned name of the device.
- **IP Address**, the management IP address of the device.
- **ResolvableName**, the fully qualified resolved name of the device.
- **ResolvableNameFQ)** the fully qualified resolved name of the device.
- **Custom** to manually enter a device display name.

The device display name must be unique. When you:

- Attempt to add a device to Entuity and its name is the same as a device already under management Entuity does not add the device. Entuity raises an error message reporting the device has failed due to a duplicate name.
- Modify a device name Entuity checks that the new name is unique. If Entuity already has a device under management with that name then it appends to the name of the device you are modifying, in brackets, the device's *Device ID*. If this would make the device name longer than 59 characters then it reduces the name to 59 characters but retains the full *Device ID*.



Managed Host: vortex (20)

*My Network (admin) (ENTLONPPVM01)*

| Attribute | Value |
|---|---|
| BGP Identifier | |
| BGP Local AS | |
| Certified | Certified |
| Configuration Transfer Server | 10.44.2.142 |
| Description | |
| Device ID | 20 |
| Device Type | Managed Host |
| Firmware Version | |
| Hardware Version | |
| Location | VM at Galaxy |
| Management Level | Full |
| Management MAC Address | 00:18:8b:76:d8:8a |
| Manufacturer | Fraunhofer FOKUS |
| Model | 2.3.2-RELEASE |
| Name | vortex (20) |
| OSPF Admin Status | |
| OSPF Area Border Router | |
| OSPF Autonomous System Border Router | |
| OSPF Router ID | |
| OSPF TOS Support | |
| Poll Status | Polling |
| Polled Device Name | vortex |
| Polled IP Address | 10.44.1.119 |
| Power Consumption | 0 W |
| Serial Number | n/a |
| StormWorks ID | 1162 |
| StormWorks Type | ManagedHost |
| System Capabilities | Routing |

Figure 134 Device Identifier Appended to Display Name

When `updateNames` runs it reevaluates device names, for example to identify any change to resolved names or sysNames. (See *Entuity Reference Manual*.) If Entuity already has a device under management with that name then it appends to the name of the device you are modifying, in brackets, the device's *Device ID*. If this would make the device name longer than 59 characters then it reduces the name to 59 characters but retains the full *Device ID*.

Conversely if the name currently has the *Device ID* appended it should continue to do so, even if it is no longer required, e.g. the device with the conflicting name is not under Entuity management.

When Entuity derives a device name from a reverse DNS lookup or from the SNMP polled `sysName` it can potentially result in the same name as another managed device. How Entuity handles devices with duplicate names is dependent up on the context:

✓ `autoDiscovery` discards devices with duplicate names. When modifying or auto renaming device names Entuity appends to duplicate device names the device identifier within brackets if the device name without the identifier is not unique and it is not a custom name.

## Device Inventory Administration

The inventory administration options allow you to maintain the correspondence between the devices on your network, the device details held in the Entuity database and their presentation through Entuity views. You can:

- View, add and delete devices in the Entuity database.
- Modify device attributes.
- Refresh view membership.

You must be logged on as a user who is a member of the Administrators user group, or a user group with the inventory administration permissions, to add, amend and delete devices and refresh views.

### Best Practice

When possible you should manage devices through their management IP address. Devices managed through their IP address:

- Are not reliant on accurate DNS forward and reverse databases to manage devices.
- Are not reliant on a correctly configured DNS client.
- Are not reliant on Entuity being configured with the correct device hostnames.
- Allow specific selection of a loopback, using DNS may not offer as much control.
- Are not affected by DNS look up latency.
- Are not affected if DNS based load balancing or High Availability is in use.

Also during a network upgrade if you replace a device and retain the same hostname, but with a different IP address, Entuity can distinguish between the 2 devices.

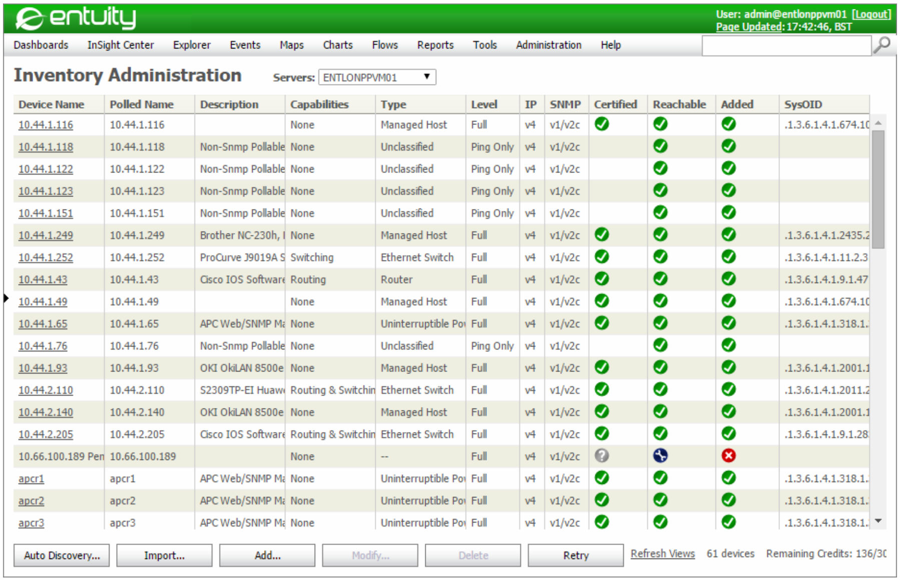
You can separately set the *Display Name* used within Entuity, for example to a device resolvable name, as it is separate from the identifier Entuity uses to poll the device. (See *Attributes Entuity Uses to Manage Devices*.)

## Viewing Devices Under Entuity Management

From the Inventory area of the web interface you can view device details:

1) Click **Administration** > **Inventory** / **Topology** > **Inventory Administration**.

   Entuity lists the devices, you can amend the sort order by clicking on the column headings. From the Inventory table headings you can open the context menu and select Configure Columns to control which columns are displayed.



User: admin@entlonppvm01 [Logout]
Page Updated: 17:42:46, BST

Inventory Administration

Servers: ENTLONPPVM01

| Device Name | Polled Name | Description | Capabilities | Type | Level | IP | SNMP | Certified | Reachable | Added | SysOID |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.44.1.116 | 10.44.1.116 | | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.674.10 |
| 10.44.1.118 | 10.44.1.118 | Non-Snmp Pollable | None | Unclassified | Ping Only | v4 | v1/v2c | | ✓ | ✓ | |
| 10.44.1.122 | 10.44.1.122 | Non-Snmp Pollable | None | Unclassified | Ping Only | v4 | v1/v2c | | ✓ | ✓ | |
| 10.44.1.123 | 10.44.1.123 | Non-Snmp Pollable | None | Unclassified | Ping Only | v4 | v1/v2c | | ✓ | ✓ | |
| 10.44.1.151 | 10.44.1.151 | Non-Snmp Pollable | None | Unclassified | Ping Only | v4 | v1/v2c | | ✓ | ✓ | |
| 10.44.1.249 | 10.44.1.249 | Brother NC-230h, I | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.2435.2 |
| 10.44.1.252 | 10.44.1.252 | ProCurve J9019A S | Switching | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.11.2.3 |
| 10.44.1.43 | 10.44.1.43 | Cisco IOS Software | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.9.1.47 |
| 10.44.1.49 | 10.44.1.49 | | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.674.10 |
| 10.44.1.65 | 10.44.1.65 | APC Web/SNMP Ma | None | Uninterruptible Pov | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.318.1. |
| 10.44.1.76 | 10.44.1.76 | Non-Snmp Pollable | None | Unclassified | Ping Only | v4 | v1/v2c | | ✓ | ✓ | |
| 10.44.1.93 | 10.44.1.93 | OKI OkiLAN 8500e | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.2001.1 |
| 10.44.2.110 | 10.44.2.110 | S2309TP-EI Huawe | Routing & Switchin | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.2011.2 |
| 10.44.2.140 | 10.44.2.140 | OKI OkiLAN 8500e | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.2001.1 |
| 10.44.2.205 | 10.44.2.205 | Cisco IOS Software | Routing & Switchin | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.9.1.28 |
| 10.66.100.189 Pen | 10.66.100.189 | | None | -- | Full | v4 | v1/v2c | ? | 🔧 | ✗ | |
| apcr1 | apcr1 | APC Web/SNMP Ma | None | Uninterruptible Pov | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.318.1. |
| apcr2 | apcr2 | APC Web/SNMP Ma | None | Uninterruptible Pov | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.318.1. |
| apcr3 | apcr3 | APC Web/SNMP Ma | None | Uninterruptible Pov | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | .1.3.6.1.4.1.318.1. |

Refresh Views 61 devices Remaining Credits: 136/30

Figure 135 Entuity Inventory Administration Page

| Attribute | Description |
|---|---|
| *Polled Name* | The device name (which must be resolvable on the Entuity server) or IP address Entuity uses to poll the device. |
| *Device Name* | Device name Entuity displays within the product. (See *Device Display Name*.) |
| *Description* | Manufacturer’s device description.This is only available with SNMP discovered devices. |
| *Location* | Description of the physical location of the device that is contained on the device, e.g. Development Cabinet. This is only available with SNMP discovered devices. |
| *Capabilities* | Indicates the device capabilities, i.e. **None**, **Unknown**, **Routing**, **Routing and Switching** |
| *Type* | Device type, e.g. **Router**, **Switch**, **Unclassified (Full)**, **VM Platform**. |

Table 19 Inventory Administration

| Attribute | Description |
|---|---|
| *Level* | Entuity allows you to manage devices using one of these levels, i.e. **Full**, **Full (Mgmt Port Only)**, **Full Management (No Ports)**, **Basic**, **Ping Only**. |
| *IP* | IP address Entuity uses to manage the device. |
| *SNMP* | Version of SNMP supported by the device. |
| *Certified* | Fully managed devices can be:<br>■ certified, have an associated vendor file created by Entuity Support. A certified vendor file ensures the device MIB is appropriately interrogated by Entuity, and that the device has the appropriate device type.<br>■ uncertified, `proliferate` has automatically created a vendor file. When the device is similar to a device for which Entuity has a certified vendor file, the new vendor file may be a very good fit. An uncertified vendor file would not assign the device type, you would have to manually assign it. (See *Modifying Attributes of Discovered Devices*.)<br>An uncertified vendor is an interim solution, you should request a certified vendor file from your Entuity representative to whom you should provide an SNMP walk of the device. |
| *Reachable* | Indicates whether the last attempt to ping the device was successful. |
| *Added* | Indicates whether the device is under Entuity management. |
| *Name Using* | Identifies the source of the device name displayed in Entuity. |
| *Management IP* | The device management IP address. |
| *SysOID* | The device sysOID Entuity uses to manage the device. |
| *Zone* | Name of the zone to which the device belongs. Zones are part of Entuity's support for overlapping IP addresses. |

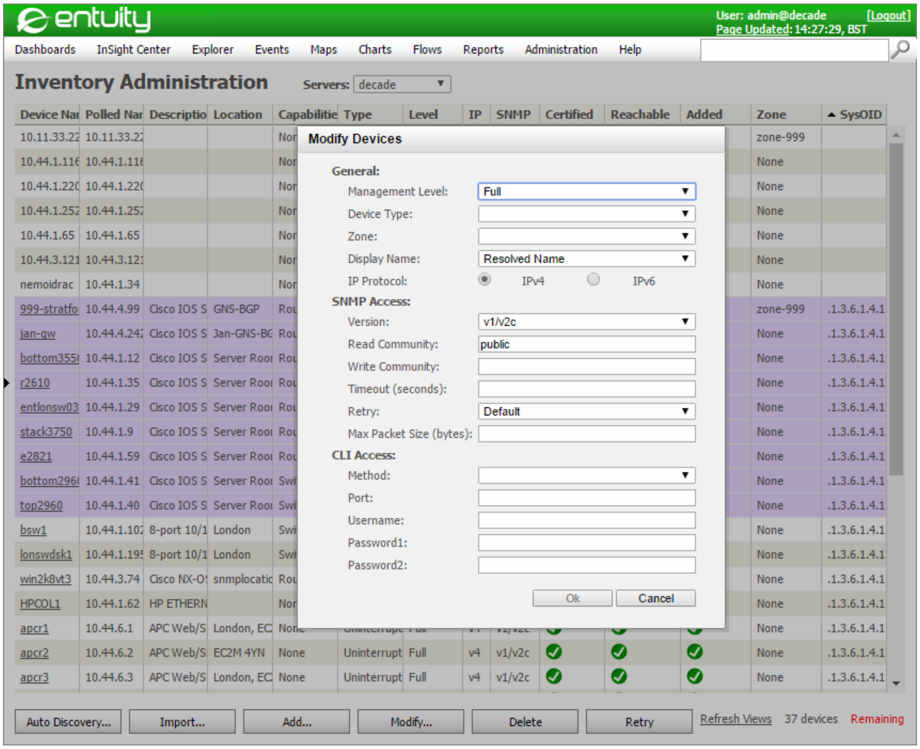
Table 19 Inventory Administration

## Modify Attributes Entuity uses to Manage a Device

You can modify the attributes Entuity uses to manage a device. You may have to modify these attributes, for example, when:

- Setting CLI access.

  You can set CLI details for multiple devices. For example to set the same access details for all Cisco devices display and then sort on the SysOID column. Highlight all of the Cisco devices and then click Modify.


entuity
User: admin@decade [Logout]
Page Updated: 14:27:29, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help

Inventory Administration

Servers: decade

| Device Nar | Polled Nar | Descriptio | Location | Capabilitie | Type | Level | IP | SNMP | Certified | Reachable | Added | Zone | ▲ SysOID |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.11.33.22 | 10.11.33.22 | | | Nor | | | | | | | | zone-999 | |
| 10.44.1.116 | 10.44.1.116 | | | Nor | | | | | | | | None | |
| 10.44.1.220 | 10.44.1.220 | | | Nor | | | | | | | | None | |
| 10.44.1.252 | 10.44.1.252 | | | Nor | | | | | | | | None | |
| 10.44.1.65 | 10.44.1.65 | | | Nor | | | | | | | | None | |
| 10.44.3.121 | 10.44.3.121 | | | Nor | | | | | | | | None | |
| nemoidrac | 10.44.1.34 | | | Nor | | | | | | | | None | |
| 999-stratfo | 10.44.4.99 | Cisco IOS S | GNS-BGP | Rou | | | | | | | | zone-999 | .1.3.6.1.4.1 |
| jan-gw | 10.44.4.242 | Cisco IOS S | Jan-GNS-BG | Rou | | | | | | | | None | .1.3.6.1.4.1 |
| bottom3550 | 10.44.1.12 | Cisco IOS S | Server Roo | Rou | | | | | | | | None | .1.3.6.1.4.1 |
| r2610 | 10.44.1.35 | Cisco IOS S | Server Roo | Rou | | | | | | | | None | .1.3.6.1.4.1 |
| entlonsw03 | 10.44.1.29 | Cisco IOS S | Server Roo | Rou | | | | | | | | None | .1.3.6.1.4.1 |
| stack3750 | 10.44.1.9 | Cisco IOS S | Server Roo | Rou | | | | | | | | None | .1.3.6.1.4.1 |
| e2821 | 10.44.1.59 | Cisco IOS S | Server Roo | Rou | | | | | | | | None | .1.3.6.1.4.1 |
| bottom2960 | 10.44.1.41 | Cisco IOS S | Server Roo | Swi | | | | | | | | None | .1.3.6.1.4.1 |
| top2960 | 10.44.1.40 | Cisco IOS S | Server Roo | Swi | | | | | | | | None | .1.3.6.1.4.1 |
| bsw1 | 10.44.1.102 | 8-port 10/1 | London | Swi | | | | | | | | None | .1.3.6.1.4.1 |
| lonswdsk1 | 10.44.1.195 | 8-port 10/1 | London | Swi | | | | | | | | None | .1.3.6.1.4.1 |
| win2k8vt3 | 10.44.3.74 | Cisco NX-O: | snmplocatic | Rou | | | | | | | | None | .1.3.6.1.4.1 |
| HPCOL1 | 10.44.1.62 | HP ETHERN | | Nor | | | | | | | | None | .1.3.6.1.4.1 |
| apcr1 | 10.44.6.1 | APC Web/S | London, EC | None | Uninterrupt | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | None | .1.3.6.1.4.1 |
| apcr2 | 10.44.6.2 | APC Web/S | EC2M 4YN | None | Uninterrupt | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | None | .1.3.6.1.4.1 |
| apcr3 | 10.44.6.3 | APC Web/S | London, EC | None | Uninterrupt | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | None | .1.3.6.1.4.1 |

Modify Devices

General:

Management Level: Full

Device Type:

Zone:

Display Name: Resolved Name

IP Protocol: ● IPv4 ○ IPv6

SNMP Access:

Version: v1/v2c

Read Community: public

Write Community:

Timeout (seconds):

Retry: Default

Max Packet Size (bytes):

CLI Access:

Method:

Port:

Username:

Password1:

Password2:

37 devices Remaining

Figure 136 Modify Attributes of Multiple Devices

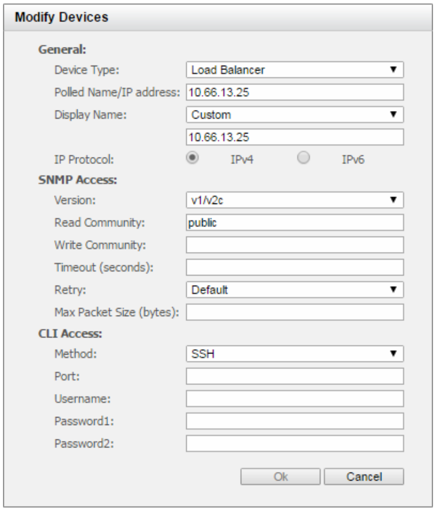
- The read community string on a device has changed.
- A device is only intermittently successfully polled by Entuity, you could extend SNMP timeout and retry values.
- A managed device has been replaced and the new device has inherited the old IP address. Therefore the device is under management but it is using for example, a different version of SNMP, a different vendor file.
- An incorrect device type is associated with a device, for example VM platforms running SNMP may be incorrectly identified as managed hosts.

To modify device attributes:

1) Click **Administration** > **Inventory** / **Topology** > **Inventory Administration**.

2) Highlight the required device and click **Modify**.

3) Amend the device attributes.



Modify Devices

General:

Device Type: Load Balancer ▼

Polled Name/IP address: 10.66.13.25

Display Name: Custom ▼

10.66.13.25

IP Protocol: ● IPv4 ○ IPv6

SNMP Access:

Version: v1/v2c ▼

Read Community: public

Write Community:

Timeout (seconds):

Retry: Default ▼

Max Packet Size (bytes):

CLI Access:

Method: SSH ▼

Port:

Username:

Password1:

Password2:

Figure 137 Modify Device Attributes

## Adding Devices Using Auto Discovery

You can configure autoDiscovery to call proliferate to search the network for devices to manage. It is most useful when you have many devices, or a potentially unknown set of devices, to manage. You can:

- Both schedule and manually run autoDiscovery.
- Configure autoDiscovery to search within set IP address ranges but also to not search in other IP address ranges.
- Configure autoDiscovery to exclude from discovery specified sysOIDs.
- Set device display name.
- Enter device authentication details.
- Set default behavior for management level, resolving IP to hostnames and determining displayed device name.

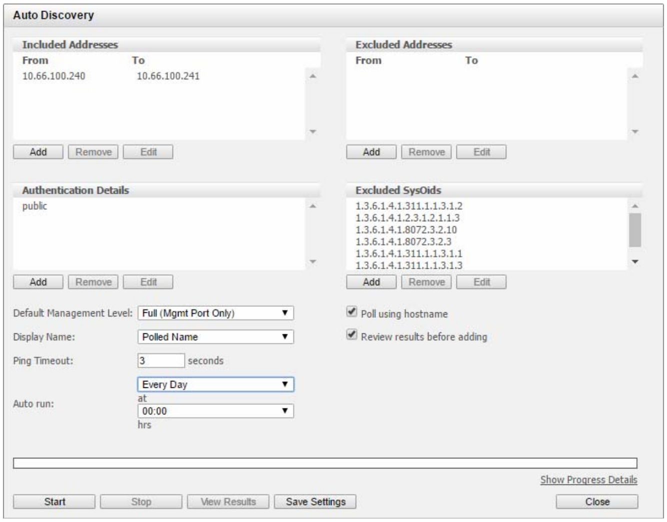
By default discovered devices are not immediately placed under management, although this is configurable, but are available for review through the Inventory Candidates page. Through the candidates page you can sort through suggested devices, for example, by their IPv4 or IPv6 management addresses.

Entuity recommend you only use Entuity to manage devices with statically assigned IP addresses. Although Entuity can manage devices that have dynamically assigned IP addresses, e.g. using DHCP, if the device’s IP address changes Entuity does not recognize the change until protean runs.

You can both schedule and manually run Auto Discovery. To run auto discovery:

1) Click **Administration** > **Inventory** / **Topology** > **Inventory Administration**.

2) From the Inventory Administration page click **Auto Discovery**.



Included Addresses

| From | To |
|---|---|
| 10.66.100.240 | 10.66.100.241 |

Excluded Addresses

| From | To |
|---|---|

Authentication Details

public

Excluded SysOids

1.3.6.1.4.1.311.1.1.3.1.2
1.3.6.1.4.1.2.3.1.2.1.1.3
1.3.6.1.4.1.8072.3.2.10
1.3.6.1.4.1.8072.3.2.3
1.3.6.1.4.1.311.1.1.3.1.1
1.3.6.1.4.1.311.1.1.3.1.3

Default Management Level: Full (Mgmt Port Only)

Display Name: Polled Name

Ping Timeout: 3 seconds

Auto run: Every Day at 00:00 hrs

☑ Poll using hostname

☑ Review results before adding

Figure 138 Set Auto Discovery Parameters

3) Specify the discovery parameters.

4) Click **Start**. Entuity runs Auto Discovery and you can track its progress by clicking:

- **Show Progress Details**.
- **Close**, to close the Auto Discovery dialog. Entuity displays the current progress of discovery as a hyperlink in the page banner. You can click on the hyperlink to re-open the dialog.

5) When Auto Discovery completes select **View Results** to view the devices discovered. Entuity displays the Inventory Candidates dialog.

These candidate devices are not managed by Entuity until you select their check boxes and add them to Entuity. (See *Viewing Candidate Devices*.)

6) Click **Add to inventory**. Entuity closes the Inventory Candidates page, displays the Inventory Administration page and starts adding the selected devices.

From the Inventory Administration page you can view the devices under Entuity management.

After running Auto Discovery, and not adding any devices to the inventory, Entuity warns that devices were not added. From the Inventory Administration page you can subsequently add devices by selecting **Auto Discovery**, **View Results** and then **Add to inventory**.

| Attribute | Description |
|---|---|
| *Included Addresses* | Specify the device, range of IP addresses and/or IP subnets for Auto Discovery to use when identifying devices for Entuity to take under management. You can include multiple rows of addresses, and on each row you have the option of entering:<br>■ A range of IP addresses, specifying the *From* and *To* values, for example 10.0.0.1 and 10.0.0.215 .<br>■ An IP address or device name.<br>■ IP subnet, specifying the *Prefix* and *Netmask* for example 10.0.0.1 and 255.255.255.0 which Entuity displays in From as 10.0.0.1/24 . |
| *Excluded Addresses* | Specify the device, range of IP addresses and/or IP subnets for Auto Discovery to use when excluding devices for Entuity to take under management. You can include multiple rows of addresses, and on each row you have the option of entering:<br>■ A range of IP addresses, specifying the *From* and *To* values, for example 10.0.0.1 and 10.0.0.215 .<br>■ An IP address or device name.<br>■ IP subnet, specifying the *Prefix* and *Netmask* for example 10.0.0.1 and 255.255.255.0 which Entuity displays in *From* as 10.0.0.1/24. |
| *Authentication Details* | Authentication details Entuity requires to manage the device.<br>For SNMPv1/v2 you should enter the device's SNMP community string, by default Public. Entuity expects devices to support both SNMPv1 and SNMPv2.<br>For SNMPv3 there are three levels of increasing security:<br>■ **noauth**, authenticates a packet by a string match of *User Name*.<br>■ **auth**, requires that you also complete *Authentication Type* and *Authentication Password*, i.e. respectively MD5 or SHA, and a password.<br>■ **priv**, requires that you also complete *Encryption Type* and *Encryption Password*, i.e. respectively DES,3DES, AES, AES192 or AES256, and a password. |
| *Excluded sysOIDs* | System object identifiers of devices that Entuity should not manage. |
| *Poll using hostname* | Select for Entuity to resolve device IP addresses to device hostnames. By default not selected.<br>Through *discovery.HostNameFormat* in `entuity.cfg` you can amend the device name format used by Entuity. By default Entuity attempts to poll a device using the qualified DNS device name, then an unqualified DNS device name and only then the device IP address. |
| *Review results before adding* | When:<br>■ **checked** (default), Entuity presents the list of discovered devices which you can then add, or not, to Entuity management<br>■ **unchecked**, Entuity automatically takes discovered devices under management. |

Table 20 Auto Discovery Parameters

| Attribute | Description |
|---|---|
| *Default Management Level* | Default level of device management, e.g. **Full** (default), **Basic**, **Ping Only**. |
| *Display Name* | Device name Entuity displays within the product. (See *Device Display Name*.) |
| *Ping Timeout* | Time in seconds auto discovery waits for a response from a ping before it times-out the ping, by default 3 seconds. |
| *Auto run* | Configure the scheduling of auto discovery. You can select:<br>■ **Never** (default), so auto discovery is only run manually.<br>■ **Every day**, to schedule auto discovery to run daily.<br>■ A particular day. |
| *at* | Time for scheduled auto discovery to run. |
| *Show Progress Details* | Select to view the progress of Auto Discovery. |

Table 20 Auto Discovery Parameters

Although 3DES, AES192 and AES256 are widely implemented encryption algorithms they are not included to the SNMP standard. Therefore a particular manufacturer's implementation of one or more of these technologies may not be supported by Entuity.

## Viewing Candidate Devices

Although you can configure `autoDiscovery` to automatically add devices to Entuity, by default after `autoDiscovery` completes you can view the discovered devices through the Inventory Candidates page. This page comprises of three tabs, each displaying a different category of results:

- SNMP tab displays all discovered devices that support SNMP.
- Non-SNMP tab displays discovered devices that only respond to ping and do not support SNMP.
- Not Responding tab displays for example devices imported through `autodisc.cfg` but have gone down or are now unreachable.

| Attribute | Description |
|---|---|
| *Device Name* | Resolved name of the device or IP address. |
| *IP* | IP address Entuity uses to manage the device. |
| *Description* | Manufacturers device description.This is only available with SNMP discovered devices. |
| *Location* | Description of the physical location of the device that is contained on the device, e.g. Development Cabinet. This is only available with SNMP discovered devices. |

Table 21 Candidate Device Details

| Attribute | Description |
|---|---|
| *Management Level* | Entuity allows you to manage devices using one of these levels, i.e. **Full**, **Full (Mgmt Port Only)**, **Full Management (No Ports)**, **Basic**, **Ping Only**. |
| *Inf* | Reports warnings received when polling the device, DNS failure, device already in inventory. |

Table 21 Candidate Device Details

## Modifying Attributes of Discovered Devices

When you use `autoDiscovery` to discover devices on your network by default Entuity does not automatically take them under management, instead you can review the devices through the Inventory Candidates panel. You can:

- Review and select or deselect the devices to add to Entuity.
- Modify the device *Management Level*.

You can also configure the Import device file function to allow inventory candidate review.

A candidate inventory review is important when taking VM Platforms and their hypervisors under management. When you have specified a device as a VM through a device file and entered its connection details then Entuity can readily assign to it the VM Platform device type. However, where Entuity has automatically determined the device type you must review the discovered device.

For example, when SNMP is installed on the VM platform, discovery assigns a device type, e.g. Managed Host and management level, e.g. Full which implies a device type using the standard set of connection attributes. If you add the device to Entuity with this management level the VM Platform device type would not be available. **Ping Only** ensures Entuity creates a record for the device that does not contain any SNMP connection attributes. Entuity communicates with VMs through their SDK and requires a different set of connection attributes to other device types. (See *Attributes Entuity Uses to Manage VM Platforms*.)

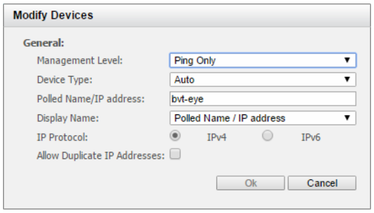
After adding a device to Entuity you can further modify the attributes Entuity uses to manage the device including *Device Type*, *Connection User*.

### Example: Modifying Device Management Level

To amend attributes of discovered devices, for example a VM platform:

1) From the Inventory Candidates panel select the check box of the device.
2) From *Management Level* select **Ping Only**.
3) Click **Add to inventory**. Entuity adds the device to the add to inventory queue and displays its details and status on the Inventory Administration page.

   The device has a *Type* of **Unclassified** and a management level of **Ping Only**.
4) From the Inventory Administration page select the check box of the device.
5) Click **Modify**. Entuity displays the Modify Devices dialog.



Modify Devices

General:

Management Level: Ping Only

Device Type: Auto

Polled Name/IP address: bvt-eye

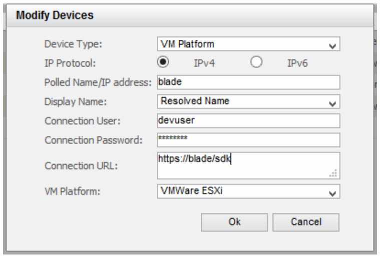
Display Name: Polled Name / IP address

IP Protocol: ● IPv4 ○ IPv6

Allow Duplicate IP Addresses: □

Figure 139 Modify Device Type

6) From *Device Type* select **VM Platform**.



Modify Devices

Device Type: VM Platform

IP Protocol: ● IPv4 ○ IPv6

Polled Name/IP address: blade

Display Name: Resolved Name

Connection User: devuser

Connection Password: ********

Connection URL: https://blade/sdk

VM Platform: VMWare ESXi

Figure 140 Modify VM Platform Attributes

7) Enter the VM Platform specific attributes and click **OK**.

## Adding Candidate Devices to Entuity

By default autoDiscovery does not automatically add devices to the Entuity server instead you can review them through the Inventory Candidates page. You can also configure the Import from device file function to have the same behavior.

To add candidate devices to Entuity:

1) Click **Administration** > **Inventory** / **Topology** > **Inventory Administration**.

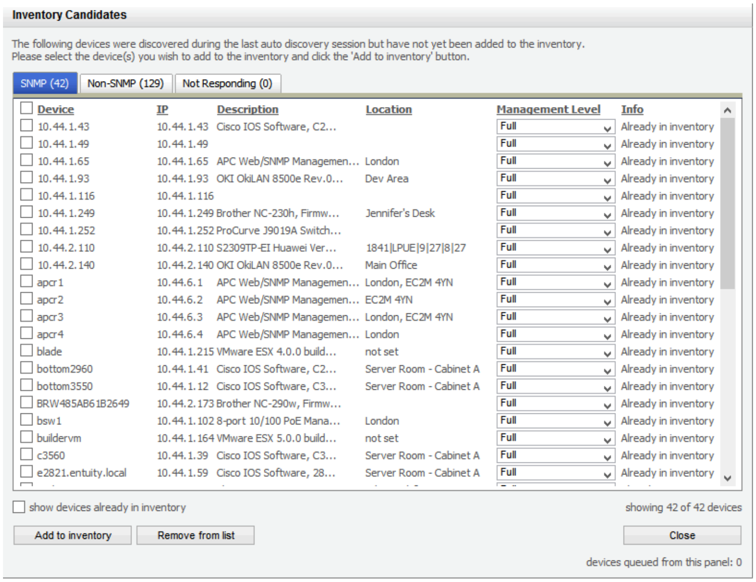
2) Click **Auto Discovery**.

3) Select **Results**. Entuity opens the Inventory Candidates page and displays the results of the last run of Auto Discovery.

4) Select the required tab, e.g. SNMP. By default all of the devices are selected, as indicated by a tick in the check box at the start of each row. You can deselect all devices by selecting the check box in the title row, and then check the check boxes of the devices you want to add to Entuity.

   You can also modify some attributes before adding the device to Entuity. (See *Modifying Attributes of Discovered Devices*.)

5) Select **Add to Inventory**. From the Inventory Administration page you can view the state of the devices as Entuity attempts to take them under management. Press **F5** to preempt the page’s own automatic progress update.



**Inventory Candidates**

The following devices were discovered during the last auto discovery session but have not yet been added to the inventory.
Please select the device(s) you wish to add to the inventory and click the 'Add to inventory' button.

| □ Device | IP | Description | Location | Management Level | Info |
|---|---|---|---|---|---|
| □ 10.44.1.43 | 10.44.1.43 | Cisco IOS Software, C2... | | Full | Already in inventory |
| □ 10.44.1.49 | 10.44.1.49 | | | Full | Already in inventory |
| □ 10.44.1.65 | 10.44.1.65 | APC Web/SNMP Managemen... | London | Full | Already in inventory |
| □ 10.44.1.93 | 10.44.1.93 | OKI OkiLAN 8500e Rev.0... | Dev Area | Full | Already in inventory |
| □ 10.44.1.116 | 10.44.1.116 | | | Full | Already in inventory |
| □ 10.44.1.249 | 10.44.1.249 | Brother NC-230h, Firmw... | Jennifer's Desk | Full | Already in inventory |
| □ 10.44.1.252 | 10.44.1.252 | ProCurve J9019A Switch... | | Full | Already in inventory |
| □ 10.44.2.110 | 10.44.2.110 | S2309TP-EI Huawei Ver... | 1841\|LPUE\|9\|27\|8\|27 | Full | Already in inventory |
| □ 10.44.2.140 | 10.44.2.140 | OKI OkiLAN 8500e Rev.0... | Main Office | Full | Already in inventory |
| □ apcr1 | 10.44.6.1 | APC Web/SNMP Managemen... | London, EC2M 4YN | Full | Already in inventory |
| □ apcr2 | 10.44.6.2 | APC Web/SNMP Managemen... | EC2M 4YN | Full | Already in inventory |
| □ apcr3 | 10.44.6.3 | APC Web/SNMP Managemen... | London, EC2M 4YN | Full | Already in inventory |
| □ apcr4 | 10.44.6.4 | APC Web/SNMP Managemen... | London | Full | Already in inventory |
| □ blade | 10.44.1.215 | VMware ESX 4.0.0 build... | not set | Full | Already in inventory |
| □ bottom2960 | 10.44.1.41 | Cisco IOS Software, C2... | Server Room - Cabinet A | Full | Already in inventory |
| □ bottom3550 | 10.44.1.12 | Cisco IOS Software, C3... | Server Room - Cabinet A | Full | Already in inventory |
| □ BRW485AB61B2649 | 10.44.2.173 | Brother NC-290w, Firmw... | | Full | Already in inventory |
| □ bsw1 | 10.44.1.102 | 8-port 10/100 PoE Mana... | London | Full | Already in inventory |
| □ buildervm | 10.44.1.164 | VMware ESX 5.0.0 build... | not set | Full | Already in inventory |
| □ c3560 | 10.44.1.39 | Cisco IOS Software, C3... | Server Room - Cabinet A | Full | Already in inventory |
| □ e2821.entuity.local | 10.44.1.59 | Cisco IOS Software, 28... | Server Room - Cabinet A | Full | Already in inventory |

□ show devices already in inventory

showing 42 of 42 devices

devices queued from this panel: 0

Figure 141 Adding Discovered Devices to Entuity

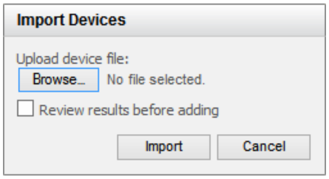
## Importing Devices Using a Device File

A device file allows you to compile a list of objects, by IP address or resolved name to add to Entuity. By default devices Entuity discovers using this seed file are automatically added to its inventory, although from the Import dialog you do have the option of amending the default so you can review the devices through the Inventory Candidates page.

To add devices to Entuity using a device file:

1) Click **Administration > Inventory / Topology > Inventory Administration**.

2) From the Inventory Administration page select **Import**. Entuity displays the Import Devices dialog.



**Import Devices**

Upload device file:

No file selected.

□ Review results before adding

Figure 142 Importing Devices Using a Seed File

3) In Upload device file, use browse to locate the device file on the client system that is hosting the browser.

4) Select **Review Results before Adding**, to review the devices in the Inventory Candidate page before they are added to Entuity.

5) Click **Import**. Entuity reads the file and compiles a candidate list of devices, displaying them in the Inventory Candidate dialog.

Entuity writes the new device file to *entuity_home*`\etc\deviceFiles`.

6) By default Entuity adds the devices in the seed file to its inventory. However when you selected to review the devices before adding them Entuity displays discovered devices in the Inventory Candidates page. Devices are displayed in one of three tabs:

   - **SNMP** for devices discovered through SNMP
   - **Non-SNMP** for devices discovered through Non-SNMP polling
   - **Not Responding** for devices not responding to polling.

   From each tab you can add devices to Entuity management; by default all discovered devices are selected and ready for addition.

   Click **Add to inventory**, to add the devices on the current tab to Entuity management.

7) From the Inventory Administration page you can view the devices under Entuity management.

## Defining A Device File

Before using the device file check that each of the devices responds to ICMP (Internet Control Message Protocol) Echo requests. For devices you want to manage at the Full or Basic management levels they must allow SNMP requests from the server with the provided community string. Ensure that there is no IP address or port management access list in operation for the devices that would prevent SNMP or ICMP replies from the devices to the Entuity server.

### SNMPv1/v2 Device File Format

It is necessary that all of the devices to be managed by Entuity are listed in the device file. For SNMPv1/2 devices the format is:

<*deviceIdentifier*>`[tab]`<*community string*>`[tab]`<*#optional comment*>

You can also specify a SNMPv1/2 device using the alternative format:

`-d` <*deviceIdentifier*>`[tab]-c` <*community string*>`[tab]`<*#optional comment*>

where:

- *deviceIdentifier* is the IP address or hostname that resolves to the IP address of the management interface on switches, and a single interface on a router.

  You should be able to resolve each of the device names into an IP address on the Entuity server using one of the following methods:

  - Static hosts file (e.g. `\etc\hosts`)
  - NIS (Network Information System) or NIS+
  - DNS (Domain Name System).

This resolution is not required if the device identifier is itself the IP address of the device. The choice of identifier is important as it is the primary method of identifying devices in Entuity.

- *Community String* is the read-only SNMP (Simple Network Management Protocol) community string required to read the MIB-II (Management Information Base-II) system group for the device, e.g. **public**.
- *Optional Comment* is a non-mandatory text string to help describe the device.

### SNMPv3 Device File Format

For SNMPv3 devices the format is:

`-d` *<deviceIdentifier>* `-u` *<UserName>* `-a MD5 -A` *<Auth passwd>* `-x DES -X` *<Privacy passwd>*

where:

- *-d*, indicates the following value is the device name.
- *deviceIdentifier* is the management interface on hubs and switches, and a single interface on a router. You should be able to resolve each of the device names into an IP address on the Entuity server using one of the following methods:
  - Static hosts file (e.g. `\etc\hosts`)
  - NIS (Network Information System) or NIS+
  - DNS (Domain Name System).

  This resolution is not required if the device identifier is itself the IP address of the device. The choice of identifier is important as it is the primary method of identifying devices in Entuity.
- *-u <UserName>*, requires a valid user name to access the device.
- *-a* MD5, sets the authentication protocol, valid values are MD5 (Message-Digest algorithm 5), SHA (Secure Hash Algorithm).
- *-A <Auth passwd>*, sets the authentication password, valid values must be between eight and thirty-two characters long. If the password contains spaces double quotes must be placed around the password.
- *-x DES*, sets the privacy protocol, valid values are DES (Data Encryption Standard), AES, 3DES, AES192, AES256.

Although 3DES, AES192 and AES256 are widely implemented encryption algorithms they are not included to the SNMP standard. Therefore a particular manufacturer's implementation of one or more of these technologies may not be supported by Entuity.

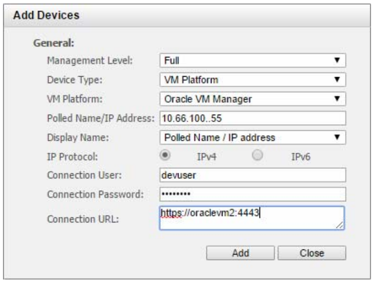
- *-X <Privacy passwd>*, sets the privacy password, valid values must be between eight and thirty-two characters long. If the password contains spaces double quotes must be placed around the password.

# Adding a Single Device

When adding a device to Entuity, or modifying the attributes Entuity uses to manage a device already under its management, there are two forms of device definition, one for:

- VM Platforms, as these devices require non-standard connection details as communication is through the VM platform SDK. (See *Attributes Entuity Uses to Manage VM Platforms*.)

  For Oracle VMs you must also include security certificates. (See *Adding Oracle VM Managers to Entuity*.)



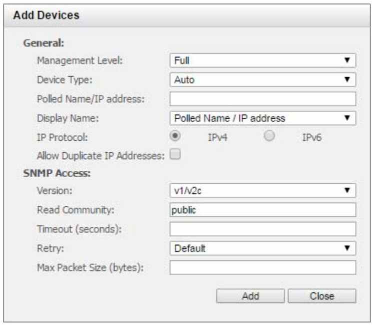
Add Devices

General:

Management Level: Full ▾
Device Type: VM Platform ▾
VM Platform: Oracle VM Manager ▾
Polled Name/IP Address: 10.66.100..55
Display Name: Polled Name / IP address ▾
IP Protocol: ● IPv4 ○ IPv6
Connection User: devuser
Connection Password: ••••••••
Connection URL: https://oraclevm2:4443

Figure 143 Add a VM Platform Device

- All other device types. (See *Attributes Entuity Uses to Manage Devices*.)



Add Devices

General:

Management Level: Full ▾
Device Type: Auto ▾
Polled Name/IP address:
Display Name: Polled Name / IP address ▾
IP Protocol: ● IPv4 ○ IPv6
Allow Duplicate IP Addresses: □

SNMP Access:

Version: v1/v2c ▾
Read Community: public
Timeout (seconds):
Retry: Default ▾
Max Packet Size (bytes):

Figure 144 Add a Device

To add a device to Entuity:

1) Click **Administration > Inventory / Topology > Inventory Administration**.
2) Click **Add**.
3) Specify the device attributes Entuity uses to discover and manage the device.
4) Click:
   - **Add**, to queue the device for adding to Entuity. The dialog remains open so you can add more devices.

- **Close**, to close the dialog and return to the Inventory Administration page.

5) From the Inventory Administration page you can view the devices under Entuity management.

## Adding Oracle VM Managers to Entuity

Entuity manages Oracle VM Manager through the VM Platform device type. Before adding an Oracle VM Manager to Entuity ensure you:

- Have the security certificate for the VM.
- Can communicate with the VM from Entuity.
- Have the appropriate connection details.

To add an Oracle VM Manager to Entuity:

1) From the command line on the Entuity server navigate to *entuity_home*`/lib/virtualization`.

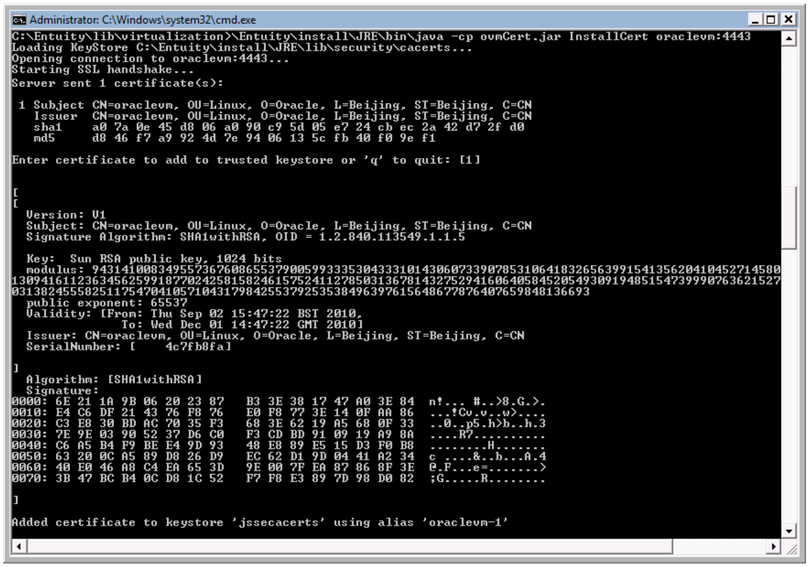
2) Apply the VM certificate by entering on the command line:

   ```
   \entuity_home\install\JRE\bin\java -cp ovmCert.jar InstallCert <params>
   ```

   where <*params*> is the hostname of the machine and the port, e.g. *oraclvm:4443.*

3) When the Entuity server successfully communicates with the VM, it displays the certificate on the screen.

   Press enter to accept the certificate, which is then written to the Entuity server’s certificate folder, `jssecacerts`. This folder is created the first time you add a certificate, and is used for all certificates in the same directory.



```
C:\Entuity\lib\virtualization>\Entuity\install\JRE\bin\java -cp ovmCert.jar InstallCert oraclevm:4443
Loading KeyStore C:\Entuity\install\JRE\lib\security\cacerts...
Opening connection to oraclevm:4443...
Starting SSL handshake...
Server sent 1 certificate(s):

 1 Subject CN=oraclevm, OU=Linux, O=Oracle, L=Beijing, ST=Beijing, C=CN
   Issuer  CN=oraclevm, OU=Linux, O=Oracle, L=Beijing, ST=Beijing, C=CN
   sha1    a0 7a 0e 45 d8 06 a0 90 c9 5d 05 e7 24 cb ec 2a 42 d7 2f d0
   md5     d8 46 f7 a9 92 4d 7e 94 06 13 5c fb 40 f0 9e f1

Enter certificate to add to trusted keystore or 'q' to quit: [1]


[
[
  Version: V1
  Subject: CN=oraclevm, OU=Linux, O=Oracle, L=Beijing, ST=Beijing, C=CN
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key:  Sun RSA public key, 1024 bits
  modulus: 9431410083495573676086553790059933353043331014306073390785310641832656399154135620410452714580
130941611236345625991877024258158246157524112785031367814327529416064058452054930919485154739990763621527
0313824555825117547041057104317984255379253538496397615648677876407659848136693
  public exponent: 65537
  Validity: [From: Thu Sep 02 15:47:22 BST 2010,
               To: Wed Dec 01 14:47:22 GMT 2010]
  Issuer: CN=oraclevm, OU=Linux, O=Oracle, L=Beijing, ST=Beijing, C=CN
  SerialNumber: [    4c7fb8fa]

]
  Algorithm: [SHA1withRSA]
  Signature:
0000: 6E 21 1A 9B 06 20 23 87   B3 3E 38 17 47 A0 3E 84  n!... #..>8.G.>.
0010: E4 C6 DF 21 43 76 F8 76   E0 F8 77 3E 14 0F AA 86  ...!Cv.v..w>....
0020: C3 E8 30 BD AC 70 35 F3   68 3E 62 19 A5 68 0F 33  ..0..p5.h>b..h.3
0030: 7E 9E 03 90 52 37 D6 C0   F3 CD BD 91 09 19 A9 8A  ....R7..........
0040: C6 A5 B4 F9 BE E4 9D 93   48 E8 89 E5 15 D3 F0 B8  ........H.......
0050: 63 20 0C A5 89 D8 26 D9   EC 62 D1 9D 04 41 A2 34  c ....&..b...A.4
0060: 40 E0 46 A8 C4 EA 65 3D   9E 00 7F EA 87 86 8F 3E  @.F...e=.......>
0070: 3B 47 BC B4 0C D8 1C 52   F7 F8 E3 89 7D 98 D0 82  ;G.....R........

]

Added certificate to keystore 'jssecacerts' using alias 'oraclevm-1'
```

Figure 145 Accepting VM Oracle Certificates

4) From the Inventory Administration page you can now add the Oracle VM Manager. (See *Adding a Single Device*.)

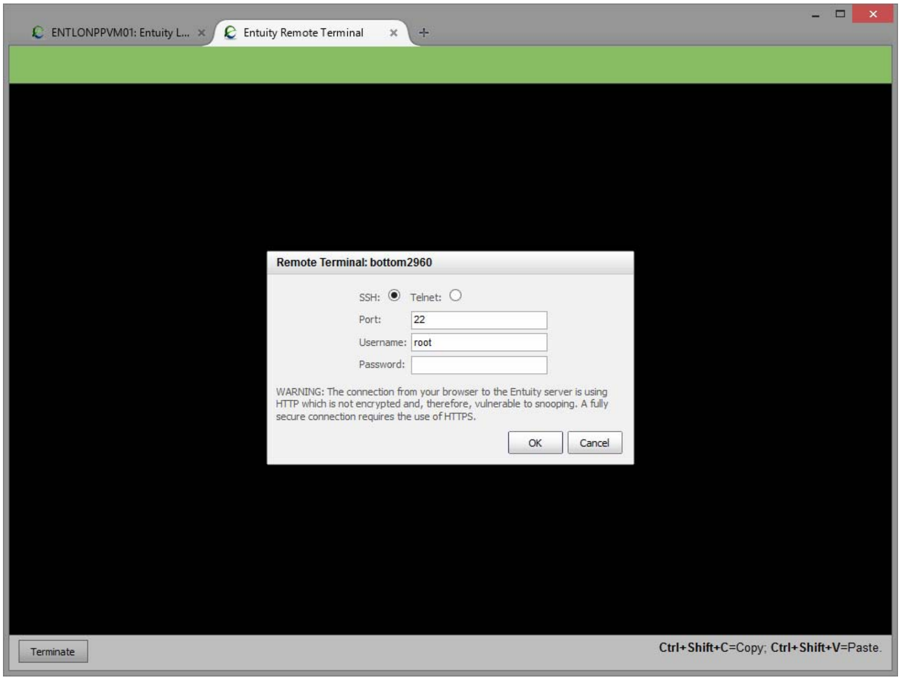
# Remote Terminal Access

From Entuity you can open a remote terminal session with a managed device. Entuity supports both SSH and Telnet remote terminal access.

To access a device:

1) Highlight the device and from the context menu click **Remote Terminal**.

   You can access Remote Terminal from devices in the Explorer Tree, returned in Search results and presented in maps.



Remote Terminal: bottom2960

SSH: ● Telnet: ○

Port: 22

Username: root

Password:

WARNING: The connection from your browser to the Entuity server is using HTTP which is not encrypted and, therefore, vulnerable to snooping. A fully secure connection requires the use of HTTPS.

Ctrl+Shift+C=Copy; Ctrl+Shift+V=Paste.

Figure 146 Remote Terminal Access

# 15 Multi-tenant Support

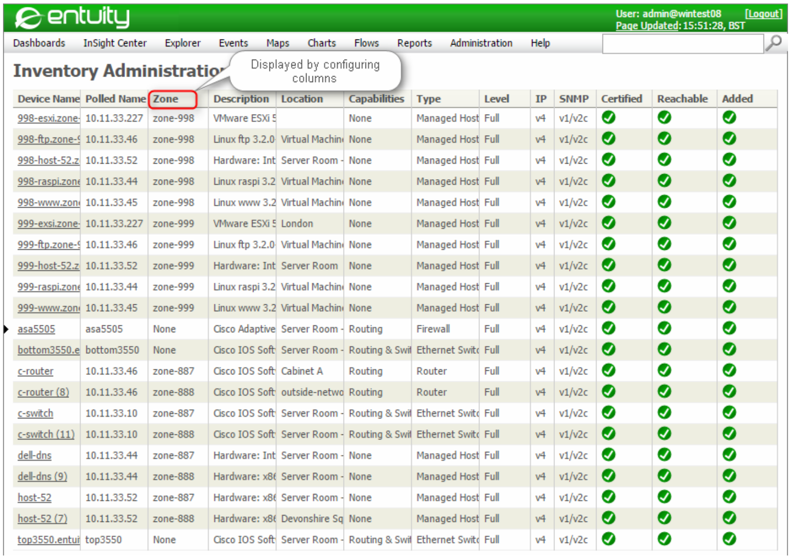
When managing a number of networks a significant challenge can be managing overlapping address spaces. Different sites using private IP address spaces in the `10.x.x.x`, `172.16-31.x.x`, or `192.168.x.x` spaces are likely to have devices with the same IP addresses. It is important that you can distinguish between these devices to:

- Ensure information gathered on devices is correct.
- Limit user access to only those devices their user role requires.
- Allow service providers to control per organization configuration.

Entuity uses the concept of zones to distinguish between sites with overlapping IP address spaces. A zone identifies the site, for example by its VPN and gateway. You can then assign devices to their appropriate zone. Entuity can then distinguish between devices with the same management IP address.

Your network administrator must have configured the network so that it can correctly route traffic to sites with overlapping IP address spaces.

When not using zones Entuity recommend device IP addresses are unique. When using zones Entuity recommend IP addresses are unique within the zone. Through Inventory Administration you can override this default and permit duplicate IP addresses.



Inventory Administration

Displayed by configuring columns

| Device Name | Polled Name | Zone | Description | Location | Capabilities | Type | Level | IP | SNMP | Certified | Reachable | Added |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 998-esxi.zone- | 10.11.33.227 | zone-998 | VMware ESXi 5 |  | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 998-ftp.zone-9 | 10.11.33.46 | zone-998 | Linux ftp 3.2.0- | Virtual Machin | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 998-host-52.z | 10.11.33.52 | zone-998 | Hardware: Int | Server Room - | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 998-raspi.zone | 10.11.33.44 | zone-998 | Linux raspi 3.2 | Virtual Machin | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 998-www.zon | 10.11.33.45 | zone-998 | Linux www 3.2 | Virtual Machin | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 999-exsi.zone- | 10.11.33.227 | zone-999 | VMware ESXi 5 | London | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 999-ftp.zone-9 | 10.11.33.46 | zone-999 | Linux ftp 3.2.0- | Virtual Machin | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 999-host-52.z | 10.11.33.52 | zone-999 | Hardware: Int | Server Room | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 999-raspi.zone | 10.11.33.44 | zone-999 | Linux raspi 3.2 | Virtual Machin | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 999-www.zon | 10.11.33.45 | zone-999 | Linux www 3.2 | Virtual Machin | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| asa5505 | asa5505 | None | Cisco Adaptive | Server Room - | Routing | Firewall | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| bottom3550.e | bottom3550 | None | Cisco IOS Soft | Server Room - | Routing & Swi | Ethernet Switc | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| c-router | 10.11.33.46 | zone-887 | Cisco IOS Soft | Cabinet A | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| c-router (8) | 10.11.33.46 | zone-888 | Cisco IOS Soft | outside-netwo | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| c-switch | 10.11.33.10 | zone-887 | Cisco IOS Soft | Server Room - | Routing & Swi | Ethernet Switc | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| c-switch (11) | 10.11.33.10 | zone-888 | Cisco IOS Soft | Server Room - | Routing & Swi | Ethernet Switc | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| dell-dns | 10.11.33.44 | zone-887 | Hardware: Int | Server Room - | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| dell-dns (9) | 10.11.33.44 | zone-888 | Hardware: x86 | Server Room - | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| host-52 | 10.11.33.52 | zone-887 | Hardware: x86 | Server Room - | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| host-52 (7) | 10.11.33.52 | zone-888 | Hardware: x86 | Devonshire Sq | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| top3550.entui | top3550 | None | Cisco IOS Soft | Server Room - | Routing & Swi | Ethernet Switc | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |

Figure 1 Display Zones in Inventory Administration

# Zones in Entuity

If Entuity is not managing sites with overlapping IP addresses you do not have to consider zones. By default Entuity does not:

- Assign devices to zones, i.e. a device’s zone is set to **None**.
- Display zone information. For example when adding a device the zone attribute is only available when one or more zones have been defined, in tables the Zone column is always hidden.

If Entuity is managing sites with overlapping IP addresses then you should configure zones. When you are using zones you should assign each device to a zone, do not leave any devices unassigned.

Zone configurations are specific to the Entuity server on which they are defined. For example two servers with zones named Zone 1 can have very different setups. Entuity would not consolidate these zone configurations. You are recommended to:

- Use a zone naming convention which readily and uniquely identifies the purpose of the zone.
- Use zone names that unique across all Entuity servers; do not define zones on different servers with the same name.

## Controlling Access to Devices by Zones

When you have configured zones Entuity segregates data storage, data processing and network communication by zone. This is for devices but also components such as VLANs, MACs, IP addresses, STP, CDP and LLDP.

Discovery of topology links is also constrained by zones; Entuity does not discover links between devices in different zones. However you can create inter-zone connections by manually adding links.

## Events Management System and Zones

Events Management System has only one live EMS project. This covers all zones. You can configure zone awareness within the EMS project by setting up actions that test for the zone of a device or port before determining the action to take.

You can also restrict non-administrators to only those views and features (permissions) that are zone specific, and which apply to them. Administrators of an Entuity server always have access to all zones. (See *Zones and View Content Filter Rules*.)

# Zones, syslog and Traps

Entuity zones support IPv4 and IPv6 traps. `syslogger` is also zone aware.

Entuity uses the IP address of the local interface on which traps and syslogs messages are received to search for the appropriate zone.

The zone's device configured IP addresses are searched to try to match the source IP address with a device but not with device IP addresses from other zones. Specifically when receiving syslogs and traps:

1) Entuity first uses the zone the message came in on.
2) If that fails then Entuity attempts to identify the device.
3) If that fails Entuity raises an event against the IP address and not the device.

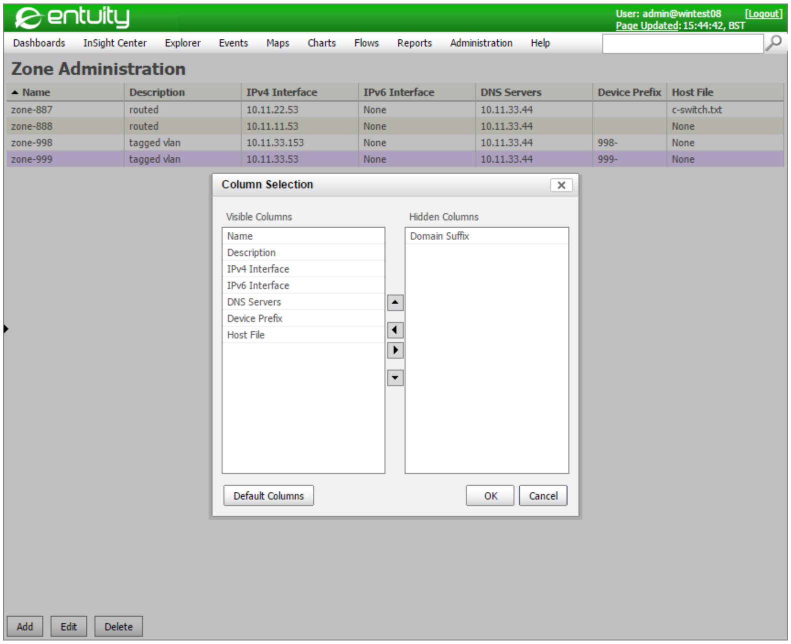
# Viewing Zones

Zone Administration displays all configured zones. Configured zones are always available to assign to devices.

To view zones:

1) Click **Administration > Inventory / Topology > Zone Administration**.

   You can use the Configure Column feature to amend the displayed attributes. (See *Figure 2 Configure Columns in Zone Administration*.)



Zone Administration

| ▲ Name | Description | IPv4 Interface | IPv6 Interface | DNS Servers | Device Prefix | Host File |
|---|---|---|---|---|---|---|
| zone-887 | routed | 10.11.22.53 | None | 10.11.33.44 | | c-switch.txt |
| zone-888 | routed | 10.11.11.53 | None | 10.11.33.44 | | None |
| zone-998 | tagged vlan | 10.11.33.153 | None | 10.11.33.44 | 998- | None |
| zone-999 | tagged vlan | 10.11.33.53 | None | 10.11.33.44 | 999- | None |

Column Selection

| Visible Columns | Hidden Columns |
|---|---|
| Name | Domain Suffix |
| Description | |
| IPv4 Interface | |
| IPv6 Interface | |
| DNS Servers | |
| Device Prefix | |
| Host File | |

Figure 2 Configure Columns in Zone Administration

# Setting up Zones

If Entuity is not managing sites with overlapping IP addresses you do not have to configure zones. This is the default state. In this state devices are assigned to None.

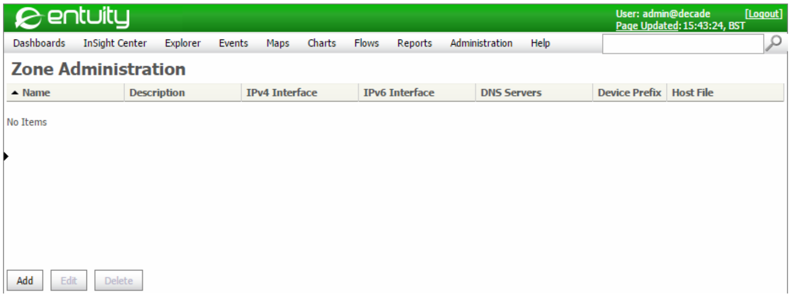
Zones are defined on a per server basis, for example Zone-1 on server A, is a distinct entity to Zone-1 on server B.

When configuring zones you must set routing information and custom DNS settings. This will allow an Entuity server to utilize multiple VPNs even though the IP addresses within them may not be unique.

When configuring zones in Entuity you are reflecting the setup on your network. Configuring your network is outside of the scope of this guide.

To set up a zone:

1) Click **Administration** > **Inventory** / **Topology** > **Zone Administration**.



Zone Administration

| Name | Description | IPv4 Interface | IPv6 Interface | DNS Servers | Device Prefix | Host File |
|---|---|---|---|---|---|---|

No Items

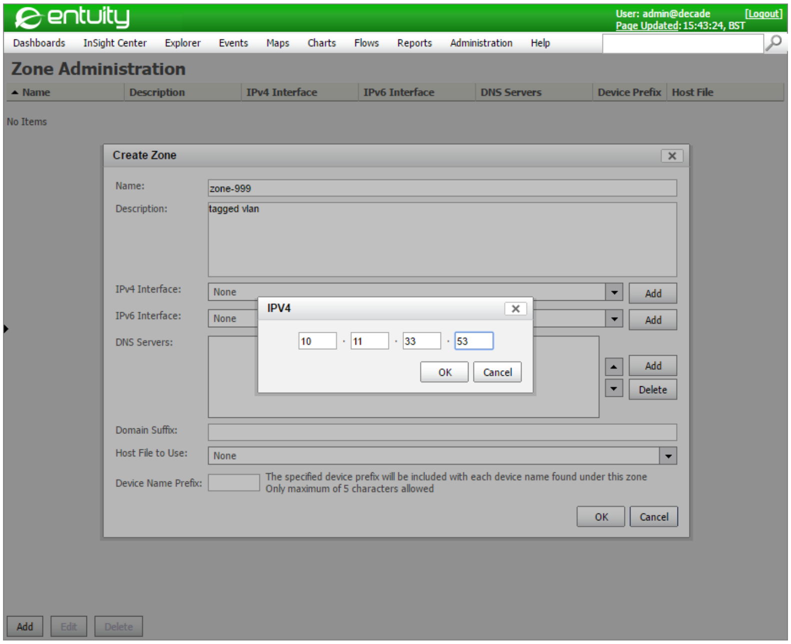
Figure 3 Zone Administration

2) Click **Add** and complete the zone configuration.

A zone’s IP address interface is used to identify and direct network traffic, for example outbound:

- UDP traffic (SNMP & DNS).
- ICMP traffic from ping and traceroute tools.
- TCP used by application monitor, Configuration Manager, the Entuity interface, and the telnet and SSH client.

Traffic is directed to the appropriate VPN by explicitly binding sockets to the interface specified in the zone's configuration. Conventional and point to point interfaces are also supported. Flow receiver, `syslogger` and trap receiver support binding to multiple interfaces.



Zone Administration

| Name | Description | IPv4 Interface | IPv6 Interface | DNS Servers | Device Prefix | Host File |
|---|---|---|---|---|---|---|

No Items

Create Zone

Name: zone-999

Description: tagged vlan

IPv4 Interface: None

IPv6 Interface: None

DNS Servers:

IPV4

10 . 11 . 33 . 53

Domain Suffix:

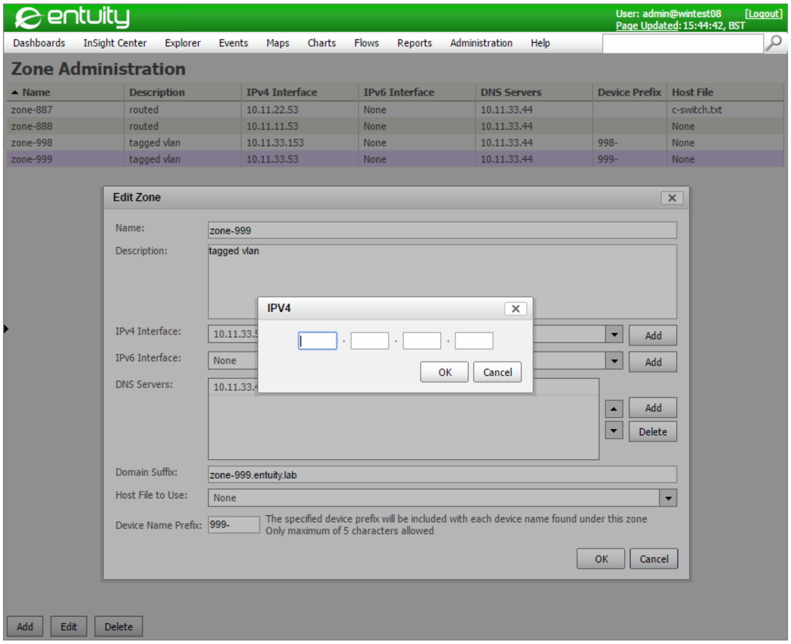
Host File to Use: None

Device Name Prefix: The specified device prefix will be included with each device name found under this zone
Only maximum of 5 characters allowed

Figure 4 Create a Zone

| Attribute | Description |
|---|---|
| *Name* | Zone name. |
| *Description* | Include a description of the purpose of the zone. |
| *IPv4 Interface* | IPv4 interface. |
| *IPv6 Interface* | IPv6 interface. |
| *DNS Servers* | You can configure multiple DNS servers for a zone but you must not mix ipV6 and ipV4 addresses.<br>The Entuity DNS client directs host and reverse lookup requests to the specified DNS server. To improve performance the client caches responses. |
| *Domain Suffix* | Domain suffixes identify domain names. (See *Edit IPv4 Interface*.) |
| *Host File to Use* | Host files for each zone can be included from `entuity_home\etc\hostfiles` on the Entuity server. |
| *Device Name Prefix* | A prefix to add to the name of each device in the zone. The prefix can have a maximum of five characters. |

Table 1 Zone Configuration



User: admin@wintest08 [Logout]
Page Updated: 15:44:42, BST

Zone Administration

| Name | Description | IPv4 Interface | IPv6 Interface | DNS Servers | Device Prefix | Host File |
|---|---|---|---|---|---|---|
| zone-887 | routed | 10.11.22.53 | None | 10.11.33.44 | | c-switch.txt |
| zone-888 | routed | 10.11.11.53 | None | 10.11.33.44 | | None |
| zone-998 | tagged vlan | 10.11.33.153 | None | 10.11.33.44 | 998- | None |
| zone-999 | tagged vlan | 10.11.33.53 | None | 10.11.33.44 | 999- | None |

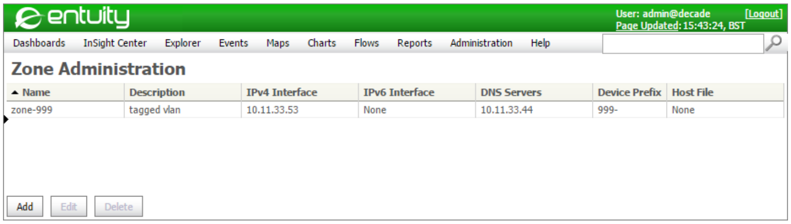
Edit Zone

Name: zone-999
Description: tagged vlan
IPv4 Interface: 10.11.33.5
IPv6 Interface: None
DNS Servers: 10.11.33.4
Domain Suffix: zone-999.entuity.lab
Host File to Use: None
Device Name Prefix: 999- The specified device prefix will be included with each device name found under this zone Only maximum of 5 characters allowed

IPV4

Figure 5 Edit IPv4 Interface

3) Click **OK** to save the zone configuration.



User: admin@decade [Logout]
Page Updated: 15:43:24, BST

Zone Administration

| Name | Description | IPv4 Interface | IPv6 Interface | DNS Servers | Device Prefix | Host File |
|---|---|---|---|---|---|---|
| zone-999 | tagged vlan | 10.11.33.53 | None | 10.11.33.44 | 999- | None |

Figure 6 Zone Listing Administration

## Adding Devices to Entuity Zones

When you have configured zones the Entuity interface updates to display zones when adding or modifying devices. For example the Auto Discovery dialog displays a drop-down list of zones. (See *Figure 7 AutoDiscovery Zone Administration*.)

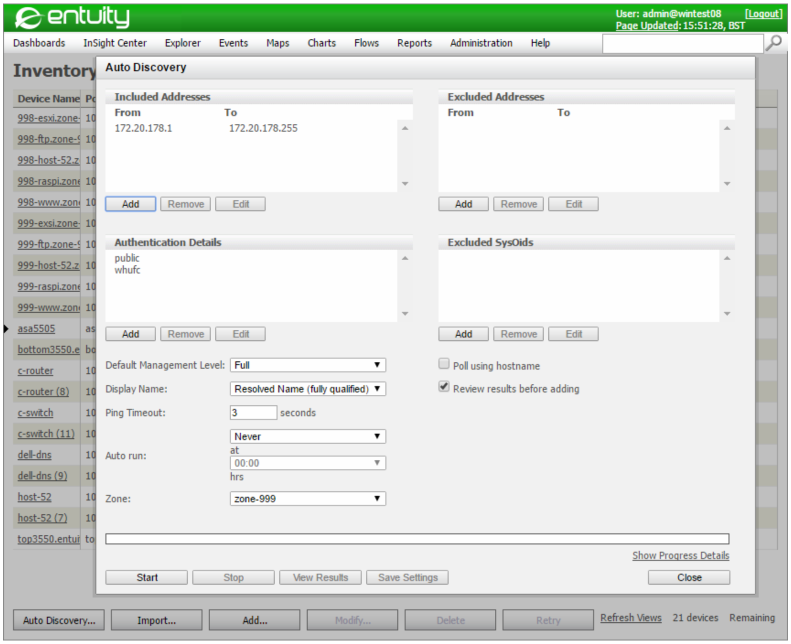
You can configure `autoDiscovery` to search the network for devices to manage. It is most useful when you have many devices, or a potentially unknown set of devices, to manage. (See *Adding Devices Using Auto Discovery*.)

To run auto discovery configured for zones:

1) Click **Administration** > **Inventory** / **Topology** > **Inventory Administration**.

2) From the Inventory Administration page click **Auto Discovery**.

3) Set *Zone*.



Included Addresses

| From | To |
|---|---|
| 172.20.178.1 | 172.20.178.255 |

Excluded Addresses

| From | To |
|---|---|

Authentication Details

public
whufc

Excluded SysOids

Default Management Level: Full

Display Name: Resolved Name (fully qualified)

Ping Timeout: 3 seconds

Auto run: Never at 00:00 hrs

Zone: zone-999

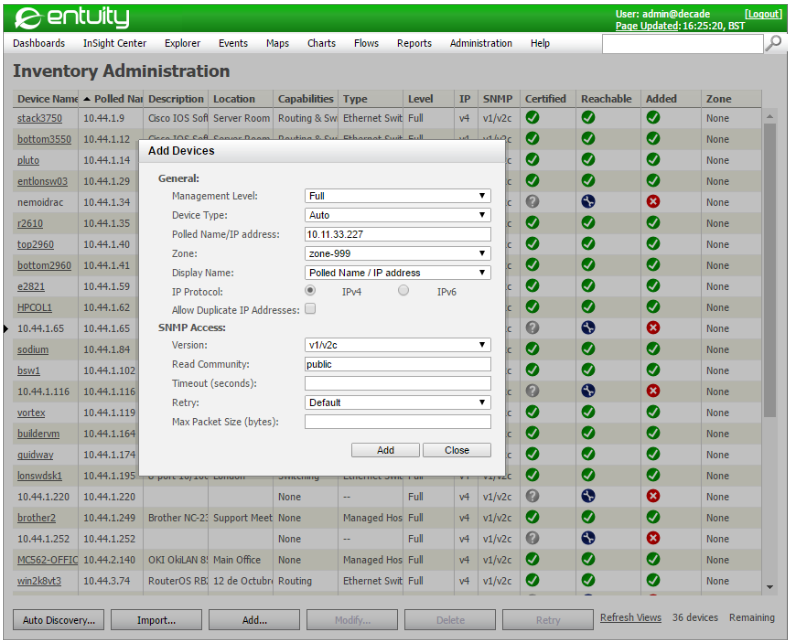
□ Poll using hostname

☑ Review results before adding

Figure 7 AutoDiscovery Zone Administration

You can also assign devices to zones when:

- Adding individual devices. (See *Figure 8 Add a Device to a Zone*.)



Inventory Administration

| Device Name | ▲ Polled Nai | Description | Location | Capabilities | Type | Level | IP | SNMP | Certified | Reachable | Added | Zone |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| stack3750 | 10.44.1.9 | Cisco IOS Soft | Server Room | Routing & Sw | Ethernet Swit | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | None |
| bottom3550 | 10.44.1.12 | Cisco IOS Soft | Server Room | Routing & Sw | Ethernet Swit | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | None |
| pluto | 10.44.1.14 | | | | | | | c | ✓ | ✓ | ✓ | None |
| entlonsw03 | 10.44.1.29 | | | | | | | c | ✓ | ✓ | ✓ | None |
| nemoidrac | 10.44.1.34 | | | | | | | c | ? | ⊕ | ✗ | None |
| r2610 | 10.44.1.35 | | | | | | | c | ✓ | ✓ | ✓ | None |
| top2960 | 10.44.1.40 | | | | | | | c | ✓ | ✓ | ✓ | None |
| bottom2960 | 10.44.1.41 | | | | | | | c | ✓ | ✓ | ✓ | None |
| e2821 | 10.44.1.59 | | | | | | | c | ✓ | ✓ | ✓ | None |
| HPCOL1 | 10.44.1.62 | | | | | | | c | ✓ | ✓ | ✓ | None |
| 10.44.1.65 | 10.44.1.65 | | | | | | | c | ? | ⊕ | ✗ | None |
| sodium | 10.44.1.84 | | | | | | | c | ✓ | ✓ | ✓ | None |
| bsw1 | 10.44.1.102 | | | | | | | c | ✓ | ✓ | ✓ | None |
| 10.44.1.116 | 10.44.1.116 | | | | | | | c | ? | ⊕ | ✗ | None |
| vortex | 10.44.1.119 | | | | | | | c | ✓ | ✓ | ✓ | None |
| buildervm | 10.44.1.164 | | | | | | | c | ✓ | ✓ | ✓ | None |
| guidway | 10.44.1.174 | | | | | | | c | ✓ | ✓ | ✓ | None |
| lonswdsk1 | 10.44.1.195 | 8 port 10/100 | London | Switching | Ethernet Swit | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | None |
| 10.44.1.220 | 10.44.1.220 | | | None | -- | Full | v4 | v1/v2c | ? | ⊕ | ✗ | None |
| brother2 | 10.44.1.249 | Brother NC-2: | Support Meet | None | Managed Hos | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | None |
| 10.44.1.252 | 10.44.1.252 | | | None | -- | Full | v4 | v1/v2c | ? | ⊕ | ✗ | None |
| MC562-OFFIC | 10.44.2.140 | OKI OkiLAN 8: | Main Office | None | Managed Hos | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | None |
| win2k8vt3 | 10.44.3.74 | RouterOS RB: | 12 de Octubre | Routing | Ethernet Swit | Full | v4 | v1/v2c | ✓ | ✓ | ✓ | None |

Add Devices

General:

Management Level: Full
Device Type: Auto
Polled Name/IP address: 10.11.33.227
Zone: zone-999
Display Name: Polled Name / IP address
IP Protocol: ● IPv4 ○ IPv6
Allow Duplicate IP Addresses: □

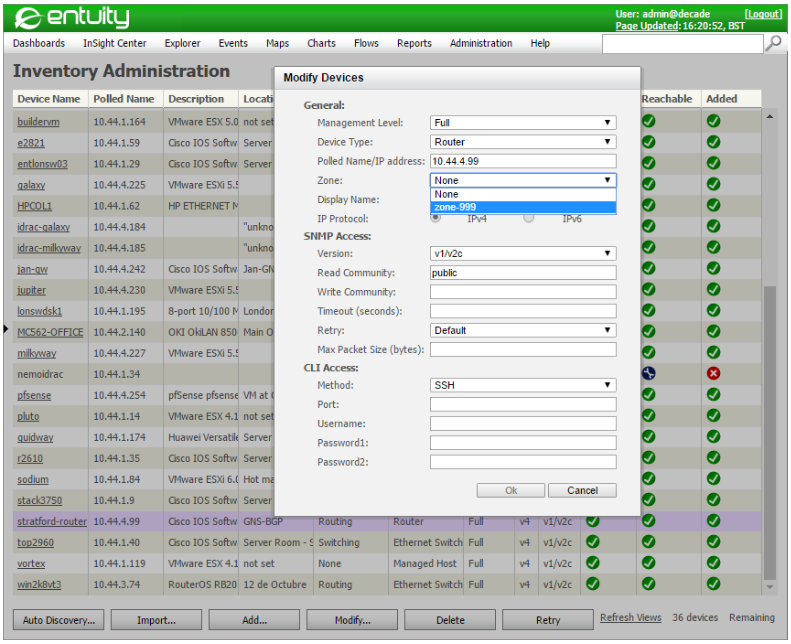
SNMP Access:

Version: v1/v2c
Read Community: public
Timeout (seconds):
Retry: Default
Max Packet Size (bytes):

36 devices Remaining

Figure 8 Add a Device to a Zone

- Modifying devices, e.g. moving a device from one zone to another. (See *Figure 9 Change a Device’s Zone*.)



Inventory Administration

| Device Name | Polled Name | Description | Locati | | | | | | | Reachable | Added |
|---|---|---|---|---|---|---|---|---|---|---|---|
| buildervm | 10.44.1.164 | VMware ESX 5.0 | not set | | | | | | | ✓ | ✓ |
| e2821 | 10.44.1.59 | Cisco IOS Softw | Server | | | | | | | ✓ | ✓ |
| entlonsw03 | 10.44.1.29 | Cisco IOS Softw | Server | | | | | | | ✓ | ✓ |
| galaxy | 10.44.4.225 | VMware ESXi 5.5 | | | | | | | | ✓ | ✓ |
| HPCOL1 | 10.44.1.62 | HP ETHERNET M | | | | | | | | ✓ | ✓ |
| idrac-galaxy | 10.44.4.184 | | "unkno | | | | | | | ✓ | ✓ |
| idrac-milkyway | 10.44.4.185 | | "unkno | | | | | | | ✓ | ✓ |
| jan-gw | 10.44.4.242 | Cisco IOS Softw | Jan-GN | | | | | | | ✓ | ✓ |
| jupiter | 10.44.4.230 | VMware ESXi 5.5 | | | | | | | | ✓ | ✓ |
| lonswdsk1 | 10.44.1.195 | 8-port 10/100 M | London | | | | | | | ✓ | ✓ |
| MC562-OFFICE | 10.44.2.140 | OKI OkiLAN 850 | Main O | | | | | | | ✓ | ✓ |
| milkyway | 10.44.4.227 | VMware ESXi 5.5 | | | | | | | | ✓ | ✓ |
| nemoidrac | 10.44.1.34 | | | | | | | | | 🔧 | ✗ |
| pfsense | 10.44.4.254 | pfSense pfsense | VM at ( | | | | | | | ✓ | ✓ |
| pluto | 10.44.1.14 | VMware ESX 4.1 | not set | | | | | | | ✓ | ✓ |
| quidway | 10.44.1.174 | Huawei Versatile | Server | | | | | | | ✓ | ✓ |
| r2610 | 10.44.1.35 | Cisco IOS Softw | Server | | | | | | | ✓ | ✓ |
| sodium | 10.44.1.84 | VMware ESXi 6.0 | Hot ma | | | | | | | ✓ | ✓ |
| stack3750 | 10.44.1.9 | Cisco IOS Softw | Server | | | | | | | ✓ | ✓ |
| stratford-router | 10.44.4.99 | Cisco IOS Softw | GNS-BGP | Routing | Router | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| top2960 | 10.44.1.40 | Cisco IOS Softw | Server Room - S | Switching | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| vortex | 10.44.1.119 | VMware ESX 4.1 | not set | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| win2k8vt3 | 10.44.3.74 | RouterOS RB20 | 12 de Octubre | Routing | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |

Modify Devices

General:

Management Level: Full

Device Type: Router

Polled Name/IP address: 10.44.4.99

Zone: None

None

zone-999

Display Name:

IP Protocol: ● IPv4 ○ IPv6

SNMP Access:

Version: v1/v2c

Read Community: public

Write Community:

Timeout (seconds):

Retry: Default

Max Packet Size (bytes):

CLI Access:

Method: SSH

Port:

Username:

Password1:

Password2:

36 devices Remaining

Figure 9 Change a Device’s Zone

# 16 Ports and VLANs Maintenance

Precise, reliable inventory is the cornerstone of network management. An Entuity server provides auto discovery capabilities that automatically find and capture device information on the network. Continual refreshes keep inventory data up-to-date. Entuity gathers detailed device specifics down to the serial number, IOS versions and more. Data gathering methods include: SNMP polling, SYSLOG events, SNMP traps, ping, TCP port probing, ping-only availability monitoring and network flows.

For the data Entuity collects to be useful it must reflect both the reality of your network and meet your management requirements. Entuity has a number of functions and utilities that allow you to maintain this correspondence.

You should always be aware that the data Entuity collects from managed objects is only as true, or as useful as the information held on that object. For example the usefulness of polled data can be impaired through incorrectly configured devices, or devices that have been upgraded but retain their original, but now outdated, factory settings. Entuity still collects and uses that data regardless. Within Entuity you can override values, e.g. port speed, however the more you validate your device settings the better Entuity can manage your network.

## Fast Port Polling

By default every five minutes Entuity polls for port utilization and status details. However you can specify ports which Entuity should poll every minute for their utilization and/or status data. This fast port polling would be suitable for key ports, or for troubleshooting problematic ports.

Fast port polling is:

- Turned off by default. You can enable it on a port by port basis.
- Separately implemented for port utilization and status. You can therefore enable fast port polling of one on a port without enabling the other.
- By default set at a frequency of one minute.
- By default restricted to 100 ports having their utilization data fast polled, and 100 ports having their status information fast polled.

### How to Activate Fast Polling on a Port

To activate fast polling of utilization data on a port:

1) From the Explorer tree highlight the target port.

2) From the context menu click **Polling** > **Fast Utilization Polling** > **Enable**.

   Entuity activates fast polling of utilization data on the port, updating on the port's Summary tab *Fast Utilization Poll Enabled* to **Yes**.

The fast polling context menus are also available elsewhere in Entuity, for example when you highlight port details in Drop Box or Search results.

## How to Identify Fast Polling Ports

Fast port polling is only intended for monitoring a subset of important ports across a network. You can identify which ports have polling enabled through the port's Summary page and the status of *Fast Utilization Polling* and *Fast Status Polling*. However with potentially 200 ports on each server having fast port polling enabled, you can use Search to provide a listing of activated ports.

To find all ports with fast polling of utilization data enabled:

1) Select the magnifying glass icon from the menu bar but do not enter a query.

2) Click **Extended Search**.

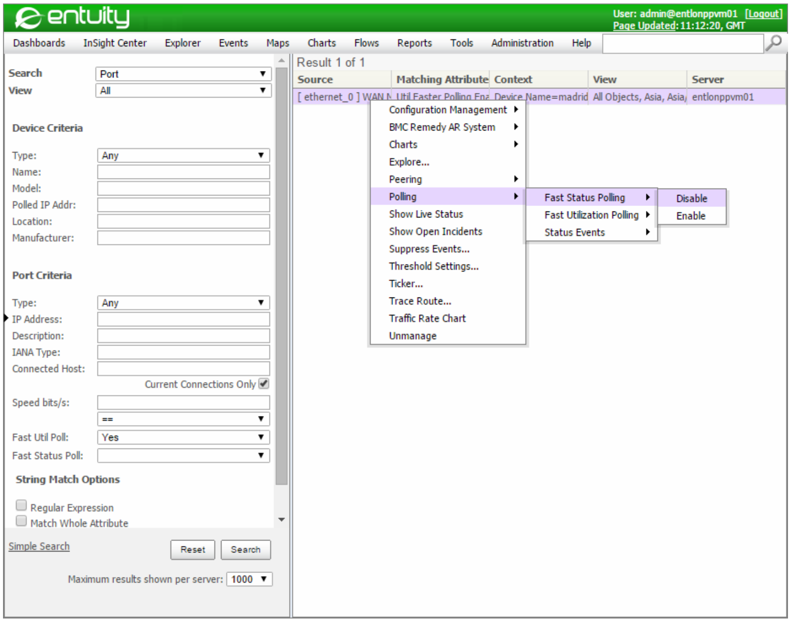
3) Enter the search criteria, for example:

   - *Search*, **Port**.
   - *View*, **London Office**.
   - *Port Criteria Type*, **Any**.
   - *Fast Util Poll*, **Yes**.

   When you are searching for ports with fast polling of status data enabled you can set *Fast Status Poll* to **Yes**.

4) Click **Search**. Entuity returns ports that match your criteria.

   You can highlight a result and from the context menu amend its fast port setting. As you can select more than one port you can also change the fast polling status of more than one port.



Search: Port
View: All

Device Criteria

Type: Any
Name:
Model:
Polled IP Addr:
Location:
Manufacturer:

Port Criteria

Type: Any
IP Address:
Description:
IANA Type:
Connected Host:
Current Connections Only ☑
Speed bits/s:
==
Fast Util Poll: Yes
Fast Status Poll:

String Match Options

☐ Regular Expression
☐ Match Whole Attribute

Maximum results shown per server: 1000

Result 1 of 1

| Source | Matching Attribute | Context | View | Server |
|---|---|---|---|---|
| [ ethernet_0 ] WAN N | Util Faster Polling Ena | Device Name=madrid | All Objects, Asia, Asia, | entlonppvm01 |

Figure 10 Searching for Fast Polled Ports

# Configurable Port Status Event Generation

By default port status events are enabled for core ports and disabled for edge ports. Entuity identifies:

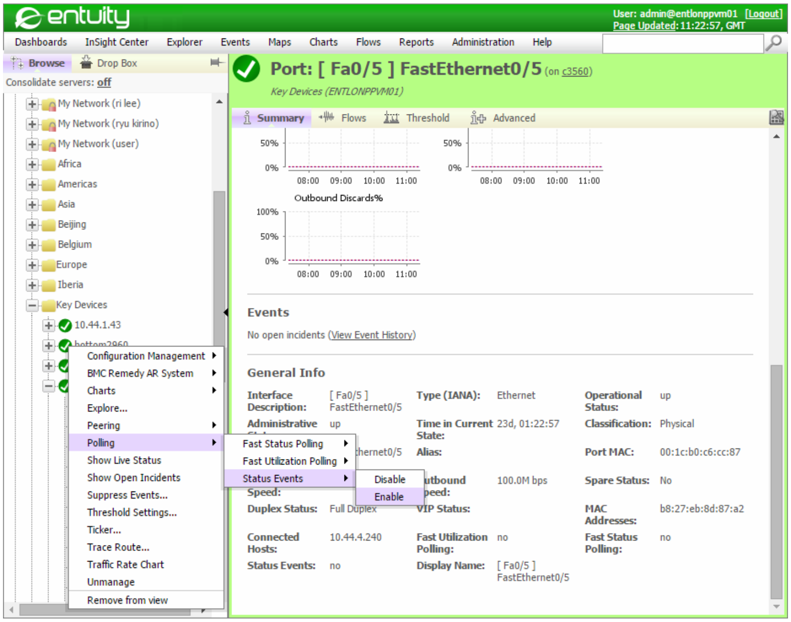
- A core port as a WAN, trunk or router port.
- Port Operationally Down and Port Operationally Down Cleared as port status events.

Through the Port Summary tab you can view the current setting of Status Events. From Explorer you can change the setting, both activating and deactivating port status events on the port.

To activate port status events on a port:

1) From the Explorer tree highlight the target port.
2) From the context menu click **Polling** > **Status Events** > **Enable**.

   Entuity activates the event on the port, updating on the port Summary tab *Status Events* to **Yes**.



Events

No open incidents (View Event History)

General Info

Interface Description: [ Fa0/5 ] FastEthernet0/5
Type (IANA): Ethernet
Operational Status: up
Administrative Status: up
Time in Current State: 23d, 01:22:57
Classification: Physical
Alias:
Port MAC: 00:1c:b0:c6:cc:87
Outbound Speed: 100.0M bps
Spare Status: No
Duplex Status: Full Duplex
VIP Status:
MAC Addresses: b8:27:eb:8d:87:a2
Connected Hosts: 10.44.4.240
Fast Utilization Polling: no
Fast Status Polling: no
Status Events: no
Display Name: [ Fa0/5 ] FastEthernet0/5

Figure 11 Set Port Status Events

# Managing Ports

By default Entuity manages all of the ports on the devices under its management. You can amend this default behavior:

- From Entuity you can unmanage one or more ports on a device.

- From a device you can set one or more of its ports to Admin Down.

## Managing and Unmanaging Ports

As a member of the Administrators user group, or a user with the Managed Port Administration tool permission, you can manually mark ports for deletion so that they are automatically removed the next time that `prodigy` runs. Entuity no longer manages these ports and they can only be viewed and remanaged when you have the Show Unmanaged Ports permission selected through Preferences.

> When you unmanage or remanage a port Entuity schedules the action. This change may not take effect for 20 minutes (until the next time `prodigy` runs).

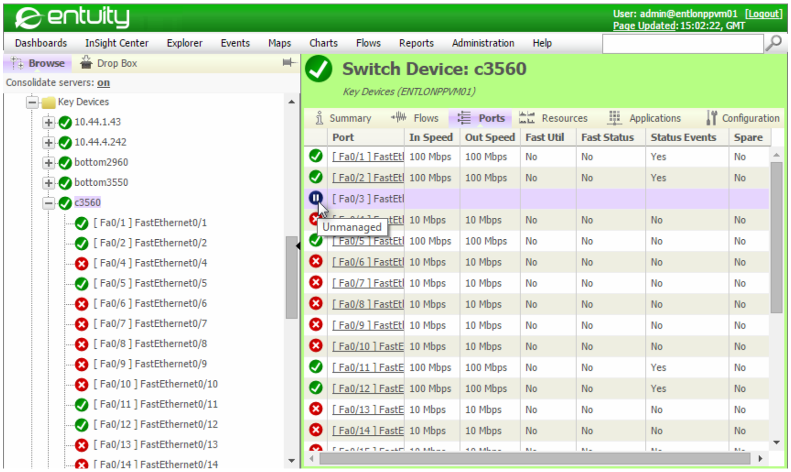
### Unmanaging Ports

To stop Entuity managing selected ports:

1) From Explorer highlight the ports.

2) From the right click context menu select **Unmanage**.

   Entuity marks the port as unmanaged. When you have the **Show Unmanaged Ports** permission selected through Preferences, you can still view the unmanaged port in Entuity through the device’s port list.



Consolidate servers: on

- Key Devices
  - 10.44.1.43
  - 10.44.4.242
  - bottom2960
  - bottom3550
  - c3560
    - [ Fa0/1 ] FastEthernet0/1
    - [ Fa0/2 ] FastEthernet0/2
    - [ Fa0/4 ] FastEthernet0/4
    - [ Fa0/5 ] FastEthernet0/5
    - [ Fa0/6 ] FastEthernet0/6
    - [ Fa0/7 ] FastEthernet0/7
    - [ Fa0/8 ] FastEthernet0/8
    - [ Fa0/9 ] FastEthernet0/9
    - [ Fa0/10 ] FastEthernet0/10
    - [ Fa0/11 ] FastEthernet0/11
    - [ Fa0/12 ] FastEthernet0/12
    - [ Fa0/13 ] FastEthernet0/13
    - [ Fa0/14 ] FastEthernet0/14

Switch Device: c3560

*Key Devices (ENTLONPPVM01)*

| | Port | In Speed | Out Speed | Fast Util | Fast Status | Status Events | Spare |
|---|---|---|---|---|---|---|---|
| ✓ | [ Fa0/1 ] FastEtl | 100 Mbps | 100 Mbps | No | No | Yes | No |
| ✓ | [ Fa0/2 ] FastEtl | 100 Mbps | 100 Mbps | No | No | Yes | No |
| ⏸ | [ Fa0/3 ] FastEtl | | | | | | |
| ✗ | tEtl | 10 Mbps | 10 Mbps | No | No | No | No |
| ✓ | [ Fa0/5 ] FastEtl | 100 Mbps | 100 Mbps | No | No | No | No |
| ✗ | [ Fa0/6 ] FastEtl | 10 Mbps | 10 Mbps | No | No | No | No |
| ✗ | [ Fa0/7 ] FastEtl | 10 Mbps | 10 Mbps | No | No | No | No |
| ✗ | [ Fa0/8 ] FastEtl | 10 Mbps | 10 Mbps | No | No | No | No |
| ✗ | [ Fa0/9 ] FastEtl | 10 Mbps | 10 Mbps | No | No | No | No |
| ✗ | [ Fa0/10 ] FastE | 10 Mbps | 10 Mbps | No | No | No | No |
| ✓ | [ Fa0/11 ] FastE | 100 Mbps | 100 Mbps | No | No | Yes | No |
| ✓ | [ Fa0/12 ] FastE | 100 Mbps | 100 Mbps | No | No | Yes | No |
| ✗ | [ Fa0/13 ] FastE | 10 Mbps | 10 Mbps | No | No | No | No |
| ✗ | [ Fa0/14 ] FastE | 10 Mbps | 10 Mbps | No | No | No | No |

Figure 12 Unmanaged Port

### Viewing and Remanaging of Unmanaged Ports

By default Entuity does not show unmanaged ports. You can view them when you have **Show Unmanaged Ports** selected through Preferences and then they are available through the device’s port list. You can also make them available again for Entuity to manage:

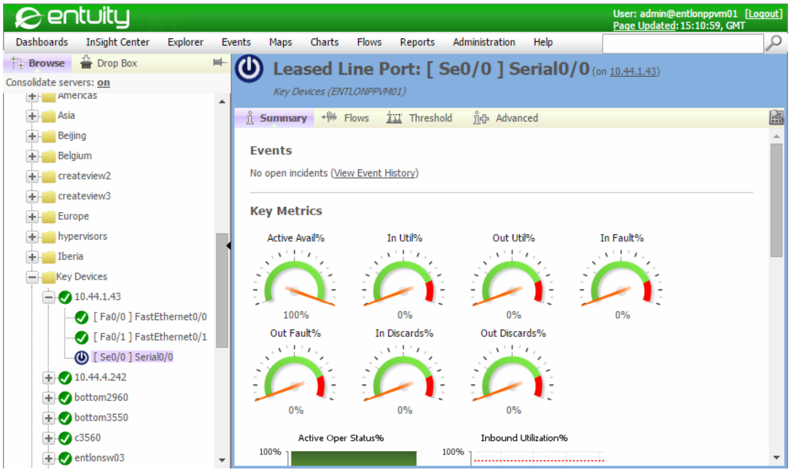
1) From Explorer display the device Ports tab.

2) Highlight the unmanaged ports and from the context menu click **Remanage**.

   Entuity adds the ports to the devices it manages the next time `prodigy` runs.

### Ports Set to Admin Down

For ports that are set to Administration Down Entuity associates to them the port Admin Down icon and sets their status color code to blue. Entuity considers these ports as available because the network administrator has taken down the ports and to associate an error state would therefore be misleading.



No open incidents (View Event History)

Figure 13 Port Admin Down

## Managing Port Attributes

Most of these fields can be amended through an Edit dialog, those fields which are grayed out are read only.

| Attribute | Description |
|---|---|
| *Operational Status* | Port's link status:<br>■ Up<br>■ Down<br>■ Testing<br>■ Dormant<br>■ Not Present<br>■ Lower Layer Down<br>■ Unknown. |
| *Description* | Interface description. |

Table 2 Extended Port Information

| Attribute | Description |
|---|---|
| *Device* | Port’s device IP address. |
| *Classification* | Indicates whether the port is a virtual or physical port. |
| *Alias* | Administrator defined interface name. |
| *Outbound Speed* | Outbound interface speed which Entuity uses when calculating port outbound utilization. Administrators can amend this reference value. |
| *Inbound Speed* | Inbound interface speed which Entuity uses when calculating port inbound utilization. Administrators can amend this reference value. |

Table 2 Extended Port Information

## Promoting Ports to Infrastructure Ports

Infrastructure Only is a presupplied content filter that limits the ports shown to infrastructure ports:

- Uplinks, i.e. ports connecting routers with switches.
- Trunk ports, i.e. ports connecting switches together.
- Router ports.

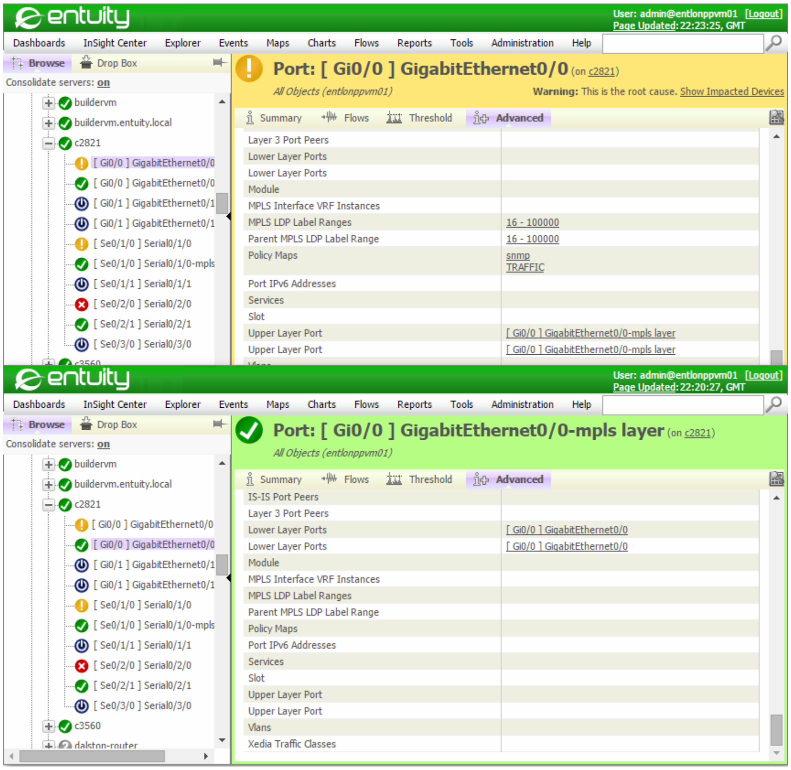
The VIPMAN Trunk Promote module, enabled through `configure`, allows you to manually promote selected ports to infrastructure port.

## Upper and Lower Layer Ports

Port channels aggregate multiple physical interfaces into one logical interface, identified in Entuity as an upper layer port.

Port channels are often used to increase link bandwidth, load balance traffic and deliver high availability. Knowledge of the interfaces contributing to a channel, and their current state is important to maintaining service delivery.

Administrators may configure physical ports into a series of channels, identified in Entuity as lower layer ports.



Port: [ Gi0/0 ] GigabitEthernet0/0 (on c2821)

All Objects (entlonppvm01)

Warning: This is the root cause. Show Impacted Devices

| | |
|---|---|
| Layer 3 Port Peers | |
| Lower Layer Ports | |
| Lower Layer Ports | |
| Module | |
| MPLS Interface VRF Instances | |
| MPLS LDP Label Ranges | 16 - 100000 |
| Parent MPLS LDP Label Range | 16 - 100000 |
| Policy Maps | snmp<br>TRAFFIC |
| Port IPv6 Addresses | |
| Services | |
| Slot | |
| Upper Layer Port | [ Gi0/0 ] GigabitEthernet0/0-mpls layer |
| Upper Layer Port | [ Gi0/0 ] GigabitEthernet0/0-mpls layer |

Port: [ Gi0/0 ] GigabitEthernet0/0-mpls layer (on c2821)

All Objects (entlonppvm01)

| | |
|---|---|
| IS-IS Port Peers | |
| Layer 3 Port Peers | |
| Lower Layer Ports | [ Gi0/0 ] GigabitEthernet0/0 |
| Lower Layer Ports | [ Gi0/0 ] GigabitEthernet0/0 |
| Module | |
| MPLS Interface VRF Instances | |
| MPLS LDP Label Ranges | |
| Parent MPLS LDP Label Range | |
| Policy Maps | |
| Port IPv6 Addresses | |
| Services | |
| Slot | |
| Upper Layer Port | |
| Upper Layer Port | |
| Vlans | |
| Xedia Traffic Classes | |

Figure 14 Upper and Lower Layer Ports

# Managing VLANs

Virtual Local Area Networks (VLANs) are single-broadcast domains that often use switches to isolate domain traffic from the network. VLANs are logical rather than physical domains, so VLAN devices do not have to be located physically together. This allows you to use VLANs to group in the same broadcast domain workstations located on different floors of a building, or even in different buildings.

VLANs configured on your network are only visible to Entuity when `protean` and `domman` have run. Each night `protean` deletes VLAN data from the Entuity database, subsequently `domman` adds the latest VLAN data.

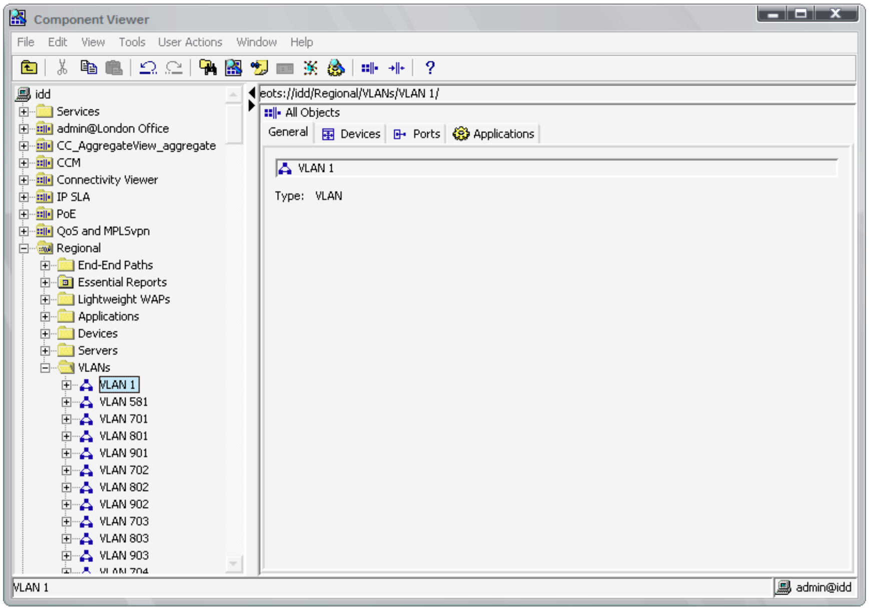
Entuity has a range of reports that you can run on the VLANs. You can also manage these VLANS through Entuity:

- Reassigning devices to different VLANs.
- Renaming VLANs.

## Viewing VLANs

You can view VLANs as properties of the highlighted:

- View, e.g. VLAN under a Regional view.
- Device, i.e. alongside port, module and application type information.
- Port.



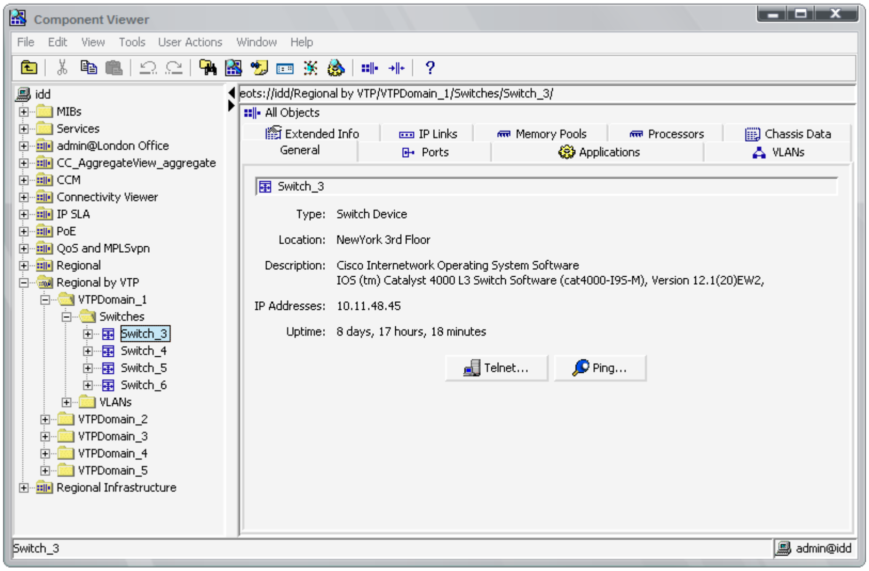
Type: VLAN

Figure 15 Viewing VLANs

## Viewing VLANs by VTP Domain

`vtpDomainTool` automatically assigns aliases for use in Entuity, enabling Entuity to distinguish between VLANs that have the same name but are members of a different VTP domain. The VLAN alias is built by combining the VTP Domain Name with the VLAN name. `vtpDomainTool` also generates a view called **All Objects by VTP**, which shows devices and VLANs grouped by VTP domain name.

`vtpDomainTool` can be run from the command line or scheduled and run by `provost`. (See *Entuity System Administrator Reference Manual.*) It uses information collected by `vtpman` to identify devices and VLANs, and their correct VTP domains. To maintain the accuracy of the view, you should schedule `vtpDomainTool` to run after `vtpman` has completed.



Type: Switch Device

Location: NewYork 3rd Floor

Description: Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I9S-M), Version 12.1(20)EW2,

IP Addresses: 10.11.48.45

Uptime: 8 days, 17 hours, 18 minutes

Figure 16 View VLANS by VTP Domain

## Reassigning Devices to Different VLANs

Reassigning devices is useful when the VLANs configured on your network differ from those represented in Entuity, e.g. in Entuity VLANs with the same name are combined. (See *Same Name VLANs Combined*.)

## Renaming VLANs

Entuity allows you to rename VLANs, either by entering a new name or restoring their original name.

To rename a VLAN:

> Entuity renames the VLAN. After the next running of `grouper` reports are available showing the amended VLAN name.

# Resetting User Override Attribute Values

Extended Information that has been amended can be reset to its discovered value using Reset User Override. Reset User Override deletes the amended attribute value, and marks the attribute for discovery. The discovered value will only appear in Entuity after the Discovery, a time delay which can take up to two hours.

Reset Override is context dependent for its scope, for example when you use Reset User Override with:

- A port highlighted then all amended Extended Info attributes on that port are reset to their discovered values.

- A device highlighted all amended Extended Info attributes on the device and its ports are reset to their discovered values.
- An Entuity server highlighted then all amended Extended Info attributes are reset to their discovered values.

To reset user override attributes:

1)

2) From the context menu click **Reset User Override**.

# 17 Performance and Availability Management

Entuity provides a set of tools that allow you to monitor the performance and availability of your network:

- Entuity availability monitoring identifies the root failure, and so does not involve the raising of misleading downstream events. It combines data from:
  - Application availability monitoring through response to TCP connect requests.
  - Availability monitoring which uses data collected through ICMP pings of network objects.
- Services which comprise of:
  - A service definition which acts as an object to which you can associate components that make up that service.
  - Components, e.g. device, ports, applications and other services, that make up the delivered service.
- Performance and Asset Utilization, Entuity delivers key measures of asset utilization across a range of technologies, allowing you to identify over and under utilized resources and make purchasing decisions based on true network requirements.
- Edge of Network Change, which monitors hardware changes and additions through changes of MAC addresses. for example, hardware changes and additions to the network in a remote office can significantly impact network performance.

All are integrated within Entuity, allowing you to use them in conjunction with other tools and access information through events and incidents, graphs and charts, and reports.

## Accessing the Network Delivery Perspective

The Network Delivery Perspective provides a high level, view based summary of network service delivery against four key components: services, applications, server devices and infrastructure devices. For each component it provides a summary of availability and latency, with a more detailed summary also including links to component specific availability reports. The perspective is also available in a layout suitable for printing.

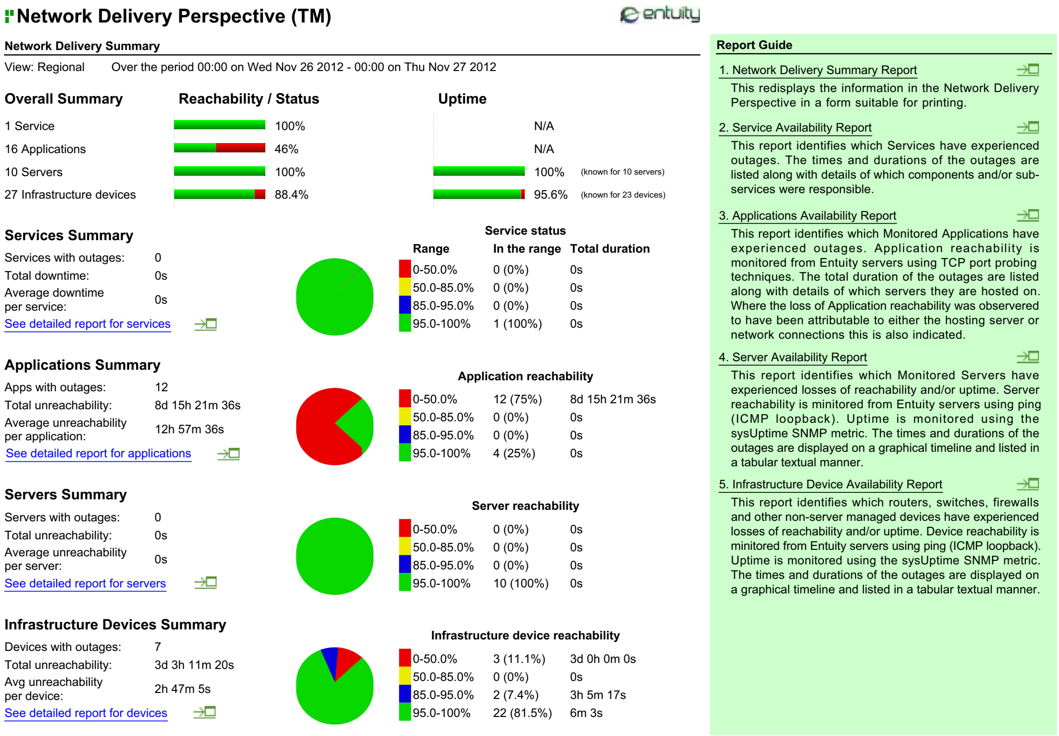
To access the Network Delivery Perspective:

1) Click **InSight Center > Network Delivery Perspective**.

   The perspective is also available through **Reports > Availability Reports > Network Delivery Perspective** or when you want the print friendly form, **Reports > Availability Reports> Network Delivery Summary**.

2) From the drop down lists select the Entuity server and view against which you want to run the report. You can also amend the reporting period which by default is set to the previous day.

Extending the reporting period and/or running the perspective against a view with a large number of components increases the amount of data the perspective must retrieve from the database. This can cause a delay in Entuity displaying the perspective.



**Network Delivery Perspective (TM)**

**Network Delivery Summary**

View: Regional     Over the period 00:00 on Wed Nov 26 2012 - 00:00 on Thu Nov 27 2012

| Overall Summary | Reachability / Status | Uptime | |
|---|---|---|---|
| 1 Service | 100% | N/A | |
| 16 Applications | 46% | N/A | |
| 10 Servers | 100% | 100% | (known for 10 servers) |
| 27 Infrastructure devices | 88.4% | 95.6% | (known for 23 devices) |

**Services Summary**

| | |
|---|---|
| Services with outages: | 0 |
| Total downtime: | 0s |
| Average downtime per service: | 0s |

See detailed report for services

**Service status**

| | Range | In the range | Total duration |
|---|---|---|---|
| 🟥 | 0-50.0% | 0 (0%) | 0s |
| 🟨 | 50.0-85.0% | 0 (0%) | 0s |
| 🟦 | 85.0-95.0% | 0 (0%) | 0s |
| 🟩 | 95.0-100% | 1 (100%) | 0s |

**Applications Summary**

| | |
|---|---|
| Apps with outages: | 12 |
| Total unreachability: | 8d 15h 21m 36s |
| Average unreachability per application: | 12h 57m 36s |

See detailed report for applications

**Application reachability**

| | | | |
|---|---|---|---|
| 🟥 | 0-50.0% | 12 (75%) | 8d 15h 21m 36s |
| 🟨 | 50.0-85.0% | 0 (0%) | 0s |
| 🟦 | 85.0-95.0% | 0 (0%) | 0s |
| 🟩 | 95.0-100% | 4 (25%) | 0s |

**Servers Summary**

| | |
|---|---|
| Servers with outages: | 0 |
| Total unreachability: | 0s |
| Average unreachability per server: | 0s |

See detailed report for servers

**Server reachability**

| | | | |
|---|---|---|---|
| 🟥 | 0-50.0% | 0 (0%) | 0s |
| 🟨 | 50.0-85.0% | 0 (0%) | 0s |
| 🟦 | 85.0-95.0% | 0 (0%) | 0s |
| 🟩 | 95.0-100% | 10 (100%) | 0s |

**Infrastructure Devices Summary**

| | |
|---|---|
| Devices with outages: | 7 |
| Total unreachability: | 3d 3h 11m 20s |
| Avg unreachability per device: | 2h 47m 5s |

See detailed report for devices

**Infrastructure device reachability**

| | | | |
|---|---|---|---|
| 🟥 | 0-50.0% | 3 (11.1%) | 3d 0h 0m 0s |
| 🟨 | 50.0-85.0% | 0 (0%) | 0s |
| 🟦 | 85.0-95.0% | 2 (7.4%) | 3h 5m 17s |
| 🟩 | 95.0-100% | 22 (81.5%) | 6m 3s |

**Report Guide**

1. Network Delivery Summary Report
   This redisplays the information in the Network Delivery Perspective in a form suitable for printing.
2. Service Availability Report
   This report identifies which Services have experienced outages. The times and durations of the outages are listed along with details of which components and/or sub-services were responsible.
3. Applications Availability Report
   This report identifies which Monitored Applications have experienced outages. Application reachability is monitored from Entuity servers using TCP port probing techniques. The total duration of the outages are listed along with details of which servers they are hosted on. Where the loss of Application reachability was observed to have been attributable to either the hosting server or network connections this is also indicated.
4. Server Availability Report
   This report identifies which Monitored Servers have experienced losses of reachability and/or uptime. Server reachability is minitored from Entuity servers using ping (ICMP loopback). Uptime is monitored using the sysUptime SNMP metric. The times and durations of the outages are displayed on a graphical timeline and listed in a tabular textual manner.
5. Infrastructure Device Availability Report
   This report identifies which routers, switches, firewalls and other non-server managed devices have experienced losses of reachability and/or uptime. Device reachability is minitored from Entuity servers using ping (ICMP loopback). Uptime is monitored using the sysUptime SNMP metric. The times and durations of the outages are displayed on a graphical timeline and listed in a tabular textual manner.

Figure 17 Network Delivery Perspective

# 18 Application Availability and Latency

Entuity monitors application availability by testing the response of defined applications to its TCP connect request. Entuity considers an application as available if Entuity can connect to the application's open socket. By default every two minutes Entuity attempts to connect to monitored applications.

Entuity can also determine application performance by measuring the latency of the application's response to the request. Also, when determining the root cause of a problem Entuity can include application state.

You can monitor application availability through:

- Reports, for example the Network Availability Perspective, Application Availability Report, Server Availability Report.
- Events and incidents, AvailMonitor events includes application details, Network Outage events a count of impacted applications.
- Summaries available through the Device Summary dashboard.
- Application page of a device where you can view hosted and attached applications.

The device-level Applications page allows you to view, add, delete and amend the applications associated with a device.

Making an application available for monitoring involves:

1) Defining the application type within Entuity or using a predefined application type. (See *Manage Application Types*.)
2) Associating the Entuity defined application with devices that are hosting these target applications. (See *Monitor Applications*).
3) Entuity using the application definition together with the entered location to discover the applications.

Entuity also measures device latency but calculates it as the time between an Entuity server sending an ICMP Ping Echo request to the management IP address of a device and receiving a response.

## Viewing Applications

Applications are monitored on devices. Once set up, you can manage applications through the hosting device or an attached device. The Application Availability report provides an inventory and status summary of all of the applications on the selected devices. Select All Devices and Entuity generates a report that lists all of the applications on the server.

From the device Applications page you can view and manage:

- Attached Applications, applications running on attached devices.

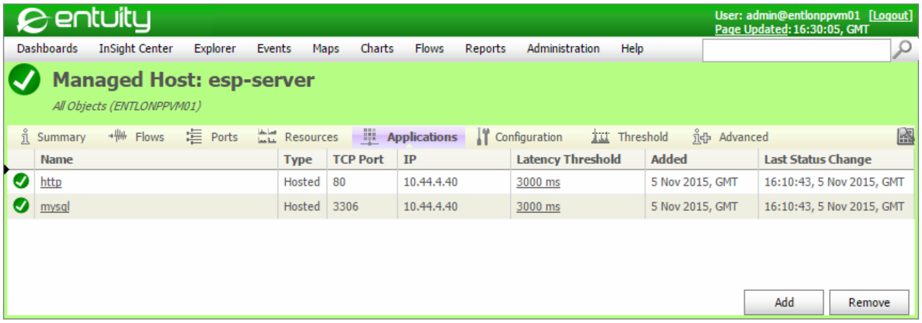
- Hosted Applications, applications running on the device itself.

Users with administrator access rights can also configure which applications to monitor on a device. Entuity regularly checks application availability on those devices for which you have set up applications.

To view applications on a device:

1) Click **Explorer** and then a device.

2) From the Device Summary page click **Applications**.



Managed Host: esp-server

*All Objects (ENTLONPPVM01)*

| | Name | Type | TCP Port | IP | Latency Threshold | Added | Last Status Change |
|---|---|---|---|---|---|---|---|
| ✓ | http | Hosted | 80 | 10.44.4.40 | 3000 ms | 5 Nov 2015, GMT | 16:10:43, 5 Nov 2015, GMT |
| ✓ | mysql | Hosted | 3306 | 10.44.4.40 | 3000 ms | 5 Nov 2015, GMT | 16:10:43, 5 Nov 2015, GMT |

Figure 18 Applications on a Device

| Attribute | Description |
|---|---|
| *Device Name* | Identifies the device. The color of the icon indicates the device status. You use the text rollover to view details. (See *Object States*.) |
| Each row in the application table details a monitored application. | |
| Application State | Icon representing the current state of the application. You use the text rollover to view details. If the application's device is down Entuity sets the port state to Unknown. (See *Object States*.) |
| *Name* | Application name which is taken from the underlying application type. It is also a hyperlink to the Application Summary page. |
| *Type* | Identifies the application type:<br>■ Hosted applications are hosted on the device.<br>■ Attached applications are hosted on devices networked to the current device. |
| *TCP Port* | Application port Entuity connects to when establishing the application's availability through a TCP connect request. |
| *IP* | IP address of the application device used when monitoring the application. |
| *Latency Threshold* | Entuity measures Entuity server to application latency through the time taken to receive a response from a successful TCP connect request. When this value is above the set threshold Entuity raises an AvailMonitor High Latency Reaching Application event. |

Table 3 Applications on a Device

| Attribute | Description |
|---|---|
| *Added* | Date the application was defined in Entuity. |
| *Last Status Change* | Date and time Entuity last reported a change in the availability status of the application. |

Table 3 Applications on a Device

## Application States

If an application does not respond to Entuity within the time frame set by the:

- Application Latency threshold Entuity sets the application state to Degraded (yellow).

  You can set threshold levels through the Thresholds page.
- Application Timeout threshold and it is the root cause of the problem then Entuity sets the application state to Down (red).
- Application Timeout threshold and it is not the root cause then Entuity sets the application state to Unknown (grey).

  You can set the application timeout threshold through a section in *entuity_home*`\etc\entuity.cfg`:

```
[applicationmonitor]
```

```
appTimeout=8
```

Where *appTimeout* defines the system wide application timeout in seconds, by default set to 5 seconds.

# Manage Application Types

Entuity is supplied with a number of application types that you can use when setting up application monitoring. For Entuity to monitor an application it must be associated to an application type. An application type definition comprises of:

- *Name* the application type name.
- *Port* (TCP) the application TCP port Entuity connects to when establishing the application's availability.

| Application Name | Port Number | Application Name | Port Number |
|---|---|---|---|
| citrix-ica | 1494 | netbios-ssn | 139 |
| dns | 53 | netware-ip | 396 |
| ftp | 21 | nfs | 2049 |
| http | 80 | novell-groupwise | 1677 |
| https | 443 | ntp | 123 |
| imap2 | 143 | oracle | 1525 |
| imap3 | 220 | pop3 | 110 |

Table 4 Default Application Types and their TCP Ports

| Application Name | Port Number | Application Name | Port Number |
|---|---|---|---|
| imap4-ssl | 993 | pop3-ssl | 995 |
| ldap | 389 | smtp | 25 |
| ldap-ssl | 636 | sun-rpc | 111 |
| ms-sqlserver | 1433 | sybase-sqlanywhere | 1498 |
| ms-termserv | 3389 | telnet | 23 |
| mysql | 3306 | web | 80 |

Table 4 Default Application Types and their TCP Ports

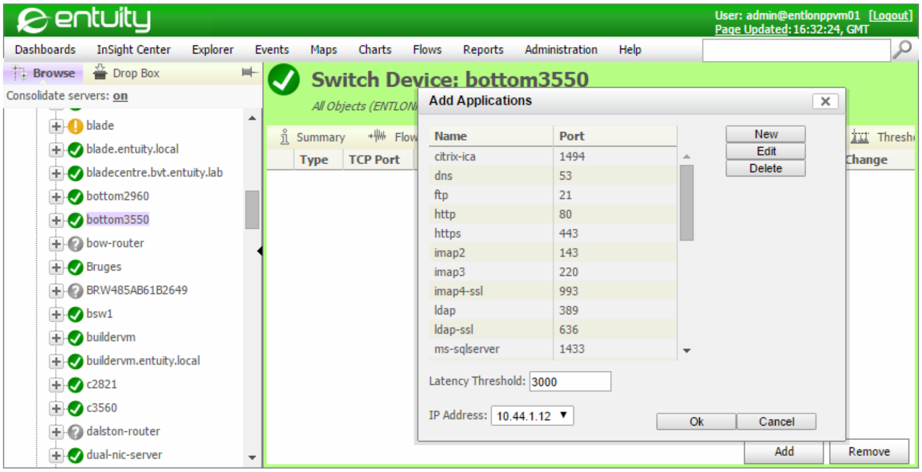
## Adding Application Types

To view and add to the current list of application types:

1) Click **Explorer** and then a device.

2) From the Device Summary page click **Applications**.

3) Click **Add**. Entuity displays the available application types.



User: admin@entlonppvm01 [Logout]
Page Updated: 16:32:24, GMT

Consolidate servers: on

Switch Device: bottom3550

All Objects (ENTLON

Add Applications

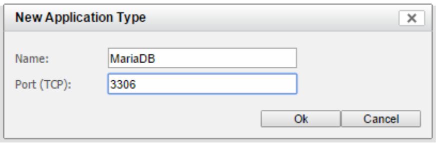
| Name | Port |
|---|---|
| citrix-ica | 1494 |
| dns | 53 |
| ftp | 21 |
| http | 80 |
| https | 443 |
| imap2 | 143 |
| imap3 | 220 |
| imap4-ssl | 993 |
| ldap | 389 |
| ldap-ssl | 636 |
| ms-sqlserver | 1433 |

Latency Threshold: 3000

IP Address: 10.44.1.12

Figure 19 Displaying Application Types

- Click **New**. and enter the *Name* and *Port* (TCP).



New Application Type

Name: MariaDB

Port (TCP): 3306

Figure 20 Adding Application Types

### Amending Application Types

To amend a user defined application type:

1) Click **Explorer** and then a device.
2) From the Device Summary page click **Applications**.
3) Click **Add**.
4) Highlight an application type and click **Edit**.
5) Amend the application type definition.

### Deleting Application Types

To delete an application type:

1) Click **Explorer** and then a device.
2) From the Device Summary page click **Applications**.
3) Click **Add**.
4) Highlight the application type and click **Delete**. Entuity deletes the application.

## Monitor Applications

A monitored application is a process running on a device that communicates with its associated clients via a TCP connection. From the Applications page you can view, create, edit and delete applications.

An Entuity defined application can only be monitored through Entuity when the location of the application on the network is known. You can associate applications with devices when:

- The application type is first created in Entuity.
- Additional copies of the application are added to servers outside of the servers currently monitored.
- A monitored application is moved to a different server.

To monitor an application:

1) Click **Explorer** and then a device.
2) From the Device Summary page click **Applications**.
3) Click **Add**.
4) Highlight the application you want to monitor on that device. Where it has more than one IP address select the appropriate one.
5) Click **OK**.

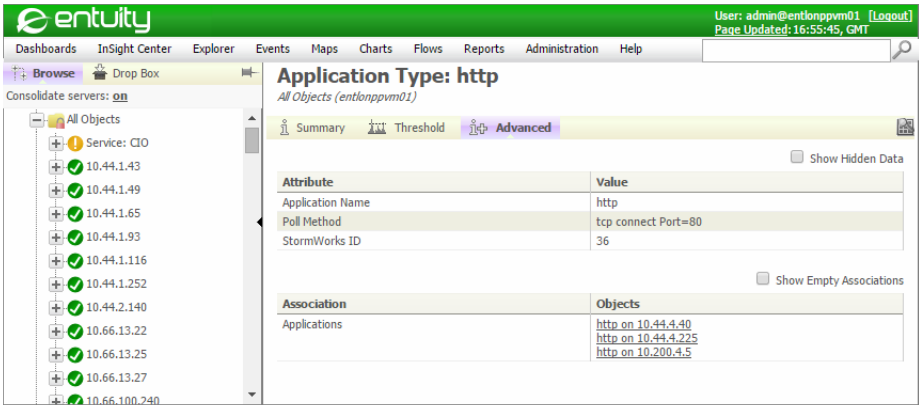
   Entuity associates the application type with the device. Depending upon the activity on your network there may be a short delay between you defining an application and Entuity discovering it.

## Finding All Instances of an Application Type

You can view all applications on a device by running the Application Availability report. You can also view all applications of the same type together with their hosting device through Explorer. You use the association between the monitored application and its application type to then view all of the applications using that application type.

For example to view all of the monitored web applications:

1) Click **Explorer** and then a device for which Entuity is monitoring a web application.
2) From the Device Summary page click **Applications**.
3) Click **web** in the applications table. This is a hyperlink to the Applications page. You may have to expand the table to view the *Name* column.
4) Click Advanced and then from the Association section for the Application Type click web.
5) Application Type Summary page provides a summary of the application type definition and also the state of each monitored application. Click **Advanced** to view a fuller listing of applications.



Application Type: http

*All Objects (entlonppvm01)*

| Attribute | Value |
|---|---|
| Application Name | http |
| Poll Method | tcp connect Port=80 |
| StormWorks ID | 36 |

| Association | Objects |
|---|---|
| Applications | http on 10.44.4.40<br>http on 10.44.4.225<br>http on 10.200.4.5 |

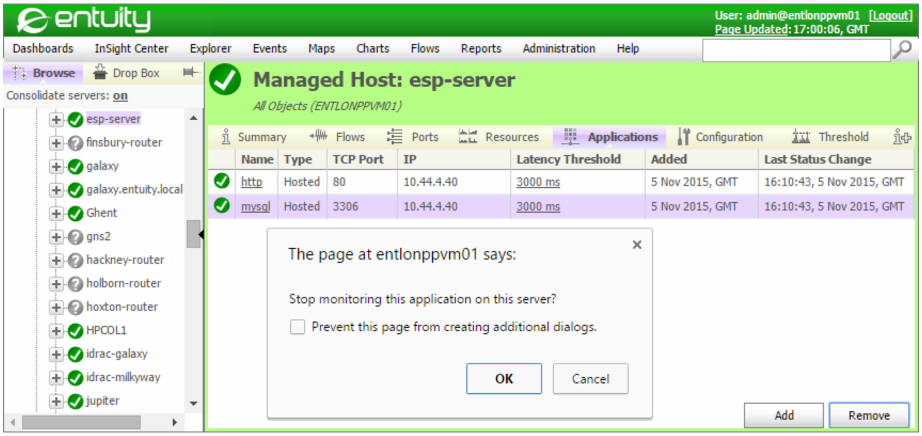
Figure 21 All Monitored Applications

## Stop Monitoring Applications on Devices

When you remove an application from a device you are not deleting the application type from Entuity. You are only stopping Entuity from monitoring the availability of an application on that device.

To stop monitoring an application on a device:

1) Click **Explorer** and then a device.
2) From the Summary page click **Applications**.
3) Highlight the application you want to delete and click **Remove**. You can select more than one application.
4) Click **OK** to confirm stopping monitoring of the application on the device.



Managed Host: esp-server

*All Objects (ENTLONPPVM01)*

| | Name | Type | TCP Port | IP | Latency Threshold | Added | Last Status Change |
|---|---|---|---|---|---|---|---|
| ✓ | http | Hosted | 80 | 10.44.4.40 | 3000 ms | 5 Nov 2015, GMT | 16:10:43, 5 Nov 2015, GMT |
| ✓ | mysql | Hosted | 3306 | 10.44.4.40 | 3000 ms | 5 Nov 2015, GMT | 16:10:43, 5 Nov 2015, GMT |

The page at entlonppvm01 says:

Stop monitoring this application on this server?

□ Prevent this page from creating additional dialogs.

OK Cancel

Figure 22 Remove Application from a Device

# 19 Network Availability Monitoring

Entuity's availability monitoring tracks the availability status of managed objects:

- Layer 3 port availability from data gathered through ICMP pinging of port IP addresses.
- Device availability by combining the results of ICMP pinging of a device's IP addresses.
- Application availability by recognizing the success or otherwise of a TCP connect to an application.
- Managed object latency by recording the time the object takes to respond to the ICMP ping.

Entuity provides clear and timely information on changes in network availability and latency:

- Events and incidents identify changes in the availability of devices, ports and IP addresses. Entuity root cause analysis clearly identifies the cause of problems in network availability, and the impact of that failure on service delivery.
- Rolling latency data into hourly averages and using it when calculating trending values. You can set thresholds against latency and latency trend data.
- You can set thresholds against views for Entuity to raise events and incidents when average latency for all devices in the view exceeds the set threshold.
- Through both supplied dashboards and reports and the option to include availability and latency data into custom dashboards and user defined reports.
- Maps provide a graphical representation of layer 3 availability, including a traceroute overlay option with real-time update of object status.

## ICMP Ping Availability Monitoring

Every ten minutes `applicationMonitor` builds a list of IP addresses on which to gather availability data. This list defines the end destinations for all traceroute and ping operations within each ten minute polling cycle. `applicationMonitor` builds the IP address polling list:

- From the list of devices under the Entuity server's management, converting host names to IP addresses.
- From the list of IP Addresses associated with ports, but ignoring IP addresses of ports with status administratively down. Layer 2 switches do not have IP addresses associated with their ports.
- By ignoring IP addresses of ports that are unmanaged.

- By excluding IP addresses discovered on more than one device.
- From the list of all IP addresses associated with managed devices. This includes IP addresses that are not mapped to ports.

The IP address polling list is then read by `applicationMonitor` and used with traceroute, which runs every two minutes. Entuity availability monitoring, by default, pings an IP address, waits three seconds for a response and, if a response is not returned, sends another ICMP Ping Echo request to the same address. Entuity pings a non-responding address up to three times before determining the address is not reachable.

When Entuity does send more than one ping to a device, and then receives a response, it can identify which ping elicited the response through the ping’s sequence number.

## Set Up ICMP Monitoring

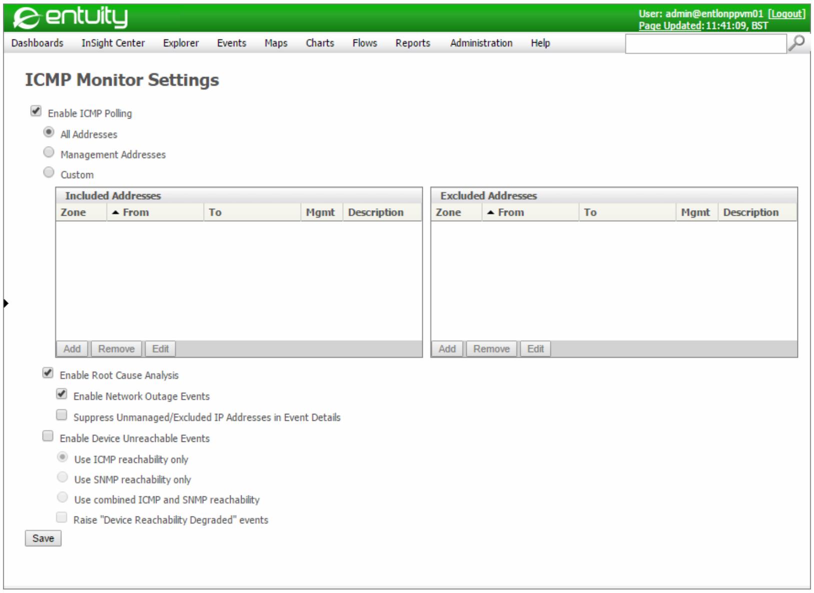
If you are a member of the Administrators user group, you can set up and maintain the IP addresses Entuity uses with availability monitoring. When you make and apply a change to your ICMP ping setup, these changes are active within ten minutes, i.e. at the time Entuity next updates its list of IP addresses to ping.

You can include and exclude individual IP addresses, include and exclude ranges of IP addresses and use a combination of both methods. If you both include and exclude an IP address Entuity considers it as excluded and therefore not on the list of monitored IP addresses. For ports with IP addresses that are excluded from pinging, Entuity sets their state to ICMP Disabled.

Entuity supports both IPv4 and IPv6 address formats.

To view and set ICMP Monitor Settings:

1) Select **Administration** > **Inventory** / **Topology** > **ICMP Monitor**.



ICMP Monitor Settings

☑ Enable ICMP Polling

● All Addresses

○ Management Addresses

○ Custom

| Included Addresses | | | | |
|---|---|---|---|---|
| Zone | ▲ From | To | Mgmt | Description |

Add Remove Edit

| Excluded Addresses | | | | |
|---|---|---|---|---|
| Zone | ▲ From | To | Mgmt | Description |

Add Remove Edit

☑ Enable Root Cause Analysis

☑ Enable Network Outage Events

☐ Suppress Unmanaged/Excluded IP Addresses in Event Details

☐ Enable Device Unreachable Events

● Use ICMP reachability only

○ Use SNMP reachability only

○ Use combined ICMP and SNMP reachability

☐ Raise "Device Reachability Degraded" events

Save

Figure 23 ICMP Monitor Settings

2) Configure the ICMP monitor settings and to apply them click **Save**.

| Attribute | Description |
|---|---|
| *Enable ICMP Polling* | Enabled by default. To control the IP addresses Entuity pings, select:<br>■ **All Addresses** for Entuity to ping all known IP addresses of devices under its management.<br>■ **Management Addresses** for Entuity to ping only the management IP addresses of devices under its management.<br>■ **Custom** to set the IP addresses for Entuity to include or exclude from its availability monitoring. You can define individual IP addresses or ranges of IP addresses, both IPv4 and IPv6.<br>Entuity sets the state of ports with IP addresses that it is not pinging to ICMP disabled. |
| *Enable Root Cause Analysis* | Enabled by default. Entuity identifies the root cause of a network failure and only raises events and incidents against that network object. When not enabled Entuity would raise events and incidents for each network object impacted by a network failure but only if *Enable Device Unreachable Events* has been enabled. |
| *Enable Network Outage Events* | Enabled by default. Network Outage is an important event for alerting you to the cause of a network outage and its impact. |

Table 5 ICMP Monitor Settings

| Attribute | Description |
|---|---|
| *Suppress Unmanaged/ Excluded IP Addresses in Event Details* | When selected, Entuity excludes from raised events and incidents the details of unmanaged IP addresses or IP addresses that you have excluded from availability monitoring. |
| *Enable Device Unreachable Events* | Not enabled by default. Select the reachability metric, or metrics, appropriate to the devices being monitored:<br>■ Use ICMP reachability only<br>■ Use SNMP reachability only<br>■ Use combined ICMP and Reachability.<br>Select **Raise Device Reachability Degraded events** to allow the raising of the Device Reachability Degraded event.<br>The Network Outage event is only raised against devices that are the root cause of the outage. The Device Unreachable and Device Reachability Degraded event are raised against any device Entuity identifies as unreachable. |

Table 5 ICMP Monitor Settings

## Device Latency

Entuity measures device latency as the time between an Entuity server sending an ICMP Ping Echo request to the management IP address of a device and receiving a response. Entuity records device response time to its ICMP ping as *ICMP Latency*. Entuity can also derive from this metric three additional latency metrics, *Average ICMP Latency Hourly*, *% ICMP Latency Exceeds Hourly* and *ICMP Latency Trend*. For Entuity to collect device average latency information you must enable the *High Latency Threshold* for each device.

You can set latency thresholds against all devices managed by the Entuity server or against individual devices. All latency thresholds are disabled by default.

Entuity also measures application latency and calculates it as the time between an Entuity server sending a TCP connect request to the IP address associated with the application and receiving a response.

You can monitor a network’s latency through:

- Gauges and charts available from the device Summary page. You can click through and view configurable charts.
- Graphs that report latency.
- Latency reports.
- Events and incidents Entuity raises when a device’s latency value exceeds a set latency threshold.

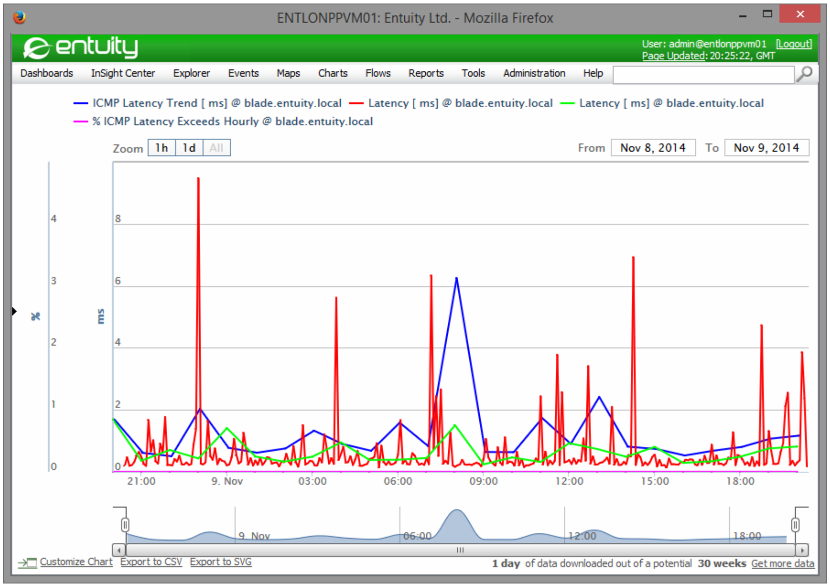

ENTLONPPVM01: Entuity Ltd. - Mozilla Firefox
entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 20:25:22, GMT
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Tools
Administration
Help
ICMP Latency Trend [ ms] @ blade.entuity.local
Latency [ ms] @ blade.entuity.local
Latency [ ms] @ blade.entuity.local
% ICMP Latency Exceeds Hourly @ blade.entuity.local
Zoom 1h 1d All
From Nov 8, 2014 To Nov 9, 2014
%
ms
0
1
2
3
4
0
2
4
6
8
21:00
9. Nov
03:00
06:00
09:00
12:00
15:00
18:00
9. Nov
06:00
12:00
18:00
Customize Chart
Export to CSV
Export to SVG
1 day of data downloaded out of a potential 30 weeks Get more data

Figure 24 Charting Device Latency

| Latency Metric | Description |
|---|---|
| *ICMP Latency* | Response time in milliseconds from Entuity sending an ICMP Ping Echo request to an IP address and receiving a response. This is original sample data from which Entuity derives all other ICMP latency values.<br>*ICMP Latency* is available through Advanced pages in the web UI and reports. |
| *Average ICMP Latency Hourly* | Mean average response time over the previous hour in milliseconds from Entuity sending an ICMP Ping Echo request to an IP address and receiving a response.<br>*Average ICMP Latency* value is available through Advanced pages in the web UI and reports. When the value for the current hourly average:<br>■ Exceeds the High Latency threshold by the set number of milliseconds, Entuity raises an AvailMonitor Latency High event.<br>■ Exceeds the previous, adjacent hourly average by the set number of milliseconds, Entuity raises an AvailMonitor Latency Rising Average event.<br>■ Falls short of the previous, adjacent hourly average by the set number of milliseconds, Entuity raises an AvailMonitor Latency Falling Average event.<br>Rising and Falling Latency thresholds are set in the device Thresholds tab. All latency events are based on hourly data. |

Table 6 Device Latency Metrics

| Latency Metric | Description |
|---|---|
| *% ICMP Latency Exceeds Hourly* | Percentage of responses over the previous hour to the IP address that exceeded the High Latency Threshold, set through the Threshold Settings dialog. Entuity does not raise events on this sample data, only on the hourly average data.<br>*% ICMP Latency Exceeds Hourly* is available through Advanced pages in the web UI and reports. |
| *ICMP Latency Trend* | Derived Exponential Moving Average (EMA) hourly trend value. To calculate the trend value Entuity combines the previous hour's average value with the EMA value calculated for the same hour a week earlier, assigning a weighting of 20 percent and 80 percent respectively.<br>For the first week Availability Monitor manages an IP address, ICMP Latency Trend and Average ICMP Latency Hourly values are the same. The data history for the object does not exceed a week so an EMA is not calculated.<br>When ICMP Latency Trend exceeds the Rising Trend Latency threshold by the set number of milliseconds, Entuity raises an AvailMonitor Rising Trend Latency event.<br>ICMP Latency Trend is available through Advanced pages in the web UI and reports. |

Table 6 Device Latency Metrics

## View Device Latency Metrics

Device Latency is a key metric, one that is charted for each device on its Summary page:

- A gauge indicates the last polled value, and when it includes a red segment also indicates that the High Latency threshold is set.
- A chart graphs the previous four hours of ICMP latency data for the device.

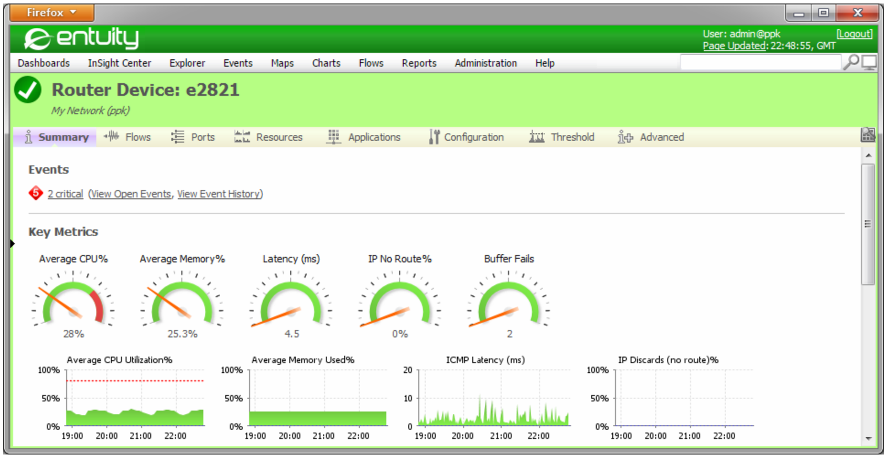


Figure 25 Device Latency Charts

If you click on the gauge or chart Entuity generates an interactive chart that displays the ICMP latency data for the device over the previous 24 hours.

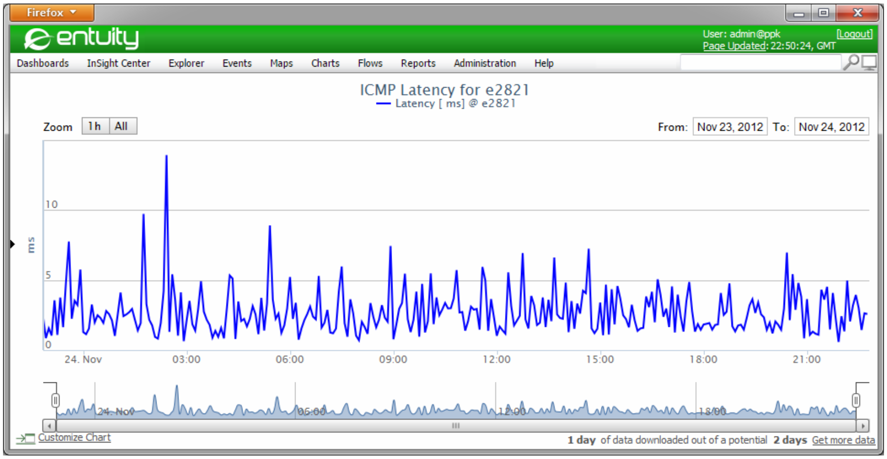


Figure 26 Charting Device Latency

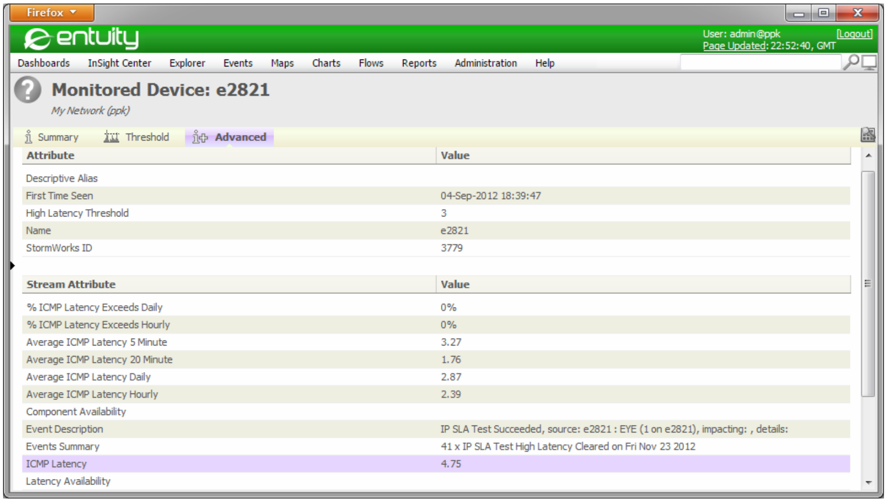
You can view and chart the raw five minute ICMP ping data, its 20 minute roll ups, hourly roll ups and daily roll ups. This data is available through the device Advanced page and utilizes the underlying data structures used by Entuity to manage object data.

To view extended device latency data:

1) From Explorer select the device and click **Advanced**.

2) Locate within the Association section *Monitored Device* and click on its hyperlink. A monitored device is a construct Entuity uses to assist in managing the selected device.

3) Click the monitored device **Advanced** tab. Entuity displays the extended ICMP latency data.



Monitored Device: e2821

*My Network (ppk)*

| Attribute | Value |
|---|---|
| Descriptive Alias | |
| First Time Seen | 04-Sep-2012 18:39:47 |
| High Latency Threshold | 3 |
| Name | e2821 |
| StormWorks ID | 3779 |

| Stream Attribute | Value |
|---|---|
| % ICMP Latency Exceeds Daily | 0% |
| % ICMP Latency Exceeds Hourly | 0% |
| Average ICMP Latency 5 Minute | 3.27 |
| Average ICMP Latency 20 Minute | 1.76 |
| Average ICMP Latency Daily | 2.87 |
| Average ICMP Latency Hourly | 2.39 |
| Component Availability | |
| Event Description | IP SLA Test Succeeded, source: e2821 : EYE (1 on e2821), impacting: , details: |
| Events Summary | 41 x IP SLA Test High Latency Cleared on Fri Nov 23 2012 |
| ICMP Latency | 4.75 |
| Latency Availability | |

Figure 27 Monitored Device for Advanced Users

## Setting Latency Thresholds

You can set latency thresholds against all devices managed by a server, all devices within Drop Box or against an individually selected device. In multi-server environments where you are using Entuity in consolidated servers mode you can set devices managed by different servers to use the same threshold setting.

| Attribute | Description |
|---|---|
| *Falling Latency Threshold* | When the average real-time latency value for the hour falls short of the previous hourly value by the set number of milliseconds, Entuity raises an AvailMonitor Falling Average Latency event. |
| *High Latency Threshold* | When the average real-time latency value for the hour exceeds the amount set, Entuity raises an AvailMonitor High Latency event.<br>For Entuity to collect device average latency information the High Latency Threshold option must be enabled. |
| *Rising Latency Threshold* | When the average real-time latency value for the hour exceeds the previous hourly value by the set number of milliseconds, Entuity raises an AvailMonitor Rising Average Latency event. |
| *Rising Trend Latency Threshold* | When the average real-time latency value for the hour exceeds the trend for the same hour of the week by the set number of milliseconds, Entuity raises an AvailMonitor Rising Average in Trend Latency event. |

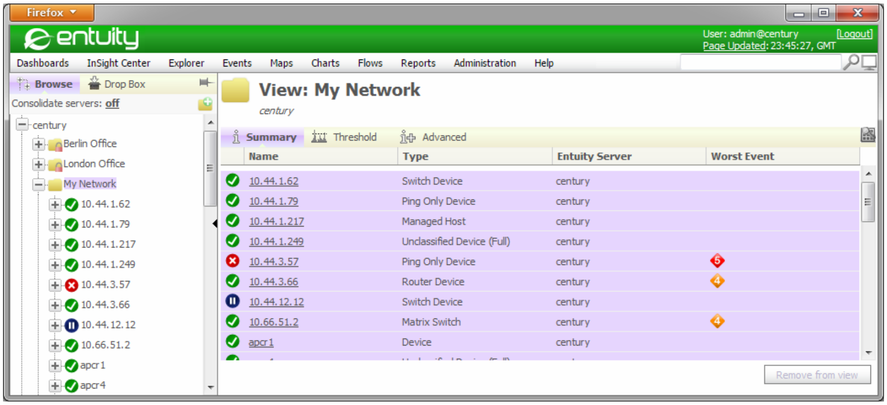
Table 7 Latency Threshold Values

✓ If a threshold is changed during the preceding hour, then the most recent setting is used in the comparison. Entuity does not retain a history of threshold settings.

For example to set latency threshold settings against all devices in a view you can use Drop Box:

1) Click **Explorer** and from the Browse tree select the view.

2) From the main Explorer pane select and then drag into Drop Box all of the devices in the view.



View: My Network

*century*

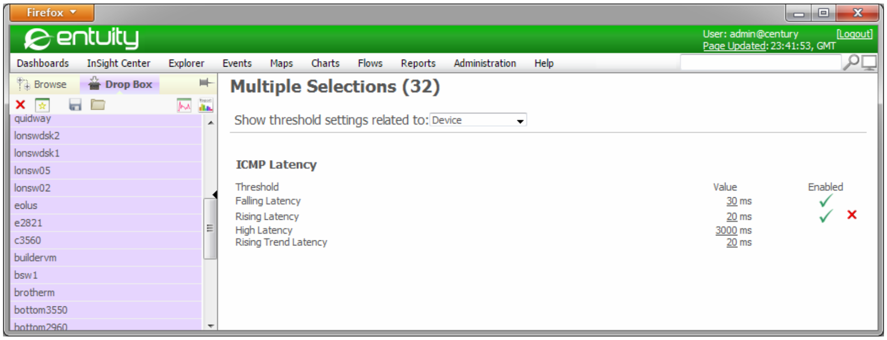
| | Name | Type | Entuity Server | Worst Event |
|---|---|---|---|---|
| ✓ | 10.44.1.62 | Switch Device | century | |
| ✓ | 10.44.1.79 | Ping Only Device | century | |
| ✓ | 10.44.1.217 | Managed Host | century | |
| ✓ | 10.44.1.249 | Unclassified Device (Full) | century | |
| ✗ | 10.44.3.57 | Ping Only Device | century | 5 |
| ✓ | 10.44.3.66 | Router Device | century | 4 |
| ⏸ | 10.44.12.12 | Switch Device | century | |
| ✓ | 10.66.51.2 | Matrix Switch | century | 4 |
| ✓ | apcr1 | Device | century | |

Figure 28 Select Devices in a View

3) Click **Drop Box** and select all of the devices.

4) From the context menu click **Threshold Settings**.

The Threshold Settings page title includes the number of multiple selections. If you dragged ten devices into Drop Box you should have ten multiple selections.



Multiple Selections (32)

Show threshold settings related to: Device

ICMP Latency

| Threshold | Value | Enabled |
|---|---|---|
| Falling Latency | 30 ms | ✓ |
| Rising Latency | 20 ms | ✓ ✗ |
| High Latency | 3000 ms | |
| Rising Trend Latency | 20 ms | |

Figure 29 Multiple Selections for Threshold Settings

5) From *Show threshold settings related to* select **Device**.

6) Set the latency thresholds.

# 20 Root Cause Analysis

Entuity Root Cause Analysis monitors the end to end delivery of IT as a service, whilst at the same time monitoring each component of the infrastructure that together make up that service. By integrating these monitoring capabilities, IT operations are able to isolate infrastructure problems at the same time as understanding their impact on business activity.

Entuity Root Cause Analysis extends the network monitoring capabilities of Entuity by alarming on both component and service failures. Entuity raises stateful alarms to the operator which automatically track ongoing problems through to resolution. Focusing on availability and latency (round trip response time) of devices and applications:

- Entuity ICMP availability monitoring pings IP addresses and maps these addresses to managed devices and ports so events and incidents are raised against devices and ports rather than IP addresses. Where Entuity does not manage the IP address Entuity associates it with the first managed port that is downstream of that IP address and indicates that the actual cause of the failure is upstream of the port.

  For every network outage that Entuity identifies, Entuity uses data derived from its ICMP availability monitoring (traceroute) to identify the layer 3 network object closest to the Entuity server involved in the outage. Entuity can then raise Network Outage incidents and events on the object.

- Entuity monitors application availability by testing the response of defined applications to its TCP connect request. Entuity considers an application as available if Entuity can connect to the application’s open socket. By default, Entuity attempts to connect to monitored applications every two minutes.

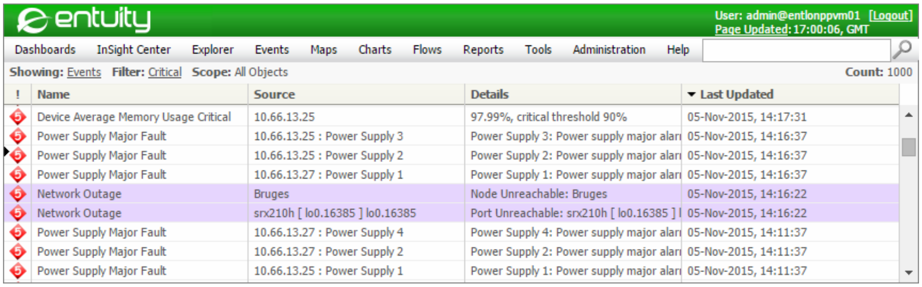
If a managed object becomes unavailable Entuity can use the discovered route to determine at what point the network failed or degraded and then raise the appropriate events and incidents. Entuity can potentially raise these events and incidents:

- After pinging of the IP address which occurs every two minutes:
  - AvailMonitor High Latency and AvailMonitor Normal Latency.
  - Network Outage. Entuity raises Network Outage events against three different network objects:
    - Devices when all of the IP addresses on the device are not responding (node down).
    - Ports when Entuity determines that the outage is on a managed port.
    - IP addresses when Entuity determines that the outage is at a point in the traceroute path not managed by the Entuity server.

    When Entuity raises a Network Outage event, *Impacted* displays a breakdown of how many devices, servers and applications are impacted by the root cause of the outage.
- After the TCP connect to an application which occurs every two minutes:
  - AvailMonitor Application Unavailable and AvailMonitor Application Available.
  - AvailMonitor High Latency Reaching Application and AvailMonitor High Latency

Reaching Application Cleared.

- On hourly rolled up data and so can only be raised hourly. They also require thresholds to be set:
  - AvailMonitor Falling Average Latency.
  - AvailMonitor Low View Device Reachability and AvailMonitor Normal View Device Reachability.
  - AvailMonitor Rising Average Latency.
  - AvailMonitor Rising Trend in Average Latency.



**Showing:** Events **Filter:** Critical **Scope:** All Objects **Count:** 1000

| ! | Name | Source | Details | Last Updated |
|---|---|---|---|---|
| 5 | Device Average Memory Usage Critical | 10.66.13.25 | 97.99%, critical threshold 90% | 05-Nov-2015, 14:17:31 |
| 5 | Power Supply Major Fault | 10.66.13.25 : Power Supply 3 | Power Supply 3: Power supply major aları | 05-Nov-2015, 14:16:37 |
| 5 | Power Supply Major Fault | 10.66.13.25 : Power Supply 2 | Power Supply 2: Power supply major aları | 05-Nov-2015, 14:16:37 |
| 5 | Power Supply Major Fault | 10.66.13.27 : Power Supply 1 | Power Supply 1: Power supply major aları | 05-Nov-2015, 14:16:37 |
| 5 | Network Outage | Bruges | Node Unreachable: Bruges | 05-Nov-2015, 14:16:22 |
| 5 | Network Outage | srx210h [ lo0.16385 ] lo0.16385 | Port Unreachable: srx210h [ lo0.16385 ] l | 05-Nov-2015, 14:16:22 |
| 5 | Power Supply Major Fault | 10.66.13.27 : Power Supply 4 | Power Supply 4: Power supply major aları | 05-Nov-2015, 14:11:37 |
| 5 | Power Supply Major Fault | 10.66.13.27 : Power Supply 2 | Power Supply 2: Power supply major aları | 05-Nov-2015, 14:11:37 |
| 5 | Power Supply Major Fault | 10.66.13.25 : Power Supply 1 | Power Supply 1: Power supply major aları | 05-Nov-2015, 14:11:37 |

Figure 30 Network Outage Events

## Application Failure

Entuity monitors application availability by establishing a TCP connection with the application. If Entuity fails to connect to the application it can raise an AvailMonitor Application Unavailable event and incident unless Entuity identifies the application's server (device) as unavailable.

For example, if the application becomes unavailable because an upstream router has failed, then Entuity raises an event relating to the router failure, and within the details of that event reports the unavailability of the application. Entuity does not raise separate events for the application being unavailable.

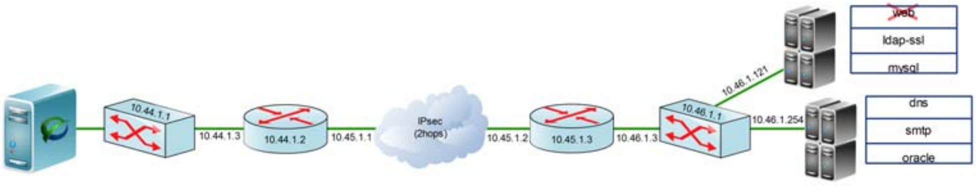


Figure 31 Root Cause Analysis detects Application Fault

# Device and Port Availability State Change

Entuity tracks the change in state of network objects, i.e. an up or down transition. When a network node was:

- Up but is now down - Entuity checks whether it is also the root cause of the failure. If it is the root cause Entuity checks whether raising a node down event is possible by associating the IP address to a device.

  To identify that a node is down all of the IP addresses on the device must be down.

  When an IP address cannot be matched, e.g. the address is on an unmanaged device, Entuity raises the event against a downstream device. The root cause IP address is identified in the details field, prefixed with UPSTREAM. These events also include the list of devices impacted by the device or port failure.
- Down and is now up - Entuity raises the appropriate node down clear event.

## Router Failure

By monitoring the availability of the network infrastructure over which application traffic flows, Entuity can both isolate the cause of IT failures and determine their impact on application services. For example, when a router fails this can impact on devices and applications monitored by Entuity. When Entuity:

- Manages the failed router Entuity raises a Network Outage event with *Details* identifying it as a **Node Down** type alarm.
- Does not manage the failed router Entuity raises a Network Outage event against edge devices, with *Details* identifying the IP address of the failed device**.**

The event also identifies impacted devices and applications. Events are not generated for symptomatic alarms caused by this outage.

Entuity identifies a device as down when all of its ports fail to respond to ping.

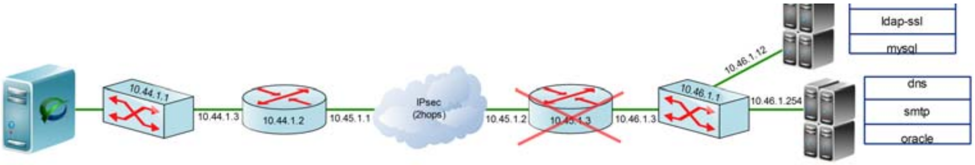


Figure 32 Root Cause Analysis detects Router Fault

## Device Failure

When identifying a device failure Entuity can also identify any monitored applications hosted by that device. In this case, rather than generating an independent alarm for each application outage, Entuity raises a Network Outage event and incident against the device and indicates the applications that are impacted.

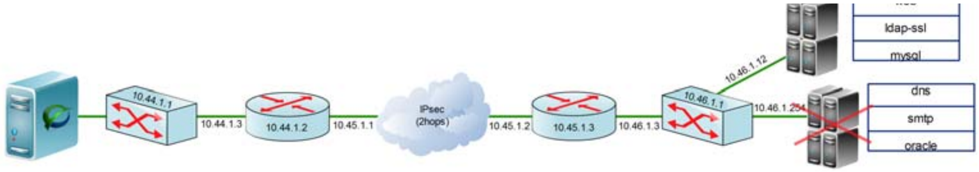


Figure 33 Root Cause Analysis detects Server Fault

## Identify Failures in the Network Cloud

IP addresses not managed by Entuity, for example on devices in the network cloud, are discovered by Entuity during traceroute and their availability state is recorded. For example where Entuity manages objects across a cloud, if:

- Some but not all IP addresses on the device go down, against the ports associated with those managed IP addresses Entuity raises a Network Outage: Port Unreachable event.

  Entuity determines the root cause of the failure by comparing the last known topology against the failed ping which it recognizes as being in the network cloud. Entuity adds this root cause IP address to the raised event details.

- All IP addresses on the device go down, Entuity raises on the device a Network Outage: Node Down event.

  Entuity determines the root cause of the failure by comparing the last known topology against the failed ping which it recognizes as being in the network cloud. Entuity adds the root cause IP address(es) to the raised event details.

- An associated port cannot be identified for any non-responding IP address on the device, Entuity raises against the managed IP address a Network Outage: Managed IP Address on Device Unreachable event.

  Entuity determines the root cause of the failure by comparing the last known topology against the failed ping, it recognizes this is in the network cloud. Entuity adds this root cause IP address to the raised event details.

### WAN Failure

Entuity can also detect a WAN link outage, for example between a central office and a remote site. As Entuity monitors each component of the networking infrastructure and understands their inter-relationship it can isolate the true cause of the service failure. If all network objects on a remote site are unavailable because of a router failure, Entuity recognizes the failure is not at the remote office and does not generate symptomatic events. Instead, Entuity raises a Network Outage event that identifies the impacted devices and applications and if it:

- Manages the failed router port raises the event against its device with *Details* identifying the outage type as **Port Unreachable**.
- Does not manage the failed port but does manage the router it raises the event against the router with *Details* identifying the outage type as **Managed IP Address Unreachable**.

- Does not manage the failed router port or the router Entuity raises the event against the devices impacted by that failure with the IP address of the failed object listed in the event *Details*.

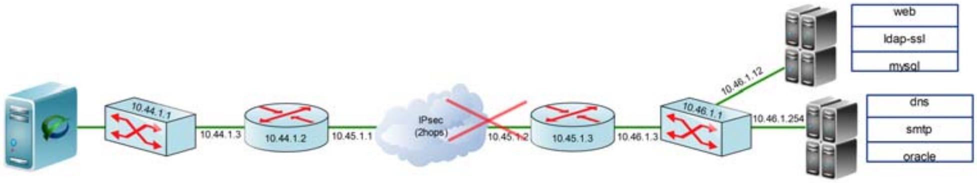


Figure 34 Root Cause Analysis detects WAN Fault

# Identifying Upstream Availability

Entuity identifies the true cause of a problem as the failing network element (IP address) closest to the Entuity server.

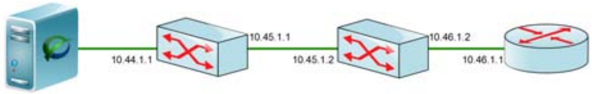


Figure 35 Simple Upstream Example Network

Entuity identifies the upstream point by first recognizing the traceroute path taken to a device, but this only includes the inbound IP addresses, for example:

| | |
|---|---|
| hop 1 | 10.44.1.1 |
| hop 2 | 10.45.1.2 |
| hop 3 | 10.46.1.1 |

To derive the outbound IP addresses Entuity identifies the IP addresses upstream of the switch, starting from 10.46.1.1. Entuity identifies its upstream node by finding the device associated with the IP address of the preceding hop (i.e. 10.45.1.2 on router-2). Entuity then searches through the list of all other IP Addresses on that device to find the one that is in the same sub-net as the downstream hop (i.e. 10.46.1.2 on router-2 is in same sub-net as 10.46.1.1 on switch-1). This IP address is then taken as the one to fill the gap between hop2 and hop3. A similar procedure is applied to fill the gap between hop1 and hop2.

# Running TraceRoute from the Entuity Server

Every ten minutes Entuity `applicationMonitor` runs traceroute to create new traceroute paths of the network and update its list of discovered IP addresses. Every two minutes it pings IP addresses on that list. You can access this traceroute path through the TraceRoute tab.

TraceRoute displays the traceroute path from the Entuity server to the selected device, useful when trouble-shooting connectivity problems. Traceroute information is collected by Entuity every two minutes, and it is this information that is presented.

| Attribute | Description |
|---|---|
| *Hops* | The number of hops from the Entuity server to an IP address. Hop 0 is the originating Entuity server. |
| *IP* | Inbound IP address pinged. |
| *Location* | Location of the pinged IP address:<br>■ Entuity Server indicates the originating Entuity server.<br>■ Unmanaged indicates the IP address is not managed by the Entuity server.<br>■ For managed ports Entuity displays the port name and its device name. |
| *State* | State of the IP address, i.e. **Reachable**, **Unreachable**. |
| *Root Cause IP* | IP address that Entuity identifies as the route cause of the availability failure. 0.0.0.0 indicates the traceroute was successful and there is no route cause to identify. |
| *ICMP Polling* | Indicates if IP address is being polled by ICMP. |

Table 8 TraceRoute from Entuity Server

TraceRoute is available to users that are members of a user group with that permission.

For each IP address listed in the traceroute path you can view its Reachability History. Reachability History is presented through a standard reporting graph, showing these metrics:

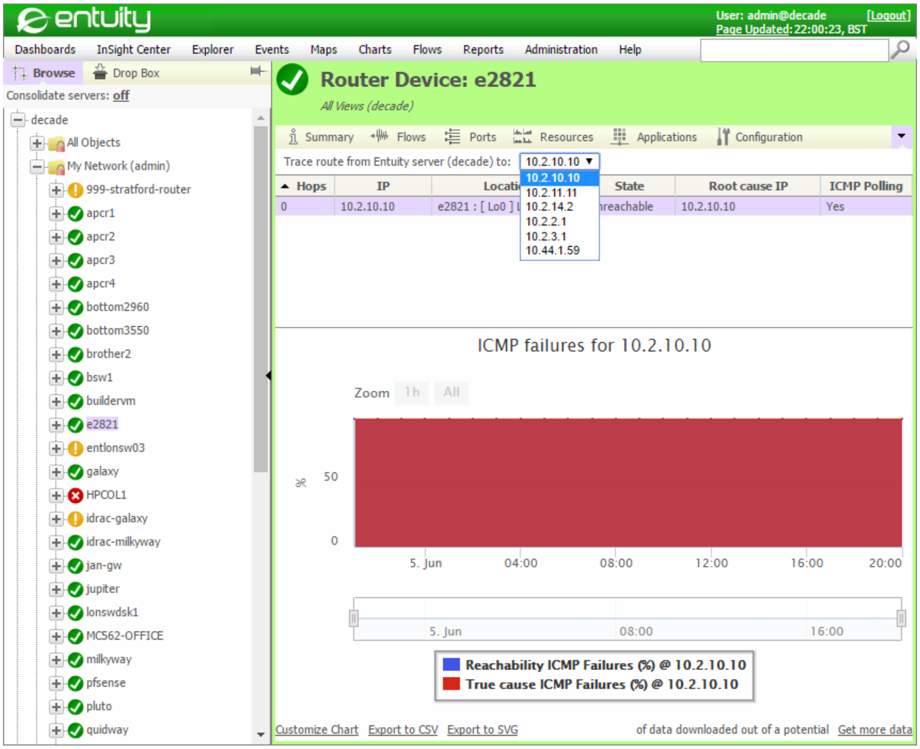
- *True Cause ICMP Failure (%)*, number of times traceroute failed to reach the IP address, when that address was the true cause of the problem, as a percentage of the number of times TraceRoute attempted to poll the IP address.
- *Reachability ICMP Failures (%)*, number of times TraceRoute failed to reach the IP address, as a percentage of the number of times TraceRoute attempted to poll the device.

To run a traceroute:

1) Select the device from the Explorer tree and click **TraceRoute** tab**.**

2) Select the IP address for which you want to view the results of the last TraceRoute query.

   Entuity populates the TraceRoute results, detailing the time each hop took and whether the trace was successfully completed.



Trace route from Entuity server (decade) to: 10.2.10.10

| Hops | IP | Locati | State | Root cause IP | ICMP Polling |
|---|---|---|---|---|---|
| 0 | 10.2.10.10 | e2821 : [ Lo0 ] L | reachable | 10.2.10.10 | Yes |

🟦 Reachability ICMP Failures (%) @ 10.2.10.10
🟥 True cause ICMP Failures (%) @ 10.2.10.10

Figure 36 TraceRoute from Server

3) You can drill-down to the Reachability History of an IP address by selecting an IP address.

# Troubleshoot Network Availability

## A Device is Down but its Downstream Devices are Up

The down device was pinged at a different time to those downstream devices that are up. The down device was up when its downstream devices were pinged but was down when it was pinged.

traceroute and ping take a finite time to run and on occasions can return counter-intuitive results.

## Intermittent and Misleading Results

traceroute and ping send ICMP packets. When a router is overloaded it may throw away these low priority ICMP packets, which will impact the recorded availability of the router and its downstream devices. Where the device is intermittently available then the impact would also be shown on increased latency values for the device.

Examine a daily availability report for that area of the network. When the suspect router and its downstream devices have a lower availability than surrounding devices you should investigate the router's performance.

## Routers and Redundant Links

When two routers are connected to form a redundant link the type of event raised when one of those routers goes down depends on the path specified in the router table. If router 3 goes down, and the path to:

- router 4 is through router 3, Entuity raises a Network Outage: Node Unreachable event against router 3.
- router 3 is through router 4, Entuity raises a Network Outage: Port Unreachable event against the inbound IP address on router 3.

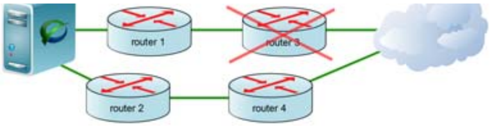


Figure 37 Routers and Redundant Links

# 21 Entuity Services

Entuity Services allow you to model network resources managed through Entuity to the business services that those resources deliver. Each Entuity service can represent a particular infrastructure service.

You can create service hierarchies with the state of sub-services contributing to the state of their parent services. This allows for modeling of complex services, potentially across all of the managed network. For example the CIO Perspective provides a high level overview of network health by reporting on the CIO service and the state of its sub-services.

The Service definition acts as an object to which you can associate the components that deliver that service. It determines, for example:

- How the states of components in the service should be interpreted to set the state of the service.
- Whether a change in the state of the service would raise an event.
- The Service Level Agreement (SLA) goal, i.e. the minimum percentage of component availability for acceptable delivery of service.

The components you can associate to a service include:

- Devices with associated components, e.g. ports.
- Devices without associated components.
- Ports.
- Servers as managed devices.
- Applications.
- IP SLA operations.
- Components of devices, e.g. fans, PSUs and temperature sensors.
- Other services which allows you to build a service hierarchy.

When populating a service with components you can add the components to the:

- View and also to the service.
- Service alone. Through the service this makes available to the user components that they do not have permission to otherwise see. If the component is removed from the service then the user loses access to that component in the view.

## Manage Entuity Services

Through the Explorer tree you can create, view, update, populate and delete services, and include them to views. You can combine the status of components of services using logical operators AND, OR, NOT and At Least when determining how to calculate the state of the service itself. As you can build service hierarchies you can use the state of a sub-service when determining the state of its parent service.

Currently a service state can be Up, Down, Degraded, Unknown and None (which is the equivalent of off). You can set whether Entuity should raise service events on service state changes. The Status Summary dashboard includes a count of services per view, and indicates when one or more have failed. It provides an overview of services, along with drill-down dashboards to view Service details.

Entuity includes service reports for you to track service performance:

- Service Delivery Summary Report, presents the Service Delivery Perspective in a layout suitable for printing.
- Service Inventory Report, presents a list of all of the services in the selected view together with their composition (e.g. operators, sub-services, components).
- Service Availability Report, presents for the selected view and time period all Services within that view and their availability over the period. This is followed by a list of time periods broken down by service status, and when the service was down indicates the cause of the outage.
- Service Event History Report, presents for the selected view all service related events for the time period.

| Feature | Description |
|---|---|
| Status Summary | A by view summary of services, with drill down to the Services in View page.<br>Available from **Dashboards**. |
| Service Summary | Available from **Dashboards**. |
| Service Delivery Perspective | Available from **InSight Center** and also **Reports > Services Reports**. |
| Service Availability Report | Available from **Reports > Services Reports**. |
| Services Event History Report | Available from **Reports > Services Reports**. |
| Network Delivery Perspective | Available from **InSight Center** and also **Reports > Availability Reports**.<br>Includes a Services Summary and access to the Server Availability report. |
| Services in View | Lists all services in the view, together with their status. You can drill down to the Service page.<br>Accessed through Status Summary. |
| Service | Details the service’s status, its definition and the components and their status. You can drill down to each component’s page.<br>Accessed through Service Summary and Service in View |
| CIO Perspective | Available from **InSight Center** and also **Reports > CIO Perspective**.<br>Includes a Services Summary and access to the Server Availability report. |

Table 9 Entuity Services Overview

Entuity also includes perspectives where services are a key component of their functionality:

- Branch Office Perspective. (See *Chapter 22 - Manage Branch Office Connectivity*.)
- CIO Perspective. (See *Chapter 7 - Chief Information Officer Perspective*.)

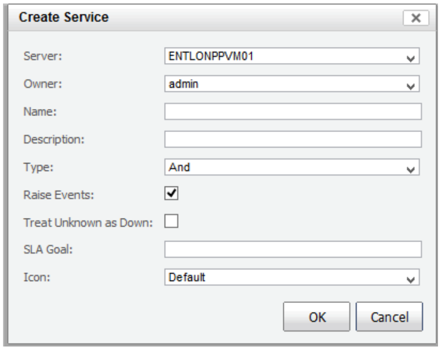
  CIO Perspective uses a special type of service which can only contain other services. These site services identify to Entuity that the service represents a logical or geographical grouping, for example an office region. (See *Site Services*.)

  CIO Perspective also uses standard services; services where you add components, for example devices, ports, IP SLA operations, which directly impact service delivery.
- Network Delivery Perspective. (See *Accessing the Network Delivery Perspective*.)

## Services Setup

When defining services consider that a service is similar to other components accessed through views; a user can only access them if they have permission to the view. (See *Services and User Permissions*.)

You can include objects from remote servers including remote sub-services. (See *Multi-Server and Remote Objects in Services*.)



Create Service

| | |
|---|---|
| Server: | ENTLONPPVM01 |
| Owner: | admin |
| Name: | |
| Description: | |
| Type: | And |
| Raise Events: | ☑ |
| Treat Unknown as Down: | □ |
| SLA Goal: | |
| Icon: | Default |

Figure 38 Service Definition

| Attribute | Description |
|---|---|
| *Parent View* | View in which the service resides. All services are also associated with the All Objects view, the service owner's My Network view and the My Network views of members of the Administrators user group. |
| *Parent Service* | Service in which a sub-service resides. |
| *Server* | Entuity server on which the service resides. In multi-server mode you select the server on which you want to create the service, Entuity does not create or consolidate the service across all of the servers.<br>A sub-service inherits the server of its parent service; you cannot set the sub-service to a different server. |

Table 10 Service Attributes

| Attribute | Description |
|---|---|
| *Owner* | The owner of the service. Only members of the Administrators user group and the owner of a service can create a sub-service within it.<br>The list of available owners is taken from the local Entuity server. Entuity prevents you from creating a service on a remote server with an owner not on that server. Entuity permits services and sub-services within the same service hierarchy to have different owners. |
| *Name* | A meaningful, short name for the service, for example used in the **Source**, **Impacted** event viewer fields. |
| *Description* | Service Description. |
| *Type* | The type of logical operator applied to the components in the service. When set to:<br>■ **None**, the service does not return a status. This is equivalent to turning off the service. None may be used when not wanting the state of a sub-service to contribute to the state of its parent service. A service set to this type uses the None status icon.<br>■ **And**, the service requires all of its components or sub-services to be up, e.g. it is suitable for a remote Customer Relationship Management (CRM) system where all of its components, e.g. edge router, access switch, database server, web server, must be up.<br>■ **Or**, the service requires any of its components to be up, e.g. where there are two internet access providers if either is up then internet connectivity is delivered.<br>■ **Not**, the service requires that the one component in the service is not operational, e.g. a backup link should be down, if it is up then there’s a problem in service delivery.<br>■ **At Least**, there are two parameters, **At Least Value** and **Degraded Threshold**. It is useful, for example, with server farms where you might have 20 servers and require at least 16 of the servers to be up for good service, 12 to15 would deliver a degraded service. |
| *At Least Value* | Only available when **Type** is set to **At Least**.<br>**At Least Value**, service requires *n* or more of its components to be fully operational. A value less than this setting is considered down unless **Degraded Threshold** is set. |
| *Degraded Threshold* | Only available when **Type** is set to **At Least**.<br>**Degraded Threshold**, a service with as few as this many components is in an Up state but less than **At Least Value** delivers a degraded state. A value less than this setting and the service is considered down. |
| *Raise Events* | When set to:<br>■ **true**, Entuity can raise an event when the state of the service changes.<br>■ **false**, Entuity does not raise an event when the state of the service changes.<br>Entuity does not raise an event when you set *Type* to **None**; the service also loses its existing state. |

Table 10   Service Attributes

| Attribute | Description |
|---|---|
| *Treat Unknown as Down* | You can set how Entuity treats components with an Unknown state when determining the state of the service, when:<br>■ Selected Unknown is treated as Down.<br>■ Not Selected (default) Unknown is treated as Unknown. |
| *SLA Goal* | The level of required service delivery, expressed as a percentage of service availability. It is used within the CIO Perspective. When set to zero it is not active. |
| *Icon* | The image appropriate for the service. Entuity includes a number of service images, and also the potential to add nine of your own custom images. The default image is of two cogs. This icon is not used in Explorer, only in the Service dashboards.<br>When you want to create your own service images they must be square, in png file format and saved to the appropriate folder (which you may have to create) using one of the nine available custom file names. (See *Service Icons*.) |

Table 10 Service Attributes

## Services and User Permissions

You can only create a top-level service if you are a member of the Administrators user group. A top-level service is one created either directly against a view or the Entuity server.

Administrators can create sub-services, services which are created within a service. Administrators can also assign service ownership to non-administrators. Service owners can edit and delete services, including top-level services. When a non-administrator is the owner of a service they can create sub-services within it.

Ownership of services within views should only be given to trusted users. Service owners can:

- Remove components from a service and if they are only included to the view through the service effectively from the view as well.
- Add components to a service and therefore to the view.

In both cases this could amend the access scope of other user groups associated with the view. Administrators must be aware of this and take care when assigning ownership of services.

## Service Definition and Components

A service comprises of two parts, the:

- Service definition, which acts as an object to which you can associate components that make up that service.
- Components, e.g. device, ports, applications, other services, that make up the delivered service.

Currently the components you can associate to a service include:

- Devices with associated components, e.g. ports.
- Devices without associated components.

- Ports.
- Servers as managed devices.
- Applications.
- IP SLA operations.
- Components of devices, e.g. fans, PSUs and temperature sensors.
- Other services which allows you to build a service hierarchy.

When populating a service with components you can add the components to the:

- View and to the service.
- Service alone. If you remove the component from the service the user loses access to that component in that view, conversely you may make available to a user through the service components that they do not have permission to otherwise see.

## Multi-Server and Remote Objects in Services

Services are defined against a selected view on a server or against the selected Entuity server (effectively the All Objects view on that server). You can only create one service at one time; for example when creating a service you can only select one server or one view.

When you access more than one Entuity server although services on those servers may share the same name Entuity does not consolidate them.These are separately defined services that only happen to have the same name, for clarity you should give services unique names. You also cannot include sub-services from different servers to a service.

Services can contain components under management by remote Entuity and SurePath servers. Entuity creates a local record of the remote object details to identify the component and its state. Users with appropriate permissions can access more details through the remote server. Users without the appropriate permissions cannot access the remote server and are therefore limited in the information they can view on the object. In this case you may want to:

- Amend the user’s permissions on the remote server to allow them to view more details.
- Amend the local service as you do not want the user to have any access to the remote object.
- Leave the service unchanged as it provides a restricted set of information on a component necessary for the user to monitor the service.

Through the Explorer tree service components are identified as local or remote, however the component’s Summary page would include the name of the managing Entuity server.

Entuity has two methods of maintaining the state of remote objects:

- Every 10 minutes the server on which the remote object is included to a service checks the remote server for the presence and state of the object.

  If the server managing the service with the remote objects loses contact with the remote Entuity server then the state of those objects becomes unknown after 10 minutes.
- The remote server maintains a record of Entuity servers using objects under its

management in their services. If one of these objects changes state the remote Entuity server notifies the server managing the service.

If remote object states are only updating every 10 minutes this indicates a firewall is preventing incoming messages initiated by the remote server, but is allowing updates that were initiated by the server managing the services.

## Identify Service State

The state of a service is determined by the state of the components within it, which may include other services, and the logical operator applied to those states. Entuity includes four logical operators, **And**, **Or**, **Not**, **At Least** and also the option of not determining a state, **None** (equivalent to turning off service state).

| Type | Component and Service States |
|---|---|
| And | Service state is the worst value of the component states, for example:<br>And (up, up, up, up, up) = up<br>And (up, up, down, up, up) = down<br>And (up, up, up, up, unknown) = unknown<br>And (up, down, up, unknown) = down |
| Or | Service state is the best value of the component states, for example:<br>Or (up, up, up, up, up) = up<br>Or (down, down, down, up, down) = up<br>Or (up, up, up, unknown, up) = up<br>Or (down, down, down, down, unknown) = unknown<br>Or (down, down, down, down, down) = down |
| Not | Service state is the inverse of the sole component state, for example:<br>Not (up) = down<br>Not (down) = up<br>Not (unknown) = unknown |
| At Least | Service state is derived through application of a weighted Or, i.e. the state of at least N (user specified) of the service components. With the At Least operator you have the option of setting a degraded threshold. However when you used by itself:, for example:<br>AtLeast(3) (up, up, up, up, down) = up<br>AtLeast(3) (up, up, up, down, down) = up<br>AtLeast(2) (up, down, down, down, down) = down<br>AtLeast(5) (up, up, up, up, down) = down (atLeast 5 = AND)<br>AtLeast(0) (down, down, down, down) = up (atLeast100% = up)<br>AtLeast(3) (up, unknown, unknown, down) = unknown |

Table 11 Service Logic Types

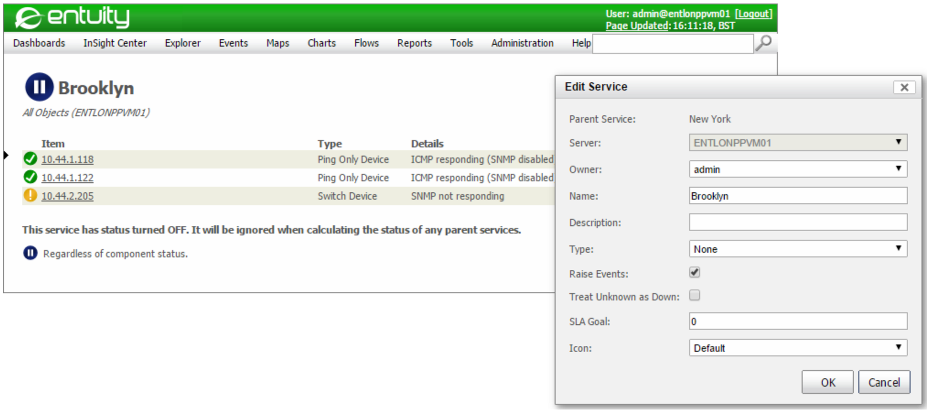
| Type | Component and Service States |
|---|---|
| Degraded Threshold | Service state is derived through application of a weighted Or, i.e. the state of at least N% (user specified) of the service components. Setting a degraded threshold is optional when you select the At Least operator. For example when there are 5 component in the service, *At Least* is set to 3 and *Degraded Threshold* set to 2:<br>(up, up, up, down, down) = up<br>(up, up, unknown, unknown, down) = degraded<br>(up, up, unknown, down, down) = degraded<br>(up, unknown, down, down, down) = unknown<br>(up, unknown, unknown, unknown, down) = unknown<br>(up, down, down, down, down) = down |

Table 11 Service Logic Types

## Services Without a State

You can set the service *Type* to **None** when you do not want the service to return a state. This is equivalent to turning the service off. You may want to use it when not wanting the state of a sub-service to contribute to the state of its parent service.

A service set to this type uses the None Status icon.



Brooklyn

*All Objects (ENTLONPPVM01)*

| Item | Type | Details |
|---|---|---|
| ✓ 10.44.1.118 | Ping Only Device | ICMP responding (SNMP disabled |
| ✓ 10.44.1.122 | Ping Only Device | ICMP responding (SNMP disabled |
| ! 10.44.2.205 | Switch Device | SNMP not responding |

This service has status turned OFF. It will be ignored when calculating the status of any parent services.

Regardless of component status.

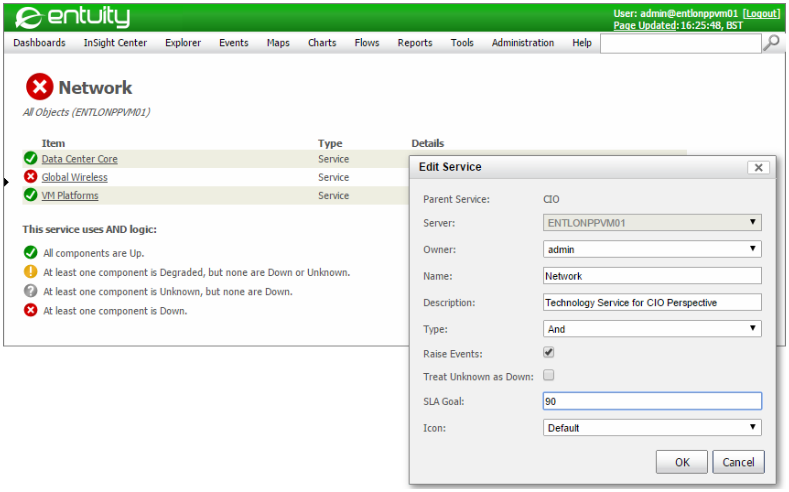
Edit Service

| | |
|---|---|
| Parent Service: | New York |
| Server: | ENTLONPPVM01 |
| Owner: | admin |
| Name: | Brooklyn |
| Description: | |
| Type: | None |
| Raise Events: | ☑ |
| Treat Unknown as Down: | □ |
| SLA Goal: | 0 |
| Icon: | Default |

Figure 39 Service State Set to None

## Services Using Logical And

When a service can only be delivered when all of its components are Up you should set service *Type* to **And**. A service state determined by applying a logical **And** requires all of its components or sub-services to be up. For example it is suitable for a remote Customer Relationship Management (CRM) system where all of its components, e.g. edge router, access switch, database server, web server, must be up for service delivery.



✗ Network

*All Objects (ENTLONPPVM01)*

| | Item | Type | Details |
|---|---|---|---|
| ✓ | Data Center Core | Service | |
| ✗ | Global Wireless | Service | |
| ✓ | VM Platforms | Service | |

This service uses AND logic:

- ✓ All components are Up.
- ! At least one component is Degraded, but none are Down or Unknown.
- ? At least one component is Unknown, but none are Down.
- ✗ At least one component is Down.

Edit Service

| | |
|---|---|
| Parent Service: | CIO |
| Server: | ENTLONPPVM01 |
| Owner: | admin |
| Name: | Network |
| Description: | Technology Service for CIO Perspective |
| Type: | And |
| Raise Events: | ☑ |
| Treat Unknown as Down: | ☐ |
| SLA Goal: | 90 |
| Icon: | Default |

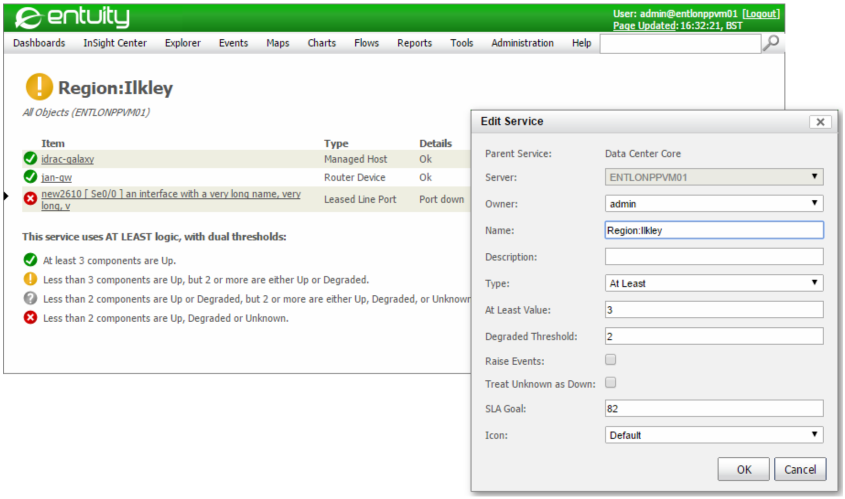
Figure 40 Down Service State Using Logical And

## Services Using Logical At Least

The At Least service type allows you to monitor services that have a built in level of resilience, where the service can still be delivered without all of the service components being available.

With the At Least type there are two parameters, At Least Value and Degraded Threshold (optional). You should use the:

- At least setting alone where the service can be delivered with a defined number of the service components, but would fail once that threshold is crossed.
- At Least and Degraded Thresholds where the service can be delivered with a defined number of the service components, a degraded service would be possible but when that threshold is crossed the service would fail. For example, where you might have a server farm with 20 servers and for delivery of a:
  - Good service you would require at least 16 of the servers to be up.
  - Degraded service between 12 to15 servers would have to be up.
  - Failed service less than 15 servers would have to be up.



Region:Ilkley

*All Objects (ENTLONPPVM01)*

| | Item | Type | Details |
|---|---|---|---|
| ✓ | idrac-galaxy | Managed Host | Ok |
| ✓ | jan-gw | Router Device | Ok |
| ☒ | new2610 [ Se0/0 ] an interface with a very long name, very long, v | Leased Line Port | Port down |

**This service uses AT LEAST logic, with dual thresholds:**

- ✓ At least 3 components are Up.
- ! Less than 3 components are Up, but 2 or more are either Up or Degraded.
- ? Less than 2 components are Up or Degraded, but 2 or more are either Up, Degraded, or Unknown
- ☒ Less than 2 components are Up, Degraded or Unknown.

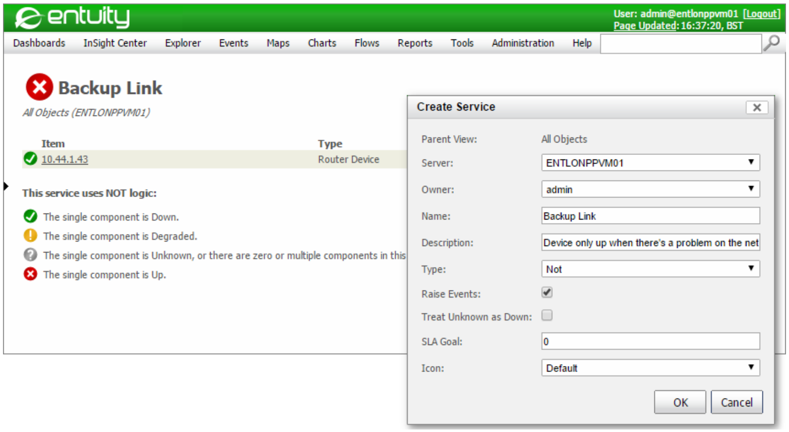
Edit Service

| | |
|---|---|
| Parent Service: | Data Center Core |
| Server: | ENTLONPPVM01 |
| Owner: | admin |
| Name: | Region:Ilkley |
| Description: | |
| Type: | At Least |
| At Least Value: | 3 |
| Degraded Threshold: | 2 |
| Raise Events: | □ |
| Treat Unknown as Down: | □ |
| SLA Goal: | 82 |
| Icon: | Default |

Figure 41 Degraded Service State Using Logical At Least

## Services Using Logical Not

There may be services which are only working as configured when the single component within it is down. You can set service *Type* to **Not**, the service is Up when its sole component is Down and is Down when its component is Up. For example you may have a backup link that should always be down, if it is up then there is a problem in service delivery that requires further investigation.



Backup Link

*All Objects (ENTLONPPVM01)*

| | Item | Type |
|---|---|---|
| ✓ | 10.44.1.43 | Router Device |

**This service uses NOT logic:**

- ✓ The single component is Down.
- ! The single component is Degraded.
- ? The single component is Unknown, or there are zero or multiple components in this
- ☒ The single component is Up.

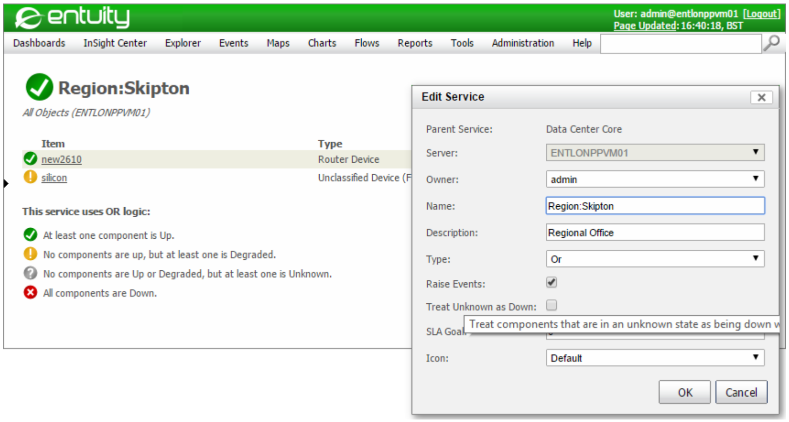
Create Service

| | |
|---|---|
| Parent View: | All Objects |
| Server: | ENTLONPPVM01 |
| Owner: | admin |
| Name: | Backup Link |
| Description: | Device only up when there's a problem on the net |
| Type: | Not |
| Raise Events: | ☑ |
| Treat Unknown as Down: | □ |
| SLA Goal: | 0 |
| Icon: | Default |

Figure 42 Down Service State Using Logical Not

## Services Using Logical Or

When a service can be delivered with one or more of its components are up you can configure it with a logical Or. For example where there are two internet access providers if either is up then internet connectivity is delivered.



Region:Skipton

All Objects (ENTLONPPVM01)

| Item | Type |
|---|---|
| new2610 | Router Device |
| silicon | Unclassified Device (F |

This service uses OR logic:

- At least one component is Up.
- No components are up, but at least one is Degraded.
- No components are Up or Degraded, but at least one is Unknown.
- All components are Down.

Edit Service

| | |
|---|---|
| Parent Service: | Data Center Core |
| Server: | ENTLONPPVM01 |
| Owner: | admin |
| Name: | Region:Skipton |
| Description: | Regional Office |
| Type: | Or |
| Raise Events: | ☑ |
| Treat Unknown as Down: | □ |
| SLA Goal: | |
| Icon: | Default |

Treat components that are in an unknown state as being down w

Figure 43 Up Service State Using Logical Or

## Service Icons

Entuity includes a number of service images, and also the potential to add nine of your own custom images. The default image is of two cogs.

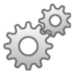
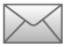
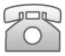
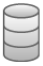
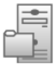
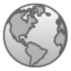
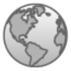
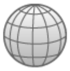
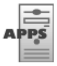
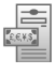
| Image | Web UI Name | Image | Web UI Name |
|---|---|---|---|
|  | Default |  | Email |
|  | VoIP |  | Database |
|  | Shared Storage |  | Web |
|  | Internet Connectivity |  | Network Connectivity |
|  | Applications |  | Ecommerce |

Table 12 Default Service Icons

When you want to create your own service images, they must be square, in PNG format and saved to the appropriate folder (which you may have to create) using one of the nine available custom file names.

| Name | Custom Filenames |
|---|---|
| Custom 1 | *entuity_home*\etc\user_images\serviceImage-1.png |
| Custom 2 | *entuity_home*\etc\user_images\serviceImage-2.png |
| Custom 3 | *entuity_home*\etc\user_images\serviceImage-3.png |
| Custom 4 | *entuity_home*\etc\user_images\serviceImage-4.png |
| Custom 5 | *entuity_home*\etc\user_images\serviceImage-5.png |
| Custom 6 | *entuity_home*\etc\user_images\serviceImage-6.png |
| Custom 7 | *entuity_home*\etc\user_images\serviceImage-7.png |
| Custom 8 | *entuity_home*\etc\user_images\serviceImage-8.png |
| Custom 9 | *entuity_home*\etc\user_images\serviceImage-9.png |

Table 13 User Defined Service Icons

# Create and Manage Services

System administrators can create services directly against a view, an Entuity server or within other services. Non-administrators may only create services within services of which they are the owner. (See *Services and User Permissions*.)

When you create a service it is only created on the specified Entuity server. Entuity does not consolidate services across multiple Entuity servers. You also cannot include services from one server to the service hierarchy on another server.However you can include components from one Entuity server to services on another Entuity server.

When populating a service with components you can add the components to the:

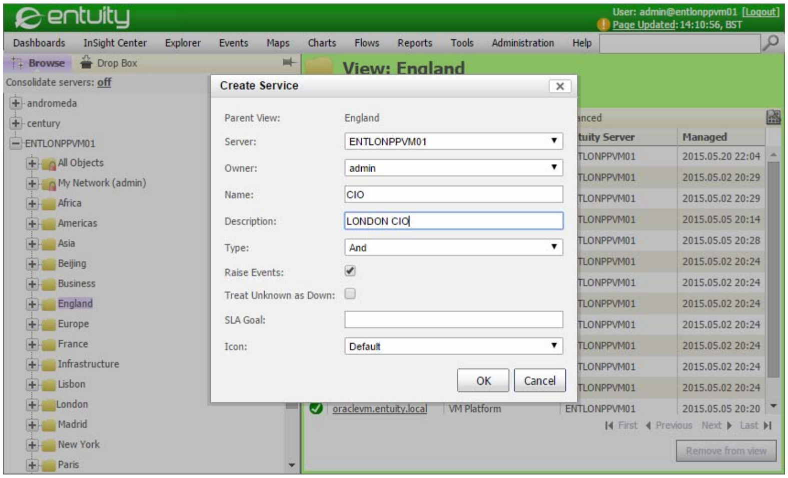
- View and to the service.
- Service alone. If you remove the component from the service the user loses access to that component in that view, conversely you may make available to a user through the service components that they do not have permission to otherwise see.

## Creating Services Against a View

When you create a service users with access to that view also have access to all objects within that view including services.

To create a service:

1) From the Explorer tree highlight the view in which you want to create the service and from the context menu click **Create Service**.



Create Service

Parent View: England

Server: ENTLONPPVM01

Owner: admin

Name: CIO

Description: LONDON CIO

Type: And

Raise Events: ☑

Treat Unknown as Down: □

SLA Goal:

Icon: Default

OK Cancel

Figure 44 Creating Services Against Views

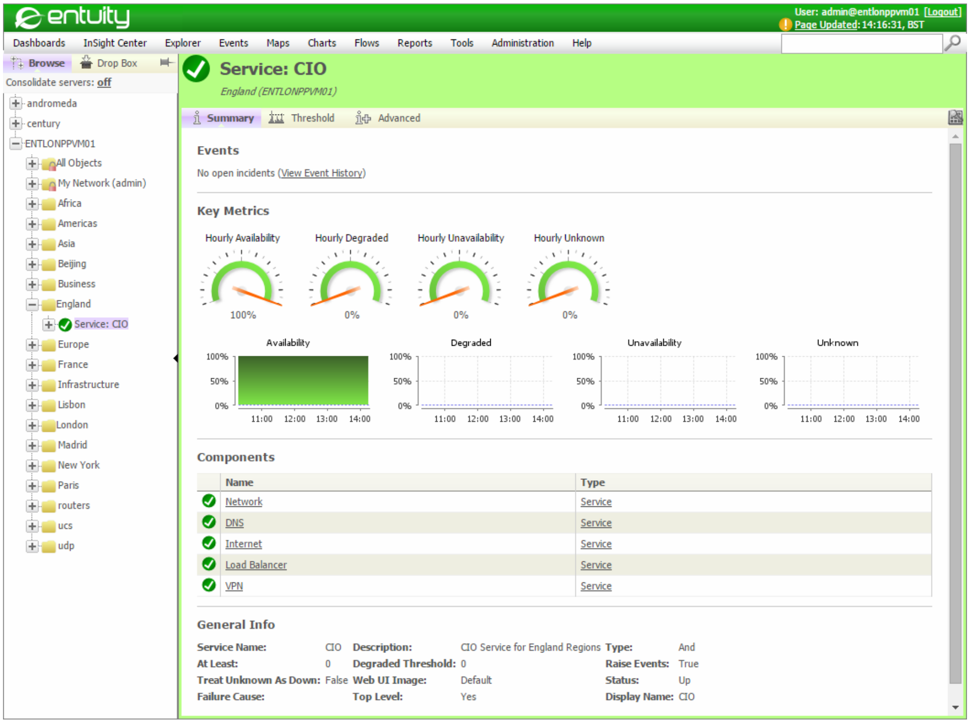
2) Complete the service definition and click **OK**. (See *Manage Entuity Services*.)

   Entuity generates a new service identified by the naming convention of **Service:** *serviceName*. The new service is available within the:

   - Selected view.
   - All Objects view.
   - The service owner’s My Network view.
   - The My Network views of members of the Administrators user group.

You can now populate the service with:

- Managed components by dragging and dropping them to the service, e.g. web server, applications, routers.
- Sub-services either by dragging and dropping services into the new service or by creating new sub-services.



**Service: CIO**

*England (ENTLONPPVM01)*

**Events**

No open incidents (View Event History)

**Key Metrics**

**Components**

| | Name | Type |
|---|---|---|
| ✓ | Network | Service |
| ✓ | DNS | Service |
| ✓ | Internet | Service |
| ✓ | Load Balancer | Service |
| ✓ | VPN | Service |

**General Info**

| | | | | | |
|---|---|---|---|---|---|
| **Service Name:** | CIO | **Description:** | CIO Service for England Regions | **Type:** | And |
| **At Least:** | 0 | **Degraded Threshold:** | 0 | **Raise Events:** | True |
| **Treat Unknown As Down:** | False | **Web UI Image:** | Default | **Status:** | Up |
| **Failure Cause:** | | **Top Level:** | Yes | **Display Name:** | CIO |

Figure 45 Services Summary

## Creating Service Hierarchies

You can use service hierarchies to model complex service delivery implementations, with the state of sub-services contributing to the state of the parent service reflecting how the performance of components contribute to service delivery.

When creating a hierarchy of services you can either select a service and create a new service within it, or drag an existing service from the view summary page into the target service in the Explorer tree. Your My Network view contains all of the services available to you; when you create a new service in a view Entuity also adds it to your My Network view and the All Objects view. When dragging and dropping services to create a hierarchy My Network is the best source.

Entuity prevents you from:

- Creating hierarchies that include a service within itself.
- Adding services defined on one Entuity server to services defined on another Entuity server.

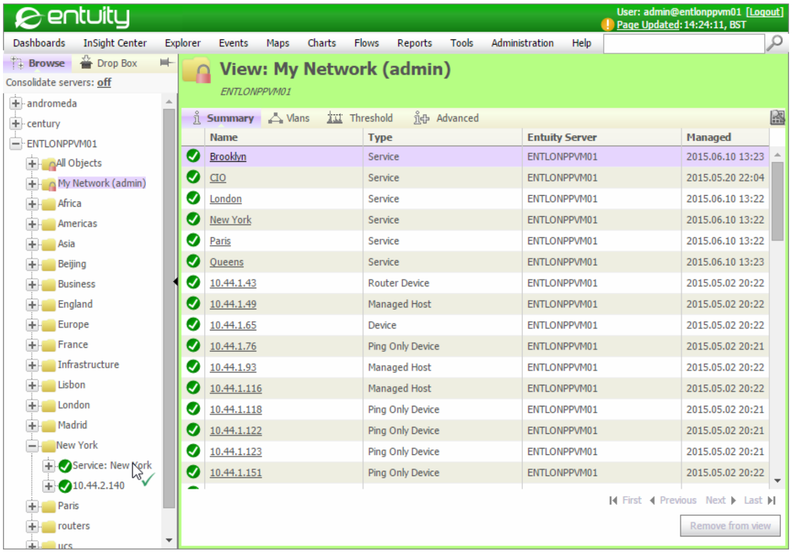
To create a service hierarchy:

1) From the Explorer tree highlight the view in which you want to create the service and from the context menu click **Create Service**.

2) In the Explorer tree click on My Network to display the View: My Network Summary page.

3) In the Explorer tree expand the view in which you created the service.

4) From the View: My Network Summary page select a service and drag it to the new service in the tree. Entuity changes the icon from red cross to green tick when the dragged service is in a location when it can be released.



View: My Network (admin)

ENTLONPPVM01

| | Name | Type | Entuity Server | Managed |
|---|---|---|---|---|
| ✓ | Brooklyn | Service | ENTLONPPVM01 | 2015.06.10 13:23 |
| ✓ | CIO | Service | ENTLONPPVM01 | 2015.05.20 22:04 |
| ✓ | London | Service | ENTLONPPVM01 | 2015.06.10 13:22 |
| ✓ | New York | Service | ENTLONPPVM01 | 2015.06.10 13:22 |
| ✓ | Paris | Service | ENTLONPPVM01 | 2015.06.10 13:22 |
| ✓ | Queens | Service | ENTLONPPVM01 | 2015.06.10 13:23 |
| ✓ | 10.44.1.43 | Router Device | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.49 | Managed Host | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.65 | Device | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.76 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:21 |
| ✓ | 10.44.1.93 | Managed Host | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.116 | Managed Host | ENTLONPPVM01 | 2015.05.02 20:22 |
| ✓ | 10.44.1.118 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:21 |
| ✓ | 10.44.1.122 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:21 |
| ✓ | 10.44.1.123 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:21 |
| ✓ | 10.44.1.151 | Ping Only Device | ENTLONPPVM01 | 2015.05.02 20:22 |

Figure 46 Dragging Services into Services

## Creating Services for Network Paths

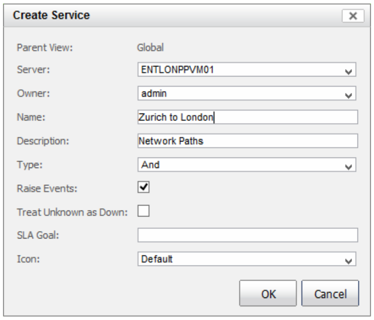
When you have a remote SurePath server you can include network paths to services. The state of a path contributes to the state of a service.

A network service may have more than one network path supporting it. In SurePath you can discover each path and save it as a reference path. You can then include each of these network paths to an Entuity service and for example set the condition on the service so that only when all of the paths are down is the service judged as down.

To create a service to hold network paths:

1) From the Explorer tree highlight the view in which you want to create the service and from the context menu click **Create New Service**.

   The view must contain all of the devices in the network paths.



**Create Service**

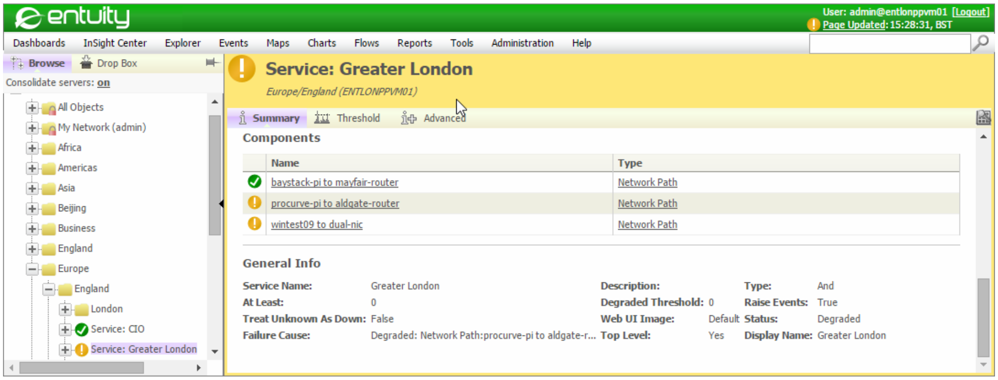
| | |
|---|---|
| Parent View: | Global |
| Server: | ENTLONPPVM01 |
| Owner: | admin |
| Name: | Zurich to London |
| Description: | Network Paths |
| Type: | And |
| Raise Events: | ☑ |
| Treat Unknown as Down: | □ |
| SLA Goal: | |
| Icon: | Default |

Figure 47 Create Network Path Service

2) In the Explorer tree navigate to and select the view holding the network paths, for example the My Network view on the SurePath server, to display the View: My Network Summary page.

3) In the Explorer tree expand the view in which you created the service.

4) From the View: My Network Summary page select a network path and drag it to the new service in the tree. Entuity changes the icon from red cross to green tick when the dragged service is in a location when it can be released.



**Service: Greater London**

*Europe/England (ENTLONPPVM01)*

**Components**

| | Name | Type |
|---|---|---|
| ✓ | baystack-pi to mayfair-router | Network Path |
| ! | procurve-pi to aldgate-router | Network Path |
| ! | wintest09 to dual-nic | Network Path |

**General Info**

| | | | | | |
|---|---|---|---|---|---|
| **Service Name:** | Greater London | **Description:** | | **Type:** | And |
| **At Least:** | 0 | **Degraded Threshold:** | 0 | **Raise Events:** | True |
| **Treat Unknown As Down:** | False | **Web UI Image:** | Default | **Status:** | Degraded |
| **Failure Cause:** | Degraded: Network Path:procurve-pi to aldgate-r... | **Top Level:** | Yes | **Display Name:** | Greater London |

Figure 48 Network Path Service

## Remove and Delete Services

Entuity distinguishes between removing a service from a view and deleting a service:

- Remove from view removes the service from the current view. This option is not available from My Network or All Objects views because all defined services must be available through those views.

- Delete Service deletes the service from the server; all instances of the service including in My Network and All Objects views are removed. If the service has a sub-service the sub-service is not deleted from the server but remains available through My Network.

  Before you delete a service consider that you cannot undo the action.

To delete a service from Entuity:

1) From the Explorer tree locate and select the service.

2) From the context menu click **Delete Service**. Entuity prompts you to confirm the deletion.

To remove a service from a view:

1) From the Explorer tree locate and select the service.

2) From the context menu click **Remove from view**. Entuity removes the service from the view.

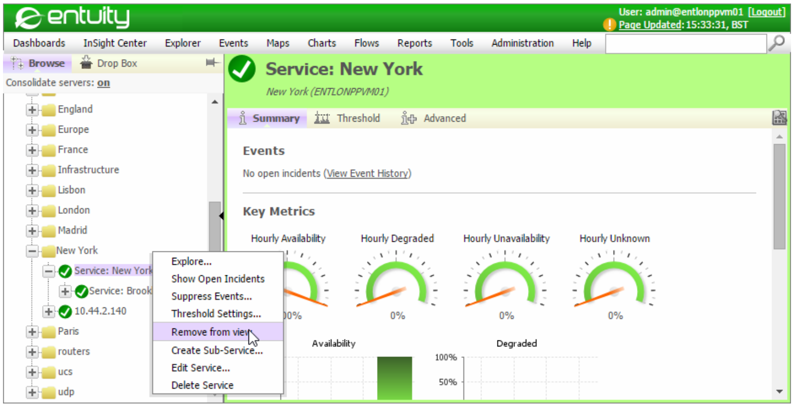
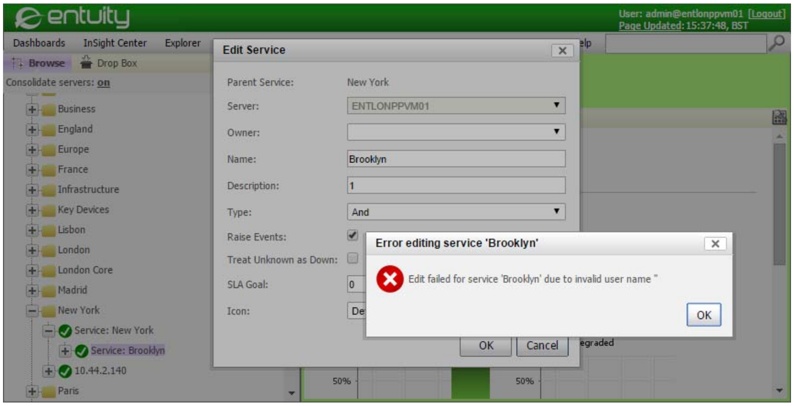


Figure 49 Deleting and Removing Services

## Services with Invalid Ownership

If a user profile with ownership of one or more services is removed from Entuity then ownership of the service is marked as **<invalid user>**. The service Advanced page still displays *Owner* as the now deleted profile, Entuity does not reassign ownership (this is the same behavior as with views and deleted owner user profiles). The next time you edit the service you can only save your updates if you also update service ownership.



Edit Service

Parent Service: New York

Server: ENTLONPPVM01

Owner:

Name: Brooklyn

Description: 1

Type: And

Raise Events: ☑

Treat Unknown as Down: □

SLA Goal: 0

Icon: De

OK Cancel

Error editing service 'Brooklyn'

Edit failed for service 'Brooklyn' due to invalid user name ''

OK

Figure 50 Services with Invalid Ownership

# Monitor Service Status

You can manage the state of your services by tracking service events and incidents through Event Viewer by investigating services through dashboards and running reports.

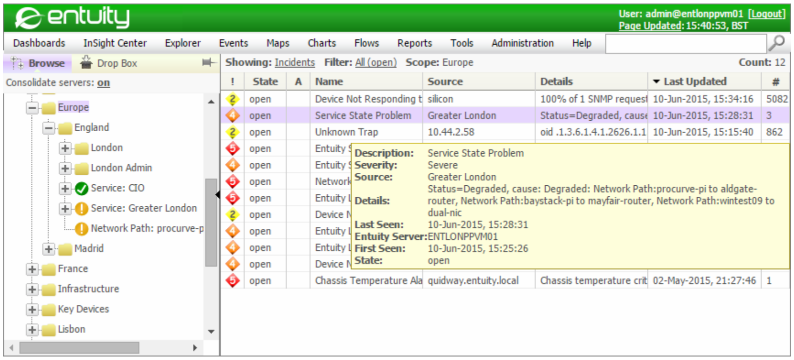
## Service Status Events

For each service you can set whether to permit Entuity to raise events against it. You should consider the purpose of the service, especially within a hierarchy of services.

Entuity includes these service specific events:

- Service Down, indicates the named service is down and that the number of components failing in the service is sufficient to cause the service to fail.
- Service State Unknown, indicates the state of the named service is unknown. The state of one or more of the components in the service is unknown.
- Service State Degraded, indicates the state of the named service is degraded. The state of components within the service meets the condition specified as degraded.
- Service State Off, indicates the service is now configured to not return a state. Its *Type*, which could be set to the logical operator to be applied to the state of its components is instead set to **None**.
- Service Up, indicates the named service is up, its state having previously been Down or Unknown.

The Service Down, Service State Degraded and Service State Unknown events can all raise the Service State Problem incident.



Showing: Incidents Filter: All (open) Scope: Europe Count: 12

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| 2 | open | | Device Not Responding t | silicon | 100% of 1 SNMP request | 10-Jun-2015, 15:34:16 | 5082 |
| 4 | open | | Service State Problem | Greater London | Status=Degraded, cause | 10-Jun-2015, 15:28:31 | 3 |
| 2 | open | | Unknown Trap | 10.44.2.58 | oid .1.3.6.1.4.1.2626.1.1 | 10-Jun-2015, 15:15:40 | 862 |
| 5 | open | | Entuity S | | | | |
| 4 | open | | Entuity S | | | | |
| 5 | open | | Network | | | | |
| 5 | open | | Entuity L | | | | |
| 2 | open | | Device N | | | | |
| 4 | open | | Entuity L | | | | |
| 4 | open | | Entuity L | | | | |
| 4 | open | | Device N | | | | |
| 5 | open | | Chassis Temperature Ala | quidway.entuity.local | Chassis temperature crit | 02-May-2015, 21:27:46 | 1 |

**Description:** Service State Problem
**Severity:** Severe
**Source:** Greater London
**Details:** Status=Degraded, cause: Degraded: Network Path:procurve-pi to aldgate-router, Network Path:baystack-pi to mayfair-router, Network Path:wintest09 to dual-nic
**Last Seen:** 10-Jun-2015, 15:28:31
**Entuity Server:** ENTLONPPVM01
**First Seen:** 10-Jun-2015, 15:25:26
**State:** open

Figure 51 Service Incidents

From Event Viewer you can place your mouse pointer over the event to display a pop up dialog that provides event details, with *Details* indicating the causal component(s) of the service event.

## Service Summary Dashboard

Service Summary dashboard provides an overview of the state of services where the:

- Service name is also a hyperlink to a breakdown of the service.
- Service icon can indicate the type of service.
- Server on which the service resides is identified.
- View or views to which the service is applied are identified.
- Service state icon indicates the current state of the service.

Depending on your user preference setting, services are grouped by:

- View, with Entuity listing the services in each view.
- Alphabetically, with Entuity listing the services in alphabetic order and also including a listing of views through which the service is available.

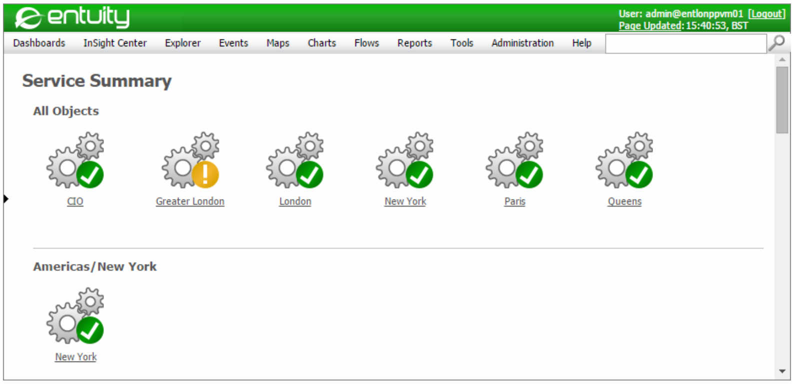


Figure 52 Service Summary Dashboard

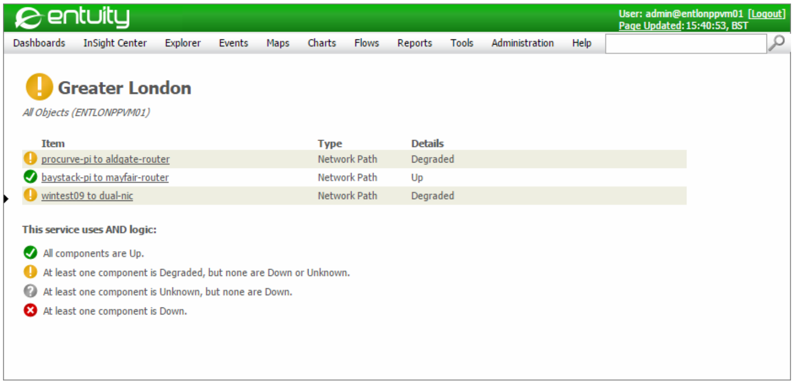
You can also investigate service performance:

1) Click **Dashboards > Service Summary**.

2) For services that are down you can place the mouse pointer over the service to view a popup that details the failing component(s).

3) Click on a service to drill down. Entuity displays details on the service, including its components, their current state and the logic used to derive the state of the service.

   You can further drill-down to investigate the cause of component failures.



Greater London

*All Objects (ENTLONPPVM01)*

| Item | Type | Details |
|---|---|---|
| ! procurve-pi to aldgate-router | Network Path | Degraded |
| ✓ baystack-pi to mayfair-router | Network Path | Up |
| ! wintest09 to dual-nic | Network Path | Degraded |

This service uses AND logic:

- ✓ All components are Up.
- ! At least one component is Degraded, but none are Down or Unknown.
- ? At least one component is Unknown, but none are Down.
- ✗ At least one component is Down.

Figure 53 Service Component Drill-Down

## Service Performance

You can track service performance through the Service Summary and Advanced pages, the Thresholds page is not used as service events are not threshold based.

## Service Summary

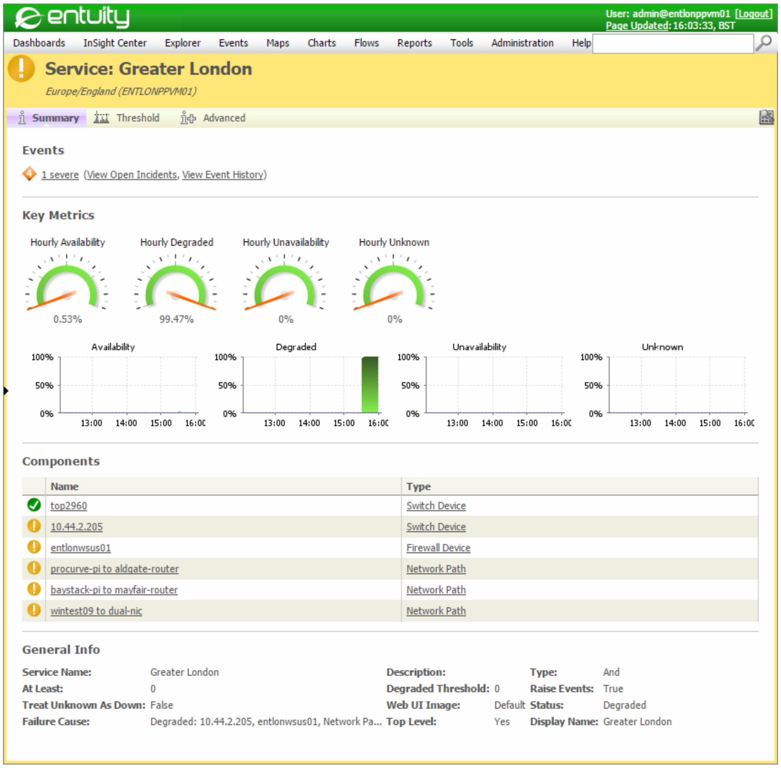
As with other component summary pages the Service Summary page identifies the state of the service and whether there are open incidents. The General Info section also provides a summary of the service definition. (See *Manage Entuity Services*.)

Service Key Metrics are graphed on 4 metrics:

- *Availability*, the amount of time the service was available during the reporting period as a percentage of the reporting period.
- *Unavailability*, the amount of time the service was unavailable during the reporting period as a percentage of the reporting period.
- *Unknown*, the amount of time the state of the service was unknown during the reporting period as a percentage of the reporting period.
- *Degraded*, the amount of time the state of the service was degraded during the reporting period as a percentage of the reporting period.

The gauge charts illustrate service performance over the past hour, the key metric charts over the previous 4 hours and the interactive charts, accessed when you click on a gauge or chart, over the previous 24 hours.

The Components section shows any sub-services of the service, including the service state and hyperlink to that service's Summary page.



Service: Greater London

*Europe/England (ENTLONPPVM01)*

Events

1 severe (View Open Incidents, View Event History)

Key Metrics

Components

| | Name | Type |
|---|---|---|
| ✓ | top2960 | Switch Device |
| ! | 10.44.2.205 | Switch Device |
| ! | entlonwsus01 | Firewall Device |
| ! | procurve-pi to aldgate-router | Network Path |
| ! | baystack-pi to mayfair-router | Network Path |
| ! | wintest09 to dual-nic | Network Path |

General Info

| | | | | | |
|---|---|---|---|---|---|
| **Service Name:** | Greater London | **Description:** | | **Type:** | And |
| **At Least:** | 0 | **Degraded Threshold:** | 0 | **Raise Events:** | True |
| **Treat Unknown As Down:** | False | **Web UI Image:** | Default | **Status:** | Degraded |
| **Failure Cause:** | Degraded: 10.44.2.205, entlonwsus01, Network Pa... | **Top Level:** | Yes | **Display Name:** | Greater London |

Figure 54 Services Summary

## Service Advanced Details

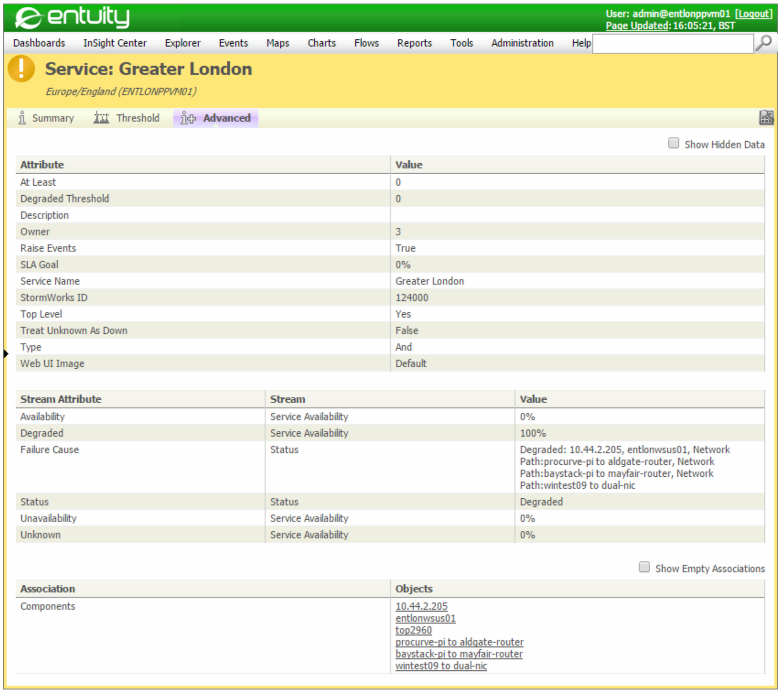
As with other component advanced pages the Service Advanced page identifies the state of the service. The Attribute section also provides a summary of the service definition (see *Manage Entuity Services*):

- Top Level indicates whether the service is directly assigned against a view, Yes, or only assigned to a service, No. Even when set to Yes a service may still be assigned to another service.
- Owner is the internal identifier of the owner of the service. The name of the owner is available through the Edit service dialog.
- StormWorks ID is the internal identifier of the service.

The stream attributes show the current state of services as measured by:

- *Availability*, the amount of time the service was available during the previous hour as a percentage of the full hour.
- *Degraded*, the amount of time the service was degraded during the previous hour as a percentage of the full hour.

- *Failure Cause*, if the service is down it details the cause of the failure.
- *Status*, current status of the service:
  - **Up**, the service is up.
  - **Degraded**, the service is available but not running in an optimal state. *Type* is set to **At Least** and the *At Least* threshold has been crossed but not the *Degraded Threshold*.
  - **Down**, the service is unavailable.
  - **None**, the service does not return a state as *Type* is set to **None**.
  - **Unknown**, Entuity does not know the status of the service due to an inability to get a status for a component.
- *Unavailability*, the amount of time the service was unavailable during the previous hour as a percentage of the full hour.
- *Unknown*, the amount of time the state of the service was unknown during the previous hour as a percentage of the full hour.



Service: Greater London

*Europe/England (ENTLONPPVM01)*

□ Show Hidden Data

| Attribute | Value |
|---|---|
| At Least | 0 |
| Degraded Threshold | 0 |
| Description | |
| Owner | 3 |
| Raise Events | True |
| SLA Goal | 0% |
| Service Name | Greater London |
| StormWorks ID | 124000 |
| Top Level | Yes |
| Treat Unknown As Down | False |
| Type | And |
| Web UI Image | Default |

| Stream Attribute | Stream | Value |
|---|---|---|
| Availability | Service Availability | 0% |
| Degraded | Service Availability | 100% |
| Failure Cause | Status | Degraded: 10.44.2.205, entlonwsus01, Network Path:procurve-pi to aldgate-router, Network Path:baystack-pi to mayfair-router, Network Path:wintest09 to dual-nic |
| Status | Status | Degraded |
| Unavailability | Service Availability | 0% |
| Unknown | Service Availability | 0% |

□ Show Empty Associations

| Association | Objects |
|---|---|
| Components | 10.44.2.205<br>entlonwsus01<br>top2960<br>procurve-pi to aldgate-router<br>baystack-pi to mayfair-router<br>wintest09 to dual-nic |

Figure 55 Services Advanced

## View Service Delivery

The Service Delivery Perspective aggregates the behavior of all the services in a chosen view and displays, by default, a summary of the previous 31days.

You can also access the more detailed service reports; Service Inventory Report, Service Availability Report, Service Event History Report. For example, allowing information about availability of key services such as email, data center connectivity, VoIP services and resilient links to satellite offices and the Internet allows IT and business managers to quickly assess the quality of services that the IT is providing to its business users.

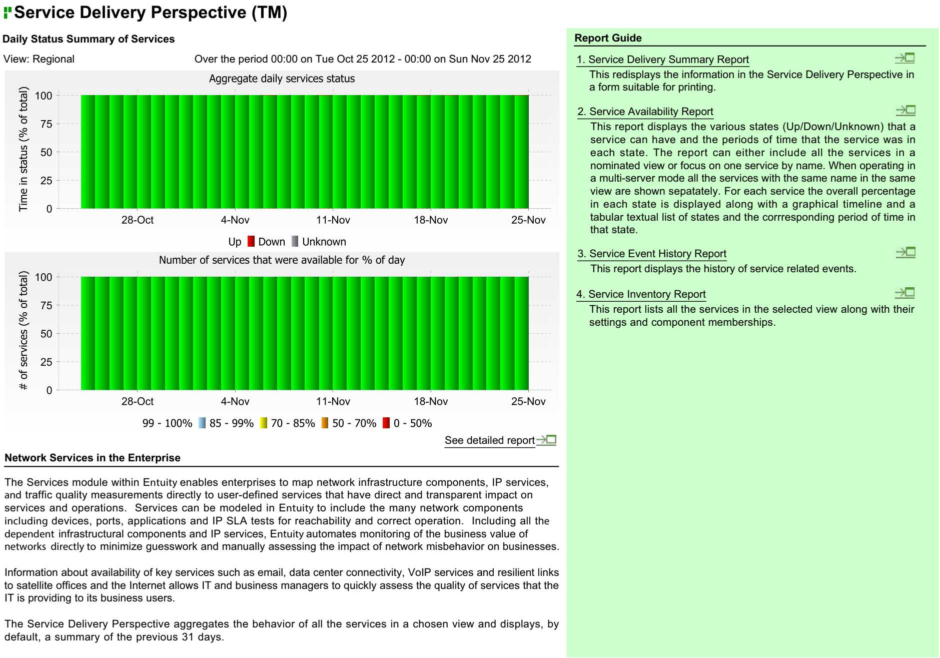
You can also view service performance within the wider context of the managed infrastructure performance through the InSight Center’s Network Delivery Perspective.

## Accessing Service Delivery Perspective

To access the Service Delivery Perspective:

1) Click **InSight Center > Service Delivery Perspective**.

2) Through Service Delivery Report Options you can select the Entuity server, view and time period against which you want to apply the perspective.



**Service Delivery Perspective (TM)**

**Daily Status Summary of Services**

View: Regional Over the period 00:00 on Tue Oct 25 2012 - 00:00 on Sun Nov 25 2012

**Network Services in the Enterprise**

The Services module within Entuity enables enterprises to map network infrastructure components, IP services, and traffic quality measurements directly to user-defined services that have direct and transparent impact on services and operations. Services can be modeled in Entuity to include the many network components including devices, ports, applications and IP SLA tests for reachability and correct operation. Including all the dependent infrastructural components and IP services, Entuity automates monitoring of the business value of networks directly to minimize guesswork and manually assessing the impact of network misbehavior on businesses.

Information about availability of key services such as email, data center connectivity, VoIP services and resilient links to satellite offices and the Internet allows IT and business managers to quickly assess the quality of services that the IT is providing to its business users.

The Service Delivery Perspective aggregates the behavior of all the services in a chosen view and displays, by default, a summary of the previous 31 days.

**Report Guide**

1. Service Delivery Summary Report
This redisplays the information in the Service Delivery Perspective in a form suitable for printing.

2. Service Availability Report
This report displays the various states (Up/Down/Unknown) that a service can have and the periods of time that the service was in each state. The report can either include all the services in a nominated view or focus on one service by name. When operating in a multi-server mode all the services with the same name in the same view are shown sepatately. For each service the overall percentage in each state is displayed along with a graphical timeline and a tabular textual list of states and the corrresponding period of time in that state.

3. Service Event History Report
This report displays the history of service related events.

4. Service Inventory Report
This report lists all the services in the selected view along with their settings and component memberships.

Figure 56 Service Delivery Perspective

# 22 Manage Branch Office Connectivity

The Branch Office Perspective is part of Entuity's InSight Center, delivering a business-centric dashboard designed to automate, simplify, and reduce the operational costs for companies having distributed network locations or branch offices. Highly interactive with actionable graphics and a variety of drill-down reports, the Branch Office Perspective helps IT managers quickly assess branch office connectivity through a variety of measures; availability, utilization, faults, discards, latency, device reachability, and SLA quality.

Entuity's distinctive service model allows for representation of even the most complex WAN circuits. Any number of WAN circuits can be logically combined to meaningfully depict and monitor redundancy and backup. Intuitive dashboards highlight performance not only over the customizable monitoring period, but also show the status of the latest sample which allows for easy differentiation between current and longer term issues.

Entuity monitors and reports on service quality metrics meaningful to your business through a customizable range of flexible synthetic transactions. The color-coded horizontal ribbon charts are also interactive, helping you understand fluctuations over time. Entuity's Branch Office Perspective helps you avoid lapses or reductions in branch office productivity due to a lack of network capacity.

The Branch Office Perspective suite includes:

- Multiple Branch Office Perspective**,** provides an overview of the health of the network equipment in all of the branch offices that are accessible to the user. For each branch office they can also drilldown to the Branch Office Perspective, which inherits its timeframe from the multiple branch office perspective.
- Branch Office Perspective, provides an overview of the health of the network equipment at the selected branch office. Where multiple IP SLA operations are configured for a branch office their results are listed separately. Drilldowns are provided to the Branch Office Details and Spare Ports reports. The green Report Guide panel provides several other report launch facilities in the context of the selected branch office view.
- Branch Office Details report, displays detailed time series charts for the WAN ports, monitored device Reachability and IP SLA operations. Various further drilldowns are available from many, but not all, of the charts and color ribbon timelines. A click on a WAN port chart line will launch the corresponding Interactive chart in the Explorer in a new browser tab. A click on an IP SLA color ribbon, HTTP chart but not the Echo chart will drill down into the IP SLA Details report and will display that specific IP SLA operation only with the time sample that was clicked in the center of the time axis but with a 10x time zoom.
- IP SLA Details report, is available from the Activity folder and also as a drilldown from the Branch Office Details report. This report displays detailed statistical results charts for IP SLA operations. Allows any/all IP SLA operations in the chosen view to be displayed.

For report and perspective details see the *Entuity Reports Reference Manual*.

# Setting up Branch Offices

Branch Office configuration requires system administrator permissions. Although a user can be granted tool permissions to create the branch office view, a system administrator is required to create the root Branch Office service.

A Branch Office comprises of two parts, the:

- Service definition, which acts as an object to which you can associate components that make up that service. (See *Services Setup*.)
- Components, e.g. device, ports, applications, other services, that make up the delivered service.

You must create for the required view the necessary folder structure for the branch office suite a:

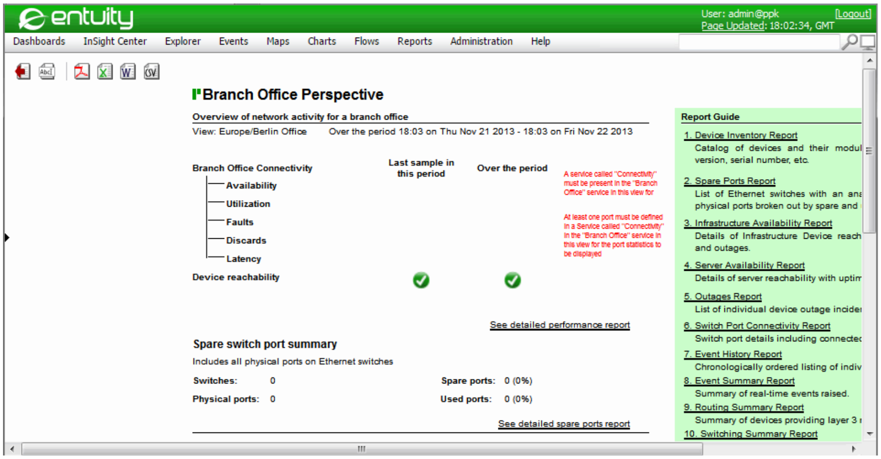
- Service called Branch Office.
- Sub-service of Branch Office called Connectivity.

  In this service you should include all the WAN ports that provide connectivity to the rest of the world. Redundant, failover or load balanced WAN circuits can be modeled using standard services techniques (logical operators and sub-services when necessary).
- Sub-service of the Branch Office called SLAs.

  When there are IP SLA operations being performed on behalf of the branch office that are to be included within the Branch Office Perspective they must exist within the SLAs service. This allows devices with IP SLA tests to be located in the view without having to expose any/all associated IP SLA operations within this package of reports.

If you fail to correctly configure the Branch Office service and sub-services or include the appropriate components to a service when run the perspective reports these errors. (See *Figure 57 Perspective Reports Misconfigured Service*.)

Entuity permits you to place in a service only those components on which you want to report, for example you can drag to the Connectivity sub-service only the ports in which you are interested. However unless you also have the port’s device within the view the Branch Office Details report cannot report on latency to that device. (See *Figure 67 Branch Office Connectivity*.)



Branch Office Perspective

Overview of network activity for a branch office

View: Europe/Berlin Office Over the period 18:03 on Thu Nov 21 2013 - 18:03 on Fri Nov 22 2013

| Branch Office Connectivity | Last sample in this period | Over the period |
|---|---|---|
| Availability | | |
| Utilization | | |
| Faults | | |
| Discards | | |
| Latency | | |
| Device reachability | ✓ | ✓ |

A service called "Connectivity" must be present in the "Branch Office" service in this view for

At least one port must be defined in a Service called "Connectivity" in the "Branch Office" service in this view for the port statistics to be displayed

See detailed performance report

Spare switch port summary

Includes all physical ports on Ethernet switches

Switches: 0 Spare ports: 0 (0%)

Physical ports: 0 Used ports: 0 (0%)

See detailed spare ports report

Report Guide

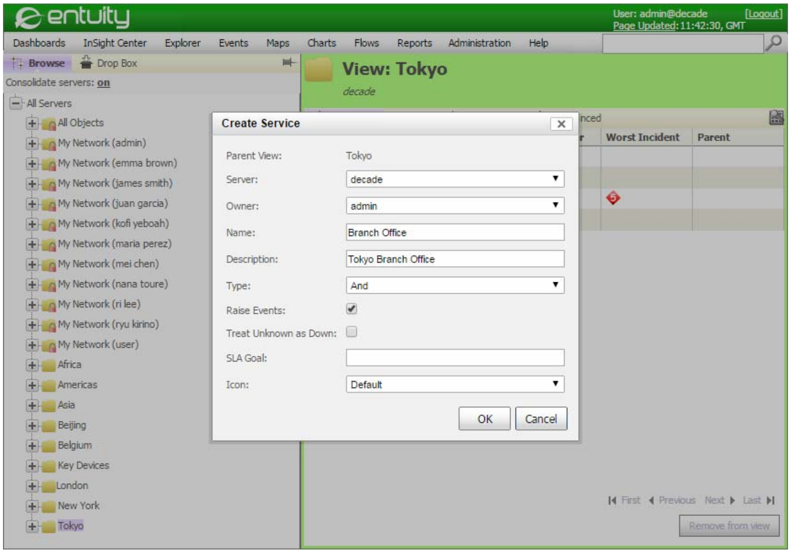
1. Device Inventory Report
   Catalog of devices and their modul version, serial number, etc.
2. Spare Ports Report
   List of Ethernet switches with an ana physical ports broken out by spare and
3. Infrastructure Availability Report
   Details of Infrastructure Device reach and outages.
4. Server Availability Report
   Details of server reachability with uptim
5. Outages Report
   List of individual device outage incide
6. Switch Port Connectivity Report
   Switch port details including connecte
7. Event History Report
   Chronologically ordered listing of indiv
8. Event Summary Report
   Summary of real-time events raised.
9. Routing Summary Report
   Summary of devices providing layer 3
10. Switching Summary Report

Figure 57 Perspective Reports Misconfigured Service

To create a Branch Office:

1) Create and name a view. The name should identify the office, e.g. Berlin Office.

2) From the view’s context menu click **Create Service**. The service must be called Branch Office. Entuity restricts the running of the Branch Office Perspective to services called Branch Office.



Create Service

| | |
|---|---|
| Parent View: | Tokyo |
| Server: | decade |
| Owner: | admin |
| Name: | Branch Office |
| Description: | Tokyo Branch Office |
| Type: | And |
| Raise Events: | ☑ |
| Treat Unknown as Down: | □ |
| SLA Goal: | |
| Icon: | Default |

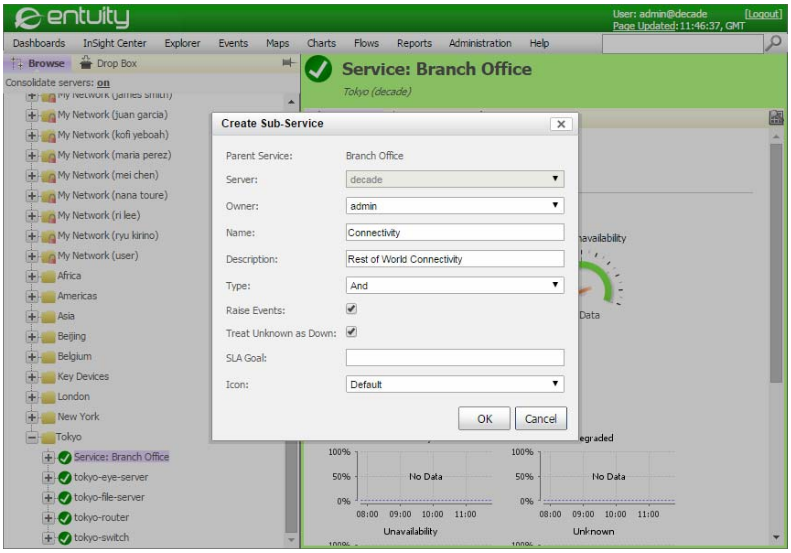
OK Cancel

Figure 58 Create a Branch Office Service

3) From the Branch Office service click **Create Sub-Service** and define the **Connectivity** service. The service must be called Connectivity for the Branch Office Perspective to

report on the service.

4) Drag and drop to the Connectivity the required connectivity components. You can also create and copy in connectivity sub-services.



Create Sub-Service

Parent Service: Branch Office

Server: decade

Owner: admin

Name: Connectivity

Description: Rest of World Connectivity

Type: And

Raise Events: ☑

Treat Unknown as Down: ☑

SLA Goal:

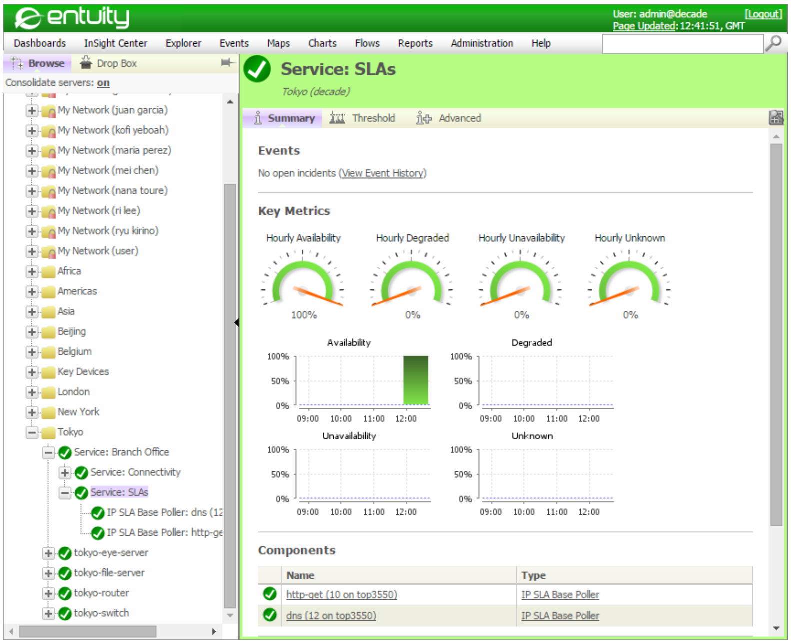
Icon: Default

OK Cancel

Figure 59 Create a Connectivity Service

5) From the Branch Office service click **Create Sub-Service** and define the **SLAs** service. The service must be called SLAs for the Branch Office Perspective to report on the service.

6) Drag and drop to SLAs sub-service IP SLA operations. You can drag and drop both monitored and managed IP SLA operations from a device’s Advanced page.



Events

No open incidents (View Event History)

Key Metrics

Components

| | Name | Type |
|---|---|---|
| ✓ | http-get (10 on top3550) | IP SLA Base Poller |
| ✓ | dns (12 on top3550) | IP SLA Base Poller |

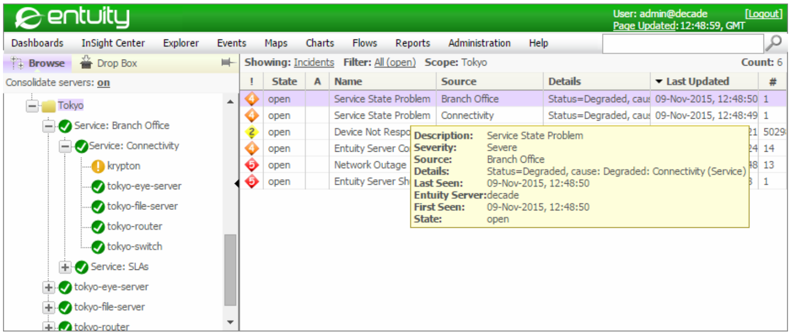
Figure 60 Branch Office SLAs Service

# Checking on Branch Office Service Status

You can manage the state of your Branch Office services by tracking service events through Event Viewer, by investigating services through dashboards and running reports.

Entuity includes these service specific events:

- Service Down indicates the named service is down and that the number of components failing in the service is sufficient to cause the service to fail.
- Service State Unknown indicates the state of the named service is unknown. The state of one or more of the components in the service is unknown.
- Service State Degraded indicates the state of the named service is degraded. The state of one or more of the components in the service is unknown.
- Service State Off indicates the named service is now configured as a service that does not return a state. Entuity closes any open incidents associated with this service.
- Service Up indicates the named service has transitioned to an up state.



Showing: Incidents Filter: All (open) Scope: Tokyo Count: 6

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| 4 | open | | Service State Problem | Branch Office | Status=Degraded, cau | 09-Nov-2015, 12:48:50 | 1 |
| 4 | open | | Service State Problem | Connectivity | Status=Degraded, cau | 09-Nov-2015, 12:48:49 | 1 |
| 2 | open | | Device Not Respo | | | | 5029 |
| 4 | open | | Entuity Server Co | | | | 14 |
| 5 | open | | Network Outage | | | | 13 |
| 5 | open | | Entuity Server Sh | | | | 1 |

Description: Service State Problem
Severity: Severe
Source: Branch Office
Details: Status=Degraded, cause: Degraded: Connectivity (Service)
Last Seen: 09-Nov-2015, 12:48:50
Entuity Server:decade
First Seen: 09-Nov-2015, 12:48:50
State: open

Figure 61 Branch Office Events

From Event Viewer you can place your mouse pointer over the event to display a pop up dialog that provides event details, with *Details* indicating the causal component(s) of the service event.

You can also investigate service performance from the web UI:

1) Click **Dashboards** > **Service Summary**. Depending on your Preferences settings, services are either grouped by view or alphabetically. You can view the current status of all services.

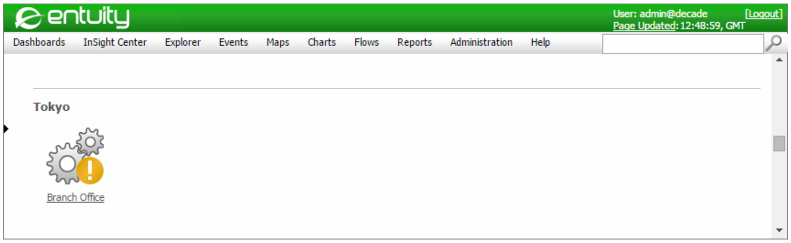
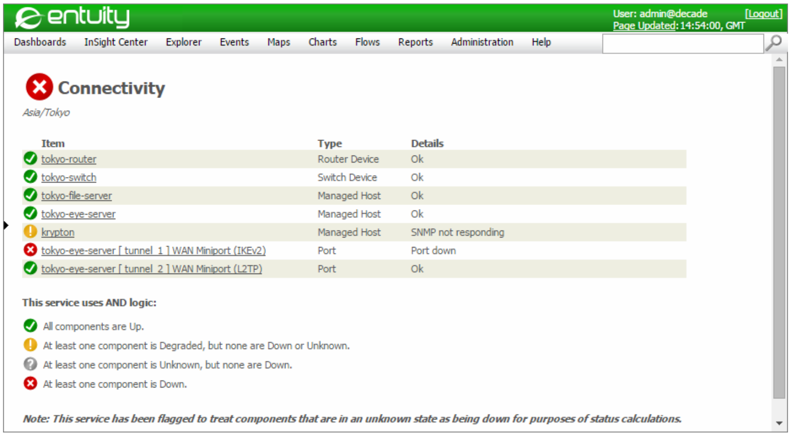


Figure 62 Service Summary Dashboard

2) For services that are down you can place the mouse pointer over the service to view a popup that details the failing component(s).

3) Click on the required service to drill down. Entuity displays details on the service, including its components, their current state and the logic used to derive the state of the service.

   You can further drill down to investigate the cause of component failures.



**Connectivity**

*Asia/Tokyo*

| | Item | Type | Details |
|---|---|---|---|
| ✓ | tokyo-router | Router Device | Ok |
| ✓ | tokyo-switch | Switch Device | Ok |
| ✓ | tokyo-file-server | Managed Host | Ok |
| ✓ | tokyo-eye-server | Managed Host | Ok |
| ! | krypton | Managed Host | SNMP not responding |
| ✗ | tokyo-eye-server [ tunnel_1 ] WAN Miniport (IKEv2) | Port | Port down |
| ✓ | tokyo-eye-server [ tunnel_2 ] WAN Miniport (L2TP) | Port | Ok |

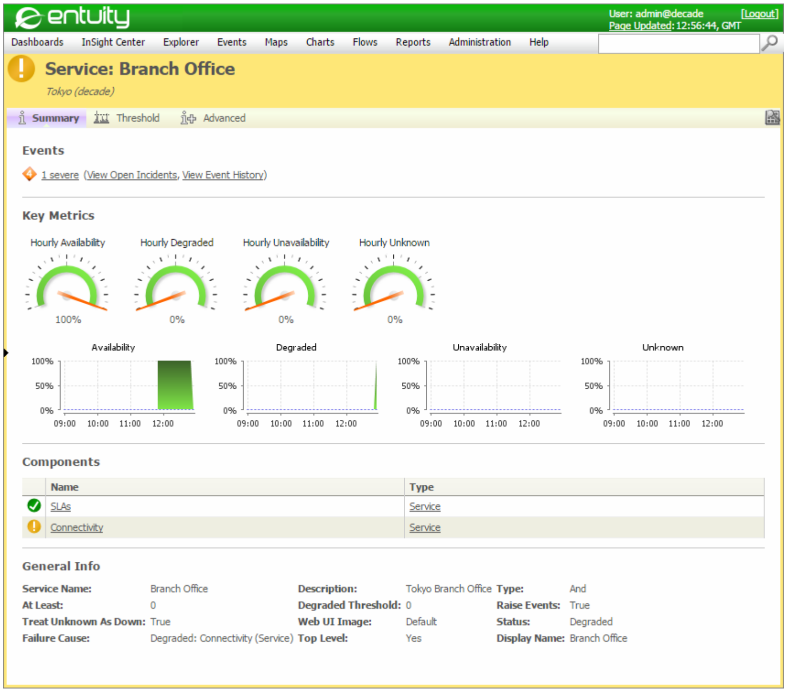
**This service uses AND logic:**

- ✓ All components are Up.
- ! At least one component is Degraded, but none are Down or Unknown.
- ? At least one component is Unknown, but none are Down.
- ✗ At least one component is Down.

*Note: This service has been flagged to treat components that are in an unknown state as being down for purposes of status calculations.*

Figure 63 Branch Office Component Drill-Down

As a service you can view further details on branch office perspective through the service Summary and Advanced pages. (See *Service Summary* and *Service Advanced Details*.)



**Service: Branch Office**

*Tokyo (decade)*

**Events**

1 severe (View Open Incidents, View Event History)

**Key Metrics**

**Components**

| | Name | Type |
|---|---|---|
| ✓ | SLAs | Service |
| ! | Connectivity | Service |

**General Info**

| | | | | | |
|---|---|---|---|---|---|
| **Service Name:** | Branch Office | **Description:** | Tokyo Branch Office | **Type:** | And |
| **At Least:** | 0 | **Degraded Threshold:** | 0 | **Raise Events:** | True |
| **Treat Unknown As Down:** | True | **Web UI Image:** | Default | **Status:** | Degraded |
| **Failure Cause:** | Degraded: Connectivity (Service) | **Top Level:** | Yes | **Display Name:** | Branch Office |

Figure 64 Branch Office Summary

# Viewing a Branch Office

The Branch Office Perspective aggregates the behavior of all the services in a chosen view and displays, by default, a summary of the previous twenty-four hours.

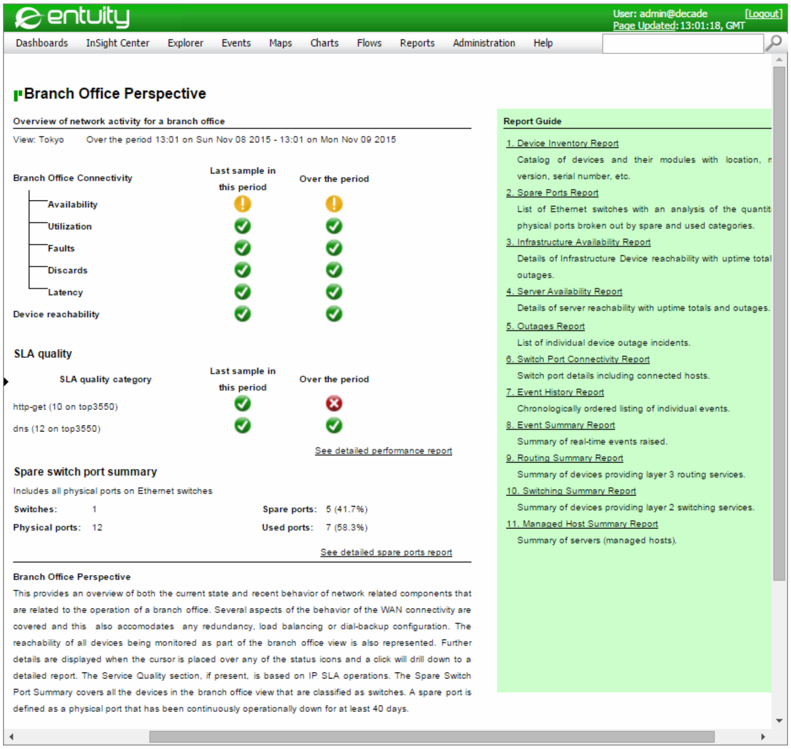
You can also access the more detailed branch office reports; Device Inventory Report, Spare Ports Report, Server Availability Report.

## Accessing the Branch Office Perspective

To access the Branch Office Perspective:

1) Click **InSight Center > Branch Office Perspective**. Entuity displays the Report Options dialog.

2) Select the Entuity server, branch office view and report period against which you want to apply the perspective.



Branch Office Perspective

Overview of network activity for a branch office

View: Tokyo Over the period 13:01 on Sun Nov 08 2015 - 13:01 on Mon Nov 09 2015

| Branch Office Connectivity | Last sample in this period | Over the period |
|---|---|---|
| Availability | ! | ! |
| Utilization | ✓ | ✓ |
| Faults | ✓ | ✓ |
| Discards | ✓ | ✓ |
| Latency | ✓ | ✓ |
| Device reachability | ✓ | ✓ |

SLA quality

| SLA quality category | Last sample in this period | Over the period |
|---|---|---|
| http-get (10 on top3550) | ✓ | ✗ |
| dns (12 on top3550) | ✓ | ✓ |

See detailed performance report

Spare switch port summary

Includes all physical ports on Ethernet switches

| | | | |
|---|---|---|---|
| Switches: | 1 | Spare ports: | 5 (41.7%) |
| Physical ports: | 12 | Used ports: | 7 (58.3%) |

See detailed spare ports report

Branch Office Perspective

This provides an overview of both the current state and recent behavior of network related components that are related to the operation of a branch office. Several aspects of the behavior of the WAN connectivity are covered and this also accomodates any redundancy, load balancing or dial-backup configuration. The reachability of all devices being monitored as part of the branch office view is also represented. Further details are displayed when the cursor is placed over any of the status icons and a click will drill down to a detailed report. The Service Quality section, if present, is based on IP SLA operations. The Spare Switch Port Summary covers all the devices in the branch office view that are classified as switches. A spare port is defined as a physical port that has been continuously operationally down for at least 40 days.

Report Guide

1. Device Inventory Report
   Catalog of devices and their modules with location, r
   version, serial number, etc.
2. Spare Ports Report
   List of Ethernet switches with an analysis of the quantit
   physical ports broken out by spare and used categories.
3. Infrastructure Availability Report
   Details of Infrastructure Device reachability with uptime total
   outages.
4. Server Availability Report
   Details of server reachability with uptime totals and outages.
5. Outages Report
   List of individual device outage incidents.
6. Switch Port Connectivity Report
   Switch port details including connected hosts.
7. Event History Report
   Chronologically ordered listing of individual events.
8. Event Summary Report
   Summary of real-time events raised.
9. Routing Summary Report
   Summary of devices providing layer 3 routing services.
10. Switching Summary Report
    Summary of devices providing layer 2 switching services.
11. Managed Host Summary Report
    Summary of servers (managed hosts).

Figure 65 Branch Office Perspective

# Viewing Multiple Branch Offices

The Multiple Branch Office perspective provides an overview of the recent behavior of network related components that are related to the operation of all the accessible branch offices. Several aspects of the behavior of the WAN connectivity are covered and this also accommodates any redundancy, load balancing or dial-backup configuration. The reachability of all devices monitored as part of the branch office view is also represented.

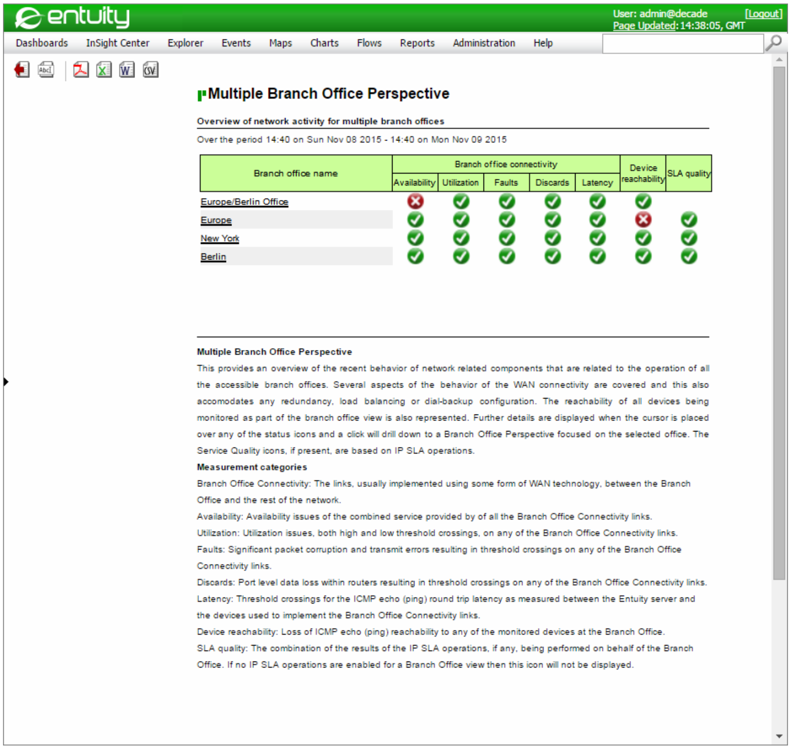
The perspective chart details:

- *Branch office name*, name of the view containing the perspective.
- *Branch office connectivity* provides different measures of the status of the links between the Branch Office and the rest of the network. Each metric icon is also a hyperlink to the Branch Office Details report:
  - Availability icon indicates the state of the combined service provided by of all the Branch Office connectivity links.
  - Utilization icon indicates threshold crossings, high or low, on any of the Branch Office connectivity links.
  - Faults icon indicates the presence of packet corruption and transmit errors on any of the Branch Office connectivity links.
  - Discards icon indicates the level of port level data loss within routers resulting in threshold crossings on any of the Branch Office Connectivity links.
  - Latency icon indicates the state of threshold crossings for the ICMP echo (ping) round trip latency as measured between the Entuity server and the devices used to implement the Branch Office connectivity links.
- Device reachability indicates loss of ICMP echo (ping) reachability to any of the monitored devices at the Branch Office. Selecting the icon drills down to the Branch Office Details report with the focus on Device Reachability.
- SLA quality icon indicates the state of the combination of the results of the IP SLA operations, if any, being performed on behalf of the Branch Office. If no IP SLA operations are enabled for a Branch Office view then this icon is not displayed. Selecting the icon drills down to the Branch Office Details report with the focus on IP SLA operations defined in the SLAs sub-service of the branch office.

## Accessing Multiple Branch Office Perspective

To access the Multiple Branch Office Perspective:

1) Click **InSight Center > Multiple Branch Office Perspective**. Entuity displays the branch offices to which the user currently has access through the server, including remote Entuity servers.



**Multiple Branch Office Perspective**

**Overview of network activity for multiple branch offices**

Over the period 14:40 on Sun Nov 08 2015 - 14:40 on Mon Nov 09 2015

| Branch office name | Branch office connectivity | | | | | Device reachability | SLA quality |
|---|---|---|---|---|---|---|---|
| | Availability | Utilization | Faults | Discards | Latency | | |
| Europe/Berlin Office | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Europe | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| New York | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Berlin | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

**Multiple Branch Office Perspective**

This provides an overview of the recent behavior of network related components that are related to the operation of all the accessible branch offices. Several aspects of the behavior of the WAN connectivity are covered and this also accomodates any redundancy, load balancing or dial-backup configuration. The reachability of all devices being monitored as part of the branch office view is also represented. Further details are displayed when the cursor is placed over any of the status icons and a click will drill down to a Branch Office Perspective focused on the selected office. The Service Quality icons, if present, are based on IP SLA operations.

**Measurement categories**

Branch Office Connectivity: The links, usually implemented using some form of WAN technology, between the Branch Office and the rest of the network.

Availability: Availability issues of the combined service provided by of all the Branch Office Connectivity links.

Utilization: Utilization issues, both high and low threshold crossings, on any of the Branch Office Connectivity links.

Faults: Significant packet corruption and transmit errors resulting in threshold crossings on any of the Branch Office Connectivity links.

Discards: Port level data loss within routers resulting in threshold crossings on any of the Branch Office Connectivity links.

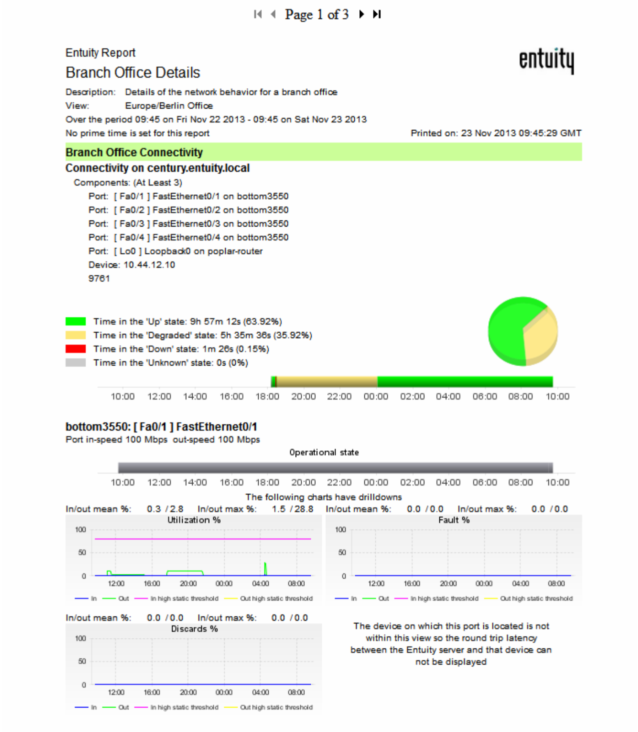
Latency: Threshold crossings for the ICMP echo (ping) round trip latency as measured between the Entuity server and the devices used to implement the Branch Office Connectivity links.

Device reachability: Loss of ICMP echo (ping) reachability to any of the monitored devices at the Branch Office.

SLA quality: The combination of the results of the IP SLA operations, if any, being performed on behalf of the Branch Office. If no IP SLA operations are enabled for a Branch Office view then this icon will not be displayed.

Figure 66 Multiple Branch Office Perspective

2) You can click on a branch office to open the Branch Office Perspective, or click on a particular metric to open a Branch Office report in that context. For example click on a branch office's Availability icon to run a report on branch office connectivity over the previous 24 hours.



Page 1 of 3

Entuity Report

Branch Office Details

Description: Details of the network behavior for a branch office

View: Europe/Berlin Office

Over the period 09:45 on Fri Nov 22 2013 - 09:45 on Sat Nov 23 2013

No prime time is set for this report

Printed on: 23 Nov 2013 09:45:29 GMT

**Branch Office Connectivity**

**Connectivity on century.entuity.local**

Components: (At Least 3)

Port: [ Fa0/1 ] FastEthernet0/1 on bottom3550
Port: [ Fa0/2 ] FastEthernet0/2 on bottom3550
Port: [ Fa0/3 ] FastEthernet0/3 on bottom3550
Port: [ Fa0/4 ] FastEthernet0/4 on bottom3550
Port: [ Lo0 ] Loopback0 on poplar-router
Device: 10.44.12.10
9761

🟩 Time in the 'Up' state: 9h 57m 12s (63.92%)
🟨 Time in the 'Degraded' state: 5h 35m 36s (35.92%)
🟥 Time in the 'Down' state: 1m 26s (0.15%)
⬜ Time in the 'Unknown' state: 0s (0%)

**bottom3550: [ Fa0/1 ] FastEthernet0/1**

Port in-speed 100 Mbps out-speed 100 Mbps

The following charts have drilldowns

In/out mean %: 0.3 / 2.8 In/out max %: 1.5 / 28.8

In/out mean %: 0.0 / 0.0 In/out max %: 0.0 / 0.0

In/out mean %: 0.0 / 0.0 In/out max %: 0.0 / 0.0

The device on which this port is located is not within this view so the round trip latency between the Entuity server and that device can not be displayed

Figure 67 Branch Office Connectivity

# 23 Managing Performance and Asset Utilization

When managing a network it is valuable to know which areas of your network are being overutilized and which are being underutilized. It may then be possible to redistribute network resources to where they are most required rather than purchasing new resources. These are key performance and asset utilization measures:

- Utilization, expressed as a percentage of actual traffic volume against the maximum volume that can be handled by the port.
- Router measurements, for example CPU and processor utilization.
- Switch backplane utilization.
- Frame Relay PVC, ATM VCC utilization.
- QoS classes.

## Monitoring Port Utilization

In Entuity port utilization is expressed as a percentage of actual traffic volume against the maximum volume that can be handled by the port. As a port can return an inaccurate maximum speed, Entuity allows you to modify its interface speed for use in this calculation.

You can monitor a port's utilization performance through:

- Graphs that report inbound and outbound utilization.
- A series of utilization reports. (See the *Entuity Reports Reference Manual.*)
- Alarms that Entuity raises when a port's utilization values cross one of the utilization thresholds. (See *Utilization Threshold Alarms*.)

### Utilization Threshold Alarms

Entuity allows you to set port utilization thresholds that when broken generate alarms that appear on the Event Viewer. There are both static and dynamic utilization thresholds for inbound high and low utilization and outbound high and low utilization.

Dynamic thresholds enable Entuity to alert the user to deviations from what Entuity's previous polling has established as normal behavior for that hour on that day. Entuity establishes normal behavior for a given attribute on a given port by maintaining the last four weeks worth of polled data, and applying an averaging algorithm.

You can set these thresholds at the:

- Network level, for all of the ports on the selected network.
- Device level, for all of the ports on a device.
- Port level, just for the selected port.

These are the types of available threshold events:

- High utilization events. Each poll that returns a value over the high utilization threshold generates an alarm. When a poll returns a value lower than the threshold, Entuity generates a high utilization cleared event. This clears all of the high utilization alarms for that port.

There are high utilization events on both inbound and outbound utilization.

- Low utilization events. Each poll that returns a value lower than the low utilization threshold generates an alarm. When a poll returns a value higher than the threshold, Entuity generates a low utilization cleared event. This clears all of the low utilization alarms for that port.

  There are low utilization events on both inbound and outbound utilization.

## Setting Utilization Thresholds

Entuity's default static threshold settings are for:

- High utilization events, 80%.
- Low utilization events, 0%. As you can never return a utilization sample lower than 0, by default this alarm is effectively suppressed.

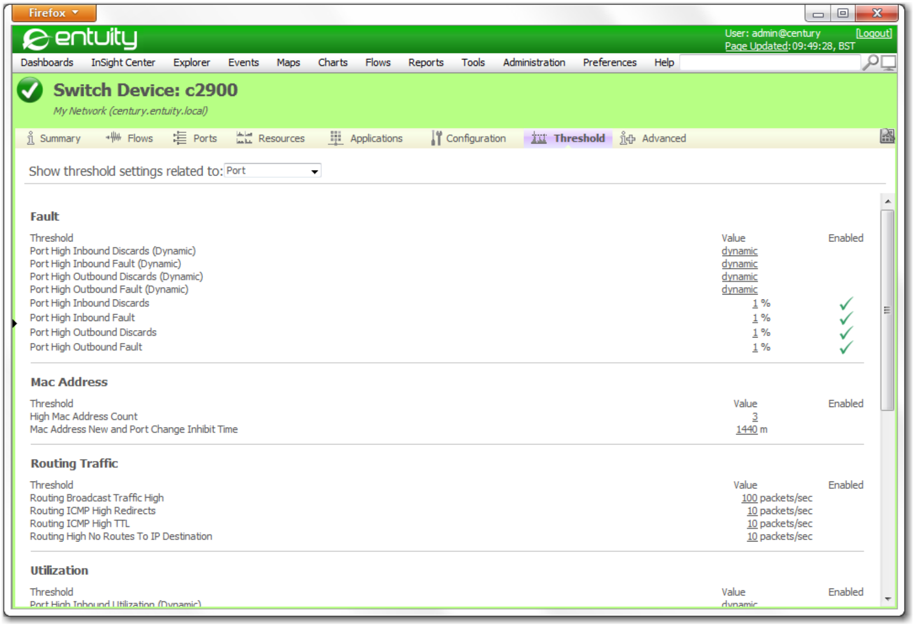
By default, all dynamic thresholds are turned off. You can turn on the dynamic threshold at the device and port level, in a similar way to static thresholds. Dynamic thresholds cannot be applied at the root (i.e. Entuity server) or view level.

To set thresholds:

1) From the Entuity web UI use Explorer to navigate to and select the object, e.g. device, against which you want to configure thresholds.
2) Click **Thresholds**. Entuity displays the threshold page.
3) From *Show threshold settings related to* select **Ports**. Entuity displays the port thresholds.
4) For the threshold you want to set, select the threshold settings (for dynamic thresholds this may be dynamic). Entuity displays the Edit Dynamic/Static Threshold dialog.
5) Select **Enabled**.

   You can also amend for:

   - Dynamic thresholds the tolerance value. Tolerance sets how much above the historic baseline utilization must be before it triggers an event.
   - Static thresholds the threshold value.
6) Click **OK**. Entuity activates the threshold, indicating that on the Thresholds page by displaying a tick in the Enabled column and Remove Override icon.



Switch Device: c2900

*My Network (century.entuity.local)*

Show threshold settings related to: Port

**Fault**

| Threshold | Value | Enabled |
|---|---|---|
| Port High Inbound Discards (Dynamic) | dynamic | |
| Port High Inbound Fault (Dynamic) | dynamic | |
| Port High Outbound Discards (Dynamic) | dynamic | |
| Port High Outbound Fault (Dynamic) | dynamic | |
| Port High Inbound Discards | 1 % | ✓ |
| Port High Inbound Fault | 1 % | ✓ |
| Port High Outbound Discards | 1 % | ✓ |
| Port High Outbound Fault | 1 % | ✓ |

**Mac Address**

| Threshold | Value | Enabled |
|---|---|---|
| High Mac Address Count | 3 | |
| Mac Address New and Port Change Inhibit Time | 1440 m | |

**Routing Traffic**

| Threshold | Value | Enabled |
|---|---|---|
| Routing Broadcast Traffic High | 100 packets/sec | |
| Routing ICMP High Redirects | 10 packets/sec | |
| Routing ICMP High TTL | 10 packets/sec | |
| Routing High No Routes To IP Destination | 10 packets/sec | |

**Utilization**

| Threshold | Value | Enabled |
|---|---|---|
| Port High Inbound Utilization (Dynamic) | dynamic | |

Figure 68 Threshold Settings

## Set Port Interface Speeds

Utilization is expressed as a percentage of actual traffic volume against the maximum volume that can be handled by the port. Occasionally ports are set to a misleading interface speed which if left unchecked would distort the port's utilization value. To handle this possibility Entuity allows you to amend port interface speed values. These amended values are only used in Entuity.

To amend port interface speed:

1)

2) From the context menu select **Edit**.

3) Through Outbound Speed and Inbound Speed you can set separate values for outbound and inbound interface speeds. To reset the value to the polled setting delete the override value and leave the field empty.

   Enter the port's interface speed and select the appropriate measurement, i.e. **bits**/**sec**, **Kbits**/**sec** or **Mbits**/**sec**.

4) Click **OK** to save the settings.

# 24 Monitoring Edge of Network Change

Entuity monitors the edge of your network for potentially harmful configuration changes using MAC (Media Access Control) addresses, the unique identifiers attached to most forms of networking equipment.

The MAC address change and MAC address high count events are useful tools for detecting and reporting configuration changes at the edge of your network, and change is the dominant cause of IT problems. The NOC typically has little visibility into hardware and change at IT extremities, such as remote offices. Hardware changes and additions to the network in a remote office can significantly impact network performance.

Once Entuity identifies a change you can investigate, for example using Maps to see the port's device in its network context and then drilling down for further details.

## Using MAC Address Events

Entuity monitors the operational state of all managed ports. By default, Entuity polls every five minutes for a state change. For fast polled ports Entuity polls every minute.

When a port transitions from inactive to active, `macScheduler` runs `macman`. A transition indicates other port changes are possible, running `macman` polls MAC addresses on the port. Entuity maintains a history of MAC addresses, by default the last 50 MAC addresses on each port. By referencing this history Entuity can determine which MAC addresses are new only to the port and which are, potentially more seriously, new to the network.

Through the port's Advanced page you can view the MAC Address history. It is also available through Flex Reports.

### Available MAC Address Events

There are three types of MAC address events:

- MAC Address New, indicates the MAC address is new to the current port
- MAC Address Port Change, indicates the MAC address is new to the current port but Entuity retains a record of it occurring on other managed ports
- MAC Address High Port Count and its correlated clearing event. This is a set threshold.

When Entuity raises MAC Address New and MAC Address Port Change events together this indicates a host has changed port, when Entuity raises only the MAC Address New event this indicates a new host and a greater potential security risk.

For full details on when the events are raised refer to the *Entuity Events Manual*.

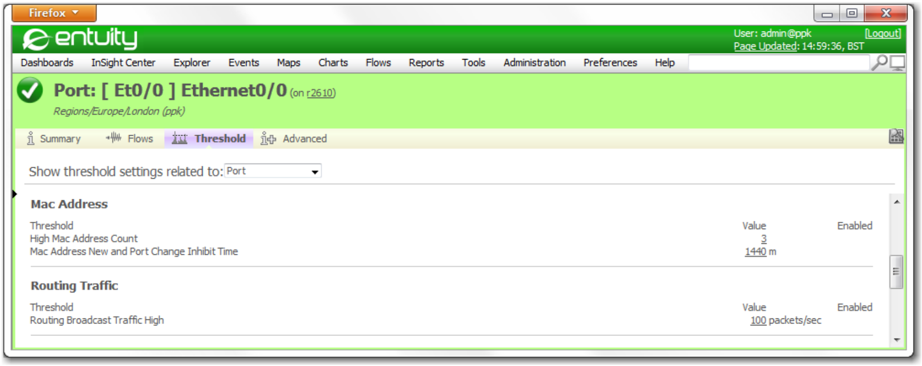
### Enabling MAC Address High Port Count Event

You can configure the number of MAC addresses held against a port that you would consider a security concern. By default the MAC Address High Port Count event is disabled.

To enable or amend its thresholds:

1) From the web UI navigate to the port’s **Threshold** tab.

2) In High MAC Address Count Threshold, select **Enable**. You can either accept or amend the number of MAC addresses permitted on the interface. When a port has more MAC addresses than this threshold value Entuity raises a MAC Address High Port Count.



Port: [ Et0/0 ] Ethernet0/0 (on r2610)
Regions/Europe/London (ppk)

Show threshold settings related to: Port

**Mac Address**

| Threshold | Value | Enabled |
|---|---|---|
| High Mac Address Count | 3 | |
| Mac Address New and Port Change Inhibit Time | 1440 m | |

**Routing Traffic**

| Threshold | Value | Enabled |
|---|---|---|
| Routing Broadcast Traffic High | 100 packets/sec | |

Figure 69 MAC Address Threshold Settings

## Enabling MAC Address New and Change Events

By default the MAC Address New and MAC Address Port Change events are disabled. They are enabled through the MAC Address New and Port Change Inhibit Time Enabled tick box within the Ports thresholds tab.

The MAC Address New and Port Change Inhibit Time setting prevents Entuity from raising MAC Address New events on newly discovered ports, i.e. you would expect Entuity to discover new MAC addresses on a newly discovered port so Entuity raising a flood of MAC Address New events would not be noteworthy. You would only want a MAC Address New event raised against a port when Entuity had previously discovered the port’s MAC addresses and had now discovered additional MAC addresses.

To enable the thresholds or amend the MAC address threshold values:

1) Navigate to the port’s **Threshold** tab and from *Show threshold settings related to* select **Port**.

2) In MAC Address New and Port Change Inhibit Time, select **Enable**.

3) You can amend the inhibit value, but Entuity Support recommend accepting the default value of 1440 minutes (24 hours).

# 25 Set-up and Manage Flow Data

Routers and switches that support flow data collection, can collect IP traffic statistics on all interfaces where flow collection is enabled. Administrators can configure the devices to later export those statistics as flow records, toward at least one Entuity server configured as a collector. The same server would usually store flow data and perform traffic analysis.

Entuity includes Integrated Flow Analyzer (IFA) for monitoring traffic flow across your managed network. The Entuity Integrated Flow Analyzer Premium (IFA Premium) module fully integrates with and extends the entry level functionality delivered by Entuity IFA.

## Integrated Flow Analyzer

The Entuity Integrated Flow Analyzer (IFA) is a short time span diagnostic and troubleshooting tool. It avoids the burden of heavy data gathering, synthesis, and storage, whilst still delivering the facility to characterize and understand IP traffic. Entuity IFA integrates flow-based performance data in the Entuity web UI alongside Entuity's traditional elemental performance metrics. You can identify network congestion, applications consuming high percentages of bandwidth, and the source and destination of network traffic.

IFA allows for:

- Collection of flow data from its own local collector.
- Collection and storing of data with a granularity of five minutes.
- Data to be retained for one month.
- Storing of flow data in a compressed, and also in its uncompressed form by disabling de-ephemeralisation.

IFA delivers:

- Data samples of five minutes, one hour, six hours and daily.
- Analysis of data with ten available breakdowns, for example.
- Four types of chart, line, bar, pie and stacked area.

## Integrated Flow Analyzer Premium Module

Integrated Flow Analyzer Premium (IFA Premium) is a separately licensed module available with Entuity. IFA Premium extends the performance of Entuity IFA, providing greater flow collection and storage capabilities, with more refined presentation and filter control.

IFA Premium allows for:

- Management of flow data collection on remote servers, the number of remote collectors is defined through the IFA Premium license.
- Collection and storing of data with a granularity of one minute. You must activate this collection through the flow section in `entuity.cfg`.
- Data to be retained by more than one month. You can amend data retention through the

flow section in `entuity.cfg`.

IFA Premium delivers an enhanced user interface which allows for:

- Entering *From* and *To* date/time for data analysis.
- Analysis of data by conversation, i.e. both source and destination IP addresses are considered, through a new Top Conversations breakdown.
- Definition of Custom Breakdowns, through which you can analyze flow data by an arbitrary combination of data types, for example source IP address, destination IP address, source port, destination port, host IP address, interface, application, protocol, QoS class.
- Definition of custom data types, whose members, are defined in terms of the available raw data types. This is synonymous with custom groups and group based analysis. (See *Create Your Own Flow Breakdowns*.)

## Prerequisites for IFA Implementation

Prerequisites for IFA and IFA Premium module are essentially the same. With IFA Premium you may want to consider storage requirements when greatly extending the retention period of collected flow data.

### Licensing IFA

The standard IFA functionality is available with the standard Entuity license. You can enable this functionality when running `configure` and selecting the appropriate Entuity server capability. (See *Server Roles and Flow Collectors*.)

Entuity IFA Premium is a licensable module. When you run `configure`, and your license includes the module, you can enable its functionality by selecting the appropriate Entuity server capability. Contact your Entuity representative if your license does not include, but you require, the Premium module.

The Entuity evaluation license includes Entuity IFA Premium.

### Configure Devices to Send Flow Data

You must configure devices to forward their flow information to the Entuity server you want to act as the flow collector. For a server to start collecting flow data from a device an Entuity server must manage that device, so you would usually configure the device to forward its flow data to its managing Entuity server.

However Entuity separates the flow receiving, data collection and processing from management of the device, which for Entuity IFA Premium allows you to assign flow data received by one server to a second server that acts as a master flow collector.

A device would usually export its data to one Entuity flow collector, but they can potentially export to two.

Entuity IFA can collect flow data from devices that use either 16-bit or 32-bit interface indexing, from devices running a supported flow version:

- NetFlow v5.

- Sampled NetFlow v5.
- NetFlow v6.
- NetFlow v7.
- NetFlow v9, support for the most commonly used templates.
- Sampled NetFlow v9.
- IPFIX, comparable support to that delivered for NetFlow v9.
- Netstream v5.
- Netstream v9.
- sFlow v4.
- sFlowv5.
- JFlow, for Juniper
- VMware NSX based flows containing VXLAN information.

Entuity supports bidirectional flows for NetFlow v9 and NetFlow v10(IPFIX). The bi-directional NetFlow template contains two fields describing the data transfer:

```
(NF_F_FWD_FLOW_DELTA_BYTES(231), NF_F_REV_FLOW_DELTA_BYTES(232))
```

Each data record describes transfer in two directions from source to destination and from destination to source. The first field is the transfer from source >destination and the second destination > source. The unidirectional template contained one field:

```
(IN_BYTES(1))
```

Entuity IFA also supports Flexible NetFlow configurations.

Entuity IFA requires the exporting router to be configured with the IP address of the target Entuity server and a port number:

- Entuity requires that sFlow and IPFIX packets are sent to specific ports and these ports are not configurable. For:
  - IPFIX you must set your router to export IPFIX to port 2055 of the Entuity server.
  - sFlow you must set your router to export sFlow to port 6343 of the Entuity server.
- All other supported flow technologies, i.e. NetFlow, Netstream and JFlow, are by default received by the Entuity server on port 9996. You can set Entuity to accept this flow data on any port, excluding ports 2055 and 6343, through:
  - *Flow Port* in `configure`. (See *Configure Flow Export on Devices*.)
  - *entuity_home*/`etc/flowcfg.properties`. (See *`Advanced Flow Collector Setup`*.)

Entuity IFA can simultaneously handle IPFIX, sFlow and other flow technology packets. However you must ensure that the routers are forwarding flow packets to the appropriate port for that technology.

## Cisco ASA NetFlow Support

Entuity IFA supports monitoring of NetFlow on Cisco ASA devices, however this is dependent on the particular Cisco ASA version.

| Cisco ASA Version | Entuity IFA Support |
|---|---|
| 8.2(5) | Not supported. |
| 8.4(5) | Supported. |
| 8.4(7)-k8 | Supported. |
| 9.0(2) | Not supported. |
| 9.1(6) | Supported. |
| 9.2(4) | Supported. |

Table 14 Cisco ASA NetFlow Support

## VMware NSX Support

Entuity supports monitoring of VMware NSX SDN flows (i.e. VXLAN overlays). It delivers detailed statistics for both native IP flows and NSX VXLAN encapsulated traffic, e.g. traffic rates, packet rates, application breakdowns, QoS settings.

Data obtained by directly monitoring the NSX infrastructure (including VMware VDS) is combined with VXLAN flow records. This allows traffic flows received from non-NSX aware devices within a network core (e.g. Cisco routers) to be presented and optionally decomposed into their constituent flows. Users can view exactly which VM-VM flows used a given VXLAN tunnel at any instrumented point in the core and at any point in time. This allows easy highlighting of, for example fragmentation, packet loss, utilization, at key points in the virtual and physical infrastructure.

## Advanced Flow Collector Setup

Entuity IFA flow collectors are shipped with a setup suitable for most network environments. This configuration is replicated in *entuity_home*/`etc/flowcfg-template.properties`. The configuration options available within it are greater than those available when you run `configure`, for example you can specify additional collector ports, amend the size of the buffers handling the incoming flow data. (See the *Entuity System Administrator Reference Manual*.)

When you want to amend the flow collection configuration you should not make changes to the template file but instead create a copy in *entuity_home*/`etc` and rename the copy to `flowcfg.properties`. Changes to this file are automatically discovered by Entuity and maintained during system upgrades.

✓ Configurations specified in *entuity_home*/`etc/flowcfg.properties` have the highest priority; it overrides values set for the same parameter through `configure`. These options are not applicable to Entuity IFA support of the IPFIX and sFlow technologies.

## Collect Flow Data

When an Entuity server has the appropriate license, is configured for the appropriate role and is receiving flows you can then configure the server to collect flow data.

You can:

- Assign the collection of flow data to an Entuity server.

  Entuity All-in-one servers have their own flow collector automatically assigned to them.

  IFA Premium allows you to assign the flow collectors of one server to another server that acts as a master flow collector. You can view and change the assignment of flow collectors through **Administration > Multi-Server Administration**.

  See *Assigning Flow Collectors*.

- Activate flow collection for the required devices.

  You activate flow collection from the Entuity server managing the device. IFA Premium allows you to manage the device on a different Entuity server to that which you configured the device to forward its flow data.

  You can stop flow collection from both the managing server and flow collector.

  See *Start and Stop Flow Collection*.

- Control user access to IFA functionality.

  All administrators have access to this functionality, and you can assign other user groups flow inspection access through Account Management.

- Configure filters to exclude specified flow data and make amendments to the application to flow data mappings.

  See *Configuring Filters to Exclude Flow Data* and *Mapping Applications to Protocol Flow Data*.

## Flow Data Retention and Security

Flows generate a large amount of data for which Entuity uses four levels of data rollup. By default IFA retains:

- Five minute samples for two hours.
- Hourly samples for twenty-four hours.
- Six-hourly samples for seven days.
- Daily samples for thirty-five days, although access to a maximum of thirty-one days is available through the web UI.

With IFA Premium you can:

- Collect, store, view and report on flow data with a granularity of one-minute, by default for one week. You must configure:
  - Routers to send flow data every sixty seconds.
  - Entuity to retain one minute samples, through the flow section of `entuity.cfg`.

- Store more than one month of flow data, the only restriction is the hard drive capacity although the default is one year.

  Although you can store more than one month of data, you can only perform flow analysis on a maximum of one month (thirty-one days) of data at one time.

When you query data Entuity IFA uses the most appropriate data sample, e.g hourly data is accessible when the requested time period is less than one day.

Users with the Flow Inspection permission have access to all of the collected flow data, this includes data from interfaces to which they otherwise do not have access to in Entuity.

### Flow Collection and Entuity Zones

Entuity IFA is zone aware. When using different Entuity servers to manage and collect flow data then the servers must have the same zone setup. Zones on separate Entuity servers are independent of each other, however if you configure them with the same setup then the Entuity servers can assign flow data to the correct zones.

## Server Roles and Flow Collectors

An Entuity flow collector receives flow records sent from devices configured to send it flow data. You can activate flow collectors on Entuity servers that are also managing and polling devices, All-in-one servers.

With IFA Premium you can assign flow collectors from one server to a second server; the second server acts as the master flow collector. You also have the option of using an All-in-one server as a dedicated flow collector, where the server only collects flow data and a separate Entuity server polls and manages the device. Role separation is useful in large networks. (See the *Entuity Getting Started Guide*.)

### Standard Entuity Server

When configured as a Standard Entuity server Entuity acts as a polling engine, e.g. managing inventory, monitoring faults, performance and availability, with multi-server consolidation, reports, event management.

The Entuity IFA flow collection capability is disabled for the server, however IFA Premium can display flow data collected by remote servers and remote assigned flow collectors, e.g. through the Flows page.

### Flow Collectors on All-in-one Servers

You can configure Entuity as an All-in-one server, where a server can act as both a polling engine and a flow collector. Where the one server both polls and collects flow data you can:

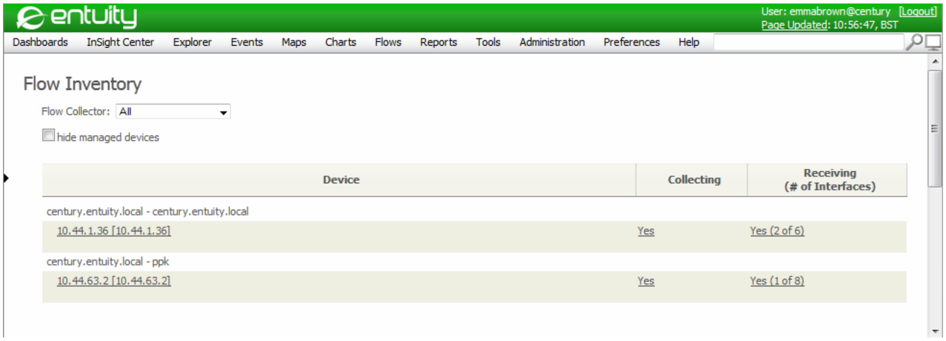
- Start and stop the collection of flow data from the device Flows page.
- View the status of flow collection.

  The flow collector accepts all valid flow data from devices configured to forward it data.
- Configure custom dashboards with summary charts on key flow data, viewing in realtime changes in the performance of your network.

- Configure exclusion filters and map port to applications.
- Access all Entuity functionality, e.g. view flow data within the context of device polled data, track related events, manage user accounts, run reports.

With IFA Premium you can:

- Assign to the server other flow collectors and remote All-in-one servers.
- Use the full flexibility of an All-in-one server, to build the structure of Entuity servers that best meet your requirements:
  - Polling only.
  - Flow Collector only.
  - Polling and Flow Collector enabled.
  - Polling and Flow Collectors disabled. This consolidation role allows you to assign to it other All-in-one servers, for example to use a server as a reporting server.



Flow Inventory

Flow Collector: All

□ hide managed devices

| Device | Collecting | Receiving<br>(# of Interfaces) |
|---|---|---|
| century.entuity.local - century.entuity.local | | |
| 10.44.1.36 [10.44.1.36] | Yes | Yes (2 of 6) |
| century.entuity.local - ppk | | |
| 10.44.63.2 [10.44.63.2] | Yes | Yes (1 of 8) |

Figure 70 Flow Inventory on an All-in-one Server

## IFA Premium and Remote Flow Collectors

With IFA Premium you can use an All-in-one Entuity server as a dedicated flow collector, where the server can only act as a flow collector. You must then assign this flow collector to an Entuity polling server. It is from the polling server that you instigate flow collection on its devices; although the flow data is collected, processed and stored on the dedicated flow collector server.

When you login to a dedicated flow collector you can:

- View the status of flow collection.

  The flow collector accepts all valid flow data from devices configured to forward it data. The flow collector does not manage the device, i.e. any polling of that device is undertaken on a separate Entuity polling server.

- Stop the collection of flow data from a device.

  You can also stop the collection of flow data from the sever to which the flow collector is assigned.

- Configure user accounts.

On the dedicated flow collector you can also configure exclusion filters and map port to applications.

The data collected by a flow collector is available from the Entuity polling server, the master flow collector, to which it is assigned. For the Entuity polling server to display this data:

- It must manage the device.
- The receiving of flow data from that device on the polling server must be enabled.

When you reassign flows to another master flow collector, all of the data already collected is lost.

## Control Access to Flow Data

By default members of the Administrators user group have full access to the IFA functionality. You must explicitly assign other user groups flow permissions through the Flow Inspection permission. Flow Inspection:

- Allows users to:
  - View flow data.
  - Start and stop flow collection.
  - Generate interactive charts.
  - Access flow data when creating reports.
- Does not allow users to:
  - Run the Flow Health report
  - Assign flow collectors to master flow collectors, a function only available when running IFA Premium.

## Assigning Flow Collectors

An Entuity server can receive and display flow data from the flow collectors which are assigned to it. A flow collector can only be assigned to one Entuity server at one time, although one Entuity server running IFA Premium can have as many collectors assigned to it as its license permits. If you reassign a flow collector from one server to another, all of the data collected and retained by that flow collector when it was managed by the original server is lost.

You can only assign flow collectors to Entuity servers configured as All-in-one servers. These servers have their own flow collector automatically assigned to them. You can view all assigned flow collector through the multi-server administration page.

✓ The role of flow collector is the same whether it is on the same server as the polling engine or on a separate machine, one acting as a dedicated flow collector.

| Attributes | Description |
|---|---|
| *Server* | Resolved name or IP address of the remote flow collector. |
| *Web Port* | Web port used by the Entuity remote flow collector. |
| *SSL* | Select SSL when used by the remote Entuity server. |
| *Username* | User account on the remote Entuity server that is a member of the administration group. |
| *Password* | Valid password for the user account. |

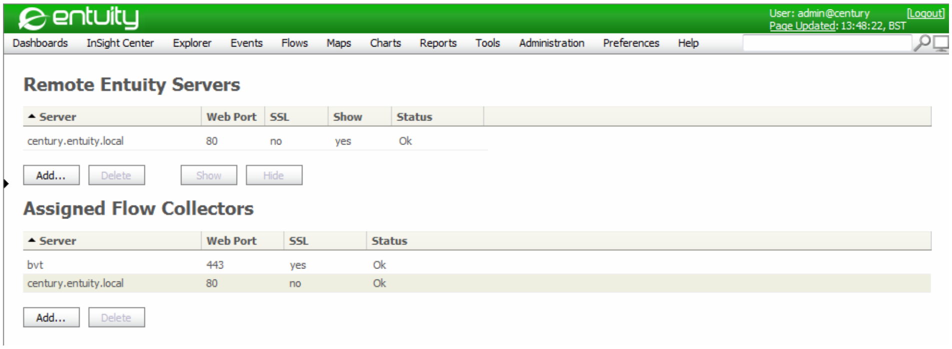
Table 15 Add a Flow Collector

To assign a flow collector to an Entuity server running IFA Premium:

1) Ensure the flow collector is running.
2) Login to the Entuity server to which you want to assign the flow collector.
3) Click **Administration > Multi-Server Administration > Remote Entuity Servers**.
4) From the Assigned Flow Collectors section click **Add**. Entuity displays the Add Flow Collector page.
5) Complete the collector details and click **Submit**.

   Entuity attempts to add the collector server, failing with an appropriate warning message if the validation details are incorrect or communication with the server cannot be established.

   Entuity also warns when connecting to a flow collector already assigned to another Entuity server as this reassignment would lose all of the data maintained on the flow collector for the original Entuity server.
6) On a successful connection Entuity displays the Remote Entuity Servers page, complete with the assigned flow collectors.



Remote Entuity Servers

| Server | Web Port | SSL | Show | Status |
|---|---|---|---|---|
| century.entuity.local | 80 | no | yes | Ok |

Assigned Flow Collectors

| Server | Web Port | SSL | Status |
|---|---|---|---|
| bvt | 443 | yes | Ok |
| century.entuity.local | 80 | no | Ok |

Figure 71 Assigned Flow Collectors

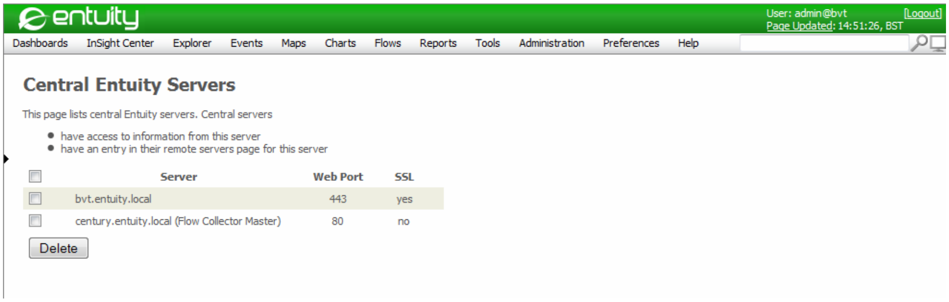
### Identifying Which Server is Managing Flow Data

With IFA the local Entuity server manages its own flow data. With IFA Premium Entuity servers can act as master flow collectors; as Entuity servers to which you can assign other Entuity server’s flow collectors. The IFA Premium license restricts the number of assigned flow collectors a master flow collector can support, you can view the number of collectors your license supports through the Remote Entuity Servers page.

To view trusted Entuity servers acting as flow collectors:

1) Click **Administration** > **Multi-Server Administration** > **Central Entity Servers**.

The Central Servers page lists the remote servers that can access information on the local server. It also indicates when the central server acts as a master server for flow collection.


entuity
User: admin@bvt [Logout]
Page Updated: 14:51:26, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Preferences Help
Delete

Central Entuity Servers

This page lists central Entuity servers. Central servers

- have access to information from this server
- have an entry in their remote servers page for this server

| □ | Server | Web Port | SSL |
|---|---|---|---|
| □ | bvt.entuity.local | 443 | yes |
| □ | century.entuity.local (Flow Collector Master) | 80 | no |

Figure 72 Central Server as a Master Flow Collector

## Configure Flow Export on Devices

You should always consult your device documentation before configuring the export of flow data from a device. This section uses an example export configuration to illustrate the configuration process and requirements. The example:

- Suggests synchronizing device times.
- Uses NetFlow version 5.
- Uses the export of ingress data.

### Ensure Synchronized Device Date and Time

All of the devices exporting flow data should have their time synchronized. You can use, for example, the Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP). Consult the appropriate documentation before synchronizing clocks.

This example is applied to router R837, and:

- Uses Ethernet0 interface on the device for NTP.
- Uses the NIST Internet Time Service clock, 131.107.13.100, as the source of its time.
- Displays the resulting NTP associations.

To synchronize device times:

1) Check the time protocol used by the device:

```
R837#sh clock detail
10:32:35.757 UTC Wed Jun 16 2010
Time source is NTP
```

2) Synchronize the clock on the device:

```
ntp source Ethernet0
ntp server 131.107.13.100
R837#sh ntp association
address          ref     s   whe   pol   reac  delay   offset   dis
                 clock   t   n     l     h                      p
*~131.107.13.10  .ACTS.  1   53    256   377   150.2   9.81     5.2
0
* master (synced), # master (unsynced), + selected, - candidate, ~
configured
```

## Configuring the Export of Ingress Flow Export Data

When you want Entuity to manage flow data from a device you must first configure the device to export its ingress flow data to the flow collector. Entuity therefore receives flow data for inbound traffic on an interface. To determine an interface's outbound flows, you should view inbound data on the interface on the device attached to this interface (where you must also have enabled flow collection.)

Always refer to the appropriate device documentation before configuring the export of flow data.

You must enable flow collection on each interface on the device, for example:

```
router#configure terminal
R8321(config)#interface GigabitEthernet0/0
R8321(config-if)#ip flow ingress
R8321(config-if)#exit
```

This sample configuration is entered on a router to enable NetFlow version 5 on the GigabitEthernet 0/0 interface and export to the machine 10.44.1.81 on port 9996.

```
router#configure terminal
R8321(config)#interface GigabitEthernet0/0
R8321(config-if)#ip flow ingress
```

```
R8321(config-if)#exit
R8321(config)#ip flow-export destination 10.44.1.81 9996
R8321(config)#ip flow-export source GigabitEthernet0/0
R8321(config)#ip flow-export version 5
R8321(config)#ip flow-cache timeout active 1
R8321(config)#ip flow-cache timeout inactive 15
R8321(config)#snmp-server ifindex persist
```

where:

- *ip flow ingress* sets monitoring of inbound flows on the selected interface.
- *ip flow-export destination* is the IP address and port of the Entuity flow collector to which the flow data is exported.
- *ip flow-export source* is the IP address the Entuity flow collector uses to identify the source of the flow data.
- *ip flow-export version* is the NetFlow version the device uses to export the flow data. Entuity currently supports NetFlow versions 5, 6, 7 and 9.
- *ip flow-cache timeout active* configures the device to every minute export flow records to the Entuity flow collector. Valid values are between 1 and 60, however you should not amend this setting.
- *ip flow-cache timeout inactive* ensures that flows that have finished are periodically exported. The default value is 15 seconds. Valid values are in the range of 10 and 600.
- *snmp-server ifindex persist* maintains the ifIndex persistence on device reboot and hot plug-ins.

## Flexible NetFlow

Flexible NetFlow permits the export of flow data containing user configurable flow information, although you must always consider the type of flow data Entuity is configured to receive and process.

Always refer to the appropriate device documentation before configuring the export of flow data. This section provides an overview of 2 export methods.

There are two methods for configuring flexible flow data:

- Use the old style input method.

  You can specify on the device the destination of the Entuity server, transport, NetFlow version and also for it to export the predefined original-input and original-output records.

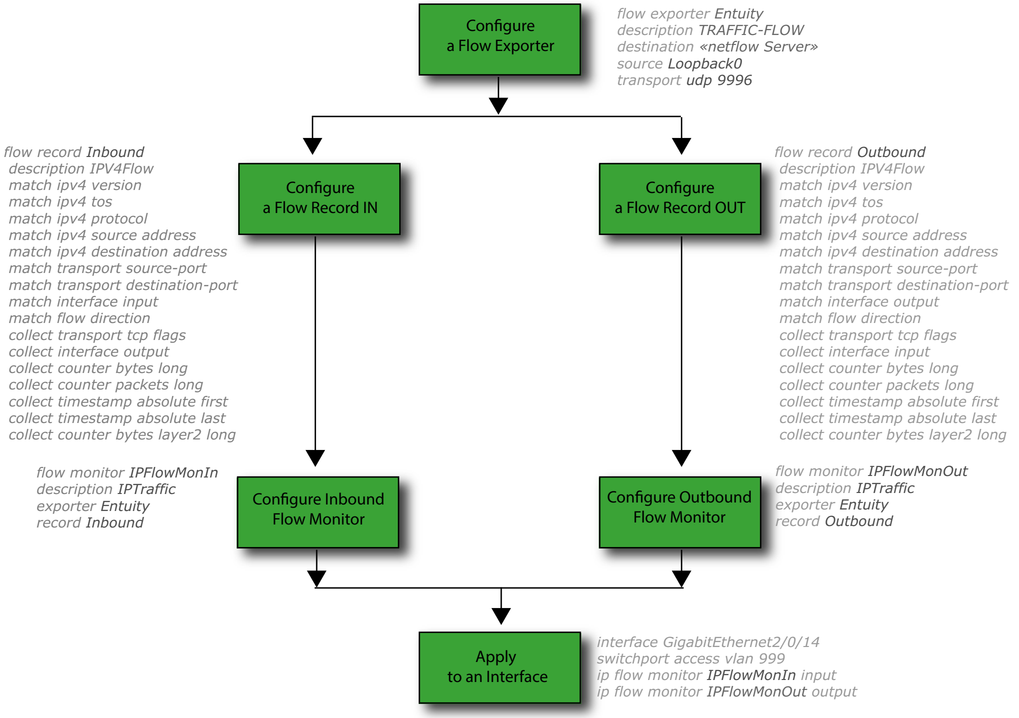
```
flow exporter EYE
  destination 10.44.1.213
  transport udp 9996
  source mgmt0
  version 9
```

```
    template data timeout 300
    option exporter-stats timeout 60
    option interface-table timeout 600
flow monitor OldStyleIPMonitoringIn
  record netflow ipv4 original-input
  exporter EYE
flow monitor OldStyleIPMonitoringOut
  record netflow ipv4 original-output
  exporter EYE
```

And then on each interface of interest enter:

```
       ip flow monitor OldStyleIPMonitoringIn input
       ip flow monitor OldStyleIPMonitoringOut output
```

- Explicitly specify the attributes that you want to export. (See *Figure 73 Example Flexible Flow*.)



```
flow exporter Entuity
description TRAFFIC-FLOW
destination «netflow Server»
source Loopback0
transport udp 9996
```

```
flow record Inbound
 description IPV4Flow
 match ipv4 version
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 match flow direction
 collect transport tcp flags
 collect interface output
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
 collect counter bytes layer2 long
```

```
flow record Outbound
 description IPV4Flow
 match ipv4 version
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface output
 match flow direction
 collect transport tcp flags
 collect interface input
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last
 collect counter bytes layer2 long
```

```
flow monitor IPFlowMonIn
description IPTraffic
exporter Entuity
record Inbound
```

```
flow monitor IPFlowMonOut
description IPTraffic
exporter Entuity
record Outbound
```

```
interface GigabitEthernet2/0/14
switchport access vlan 999
ip flow monitor IPFlowMonIn input
ip flow monitor IPFlowMonOut output
```

Figure 73 Example Flexible Flow

# Start and Stop Flow Collection

When you have configured devices to send data to a flow collector, configured the flow collector and assigned it to an Entuity server, the final step is to activate collection of the flow data for the device. Although flow data is associated with ports, you start and stop flow collection at the device level.

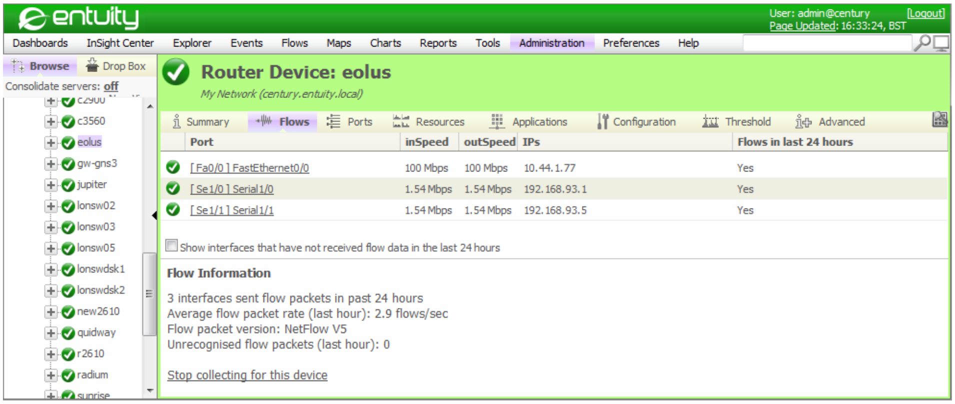
You can control flow collection from the:

- Device Flows summary page.
- Flow Inventory page.

## Managing Flow Collection on a Device

To start collecting device flow data:

1) From Explorer select the device and then click the Flows tab.
2) Click **Start collecting for this device**. This instructs the flow collector to start collecting flow data on this device. The hyperlink also changes to **Stop collecting for this device**, allowing you to stop collecting data.



Router Device: eolus

*My Network (century.entuity.local)*

| | Port | inSpeed | outSpeed | IPs | Flows in last 24 hours |
|---|---|---|---|---|---|
| ✓ | [ Fa0/0 ] FastEthernet0/0 | 100 Mbps | 100 Mbps | 10.44.1.77 | Yes |
| ✓ | [ Se1/0 ] Serial1/0 | 1.54 Mbps | 1.54 Mbps | 192.168.93.1 | Yes |
| ✓ | [ Se1/1 ] Serial1/1 | 1.54 Mbps | 1.54 Mbps | 192.168.93.5 | Yes |

☐ Show interfaces that have not received flow data in the last 24 hours

**Flow Information**

3 interfaces sent flow packets in past 24 hours
Average flow packet rate (last hour): 2.9 flows/sec
Flow packet version: NetFlow V5
Unrecognised flow packets (last hour): 0

Stop collecting for this device

Figure 74 Activate Device Flow Collection

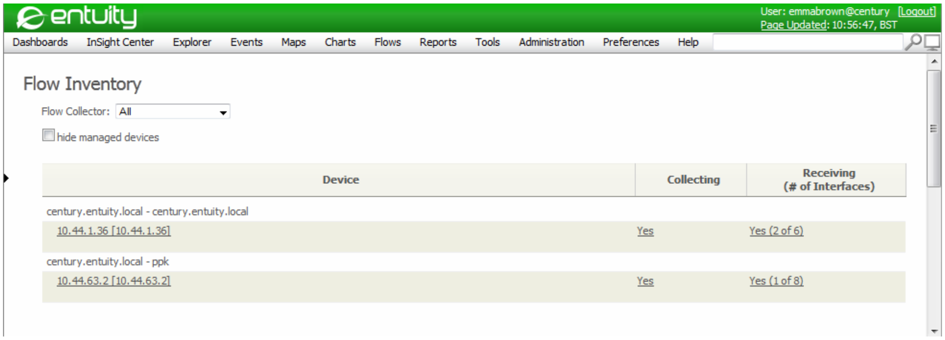
## Managing Flow Collection Across Devices

From the Flow Inventory page you can view a summary of flow collection by device. There are options to control flow collection and to access the Flow Inventory Details page.

When using IFA Premium in a multi-server environment devices are grouped by the receiving Entuity server.

To view the state of flow collection:

1) Click **Administration** > **Flow Collector** > **Flow Inventory**.



Flow Inventory

Flow Collector: All

□ hide managed devices

| Device | Collecting | Receiving (# of Interfaces) |
|---|---|---|
| century.entuity.local - century.entuity.local | | |
| 10.44.1.36 [10.44.1.36] | Yes | Yes (2 of 6) |
| century.entuity.local - ppk | | |
| 10.44.63.2 [10.44.63.2] | Yes | Yes (1 of 8) |

Figure 75 Flow Inventory

| Attribute | Description |
|---|---|
| Entuity Servers | Indicates the Entuity server managing device flow collection and the server receiving, collecting and processing that data. |
| *Device* | Device IP address or resolved hostname with interfaces configured to send flow data to the Entuity server. When the device is not managed by that server name is Unknown. |
| *Collection* | When set to Yes, Entuity collects flow data from the device, when set to No data is not collected.<br>You can click on the collection indicator to open the Flow Collector Inventory through which you control flow collection. |
| *Receiving* | Indicates whether the device is sending flow data to the server and from how many of the known interfaces.<br>You can click on the receiving indicator to view the Flow Inventory Details page. |

Table 16 Flow Inventory

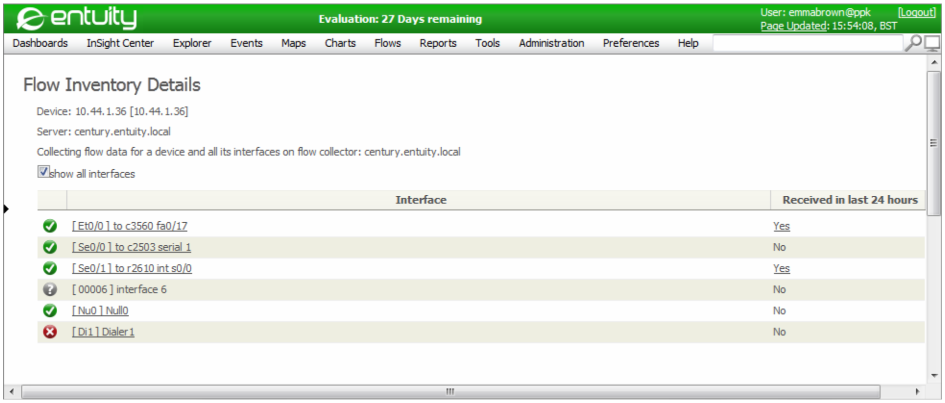
## State of Flow Collection on all Ports on a Device

When you want to view in detail the flow status of a selected device access the Flow Inventory Details page.

To view the state of flow collection on all ports on a device:

1) Click **Administration > Flow Collector > Flow Inventory**.

2) Click on its Receiving hyperlink.



Flow Inventory Details

Device: 10.44.1.36 [10.44.1.36]

Server: century.entuity.local

Collecting flow data for a device and all its interfaces on flow collector: century.entuity.local

☑ show all interfaces

| | Interface | Received in last 24 hours |
|---|---|---|
| ✓ | [ Et0/0 ] to c3560 fa0/17 | Yes |
| ✓ | [ Se0/0 ] to c2503 serial 1 | No |
| ✓ | [ Se0/1 ] to r2610 int s0/0 | Yes |
| ? | [ 00006 ] interface 6 | No |
| ✓ | [ Nu0 ] Null0 | No |
| ✕ | [ Di1 ] Dialer1 | No |

Figure 76 Flow Inventory Details

| Attribute | Description |
|---|---|
| *Device* | Device IP address or resolved hostname with interfaces configured to send flow data to the Entuity server. When the device is not managed by that server name is Unknown. |
| Server | Entuity server receiving flow data. |
| *Collector* | Entuity server collecting flow data. |
| Show all interfaces | When selected Entuity displays all ports on the device, when not selected Entuity only displays those ports sending flow data. |
| *Interface* | Name and state of the port, with a hyperlink to the Port Summary page. |
| *Received in last 24 hours* | Indicates whether the interface is sending flow data to the server.<br>You can click on the receiving indicator to view the port’s Flows page. |

Table 17 Flow Inventory Details

## Create Your Own Flow Breakdowns

With IFA Premium you can define your own flow breakdowns. You can:

- Create new custom data types, for example to track flows by location, department, customer.
- Specify group members in terms of the available raw data types, for example UK, US, Dev, Sales, Customer A, Customer B.

  This example is synonymous with custom groups and group based analysis.

Custom data types and groups are defined through a configuration file, *entuity_home*/`etc/flowUserDefGroups.xml`. You must create your own XML file and then install it to the Entuity server managing flow collection. (For an example file see the *Entuity System Administrator Reference Manual*.)

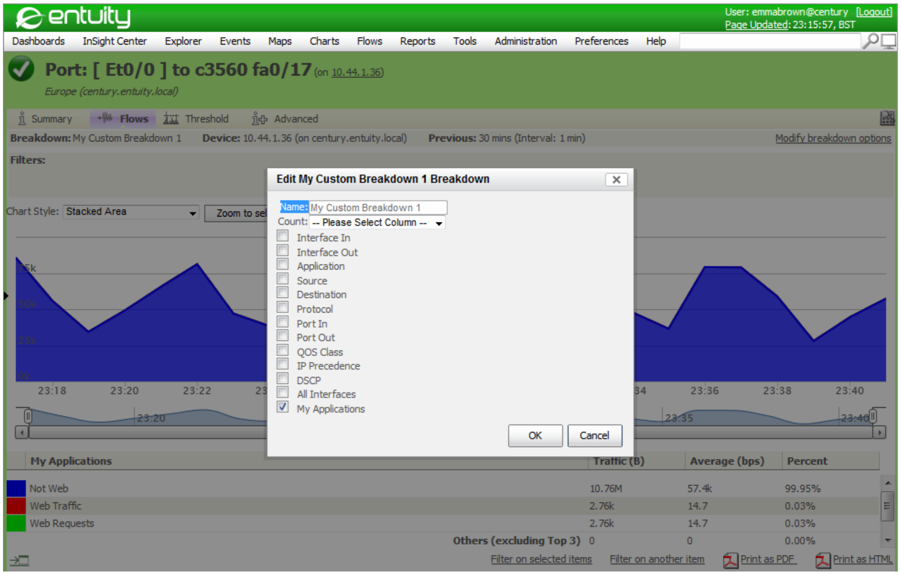
### Creating a Chart using a Custom Breakdown

To create charts using custom data types:

1) Ensure the data type and group is loaded onto the Entuity server collecting the flow data.

   Entuity requires the new configuration is included to *entuity_home*`/etc/flowUserDefGroups.xml`.

2) Open the Flows page of the interface against which you want to generate the report.
3) From the Flow Analysis Options dialog click **Edit**.
4) Select the new breakdown, it is appended to the list of standard breakdowns.



Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)
*Europe (century.entuity.local)*

**Breakdown:** My Custom Breakdown 1 **Device:** 10.44.1.36 (on century.entuity.local) **Previous:** 30 mins (Interval: 1 min)

Chart Style: Stacked Area

**Edit My Custom Breakdown 1 Breakdown**

Name: My Custom Breakdown 1
Count: -- Please Select Column --

- □ Interface In
- □ Interface Out
- □ Application
- □ Source
- □ Destination
- □ Protocol
- □ Port In
- □ Port Out
- □ QOS Class
- □ IP Precedence
- □ DSCP
- □ All Interfaces
- ☑ My Applications

| | My Applications | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|
| 🟦 | Not Web | 10.76M | 57.4k | 99.95% |
| 🟥 | Web Traffic | 2.76k | 14.7 | 0.03% |
| 🟩 | Web Requests | 2.76k | 14.7 | 0.03% |
| | **Others (excluding Top 3)** | 0 | 0 | 0.00% |

Figure 77 Custom Flow Data Types

## Configuring Filters to Exclude Flow Data

Exclusion filters allow you to exclude flow data from collection by the Entuity server based on the flow source and destination IP addresses and/or source and destination ports. You can enter exact values, or use wild cards to create more extensive filters.

You define exclusion filters through the configuration file *entuity_home*`\etc\flow-exclusions.properties`. An example configuration definition is included in *entuity_home*`\etc\flow-exclusions-template.properties`. You should specify your exclusion filters in *entuity_home*`\etc\flow-exclusions.properties` on each server acting as a flow collector.

You specify exclusion filters:

- On the endpoint, so flows outgoing from or incoming to the specified endpoint are filtered out.

  ```
  IPAddressPattern : PortPattern
  ```

- That are unidirectional, so flows which originate from the specified source endpoint and end at the specified destination endpoint are filtered out.

  ```
  SrcIPAddressPattern : SrcPortPattern > DstIPAddressPattern : DstPort-
  Pattern
  ```

- That are bidirectional, so flows in both directions between two endpoints are filtered out:

  ```
  IPAddressPattern1 : PortPattern1 = IPAddressPattern2 : PortPattern2
  ```

You can check the number of excluded flows and number of exclusion rules through the Flow Collector Health page.

## Exclusion Filter Patterns

An *IPAddressPattern* can be one or more IP address or range of IP addresses. These are examples of valid patterns:

- Matches a single IP address.

  ```
  10.44.1.101
  ```

- Matches all IP addresses within the range.

  ```
  10.44.1/24
  ```

- An asterisk matches all IP addresses.

  ```
  *
  ```

A *PortPattern* can be one or more port numbers, or range of port numbers. These are examples of valid patterns.

- Matches a single port:

  ```
  3066
  ```

- Matches all ports within the range:

  ```
  2048-2099
  ```

- An asterisk matches all ports, equivalent to 0 to 65535:

  ```
  *
  ```

These are example exclusion filters:

- Filter all flows going from or to applications on port 3306 on the host10.44.1.101.

  ```
  10.44.1.101:3306
  ```

- Filter all flows going from or to applications (ports 3306, 1433) on any of the listed hosts.

  ```
  10.44.1.101, 10.44.1.102 : 1433, 3306
  ```

- Filter all flows going from host 10.44.1.101 to host 10.44.1.10

  ```
  10.44.1.101:* > 10.44.1.10:*
  ```

- Filter all flows between host 10.44.1.101 and host 10.44.1.10

  ```
  10.44.1.101:* = 10.44.1.10:*
  ```

## Mapping Applications to Protocol Flow Data

One of the critical operations performed by Entuity IFA is the removal of ephemeral port records from the database. When a connection is made from a client to a server the TCP/ UDP port on the server end of the connection determines the application in use. The port number allocated to the client end of the connection is referred to as an ephemeral port and has no meaning. Entuity determines which end of a connection is the server end so that its port number can be used to identify the application, by:

1) Considering ports < 1024 as having the highest priority, regardless of whether the other port has an Entuity application port mapping.

   Ports below 1024 are reserved port numbers, and so only one port (either the source or the destination port) should be in the range.

2) Where both ports are greater than 1023, or, more unlikely, both are below 1024 Entuity determines which port to use as the server port by using its port mapping priority configuration.

Entuity identifies application data within the flow data by mapping TCP and UDP port numbers to application names. As an application may use multiple port numbers, you can map multiple ports to an application name. When a port-protocol combination is mapped to two applications, Entuity resolves this conflict by using the application with the highest mapping priority.

Entuity automatically maps protocols other than TCP and UDP to the protocol name, this mapping takes the most generic name, for example all ICMP traffic maps to ICMP and not to ICMP type, ICMP code. Entuity includes a list of the mappings which you can amend and add to.

IFA application to port mapping is not integrated with the existing list of applications and ports used in application monitoring.

### Viewing Application Port Mappings

By default the Application Port Mappings table is sorted by priority in ascending order. You can use the column headers to sort the table by other fields. The table shows 500 port mappings at a time with navigation links at the foot of the page.

Application Port Mappings includes two check box settings:

- Consolidate port mappings, when:
  - Selected, the table displays one entry per application port mapping in the table. All ports assigned to the application are visible in a comma separated list in the ports column.
  - Not Selected, an application with multiple ports assigned has an entry for each port.

- Hide reserved port mappings, when:
  - Selected, reserved port mappings not displayed.
  - Not Selected, reserved port mappings are displayed.

  Reserved port mappings are applications that have ports assigned with a value of 1023 or less. All reserved port mappings have a priority of 0.

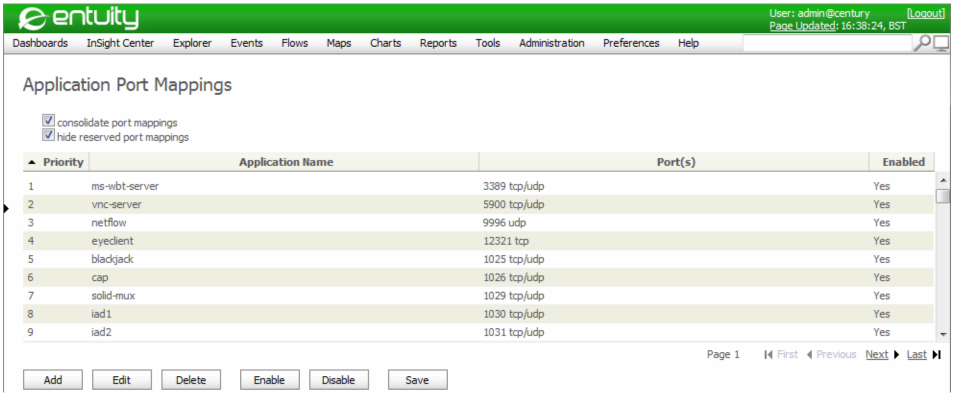
| Attribute | Description |
|---|---|
| *Priority* | Priority of the mapping. The lower the number the higher the priority. |
| *Application Name* | Name of the mapped application. |
| *Port(s)* | Ports associated with this application. |
| *Enabled* | Indicates whether the mapping is active or inactive. |

Table 18 Application Port Mapping

To view the application port mappings:

1) Click **Administration > Flow Collector > Application Port Mappings**.

   Entuity displays the Application Port Mappings page. Where you have more than one polling server Entuity displays a table of flow collectors, with hyperlinks to retrieve the individual server's application port mappings configuration.



Application Port Mappings

☑ consolidate port mappings
☑ hide reserved port mappings

| Priority | Application Name | Port(s) | Enabled |
|---|---|---|---|
| 1 | ms-wbt-server | 3389 tcp/udp | Yes |
| 2 | vnc-server | 5900 tcp/udp | Yes |
| 3 | netflow | 9996 udp | Yes |
| 4 | eyeclient | 12321 tcp | Yes |
| 5 | blackjack | 1025 tcp/udp | Yes |
| 6 | cap | 1026 tcp/udp | Yes |
| 7 | solid-mux | 1029 tcp/udp | Yes |
| 8 | iad1 | 1030 tcp/udp | Yes |
| 9 | iad2 | 1031 tcp/udp | Yes |

Figure 78 Application Port Mappings

## Editing Application Port Mappings

From the Application Port Mappings page you can click:

- **consolidate port mappings** to group ports mapped to the same application on the same row.
- **hide reserved port mappings** to only display ports available for amendment.
- **Add** for Entuity to display the Add Application Port Mapping dialog through which you can add a mapping.

- **Edit** for Entuity to display the Edit Application Port Mapping dialog through which you can amend existing mappings, by adding ports, removing ports, changing priority levels.
- **Delete** to delete the highlighted mapping from Entuity. Entuity displays a delete confirmation message before deleting the mapping.
- **Enable** or **Disable** to activate, or deactivate, the highlighted application port mapping.

The Edit Application Port Mapping and Add Application Port Mapping dialogs contain almost the same attributes and options:

| Attribute | Description |
|---|---|
| *Application Name* | Name of the application displayed in Entuity. Once created it cannot be amended, it is display only in the Edit dialog. |
| *Ports* | lists the ports associated with the application mapping. You can use:<br>■ **Add**, to open the Add Port dialog, through which you can enter a port number and specify the applicable protocol, i.e. TCP, UDP or both.<br>■ **Remove**, to delete the highlighted port from the mapping. |
| *Priority* | to set the priority level of the mapping. Entuity prevents you from assigning a priority level that is already assigned to another mapping. |

Table 19 Set Application Port Mapping

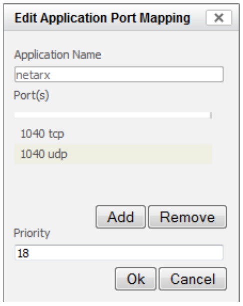
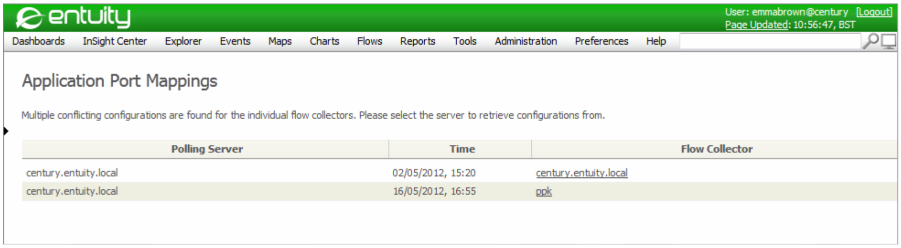


Figure 79 Edit Application Port Mappings

## Multiple Flow Collectors

Where a server is managing more than one flow collector, you can view and amend the mappings for each collector from the Entuity server:

1) Click **Administration** > **Flow Collector** > **Application Port Mappings**. Entuity displays a page from which you can view for each flow collector the last edit times of their application port mappings.



Application Port Mappings

Multiple conflicting configurations are found for the individual flow collectors. Please select the server to retrieve configurations from.

| Polling Server | Time | Flow Collector |
|---|---|---|
| century.entuity.local | 02/05/2012, 15:20 | century.entuity.local |
| century.entuity.local | 16/05/2012, 16:55 | ppk |

Figure 80 Multi-server Application Port Mappings

2) Select the flow collector for which you want to amend the mappings. Entuity displays the Application Port Mappings page.

## Viewing Flow Inventory

From the Flow Inventory page you can:

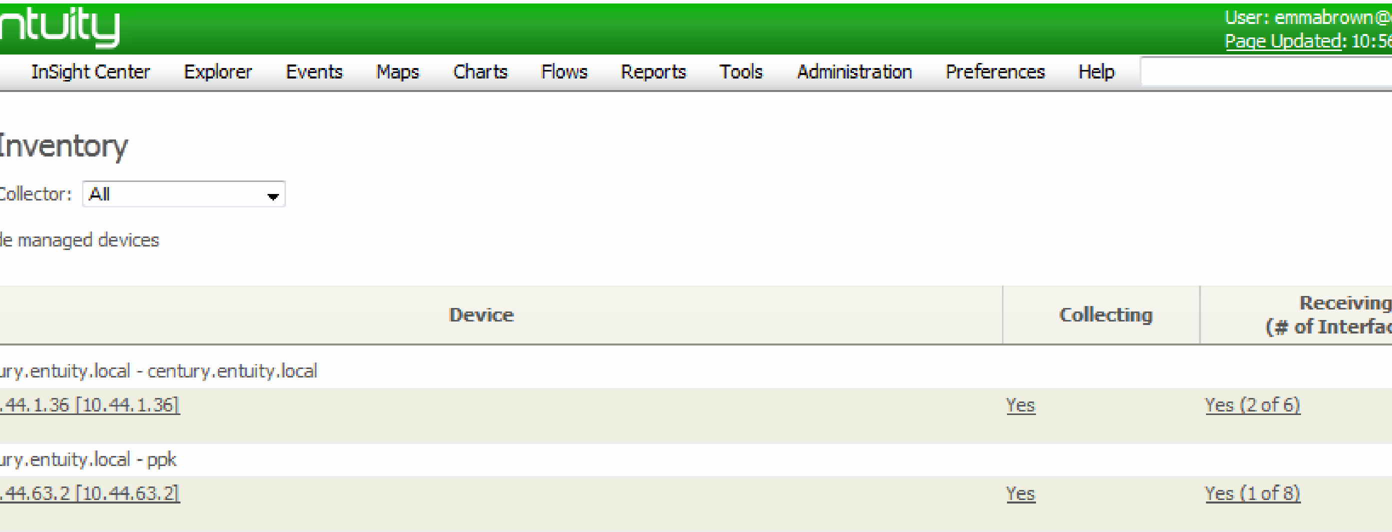
- View the flow collectors assigned to the server.
- View the devices associated with each flow collector.
- Start and stop flow data collection on devices.
- View the status of interfaces on each device.
- Drill down from the hyperlink on the:
  - Device to display the inventory details of the device in Explorer.
  - Interface to display the device’s interfaces on the Flow Inventory page.

To view flow inventory:

1) Ensure the flow collector is running.

2) Login to the Entuity polling server.

3) Select **Administration** > **Flow Collector** > **Flow Inventory**.

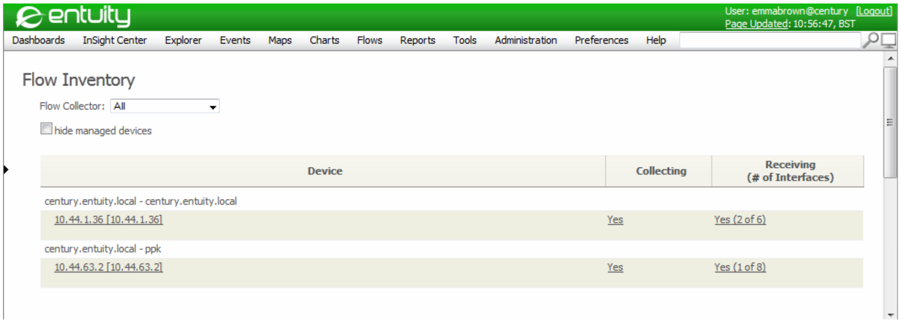


Inventory

Collector: All

le managed devices

| Device | Collecting | Receiving (# of Interfac |
|---|---|---|
| ury.entuity.local - century.entuity.local | | |
| .44.1.36 [10.44.1.36] | Yes | Yes (2 of 6) |
| ury.entuity.local - ppk | | |
| .44.63.2 [10.44.63.2] | Yes | Yes (1 of 8) |



Flow Inventory

Flow Collector: All

□ hide managed devices

| Device | Collecting | Receiving (# of Interfaces) |
|---|---|---|
| century.entuity.local - century.entuity.local | | |
| 10.44.1.36 [10.44.1.36] | Yes | Yes (2 of 6) |
| century.entuity.local - ppk | | |
| 10.44.63.2 [10.44.63.2] | Yes | Yes (1 of 8) |

Figure 81 Flow Inventory

| Attribute | Description |
|---|---|
| *Hide Managed Devices* | Select when wanting to identify devices that are collecting or sending flow data, but are not in the inventory. |
| This table groups the devices by Entuity server and flow collector. | |
| *Entuity Server - Flow Collector* | Name of the Entuity server managing the device, and then the name of the Flow Collector to which the device sends its flow data.<br>On a Dedicated Flow Collector, the flow collector name is repeated, as a flow collector cannot identify the server managing the device. |

Table 20 Flow Inventory Data

| Attribute | Description |
|---|---|
| *Device* | The IP address or resolved name of the device exporting the data flow records. These records may contain many IP addresses, making host name resolution a potentially resource intensive process. Entuity uses a cache to quicken the process, when the name cannot be resolved through the cache then resolution request is queued.<br>When you select the hyperlink Entuity displays the device details in its Explorer. |
| *Collecting* | Indicates whether the flow server is collecting data from interfaces on the device.<br>When you select the hyperlink Entuity displays a pop-up dialog showing the current status of the device. You can also start and stop flow collection on the device. |
| *Received in last 24 hours (# of interfaces)* | Indicates whether the flow collector is currently receiving flow data on any interfaces on the device, the number of interfaces on the device for which it has received flow data in the previous twenty-four hours, and also the total number of interfaces.<br>When you select the hyperlink Entuity re-displays the Flow Inventory page, but with a breakdown of the interfaces on the device. |

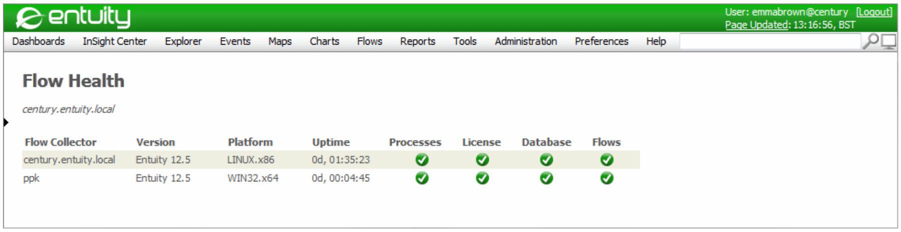
Table 20 Flow Inventory Data

## Checking on Flow Collector Health

You can check flow collector health using the Flow Health page and the Entuity Server Health report.

There are two forms of the flow health page:

- A summary Flow Health page which Entuity displays when the server has at least one assigned remote flow collector. You can select the flow status icon to drill down to the Flow Collector Health page.
- Flow Collector Health page provides detailed statistics on the flow collectors flow data performance and data loss.



Flow Health

*century.entuity.local*

| Flow Collector | Version | Platform | Uptime | Processes | License | Database | Flows |
|---|---|---|---|---|---|---|---|
| century.entuity.local | Entuity 12.5 | LINUX.x86 | 0d, 01:35:23 | ✓ | ✓ | ✓ | ✓ |
| ppk | Entuity 12.5 | WIN32.x64 | 0d, 00:04:45 | ✓ | ✓ | ✓ | ✓ |

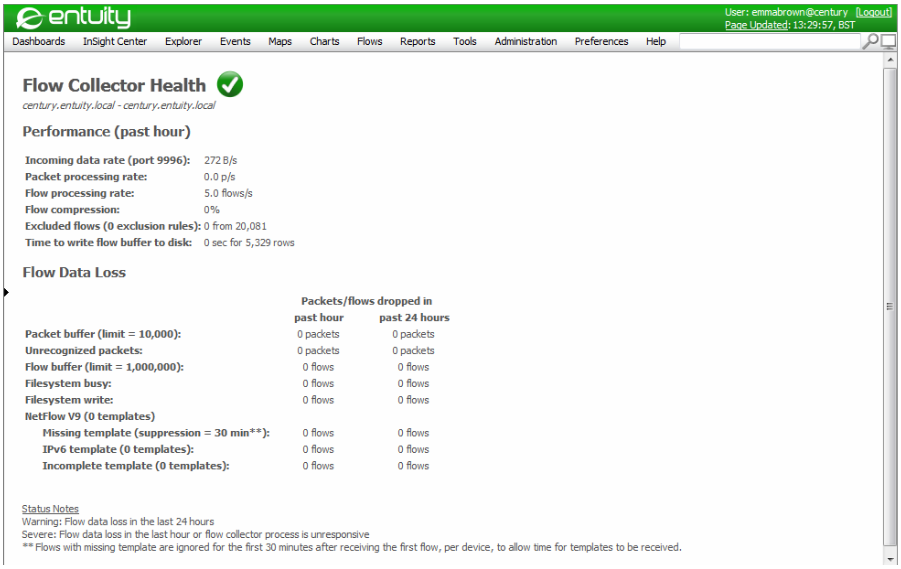
Figure 82 Multi-Server Flow Health

To access the Entuity Flow Collector Health page:

1) Click **Administration > Entuity Health > Flow Health**. Entuity displays the:

   - Flow Collector Health page.

- Flow Health page, when the server includes remote assigned flow collectors. You can select the flow icon to display the Flow Collector Health page.



**Flow Collector Health** ✓

*century.entuity.local - century.entuity.local*

**Performance (past hour)**

| | |
|---|---|
| **Incoming data rate (port 9996):** | 272 B/s |
| **Packet processing rate:** | 0.0 p/s |
| **Flow processing rate:** | 5.0 flows/s |
| **Flow compression:** | 0% |
| **Excluded flows (0 exclusion rules):** | 0 from 20,081 |
| **Time to write flow buffer to disk:** | 0 sec for 5,329 rows |

**Flow Data Loss**

| | **Packets/flows dropped in** | |
|---|---|---|
| | **past hour** | **past 24 hours** |
| **Packet buffer (limit = 10,000):** | 0 packets | 0 packets |
| **Unrecognized packets:** | 0 packets | 0 packets |
| **Flow buffer (limit = 1,000,000):** | 0 flows | 0 flows |
| **Filesystem busy:** | 0 flows | 0 flows |
| **Filesystem write:** | 0 flows | 0 flows |
| **NetFlow V9 (0 templates)** | | |
| **Missing template (suppression = 30 min**):** | 0 flows | 0 flows |
| **IPv6 template (0 templates):** | 0 flows | 0 flows |
| **Incomplete template (0 templates):** | 0 flows | 0 flows |

Status Notes
Warning: Flow data loss in the last 24 hours
Severe: Flow data loss in the last hour or flow collector process is unresponsive
** Flows with missing template are ignored for the first 30 minutes after receiving the first flow, per device, to allow time for templates to be received.

Figure 83 Flow Collector Health

These health metrics are intended for Entuity representatives, or advanced users, investigating performance problems or data loss on flow collectors.

| Attribute | Description |
|---|---|
| *Flow Collector Health Status* | Flow collector health status level is:<br>- **Severe** when there was data loss in the past hour, unless the data loss is NetFlow v9 or IPFIX related or the flow collector process could not be contacted.<br>- **Warning** when the data loss was NetFlow v9 or IPFIX related or occurred between one and twenty-four hours ago.<br>- **OK** when there has been no data loss over the previous twenty-four hours. |
| Performance over the previous hour | |
| *Incoming data rate* | Number of bytes per second received on the flow collector port. |
| *Packet processing rate* | Indicates the rate of the incoming export packets (each packet may contain multiple flow records). |
| *Flow processing rate* | Indicates the rate of the flows the flow collector processes. |
| *Flow compression* | Indicates the degree of compression of the original flow data in a five minute interval. The greater the number, the better the compression. |

Table 21 Flow Collector Health

| Attribute | Description |
|---|---|
| *Excluded flows*<br>*(0 exclusion rules)* | The number of flows, which were dropped due to flow collection not being enabled on the device or due to the exclusion rules. The current number of exclusion rules is shown in parenthesis.<br>Exclusion rules are specified in *entuity_home*`\etc\flow-exclusions.properties`. |
| *Time to write flow buffer to disk* | The time spent over a five minute period performing database writes. Also specified are the number of records inserted. |
| Flow Data Loss | |
| *Packet buffer*<br>*(limit = 1,000)* | The number of packets dropped due to the front packet buffer being full (the size of the buffer is specified in parenthesis). Losses indicate the flow collector process is not fast enough to process incoming packets:<br>■ Check CPU usage. Adjust greedy processes, or you may have to upgrade hardware.<br>■ Increase packet_queue_limit, although this also increases the flow collector's memory usage.<br>■ Reduce the load on the flow collector, by switching off the export of flow packets on the device. |
| *Unrecognized Packets* | The flow collector receives packets it cannot parse. A device may be sending flow packets using an unsupported NetFlow version, or packet corruption is occurring on the network. |
| *Flow buffer (5 min) is full*<br>*(limit = 1,000,000)* | Flow collector maintains two buffers for flow compression (5-min and 1-hour). If a buffer gets full, then flows are dropped to avoid memory-related errors. Buffer sizes are specified with `partition1_maxCount` and `partition2_maxCount properties`. You can:<br>■ Reduce the load on the flow collector, for example disable flow collection for some devices, or direct flows to another flow collector<br>■ Increase the buffer limits, although this also increases the memory consumption of the flow collector.<br>You can set flow collector memory limits in *entuity_home*`/etc/startup_`*O/S*`_site_specific.cfg` using `-Xmx`, by default it is set to `-Xmx512m`. |
| *Flow buffer (1 hour) is full*<br>*(limit = 3,000,000)* | |
| *File system busy* | If a flow collector is not fast enough to flush the buffers and make them available for incoming flows, then flows are dropped. This can happen when the database write operation takes too much time.<br>You should reduce the load on the flow collector, for example by changing on some devices their destination flow collector. |
| *File system write* | There is a limit on the number of flows that can be stored in the database. Once the limit is reached, new flows cannot be inserted and are dropped. You can:<br>■ Reduce the load on the flow collector, e.g. direct some device flow data to another collector, resulting in a lower number of flows<br>■ Increase table size limit (`max_heap_table_size` property in `my_eye.cnf`). This will increase the UI response times. |

Table 21 Flow Collector Health

| Attribute | Description |
|---|---|
| *NetFlow V9*<br>*(0 templates)* | Indicates the number of unique NetFlow v9 templates received. |
| *Missing template*<br>*(suppression = 30 min)* | Number of flows lost due to template unavailability. Flows with a missing template are ignored for the first thirty minutes after receiving the first flow, per device, to allow time for templates to be received. |
| *IPv6 template*<br>*(0 templates)* | Number of flows lost due to non-support for IPv6, flows with IPv6 addresses are dropped. |
| *Incomplete template*<br>*(0 templates)* | Number of flows lost due to the template not being sufficient enough to recognize a flow correctly. |

Table 21 Flow Collector Health

# 26 View and Report on Flow Data

Entuity administrators, and users who have the Flow Inspection permission, can view flow data against devices and interfaces through Explorer. They can also create charts to track data flow.

You can create interactive charts for interfaces collecting flow data, updated in realtime. These charts are highly configurable, allowing control over time period, chart style, type of flow data, i.e. interfaces, protocols, applications, talkers, listeners, QoS classes and Ports. Also detailed visibility down to individual UDP/TCP port simplifies identification of any unmapped applications consuming bandwidth. You can save these breakdowns to Custom Dashboards.

## Identify Flow Inventory on the Server

Entuity IFA integrates flow-based performance data in the Entuity web UI alongside Entuity's traditional elemental performance metrics. Through Explorer you can view and access configuration of flow data at the device and port level.

## Identify Flow Status on a Device

The Device Summary page provides a summary of the selected device's inventory and performance with links to more detailed pages. The Flow Summary tab indicates the state of flow collection on the device.

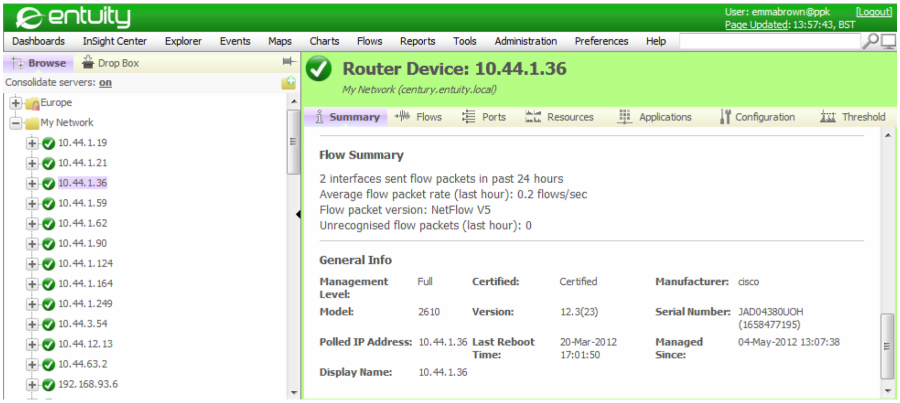
When you select the Flows tab, Entuity displays the Flow Information page which:

- Displays the flow information from the Summary page.
- Allows system administrators to start and stop flow collection on the device.
- Lists the ports on the device, including their flow status. You can limit the displayed ports to those with flow enabled. There are also hyperlinks to the port summary page.

To view device flow summary:

1) Click **Explorer**.

2) Use the Explorer pane to select the device.


entuity
User: emmabrown@ppk [Logout]
Page Updated: 13:57:43, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Preferences Help
Browse Drop Box
Consolidate servers: on
Europe
My Network
10.44.1.19
10.44.1.21
10.44.1.36
10.44.1.59
10.44.1.62
10.44.1.90
10.44.1.124
10.44.1.164
10.44.1.249
10.44.3.54
10.44.12.13
10.44.63.2
192.168.93.6
Summary Flows Ports Resources Applications Configuration Threshold

**Router Device: 10.44.1.36**

*My Network (century.entuity.local)*

**Flow Summary**

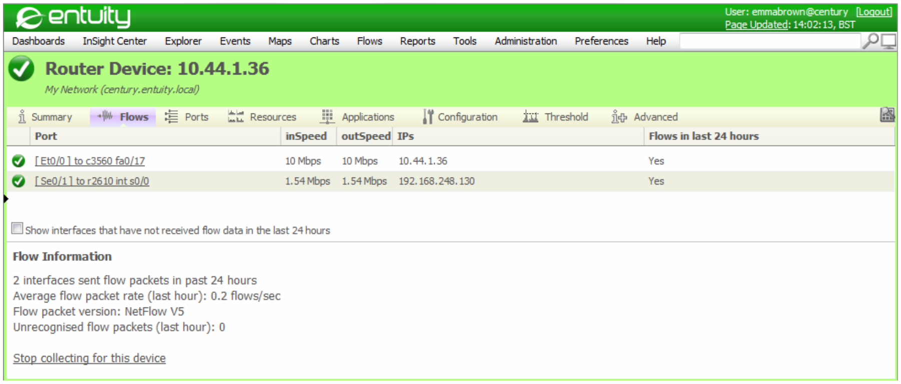
2 interfaces sent flow packets in past 24 hours
Average flow packet rate (last hour): 0.2 flows/sec
Flow packet version: NetFlow V5
Unrecognised flow packets (last hour): 0

**General Info**

| | | | | | |
|---|---|---|---|---|---|
| **Management Level:** | Full | **Certified:** | Certified | **Manufacturer:** | cisco |
| **Model:** | 2610 | **Version:** | 12.3(23) | **Serial Number:** | JAD04380UOH (1658477195) |
| **Polled IP Address:** | 10.44.1.36 | **Last Reboot Time:** | 20-Mar-2012 17:01:50 | **Managed Since:** | 04-May-2012 13:07:38 |
| **Display Name:** | 10.44.1.36 | | | | |

Figure 84 Flow Summary General Details

3) Click the Flows tab to view a detailed breakdown of flow information.


entuity
User: emmabrown@century [Logout]
Page Updated: 14:02:13, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Preferences Help
Summary Flows Ports Resources Applications Configuration Threshold Advanced

**Router Device: 10.44.1.36**

*My Network (century.entuity.local)*

| | Port | inSpeed | outSpeed | IPs | Flows in last 24 hours |
|---|---|---|---|---|---|
| ✓ | [Et0/0] to c3560 fa0/17 | 10 Mbps | 10 Mbps | 10.44.1.36 | Yes |
| ✓ | [Se0/1] to r2610 int s0/0 | 1.54 Mbps | 1.54 Mbps | 192.168.248.130 | Yes |

□ Show interfaces that have not received flow data in the last 24 hours

**Flow Information**

2 interfaces sent flow packets in past 24 hours
Average flow packet rate (last hour): 0.2 flows/sec
Flow packet version: NetFlow V5
Unrecognised flow packets (last hour): 0

Stop collecting for this device

Figure 85 Device Flows Details in Explorer

## Device Flows Attribute

| Attribute | Description |
|---|---|
| *Flow Information* | Provides an overview of flow data collected on the device over the previous twenty-four hours, including:<br>- Flow packet version<br>- Number of interfaces sending data<br>- Average flow packet rate over the last hour<br>- Unrecognized flow packets. |
| *Control Flow Collection* | System administrators and users with the Flow Inspection permission have the option of starting and stopping flow collection on the device. |

Table 22 Device Flows Page

| Attribute | Description |
|---|---|
| *Ports* | By default Entuity only lists the ports returning flow data over the last twenty-four hours, you can view all ports by enabling the check box. For each port Entuity displays name, speed, associated IPs and flow status. There are also hyperlinks to the port summary page. |

Table 22 Device Flows Page

# Access Port Flow Data

The Port Summary page is accessible through Explorer and provides a summary of flow status, event status, key metrics and general information on the port. The Flow Summary section includes four charts:

- Top 5 Applications
- Top 5 Talkers
- Top 5 Listeners
- Top 5 QoS Classes.

When you click on a:

- Chart Entuity opens the Flow Analysis page using that breakdown. For example, select the Top 5 Applications chart to display the Flow Analysis page with the application breakdown for the interface.
- Data set in a chart Entuity opens the Flow Analysis page using that breakdown and filter. For example, select an application in the Top 5 Applications chart to display the Flow Analysis page for the interface with an application filter applied.

IFA Premium includes an additional chart for Top Conversations.

You can also select the port Flows tab for Entuity to display the port’s Flow Analysis page, through which you can configure charts to print to PDF files, to save as Flow Analysis HTML reports, or add to a custom dashboard. (See *Creating Flow Dashboards*.)

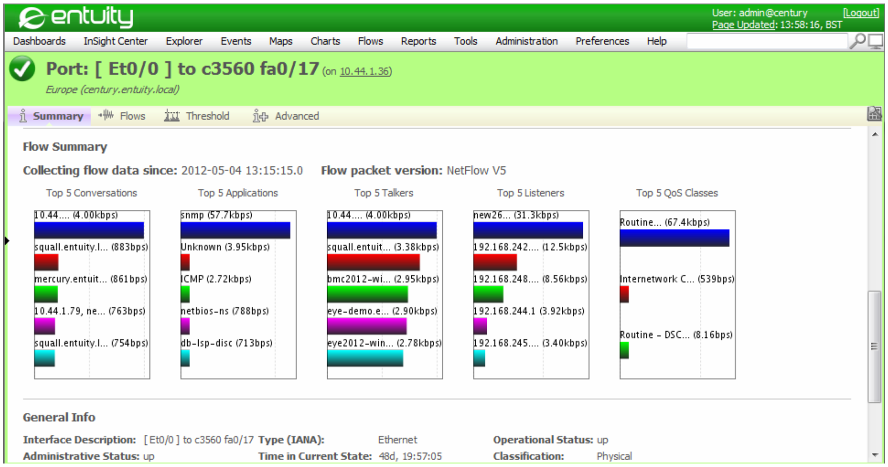
## Viewing Port Flow Data

To view a summary of a port’s flow performance:

1) Click **Explorer**.

2) Use the Explorer pane to select the required interface.

   Entuity displays the Port Summary page.



Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)

Europe (century.entuity.local)

Flow Summary

Collecting flow data since: 2012-05-04 13:15:15.0 Flow packet version: NetFlow V5

General Info

Interface Description: [ Et0/0 ] to c3560 fa0/17
Type (IANA): Ethernet
Operational Status: up
Administrative Status: up
Time in Current State: 48d, 19:57:05
Classification: Physical

Figure 86 IFA Premium Flow Summary Interface

## Flow Summary Attributes

| Attribute | Description |
|---|---|
| *Collecting Flow Data Since* | The date and time the Entuity flow collector started collecting. |
| *Flow Packet Version* | The name and version of the flow data protocol, e.g. NetFlow5. |
| *Top Applications* | The top *n* applications on the interface, as derived by measuring application traffic flow in bits per second (bps). When you click on a chart Entuity opens the Flow Analysis page for the interface with the application filter applied. |
| *Top Talkers* | The top *n* talking hosts on the interface, measured as outbound traffic in bits per second (bps). When you click on a chart Entuity opens the Flow Analysis page for the interface with the Host Outbound filter applied. |
| *Top Listeners* | The top *n* listening hosts on the interface, measured as inbound traffic in bits per second (bps). When you click on a chart Entuity opens the Flow Analysis page for the interface with the Host Inbound filter applied. |
| *Top QoS Classes* | The top *n* QoS classes on the interface, as derived by measuring QoS class traffic flow in bits per second (bps). When you click on a chart Entuity opens the Flow Analysis page for the interface with the QoS Classes filter applied. |
| Top Conversations | Breakdown by conversation is only available with Integrated Flow Analysis Premium. Entuity considers a conversation as flow data from both the source and destination IP address. |

Table 23 Flow Summary on the Port Summary Page

# Flow Breakdown Categories

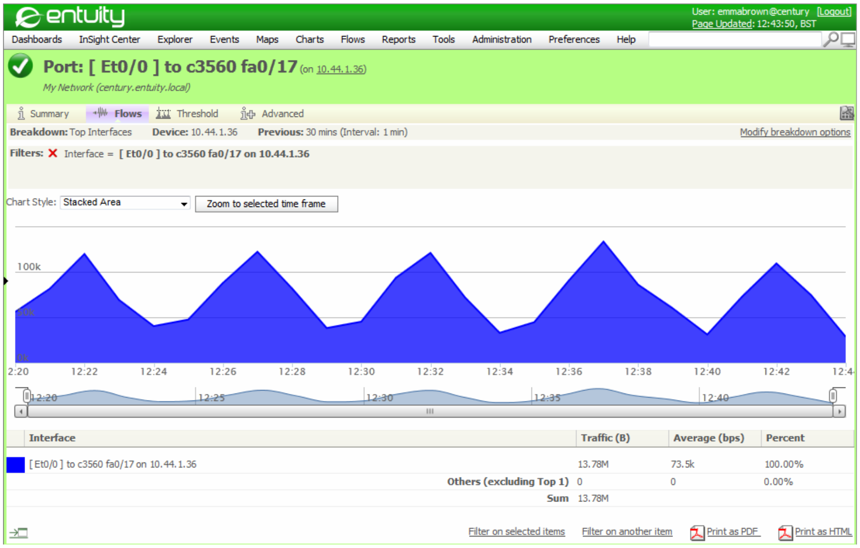
## Interfaces Breakdown

The Top Interfaces Flow Analysis chart graphs the top N interfaces on the selected flow collector, as measured by inbound or outbound flow traffic in bits per second (bps). With IFA Premium you can select whether to report on interface inbound or outbound flows.

Below the chart the list of top entries is shown, the first entries have color icons corresponding to the chart colors. By default this list of interfaces is limited to a maximum number of five entries.

If the source IP address of the device cannot be matched to the inventory object, then Entuity displays the IP address. Similarly, if Entuity cannot match the ifIndex to the interface in the inventory, Entuity displays *ifIndex N*. An interface entry is masked (###) if the user has no access to it, non-inventory interfaces are not be masked.

When a user has access to the interface but not the device then the device name is not displayed, but a drill-down is possible.



**Port: [ Et0/0 ] to c3560 fa0/17** (on 10.44.1.36)

*My Network (century.entuity.local)*

**Breakdown:** Top Interfaces **Device:** 10.44.1.36 **Previous:** 30 mins (Interval: 1 min)

**Filters:** ✗ Interface = **[ Et0/0 ] to c3560 fa0/17 on 10.44.1.36**

Chart Style: Stacked Area

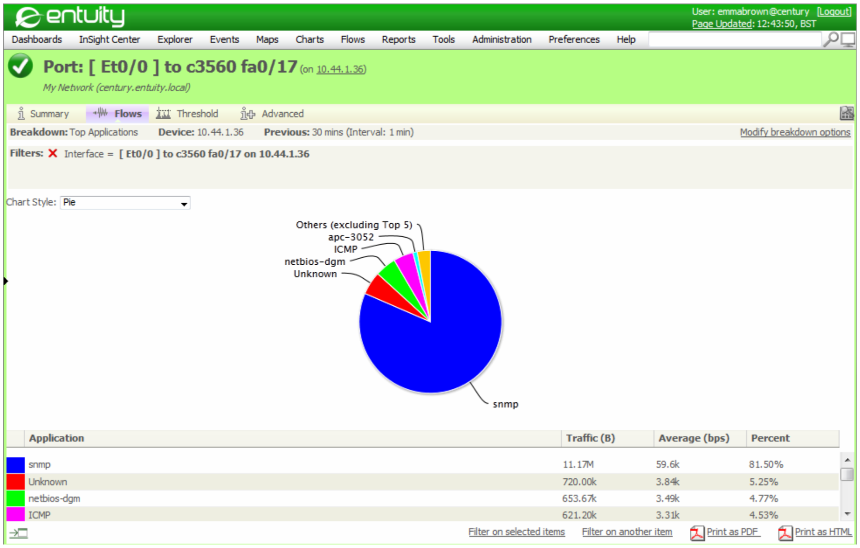
| | Interface | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|
| 🟦 | [ Et0/0 ] to c3560 fa0/17 on 10.44.1.36 | 13.78M | 73.5k | 100.00% |
| | **Others (excluding Top 1)** | 0 | 0 | 0.00% |
| | **Sum** | 13.78M | | |

Figure 87 Flow Interface Chart

## Applications Breakdown

This Flow Analysis chart graphs the top N applications on the selected flow collector, measured in bits per second (bps). Below the chart the list of top entries is shown, the first entries have color icons corresponding to the chart colors. By default this list of applications is limited to a maximum number of 20 entries.

If there is an unknown application in the list, system administrators can update the mapping through the Application Port Mappings page. Administrators could also use `flow-applications-template.txt`, and upload these changes to the Entuity database using `flowCollector.bat`. When you want to view which ports are sending and receiving flow data without the overlay of application mapping you can create a chart using the Ports category.



Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)

*My Network (century.entuity.local)*

**Breakdown:** Top Applications **Device:** 10.44.1.36 **Previous:** 30 mins (Interval: 1 min)

**Filters:** ✗ Interface = **[ Et0/0 ] to c3560 fa0/17 on 10.44.1.36**

Chart Style: Pie

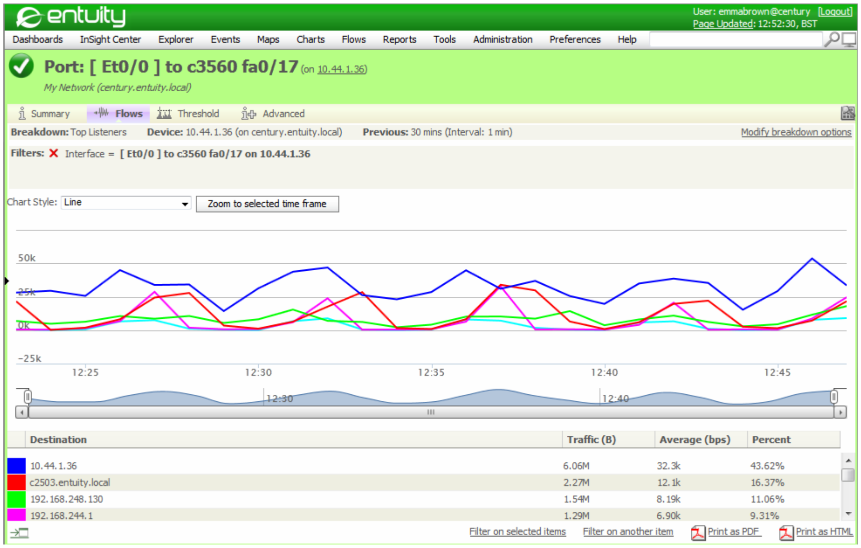
| | Application | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|
| 🟦 | snmp | 11.17M | 59.6k | 81.50% |
| 🟥 | Unknown | 720.00k | 3.84k | 5.25% |
| 🟩 | netbios-dgm | 653.67k | 3.49k | 4.77% |
| 🟪 | ICMP | 621.20k | 3.31k | 4.53% |

Figure 88 Flow Applications Chart

## Conversation, Listeners and Talkers Breakdown

IFA and IFA Premium include these related breakdown:

- Top Talkers, the top n talking hosts on the interface, measured as outbound traffic in bits per second (bps).
- Top Listeners, the top n listening hosts on the interface, measured as inbound traffic in bits per second (bps).
- Top Conversations, Entuity considers a conversation as flow data from both the source and destination IP address. Breakdown by conversation is only available with Integrated Flow Analysis Premium.



**Port: [ Et0/0 ] to c3560 fa0/17** (on 10.44.1.36)

*My Network (century.entuity.local)*

**Breakdown:** Top Listeners **Device:** 10.44.1.36 (on century.entuity.local) **Previous:** 30 mins (Interval: 1 min) Modify breakdown options

**Filters:** ✗ Interface = **[ Et0/0 ] to c3560 fa0/17 on 10.44.1.36**

Chart Style: Line

| | Destination | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|
| 🟦 | 10.44.1.36 | 6.06M | 32.3k | 43.62% |
| 🟥 | c2503.entuity.local | 2.27M | 12.1k | 16.37% |
| 🟩 | 192.168.248.130 | 1.54M | 8.19k | 11.06% |
| 🟪 | 192.168.244.1 | 1.29M | 6.90k | 9.31% |

Figure 89 Top N Listeners Chart

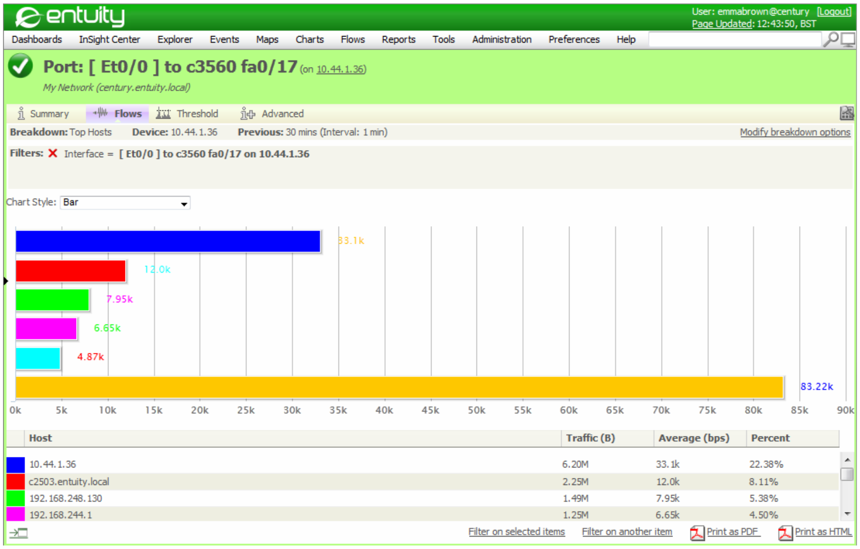
## Hosts Breakdown

There are three categories of Host Flow Analysis charts:

- Inbound host traffic, flows with the same destination IP address.
- Outbound host traffic, flows with the same source IP address.
- Combined inbound and outbound host traffic.

Entuity does not match the IP address to any of the inventory objects (device or managed host) to perform masking based on the users’ access scope.

If the required host is not in the list you can search for it by IP address, by Select another Hosts link. Entuity displays the a dialog through which you can enter the host IP address.



User: emmabrown@century [Logout]
Page Updated: 12:43:50, BST

Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)
My Network (century.entuity.local)

**Breakdown:** Top Hosts **Device:** 10.44.1.36 **Previous:** 30 mins (Interval: 1 min) Modify breakdown options

**Filters:** ✗ Interface = **[ Et0/0 ] to c3560 fa0/17 on 10.44.1.36**

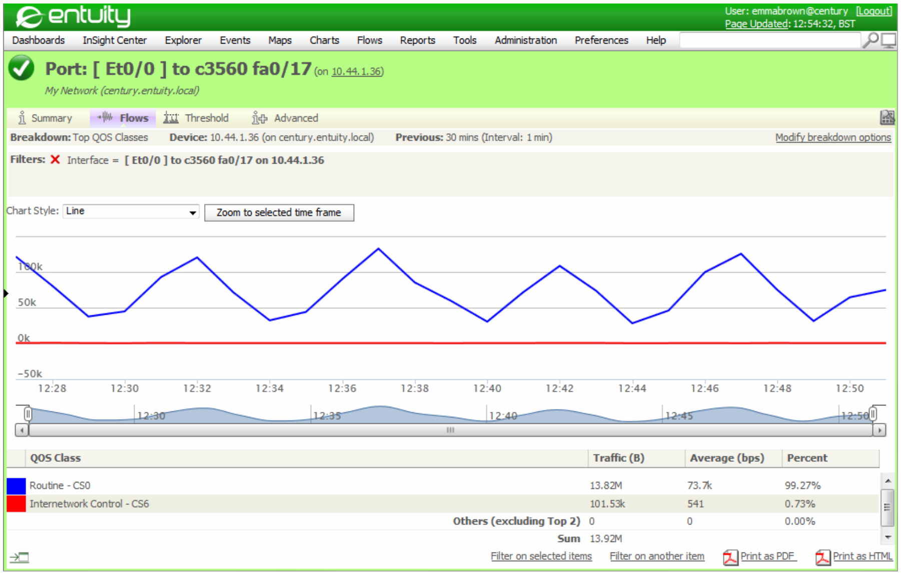
Chart Style: Bar

| | Host | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|
| 🟦 | 10.44.1.36 | 6.20M | 33.1k | 22.38% |
| 🟥 | c2503.entuity.local | 2.25M | 12.0k | 8.11% |
| 🟩 | 192.168.248.130 | 1.49M | 7.95k | 5.38% |
| 🟪 | 192.168.244.1 | 1.25M | 6.65k | 4.50% |

Figure 90 Flow Hosts Chart

## QoS, DSCP and IP Precedence Breakdowns

The QoS, DSCP and IP Precedence breakdowns chart the top N QoS classes on the selected flow collector, as measured in bits per second (bps). Below the chart the list of top entries is shown, the first entries have color icons corresponding to the chart colors. By default this list of classes is limited to a maximum number of 20 entries.



Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)

My Network (century.entuity.local)

Breakdown: Top QOS Classes    Device: 10.44.1.36 (on century.entuity.local)    Previous: 30 mins (Interval: 1 min)    Modify breakdown options

Filters: ✕ Interface = [ Et0/0 ] to c3560 fa0/17 on 10.44.1.36

Chart Style: Line

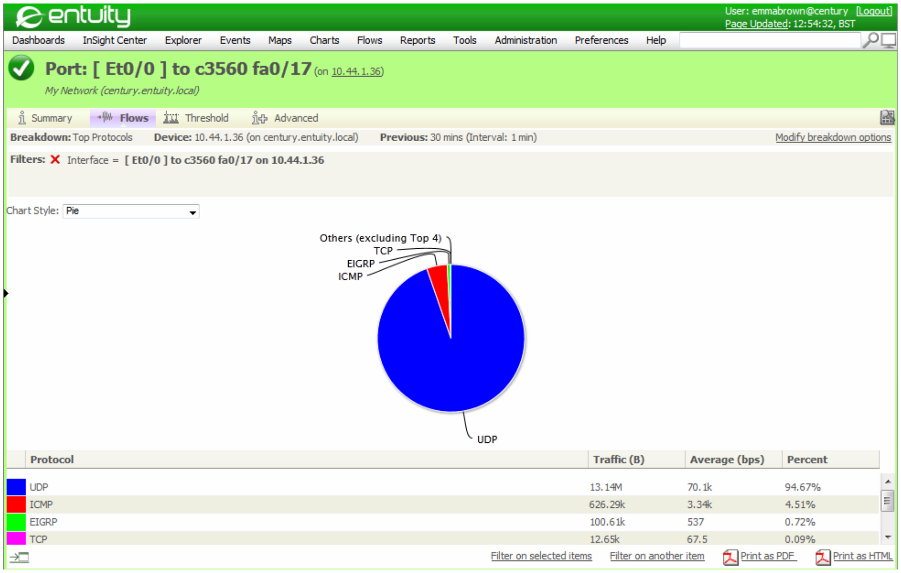
| | QOS Class | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|
| 🟦 | Routine - CS0 | 13.82M | 73.7k | 99.27% |
| 🟥 | Internetwork Control - CS6 | 101.53k | 541 | 0.73% |
| | Others (excluding Top 2) | 0 | 0 | 0.00% |
| | Sum | 13.92M | | |

Figure 91 Flow QoS Classes Chart

From the QoS Classes list you can select a class, Entuity then applies this class as a filter and updates the chart to show the topN interfaces for this class. You can remove the filter, and Entuity displays the interfaces Flow Analysis chart.

## Protocols Breakdown

This Flow Analysis chart graphs the top N Protocols on the selected flow collector, as measured in bits per second (bps). Below the chart the list of top entries is shown, the first entries have color icons corresponding to their chart colors. By default this list of protocols is limited to a maximum number of 20 entries.



Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)

My Network (century.entuity.local)

**Breakdown:** Top Protocols **Device:** 10.44.1.36 (on century.entuity.local) **Previous:** 30 mins (Interval: 1 min) Modify breakdown options

**Filters:** ✗ Interface = **[ Et0/0 ] to c3560 fa0/17 on 10.44.1.36**

Chart Style: Pie

| | Protocol | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|
| 🟦 | UDP | 13.14M | 70.1k | 94.67% |
| 🟥 | ICMP | 626.29k | 3.34k | 4.51% |
| 🟩 | EIGRP | 100.61k | 537 | 0.72% |
| 🟪 | TCP | 12.65k | 67.5 | 0.09% |

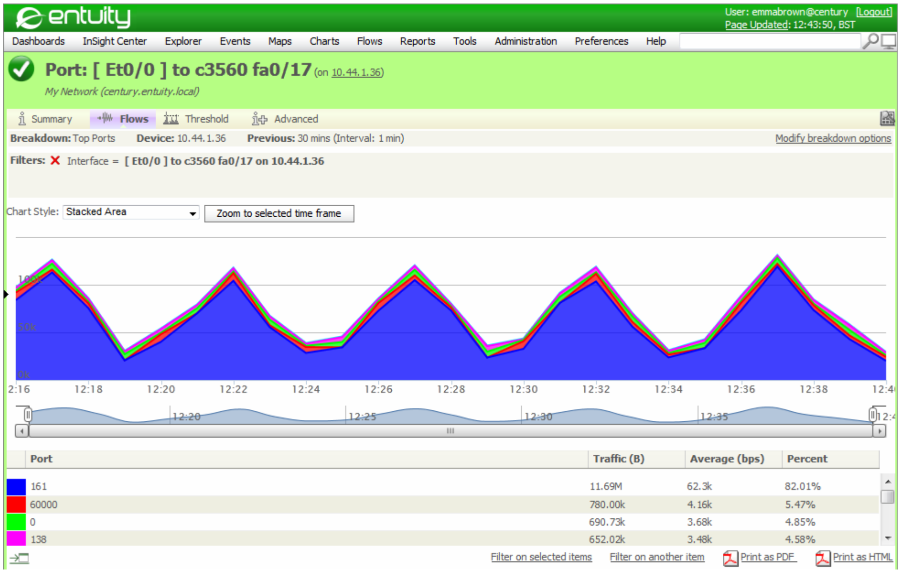
Figure 92 Flow Protocols Chart

From the Protocols list you can select a protocol, Entuity then applies this protocol as a filter and updates the chart to show the topN interfaces for this protocol. You can remove the filter, and Entuity displays the interfaces Flow Analysis chart.

## Port Breakdown

This Flow Analysis chart graphs the primary UDP/TCP ports sending and receiving flow data. When you want to view port data mapped against applications you can create a chart using the Applications category.

Below the chart the list of top entries is shown, the first entries have color icons corresponding to their chart colors. By default this list of ports is limited to a maximum number of 20 entries.



Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)

My Network (century.entuity.local)

**Breakdown:** Top Ports **Device:** 10.44.1.36 **Previous:** 30 mins (Interval: 1 min)

**Filters:** ✗ Interface = **[ Et0/0 ] to c3560 fa0/17 on 10.44.1.36**

Chart Style: Stacked Area

| | Port | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|
| 🟦 | 161 | 11.69M | 62.3k | 82.01% |
| 🟥 | 60000 | 780.00k | 4.16k | 5.47% |
| 🟩 | 0 | 690.73k | 3.68k | 4.85% |
| 🟪 | 138 | 652.02k | 3.48k | 4.58% |

Figure 93 Flow Port Chart

## Configure Flow Analysis Graphs

Flow Analysis graphs are displayed on a port’s Flows page, which you can access through Explorer or the Flow Inventory pages.

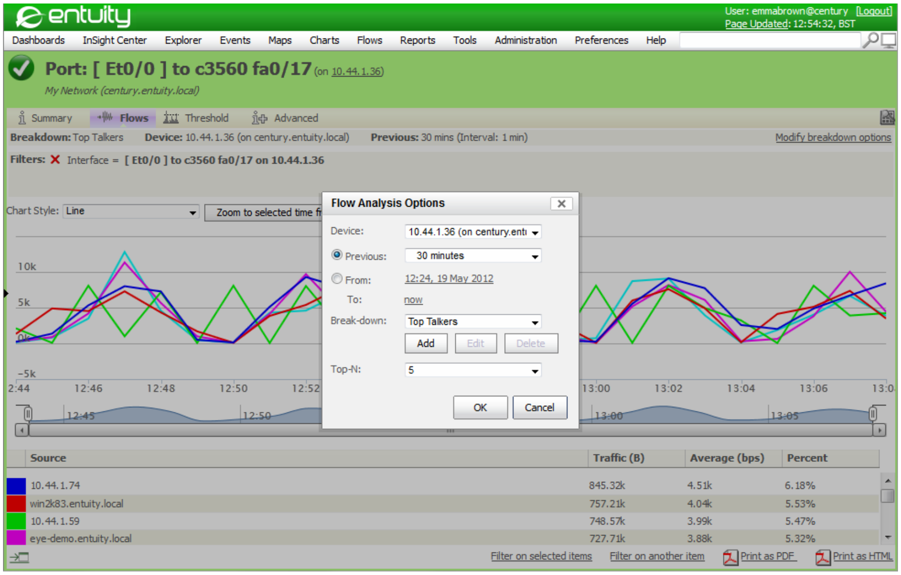
When you access a port’s Flows page Entuity displays the Flow Analysis Options dialog through which you can configure flow data.

| Attribute | Description |
|---|---|
| *Device* | Device name. When the device sends flows to more than one collector Entuity displays the collector name in brackets. Select a specific device. |

Table 24 Defining Flow Graphs

| Attribute | Description |
|---|---|
| *Interval* | You can select the time interval over which traffic rate is calculated and Entuity uses the most appropriate sample rate:<br>1 minute samples (this option is only available with IFA Premium and when you activate collection of one minute samples)<br>- Last 30 minutes<br>5 minute samples<br>- Last 1 hour<br>- Last 2 hours<br>1 hour samples<br>- Last 4 hours<br>- Last 8 hours<br>- Last 24 hours<br>6 hour samples<br>- Last 2 Days<br>- Last 4 Days<br>- Last Week<br>1 day samples<br>- All.<br>It is possible that there is no data for the whole interval selected. In this case UI will show an information message indicating that. |
| *Chart Style* | There are four chart styles, Stacked Area, Line, Bar Chart and Pie Chart. You can select items in the bar and pie charts and use the Filter on Selected Items when building complex charts. |
| *Top-N* | There are three predefined Top-N numbers, 5, 10 and 20 that set the maximum number of records that can appear on a chart. For the clearest presentation of data you should set stacked area and line charts to 5, pie charts to a maximum of 10 and bar charts can be used with 20 entries. |
| *Breakdown* | The category of flow data to be graphed, i.e. Interface, Application, Host (In, Out) QOS (All, DSCP, IP Precedence), Protocol, Port.<br>You can build complex graphs by selecting values from different categories for the one graph. Each category selection acts as a filter on the objects available from the next selected category. |
| *Print as PDF* | Select the PDF icon to export the current chart as a Flow Analysis report in a PDF file. |
| *Print as HTML* | Select the HTML icon to export the current chart as a Flow Analysis report. You have the option of accessing the Flow Analysis Report Options and saving the report definition, which is then available to run at a later date. |

Table 24 Defining Flow Graphs



Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)

My Network (century.entuity.local)

Breakdown: Top Talkers Device: 10.44.1.36 (on century.entuity.local) Previous: 30 mins (Interval: 1 min)

Filters: ✗ Interface = [ Et0/0 ] to c3560 fa0/17 on 10.44.1.36

Device: 10.44.1.36 (on century.enti

● Previous: 30 minutes

○ From: 12:24, 19 May 2012

To: now

Break-down: Top Talkers

Top-N: 5

| | Source | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|
| 🟦 | 10.44.1.74 | 845.32k | 4.51k | 6.18% |
| 🟥 | win2k83.entuity.local | 757.21k | 4.04k | 5.53% |
| 🟩 | 10.44.1.59 | 748.57k | 3.99k | 5.47% |
| 🟪 | eye-demo.entuity.local | 727.71k | 3.88k | 5.32% |

Figure 94 IFA Premium Flow Analysis Options

## Creating Simple Flow Graphs

The simplest Flow Analysis chart applies one filter (breakdown category) for the selected flow collector. For example you can filter on the top N interfaces, top N applications.

To create a simple flow graph:

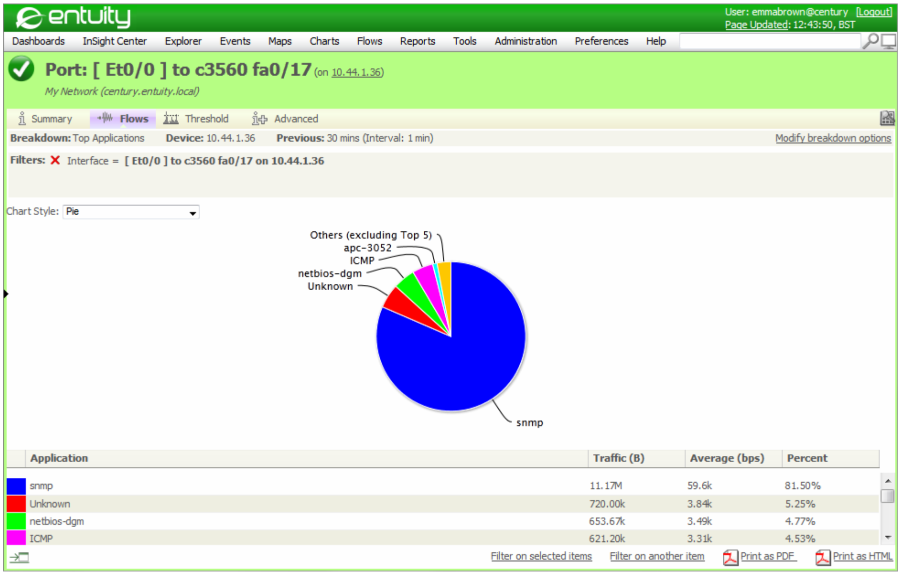
1) From Explorer find the port receiving the flow data and select its Flow tab.

2) Through the Flow Analysis Options dialog configure the Flow Analysis graph.

   For example select the flow category **Application** to create a chart for the Top N applications, as measured by traffic flow, on that collector.

3) Click **OK**.

   Entuity generates the flow chart. If you can amend the flow configuration Entuity automatically updates the graph display.



Port: [ Et0/0 ] to c3560 fa0/17 (on 10.44.1.36)

My Network (century.entuity.local)

Breakdown: Top Applications Device: 10.44.1.36 Previous: 30 mins (Interval: 1 min)

Filters: ✕ Interface = [ Et0/0 ] to c3560 fa0/17 on 10.44.1.36

Chart Style: Pie

| | Application | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|
| 🟦 | snmp | 11.17M | 59.6k | 81.50% |
| 🟥 | Unknown | 720.00k | 3.84k | 5.25% |
| 🟩 | netbios-dgm | 653.67k | 3.49k | 4.77% |
| 🟪 | ICMP | 621.20k | 3.31k | 4.53% |

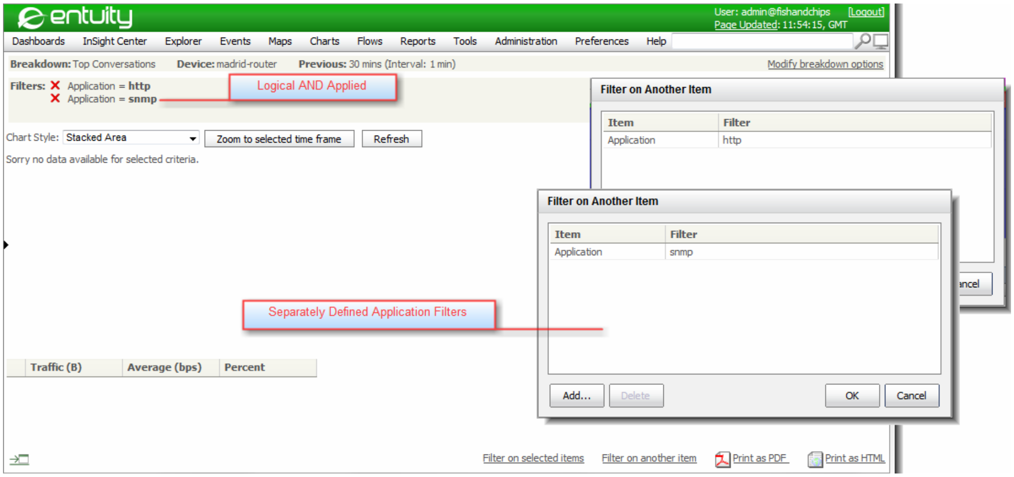
Figure 95 Flow Analysis Top Applications

## Creating Flow Graphs with Filters

You can use one category to select an object and use that as a filter for another flow category. For example, you can select from the Applications category SNMP. This becomes the selected filter, so when you select the Port category only ports that the Integrated Flow Analyzer has not mapped to an application are displayed. Similarly you could select an application, and then the Port category to view the ports that the application is using.

You can build more complex filters by selecting more than one value and you then have the option of applying a logical AND or OR to those filter components. To apply a logical:

- AND you separately select each of the components of the filter in the Filter on Another Item dialog. For example if you want the flow graph to only include top conversations with both SNMP and HTTP applications then you define separate application filters.



**Breakdown:** Top Conversations **Device:** madrid-router **Previous:** 30 mins (Interval: 1 min)

**Filters:** ✕ Application = **http**
✕ Application = **snmp**

Chart Style: Stacked Area

Sorry no data available for selected criteria.

| Traffic (B) | Average (bps) | Percent |
|---|---|---|

**Filter on Another Item**

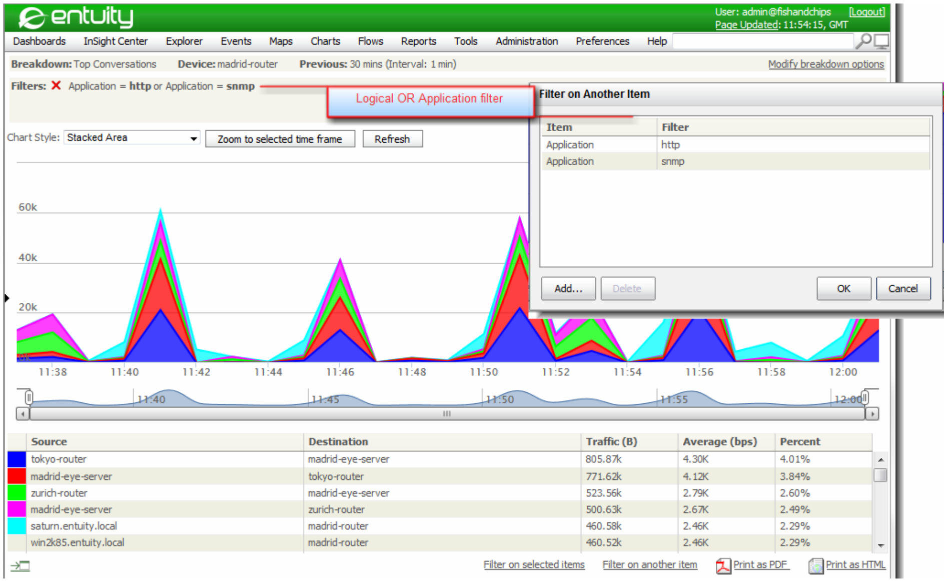
| Item | Filter |
|---|---|
| Application | http |

**Filter on Another Item**

| Item | Filter |
|---|---|
| Application | snmp |

Figure 96 Logical AND Filters

- OR you select all of the components of the filter in the same Filter on Another Item dialog. For example if you want the flow graph to include top conversations with either SNMP or HTTP applications then you define them within the same dialog.



**Breakdown:** Top Conversations **Device:** madrid-router **Previous:** 30 mins (Interval: 1 min)

**Filters:** ✕ Application = **http** or Application = **snmp**

Chart Style: Stacked Area

**Filter on Another Item**

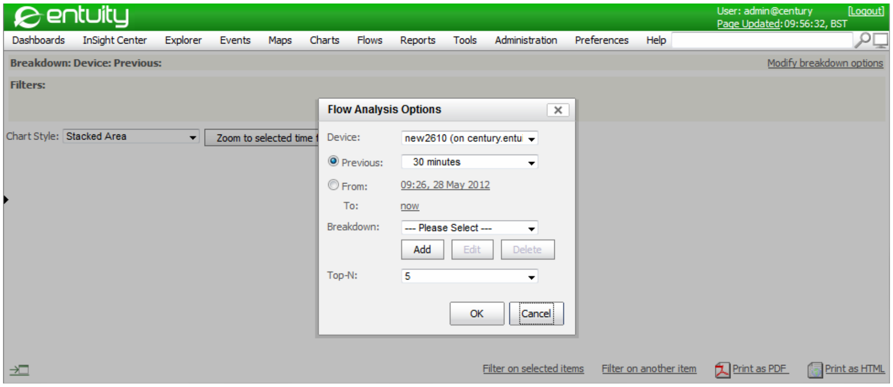
| Item | Filter |
|---|---|
| Application | http |
| Application | snmp |

| | Source | Destination | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|---|
| 🟦 | tokyo-router | madrid-eye-server | 805.87k | 4.30K | 4.01% |
| 🟥 | madrid-eye-server | tokyo-router | 771.62k | 4.12K | 3.84% |
| 🟩 | zurich-router | madrid-eye-server | 523.56k | 2.79K | 2.60% |
| 🟪 | madrid-eye-server | zurich-router | 500.63k | 2.67K | 2.49% |
| 🟦 | saturn.entuity.local | madrid-router | 460.58k | 2.46K | 2.29% |
| | win2k85.entuity.local | madrid-router | 460.52k | 2.46K | 2.29% |

Figure 97 Logical OR Filter

To create a flow graph that uses filters, for example to view top conversations and filter down on a particular application:

1) Click **Flows**.


entuity
User: admin@century [Logout]
Page Updated: 09:56:32, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Preferences Help
Modify breakdown options
Zoom to selected time
Add Edit Delete
OK Cancel
Filter on selected items Filter on another item Print as PDF Print as HTML

Breakdown: Device: Previous:

Filters:

Chart Style: Stacked Area

Flow Analysis Options

Device: new2610 (on century.entu

● Previous: 30 minutes

○ From: 09:26, 28 May 2012

To: now

Breakdown: --- Please Select ---

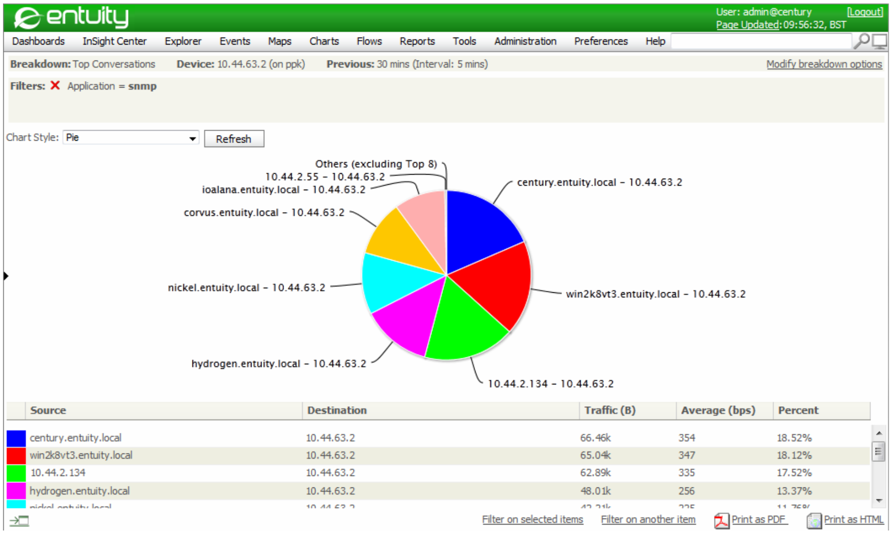
Top-N: 5

Figure 98 Set Flow Analysis Options

2) Select the breakdown category **Top Conversations** and set Top-N to **20**.

3) Select *Filter on another item* and from the Applications list select **snmp**. Entuity adds SNMP to the *Select Filters*.

When the chart style is Pie or Bar, you can select on an item in the chart to select and then filter on it.


entuity
User: admin@century [Logout]
Page Updated: 09:56:32, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Preferences Help
Modify breakdown options
Refresh
Others (excluding Top 8)
10.44.2.55 – 10.44.63.2
ioalana.entuity.local – 10.44.63.2
century.entuity.local – 10.44.63.2
corvus.entuity.local – 10.44.63.2
nickel.entuity.local – 10.44.63.2
win2k8vt3.entuity.local – 10.44.63.2
hydrogen.entuity.local – 10.44.63.2
10.44.2.134 – 10.44.63.2
Filter on selected items Filter on another item Print as PDF Print as HTML

Breakdown: Top Conversations Device: 10.44.63.2 (on ppk) Previous: 30 mins (Interval: 5 mins)

Filters: ✗ Application = snmp

Chart Style: Pie

| | Source | Destination | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|---|
| 🟦 | century.entuity.local | 10.44.63.2 | 66.46k | 354 | 18.52% |
| 🟥 | win2k8vt3.entuity.local | 10.44.63.2 | 65.04k | 347 | 18.12% |
| 🟩 | 10.44.2.134 | 10.44.63.2 | 62.89k | 335 | 17.52% |
| 🟪 | hydrogen.entuity.local | 10.44.63.2 | 48.01k | 256 | 13.37% |
| 🟦 | nickel.entuity.local | 10.44.63.2 | 42.21k | 225 | 11.76% |

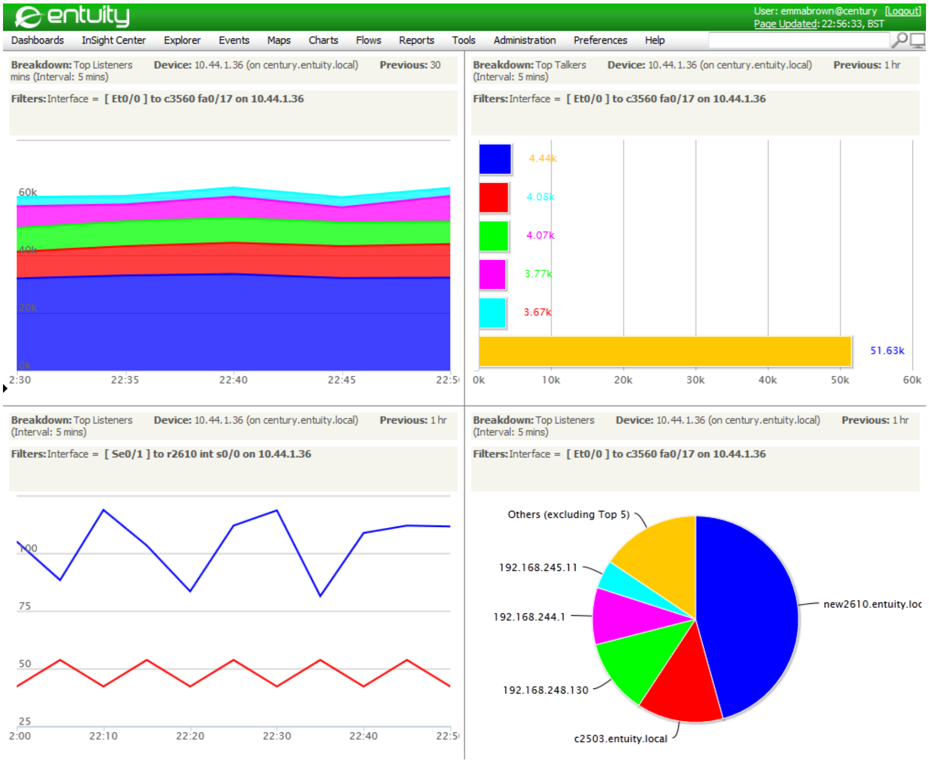
Figure 99 Top Conversations Filtered on SNMP Applications

## Creating Flow Dashboards

You can integrate flow data within Custom Dashboards. When you set the dashboard to update every five minutes you can to easily track key flow data metrics.

To add a Flow Analysis chart to a dashboard:

1) Set-up the chart.
2) Click **Dashboards** > **Custom Dashboards** > **Edit**.
3) Click the Edit Name icon to display the dialog through which you can specify the dashboard name.
4) Select the icon representing the required layout of your dashboard.
5) Populate a pane with the flow chart by dragging the chart link into it.
6) Click **Preview** for Entuity to display the current dashboard setup.
7) Click **Save** to save the dashboard.



**Breakdown:** Top Listeners **Device:** 10.44.1.36 (on century.entuity.local) **Previous:** 30 mins (Interval: 5 mins)

**Filters:** Interface = **[ Et0/0 ] to c3560 fa0/17 on 10.44.1.36**

**Breakdown:** Top Talkers **Device:** 10.44.1.36 (on century.entuity.local) **Previous:** 1 hr (Interval: 5 mins)

**Filters:** Interface = **[ Et0/0 ] to c3560 fa0/17 on 10.44.1.36**

**Breakdown:** Top Listeners **Device:** 10.44.1.36 (on century.entuity.local) **Previous:** 1 hr (Interval: 5 mins)

**Filters:** Interface = **[ Se0/1 ] to r2610 int s0/0 on 10.44.1.36**

**Breakdown:** Top Listeners **Device:** 10.44.1.36 (on century.entuity.local) **Previous:** 1 hr (Interval: 5 mins)

**Filters:** Interface = **[ Et0/0 ] to c3560 fa0/17 on 10.44.1.36**

Figure 100 Flow Custom Dashboard

# Automatic Path Creation from Flows

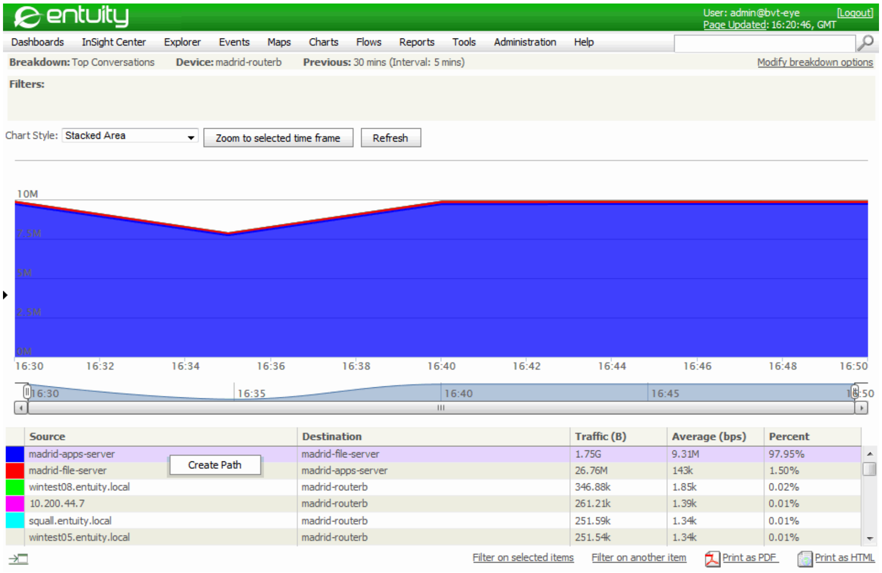
When IFA Premium indicates a performance issue and you have access to a SurePath server you can automatically create paths from the monitored Top Conversation. The conversation includes the source and destination IP address of the path to discover, therefore Entuity can default in these values to the Create Path dialog accelerating the path creation workflow.

SurePath is a separate licensable product to Entuity. For more details refer to the SurePath documentation or contact your Entuity representative.

To create a path from flow data:

1) From the flow **Top Conversations** breakdown table highlight the required row.

2) From the context menu select **Create Path**.



**Breakdown:** Top Conversations **Device:** madrid-routerb **Previous:** 30 mins (Interval: 5 mins)

**Filters:**

Chart Style: Stacked Area

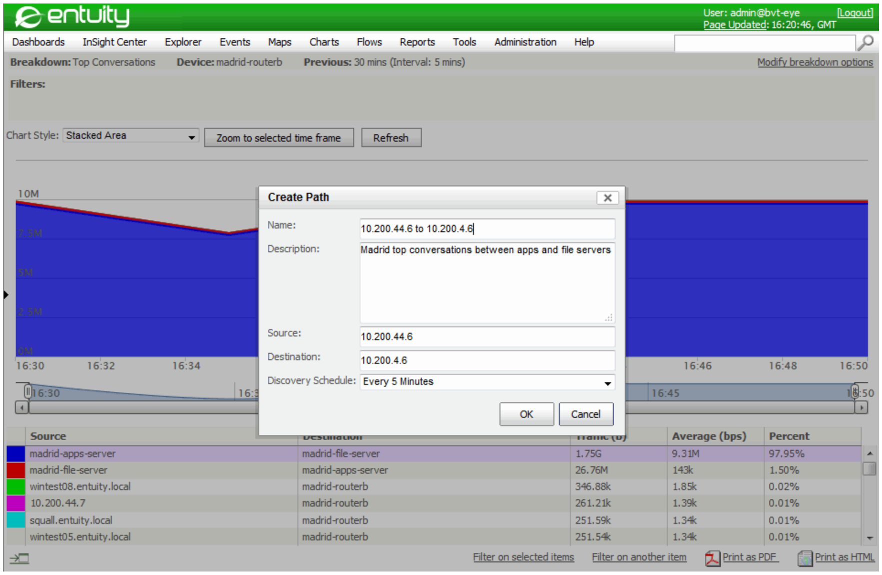
| | Source | Destination | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|---|
| 🟦 | madrid-apps-server | madrid-file-server | 1.75G | 9.31M | 97.95% |
| 🟥 | madrid-file-server | madrid-apps-server | 26.76M | 143k | 1.50% |
| 🟩 | wintest08.entuity.local | madrid-routerb | 346.88k | 1.85k | 0.02% |
| 🟪 | 10.200.44.7 | madrid-routerb | 261.21k | 1.39k | 0.01% |
| 🟦 | squall.entuity.local | madrid-routerb | 251.59k | 1.34k | 0.01% |
| | wintest05.entuity.local | madrid-routerb | 251.54k | 1.34k | 0.01% |

Figure 101 Automatic Path Creation

3) Entuity defaults in the source and destination IP address from the selected flow. Enter:

- *Name*, which is used throughout SurePath, for example on the Path Summary dashboard.
- *Description*, meaningful description of the path, for example its purpose.
- *Discovery Schedule*, how frequently SurePath discovers the path between the source and destination.

Click **OK**.



**Breakdown:** Top Conversations **Device:** madrid-routerb **Previous:** 30 mins (Interval: 5 mins)

**Filters:**

Chart Style: Stacked Area

**Create Path**

Name: 10.200.44.6 to 10.200.4.6

Description: Madrid top conversations between apps and file servers

Source: 10.200.44.6

Destination: 10.200.4.6

Discovery Schedule: Every 5 Minutes

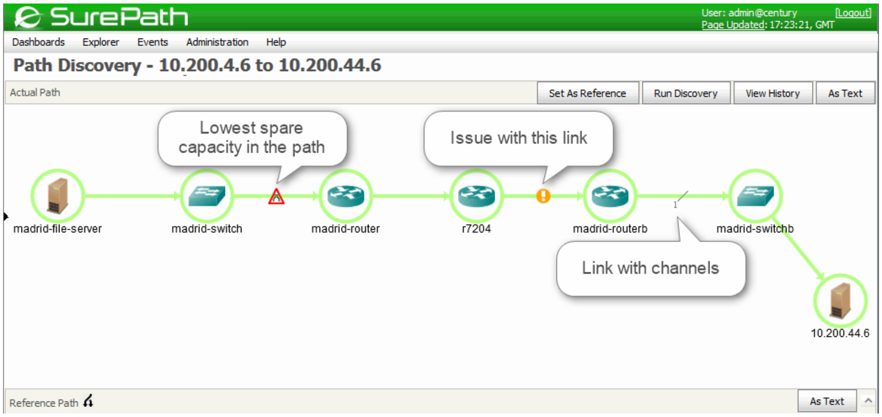
OK Cancel

| | Source | Destination | Traffic (B) | Average (bps) | Percent |
|---|---|---|---|---|---|
| 🟦 | madrid-apps-server | madrid-file-server | 1.75G | 9.31M | 97.95% |
| 🟥 | madrid-file-server | madrid-apps-server | 26.76M | 143k | 1.50% |
| 🟩 | wintest08.entuity.local | madrid-routerb | 346.88k | 1.85k | 0.02% |
| 🟪 | 10.200.44.7 | madrid-routerb | 261.21k | 1.39k | 0.01% |
| 🟦 | squall.entuity.local | madrid-routerb | 251.59k | 1.34k | 0.01% |
| | wintest05.entuity.local | madrid-routerb | 251.54k | 1.34k | 0.01% |

Figure 102 Automatic Path Creation

4) SurePath creates the path definition, initiates a path discovery. and displays the discovered path.

Paths can always be viewed through the Path Summary dashboard. Select **Dashboards > Path Summary** and then the path.



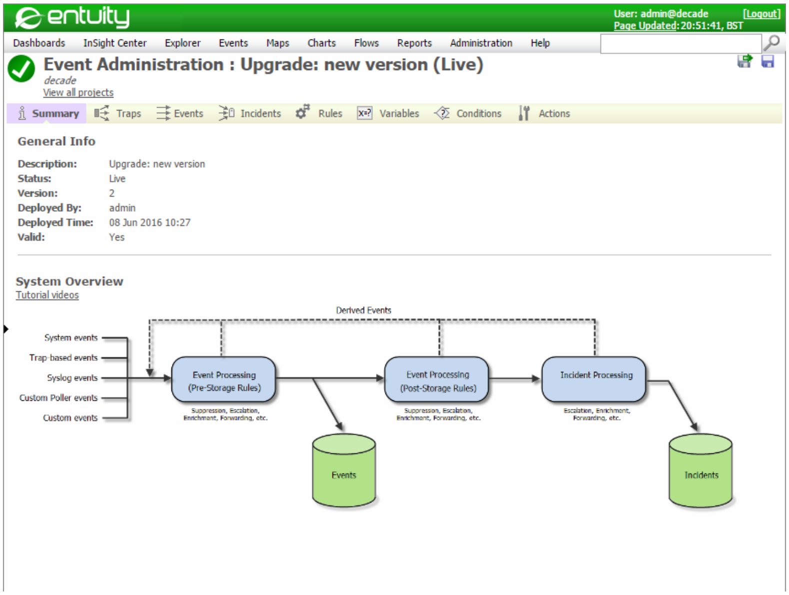
**Path Discovery - 10.200.4.6 to 10.200.44.6**

Figure 103 Path Discovered from Flow Analysis

# 27 Event Management System

Entuity includes a powerful Event Management System which assists you in proactively and rapidly addressing network problems. You can choose between using the sophisticated out-of-the-box rules as supplied or customizing the system to handle events based on your defined conditions and specific work-flows.

The Event Management System improves operational efficiency and business focus by combining multiple events into higher-level incidents. You can configure the system to handle events based on defined conditions, which also reduces clutter, helps speed response time, and allows users to focus on the events most relevant to their business without losing Event Management System sensitivity.



Event Administration : Upgrade: new version (Live)

*decade*

View all projects

General Info

**Description:** Upgrade: new version
**Status:** Live
**Version:** 2
**Deployed By:** admin
**Deployed Time:** 08 Jun 2016 10:27
**Valid:** Yes

System Overview

Tutorial videos

Figure 104 Event Management System Summary

## Tutorial Videos

Entuity includes an extensive set of tutorials which you are recommended to view before attempting to configure the Event Management System. Entuity currently provides these tutorials, which you should view in the following order:

1) Events and Incidents
2) Projects
3) Rules
4) Conditions

5) Special Rule types
6) Custom Events
7) Actions
8) Configuring Incidents
9) Escalations
10) Enrichment and Attributes
11) Trap Management.

### Viewing the Tutorials

The videos are provided as `mp4` files and you will require an appropriate browser and plugin. Depending upon your browser and plugin setup the videos play either in the browser window or launch an appropriate external application.

To access the tutorials:

1) Click **Administration** > **Events** > **Event Administration**.
2) Click the **Tutorial videos** hyperlink, situated below the System Overview section title.

   The tutorials are listed in the suggested viewing order.

## Incidents and Events Overview

Entuity separates how it receives information from the network and then how the Event Management System processes that data into events and incidents. For example you can:

- Enable system events and set event thresholds against polled data.
- Define custom events and rules to handle traps.
- Define your own custom polling of network objects and define events to be raised against that data.

How Entuity processes those events, for example whether they are saved to the database or discarded, generate incidents or not, is managed through the Event Management System.

Entuity distinguishes between an event which is raised to indicate a happening on the network or within Entuity, and an incident which can indicate the persistence of an event, can be called, amended and closed by more than one type of event.

| Event Types | Description |
|---|---|
| System Events | System events are shipped with Entuity and may be generated from SNMP polling, layer 3 node reachability or layer 4 application availability data. |
| Syslog Events | Syslog events are matched to syslog alerts. |
| Custom Events | Custom Events are defined within the Event Management System and their definitions are stored in the event project. |

Table 25 Event Types

| Event Types | Description |
|---|---|
| Derived Events | Derived Events are based upon existing event definitions within the Event Management System. They are raised by other events and actions in the Event Management System for example the Port Flapping event is raised according to rules applied to the Port Up and Port Down events. |
| Unifying Events | An event to which other events have their event type changed. For example the Port Link Down and Port Operationally Down events both have their event type changed to Port Down. This is not easily apparent to the end user as all other details of these events remain unaffected, including their names. |

Table 25 Event Types

Event Management System categorizes events according to how they are implemented and their usage. There is only one type of incident as all incidents are a product of their contributing events. However the intelligence you can build into an incident through the application of rules allows you great control over when they are raised. For this reason event viewer displays incidents by default.

The Event Management System is configured through an event project; Entuity includes a default event project. Administrators and users with the Event Administration permission can edit projects and when ready deploy them to the server. The new event project is considered live and the previous project is archived.

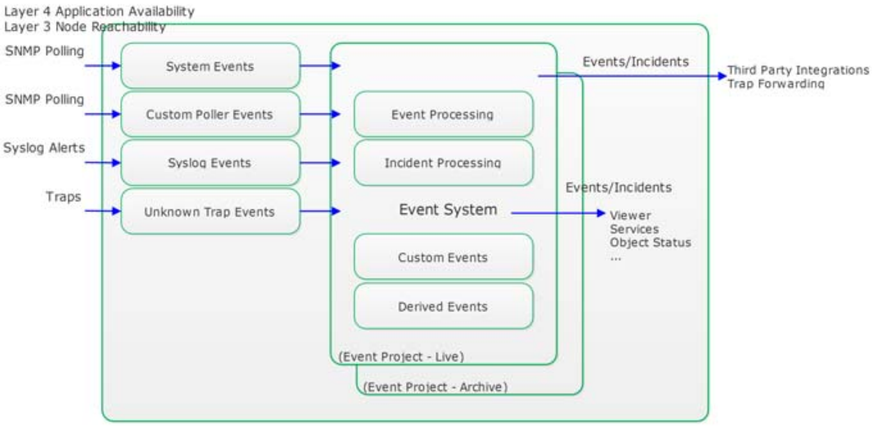


Figure 105 Entuity Handling Events and Incidents

## Event Management System Administrators and Users

When configuring the event project you should consider how to document your implementation, for other system administrators and also for users of the events system. For example whether an N of M rule is enabled or not could determine how the user manages an incidents.

# Event Management System and the Event Project

An event project configures the Event Management System. Entuity is shipped with a default event project that includes:

- Over 400 system events, the majority with an associated incident.
- Syslog events.
- Derived events, for example Port Flapping which is only generated when the Detect Flapping Rule is met with the Port Down and Port Up events, events which are derived from the Port Link Down and Port Link Up events.
- Rules, for example the:
  - Filter Port Status Events rule does not raise Port Link Down and Port link Up events for ports that have status events deactivated.
  - N of M for Network Outage rule filters out temporary outages by only raising the network outage event when two consecutive 5 minute polls indicate an outage.

  Rules defined under the Pre Storage folder are applied to events before they are saved to the database or raised in the viewer. Rules defined under the Post Storage folder are applied to events after they are saved to the database but before incidents are raised.
- Incidents for system and syslog events.
- Actions, for example how to send emails, forward SNMP traps.

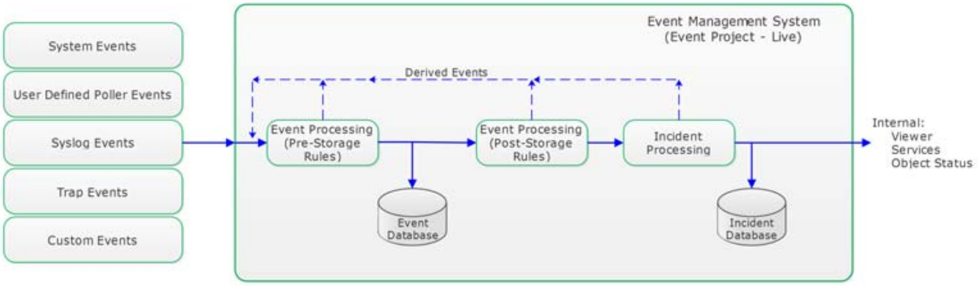


Figure 106 Flow of the Event Management System

The changes you make to an event project only configure the Event Management System once you save and deploy the project. Alongside the Event Administration title of each page in the event administration area Entuity displays the state of the event project that you are viewing. This would usually be the live project, but if you are amending a project then its state would change to draft, or viewing an old project then its state would be archived.

From the Project List page you can view and manage the event projects on your Entuity server. (See *Event Management System Administration*.)

# Comparison of Events and Incidents

Incidents and events have separate but related roles in managing your network. The primary difference is in their life cycle:

- An event is raised against an object and later a second event may be raised to indicate the problem is resolved. Later still the problem may return so another separate opening event is raised. Each event indicates the state of the managed object at the time the event was raised. Although all three events relate to the same source and to the same problem they are separate entities.
- An incident may be raised by an event, which indicates a problem on an object. It may be closed when Entuity identifies the issue as resolved through a closing event, the incident ages out or it is manually closed. If the issue on the object recurs and Entuity raises another opening event within the set expiry period Entuity also re-opens the original incident.

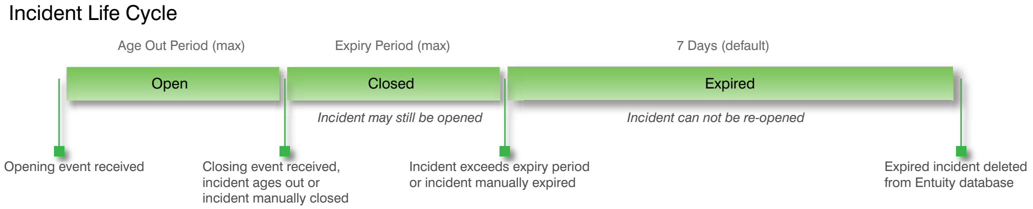
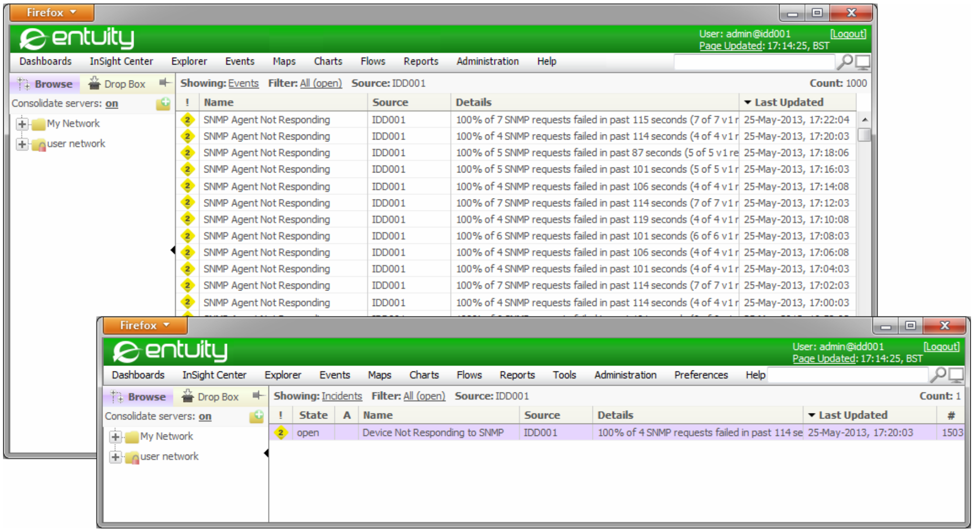

Incident Life Cycle
Age Out Period (max)
Expiry Period (max)
7 Days (default)
Open
Closed
Expired
Incident may still be opened
Incident can not be re-opened
Opening event received
Closing event received, incident ages out or incident manually closed
Incident exceeds expiry period or incident manually expired
Expired incident deleted from Entuity database

Figure 107 Event and Incident Life Cycle

So Entuity raises an event to warn that a specific condition is currently present, whereas incidents can indicate that this is an ongoing problem. Event Viewer, by default, displays incidents as they provide a better summary of items of concern on the network. For example Entuity may raise an SNMP Agent Not Responding event every time the device fails to respond, when you set Event Viewer *Showing* to:

- **Incidents** you view one incident, no matter how many events are raised.
- **Events** you may have hundreds even thousands of the events from the same source.



Showing: Events Filter: All (open) Source: IDD001 Count: 1000

| ! | Name | Source | Details | Last Updated |
|---|---|---|---|---|
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 7 SNMP requests failed in past 115 seconds (7 of 7 v1 r | 25-May-2013, 17:22:04 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 4 SNMP requests failed in past 114 seconds (4 of 4 v1 r | 25-May-2013, 17:20:03 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 5 SNMP requests failed in past 87 seconds (5 of 5 v1 re | 25-May-2013, 17:18:06 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 5 SNMP requests failed in past 101 seconds (5 of 5 v1 r | 25-May-2013, 17:16:03 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 4 SNMP requests failed in past 106 seconds (4 of 4 v1 r | 25-May-2013, 17:14:08 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 7 SNMP requests failed in past 114 seconds (7 of 7 v1 r | 25-May-2013, 17:12:03 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 4 SNMP requests failed in past 119 seconds (4 of 4 v1 r | 25-May-2013, 17:10:08 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 6 SNMP requests failed in past 101 seconds (6 of 6 v1 r | 25-May-2013, 17:08:03 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 4 SNMP requests failed in past 106 seconds (4 of 4 v1 r | 25-May-2013, 17:06:08 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 4 SNMP requests failed in past 101 seconds (4 of 4 v1 r | 25-May-2013, 17:04:03 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 7 SNMP requests failed in past 114 seconds (7 of 7 v1 r | 25-May-2013, 17:02:03 |
| 2 | SNMP Agent Not Responding | IDD001 | 100% of 4 SNMP requests failed in past 114 seconds (4 of 4 v1 r | 25-May-2013, 17:00:03 |

Showing: Incidents Filter: All (open) Source: IDD001 Count: 1

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| 2 | open | | Device Not Responding to SNMP | IDD001 | 100% of 4 SNMP requests failed in past 114 se | 25-May-2013, 17:20:03 | 1503 |

Figure 108 One Incident Represents Thousands of Events

The relationship between events and incidents can be of varying levels of complexity:

- Where one event raises an incident and a second event closes the incident.

  For example the Port Inbound Fault High (Packet Corruption) incident is raised by the Port Inbound Fault High (Packet Corruption) event and closed by the Port Inbound Fault High (Packet Corruption) Cleared event.

- Where more than one type of event can raise an incident and more than one type of event can close the incident.

  For example the AP Host Count Abnormality incident is raised by either the AP Host Count High or AP Host Count Low events and is closed by the AP Host Count High Cleared AP Host Count Low Cleared events.

- Where an incident may be raised and closed by particular event types, and an additional event type updates the state of that incident.

  For example the Device Not Responding to SNMP incident is raised by the SNMP Agent Not Responding event and its state is updated by the Device Cold Reboot, Device Warm Reboot and Device Reboot Detected events. (See *Tailored Events and Incidents*.)

## Tailored Events and Incidents

The Port Status Problem incident includes a number of techniques that you can also use to build a tailored Event Management System.

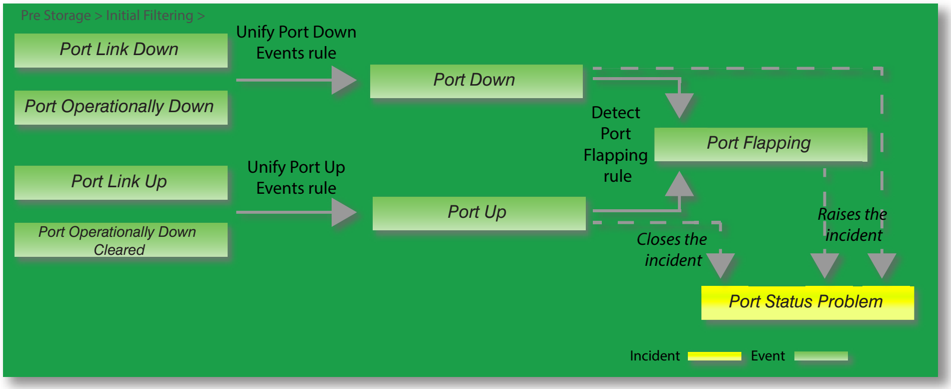


Figure 109 Unify Rules

The Port Link Down and Port Operationally Down events both report on port failure:

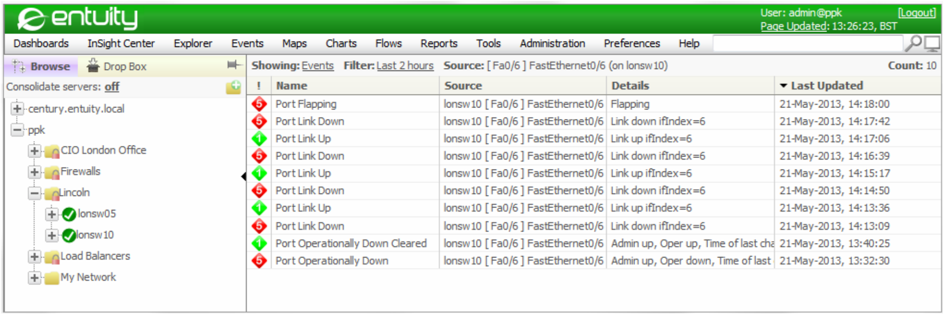
- Port Link Down is generated from trap data. Traps are useful as they are raised when a problem occurs, however a device may not be configured to forward traps and traps are more likely to be lost in transit.
- Port Operationally Down is generated from SNMP polling. SNMP polling is usually easily configurable and reliable, however polling is conducted at a set interval and so involves a delay.

The Unify Ports Down Events rule instructs Entuity to change the event type to Port Down when it receives either a Port Link Down or Port Operationally Down event. All other details remain the same, e.g. event name, severity level.

Entuity uses the same approach to define the Port Down event.

The Port Up and Port Down events are used to generate the Port Flapping event. The Detect Port Flapping rule identifies when the port alternates between Up and Down 4 times within 2 minutes.

When Entuity raises a Port Flapping event it also raises a Port Status Problem incident.



Showing: Events Filter: Last 2 hours Source: [ Fa0/6 ] FastEthernet0/6 (on lonsw10) Count: 10

| ! | Name | Source | Details | Last Updated |
|---|---|---|---|---|
| 5 | Port Flapping | lonsw10 [ Fa0/6 ] FastEthernet0/6 | Flapping | 21-May-2013, 14:18:00 |
| 5 | Port Link Down | lonsw10 [ Fa0/6 ] FastEthernet0/6 | Link down ifIndex=6 | 21-May-2013, 14:17:42 |
| 1 | Port Link Up | lonsw10 [ Fa0/6 ] FastEthernet0/6 | Link up ifIndex=6 | 21-May-2013, 14:17:06 |
| 5 | Port Link Down | lonsw10 [ Fa0/6 ] FastEthernet0/6 | Link down ifIndex=6 | 21-May-2013, 14:16:39 |
| 1 | Port Link Up | lonsw10 [ Fa0/6 ] FastEthernet0/6 | Link up ifIndex=6 | 21-May-2013, 14:15:17 |
| 5 | Port Link Down | lonsw10 [ Fa0/6 ] FastEthernet0/6 | Link down ifIndex=6 | 21-May-2013, 14:14:50 |
| 1 | Port Link Up | lonsw10 [ Fa0/6 ] FastEthernet0/6 | Link up ifIndex=6 | 21-May-2013, 14:13:36 |
| 5 | Port Link Down | lonsw10 [ Fa0/6 ] FastEthernet0/6 | Link down ifIndex=6 | 21-May-2013, 14:13:09 |
| 1 | Port Operationally Down Cleared | lonsw10 [ Fa0/6 ] FastEthernet0/6 | Admin up, Oper up, Time of last cha | 21-May-2013, 13:40:25 |
| 5 | Port Operationally Down | lonsw10 [ Fa0/6 ] FastEthernet0/6 | Admin up, Oper down, Time of last | 21-May-2013, 13:32:30 |

Figure 110 Flapping Port Raising Port Flapping Event

## Port Flapping Workflow for Advanced Users

The port flapping implementation includes techniques that you can also use when developing your own events. Flapping is a set of rules applied during Pre Storage processing which is before events are saved to the Entuity database, displayed through the viewer or forwarded to integrations.

This work through:

- Assumes the port alternates between 4 states within a 2 minute period, which is the Entuity default definition of a flapping port.
- Shows how the unifying events, Port Up and Port Down, are used to combine the same type of information coming from different types of alerts (traps and SNMP polling).
- Details why the unifying event appears to the end user as the originating event, for example Entuity may raise the Port Down event but it displays as Port Link Down (or Port Operationally Down). And how you can amend this default behavior.
- Includes the derived event Port Flapping.
- Shows how and why events control an associated incident.

How Entuity handles a flapping port, one that goes up, down, up, down:

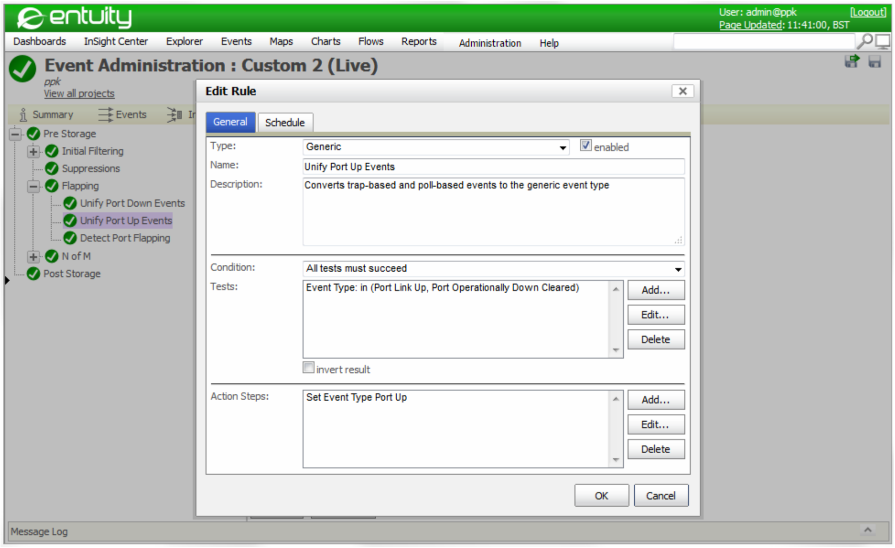
1) Entuity receives a trap which it handles as a Port Link Up event.

   Entuity applies the Unify Port Up Event rule. As a Port Link Up event it meets the condition and so Entuity performs the action, setting the event type to Port Up. All other details associated with the event are retained, including the event name.

   If you wanted to set the event name to match the event type then you would create an additional action to set the event name attribute:

   ```
   Set Attribute name = "Port Up"
   ```

   Entuity applies the Detect Port Flapping rule which identifies the port as not flapping because the number of changes in the port state is not 4 or more within the previous 2 minutes. Entuity saves to the database the Port Up event which displays in the viewer with the event name Port Link Up.



Type: Generic ☑ enabled

Name: Unify Port Up Events

Description: Converts trap-based and poll-based events to the generic event type

Condition: All tests must succeed

Tests: Event Type: in (Port Link Up, Port Operationally Down Cleared)

□ invert result

Action Steps: Set Event Type Port Up

Figure 111 Unify Port Up Events

2) Entuity polls the port, detects it is up and raises a Port Operationally Down Cleared event.

Entuity applies the Unify Port Up Event rule. As a Port Operationally Down Cleared event it meets the condition and so Entuity performs the action, setting the event type to Port Up. All other details associated with the event are retained, including the event name.

Entuity applies the Detect Port Flapping rule which identifies the port as not flapping because the port is already set to down. Entuity saves to the database the Port Up event which displays in the viewer as a Port Operationally Down Cleared event.

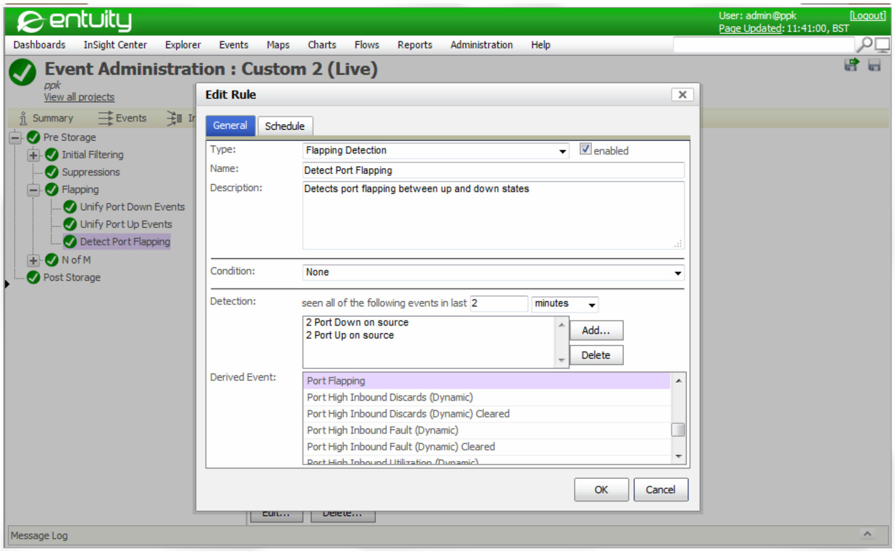
3) Next the port goes down, for simplicity we will restrict the example to trap events.

Entuity receives a trap which it handles as a Port Link Down event.

Entuity applies the Unify Port Down Event rule. As a Port Link Down event it meets the condition and so Entuity performs the action, setting the event type to Port Down. All other details associated with the event are retained, including the event name.

Entuity raises the Port Status Problem incident.

Entuity applies the Detect Port Flapping rule which identifies the port as not flapping because the number of changes in the port state is not 4 or more within the previous 2 minutes. Entuity saves to the database the Port Down event which displays in the viewer as a Port Link Down event.



Type: Flapping Detection ☑ enabled

Name: Detect Port Flapping

Description: Detects port flapping between up and down states

Condition: None

Detection: seen all of the following events in last 2 minutes

2 Port Down on source
2 Port Up on source

Derived Event:
Port Flapping
Port High Inbound Discards (Dynamic)
Port High Inbound Discards (Dynamic) Cleared
Port High Inbound Fault (Dynamic)
Port High Inbound Fault (Dynamic) Cleared

Figure 112 Detect Port Flapping Rule

4) The port goes up. Entuity receives a trap which it handles as a Port Link Up event and after applying the Unify Port Up Event rule raises a Port Up event.

Entuity closes the Port Status Problem incident.

Entuity applies the Detect Port Flapping rule, identifies the port as not flapping and so saves to the database the underlying Port Up event but displays it in the viewer as a Port Link Up event. Entuity also closes the Port Status Problem incident.

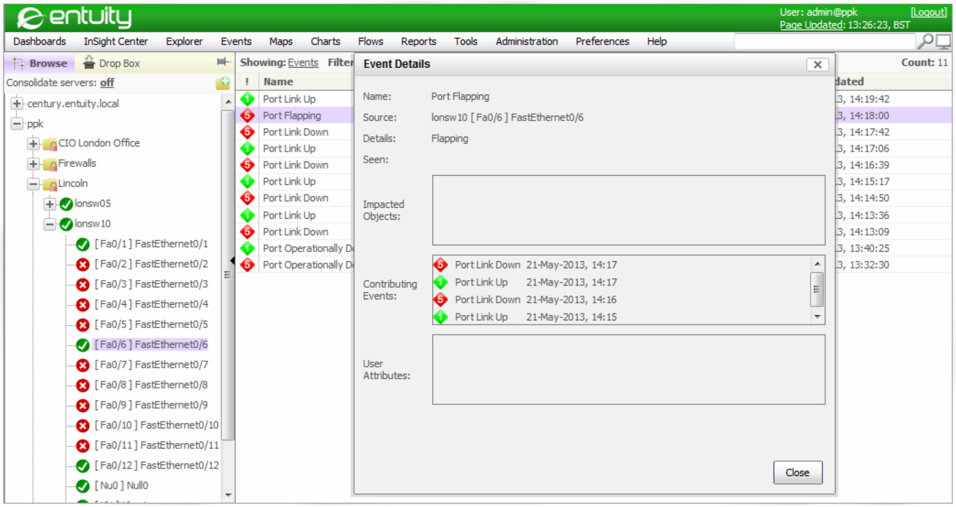
5) Next the port goes down. Entuity receives a trap which it handles as a Port Link Down event.

Entuity applies the Unify Port Down Event rule. As a Port Link Down event it meets the condition and so Entuity performs the action, setting the event type to Port Down. All other details associated with the event are retained, including the event name.

Entuity raises the Port Status Problem incident.

Entuity applies the Detect Port Flapping rule which identifies the port as flapping because the number of changes in the port state is 4 within the previous 2 minutes. Entuity saves to the database the Port Down event and raises the Port Flapping event. The Port Link Down event is not displayed until the Port Flapping event expires, or the port again changes state.

You can view the events that contribute to the derived Port Flapping event by highlighting the event and from the context menu clicking **Show Details**.


entuity
User: admin@ppk [Logout]
Page Updated: 13:26:23, BST
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Tools
Administration
Preferences
Help
Browse
Drop Box
Consolidate servers: off
century.entuity.local
ppk
CIO London Office
Firewalls
Lincoln
lonsw05
lonsw10
[ Fa0/1 ] FastEthernet0/1
[ Fa0/2 ] FastEthernet0/2
[ Fa0/3 ] FastEthernet0/3
[ Fa0/4 ] FastEthernet0/4
[ Fa0/5 ] FastEthernet0/5
[ Fa0/6 ] FastEthernet0/6
[ Fa0/7 ] FastEthernet0/7
[ Fa0/8 ] FastEthernet0/8
[ Fa0/9 ] FastEthernet0/9
[ Fa0/10 ] FastEthernet0/10
[ Fa0/11 ] FastEthernet0/11
[ Fa0/12 ] FastEthernet0/12
[ Nu0 ] Null0
Showing: Events
Filter
Count: 11
Close

| ! | Name | dated |
|---|---|---|
| | Port Link Up | 3, 14:19:42 |
| 5 | Port Flapping | 3, 14:18:00 |
| 5 | Port Link Down | 3, 14:17:42 |
| | Port Link Up | 3, 14:17:06 |
| 5 | Port Link Down | 3, 14:16:39 |
| | Port Link Up | 3, 14:15:17 |
| 5 | Port Link Down | 3, 14:14:50 |
| | Port Link Up | 3, 14:13:36 |
| 5 | Port Link Down | 3, 14:13:09 |
| | Port Operationally D | 3, 13:40:25 |
| 5 | Port Operationally D | 3, 13:32:30 |

**Event Details**

Name: Port Flapping

Source: lonsw10 [ Fa0/6 ] FastEthernet0/6

Details: Flapping

Seen:

Impacted Objects:

Contributing Events:

| | | |
|---|---|---|
| 5 | Port Link Down | 21-May-2013, 14:17 |
| | Port Link Up | 21-May-2013, 14:17 |
| 5 | Port Link Down | 21-May-2013, 14:16 |
| | Port Link Up | 21-May-2013, 14:15 |

User Attributes:

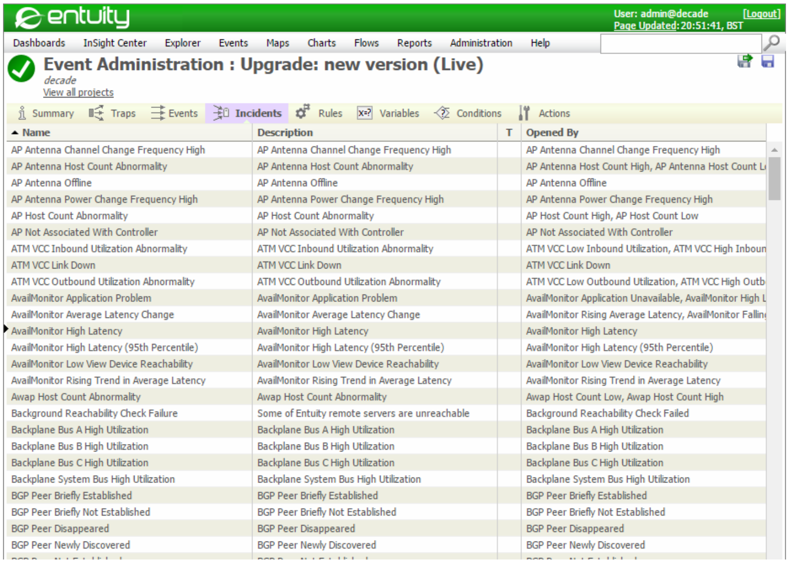
Figure 113 Port Status Problem Incident

# Incidents

Entuity includes over 100 standard incident definitions with the default event project. As part of the Event Management System’s event project these incidents are fully editable. You can also create incidents, for example if you create custom events you may want to create associated incidents.

By default, if the Event Management System raises an event with a severity level greater than Information that does not have an associated incident, Event Management System creates an on-the-fly incident using the details of the event and applying the default incident template (defined in *entuity_home*`\etc\event-engine-cfg-template.properties`). These on-the-fly incidents do not have an incident definition, therefore you cannot apply incident processing or implement event correlation.

Within the Event Management System there is not a distinction between incidents based on whether an incident was shipped with Entuity or created by a user, unlike events where, for example system events can only have their severity level amended. With incidents you could, although it is not recommended, delete all supplied incidents.



Event Administration : Upgrade: new version (Live)

*decade*

View all projects

| ▲ Name | Description | T | Opened By |
|---|---|---|---|
| AP Antenna Channel Change Frequency High | AP Antenna Channel Change Frequency High | | AP Antenna Channel Change Frequency High |
| AP Antenna Host Count Abnormality | AP Antenna Host Count Abnormality | | AP Antenna Host Count High, AP Antenna Host Count L |
| AP Antenna Offline | AP Antenna Offline | | AP Antenna Offline |
| AP Antenna Power Change Frequency High | AP Antenna Power Change Frequency High | | AP Antenna Power Change Frequency High |
| AP Host Count Abnormality | AP Host Count Abnormality | | AP Host Count High, AP Host Count Low |
| AP Not Associated With Controller | AP Not Associated With Controller | | AP Not Associated With Controller |
| ATM VCC Inbound Utilization Abnormality | ATM VCC Inbound Utilization Abnormality | | ATM VCC Low Inbound Utilization, ATM VCC High Inboun |
| ATM VCC Link Down | ATM VCC Link Down | | ATM VCC Link Down |
| ATM VCC Outbound Utilization Abnormality | ATM VCC Outbound Utilization Abnormality | | ATM VCC Low Outbound Utilization, ATM VCC High Outb |
| AvailMonitor Application Problem | AvailMonitor Application Problem | | AvailMonitor Application Unavailable, AvailMonitor High L |
| AvailMonitor Average Latency Change | AvailMonitor Average Latency Change | | AvailMonitor Rising Average Latency, AvailMonitor Fallin |
| AvailMonitor High Latency | AvailMonitor High Latency | | AvailMonitor High Latency |
| AvailMonitor High Latency (95th Percentile) | AvailMonitor High Latency (95th Percentile) | | AvailMonitor High Latency (95th Percentile) |
| AvailMonitor Low View Device Reachability | AvailMonitor Low View Device Reachability | | AvailMonitor Low View Device Reachability |
| AvailMonitor Rising Trend in Average Latency | AvailMonitor Rising Trend in Average Latency | | AvailMonitor Rising Trend in Average Latency |
| Awap Host Count Abnormality | Awap Host Count Abnormality | | Awap Host Count Low, Awap Host Count High |
| Background Reachability Check Failure | Some of Entuity remote servers are unreachable | | Background Reachability Check Failed |
| Backplane Bus A High Utilization | Backplane Bus A High Utilization | | Backplane Bus A High Utilization |
| Backplane Bus B High Utilization | Backplane Bus B High Utilization | | Backplane Bus B High Utilization |
| Backplane Bus C High Utilization | Backplane Bus C High Utilization | | Backplane Bus C High Utilization |
| Backplane System Bus High Utilization | Backplane System Bus High Utilization | | Backplane System Bus High Utilization |
| BGP Peer Briefly Established | BGP Peer Briefly Established | | BGP Peer Briefly Established |
| BGP Peer Briefly Not Established | BGP Peer Briefly Not Established | | BGP Peer Briefly Not Established |
| BGP Peer Disappeared | BGP Peer Disappeared | | BGP Peer Disappeared |
| BGP Peer Newly Discovered | BGP Peer Newly Discovered | | BGP Peer Newly Discovered |

Figure 114 Incidents

| Attribute | Description |
|---|---|
| *Name* | Incident name displayed throughout Entuity |
| *Description* | Description of the incident. |
| *T* | A green tick indicates the incident includes triggers. |
| *Opened By* | Lists the events that open the incident. |

Table 26 Incidents

## Incident and Global Incident Triggers

A trigger is a method of associating an action to the change in state of an incident. You can, for example control what state causes a trigger to action, if there is any delay to that action and whether the state of incident after that delay (precondition) impacts on the action.

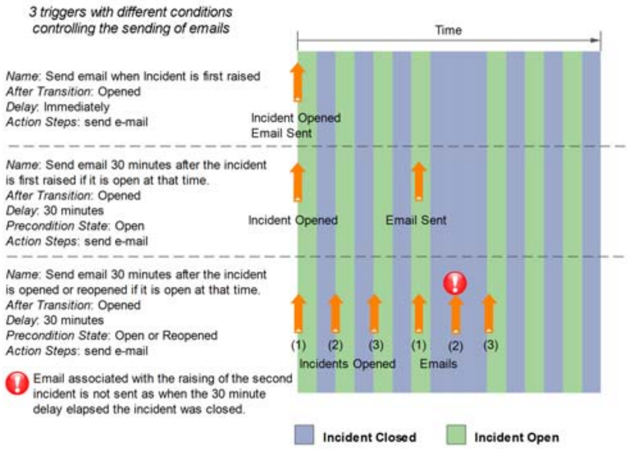

3 triggers with different conditions controlling the sending of emails
Time
Name: Send email when Incident is first raised
After Transition: Opened
Delay: Immediately
Action Steps: send e-mail
Incident Opened
Email Sent
Name: Send email 30 minutes after the incident is first raised if it is open at that time.
After Transition: Opened
Delay: 30 minutes
Precondition State: Open
Action Steps: send e-mail
Incident Opened
Email Sent
Name: Send email 30 minutes after the incident is opened or reopened if it is open at that time.
After Transition: Opened
Delay: 30 minutes
Precondition State: Open or Reopened
Action Steps: send e-mail
(1) (2) (3)
Incidents Opened
(1) (2) (3)
Emails
Email associated with the raising of the second incident is not sent as when the 30 minute delay elapsed the incident was closed.
Incident Closed
Incident Open

Figure 115 Triggers, Delays and Preconditions

You can create triggers that are associated to a particular incident or create global triggers that you can associate to all or a defined set of incidents. Triggers are useful for example when designing an event system with inbuilt escalation processes. You could create a trigger that would notify a network administrator when a particular incident has been opened for an hour, and also define a second trigger which would email a senior network administrator if the incident were to remain open for two hours.

| Attribute | Description |
|---|---|
| *Name* | Name of the trigger. |
| *Description* | Meaningful description, for example its purpose, |

Table 27 Set Trigger

| Attribute | Description |
|---|---|
| *On Transition To* | An incident can change state, for example be opened for the first time, closed, reopened. You can set when the trigger is applied dependent upon the state the incident is transitioning to.<br>You can set the transitioned to state to:<br>■ **Opened**. The action is only run once for the incident, when it is first raised.<br>■ **Reopened**. The action is not run the first time the incident is raised, but it is run each time the incident is subsequently reopened.<br>■ **Opened** or **Reopened**. The action is run the first time the incident is raised, and each time the incident is subsequently reopened.<br>■ **Closed.** The action is run each time the incident is closed.<br>■ **Expired.** The action is run each time the incident is expired.<br>■ **Any Change**. When you want the action to occur whenever there is a change in the incident then select **Any Change**. **Any Change** is useful when forwarding events to third party software and wanting to ensure all incidents are forwarded.<br>If you have set *State Precondition* Event Management System runs an extra evaluation before running the action. |
| *Delay* | When creating a trigger you may want to delay when and if an action is performed. For example you may set a delay of 1 hour and *State Precondition* to **Open**. Event Management System would only trigger an action if the incident is in an open state 1 hour after it was raised.<br>You can set *Delay* to **Immediately** (no delay), or a delay of seconds, minutes, hours or days. |
| Condition | Through setting a condition you can control the scope of the trigger. For example you can define tests based on incident severity, incident type and incident attributes. (See *Conditions and Tests*.) |
| Tests | When setting a condition you must then define one or more tests. (See *Conditions and Tests*.) |
| *State After Delay* | When you have set *Delay* (to anything other than **Immediately**) you can apply an additional test before Event Management System runs the action steps. For example with *State Precondition* set to **Open** and `Delay` set to 30 minutes Event Management System only runs the action steps for an incident in an Open state 30 minutes after it was raised.<br>You can set the incident precondition state to:<br>■ **Open**<br>■ **Closed**<br>■ **Expired**<br>■ **Open or Closed**<br>■ **Any**. |
| *Action Steps* | Defines the operations the trigger applies. You can select from saved actions or define new actions. You can also edit and delete actions. (See *Actions*.) |

Table 27 Set Trigger

## Create Incidents

An incident definition consists of contributing events, ageout and expiry values and potentially triggers. You can use new combinations of supplied events to create new incidents, use custom events or a combination of the two.

| Attribute | Description |
|---|---|
| *Name* | Incident name displayed throughout Entuity |
| *enabled* | When selected the incident can be raised by Entuity. |
| *Description* | Description of the incident. |
| *Opened by any of* | Each row shows an event type and its source that can open the incident. You can:<br>■ Click **Add** and from the Event Type Selection dialog select an event type and its *Target*. By default *Target* is set to **source** which causes Entuity to raise incidents against the same source as the event. You can define an expression to set a different source, for example for port event raising the incident against its device enter `source.device`.<br>■ Highlight a row and click **Delete** to remove the event - source combination from the incident definition. |
| *Updated By* | Each row shows an event type and its source that can update the incident. You can:<br>■ Click **Add** and from the Event Type Selection dialog select an event type and its *Target*. By default *Target* is set to **source** which causes Entuity to update incidents raised against the same source as the event. You can define an expression to set a different source, for example for port event raising the incident against its device enter `source.device`.<br>■ Highlight a row and click **Delete** to remove the event - source combination from the incident definition. |
| *Closed by any of* | Each row shows an event type and its source that can close the incident. You can:<br>■ Click **Add** and from the Event Type Selection dialog select an event type and its *Target*. By default *Target* is set to **source** which causes Entuity to close incidents raised against the same source as the event. You can define an expression to set a different source, for example for port event raising the incident against its device enter `source.device`.<br>■ Highlight a row and click **Delete** to remove the event - source combination from the incident definition. |
| *Update incident details* | You can control how Entuity updates the incidents as events are raised that are associated with the incident, select:<br>■ Update severity and details to match the most recent event.<br>■ Use the severity and details of the most severe event. |

Table 28 Incident Definition

| Attribute | Description |
|---|---|
| *Age Out* | Time period during which if the incident state is not updated the incident ages out and is closed. If the issue on the object recurs and Entuity raises another opening event within the set *Expiry* period Entuity also re-opens the original incident. |
| *Expiry* | Time period during which the closed incident state can be reopened if the issue on the object recurs and Entuity raises another opening event. After the expiry period if the issue on the object recurs and Entuity raises another opening event Entuity opens a new incident. |

Table 28 Incident Definition

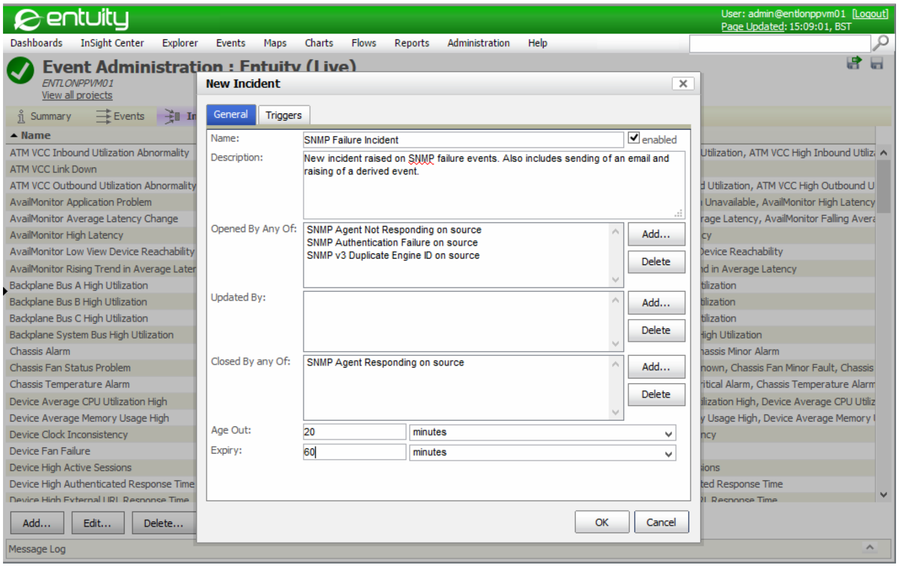
This example creates a new SNMP failure incident that:

- Is raised when one of any three specified SNMP events occur.
- Is closed when an SNMP Agent Responding event is raised on the same source as the opening events.
- Ages out after 20 minutes and expires after 60 minutes.
- Includes two triggers:
  - A derived event which is generated when the incident is open five minutes after it is raised, i.e. *State Precondition* is set to five minutes.
  - An email which is sent two seconds after the incident is raised.

Incidents are configured from the Incidents tab of the Event Administration page. To create the example incident:

1) Click **Administration** > **Events** > **Event Administration**.
2) Click **Incidents** and then **Add**.
3) Define the incident general details. Enter:
   - A meaningful name and description of the incident.
   - In *Opened By Any Of* click **Add**, highlight an event and then click **OK** to add an opening event type. Repeat this for the three event types.
   - In *Updated By* you could add events that update the state of the incident. For example you may select an event that if raised against the source object indicates an escalation in the problem.
   - In *Closed By Any Of* click **Add**, highlight the SNMP Agent Responding event type and then click **OK** to add the incident closing event.
   - A 20 minute Age Out and 60 minute Expiry times for the incident.

   When you want to use the incident ensure you have selected Enable.



Name: SNMP Failure Incident ☑ enabled

Description: New incident raised on SNMP failure events. Also includes sending of an email and raising of a derived event.

Opened By Any Of: SNMP Agent Not Responding on source<br>SNMP Authentication Failure on source<br>SNMP v3 Duplicate Engine ID on source

Updated By:

Closed By any Of: SNMP Agent Responding on source

Age Out: 20 minutes

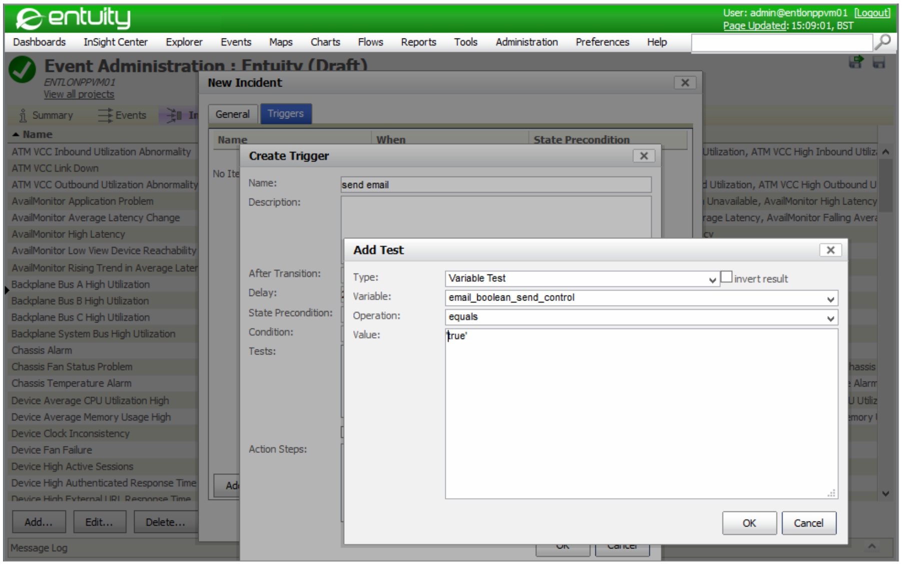
Expiry: 60 minutes

Figure 116 Create Incident

4) Click the Triggers tab and then **Add** the email notification and derived event triggers.

5) Define the email notification trigger details and test condition:

- Enter a meaningful name and description.
- Set Delay to 2 seconds.
- Set *Condition* to **All Tests must succeed**. Click **Add** and define the test by setting *Type* to **Variable Test**, selecting the `email_boolean_send_control` variable, *Operations* to **equals** and *Value* to `'true'`.


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 15:09:01, BST
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Tools
Administration
Preferences
Help
Event Administration : Entuity (Draft)
ENTLONPPVM01
View all projects
Summary
Events
Name
ATM VCC Inbound Utilization Abnormality
ATM VCC Link Down
ATM VCC Outbound Utilization Abnormality
AvailMonitor Application Problem
AvailMonitor Average Latency Change
AvailMonitor High Latency
AvailMonitor Low View Device Reachability
AvailMonitor Rising Trend in Average Latency
Backplane Bus A High Utilization
Backplane Bus B High Utilization
Backplane Bus C High Utilization
Backplane System Bus High Utilization
Chassis Alarm
Chassis Fan Status Problem
Chassis Temperature Alarm
Device Average CPU Utilization High
Device Average Memory Usage High
Device Clock Inconsistency
Device Fan Failure
Device High Active Sessions
Device High Authenticated Response Time
Device High External URL Response Time
Add...
Edit...
Delete...
Message Log
New Incident
General
Triggers
Name
When
State Precondition
No Items
Create Trigger
Description:
After Transition:
Delay:
State Precondition:
Condition:
Tests:
Action Steps:
Add Test
OK
Cancel

Name: send email

Type: Variable Test ☐ invert result

Variable: email_boolean_send_control

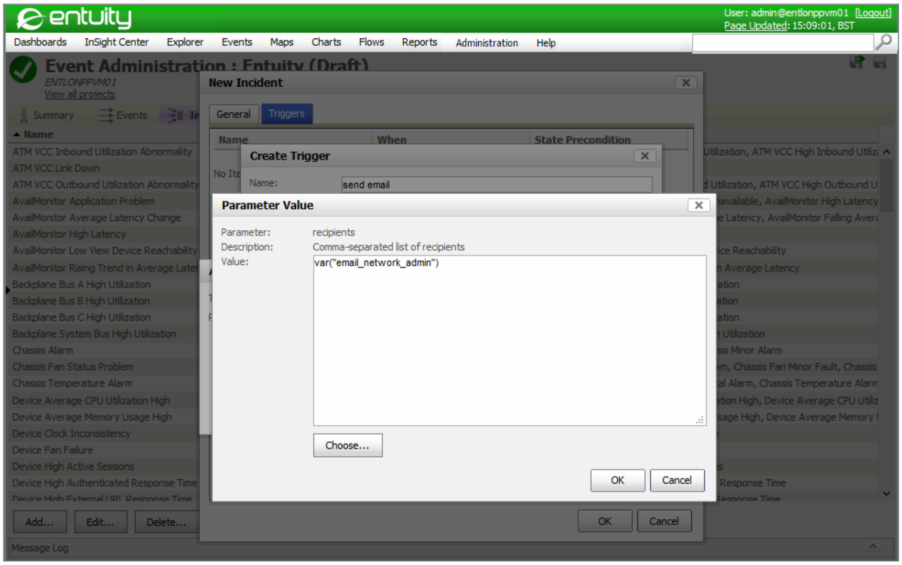
Operation: equals

Value: 'true'

Figure 117 Use a Variable for a Boolean Test

6) In Actions define the email action. Click **Add** and define the action in:

- *Type* select **Send e-mail**.
- Parameters highlight **recipients**, click **Set** and then **Choose**. Set *Value Kind* to **Variable Reference** and *Variable* to the `email_network_admin` variable.
- Parameters complete the subject and body parameters.



Name: send email

Parameter: recipients
Description: Comma-separated list of recipients
Value: var("email_network_admin")

Figure 118 Chosen Parameter

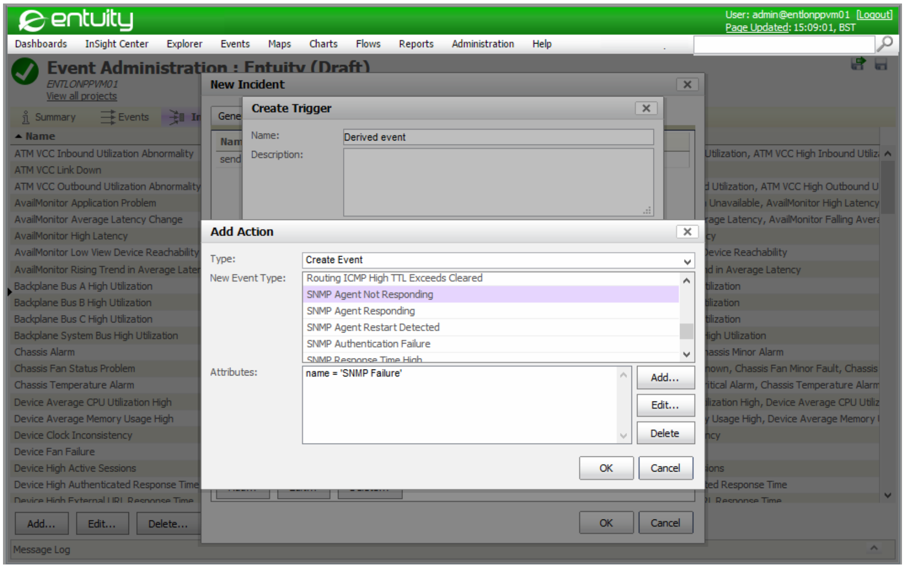
7) Click **OK** to create the trigger.

8) Define the derived event trigger details and test condition:

- Enter a meaningful name and description.
- Set Delay to 5 minutes.

9) In Actions define the create event action. Click **Add** and define the action in:

- *Type* select **Create event**.
- *Event Type* select the event type on which you want to base the new event.
- Attributes click **Add** and then define the new event attributes, for example select name to rename the event.



Name: Derived event

Description:

Type: Create Event

New Event Type:
Routing ICMP High TTL Exceeds Cleared
SNMP Agent Not Responding
SNMP Agent Responding
SNMP Agent Restart Detected
SNMP Authentication Failure
SNMP Response Time High

Attributes: name = 'SNMP Failure'

Figure 119 Create an Event Type

10) Close and save your changes by clicking **OK** to the open Event Management System dialogs.

11) Your changes are not applied to the Event Management System until you save and deploy the project.

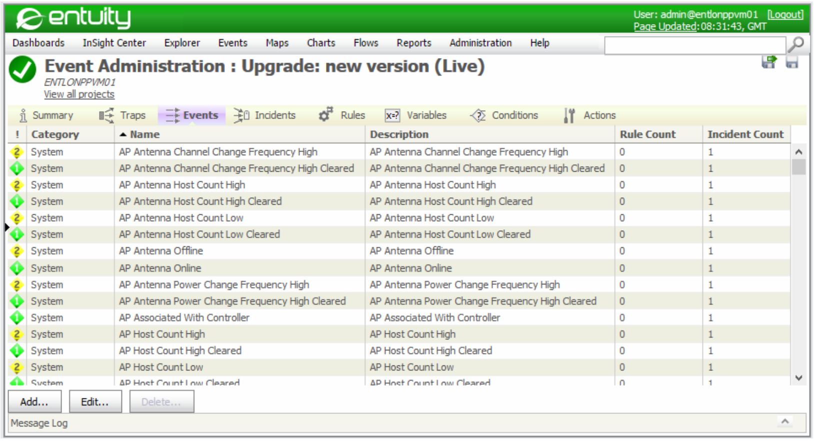
Click the Save and Deploy icon, enter a meaningful description of your updates and click **OK**.

## Custom Events

Entuity includes more than 400 system events and 8 syslog events. Administrators and users with the Event Administration permission can create custom events. When you add a custom event:

- Define the custom event name, description and severity level.
- You can associate a custom closing event, which also consists of a name, description and severity.
- You can also create an associated incident. An incident consists of a name, description, age out and expiry settings.

You have created the event but not how the event is raised. Custom events are raised by other events or incidents, more specifically their associated rules and actions. For example the Port Down and Port Up flapping events are both dependent upon other events, or rather the application of rules applied to other events, for them to be raised.



Event Administration : Upgrade: new version (Live)

*ENTLONPPVM01*

View all projects

| ! | Category | Name | Description | Rule Count | Incident Count |
|---|---|---|---|---|---|
| 2 | System | AP Antenna Channel Change Frequency High | AP Antenna Channel Change Frequency High | 0 | 1 |
| 1 | System | AP Antenna Channel Change Frequency High Cleared | AP Antenna Channel Change Frequency High Cleared | 0 | 1 |
| 2 | System | AP Antenna Host Count High | AP Antenna Host Count High | 0 | 1 |
| 1 | System | AP Antenna Host Count High Cleared | AP Antenna Host Count High Cleared | 0 | 1 |
| 2 | System | AP Antenna Host Count Low | AP Antenna Host Count Low | 0 | 1 |
| 1 | System | AP Antenna Host Count Low Cleared | AP Antenna Host Count Low Cleared | 0 | 1 |
| 2 | System | AP Antenna Offline | AP Antenna Offline | 0 | 1 |
| 1 | System | AP Antenna Online | AP Antenna Online | 0 | 1 |
| 2 | System | AP Antenna Power Change Frequency High | AP Antenna Power Change Frequency High | 0 | 1 |
| 1 | System | AP Antenna Power Change Frequency High Cleared | AP Antenna Power Change Frequency High Cleared | 0 | 1 |
| 1 | System | AP Associated With Controller | AP Associated With Controller | 0 | 1 |
| 2 | System | AP Host Count High | AP Host Count High | 0 | 1 |
| 1 | System | AP Host Count High Cleared | AP Host Count High Cleared | 0 | 1 |
| 2 | System | AP Host Count Low | AP Host Count Low | 0 | 1 |
| 1 | System | AP Host Count Low Cleared | AP Host Count Low Cleared | 0 | 1 |

Figure 120 Events

| Attribute | Description |
|---|---|
| ! | Event severity. |
| Category | Category of event:<br>■ system, shipped with the Entuity.<br>■ custom, created by the user. |
| *Name* | Event name displayed throughout Entuity |
| *Description* | Description of the event. |
| *Rule count* | Number of rules associated with the event. You can click on the column to view the rule and incidents associated with the event. |
| *Incident count* | Number of incidents associated with the event. You can click on the column to view the rule and incidents associated with the event. |

Table 29 Event Attributes

## Create Custom Events

When you create a custom event at the same time you can create its clearing event and an associated incident.

| Attribute | Description |
|---|---|
| *Name* | Event name displayed throughout Entuity. |
| Severity | Event severity level. |
| *Description* | Description of the event. |
| Add clearing event | Select to define a clearing event and then enter its *Name* and *Description*. |

Table 30 Custom Event Attributes

| Attribute | Description |
|---|---|
| *Add incident definition* | Select to define an associated incident and then enter its *Name* and *Description*. |
| *Update incident details* | You can control how Entity updates the incidents as events are raised that are associated with the incident, select:<br>■ Update severity and details to match the most recent event.<br>■ Use the severity and details of the most severe event. |
| *Ageout* | Time period during which if the incident state is not updated the incident ages out and is closed. If the issue on the object recurs and Entuity raises another opening event within the set Expiry period Entuity also re-opens the original incident. |
| *Expiry* | Time period during which the closed incident state can be reopened if the issue on the object recurs and Entuity raises another opening event. After the expiry period if the issue on the object recurs and Entuity raises another opening event Entuity opens a new incident. |

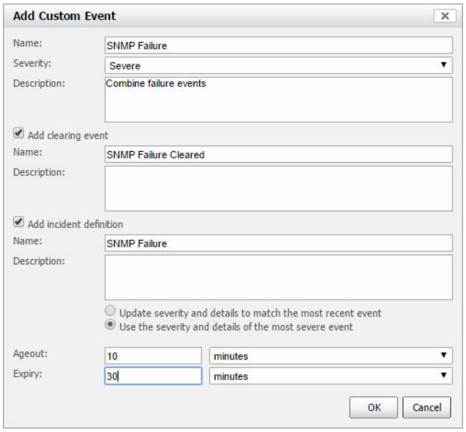
Table 30 Custom Event Attributes

To create a custom event:

1) Click **Administration** > **Events** > **Event Administration**.

2) Click **Events** and then **Add**.

3) Define the event attributes and any associated clearing event and incident.



Add Custom Event

Name: SNMP Failure

Severity: Severe

Description: Combine failure events

☑ Add clearing event

Name: SNMP Failure Cleared

Description:

☑ Add incident definition

Name: SNMP Failure

Description:

○ Update severity and details to match the most recent event

● Use the severity and details of the most severe event

Ageout: 10 minutes

Expiry: 30 minutes

Figure 121 Add Custom Events

## Rules and Processing Stages

Rules provide the logic underpinning the actions of the Event Management System. You can set conditions and tests to determine when a rule should be applied. You can also define one or more actions within a rule, for example to change event severity, discard events, run Groovy scripts.

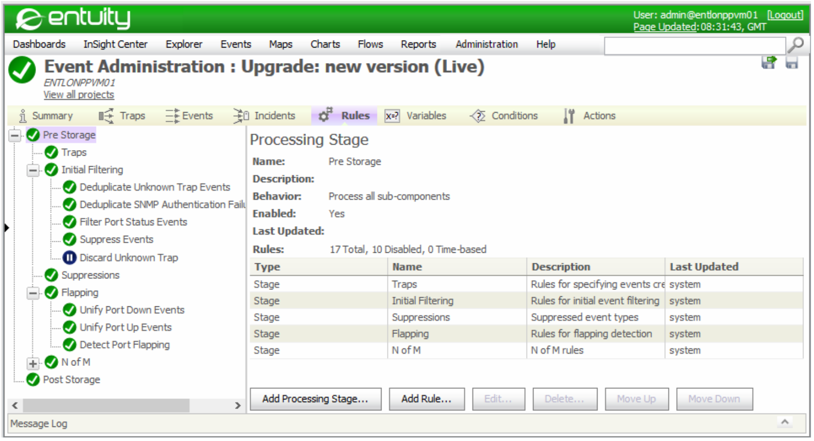
Entuity applies rules during the processing of events and divides this processing into two stages:

- Pre Storage, before events are saved to the database.
- Post Storage, after events are saved to the database.

Processing stages act as containers for rules, allowing you to put some structure and order on your rules. In the same way that you can set conditions and tests against rules which must be met before rules can run, you can set conditions and tests against processing stages before the rules in those stages can run (or at least be tested to run).

You can also choose to enable, or not, rules and processing stages. By default all of the supplied processing stages are enabled, as are most of the rules. The exceptions are the N of M rules which are not enabled. The enable state is indicated by its state icon, Tick for enabled, Paused for not.

For rules you can also define a schedule, which is the time period in which the rule can run. By default the supplied rules are not time-based, they do not have a schedule and so are always available to run, if enabled.



Event Administration : Upgrade: new version (Live)

ENTLONPPVM01

View all projects

Processing Stage

**Name:** Pre Storage

**Description:**

**Behavior:** Process all sub-components

**Enabled:** Yes

**Last Updated:**

**Rules:** 17 Total, 10 Disabled, 0 Time-based

| Type | Name | Description | Last Updated |
|---|---|---|---|
| Stage | Traps | Rules for specifying events cre | system |
| Stage | Initial Filtering | Rules for initial event filtering | system |
| Stage | Suppressions | Suppressed event types | system |
| Stage | Flapping | Rules for flapping detection | system |
| Stage | N of M | N of M rules | system |

Figure 122 Rules and Processing Stages

## Rule Types and Supplied Rules

The Event Management System supplied event project includes rules that you can apply to your event system. You can also refer to these rules when developing your own rules. Rules are based on a rule type, of which Event Management System has five.

| Rule Type | Supplied Rules |
|---|---|
| Deduplication | Deduplicate Enterprise Trap Events, SNMP Authentication Failure |
| Event Set Detection | - |
| Flapping Detection | Detect Port Flapping |

Table 31 Supplied Rules and their Rule Types

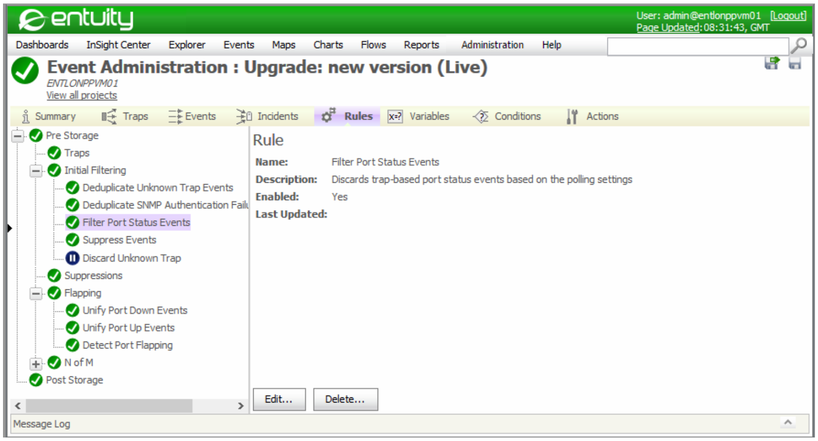
| Rule Type | Supplied Rules |
|---|---|
| Generic | Filter Port Status Event, Unify Port Up Events, Unify Port Down Events, Discard Unknown Trap |
| N of M Suppression | N of M for Processor Utilization |
| Trap Processing | - |

Table 31 Supplied Rules and their Rule Types

When developing rules consider:

- Which rule type is most appropriate to your task.
- When to apply the rule. The supplied rules are all processed during the Pre Storage stage of event processing but you can also develop rules to apply during the Post Storage stage.
- The order in which rules are applied, the order they are in the tree is the order in which they are applied. You can use drag and drop techniques to move both rules and processing stages.
- If the rules should always be available. You can:
  - Use the schedule feature to only apply a rule for a set period. For example you may define a rule that instructs Event Management System to discard all events for a 4 hour period from an area of your network because it is unavailable due to planned maintenance.
  - Enable and disable rules, and also the processing stages in which they sit. Rules that are in development should always be disabled, rules that you do not currently require you can disable rather than delete.

✓ Event Suppression rules can also be configured through a wholly separate process. The Suppress Events dialog is available from a context menu called from objects in the Explorer tree and Event Viewer.



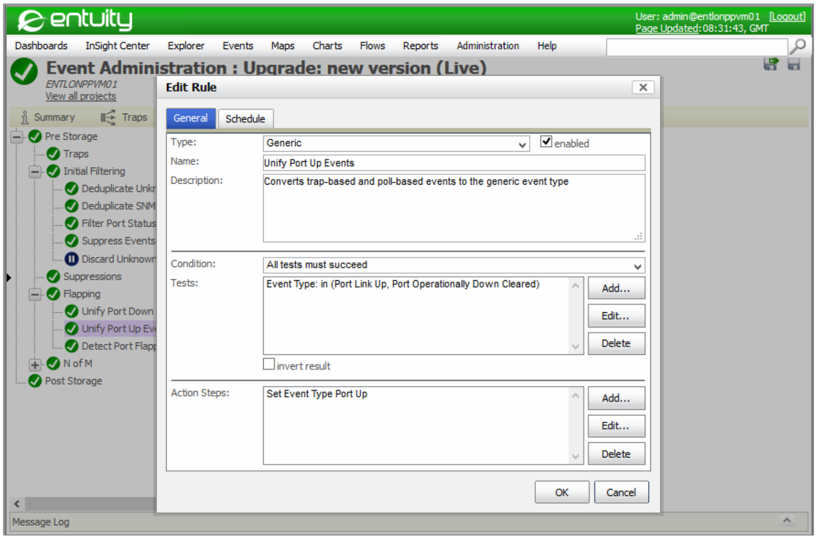
**Name:** Filter Port Status Events
**Description:** Discards trap-based port status events based on the polling settings
**Enabled:** Yes
**Last Updated:**

Figure 123 Event Management System Rules

## Generic Rule Type

The four task specific rules contain task specific algorithms, you should use the generic rule type when developing rules for tasks not requiring those algorithms. Event Management System includes these shipped rules that use the Generic rule type:

- Filter Port Status Event
- Unify Port Up Events
- Unify Port Down Events
- Discard Unknown Trap.



Type: Generic ☑ enabled
Name: Unify Port Up Events
Description: Converts trap-based and poll-based events to the generic event type
Condition: All tests must succeed
Tests: Event Type: in (Port Link Up, Port Operationally Down Cleared)
□ invert result
Action Steps: Set Event Type Port Up

Figure 124 Generic Rule Type

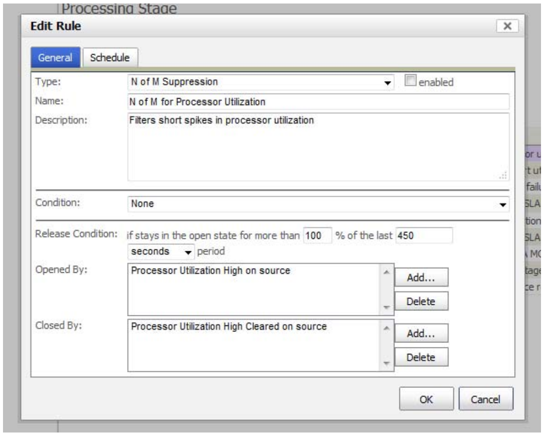
## N of M Rule Type

Event Management System allows suppression of events according to simple N of M rules, i.e. it only raises the event if the associated threshold is exceeded a defined percentage of the set time period. For example, a busy device may not respond to pings because it is prioritizing its core functionality. Entuity could then raise multiple spurious events indicating the device is down, followed by the next successful poll raising a clearing event. With N of M Entuity does not raise events each and every time a ping failure occurs, but instead calculates the percentage of time ping failures indicate the device was unreachable in a rolling window.

By setting sensible values for N and M spurious noise can therefore be reduced. After a threshold is crossed and an event raised one successful poll results in Entuity raising a clearing event. Entuity also resets the N of M count to zero.

Entuity provides 9 N of M rules, which are not enabled by default:

- Processor Utilization
- High Port Utilization
- IP SLA Test Failed
- IP SLA Test High Latency
- IP SLA Creation Failure
- IP SLA High ICPIF
- IP SLA Low MoS
- Network Outage
- Device Reachability.



Type: N of M Suppression ☐ enabled
Name: N of M for Processor Utilization
Description: Filters short spikes in processor utilization
Condition: None
Release Condition: if stays in the open state for more than 100 % of the last 450 seconds period
Opened By: Processor Utilization High on source
Closed By: Processor Utilization High Cleared on source

Figure 125 N of M for Processor Utilization

When defining N of M rules you should consider how often Entuity polls for the metric on the object. For example Entuity polls for CPU utilization every 5 minutes. When you wanted to raise an event when utilization was above the threshold for 15 minutes then you would set it to 100% of 15 minutes.

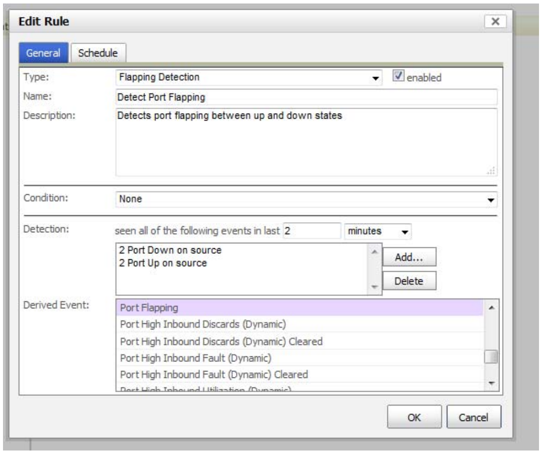
## Flapping Rule Type

Flapping rules detect a sequence of events, usually corresponding to a state oscillating between two values, for example the operational state of a physical port going up and down more than a defined number of times within a set period.

When Entuity detects the flapping condition it suppresses the original events and raises a new event to indicate the flapping state. The rule then continues to monitor the incoming events to determine when the flapping has ended and, when this happens, the most recently received incoming event is released and all suppression removed.

| Attribute | Description |
|---|---|
| *Type* | Rule type. |
| *Name* | Name of the rule. |
| *Description* | Description of the rule. |
| *Condition* | The condition is applied to *Tests*. Select:<br>- **None** for Entuity to always process the rule.<br>- **All tests must succeed** for Entuity to only process the rule when all tests are met.<br>- **At least one test must succeed** for Entuity to process the rule. |
| *Enabled* | Select to enable the rule. |
| *Tests* | Define the tests which are applied against the event. |
| invert result | Select to invert the result of a test, which is useful where the failure of the test is the correct outcome. The reported failure is inverted to reflect the real success of the test. |
| *Detection* | Defines the events, and number of those events that must be raised within the defined period for the source to be considered as flapping. |
| *Derived Event* | Derived Events are based upon existing event definitions within the Event Management System. They are raised by other events and actions in the Event Management System for example the Port Flapping event is raised according to rules applied to the Port Up and Port Down events. |

Table 32 Flapping Rule Type



Type: Flapping Detection ☑ enabled
Name: Detect Port Flapping
Description: Detects port flapping between up and down states
Condition: None
Detection: seen all of the following events in last 2 minutes
2 Port Down on source
2 Port Up on source
Derived Event:
Port Flapping
Port High Inbound Discards (Dynamic)
Port High Inbound Discards (Dynamic) Cleared
Port High Inbound Fault (Dynamic)
Port High Inbound Fault (Dynamic) Cleared
Port High Inbound Utilization (Dynamic)

Figure 126 Flapping Detection

## Deduplication Rule Type

You can use the deduplication rule type in situations where multiple events are raised from the same network object source and threaten to flood Event Management System. You can define the rule so it raises an event on the first occurrence of the event, but suppresses repeated occurrences of the event from that source until a defined period of time has elapsed and/or a releasing event is raised.

The Deduplicate Enterprise Trap Events rule is applied at the initial filtering stage and is enabled by default. It protects against a flood of enterprise traps from one source generating a flood of Enterprise Trap events that would overwhelm your capability to manage the network.

You can use the Deduplicate Enterprise Trap Events rule with its default settings to work through how Event Management System applies deduplication rules:

1) Entuity receives an Enterprise trap and creates an Enterprise Trap event.

2) Event Management System receives the Enterprise Trap event and applies the Deduplicate Enterprise Trap Events rule.

   As it is the first event from that source Event Management System saves the event to the database, raises the event in Event Viewer and also generates the associated incident.

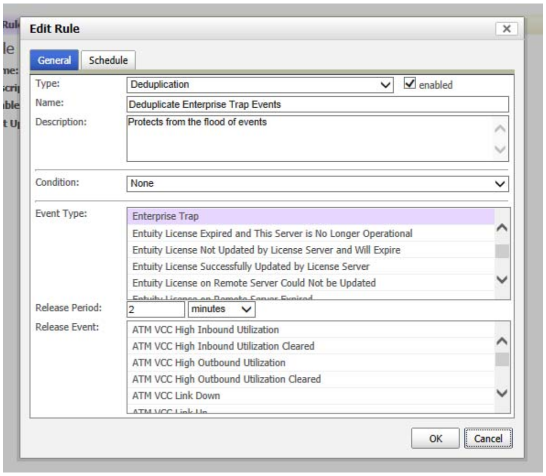
3) Within a second Entuity receives another Enterprise trap from the same source and it again creates an Enterprise Trap event.

4) Event Management System receives the Enterprise Trap event and applies the Deduplicate Enterprise Trap Events rule.

   As its has already raised an event from that source Event Management System checks whether the new event is within the set *Release Period*, by default 2 minutes. The event was raised within a second of the first event and is within the *Release Period*.

Event Management System therefore suppresses the event, it is not written to the database. Within Entuity there is no record of the event.

5) When 2 minutes have elapsed Event Management System raises the last suppressed event, if any.



Type: Deduplication ☑ enabled

Name: Deduplicate Enterprise Trap Events

Description: Protects from the flood of events

Condition: None

Event Type:
- Enterprise Trap
- Entuity License Expired and This Server is No Longer Operational
- Entuity License Not Updated by License Server and Will Expire
- Entuity License Successfully Updated by License Server
- Entuity License on Remote Server Could Not be Updated
- Entuity License on Remote Server Expired

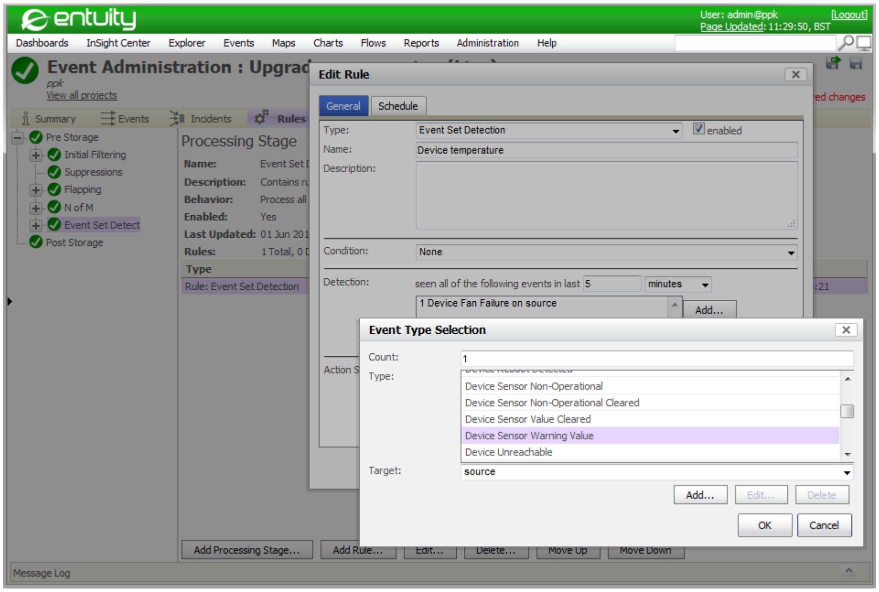
Release Period: 2 minutes

Release Event:
- ATM VCC High Inbound Utilization
- ATM VCC High Inbound Utilization Cleared
- ATM VCC High Outbound Utilization
- ATM VCC High Outbound Utilization Cleared
- ATM VCC Link Down
- ATM VCC Link Up

Figure 127 Deduplicate Enterprise Trap Events Rule

## Event Set Detection Rule Type

When you know that one type of event is likely to be followed by another type of event you can use the Event Set Detection rule to test for such an occurrence. For example, a fan failure event is likely to be followed by a high temperature warning event.



Type: Event Set Detection ☑ enabled
Name: Device temperature
Description:
Condition: None
Detection: seen all of the following events in last 5 minutes
1 Device Fan Failure on source
Add...

Count: 1
Type:
Device Sensor Non-Operational
Device Sensor Non-Operational Cleared
Device Sensor Value Cleared
Device Sensor Warning Value
Device Unreachable
Target: source

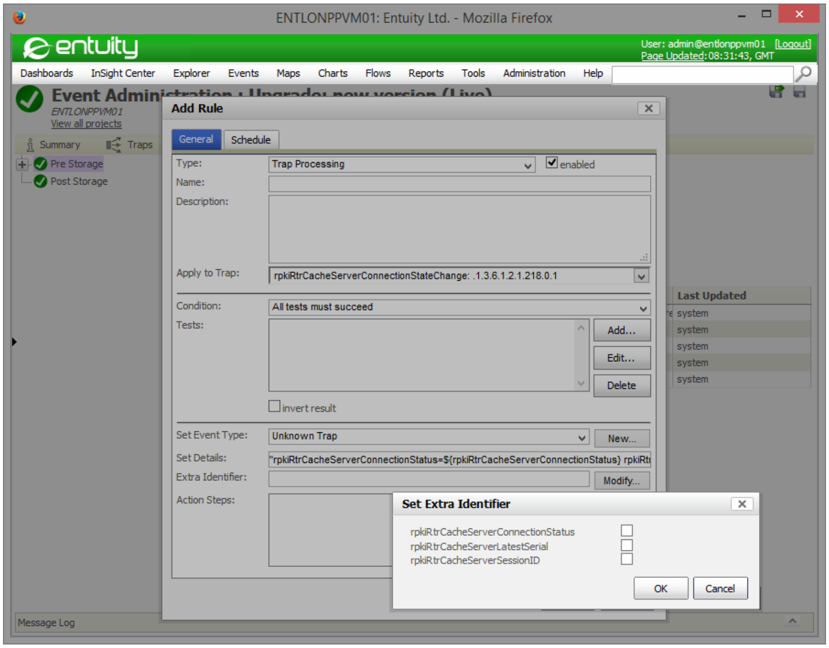
Figure 128 Event Set Detection

You can specify one or more actions to be carried out but only when each of a list of specific events are raised within a defined period of time are they performed.

## Trap Processing Rule Type

When you load a MIB Entuity parses the file and when instructed can interpret the trap definitions generating a new processing rule for each trap. You can then amend the rule if required. From the Rules page you can also create trap processing rules.

When creating custom events you can establish a varbind value as a contributor to the source identification of the trap. To prevent varbind values being automatically included as part of the source identifier *Extra Identifier* is not populated by default, however when you click Modify Entuity displays the available varbind values.



Add Rule

General | Schedule

Type: Trap Processing ☑ enabled

Name:

Description:

Apply to Trap: rpkiRtrCacheServerConnectionStateChange: .1.3.6.1.2.1.218.0.1

Condition: All tests must succeed

Tests:

Add... Edit... Delete

□ invert result

Set Event Type: Unknown Trap New...

Set Details: "rpkiRtrCacheServerConnectionStatus=${rpkiRtrCacheServerConnectionStatus} rpkiRt

Extra Identifier: Modify...

Action Steps:

Set Extra Identifier

rpkiRtrCacheServerConnectionStatus □
rpkiRtrCacheServerLatestSerial □
rpkiRtrCacheServerSessionID □

OK Cancel

Figure 129 Trap processing Rule

## Processing Stages

Entuity applies rules during the processing of events and splits this event processing into two stages; rules set in the:

- Pre Storage processing stage are applied before incoming events are saved to the database.
- Post Storage processing stage are applied after events are saved to the database but before incident processing.

Processing stages act as containers allowing you to put some structure and order on your rules. So, within the two root processing stages you can create sub processing stages, for example to contain rules:

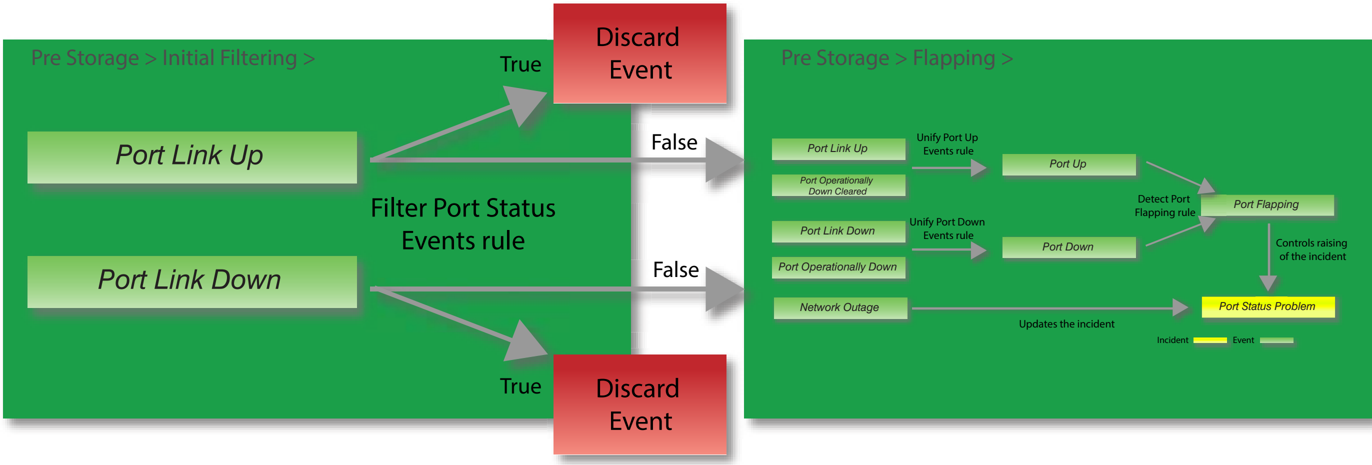
- Of the same type, the N of M folder contains all of the supplied N of M rules.
- Which work together to achieve a particular aim; the Flapping folder contains rules which detect port flapping.

In the same way that you can set conditions and tests against rules which must be met before the rule can run, you can set conditions and tests against processing stages before the rules in those stages can run (or at least be tested to run).

Entuity includes processing stages within the Pre and Post Storage root stages, you can also create stages to assist with rule management. Stages are processed from top to bottom so you should consider the relationship between different rules and stages. For example within the:

- Initial Filtering processing stage the Filter Port Status Events rule discards trap based port status events from those ports you have configured Entuity to ignore.
- Flapping processing stage the two unify rules both handle trap based port events.

It is more efficient that Entuity applies the port status filter rule first as it discards events from identified ports, if it were run after the flapping rules then the flapping rules would be processing events it would subsequently discard.



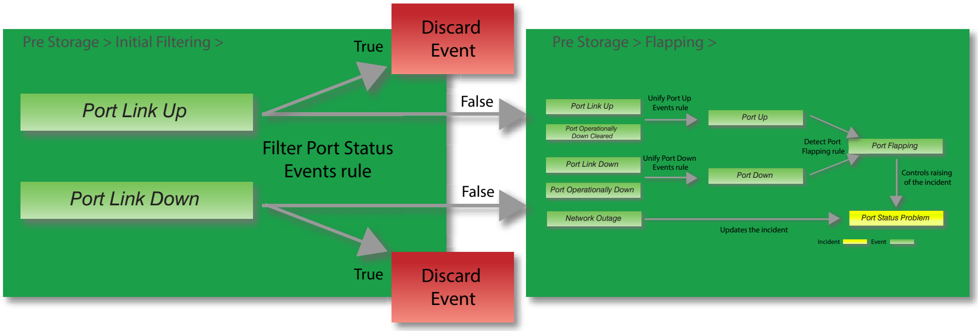


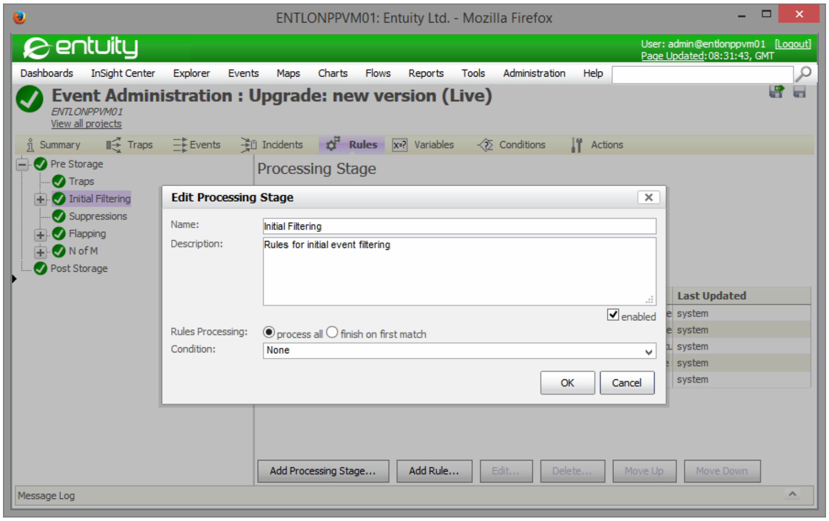
Figure 130 Filter Port Status Events Rule

| Attribute | Description |
|---|---|
| *Name* | Name of the processing stage. |
| *Description* | Enter a meaningful description of the stage, its purpose. |

Table 33 Processing Stage Attributes

| Attribute | Description |
|---|---|
| *Rules Processing* | Select:<br>- **process all** for Entuity to process all rules in the stage.<br>- **finish on first match** for Entuity to process the first rule that matches the set Condition. |
| *Condition* | The condition is applied to *Tests*. Select:<br>- **None** for Entuity to always process the rule.<br>- **All tests must succeed** for Entuity to only process the rule when all tests are met.<br>- **At least one test must succeed** for Entuity to process the rule. |
| *Enabled* | Select to enable the processing stage. |
| *Tests* | Define the tests which are applied against the event. |
| invert result | Select to invert the result of a test, which is useful where the failure of the test is the correct outcome. The reported failure is inverted to reflect the real success of the test. |

Table 33 Processing Stage Attributes



Edit Processing Stage

Name: Initial Filtering

Description: Rules for initial event filtering

☑ enabled

Rules Processing: ● process all ○ finish on first match

Condition: None

Figure 131 Configure a Processing Stage

## Event Attributes

Throughout the Event Management System you can access event attributes, for example to:

- Define actions that set the value of an attribute, for example the supplied flapping unify rules include a set event type action.
- Define conditions based on the testing of an attribute.

- Add additional information to the event and store it within the database. (See *Event Enrichment*.)
- Include in emails event details. (See *Send an Email Containing Event Attributes*.)

Entuity events and incidents share a standard set of attributes. You can also create your own attributes.

| Event Attribute | Description |
|---|---|
| *type* | The identifier of the event type or incident type. See the *Entuity Events Reference Manual* for a listing of identifiers. |
| *name* | The name of the event or incident. |
| *severity* | The severity level of the event or incident. |
| *reason* | The reason the event is raised, for example for an SNMP failure it may be 100% of 4 SNMP requests failed in the past 40 seconds. |
| *context* | Extra textual information for the event. It may include a description of the state object the was in before raising the event or some other environment description helpful in understanding the cause of the event. This field is not always present. |
| *reportId* | Identification of the process, which have sent the event. This field is not always present. |
| *source* | Source of the incidence within Entuity, for example `com.entuity.events.engine.groovy.InventoryObjectProxy@3c5` |
| *sourcecompleteIdString* | An internal identifier of the object within Entuity. Each component may have two identifiers, the separate identifier is the StormWorks identifier. |
| *sourceExternalId* | Additional textual identification for the object which may be useful in identifying objects which may not be represented by StormWorks. Values may be an IP address of the object, but may be any text. |
| *SourceName* | The name of the source object, it may be a resolved name or an IP address. |

Table 34 Event Attributes

## Send an Email Containing Event Attributes

When developing events and incidents, or becoming familiar with the Event Management System you may want to view values of the standard attributes associated with an event or incident.

This example uses a number of techniques:

- Variables to set the email recipient and to control when the email is sent.
- Variable Test condition.
- Send email action.
- Set the email throttle action. This allows the server to combine emails to the same recipient when they are raised within a defined period.

- Assign the email action to an incident.

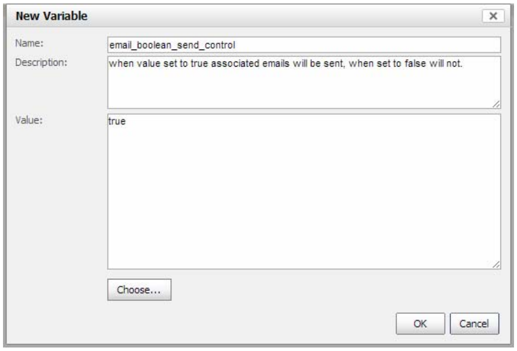
To define an incident that when raised triggers an email:

1) From Variables tab create two variables that will be used with the email action.

   `email_boolean_send_control` variable can contain one of two values, set *Value* to:

   - **true** when you want the email action it will be associated with to run.
   - **false** when you want the email action it will be associated with not to run.

   `email_network_admin` variable contains the email address of the recipient, for example set *Value* to "**james.smith@entuity.com**".


New Variable

Name: email_boolean_send_control

Description: when value set to true associated emails will be sent, when set to false will not.

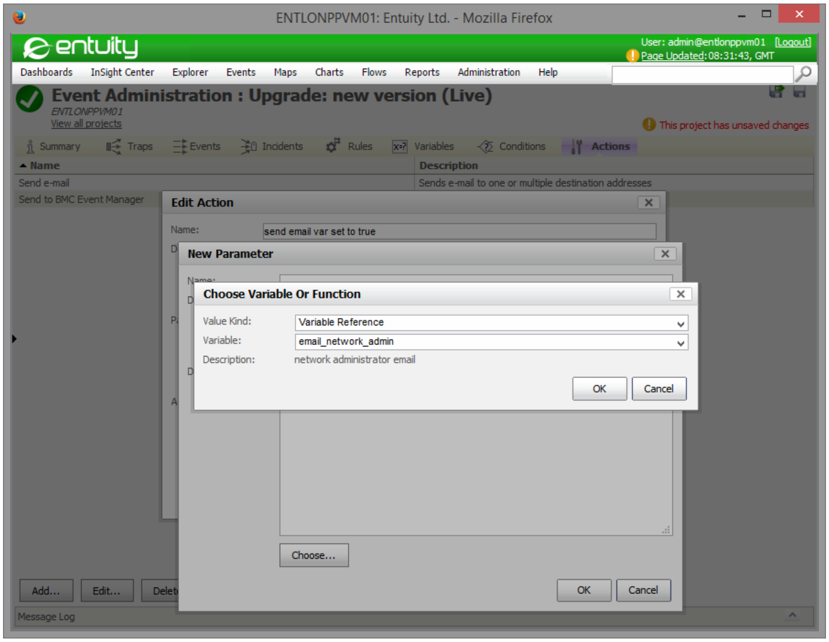
Value: true

Figure 132 Create Boolean Variables

2) From the Actions tab click **Add** and enter in *Name* and *Description* short and longer descriptions.

3) Enter the email parameter.

   Click **Choose** and select for *Value Kind* **Variable Reference** and in *Variable* select `email_network_admin`.



Event Administration : Upgrade: new version (Live)

ENTLONPPVM01

View all projects

This project has unsaved changes

| Name | Description |
|---|---|
| Send e-mail | Sends e-mail to one or multiple destination addresses |
| Send to BMC Event Manager | |

Edit Action

Name: send email var set to true

New Parameter

Choose Variable Or Function

Value Kind: Variable Reference

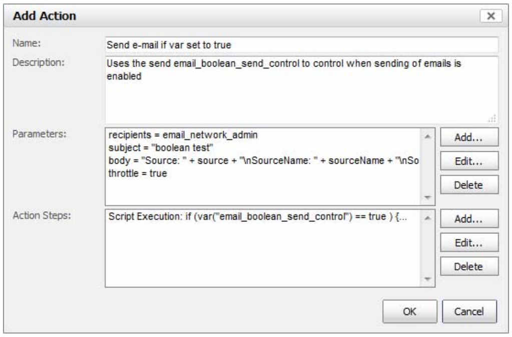
Variable: email_network_admin

Description: network administrator email

Figure 133 Choose Variable

4) Enter the body of the email. This example includes all standard attributes available against events and incidents, with each attribute labeled and starting on its own line:

```
"Source: " + source + "\nSourceName: " + sourceName + "\nSourceCompId-
String: " + sourceCompIdString + "\nSourceExternalId: " + sourceExter-
nalId + "\nContext:" + context + "\nType: " + type + "\nreportId: " +
reportId + "\nReason: " + reason
```



Add Action

Name: Send e-mail if var set to true

Description: Uses the send email_boolean_send_control to control when sending of emails is enabled

Parameters:

```
recipients = email_network_admin
subject = "boolean test"
body = "Source: " + source + "\nSourceName: " + sourceName + "\nSo
throttle = true
```

Action Steps: Script Execution: if (var("email_boolean_send_control") == true ) {...

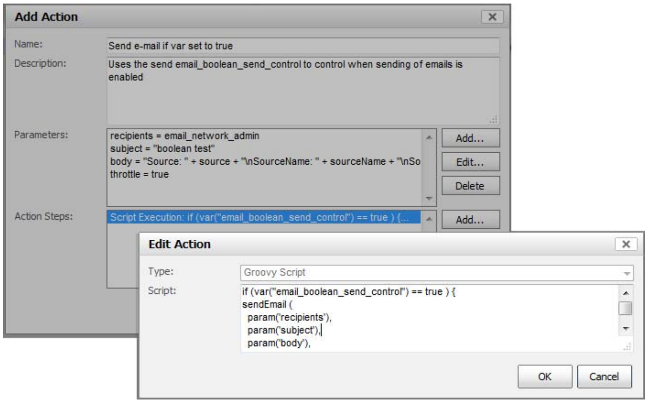
Figure 134 Add Action

5) Add throttle parameter and set it to true.

6) In Action Steps click **Add** and define a Groovy Script. This example tests that

`email_boolean_send_control` is set to true and within the `sendEmail` section specifies the email content.

```
if (var("email_boolean_send_control") == true ) {
sendEmail (
  param('recipients'),
  param('subject'),
  param('body'),
  param('throttle')
)
}
```



Add Action

Name: Send e-mail if var set to true

Description: Uses the send email_boolean_send_control to control when sending of emails is enabled

Parameters:

```
recipients = email_network_admin
subject = "boolean test"
body = "Source: " + source + "\nSourceName: " + sourceName + "\nSo
throttle = true
```

Action Steps: Script Execution: if (var("email_boolean_send_control") == true ) {...

Edit Action

Type: Groovy Script

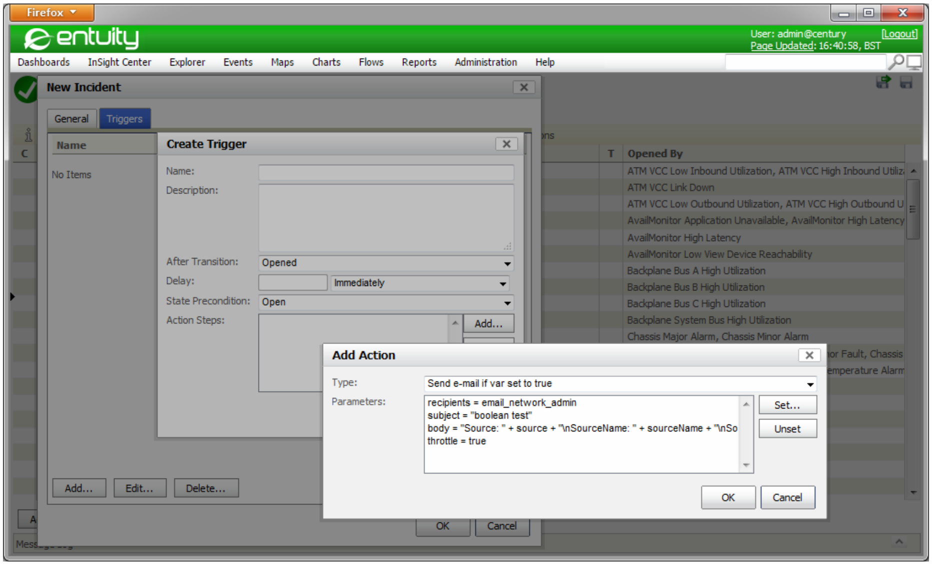
Script:

```
if (var("email_boolean_send_control") == true ) {
sendEmail (
 param('recipients'),
 param('subject'),
 param('body'),
```

Figure 135 Set Action Steps

7) Save the action.

This action is now available as a Named Action that you can select when adding triggers to incidents.



Firefox
entuity
User: admin@century [Logout]
Page Updated: 16:40:58, BST
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Administration
Help
New Incident
General
Triggers
Name
No Items
Add...
Edit...
Delete...
OK
Cancel
Create Trigger
Add...
Opened By
ATM VCC Low Inbound Utilization, ATM VCC High Inbound Utiliz
ATM VCC Link Down
ATM VCC Low Outbound Utilization, ATM VCC High Outbound U
AvailMonitor Application Unavailable, AvailMonitor High Latency
AvailMonitor High Latency
AvailMonitor Low View Device Reachability
Backplane Bus A High Utilization
Backplane Bus B High Utilization
Backplane Bus C High Utilization
Backplane System Bus High Utilization
Chassis Major Alarm, Chassis Minor Alarm
Add Action
Set...
Unset
OK
Cancel

Name:

Description:

After Transition: Opened

Delay: Immediately

State Precondition: Open

Action Steps:

Type: Send e-mail if var set to true

Parameters:

```
recipients = email_network_admin
subject = "boolean test"
body = "Source: " + source + "\nSourceName: " + sourceName + "\nSo
throttle = true
```

Figure 136 Add Named Action to an Incident Trigger

## Event Enrichment

Events include a standard set of attributes, for example `source`, `name`, `severity`. You can add additional information to the event and store it within the database.

This example involves:

- Creation of a Pre Storage Generic processing stage and rule.
- An Event Type Test matching on the Port Speed Change event type.
- A new Database attribute to hold the location of a port.
- Groovy script which navigates the Entuity type hierarchy to identify a port's location through attributes held against its device:

  `source.device.sysLocation`

You can use the Entuity Data Dictionary tool to view the Entuity data model. It is available through a hyperlink from **Help** > **Contents**.

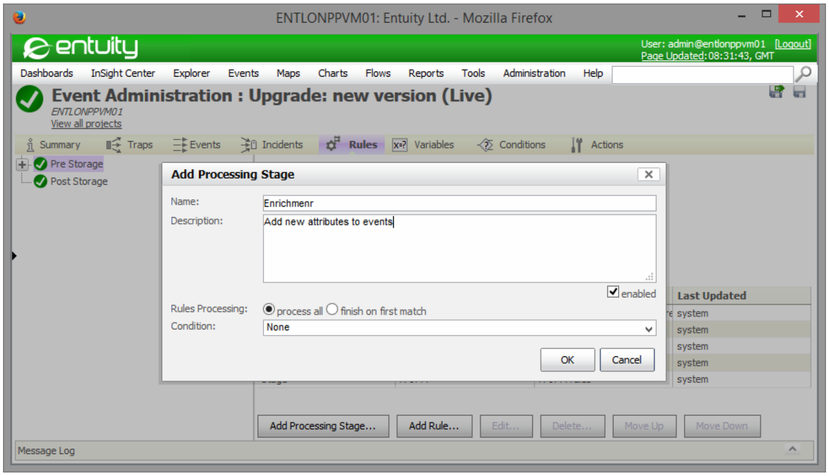
To define a rule which adds location to a the Port Speed Change event:

1) Click **Administration** > **Events** > **Event Administration**.

2) Click **Incidents.**

3) Highlight Pre Storage and from the context menu click **Add Processing Stage**.

   Define the stage, call it Enrichment.


ENTLONPPVM01: Entuity Ltd. - Mozilla Firefox
entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 08:31:43, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Event Administration : Upgrade: new version (Live)
ENTLONPPVM01
View all projects
Summary Traps Events Incidents Rules Variables Conditions Actions
Pre Storage
Post Storage
Last Updated
system
system
system
system
system
Add Processing Stage... Add Rule... Edit... Delete... Move Up Move Down
Message Log

Add Processing Stage

Name: Enrichmenr

Description: Add new attributes to events

☑ enabled

Rules Processing: ● process all ○ finish on first match

Condition: None

OK Cancel

Figure 137 Add Processing Stage

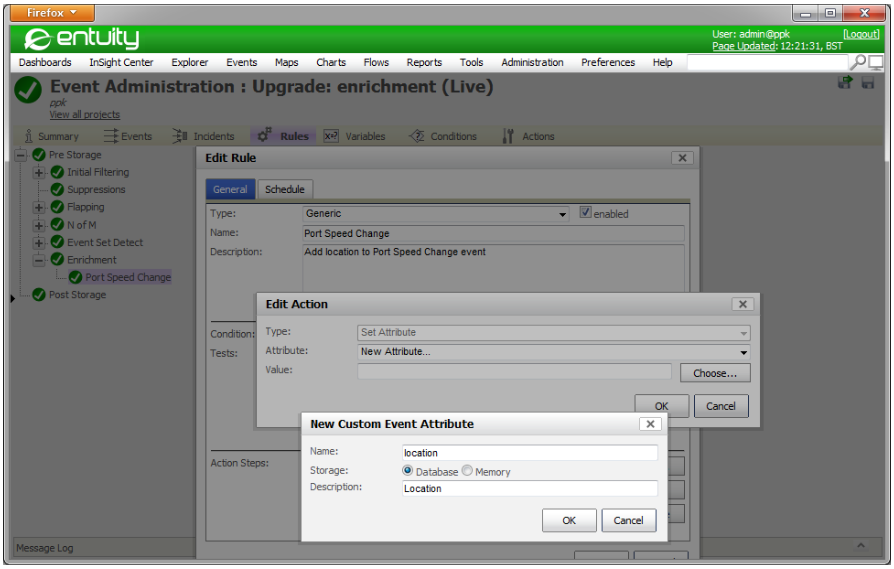
4) Highlight the Enrichment stage and from the context menu select **Add Rule**. Set:

- Type to Generic and enter a meaningful name and description for the rule.
- Condition to All tests must succeed and add an Event Type Test that matches on Port Speed Change.

5) From Action Steps click **Add** and from:

- *Type* select Set Attribute
- Attribute Select **New Attribute**. For the custom event attribute enter a name, set *Storage* to **Database** and enter a description. The description is the display name.
- *Value* enter:

```
source.device.sysLocation
```



Event Administration : Upgrade: enrichment (Live)

ppk

View all projects

Edit Rule

Type: Generic ☑ enabled

Name: Port Speed Change

Description: Add location to Port Speed Change event

Condition:

Tests:

Action Steps:

Edit Action

Type: Set Attribute

Attribute: New Attribute...

Value:

New Custom Event Attribute

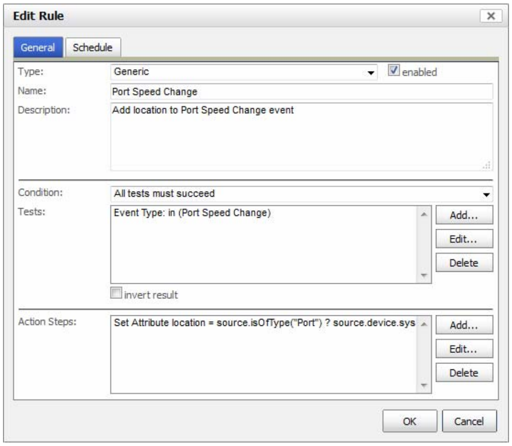
Name: location

Storage: ● Database ○ Memory

Description: Location

Figure 138 Custom Event Attribute

6) Click **OK** to save the rule.



Edit Rule

Type: Generic ☑ enabled

Name: Port Speed Change

Description: Add location to Port Speed Change event

Condition: All tests must succeed

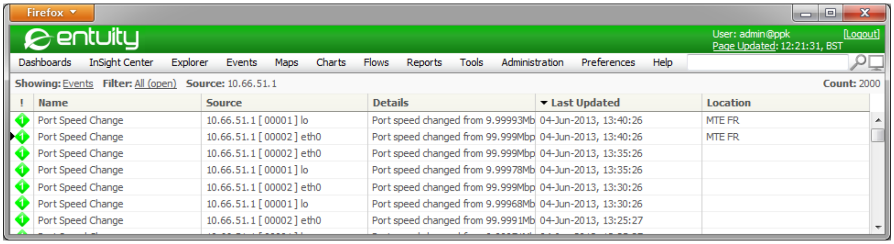
Tests: Event Type: in (Port Speed Change)

□ invert result

Action Steps: Set Attribute location = source.isOfType("Port") ? source.device.sys

Figure 139 Edit Generic Rule

7) After saving and deploying the event project to view the new attribute in Event Viewer you must configure its columns. Port Speed Change events raised after the event project deployment include their location, events raised before do not.


Firefox
entuity
User: admin@ppk [Logout]
Page Updated: 12:21:31, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Preferences Help

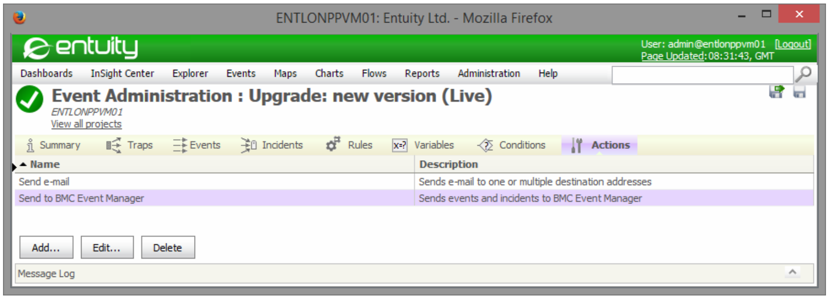
Showing: Events Filter: All (open) Source: 10.66.51.1 Count: 2000

| ! | Name | Source | Details | Last Updated | Location |
|---|---|---|---|---|---|
|  | Port Speed Change | 10.66.51.1 [ 00001 ] lo | Port speed changed from 9.99993Mb | 04-Jun-2013, 13:40:26 | MTE FR |
|  | Port Speed Change | 10.66.51.1 [ 00002 ] eth0 | Port speed changed from 99.999Mbp | 04-Jun-2013, 13:40:26 | MTE FR |
|  | Port Speed Change | 10.66.51.1 [ 00002 ] eth0 | Port speed changed from 99.999Mbp | 04-Jun-2013, 13:35:26 |  |
|  | Port Speed Change | 10.66.51.1 [ 00001 ] lo | Port speed changed from 9.99978Mb | 04-Jun-2013, 13:35:26 |  |
|  | Port Speed Change | 10.66.51.1 [ 00002 ] eth0 | Port speed changed from 99.999Mbp | 04-Jun-2013, 13:30:26 |  |
|  | Port Speed Change | 10.66.51.1 [ 00001 ] lo | Port speed changed from 9.99968Mb | 04-Jun-2013, 13:30:26 |  |
|  | Port Speed Change | 10.66.51.1 [ 00002 ] eth0 | Port speed changed from 99.9991Mb | 04-Jun-2013, 13:25:27 |  |

Figure 140 Enriched Events in Event Viewer

# Actions

You can associate actions against an incident and the incident then triggers the actions, depending upon any set conditions being met. You can also set actions within rules, rules are applied during the processing of events. Every event rule has to have some sort of operation included in its definition.


ENTLONPPVM01: Entuity Ltd. - Mozilla Firefox
entuity
User: admin@entlonppvm01 [Logout]
Page Updated:08:31:43, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
Event Administration : Upgrade: new version (Live)
ENTLONPPVM01
View all projects
Summary Traps Events Incidents Rules Variables Conditions Actions
Add... Edit... Delete
Message Log

| Name | Description |
|---|---|
| Send e-mail | Sends e-mail to one or multiple destination addresses |
| Send to BMC Event Manager | Sends events and incidents to BMC Event Manager |

Figure 141 Event Management System Actions

Entuity includes a set of action types that you can use to build your rules, or action steps in incident triggers. When you can define your own Custom Actions they are available for use from the same menus as Standard Actions.

| Action Type | Description |
|---|---|
| Create Event | Generates a new event type based upon the selected event type and uses the same source. This new event is processed in addition to the original event. Any of the standard attributes can be set and new ones defined. |
| Decrease Severity | Decreases the severity by one level. |
| Derive Event | Generates a new event type based upon the selected event type and uses the same source as the original. This new event is processed in addition to the original event, and raised events maintain a relationship to the original events. For example selecting Show Details on the derived event also shows the details of the original events.<br>Any of the standard attributes can be set and new ones defined. |

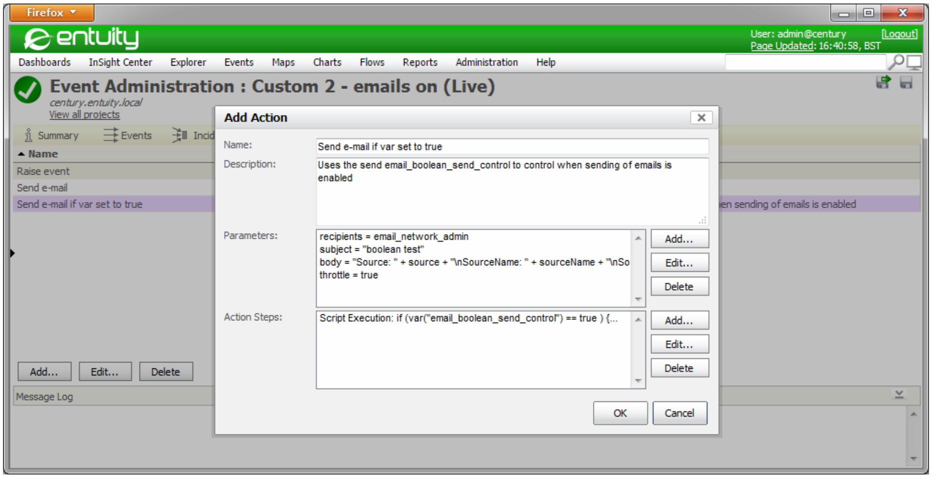
Table 35 Standard Action Types

| Action Type | Description |
|---|---|
| Discard Event | Discards the current event. An example of its use is in the Pre-Storage rule Filter Port Status Events where trap-based events are not raised against ports where *Status Events* is set to **No**.<br>An event discarded at the Pre-Storage stage is not saved to the database or forwarded to other external and internal event handlers; there is no record of the event being raised. |
| Groovy Script | Expressions developed using Groovy Script; an object oriented programming language for the Java platform. Through Groovy you can access the database, for example the Filter Port Status Events rule evaluates whether Entuity is configured to raise status events against the current port. |
| Increase Severity | Increments the severity by one level. |
| Process | Allows Entuity to execute a process, utility or script as though it were run from the command line. You can pass parameters to a process using a configurable list of arguments. |
| Set Attribute | You can set a value against a new or existing event or incident attribute, this enrichment is through 2 attribute types: (See *Event Attributes*.)<br>■ Database attributes which are stored in the database, are visible in the Event Viewer and available to forward to third party integrations.<br>■ Memory attributes which exist only for the duration of the event processing. You can use them to pass values between rules.<br>You can assign static values to attributes or access the database values, variables and function calls. For example, an event related to a device might look up the location of that device and include it in one of the event attributes. |
| Set Event Type | Allows you to change the event type. This action is used with the unify rules used in the default flapping solution. For example the Port Link Down and Port Operationally Down events have their event type amended to Port Down. |
| Set Severity | Enter the internal severity level values to reset the current event:<br>2, Information or Cleared<br>4, Minor<br>6, Major<br>8, Severe<br>10, Critical. |

Table 35 Standard Action Types

The standard configuration is delivered with two Custom Actions:

- For sending email. When you review the definition of this action you can see it is produced using Groovy script. This script forms the basis of the email example. (See *Send an Email Containing Event Attributes*.)
- For forwarding events and incidents to BMC TrueSight Infrastructure Management Servers. (See *Chapter 30 - TrueSight Operations Management Integration*.)


Firefox
entuity
User: admin@century [Logout]
Page Updated: 16:40:58, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help

Event Administration : Custom 2 - emails on (Live)

century.entuity.local

View all projects
Summary
Events
Incid
Name

Raise event

Send e-mail

Send e-mail if var set to true

Add... Edit... Delete
Message Log
Add Action

Name: Send e-mail if var set to true

Description: Uses the send email_boolean_send_control to control when sending of emails is enabled

Parameters:

```
recipients = email_network_admin
subject = "boolean test"
body = "Source: " + source + "\nSourceName: " + sourceName + "\nSo
throttle = true
```

Action Steps:

```
Script Execution: if (var("email_boolean_send_control") == true ) {...
```

Figure 142 Adding Actions

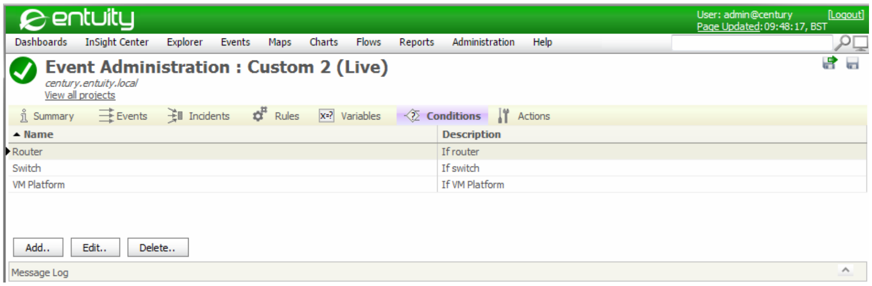
## Conditions and Tests

A condition is a key component of a rule; it tests whether a rule is appropriate to the current event and therefore whether the actions within it should be applied. When a condition is not specified then the rule is always applied. You can combine conditions to make more complex tests. When combining conditions you can determine how strict the test is that Entuity applies:

- **All tests must succeed**, requires that all of the conditions are met by the event.
- **At least one test must succeed**, the test is passed when the first condition is passed.

You can also invert the result of a test, which is useful where the failure of the test is the correct outcome. The reported failure is inverted to reflect the real success of the test. You can also invert the outcome of a combination of conditions.

For conditions that you may want re-use you should define them from the Conditions page. When you set rules and triggers you can select these saved conditions. It also allows you to globally change a condition. You also have the option of specifying a condition within a rule or trigger.



Event Administration : Custom 2 (Live)

century.entuity.local

View all projects

| Name | Description |
|---|---|
| Router | If router |
| Switch | If switch |
| VM Platform | If VM Platform |

Figure 143 Event Management System Conditions

| Test Type | Description |
|---|---|
| Event Attribute Test | All events share a set of standard attributes. You can select an attribute and compare its value to a set value, using one of the comparison operators. Each attribute has tooltip help. |
| Event Severity Test | Enter the severity level to test events against. This is the internal numeric severity level, valid values are:<br>2, Information or Cleared<br>4, Minor<br>6, Major<br>8, Severe<br>10, Critical. |
| Event Type Test | Select an event type to test against. |
| Groovy Script | Expressions developed using Groovy Script; an object oriented programming language for the Java platform. Through Groovy you can access the database, for example the Filter Port Status Events rule evaluates whether Entuity is configured to raise status events against the current port. |
| Incident Attribute Test | All incidents share a set of standard attributes. You can select an attribute and compare its value to a set value, using one of the comparison operators. Each attribute has tooltip help. |
| Incident Severity Test | Enter the severity level to test incidents against. This is the internal numeric severity level, valid values are:<br>2, Information or Cleared<br>4, Minor<br>6, Major<br>8, Severe<br>10, Critical. |
| Incident Type Test | Select one or more incident types to test against. |
| IP Test | Allows the management IP to be compared to a specified IP, and IP range or a subnet using either a mask or mask length. |

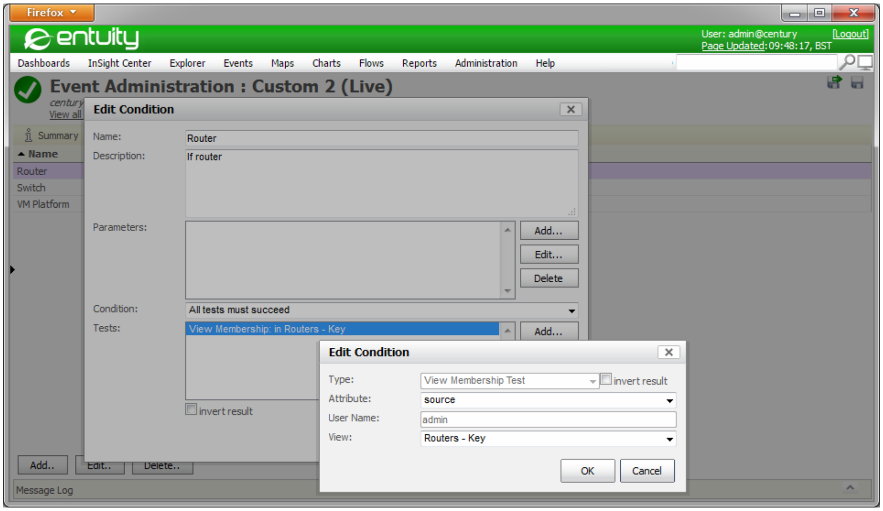
Table 36 Standard Conditions

| Test Type | Description |
|---|---|
| Trap Varbind Test | Allows you to test varbind name values, for example the value may determine the event type to raise. When you select Trap Varbind Test Entuity allows you to:<br>- Select the Varbind from a drop down list of varbinds loaded with the MIB.<br>- Select the Operation, e.g. equals, greater than.<br>- Enter the comparison value. |
| Variable Test | Tests the value of a variable. |
| View Membership Test | Tests whether the event is raised from an object within the selected view. |

Table 36 Standard Conditions

## View Membership Test

The view membership tests that the managed object is in the specified view. Specify a view against which you test whether the source of the current event is a member. You can therefore apply actions to sets of objects that you have already segregated, for example the key routers on a particular network.



Edit Condition

Name: Router

Description: If router

Parameters:

Condition: All tests must succeed

Tests: View Membership: in Routers - Key

□ invert result

Edit Condition

Type: View Membership Test □ invert result

Attribute: source

User Name: admin

View: Routers - Key

Figure 144 View Membership Condition

## Variable Test

Variable test is intended for test and debug scenarios and allows the contents of a project variable to be checked to enable or disable one or more rules.

# Variables

From the Variables page you can create variables to use within the Event Management System. This allows an administrator to make a single change and have that picked up by multiple rules. For example:

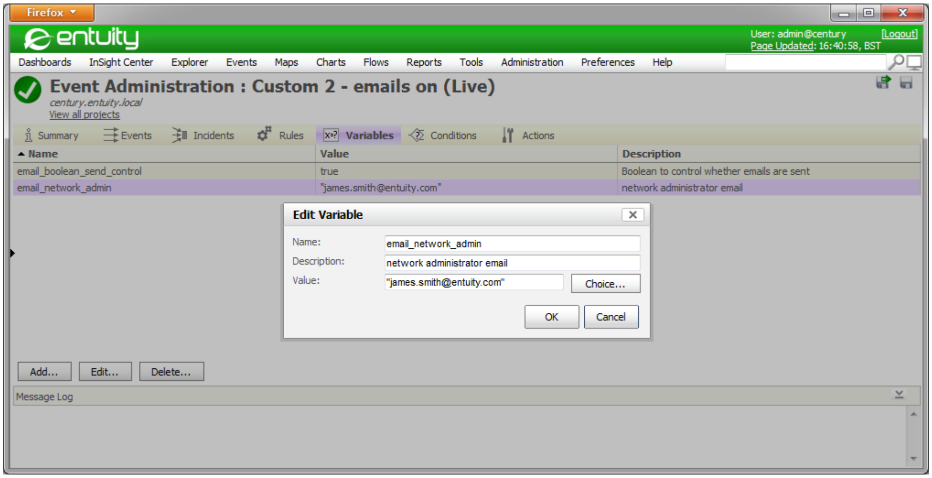
- Instead of typing into each action that sends an email the email address you can create a variable that contains the email address. If the email address changes you can update the variable and all of the actions that use the variable are also updated.
- You may want to control when particular actions are enabled. For example with the sending of emails you could add a test against a variable, so only when the variable contains the value true would the email be generated.

When defining a variable enter a Name and Description along with the Value. Value must be entered in a format suitable for Groovy syntax:

- Numbers are entered verbatim, e.g. 1.
- Strings are enclosed within quotes, e.g. "James.Smith@entuity.com".

Scripts written for the Entuity Configuration Management module do not have their variable values enclosed in quotes.

When you are familiar with Groovy syntax you can develop variables that have a more sophisticated background, for example the product of logical operations on values from the database, events and incidents.


Firefox
entuity
User: admin@century [Logout]
Page Updated: 16:40:58, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Preferences Help
Summary Events Incidents Rules Variables Conditions Actions
Add... Edit... Delete...
Message Log

Event Administration : Custom 2 - emails on (Live)
century.entuity.local
View all projects

| Name | Value | Description |
|---|---|---|
| email_boolean_send_control | true | Boolean to control whether emails are sent |
| email_network_admin | "james.smith@entuity.com" | network administrator email |

Edit Variable

Name: email_network_admin
Description: network administrator email
Value: "james.smith@entuity.com" Choice...

OK Cancel

Figure 145 Event Management System Variables

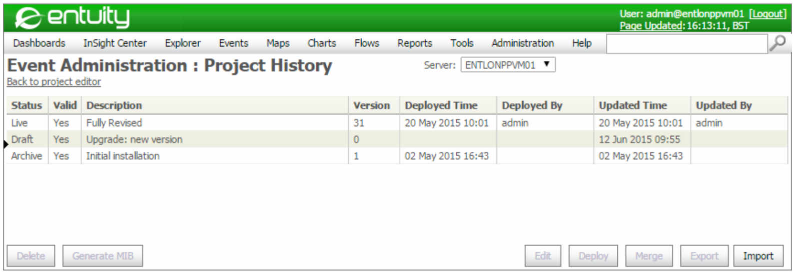
# 28 Event Management System Administration

The changes you make to an event project only configure the Event Management System once you save and deploy the project. The currently deployed project is the Live project. Event projects can be:

- Live, the project is currently applied to the Event Management System.
- Draft, the project is different from the current live project, it is saved to the server but it has never been deployed to the server. You can have more than one draft project and you can delete them from the system.
- Archived, the project was once applied to the server but it is not currently applied. Archived projects are retained to allow you to re-instate a previous event project. You can delete archived event projects, although not the initial project supplied with Entuity.

Entuity lists the event project history for the current Entuity server. When the server has remote Entuity servers you can access the event project history of a remote sever by selecting it from the *Server* drop-down list. You can then edit and export projects on the remote server, you can also export projects to the remote server.

Entuity also allows you to merge any two selected projects. The event project merge function identifies differences between two selected event projects and allows you to select the required version of each conflict. When the merge is complete you have a new event project, the two source event projects remain unchanged.



Event Administration : Project History

Server: ENTLONPPVM01

| Status | Valid | Description | Version | Deployed Time | Deployed By | Updated Time | Updated By |
|---|---|---|---|---|---|---|---|
| Live | Yes | Fully Revised | 31 | 20 May 2015 10:01 | admin | 20 May 2015 10:01 | admin |
| Draft | Yes | Upgrade: new version | 0 | | | 12 Jun 2015 09:55 | |
| Archive | Yes | Initial installation | 1 | 02 May 2015 16:43 | | 02 May 2015 16:43 | |

Figure 146 Event Project History

## Deploy Event Projects

An event project is not applied to your Event Management System until you deploy it. You can deploy draft projects, which have never been installed to the server, and also archived projects which have been previously deployed. You can also deploy event projects imported from other Entuity servers.

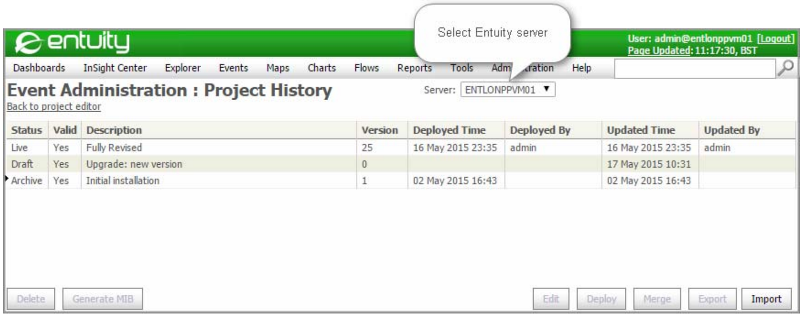
You can deploy a project from:

- The Project History page which lists all of the event projects on Entuity.
- Any of the Event Administration pages on which you have an event project open. You can use the **Save and Deploy** button.

To deploy a project using the Project History page:

1) Click **Administration** > **Events** > **Event Administration**.

2) Click **View all projects**. Entuity lists the event project history.

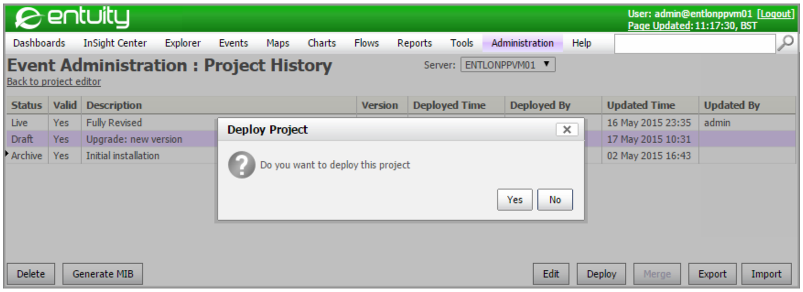

entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 11:17:30, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Select Entuity server
Server: ENTLONPPVM01
Back to project editor
Delete
Generate MIB
Edit
Deploy
Merge
Export
Import

Event Administration : Project History

| Status | Valid | Description | Version | Deployed Time | Deployed By | Updated Time | Updated By |
|---|---|---|---|---|---|---|---|
| Live | Yes | Fully Revised | 25 | 16 May 2015 23:35 | admin | 16 May 2015 23:35 | admin |
| Draft | Yes | Upgrade: new version | 0 | | | 17 May 2015 10:31 | |
| Archive | Yes | Initial installation | 1 | 02 May 2015 16:43 | | 02 May 2015 16:43 | |

Figure 147 Event Project List

3) Highlight the project to deploy and click **Deploy**. Confirm that you want to deploy the project.


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 11:17:30, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Server: ENTLONPPVM01
Back to project editor
Deploy Project
Yes
No
Delete
Generate MIB
Edit
Deploy
Merge
Export
Import

Event Administration : Project History

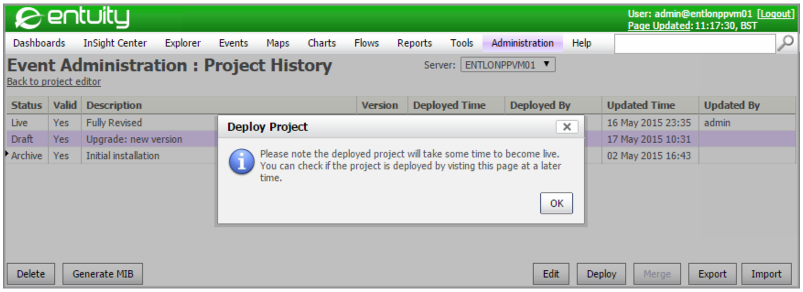
| Status | Valid | Description | Version | Deployed Time | Deployed By | Updated Time | Updated By |
|---|---|---|---|---|---|---|---|
| Live | Yes | Fully Revised | | | | 16 May 2015 23:35 | admin |
| Draft | Yes | Upgrade: new version | | | | 17 May 2015 10:31 | |
| Archive | Yes | Initial installation | | | | 02 May 2015 16:43 | |

Do you want to deploy this project

Figure 148 Event Project Deploy

4) Entuity warns you that event project deployment may take some time.

After the project is deployed you can use the Events Health page to check time taken to deploy.


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 11:17:30, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Server: ENTLONPPVM01
Back to project editor
Deploy Project
OK
Delete
Generate MIB
Edit
Deploy
Merge
Export
Import

Event Administration : Project History

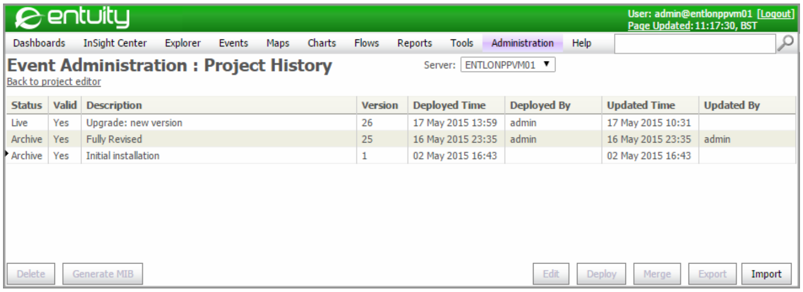
| Status | Valid | Description | Version | Deployed Time | Deployed By | Updated Time | Updated By |
|---|---|---|---|---|---|---|---|
| Live | Yes | Fully Revised | | | | 16 May 2015 23:35 | admin |
| Draft | Yes | Upgrade: new version | | | | 17 May 2015 10:31 | |
| Archive | Yes | Initial installation | | | | 02 May 2015 16:43 | |

Please note the deployed project will take some time to become live. You can check if the project is deployed by visting this page at a later time.

Figure 149 Deploy Event Project Notification

5) When the event project is deployed Entuity updates:

   - Its status to Live, assigns a version number and record when and who made the deployment.
   - The previous project’s status to Archive.



Event Administration : Project History

| Status | Valid | Description | Version | Deployed Time | Deployed By | Updated Time | Updated By |
|---|---|---|---|---|---|---|---|
| Live | Yes | Upgrade: new version | 26 | 17 May 2015 13:59 | admin | 17 May 2015 10:31 | |
| Archive | Yes | Fully Revised | 25 | 16 May 2015 23:35 | admin | 16 May 2015 23:35 | admin |
| Archive | Yes | Initial installation | 1 | 02 May 2015 16:43 | | 02 May 2015 16:43 | |

Figure 150 Event Project History

Each event project has its own unique number that Entuity generates when it deploys the project.

## Delete Event Projects

You can delete all event projects, apart from the currently live project or one that you editing but have not saved. If you have made changes to an event project that you have not saved then when you log out of Entuity those changes are lost.

To delete an event project:

1) Click **Administration** > **Events** > **Event Administration**.

2) Click **View all projects**.

   Entuity lists the event project history for the current Entuity server. When the server has remote Entuity servers you can access the event project history of a remote sever by selecting it from the *Server* drop-down list.

3) Highlight the project and click **Delete**. When you confirm that you want to delete the project Entuity deletes it.

## Import and Export Event Projects

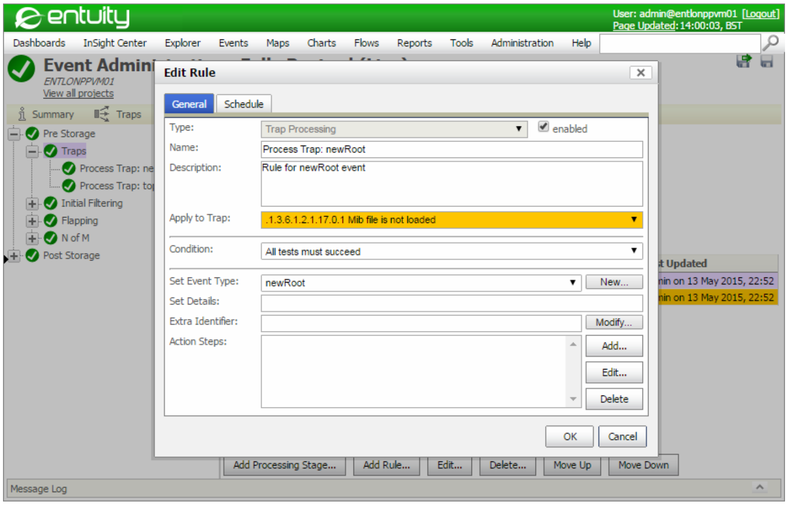
The default event project definition is defined in *entuity_home*`\etc\eventProject.xml`. When you want to transfer an event project configuration from one Entuity server to another you export the event configuration from the first server to an XML file and then import that XML file to the second server. You then have the option of merging the two project files.

Before importing and exporting event projects:

- You should ensure the exporting Entuity and importing Entuity servers are running the same version of the Entuity software.

- If you have defined trap management rules then the receiving server must also have the same MIB files and parsed MIB files. If they are not present then Entuity will highlight the impacted rules and depending upon the trap configuration Entuity may fail to generate the trap.

  You can copy the MIB files and parsed MIB files from the export server directly to the import server. If you have placed the files into the correct folders then you must stop and restart the importing Entuity server for it to recognize the parsed MIBs.



User: admin@entlonppvm01 [Logout]
Page Updated: 14:00:03, BST

Edit Rule

Type: Trap Processing ☑ enabled
Name: Process Trap: newRoot
Description: Rule for newRoot event
Apply to Trap: .1.3.6.1.2.1.17.0.1 Mib file is not loaded
Condition: All tests must succeed
Set Event Type: newRoot
Set Details:
Extra Identifier:
Action Steps:

Figure 151 Missing MIB Files

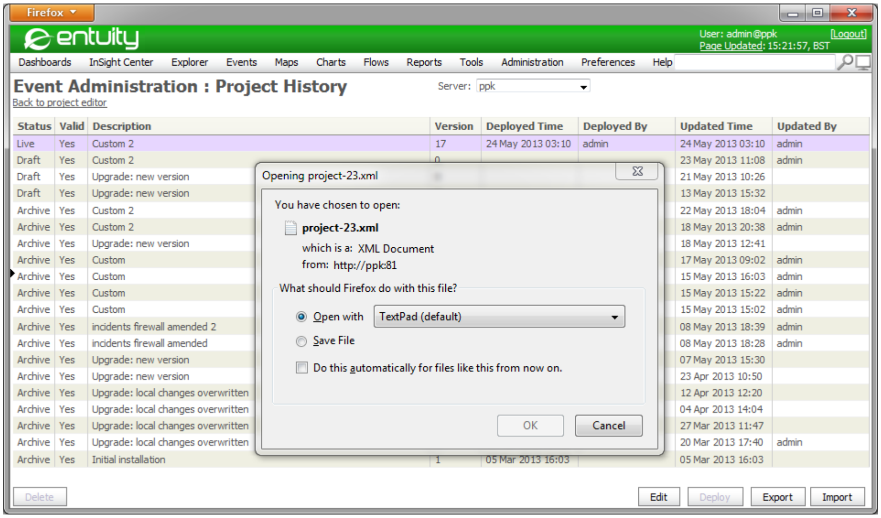
## Copy Event Projects Between Servers

The import and export of event project files allows you to copy Event Management System configurations between Entuity servers. You should:

- Ensure the servers are running the same version of Entuity.
- Review all of the event projects on your servers. There maybe bespoke configurations that you want to retain on individual servers, or include to other servers. Where event projects have diverged across servers you should consider creating one project with all of the required configurations and then using it to apply changes across all of your servers.

To copy event projects between Entuity servers:

1) From the export server click **Administration** > **Events** > **Event Administration**.
2) Click **View all projects**. You can highlight any project for export.
3) Highlight the required project and click **Export**.
4) Entuity generates a unique filename and prompts you to open or save the project file. Save the file.



Event Administration : Project History

Back to project editor

Server: ppk

| Status | Valid | Description | Version | Deployed Time | Deployed By | Updated Time | Updated By |
|---|---|---|---|---|---|---|---|
| Live | Yes | Custom 2 | 17 | 24 May 2013 03:10 | admin | 24 May 2013 03:10 | admin |
| Draft | Yes | Custom 2 | 0 | | | 23 May 2013 11:08 | admin |
| Draft | Yes | Upgrade: new version | | | | 21 May 2013 10:26 | |
| Draft | Yes | Upgrade: new version | | | | 13 May 2013 15:32 | |
| Archive | Yes | Custom 2 | | | | 22 May 2013 18:04 | admin |
| Archive | Yes | Custom 2 | | | | 18 May 2013 20:38 | admin |
| Archive | Yes | Upgrade: new version | | | | 18 May 2013 12:41 | |
| Archive | Yes | Custom | | | | 17 May 2013 09:02 | admin |
| Archive | Yes | Custom | | | | 15 May 2013 16:03 | admin |
| Archive | Yes | Custom | | | | 15 May 2013 15:22 | admin |
| Archive | Yes | Custom | | | | 15 May 2013 15:02 | admin |
| Archive | Yes | incidents firewall amended 2 | | | | 08 May 2013 18:39 | admin |
| Archive | Yes | incidents firewall amended | | | | 08 May 2013 18:28 | admin |
| Archive | Yes | Upgrade: new version | | | | 07 May 2013 15:30 | |
| Archive | Yes | Upgrade: new version | | | | 23 Apr 2013 10:50 | |
| Archive | Yes | Upgrade: local changes overwritten | | | | 12 Apr 2013 12:20 | |
| Archive | Yes | Upgrade: local changes overwritten | | | | 04 Apr 2013 14:04 | |
| Archive | Yes | Upgrade: local changes overwritten | | | | 27 Mar 2013 11:47 | |
| Archive | Yes | Upgrade: local changes overwritten | | | | 20 Mar 2013 17:40 | admin |
| Archive | Yes | Initial installation | 1 | 05 Mar 2013 16:03 | | 05 Mar 2013 16:03 | |

Opening project-23.xml

You have chosen to open:

**project-23.xml**

which is a: XML Document

from: http://ppk:81

What should Firefox do with this file?

● Open with TextPad (default)

○ Save File

□ Do this automatically for files like this from now on.

OK Cancel

Figure 152 Event Project Export

5) Copy the event project file to a location from which you can access it from the import server.

6) From the import server click **Administration > Events > Event Administration**.

7) Click **View all projects**.

8) Click **Import** and then upload the project. The project is loaded as a draft project which you can now deploy.

After creating your own events and incidents you may want to reference them through their unique identifiers. You can find these numbers in the event project file. Although you can directly edit the event project file and then import it and its amendments into Entuity you should do so only under guidance of Entuity Support.

# Merge Event Management System Projects

Entuity administrators are encouraged to customize the Event Management System to best meet their requirements. Usually you would amend the current live project and then save and apply this updated project. Entuity retains the previous event project and over time, with a series of amendments Entuity can retain many help projects (administrators can also delete unwanted projects). Any of these archived event projects you can set as the live project.

Entuity also allows you to merge any two selected projects. You may want to merge when for example:

- Installing a new Entuity release that has an updated event project but also wanting to retain the customizations in your current project.

Entuity does not automatically apply the updated event project. You should consult the *Entuity Migration Guide* to familiarize yourself with any changes included in the new event project.

Entuity Best Practice would be to merge the new event project into your customized project.

- Wanting to apply to the current event project a particular event project setup from an old event project.
- Wanting to apply to the current event project settings from an event project imported from another Entuity server.

The event project merge function identifies differences between the two selected event projects and allows you to select the required version of each conflict. When the merge is complete you have a new event project, the two source event projects remain unchanged.

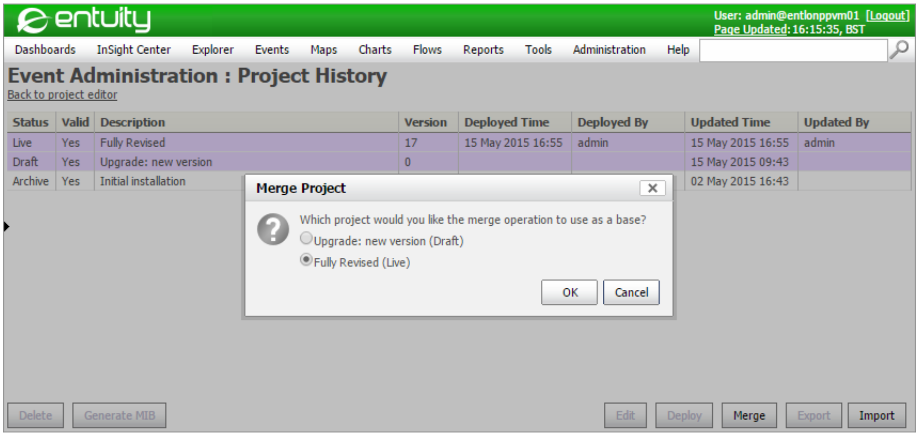
This merge utility compares more than the underlying event project XML files, for example changes in a system event's severity level.

## Event Management System Merge Process Overview

The Event Management System merge process:

1) From the Event Management System Project History page you can select the two projects to merge. This might be you current live project and Entuity's latest released project.

2) Entuity prompts you to identify which of the two selected projects is the base project, the second project is then compared to the base project.



Event Administration : Project History

| Status | Valid | Description | Version | Deployed Time | Deployed By | Updated Time | Updated By |
|---|---|---|---|---|---|---|---|
| Live | Yes | Fully Revised | 17 | 15 May 2015 16:55 | admin | 15 May 2015 16:55 | admin |
| Draft | Yes | Upgrade: new version | 0 | | | 15 May 2015 09:43 | |
| Archive | Yes | Initial installation | | | | 02 May 2015 16:43 | |

Merge Project

Which project would you like the merge operation to use as a base?

○ Upgrade: new version (Draft)

● Fully Revised (Live)

Figure 153 Merge Event Projects

3) Entuity compares an extensive set of components and attributes to identify differences between the projects. (See *Table 37 Component Attributes Compared During Merge*.) Entuity would also identify if the two projects were identical.

| Component | Comparison Attributes |
|---|---|
| Events | Name (custom events only)<br>Severity<br>Description (custom events only) |
| Incidents | Name<br>Enabled<br>Description<br>Opened By<br>Updated By<br>Closed By<br>Age Out<br>Expiry |
| Trigger | Name<br>Description<br>On Transition To<br>Condition<br>Tests (when condition is not none)<br>Invert Test Result (when condition is not none)<br>Delay<br>State After Delay (when delay is not none)<br>Action Steps |
| Rules | Name<br>Description<br>Enabled<br>Validity<br>Condition<br>Behavior (Processing Stages Only)<br>Schedule (Rules Only)<br>Action (Rules Only)<br>Parent<br>Order of common children (Processing Stages Only) |
| Variables | Description<br>Value |
| Conditions | Description<br>Parameters<br>Condition<br>Tests<br>Invert Test Result |
| Actions | Description<br>Parameters<br>Action Steps |
| Others | Description<br>Expression (target alias only)<br>Storage (custom attribute only) |

Table 37 Component Attributes Compared During Merge

The merge utility adopts the Event Management System interface with its division of different Event Management System functionality (e.g. rules, actions, events) across tabs.

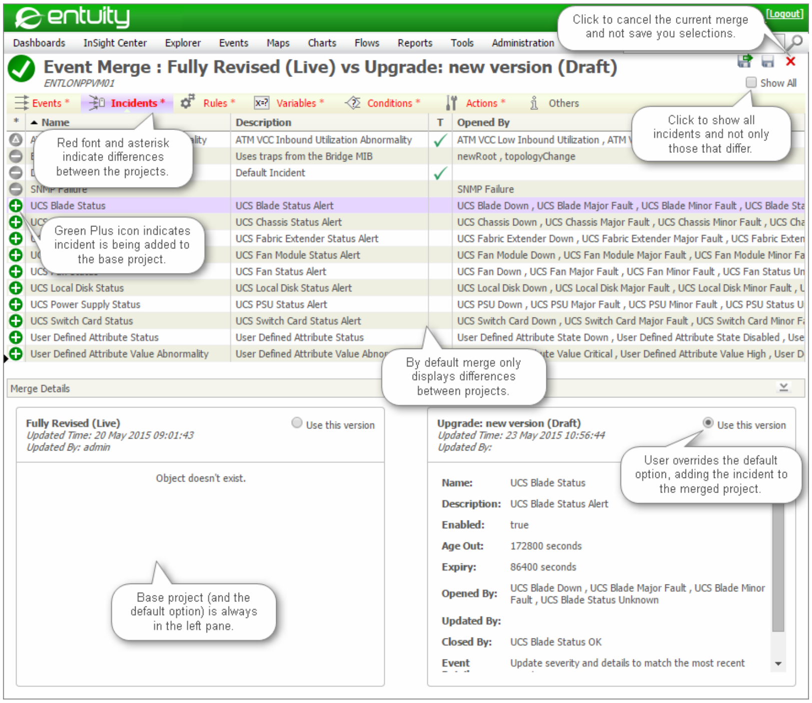
Where a tab includes a difference Entuity changes the font of the tab title to red and includes an asterisk.

4) Where merge identifies differences between the two projects then by default the base setting is selected. Entuity does flag the differences between the two projects with the merge icons and font style indicating the type of difference. (See *Table 38 Merge Project Icons and Color Codes*.)

From the Merge Details panel you have the option of selecting the setting in the second project and if you do Entuity would update the merge icon and font style to reflect the new state. The Merge Details panel is closed by default. Click any flagged item to open the panel, or click on the panel's Up Arrow icon. To close the panel click on its Down Arrow.

| Indicator | Description |
|---|---|
| ⊕<br>Grey Italic Font | Indicates the object does not exist in the base project.<br>The proposal is to include this object to the merged project but it requires you to select this version from the Merge Details panel. |
| ⊕<br>Black Normal Font | Indicates the object does not exist in the base project but you have selected to include it to the merged project. |
| ⊖<br>Black Text | Indicates the object exists in the base project but does not exist in the second project.<br>The proposal is to not include this object to the merged project but it requires you to select this version from the Merge Details panel. |
| ⊖<br>Grey Italic Text | Indicates the object exists in the base project but by selecting the version in the second event project you have decided to not include it to the merged project. |
| △<br>Black Text | Indicates the object exists in both projects but with different attribute values.<br>The proposal is to apply values from the second project but it requires you to select this version from the Merge Details panel. |
| △<br>Grey Italic Text | Indicates the object exists in both projects, with different attribute values, but you have selected to include the values from the second project to the merged project. |
| ⊞ | Indicates the position of the node in the base project and that it has changed position in the second project. |
| ⊞ | Indicates the position of the node in the second project and that you have selected that position for the merged project. |

Table 38 Merge Project Icons and Color Codes



Event Merge : Fully Revised (Live) vs Upgrade: new version (Draft)
*ENTLONPPVM01*

| * | Name | Description | T | Opened By |
|---|---|---|---|---|
| | A… …ality | ATM VCC Inbound Utilization Abnormality | ✓ | ATM VCC Low Inbound Utilization , ATM V… |
| | B… | Uses traps from the Bridge MIB | | newRoot , topologyChange |
| | D… | Default Incident | ✓ | |
| | SNMP Failure | | | SNMP Failure |
| ⊕ | UCS Blade Status | UCS Blade Status Alert | | UCS Blade Down , UCS Blade Major Fault , UCS Blade Minor Fault , UCS Blade Sta |
| ⊕ | UCS… | UCS Chassis Status Alert | | UCS Chassis Down , UCS Chassis Major Fault , UCS Chassis Minor Fault , UCS Cha |
| ⊕ | U… | UCS Fabric Extender Status Alert | | UCS Fabric Extender Down , UCS Fabric Extender Major Fault , UCS Fabric Exten |
| ⊕ | U… | UCS Fan Module Status Alert | | UCS Fan Module Down , UCS Fan Module Major Fault , UCS Fan Module Minor Fa |
| ⊕ | UCS… | UCS Fan Status Alert | | UCS Fan Down , UCS Fan Major Fault , UCS Fan Minor Fault , UCS Fan Status Un |
| ⊕ | UCS Local Disk Status | UCS Local Disk Status Alert | | UCS Local Disk Down , UCS Local Disk Major Fault , UCS Local Disk Minor Fault , U |
| ⊕ | UCS Power Supply Status | UCS PSU Status Alert | | UCS PSU Down , UCS PSU Major Fault , UCS PSU Minor Fault , UCS PSU Status U |
| ⊕ | UCS Switch Card Status | UCS Switch Card Status Alert | | UCS Switch Card Down , UCS Switch Card Major Fault , UCS Switch Card Minor Fa |
| ⊕ | User Defined Attribute Status | User Defined Attribute Status | | User Defined Attribute State Down , User Defined Attribute State Disabled , Use |
| ⊕ | User Defined Attribute Value Abnormality | User Defined Attribute Value Abnor… | | …ute Value Critical , User Defined Attribute Value High , User D |

**Fully Revised (Live)** ○ Use this version
*Updated Time: 20 May 2015 09:01:43*
*Updated By: admin*

Object doesn't exist.

**Upgrade: new version (Draft)** ● Use this version
*Updated Time: 23 May 2015 10:56:44*
*Updated By:*

**Name:** UCS Blade Status
**Description:** UCS Blade Status Alert
**Enabled:** true
**Age Out:** 172800 seconds
**Expiry:** 86400 seconds
**Opened By:** UCS Blade Down , UCS Blade Major Fault , UCS Blade Minor Fault , UCS Blade Status Unknown
**Updated By:**
**Closed By:** UCS Blade Status OK
**Event** Update severity and details to match the most recent

Click to cancel the current merge and not save you selections.

Click to show all incidents and not only those that differ.

Red font and asterisk indicate differences between the projects.

Green Plus icon indicates incident is being added to the base project.

By default merge only displays differences between projects.

User overrides the default option, adding the incident to the merged project.

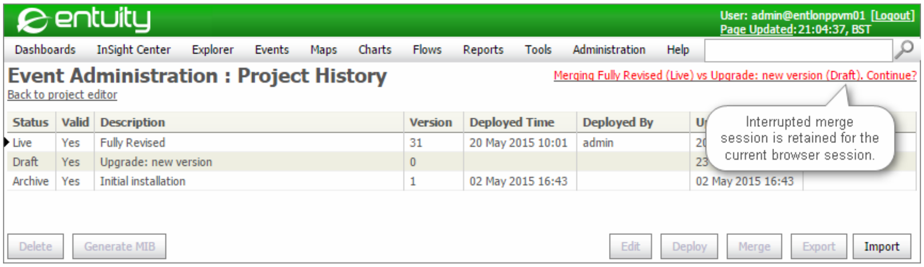
Base project (and the default option) is always in the left pane.

Figure 154 Event Management System Merge

5) During the merge process you can navigate away from the Event Management System and Entuity maintains the current state of the merge process in your browser session. If you:

- End the browser session then your changes are lost.
- Attempt to start a new merge during the same browser session Entuity will warn you that a merge job is in progress and that to continue would result in the loss of the in progress merge.

At the end of the merge process as with any other project you can save the project as a draft project or immediately deploy it. Only when you save the project are your selections saved, and only if you deploy the merged project are they applied to the Event Management System.



Event Administration : Project History

Back to project editor

Merging Fully Revised (Live) vs Upgrade: new version (Draft). Continue?

| Status | Valid | Description | Version | Deployed Time | Deployed By | U |
|---|---|---|---|---|---|---|
| Live | Yes | Fully Revised | 31 | 20 May 2015 10:01 | admin | 20 |
| Draft | Yes | Upgrade: new version | 0 | | | 23 |
| Archive | Yes | Initial installation | 1 | 02 May 2015 16:43 | | 02 May 2015 16:43 |

Interrupted merge session is retained for the current browser session.

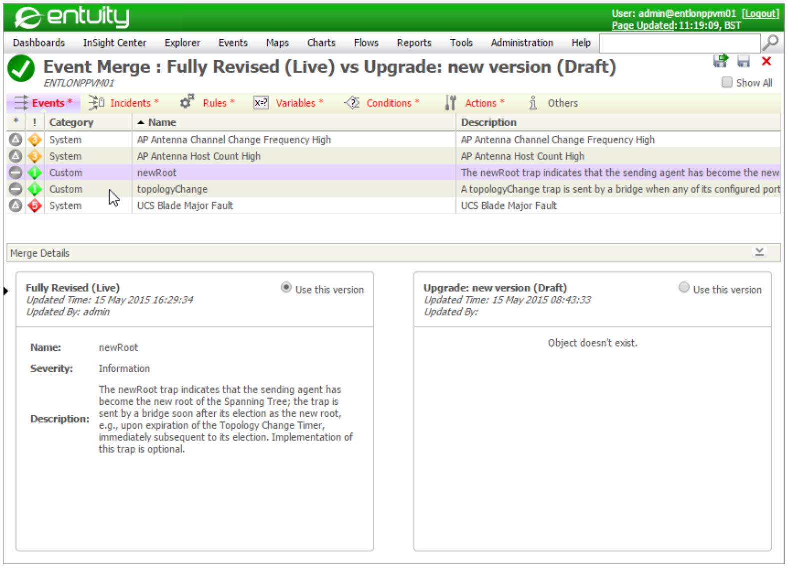
Figure 155 Interrupted Merge

## Merge Events

Entuity merge checks for differences in these event attributes:

- *Name* of custom events.
- *Severity* level.
- *Description* of custom events.

System event *Name* and *Description* are not project specific or user definable, they are only changed as part of an Entuity upgrade. These attributes are not user definable and Event Management System merge would not identify any changes to them.



Event Merge : Fully Revised (Live) vs Upgrade: new version (Draft)

ENTLONPPVM01

| * | ! | Category | Name | Description |
|---|---|---|---|---|
| | 3 | System | AP Antenna Channel Change Frequency High | AP Antenna Channel Change Frequency High |
| | 3 | System | AP Antenna Host Count High | AP Antenna Host Count High |
| | 1 | Custom | newRoot | The newRoot trap indicates that the sending agent has become the new |
| | 1 | Custom | topologyChange | A topologyChange trap is sent by a bridge when any of its configured port |
| | 5 | System | UCS Blade Major Fault | UCS Blade Major Fault |

**Fully Revised (Live)** ● Use this version
*Updated Time: 15 May 2015 16:29:34*
*Updated By: admin*

**Name:** newRoot

**Severity:** Information

**Description:** The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.

**Upgrade: new version (Draft)** ○ Use this version
*Updated Time: 15 May 2015 08:43:33*
*Updated By:*

Object doesn't exist.

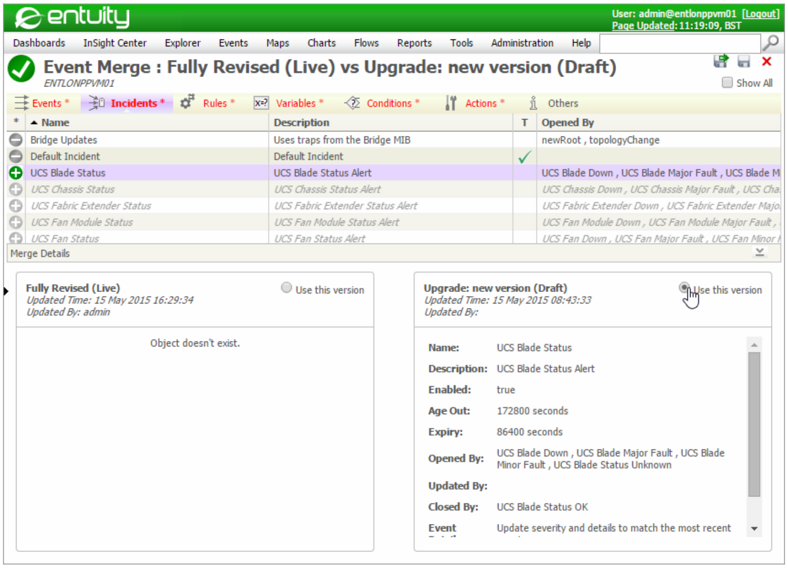
Figure 156 Merge Events

## Merge Incidents

Incident definitions are completely user configurable. Therefore all incident attributes are compared during an Event Management System merge. (See *Event Management System Merge Process Overview* and *Create Incidents*.)

The Event Management System Incident merge tab lists one row per incident, select a row to views its merge details. The Merge Details panel has two panes, the:

- Left side pane always displays the incident values in the base project. By default **Use this version** is selected indicating this setting will be included to the merged project.
- Right side pane always displays the incident values in the second project. When you want to use this setting in the merged project select **Use this version**.



Event Merge : Fully Revised (Live) vs Upgrade: new version (Draft)
ENTLONPPVM01

| * | Name | Description | T | Opened By |
|---|---|---|---|---|
| ⊖ | Bridge Updates | Uses traps from the Bridge MIB | | newRoot , topologyChange |
| ⊖ | Default Incident | Default Incident | ✓ | |
| ⊕ | UCS Blade Status | UCS Blade Status Alert | | UCS Blade Down , UCS Blade Major Fault , UCS Blade M |
| ⊕ | *UCS Chassis Status* | *UCS Chassis Status Alert* | | *UCS Chassis Down , UCS Chassis Major Fault , UCS Cha* |
| ⊕ | *UCS Fabric Extender Status* | *UCS Fabric Extender Status Alert* | | *UCS Fabric Extender Down , UCS Fabric Extender Majo* |
| ⊕ | *UCS Fan Module Status* | *UCS Fan Module Status Alert* | | *UCS Fan Module Down , UCS Fan Module Major Fault ,* |
| ⊕ | *UCS Fan Status* | *UCS Fan Status Alert* | | *UCS Fan Down , UCS Fan Major Fault , UCS Fan Minor* |

**Fully Revised (Live)**
*Updated Time: 15 May 2015 16:29:34*
*Updated By: admin*

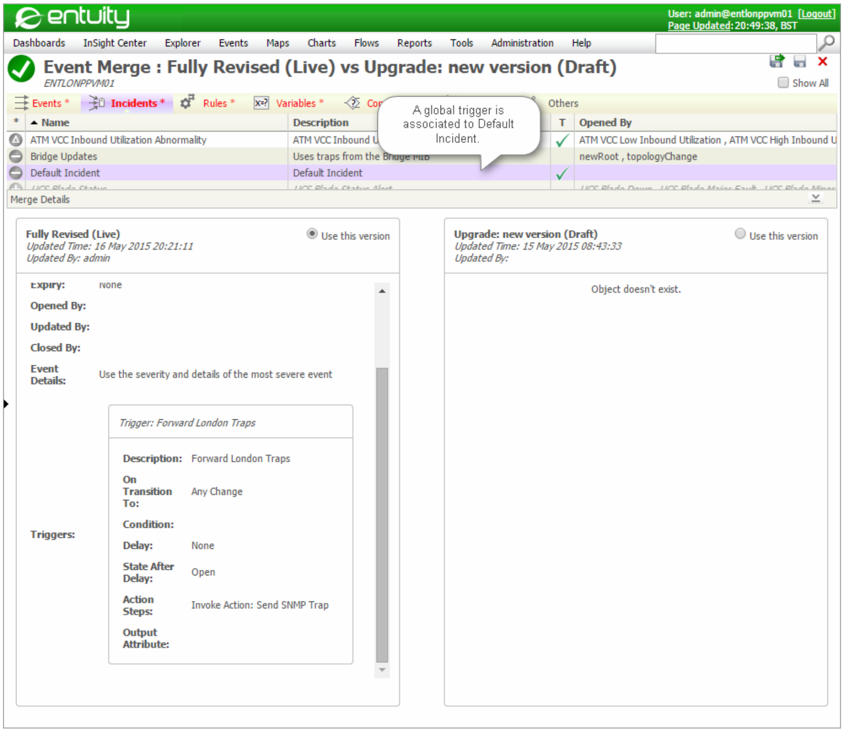
Object doesn't exist.

**Upgrade: new version (Draft)**
*Updated Time: 15 May 2015 08:43:33*
*Updated By:*

**Name:** UCS Blade Status
**Description:** UCS Blade Status Alert
**Enabled:** true
**Age Out:** 172800 seconds
**Expiry:** 86400 seconds
**Opened By:** UCS Blade Down , UCS Blade Major Fault , UCS Blade Minor Fault , UCS Blade Status Unknown
**Updated By:**
**Closed By:** UCS Blade Status OK
**Event** Update severity and details to match the most recent

Figure 157 Merge Incidents

Global triggers are not associated to a particular incident but are available to all incidents. Event Management System merge associates a change to a Global Trigger with the Default Incident.



**Event Merge : Fully Revised (Live) vs Upgrade: new version (Draft)**
*ENTLONPPVM01*

| * | Name | Description | T | Opened By |
|---|---|---|---|---|
| | ATM VCC Inbound Utilization Abnormality | ATM VCC Inbound U | ✓ | ATM VCC Low Inbound Utilization , ATM VCC High Inbound U |
| | Bridge Updates | Uses traps from the Bridge MIB | | newRoot , topologyChange |
| | Default Incident | Default Incident | ✓ | |

**Fully Revised (Live)** ● Use this version
*Updated Time: 16 May 2015 20:21:11*
*Updated By: admin*

Expiry: None
Opened By:
Updated By:
Closed By:
Event Details: Use the severity and details of the most severe event
Triggers:

*Trigger: Forward London Traps*

Description: Forward London Traps
On Transition To: Any Change
Condition:
Delay: None
State After Delay: Open
Action Steps: Invoke Action: Send SNMP Trap
Output Attribute:

**Upgrade: new version (Draft)** ○ Use this version
*Updated Time: 15 May 2015 08:43:33*
*Updated By:*

Object doesn't exist.

Figure 158 Global Trigger associated to Default Incident

## Merge Rules

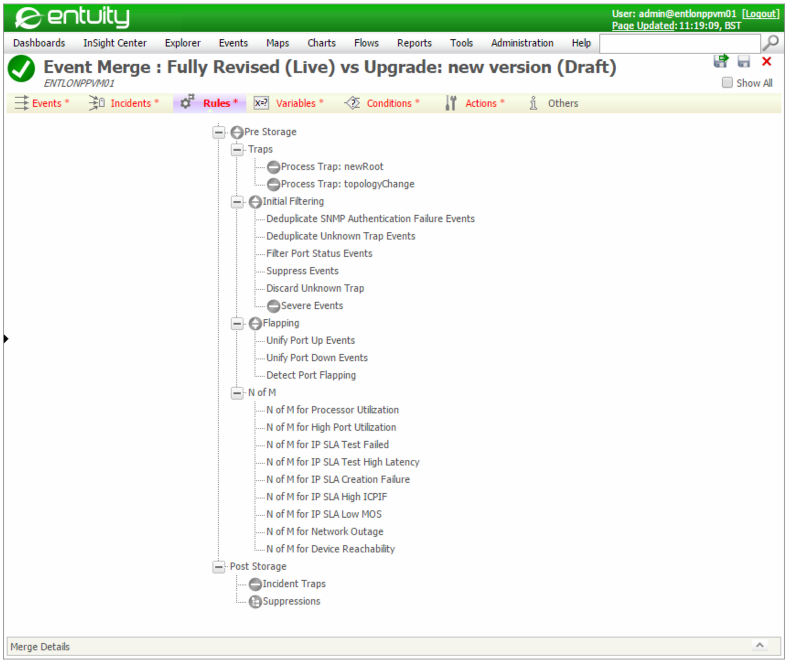
The Rules merge tab includes the results of comparing rules and processing stage definitions in the two project files. (See *Event Management System Merge Process Overview* and *Rule Types and Supplied Rules*.)

Event Management System merge compares the rule:

- Name
- Description
- Enabled state
- Validity
- Condition
- Behavior (Processing Stages Only)
- Schedule (Rules Only)
- Action (Rules Only)
- Parent
- Order of common children (Processing Stages Only).

The Event Management System merge Rules tab displays the Rules tree, select a node to display the Merge Details. The Merge Details panel has two panes, the:

- Left side pane always displays the rules values in the base project. By default **Use this version** is selected indicating this setting will be included to the merged project.
- Right side pane always displays the rules values in the second project. When you want to use this setting in the merged project select **Use this version**. Entuity will update the Rules tree, both the icon color and if appropriate the rules place in the tree.



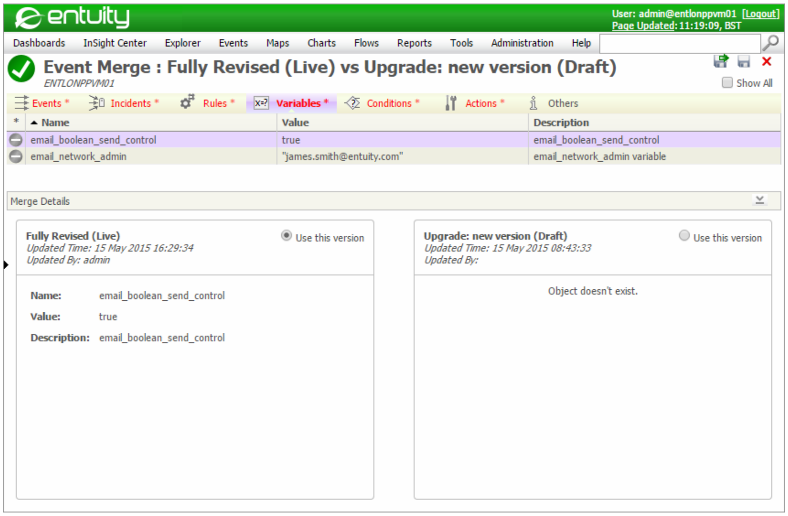
Event Merge : Fully Revised (Live) vs Upgrade: new version (Draft)
ENTLONPPVM01

```
Pre Storage
    Traps
        Process Trap: newRoot
        Process Trap: topologyChange
    Initial Filtering
        Deduplicate SNMP Authentication Failure Events
        Deduplicate Unknown Trap Events
        Filter Port Status Events
        Suppress Events
        Discard Unknown Trap
        Severe Events
    Flapping
        Unify Port Up Events
        Unify Port Down Events
        Detect Port Flapping
    N of M
        N of M for Processor Utilization
        N of M for High Port Utilization
        N of M for IP SLA Test Failed
        N of M for IP SLA Test High Latency
        N of M for IP SLA Creation Failure
        N of M for IP SLA High ICPIF
        N of M for IP SLA Low MOS
        N of M for Network Outage
        N of M for Device Reachability
Post Storage
    Incident Traps
    Suppressions
```

Figure 159 Merge Rules

## Merge Variables

The Variable merge tab includes the results of comparing variable definitions, their *Description* and *Value* in the two project files. (See *Event Management System Merge Process Overview* and *Variables*.)



Event Merge : Fully Revised (Live) vs Upgrade: new version (Draft)
ENTLONPPVM01

| * | Name | Value | Description |
|---|---|---|---|
| ⊖ | email_boolean_send_control | true | email_boolean_send_control |
| ⊖ | email_network_admin | "james.smith@entuity.com" | email_network_admin variable |

Fully Revised (Live)
*Updated Time: 15 May 2015 16:29:34*
*Updated By: admin*
● Use this version

Name: email_boolean_send_control
Value: true
Description: email_boolean_send_control

Upgrade: new version (Draft)
*Updated Time: 15 May 2015 08:43:33*
*Updated By:*
○ Use this version

Object doesn't exist.

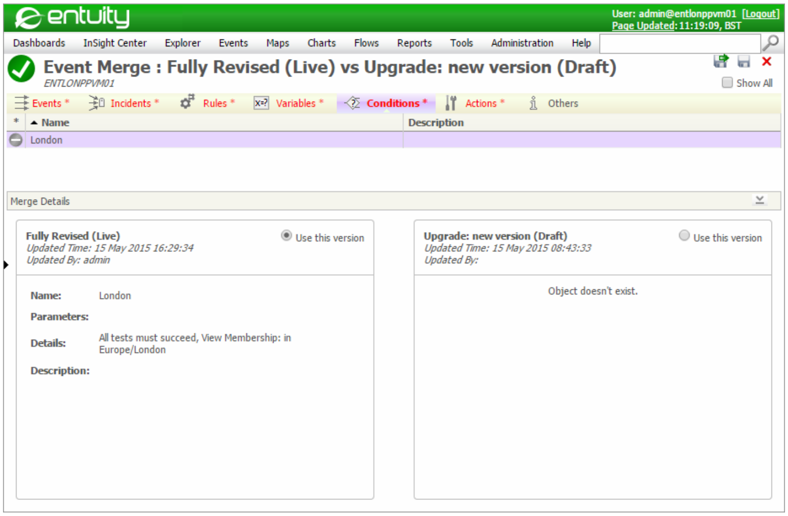
Figure 160 Merge Variables

## Merge Conditions

The Conditions merge tab includes the results of comparing condition definitions, specifically:

- *Description*
- *Parameters*
- *Condition*
- *Tests*
- *Invert Test Result*.

(See *Event Management System Merge Process Overview* and *Conditions and Tests*.)


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 11:19:09, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Show All
Events * Incidents * Rules * Variables * Conditions * Actions * Others
Merge Details

Event Merge : Fully Revised (Live) vs Upgrade: new version (Draft)

ENTLONPPVM01

| * | Name | Description |
|---|---|---|
| | London | |

Fully Revised (Live) ● Use this version
*Updated Time: 15 May 2015 16:29:34*
*Updated By: admin*

**Name:** London

**Parameters:**

**Details:** All tests must succeed, View Membership: in Europe/London

**Description:**

Upgrade: new version (Draft) ○ Use this version
*Updated Time: 15 May 2015 08:43:33*
*Updated By:*

Object doesn't exist.

Figure 161 Merge Conditions

## Merge Actions

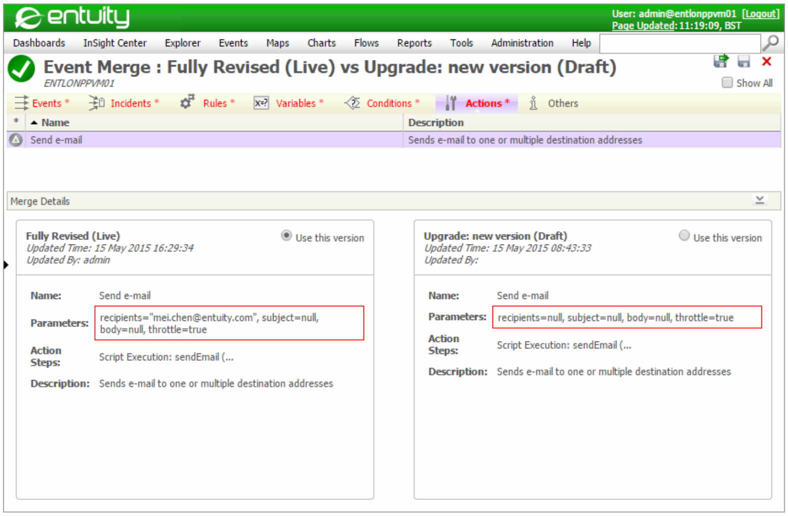
The Actions merge tab includes the results of comparing action definitions, specifically:

*Description*

*Parameters*

*Action Steps*.

(See *Event Management System Merge Process Overview* and *Actions*.)


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 11:19:09, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Show All
Events * Incidents * Rules * Variables * Conditions * Actions * Others
Merge Details

Event Merge : Fully Revised (Live) vs Upgrade: new version (Draft)

ENTLONPPVM01

| * | Name | Description |
|---|---|---|
| | Send e-mail | Sends e-mail to one or multiple destination addresses |

Fully Revised (Live) ● Use this version
*Updated Time: 15 May 2015 16:29:34*
*Updated By: admin*

**Name:** Send e-mail

**Parameters:** recipients="mei.chen@entuity.com", subject=null, body=null, throttle=true

**Action Steps:** Script Execution: sendEmail (...

**Description:** Sends e-mail to one or multiple destination addresses

Upgrade: new version (Draft) ○ Use this version
*Updated Time: 15 May 2015 08:43:33*
*Updated By:*

**Name:** Send e-mail

**Parameters:** recipients=null, subject=null, body=null, throttle=true

**Action Steps:** Script Execution: sendEmail (...

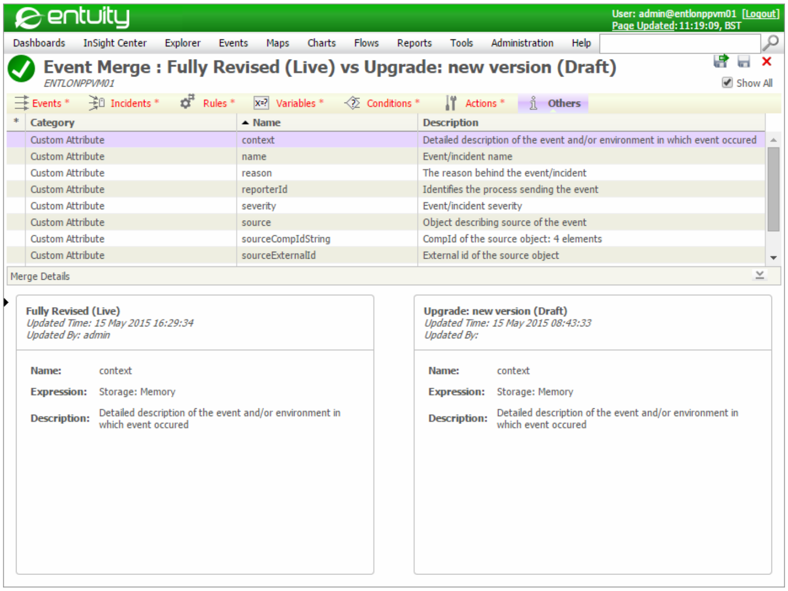
**Description:** Sends e-mail to one or multiple destination addresses

Figure 162 Merge Actions

## Merge Others

The Others merge tab includes the results of comparing these Custom Attributes:

- Description
- Expression (target alias only)
- Storage (custom attribute only).



Event Merge : Fully Revised (Live) vs Upgrade: new version (Draft)

ENTLONPPVM01

| * | Category | Name | Description |
|---|---|---|---|
| | Custom Attribute | context | Detailed description of the event and/or environment in which event occured |
| | Custom Attribute | name | Event/incident name |
| | Custom Attribute | reason | The reason behind the event/incident |
| | Custom Attribute | reporterId | Identifies the process sending the event |
| | Custom Attribute | severity | Event/incident severity |
| | Custom Attribute | source | Object describing source of the event |
| | Custom Attribute | sourceCompIdString | CompId of the source object: 4 elements |
| | Custom Attribute | sourceExternalId | External id of the source object |

**Fully Revised (Live)**
*Updated Time: 15 May 2015 16:29:34*
*Updated By: admin*

**Name:** context

**Expression:** Storage: Memory

**Description:** Detailed description of the event and/or environment in which event occured

**Upgrade: new version (Draft)**
*Updated Time: 15 May 2015 08:43:33*
*Updated By:*

**Name:** context

**Expression:** Storage: Memory

**Description:** Detailed description of the event and/or environment in which event occured

Figure 163 Merge Others

# 29Manage Event and Incident Settings

You can view and manage incidents and events through the Entuity web interface. You can:

- View and amend the severity level of each event. (See *Event Severity Settings*.)
- Set whether an event threshold is active, disabled thresholds also disable the event. Entuity supports both static and dynamic threshold types.(See *Set Event Thresholds* and *Set Event Baselines for Dynamic Thresholds*.)
- Control which events and incidents are displayed by using the event viewer filters. (See *Controlling Display of System Events and Incidents*.)
- Suppress the raising of events. (See *Event Suppression*.)
- Annotate and acknowledge incidents. (See *Incident Annotations*.)
- Drill-down from an event to view more detailed information.

## Event Severity Settings

Event severity is an attribute on which you can filter events, for example only show events with a severity equal to or greater than **Severe**. The factory settings are usually appropriate but through the Event Administration page you can amend these defaults. Incidents inherit the highest severity level of their raised events. (For more details on event severity see the *Entuity Events Reference Manual*.)

| Display Severity | Color Code | Description |
|---|---|---|
| 1 | Green | Information or Cleared |
| 2 | Yellow | Minor |
| 3 | Amber | Major |
| 4 | Orange | Severe |
| 5 | Red | Critical |

Table 39 Event Severity

### How to Change Event Severity and Age Out Settings

To view and maintain event severity and age out settings:

1) Click **Administration** > **Events** > **Events Administration**. Entuity displays the Event Administration page, with events sorted alphabetically.
2) Highlight one or more events and click **Edit**. Amend the event severity settings.
3) Click **OK** to close the dialog. Entuity updates the Event Administration page.
4) Click **Submit** to save and apply these changes.

You can set to events back to their factory settings by highlighting events and clicking **Restore Defaults**.

# Set Event Thresholds

Static threshold settings allow you to configure the trigger points which when crossed cause Entuity to raise events. You can set thresholds against an individual event, a managed object, view or all objects on an Entuity server.

The factory default is for all static thresholds to be turned off. By selecting an object, e.g. device, port, view, you can set one or more of the thresholds associated with that object.

Entuity indicates when a threshold:

- Is enabled by placing a green tick alongside it.
- Setting was made directly on that particular object by placing the Remove Override icon alongside it. This icon (a cross) alongside the object indicates where the override was set, for example against the:
  - Device indicates the threshold setting was made on the device. All of its ports, without an override, inherit this setting.
  - Port indicates the threshold setting was made on the port. The port does not inherit any values from the device.

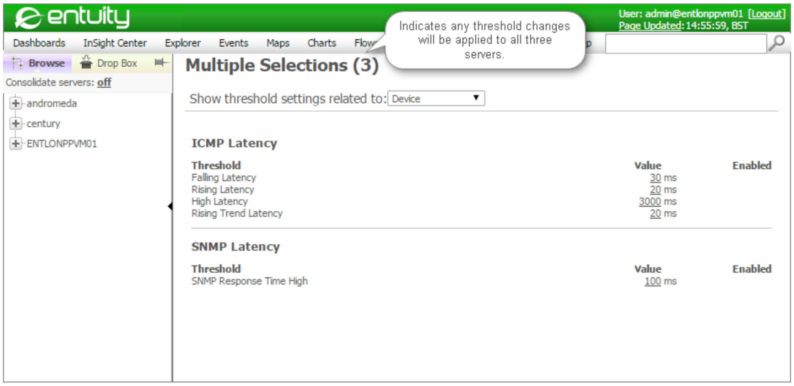
  There is a threshold hierarchy, for example you can also set thresholds at the port level. When you set a threshold at the port level it overrides the factory default and any setting on the device, even if that threshold is subsequently amended at the device level.

## Viewing Static Thresholds

To view thresholds on an Entuity server:

1) From Explorer select the Entuity server.
2) Click **Administration** > **Events** > **Threshold Settings**.

   Entuity displays the Threshold Settings for the server.
3) From *Show threshold settings related to* select the threshold type to view. Entuity groups thresholds by type, e.g. ATM, BladeCenter, Device, Firewall, Managed Hosts.



Indicates any threshold changes will be applied to all three servers.

Multiple Selections (3)

Show threshold settings related to: Device

**ICMP Latency**

| Threshold | Value | Enabled |
|---|---|---|
| Falling Latency | 30 ms | |
| Rising Latency | 20 ms | |
| High Latency | 3000 ms | |
| Rising Trend Latency | 20 ms | |

**SNMP Latency**

| Threshold | Value | Enabled |
|---|---|---|
| SNMP Response Time High | 100 ms | |

Figure 164 Viewing Threshold Settings

To view thresholds on a device:

1) From Explorer select the device.

2) Click **Thresholds**. Entuity displays the Threshold Settings for the device.

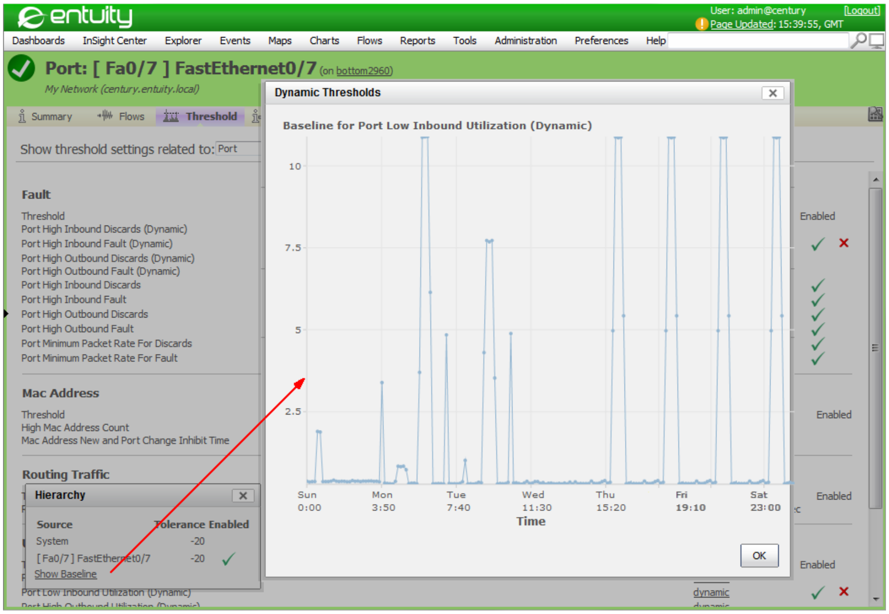
3) From *Show threshold settings related to* select the threshold type to view. Entuity groups thresholds by type, e.g. ATM, BladeCenter, Device, Firewall.

## Set Event Baselines for Dynamic Thresholds

Dynamic thresholds enable Entuity to alert the user to deviations from what Entuity's previous polling has established as normal behavior for that hour on that day. Entuity establishes normal behavior for a given attribute on a given port by maintaining the last four weeks worth of polled data, and applying an averaging algorithm. The dynamic threshold calculation is performed periodically in a weekly job.

The baseline provides a week's worth of threshold values, divided into hourly slots. The polled attributes are compared against the baseline threshold value for the corresponding hourly slot, once per hour (when the stream's roll-ups occur). The baseline chart is available from the dynamic thresholds set page. When thresholds are crossed Entuity can raise the appropriate dynamic events.

You have the option of setting a tolerance level which determines by how much the threshold must be crossed before Entuity raises an event. *Tolerance* is an absolute value above the baseline, not a percentage of the baseline. For example when the baseline is 10 and the tolerance is 20 the threshold above which Entuity raises an event is 30 and not 12 (20 percent of 10).



Port: [ Fa0/7 ] FastEthernet0/7 (on bottom2960)

My Network (century.entuity.local)

Show threshold settings related to: Port

Dynamic Thresholds

Baseline for Port Low Inbound Utilization (Dynamic)

Fault

Threshold
Port High Inbound Discards (Dynamic)
Port High Inbound Fault (Dynamic)
Port High Outbound Discards (Dynamic)
Port High Outbound Fault (Dynamic)
Port High Inbound Discards
Port High Inbound Fault
Port High Outbound Discards
Port High Outbound Fault
Port Minimum Packet Rate For Discards
Port Minimum Packet Rate For Fault

Mac Address

Threshold
High Mac Address Count
Mac Address New and Port Change Inhibit Time

Routing Traffic

Hierarchy

| Source | Tolerance | Enabled |
|---|---|---|
| System | -20 | |
| [ Fa0/7 ] FastEthernet0/7 | -20 | ✓ |

Show Baseline

Port Low Inbound Utilization (Dynamic)
Port High Outbound Utilization (Dynamic)

Figure 165 Dynamic Threshold Tolerance and Baseline

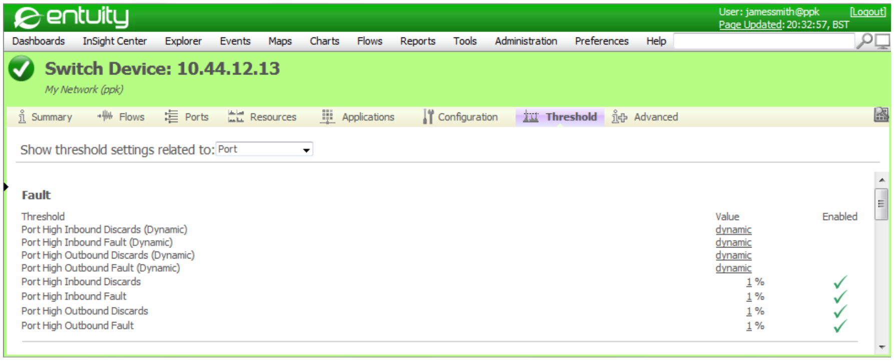
These are the port-level dynamic thresholds, which can be applied at device and port level:

- Port High Inbound Utilization (Dynamic)
- Port High Outbound Utilization (Dynamic)
- Port Low Inbound Utilization (Dynamic)
- Port Low Outbound Utilization (Dynamic)
- Port High Inbound Fault (Dynamic)
- Port High Outbound Fault (Dynamic)
- Port High Inbound Discards (Dynamic)
- Port High Outbound Discards (Dynamic).

Care should be taken when applying dynamic thresholds. Enabling a single dynamic threshold on 10,000 interfaces requires approximately 5MB of memory. Enabling all eight dynamic thresholds on 100,000 interfaces would increase memory requirement by 400MB.

## Configuring Dynamic Thresholds

By default, all dynamic thresholds are turned off. You can turn on the dynamic threshold at the device and port level, in a similar way to static thresholds. Dynamic thresholds cannot be applied at the root (i.e. Entuity server) or view level.



Switch Device: 10.44.12.13

*My Network (ppk)*

Show threshold settings related to: Port

**Fault**

| Threshold | Value | Enabled |
|---|---|---|
| Port High Inbound Discards (Dynamic) | dynamic | |
| Port High Inbound Fault (Dynamic) | dynamic | |
| Port High Outbound Discards (Dynamic) | dynamic | |
| Port High Outbound Fault (Dynamic) | dynamic | |
| Port High Inbound Discards | 1 % | ✓ |
| Port High Inbound Fault | 1 % | ✓ |
| Port High Outbound Discards | 1 % | ✓ |
| Port High Outbound Fault | 1 % | ✓ |

Figure 166 Dynamic Threshold Settings

To set the Port High Inbound Utilization (Dynamic) threshold for all ports on the device:

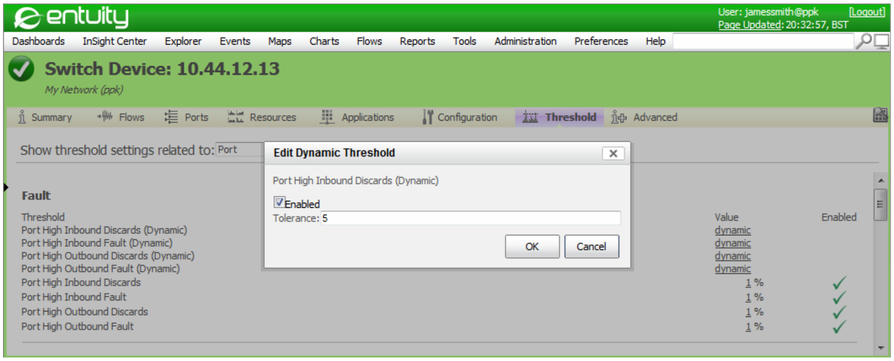
1) From Explorer navigate to and select the device against which you want to configure dynamic thresholds.

   Entuity displays the Device page.

2) Click **Thresholds**. Entuity displays the threshold page.

3) From *Show threshold settings related to* select **Ports**. Entuity displays the port thresholds, including the dynamic thresholds.

4) From the Port High Inbound Utilization (Dynamic) value select dynamic. Entuity displays the Edit Dynamic Threshold dialog.



Switch Device: 10.44.12.13

*My Network (ppk)*

Show threshold settings related to: Port

**Edit Dynamic Threshold**

Port High Inbound Discards (Dynamic)

☑ Enabled

Tolerance: 5

**Fault**

| Threshold | Value | Enabled |
|---|---|---|
| Port High Inbound Discards (Dynamic) | dynamic | |
| Port High Inbound Fault (Dynamic) | dynamic | |
| Port High Outbound Discards (Dynamic) | dynamic | |
| Port High Outbound Fault (Dynamic) | dynamic | |
| Port High Inbound Discards | 1 % | ✓ |
| Port High Inbound Fault | 1 % | ✓ |
| Port High Outbound Discards | 1 % | ✓ |
| Port High Outbound Fault | 1 % | ✓ |

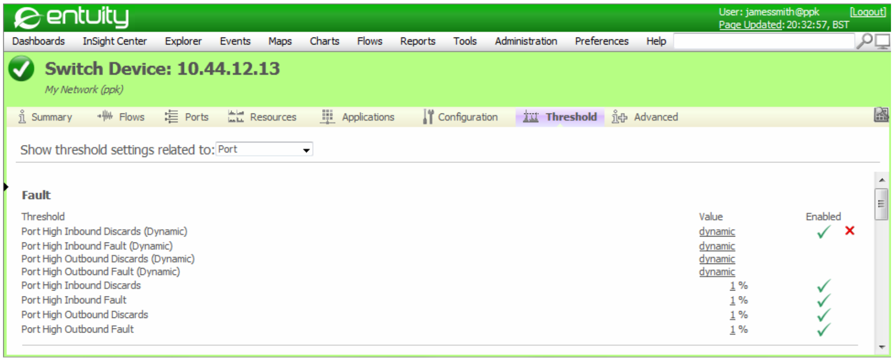
Figure 167 Setting Dynamic Threshold

5) Click **Enabled**.

   You can also amend the tolerance value. Tolerance sets how much above the historic baseline utilization must be before it triggers an event.

6) Click **OK**.

Entuity activates the Port High Inbound Utilization (Dynamic) threshold, indicating that on the Thresholds page by displaying a tick in the Enabled column and Remove Override icon.



Switch Device: 10.44.12.13

*My Network (ppk)*

Show threshold settings related to: Port

**Fault**

| Threshold | Value | Enabled |
|---|---|---|
| Port High Inbound Discards (Dynamic) | dynamic | ✓ ✗ |
| Port High Inbound Fault (Dynamic) | dynamic | |
| Port High Outbound Discards (Dynamic) | dynamic | |
| Port High Outbound Fault (Dynamic) | dynamic | |
| Port High Inbound Discards | 1 % | ✓ |
| Port High Inbound Fault | 1 % | ✓ |
| Port High Outbound Discards | 1 % | ✓ |
| Port High Outbound Fault | 1 % | ✓ |

Figure 168 Dynamic Threshold Set

## Dynamic Thresholds, Hierarchy and Remove Overrides

The factory default is for all dynamic thresholds on all ports to be turned off. By selecting a device you can set one or more of the dynamic thresholds on all of that device’s ports. You can also set thresholds at the port level. When you set a threshold at the port level it overrides the factory default and any setting on the device, even if that threshold is subsequently amended at the device level.

Entuity indicates when a threshold:

- Is enabled by placing a green tick alongside it
- Setting was made directly on that particular object by placing the Remove Override icon alongside it. This icon (a cross) alongside the:
  - Device indicates the threshold setting was made on the device. All of its ports, without an override, inherit this setting.
  - Port indicates the threshold setting was made on the port. The port does not inherit any values from the device.

For example, consider that you want to monitor the large majority of ports on a device. You should enable the threshold on the device and disable the threshold on those ports you do not want to monitor.

## How to Set Dynamic Thresholds on a Device

To set thresholds on a device but not on a particular port:

1) Open the port’s Threshold page.
2) From *Show threshold settings related to* select **Ports**.

   Entuity displays the port thresholds, including the dynamic thresholds.
3) For the particular threshold select **dynamic**.

Entuity displays the Edit Dynamic Threshold dialog.

4) Without enabling the threshold click **OK**. Entuity closes the dialog, saves this setting as a port override and displays against the threshold the Remove Override icon.

5) Open the device’s Threshold page.

6) From *Show threshold settings related to* select **Ports**.

   Entuity displays the port thresholds, including the dynamic thresholds.

7) For the particular threshold select **dynamic**.

   Entuity displays the Edit Dynamic Threshold dialog.

8) Select Enable and amend the tolerance value if required.

9) Click **OK**. Entuity closes the dialog and sets the dynamic threshold to this value on all of the device’s ports that do not have a port override. Entuity also displays against the device’s threshold the Override icon, ports that inherit this setting are enabled but do not have the Override icon.

## How to Remove Dynamic Threshold Overrides

To remove a threshold override on a device or port:

1) Open the managed object’s Threshold page.

2) From *Show threshold settings related to* select **Ports**.

   Entuity displays the port thresholds, including the dynamic thresholds.

3) For the particular threshold select its Remove Override icon.

   Entuity displays a remove confirmation message.

4) Click **OK**. Entuity removes the override setting and its icon.

## Viewing Dynamic Threshold Baselines

Baselines are generated against attributes associated with ports, and it is at this port-attribute level that you can view baseline graphs. (See *Set Event Baselines for Dynamic Thresholds*.)

To view the threshold baseline:

1) Use Explorer to navigate to and then select the device’s port for which you want to view its baseline.

   Entuity displays the Port page.

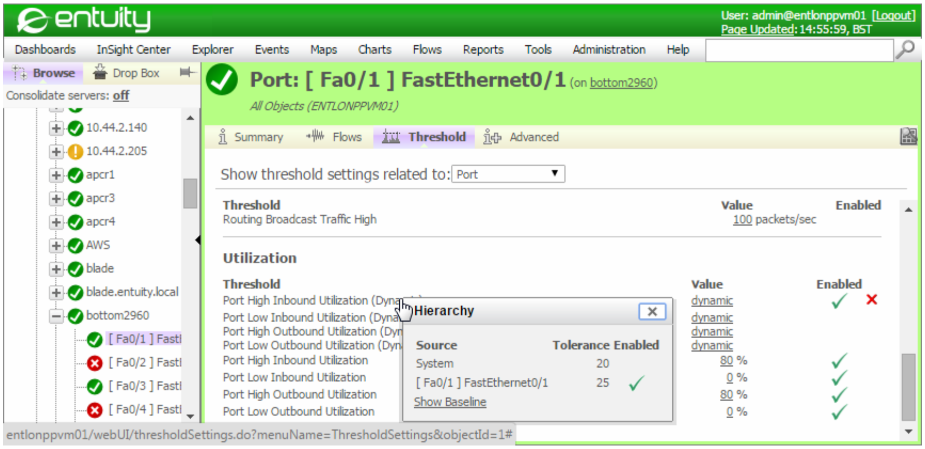
2) Click **Thresholds**.

   Entuity displays the threshold page for the port.

3) Select the required threshold by clicking on its name, e.g. From the Port High Inbound Utilization (Dynamic) value select dynamic.

   Entuity displays the Dynamic Threshold Hierarchy dialog.

At the port level this dialog shows the tolerance settings for the system, for the device, for the port and indicates whether they are enabled.



Port: [ Fa0/1 ] FastEthernet0/1 (on bottom2960)

*All Objects (ENTLONPPVM01)*

Show threshold settings related to: Port

| Threshold | Value | Enabled |
|---|---|---|
| Routing Broadcast Traffic High | 100 packets/sec | |

Utilization

| Threshold | Value | Enabled |
|---|---|---|
| Port High Inbound Utilization (Dyna | dynamic | ✓ ✗ |
| Port Low Inbound Utilization (Dyna | dynamic | |
| Port High Outbound Utilization (Dyn | dynamic | |
| Port Low Outbound Utilization (Dyn | dynamic | |
| Port High Inbound Utilization | 80 % | ✓ |
| Port Low Inbound Utilization | 0 % | ✓ |
| Port High Outbound Utilization | 80 % | ✓ |
| Port Low Outbound Utilization | 0 % | ✓ |

Hierarchy

| Source | Tolerance | Enabled |
|---|---|---|
| System | 20 | |
| [ Fa0/1 ] FastEthernet0/1 | 25 | ✓ |

Show Baseline

Figure 169 Threshold Hierarchy Dialog

## Prevent Raising of Events on Ports with Low Traffic

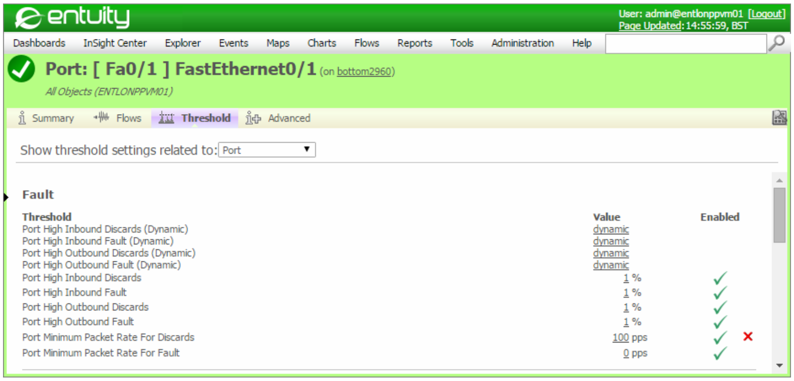
You can prevent Entuity from raising events and incidents on ports with low packet throughput. The behavior of the port discard and fault events (both static and dynamic) can be amended through an additional filter applied as a threshold.

The Port Minimum Packet Rate for Discards and Port Minimum Packet Rate for Faults allow you to set a packets per second threshold; only when this threshold is crossed could Entuity potentially raise the associated fault or discard events. By default these thresholds are not set. When they are set Entuity includes the threshold information to the event details, for example:

```
InFault=0.28% (threshold=1.00%) of 24.05Mpkts/300s --> align=9%,
crc=4%, abort=16%. Packet-rate=80.16kpkts/s (threshold=1.00pkts/s)
```

```
OutFault=7.40% (threshold=1.00%) of 2.21Mpkts/300s --> SQE=1%, late
col=7%, ex col=11%, abort=7%, car loss=75%. Packet-rate=7.37kpkts/s
(threshold=1.00pkts/s)
```

```
InDiscards=0.32% (threshold=1%) of 7.66Mpkts/300s. Packet-
rate=25.54kpkts/s (threshold=0.001pkts/s)
```



Port: [ Fa0/1 ] FastEthernet0/1 (on bottom2960)

All Objects (ENTLONPPVM01)

Show threshold settings related to: Port

Fault

| Threshold | Value | Enabled | |
|---|---|---|---|
| Port High Inbound Discards (Dynamic) | dynamic | | |
| Port High Inbound Fault (Dynamic) | dynamic | | |
| Port High Outbound Discards (Dynamic) | dynamic | | |
| Port High Outbound Fault (Dynamic) | dynamic | | |
| Port High Inbound Discards | 1 % | ✓ | |
| Port High Inbound Fault | 1 % | ✓ | |
| Port High Outbound Discards | 1 % | ✓ | |
| Port High Outbound Fault | 1 % | ✓ | |
| Port Minimum Packet Rate For Discards | 100 pps | ✓ | ✗ |
| Port Minimum Packet Rate For Fault | 0 pps | ✓ | |

Figure 170 Thresholds for Minimum Packet Rate

For example, if Port High Inbound Discards is set to 1% and Port Minimum Packet Rate for Discards is:

- Not enabled then if inbound discards for the port is 2% Entuity would raise the Port Inbound Discards High (Device Congestion) event.
- Enabled and set to 100 then only if the inbound packet rate is above 100 and the inbound discards for the port is over 1% would Entuity raise the Port Inbound Discards High (Device Congestion) event. If subsequently the inbound packet rate dropped below 100 then Entuity would close the event even when inbound discards was still above the 1% threshold.

You can set the Port Minimum Packet Rate for Discards and Port Minimum Packet Rate for Faults thresholds to 3 decimal places.

The Port Minimum Packet Rate for Discards threshold filter applies to these events:

- Port Inbound Discards High (Device Congestion) / Port Inbound Discards High Cleared (No Device Congestion)
- Port Outbound Discards High (Port Congestion) / Port Outbound Discards High Cleared (No Port Congestion)
- Port High Inbound Discards (Dynamic) / Port High Inbound Discards (Dynamic) Cleared
- Port High Outbound Discards (Dynamic) / Port High Outbound Discards (Dynamic) Cleared.

The Port Minimum Packet Rate for Faults threshold filter applies to these events:

- Port Inbound Fault High (Packet Corruption) / Port Inbound Fault High Cleared (No Packet Corruption)
- Port Outbound Fault High (Transmit Errors) / Port Outbound Fault High Cleared (No Transmit Errors)
- Port High Inbound Faults (Dynamic) / Port High Inbound Faults (Dynamic) Cleared
- Port High Outbound Faults (Dynamic) / Port High Outbound Faults (Dynamic) Cleared.

# Controlling Display of System Events and Incidents

By default Entuity raises and displays system events and incidents across all views, by default views use the All Events and All Incidents filters. A system event is one raised against the Entuity server, for example Entuity Server Disk Space Alert, Entuity Server Started. However when you want only want certain users through defined views to have access to these system events you can set view event and incident filters that exclude system events.

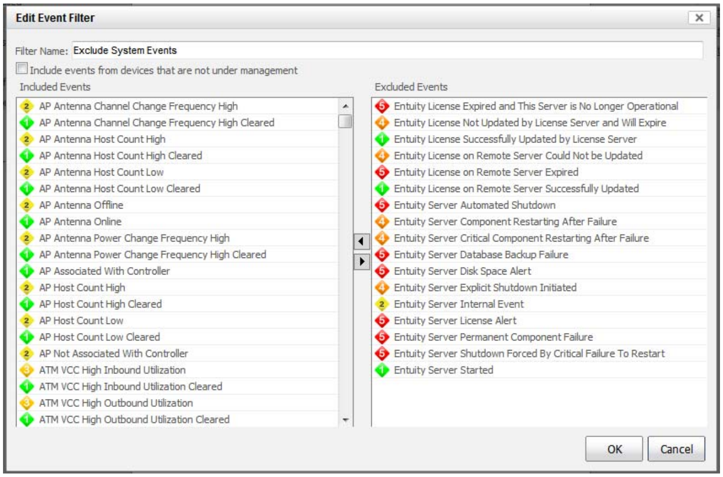
To exclude system events from a view:

1) From Explorer highlight the view and from the context menu click **Edit View**.

2) Click the Events tab and then click **New Filter**.

   By default all events are excluded from the filter.

3) Move to the Included Events column those events you want to permit in the view.



Edit Event Filter

Filter Name: Exclude System Events

□ Include events from devices that are not under management

Included Events

AP Antenna Channel Change Frequency High
AP Antenna Channel Change Frequency High Cleared
AP Antenna Host Count High
AP Antenna Host Count High Cleared
AP Antenna Host Count Low
AP Antenna Host Count Low Cleared
AP Antenna Offline
AP Antenna Online
AP Antenna Power Change Frequency High
AP Antenna Power Change Frequency High Cleared
AP Associated With Controller
AP Host Count High
AP Host Count High Cleared
AP Host Count Low
AP Host Count Low Cleared
AP Not Associated With Controller
ATM VCC High Inbound Utilization
ATM VCC High Inbound Utilization Cleared
ATM VCC High Outbound Utilization
ATM VCC High Outbound Utilization Cleared

Excluded Events

Entuity License Expired and This Server is No Longer Operational
Entuity License Not Updated by License Server and Will Expire
Entuity License Successfully Updated by License Server
Entuity License on Remote Server Could Not be Updated
Entuity License on Remote Server Expired
Entuity License on Remote Server Successfully Updated
Entuity Server Automated Shutdown
Entuity Server Component Restarting After Failure
Entuity Server Critical Component Restarting After Failure
Entuity Server Database Backup Failure
Entuity Server Disk Space Alert
Entuity Server Explicit Shutdown Initiated
Entuity Server Internal Event
Entuity Server License Alert
Entuity Server Permanent Component Failure
Entuity Server Shutdown Forced By Critical Failure To Restart
Entuity Server Started

Figure 171 Event Filter to Exclude System Events

# 30 TrueSight Operations Management Integration

You can setup Entuity to forward events and incidents to the TrueSight Operations Management suite, specifically to cells on the BMC TrueSight Infrastructure Management Server. Through:

- `configure` you can specify the target TrueSight Infrastructure Management Server and cell.
- `bem-connections.cfg` you can specify additional target TrueSight Infrastructure Management Servers and cells.
- `entuity.cfg` section `bem` you can set:
  - The view and user account used when from the BMC event manager accessing the Entuity server through the URL associated with the raised incident or event.
  - Change the Entuity server name, for example from the Entuity server raising an event to the Entuity consolidation server through which you want the user to access the event. You can also change the web port of the Entuity server.
- `entuity.cfg` section `bemsender` you can amend performance parameters. (See the *Entuity System Administrator Reference Manual.)*
- Event Management System you can use the Send to BMC Event Manager action within a:
  - Rule which Entuity then uses to forward events to the TrueSight Infrastructure Management Server.
  - Trigger which Entuity uses to forward the associated incidents to the TrueSight Infrastructure Management Server.

  Changes you make within an Event Management System project are applied when you save and then deploy that project.

✓ Entuity Support recommend developing forwarding rules that rely on incidents raised by Entuity. You could setup event forwarding but you are forfeiting the benefits of the incident handling mechanism. What you should avoid is forwarding a combination of events and incidents to the same TrueSight Infrastructure Management Server cell.

- A BAROC file that maps Entuity event and incident details to TrueSight Infrastructure Management Server event slots. This mapping also includes the source component's URL so from TrueSight Operations Management Operations Console you can drill-back to the event source.

Entuity is approved for use with these solutions:

- BMC TrueSight Operations Management 10.0.00
- BMC ProactiveNet Performance Management 9.6.00
- BMC ProactiveNet Performance Management 9.5.00
- BMC ProactiveNet Performance Management 9.0.50

- BMC ProactiveNet Performance Management 8.6.

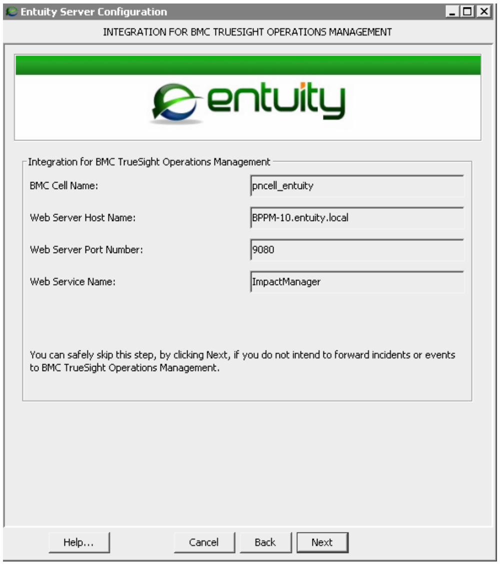
## Configure the TrueSight Infrastructure Management Server Connection

Through `configure` you can setup one TrueSight Infrastructure Management Server and cell to forward incidents and events. You can configure additional servers and cells for incident and event forwarding through `bem-connections.cfg` although you must always use `configure` to set the default connection.

> Ensure the firewall settings in the BMC II Web Services Server allow connections from the Entuity Server.

| Attribute | Description |
|---|---|
| *BMC Cell Name* | TrueSight Infrastructure Management Server instance to which Entuity forwards events or incidents.<br>A TrueSight Infrastructure Management Server administrator can find the cell name by opening:<br>`<IIWS HOME>\Tomcat\webapps\imws\WEB-INF\etc\mcell.dir`<br>and locating the cell definition, for example:<br>`cell` **pncell_entuity** `gateway.pn_server mc  entuity:1828` |
| *Web Server Host Name* | Hostname of the server where the BMC II Web Services Server is located. |
| *Web Server Port Number* | Port number used by the BMC II Web Services Server, by default **9080**. |
| *Web Service Name* | Name of the web service, by default **ImpactManager**. |

Table 40 Connection Details



Entuity Server Configuration
INTEGRATION FOR BMC TRUESIGHT OPERATIONS MANAGEMENT
entuity

Integration for BMC TrueSight Operations Management

BMC Cell Name: pncell_entuity

Web Server Host Name: BPPM-10.entuity.local

Web Server Port Number: 9080

Web Service Name: ImpactManager

You can safely skip this step, by clicking Next, if you do not intend to forward incidents or events to BMC TrueSight Operations Management.

Figure 172 Configure BMC TrueSight Operations Management

# Configure BMC TrueSight Infrastructure Management Server

TrueSight Infrastructure Management Server configuration is required to allow for Entuity to forward events and incidents to specific slots. This server side configuration also adds Entuity collectors, cancellation and deduplication rules and context cross launch. Forwarded Entuity opening and closing events are not correlated, forwarded incidents are correlated.

Entuity recommend you always consult the BMC TrueSight Operations Management documentation when configuring TrueSight Infrastructure Management Server.

## Configuring the Entuity Classes, Rules and Collectors

You must configure the TrueSight Infrastructure Management Server to handle Entuity forwarded events and incidents:

1) You must ensure the class, rules and collector files are in the appropriate folders on the TrueSight Infrastructure Management Server. If you have installed:

   - BMC TrueSight Operations Management 10.0.00, BMC ProactiveNet Performance Management 9.6.00, 9.5.00 or 9.0.50 with the Extended Repository then the class, rules and collector files are already available in the correct folders. You can proceed to Step 2).
   - BMC ProactiveNet Performance Management 8.6 then you must copy the class, rules and collector files to the correct folders.

   Copy the class, rules and collector files:

- *entuity_home*`/integ/BEM/server/etc/CELL/kb/classes/eye_event.baroc` to *MCELL_HOME*`/etc/<`*CELL_NAME*`>/kb/classes`.
- *entuity_home*`/integ/BEM/server/etc/CELL/kb/rules/eye_integration.mrl` to *MCELL_HOME*`/etc/<`*CELL_NAME*`>/kb/rules`.
- *entuity_home*`/integ/BEM/server/etc/CELL/kb/collectors/eye_collector.mrl` to *MCELL_HOME*`/etc/<`*CELL_NAME*`>/kb/collectors`.

where:

- *MCELL_HOME* is the root of the BMC Server Impact Manager.
- *<CELL_NAME>* is the name of the cell that you are forwarding events to.

2) Amend *MCELL_HOME*`/etc/<`*CELL_NAME*`>/kb/classes/.load` to include:

```
#Integration for Entuity
EYE_EVENT
```

3) Update the file *MCELL_HOME*`/etc/<`*CELL_NAME*`>/kb/rules/.load` to include:

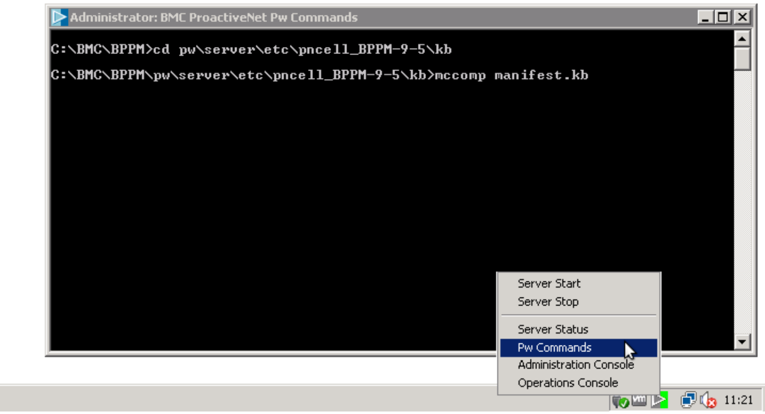
```
#Integration for Entuity
eye_integration
```

4) Update the file *MCELL_HOME*`/etc/<`*CELL_NAME*`>/kb/collectors/.load` to include:

```
#Integration for Entuity
eye_collector
```

5) Open the TrueSight Infrastructure Management Server Pw command prompt and from *MCELL_HOME*`/etc/<`*CELL_NAME*`>/kb/` run:

```
mccomp manifest.kb
```



```
C:\BMC\BPPM>cd pw\server\etc\pncell_BPPM-9-5\kb
C:\BMC\BPPM\pw\server\etc\pncell_BPPM-9-5\kb>mccomp manifest.kb
```

Figure 173 Pw Command Prompt

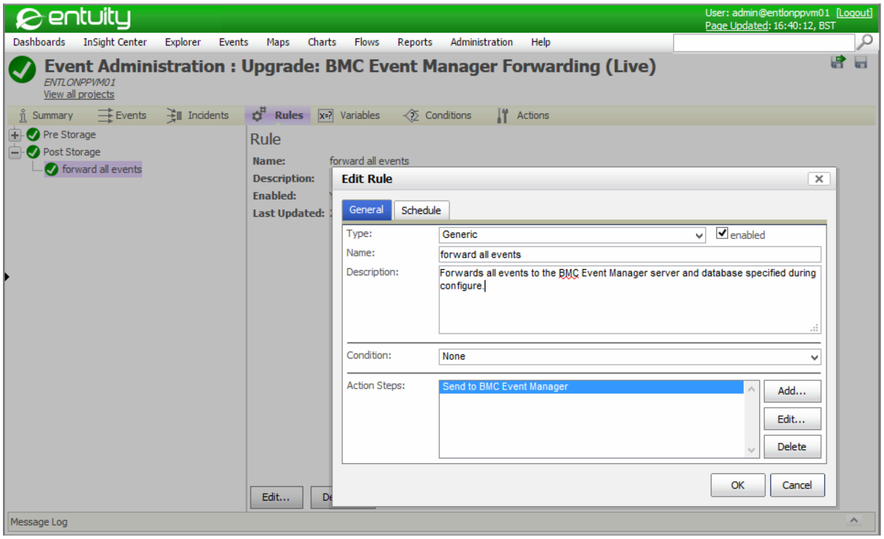
6) Restart <*CELL_NAME*>.

`mccomp manifest.kb` only has to be run once after all the files have been copied to their correct locations and the appropriate `.load` files have been updated. Once compilation is complete, the cell can be restarted.

## Set Up Event Forwarding

You can forward events to TrueSight Infrastructure Management Server using the Send to BMC Event Manager action and applying it to a rule, to forward incidents you can use the same action but apply it through a trigger. (See *Set Up Incident Forwarding*.)

When you have updated the Event Management System project with the new forwarding rule it forwards all events to the TrueSight Infrastructure Management Server and cell defined through `configure`. You can amend the rule filter to control the events forwarded and also specify alternative receiving TrueSight Infrastructure Management Servers.



Event Administration : Upgrade: BMC Event Manager Forwarding (Live)
ENTLONPPVM01
View all projects

Name: forward all events
Description:
Enabled:
Last Updated:

Edit Rule

Type: Generic ☑ enabled
Name: forward all events
Description: Forwards all events to the BMC Event Manager server and database specified during configure.
Condition: None
Action Steps: Send to BMC Event Manager

Figure 174 Setup Event Forwarding

Forwarded Entuity opening and closing events are not correlated, forwarded incidents are correlated.

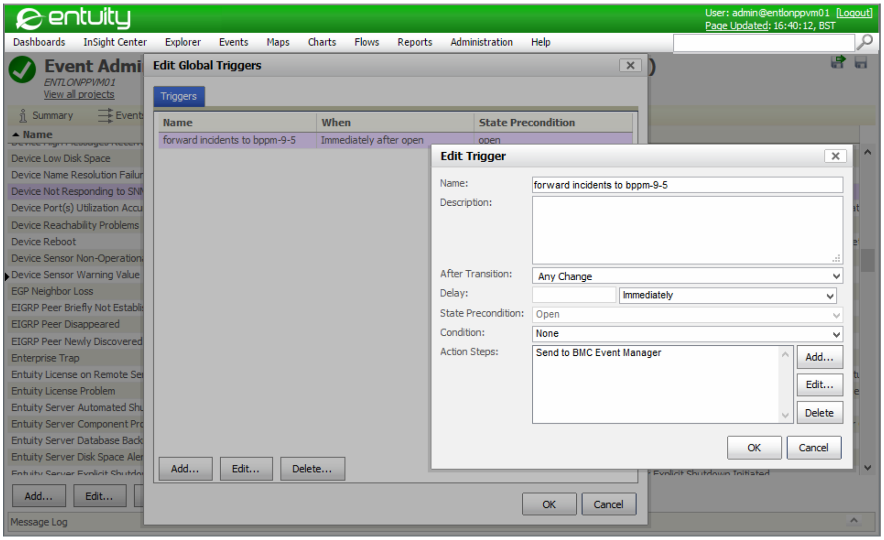
## Set Up Incident Forwarding

Through the Event Management System you can use the Send to BMC Event Manager action within a trigger to configure Entuity to forward the associated incidents to the TrueSight Infrastructure Management Server. You can configure:

- A global trigger so all incidents are forwarded to the server.
- Triggers against individual incidents to forward only those incidents.

You can forward events to TrueSight Infrastructure Management Servers using the same Send to BMC Event Manager action but applying it to a rule. (See *Set Up Event Forwarding*.)

To ensure all incidents raised against the same source are sent to TrueSight Infrastructure Management Server set *After transition* to **Any Change**, for example this ensures that closed incidents are closed on the BMC event manager and re-opened incidents are re-opened on the BMC event manager.



Edit Global Triggers

| Name | When | State Precondition |
|---|---|---|
| forward incidents to bppm-9-5 | Immediately after open | open |

Edit Trigger

Name: forward incidents to bppm-9-5
Description:
After Transition: Any Change
Delay: Immediately
State Precondition: Open
Condition: None
Action Steps: Send to BMC Event Manager

entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 16:40:12, BST
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Administration
Help
Event Admi
ENTLONPPVM01
View all projects
Summary
Events
Name
Device Low Disk Space
Device Name Resolution Failur
Device Not Responding to SN
Device Port(s) Utilization Accu
Device Reachability Problems
Device Reboot
Device Sensor Non-Operation
Device Sensor Warning Value
EGP Neighbor Loss
EIGRP Peer Briefly Not Establi
EIGRP Peer Disappeared
EIGRP Peer Newly Discovered
Enterprise Trap
Entuity License on Remote Se
Entuity License Problem
Entuity Server Automated Sh
Entuity Server Component Pr
Entuity Server Database Back
Entuity Server Disk Space Ale
Triggers
Add...
Edit...
Delete...
Delete
OK
Cancel
Message Log

Figure 175 Forward Incidents

## Forwarding Incidents and Events to Multiple Servers

By default Entuity forwards incidents and events to the TrueSight Infrastructure Management Server and cell defined through `configure`. You can specify additional TrueSight Infrastructure Management Servers and cells through *entuity_home*`\etc\bem-connections.cfg`. You can then refer to these definitions when setting up triggers and rules to respectively forward incidents and events.

When forwarding incidents and events to multiple BMC event managers through `configure` you must still define a target TrueSight Infrastructure Management Server and cell. If you do not then Entuity ignores any additional servers and cells defined through `bem-connections.cfg` and does not forward any incidents and events to TrueSight Infrastructure Management Servers.

This example:

- Forwards all incidents of severity level Severe or higher to TrueSight Infrastructure Management Server **bppm** by using a Global Trigger with the Send to BMC Event Manager action. This condition prevents Entuity forwarding incidents lower than the Severe severity level which would usually prevent the forwarding of closing incidents.
- Forwards events to TrueSight Infrastructure Management Server **bppm2** by using a Rule with the Send to BMC Event Manager action.
- Through *entuity_home*`\etc\bem-connections.cfg` defines the target TrueSight Infrastructure Management Servers and cells.

  Entuity includes a template file, *entuity_home*`\etc\bem-connections-example.cfg`, which you can copy and rename to `bem-connections.cfg`.
- Requires a target TrueSight Infrastructure Management Server is defined through `configure`, although it is not used as part of this example.

✓ Entuity Support recommend developing forwarding rules that rely on incidents raised by Entuity. Alternatively you could setup event forwarding but you are forfeiting the benefits of the incident handling mechanism. What you should avoid is forwarding a combination of events and incidents to the same TrueSight Infrastructure Management Server cell.

To forward incidents and events:

1) Through *entuity_home*`\etc\bem-connections.cfg` define the two target TrueSight Infrastructure Management Servers and cells:

```
[connection BEM1]
cellname=pncell_bppm
webServerHostName=bppm
webServerPortNumber=9080
webServiceName=ImpactManager

[connection BEM2]
cellname=pncell_bppm
webServerHostName=bppm2
webServerPortNumber=9080
webServiceName=ImpactManager
```

   It is the connection names, BEM1 and BEM2, that are used when configuring the Send to BMC Event Manager action.

   Changes to `bem-connections.cfg` are only discovered by Entuity after a restart (you do not have to run `configure` unless you want to amend the default TrueSight Infrastructure Management Server settings that are set through `configure`).

2) Access the Event Management System to define incident and event forwarding.

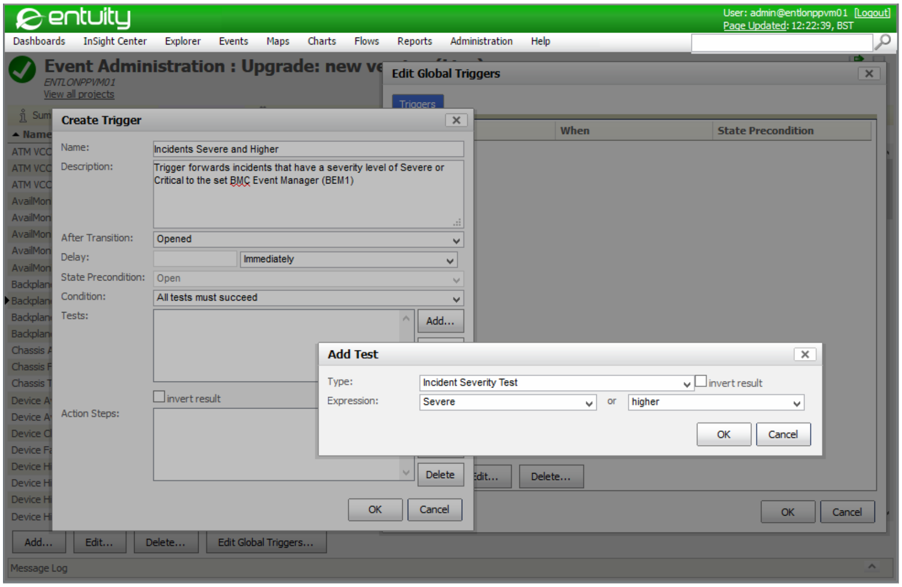
   Click **Administration** > **Events** > **Event Administration**.

3) Define the forwarding of incidents with a severity level of Severe or higher to server **bppm**.

   Click **Incidents** tab and then **Edit Global Triggers** and click **Add**.

4) Enter the trigger name and description, set *Conditions* to **All tests must succeed** and then click **Add** to define the condition test.

5) Set *Type* to **Incident Severity Test**, *Expression* to **Severe or higher** and click **OK**.



Create Trigger

Name: Incidents Severe and Higher

Description: Trigger forwards incidents that have a severity level of Severe or Critical to the set BMC Event Manager (BEM1)

After Transition: Opened

Delay: Immediately

State Precondition: Open

Condition: All tests must succeed

Tests:

□ invert result

Action Steps:

Add Test

Type: Incident Severity Test □ invert result

Expression: Severe or higher

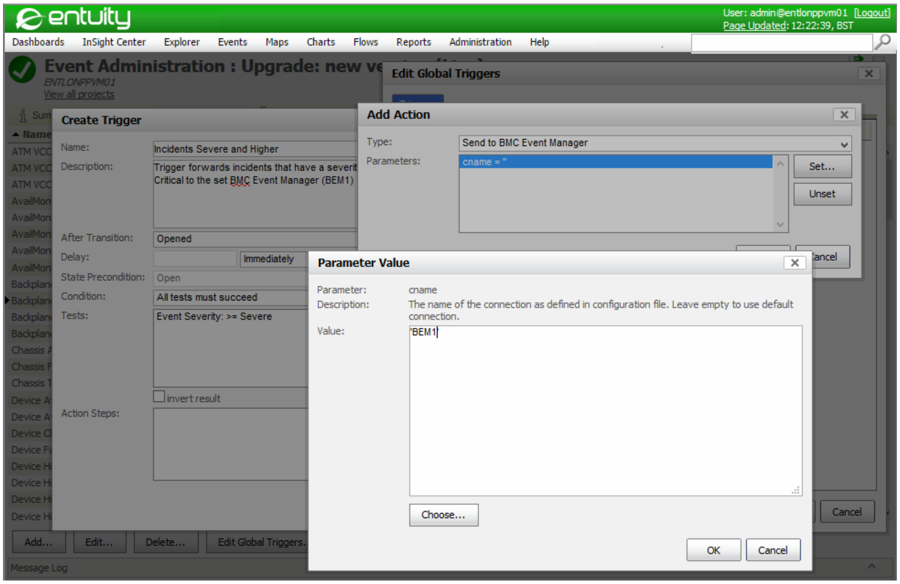
Figure 176 Add an Incident Severity Test

6) In *Action Steps* click **Add** and set *Type* to **Send to BMC Event Manager**.

   Select the **cname** parameter, click **Set** and enter the connection name as defined in `bem-connections.cfg` within the single quote marks:

   `’BEM1’`

If you do not enter a value in **cname**, leave it with its default single quotes, then Entuity uses the TrueSight Infrastructure Management Server details entered through `configure`.



Event Administration : Upgrade: new ve
ENTLONPPVM01
View all projects

Create Trigger

Name: Incidents Severe and Higher

Description: Trigger forwards incidents that have a severit
Critical to the set BMC Event Manager (BEM1)

After Transition: Opened

Delay: Immediately

State Precondition: Open

Condition: All tests must succeed

Tests: Event Severity: >= Severe

□ invert result

Action Steps:

Add Action

Type: Send to BMC Event Manager

Parameters: cname = ''

Parameter Value

Parameter: cname

Description: The name of the connection as defined in configuration file. Leave empty to use default connection.

Value: 'BEM1'

Figure 177 Add an Incident Action

7) Close and save your changes by clicking **OK** to the open dialogs.

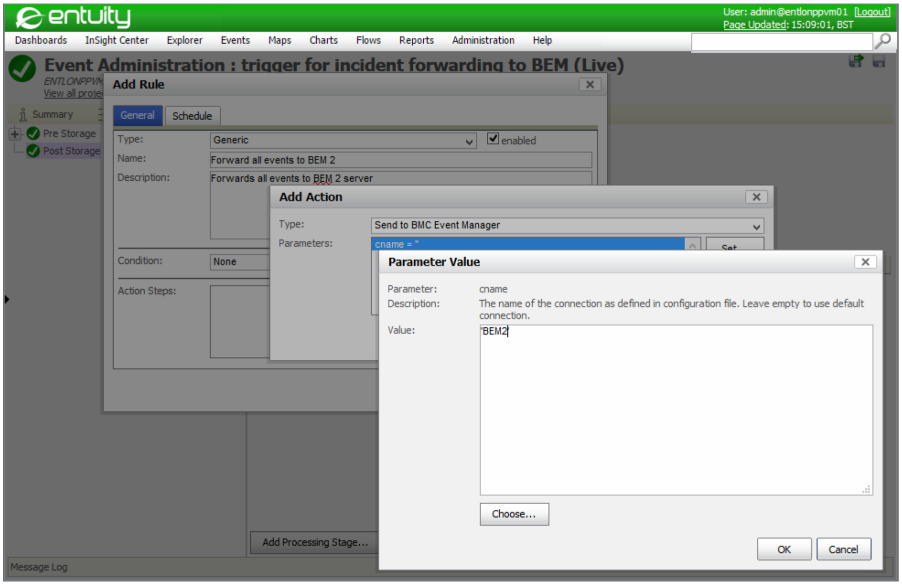
8) To define event forwarding click the Rules tab, select **Post Storage** and click **Add Rule**. Enter the rule name and description.

9) In *Action Steps* click **Add** and set *Type* to **Send to BMC Event Manager**.

   Select the **cname** parameter, click **Set** and enter within the single quote marks the connection name as defined in `bem-connections.cfg`:

   ```
   'BEM2'
   ```

If you do not enter a value in **cname**, leave it with its default single quotes, then Entuity uses the TrueSight Infrastructure Management Server details entered through `configure`.



Type: Generic ☑ enabled

Name: Forward all events to BEM 2

Description: Forwards all events to BEM 2 server

Condition: None

Action Steps:

Type: Send to BMC Event Manager

Parameters: cname = ''

Parameter: cname

Description: The name of the connection as defined in configuration file. Leave empty to use default connection.

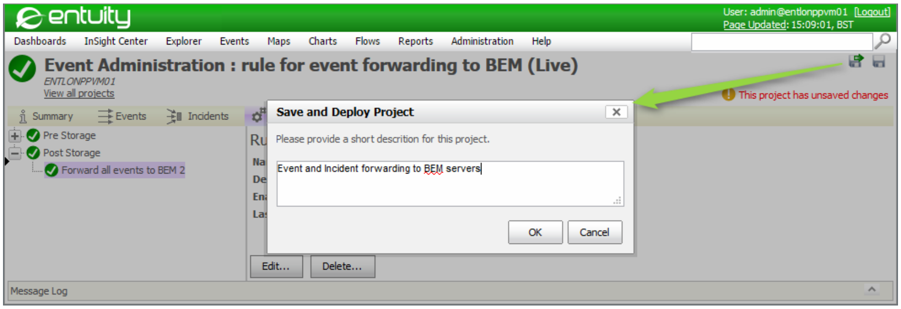
Value: "BEM2"

Figure 178 Add an Event Forwarding Rule

10) Close and save your changes by clicking **OK** to the open Event Management System dialogs.

11) Your changes are not applied to the Event Management System until you save and deploy the project.

Click the Save and Deploy icon, enter a meaningful description of your updates and click **OK**.



This project has unsaved changes

Please provide a short description for this project.

Event and Incident forwarding to BEM servers

Figure 179 Save and Deploy the Project

## Check Forwarding Performance

Entuity includes log files through which you can monitor and troubleshoot incident and event forwarding. The three log files are available from *entuity_home*`\log`.

### BemEventEngine.log

BemEventEngine.log identifies the configuration file used and the set TrueSight Infrastructure Management Servers and cells. This example identifies the connections file used and connection details of the two TrueSight Infrastructure Management Servers and cells:

```
07/15/2014 16:24:07 INFO   com.entuity.bem.eventsengine.ConfigFactory
- Found bem-connections.cfg file. Will use it.

07/15/2014 16:24:20 INFO   com.entuity.bem.eventsengine.BemConnection
- Looking for cell: pncell_bppm-2. Get CellInfo from iiws on server:
bppm-2. Total cell entries: 1

   cell pncell_bppm-2 mc bppm-2

07/15/2014 16:24:20 INFO   com.entuity.bem.eventsengine.BemConnection
- Looking for cell: pncell_bppm-9-5. Get CellInfo from iiws on server:
bppm-9-5. Total cell entries: 1

   cell pncell_bppm-9-5 mc bppm-9-5
```

This example identifies a failed connection which may be through a BEM server and cell not being defined in configure:

```
WARN   com.entuity.events.engine.util.bemsender.MisconfiguredBemSender
- BEM could not be configured or the Integration module for BMC
ProactiveNet Performance Management is not enabled.
```

### BemEventEngineSent.log

BemEventEngineSent.log lists the incidents and events that Entuity forwarded including the details sent for the TrueSight Infrastructure Management Server to handle, for example:

```
07/16/2014 14:47:32 INFO   com.entuity.bem.eventsengine.BemEventEngineSentLog
- The event has been sent to BEM (connection = 'BEM1'):
{mc_ueid=EYE.ENTLONPPVM01.MyNetwork.i133.4728, mc_long_msg=Device
Average Memory Usage High on bottom3550 - 46.047935%, critical
threshold 30%, msg=Device Average Memory Usage High on bottom3550,
severity=CRITICAL, mc_tool_sev=10, mc_tool=Eye of the Storm,
mc_tool_id=ENTLONPPVM01, mc_tool_address=10.44.2.58, mc_tool_class=Windows 7,
mc_parameter=Device Average Memory Usage High, mc_parameter_value=1,
mc_parameter_unit=i133, mc_incident_time=1405518450,
mc_object=bottom3550, mc_object_class=Device, mc_tool_key=133, mc_object_uri=http://ENTLONPPVM01/webUI/main.do?url=/webUI/objectSummary.do%3Fserver%3D205fbb05-9890-4bd3-bd62-
b359c35b3a83%26id%3D1268, mc_host=bottom3550, mc_host_address=10.44.1.12,
eye_userId=admin, eye_impact_descr=, eye_stormworks_id=1268,
eye_comp_id=4.6.0.0, eye_event_group=1,
eye_event_id=i655416, eye_view=All Objects}
```

### BemEventEngineFailedSent.log

BemEventEngineFailedSent.log lists the incidents and events that Entuity failed to send.

# Set Up Entity Object URLs

From the TrueSight Operations Management server you can access event and incident details on the originating Entuity server through the object URL. However the original URL supplied by the Entuity server must include the user credentials that would allow you access. You setup user credentials through the `bem` section of *entuity_home*`\etc\entuity.cfg`:

```
[bem]
connection_username=admin
connection_view=All Objects
```

Where:

- *connection_username* is the Entuity user account used to access the Entuity server from the associated event or incident URL.
- *connection_view* is the Entuity view used to access the Entuity server from the associated event or incident URL available.

Which events and incidents are forwarded to the TrueSight Infrastructure Management Server is determined by the conditions added to rules or triggers. The *connection_username* and *connection_view* settings must allow access to the data associated with those events and incidents for the associated URL to succeed. For example **admin** and **All Objects** provide access to all managed objects on a server, however Entuity support recommend using a non-administrator account.

## Amend Entuity Server URL Details

By default the event (or incident) URL provided by the Entuity server forwarding the event includes the details of the Entuity server that originally raised and is forwarding that event. However you may want the user to view the raised event through the Entuity consolidation server and not the originating Entuity server.

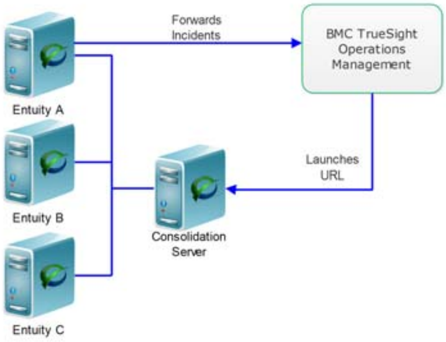


Figure 180 URL Launching the Consolidation Server

You can amend the Entuity server URL details through the `bem` section of *entuity_home*`\etc\entuity.cfg`:

```
[bem]
consolidation_server_name=entlonppvm01
consolidation_server_web_port=81
```

Where:

- *consolidation_server_name* is the resolved name of the Entity consolidation server that you want to use to access the event or incident data. This replaces the name of the Entity server that actually raised and forwarded the event or incident.
- *consolidation_server_web_port* is the port number of the Entity consolidation server that you want to use to access the event or incident data. By default it is port 80.

  If the Entity server forwarding events and incidents is using a non-default web port you can also use *consolidation_server_name* and *consolidation_server_web_port* to amend the URL to use the non-default port. You must set both parameters even when the Entity server remains the same.

## Map Severity Levels

Entity forwards events and incidents to TrueSight Infrastructure Management Server using the TrueSight Operations Management severity levels. Entity maps its event severity levels to TrueSight Operations Management severity levels through `BEMSeverityMapping.properties`. When Entity cannot make a mapping then it forwards events are forwarded with the severity level marked as UNKNOWN.

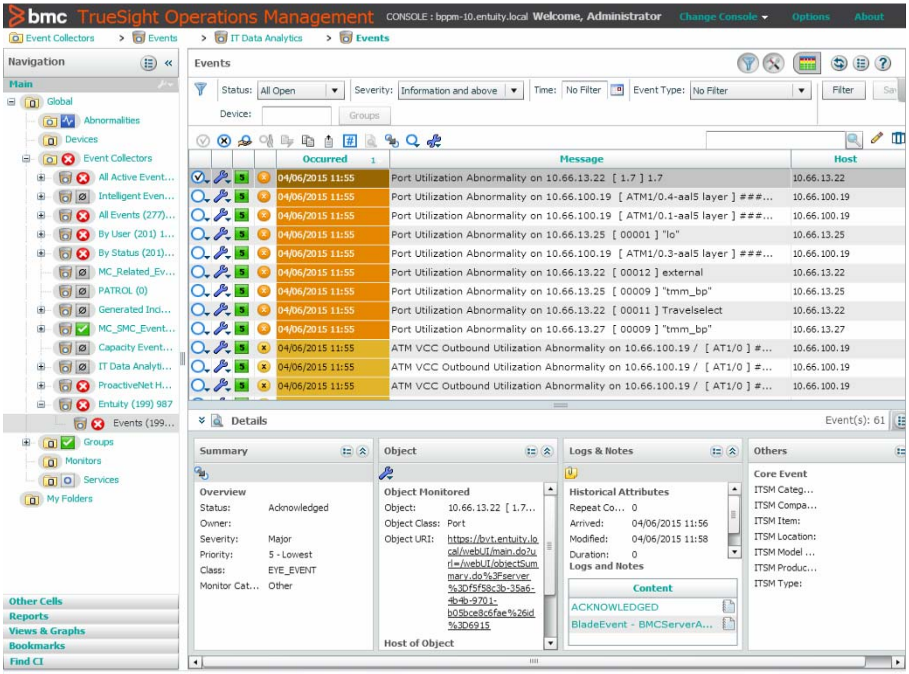
| Entity Severity | | | BMC TrueSight Operations Management Severity | | |
|---|---|---|---|---|---|
| Description | Internal Value | Color | Description | Value | Color |
| Critical | 10 | Red | Critical | CRITICAL | Red |
| Severe | 8 | Orange | Major | MAJOR | Orange |
| Major | 6 | Amber | Minor | MINOR | Amber |
| Minor | 4 | Yellow | Warning | WARNING | Yellow |
| - | - | - | Info | INFO | Blue |
| Info | 2 | Green | OK | OK | Green |
| - | - | - | Unknown | UNKNOWN | Grey |

Table 41 Map Entity and TrueSight Operations Management Severity Levels

The event severity values visible from Event Viewer run from 1 to 5, the internal values which you should use for mapping run from 2 to 10.

# Entuity Events in BMC TrueSight Operations Management

From TrueSight Operations Management event manager you have available a full history of the event including severity levels, event type, event source. You can also drill-back from TrueSight Operations Management to the event source in Entuity.



Status: All Open Severity: Information and above Time: No Filter Event Type: No Filter

Device:

| Occurred | Message | Host |
|---|---|---|
| 04/06/2015 11:55 | Port Utilization Abnormality on 10.66.13.22 [ 1.7 ] 1.7 | 10.66.13.22 |
| 04/06/2015 11:55 | Port Utilization Abnormality on 10.66.100.19 [ ATM1/0.4-aal5 layer ] ###… | 10.66.100.19 |
| 04/06/2015 11:55 | Port Utilization Abnormality on 10.66.100.19 [ ATM1/0.1-aal5 layer ] ###… | 10.66.100.19 |
| 04/06/2015 11:55 | Port Utilization Abnormality on 10.66.13.25 [ 00001 ] "lo" | 10.66.13.25 |
| 04/06/2015 11:55 | Port Utilization Abnormality on 10.66.100.19 [ ATM1/0.3-aal5 layer ] ###… | 10.66.100.19 |
| 04/06/2015 11:55 | Port Utilization Abnormality on 10.66.13.22 [ 00012 ] external | 10.66.13.22 |
| 04/06/2015 11:55 | Port Utilization Abnormality on 10.66.13.25 [ 00009 ] "tmm_bp" | 10.66.13.25 |
| 04/06/2015 11:55 | Port Utilization Abnormality on 10.66.13.22 [ 00011 ] Travelselect | 10.66.13.22 |
| 04/06/2015 11:55 | Port Utilization Abnormality on 10.66.13.27 [ 00009 ] "tmm_bp" | 10.66.13.27 |
| 04/06/2015 11:55 | ATM VCC Outbound Utilization Abnormality on 10.66.100.19 / [ AT1/0 ] #… | 10.66.100.19 |
| 04/06/2015 11:55 | ATM VCC Outbound Utilization Abnormality on 10.66.100.19 / [ AT1/0 ] #… | 10.66.100.19 |
| 04/06/2015 11:55 | ATM VCC Outbound Utilization Abnormality on 10.66.100.19 / [ AT1/0 ] #… | 10.66.100.19 |

Event(s): 61

Overview
Status: Acknowledged
Owner:
Severity: Major
Priority: 5 - Lowest
Class: EYE_EVENT
Monitor Cat… Other

Object Monitored
Object: 10.66.13.22 [ 1.7…
Object Class: Port
Object URI: https://bvt.entuity.local/webUI/main.do?url=/webUI/objectSummary.do%3Fserver%3Df5f58c3b-35a6-4b4b-9701-b05bce8c6fae%26id%3D6915
Host of Object

Historical Attributes
Repeat Co… 0
Arrived: 04/06/2015 11:56
Modified: 04/06/2015 11:58
Duration: 0
Logs and Notes

| Content |
|---|
| ACKNOWLEDGED |
| BladeEvent - BMCServerA… |

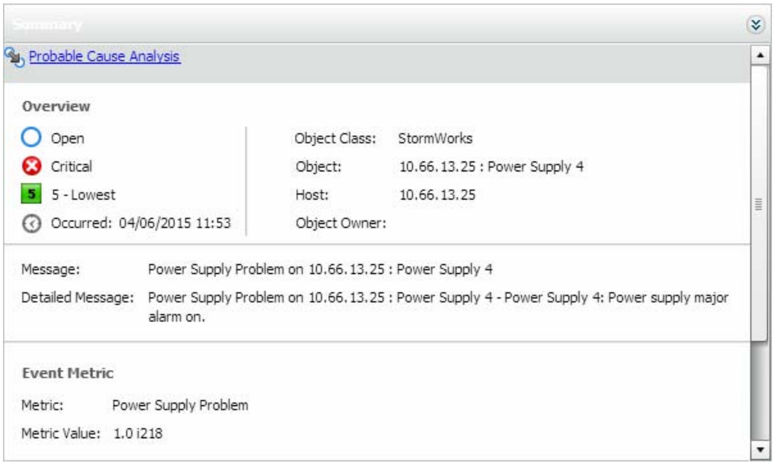
Core Event
ITSM Categ…
ITSM Compa…
ITSM Item:
ITSM Location:
ITSM Model …
ITSM Produc…
ITSM Type:

Figure 181 Entuity Forwarded Events

## Event Summary Information

The Event Information section details:

- *Status*, indicates current status of the event, e.g. Open.
- *Severity*, TrueSight Operations Management event severity.
- *Message*, Entuity event name and source Entuity server.
- *Detailed Message*, Entuity event name, source Entuity server and event details.
- *Class*, Entuity event class, EYE_EVENT.
- *Repeated*, number of times the event is repeated.
- *Metric*, Entuity event name.



Summary

Probable Cause Analysis

Overview

○ Open

Critical

5 - Lowest

Occurred: 04/06/2015 11:53

Object Class: StormWorks

Object: 10.66.13.25 : Power Supply 4

Host: 10.66.13.25

Object Owner:

Message: Power Supply Problem on 10.66.13.25 : Power Supply 4

Detailed Message: Power Supply Problem on 10.66.13.25 : Power Supply 4 - Power Supply 4: Power supply major alarm on.

Event Metric

Metric: Power Supply Problem

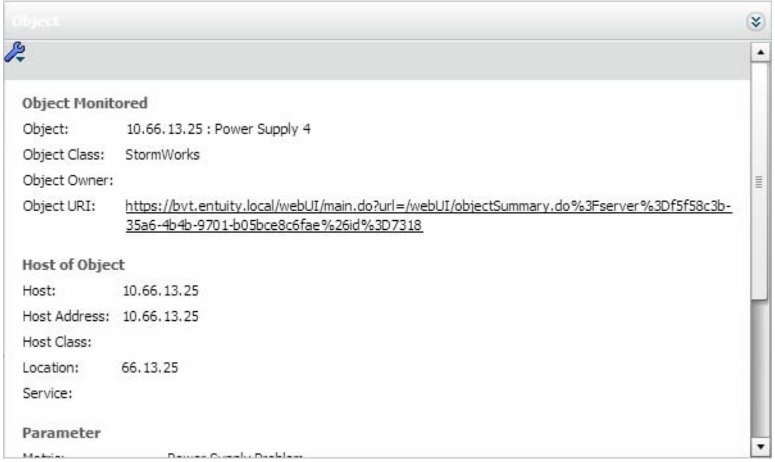
Metric Value: 1.0 i218

Figure 182 Entuity Event Summary

## Event Object Information

The Event Monitored section details:

- *Object*, identifier of the managed object, e.g. the interface on the device.
- *Object Class*, type of Entuity object, e.g. StormWorks, Device, Application.
- *Object URI*, opens the event in Entuity.
- *Host*, identifier of the managed device.
- *Parameter*, name of the Entuity event.
- *Location*, physical location of the managed object.



Object

Object Monitored

Object: 10.66.13.25 : Power Supply 4

Object Class: StormWorks

Object Owner:

Object URI: https://bvt.entuity.local/webUI/main.do?url=/webUI/objectSummary.do%3Fserver%3Df5f58c3b-35a6-4b4b-9701-b05bce8c6fae%26id%3D7318

Host of Object

Host: 10.66.13.25

Host Address: 10.66.13.25

Host Class:

Location: 66.13.25

Service:

Parameter

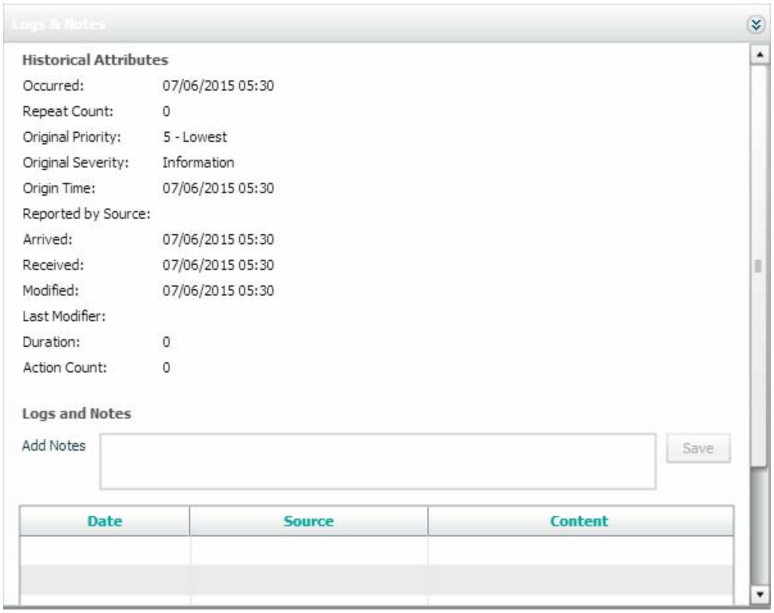
Metric: Power Supply Problem

Figure 183 Entuity Event Object Details

## Event Log and Note Information

Time Stamps section provides the event’s history:

- *Occurred*, time the event was raised in Entuity.
- *Origin Time*, time the event was raised in Entuity.
- *Arrived*, time the event arrived at the TrueSight Operations Management server.
- *Received*, time the event received at the TrueSight Operations Management server.
- *Modified*, time the event was last modified, indicating the event has been repeatedly raised.
- *Repeated*, number of times Entuity raised the event.



Logs & Notes

Historical Attributes

Occurred: 07/06/2015 05:30
Repeat Count: 0
Original Priority: 5 - Lowest
Original Severity: Information
Origin Time: 07/06/2015 05:30
Reported by Source:
Arrived: 07/06/2015 05:30
Received: 07/06/2015 05:30
Modified: 07/06/2015 05:30
Last Modifier:
Duration: 0
Action Count: 0

Logs and Notes

Add Notes

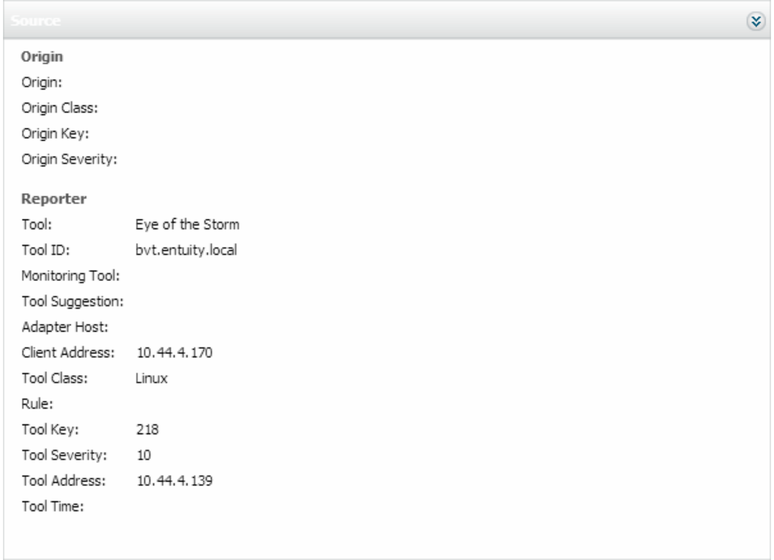
| Date | Source | Content |
|---|---|---|

Figure 184 Entuity Event Logs and Notes

## Event Source Information

Event Source section details:

- *Tool*, name of the event provider software, i.e. Entuity.
- *Tool ID*, Entuity server name.
- *Client Address*, Entuity client address.
- *Tool Class*, environment Entuity is installed to.
- *Tool Severity*, Entuity severity level.
- *Tool Address*, Entuity server IP address.



**Origin**

Origin:

Origin Class:

Origin Key:

Origin Severity:

**Reporter**

Tool: Eye of the Storm

Tool ID: bvt.entuity.local

Monitoring Tool:

Tool Suggestion:

Adapter Host:

Client Address: 10.44.4.170

Tool Class: Linux

Rule:

Tool Key: 218

Tool Severity: 10

Tool Address: 10.44.4.139

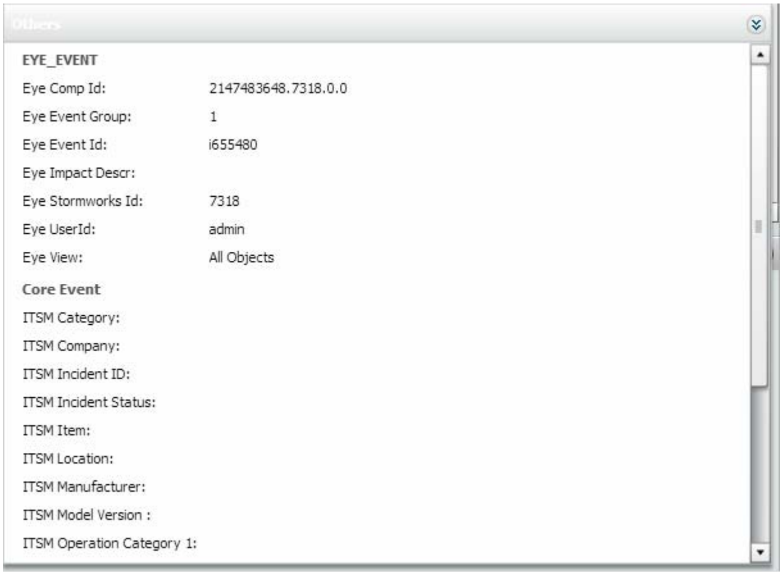
Tool Time:

Figure 185 Entuity Event Source Details

## Event Other Details

Event Other section details:

- *eye_comp_id*, internal Entuity component identifier.
- *eye_event_group* Entuity event group identifier.
- *eye_event_id*, Entuity event identifier which is unique within the event group.
- *eye_impact_descr*, indicates the impact of the network event on performance.
- *eye_stormworks_id*, internal Entuity unique object identifier.
- *eye_userID*, Entuity user account name used for forwarding events.



EYE_EVENT

Eye Comp Id: 2147483648.7318.0.0

Eye Event Group: 1

Eye Event Id: i655480

Eye Impact Descr:

Eye Stormworks Id: 7318

Eye UserId: admin

Eye View: All Objects

Core Event

ITSM Category:

ITSM Company:

ITSM Incident ID:

ITSM Incident Status:

ITSM Item:

ITSM Location:

ITSM Manufacturer:

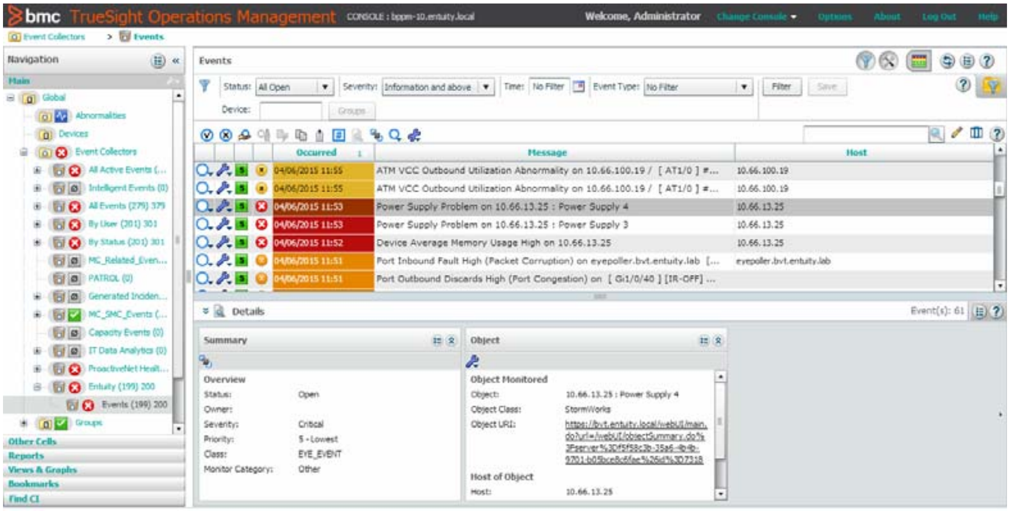
ITSM Model Version :

ITSM Operation Category 1:

Figure 186 Entuity Event Other Details

## Launch Entuity

You can launch Entuity from the TrueSight Operations Management event manager. This launch uses the *Object URI* available from the event's object panel, displaying the event's object details in Entuity.



Status: All Open
Severity: Information and above
Time: No Filter
Event Type: No Filter
Device:

| Occurred | Message | Host |
|---|---|---|
| 04/06/2015 11:55 | ATM VCC Outbound Utilization Abnormality on 10.66.100.19 / [ AT1/0 ] #... | 10.66.100.19 |
| 04/06/2015 11:55 | ATM VCC Outbound Utilization Abnormality on 10.66.100.19 / [ AT1/0 ] #... | 10.66.100.19 |
| 04/06/2015 11:53 | Power Supply Problem on 10.66.13.25 : Power Supply 4 | 10.66.13.25 |
| 04/06/2015 11:53 | Power Supply Problem on 10.66.13.25 : Power Supply 3 | 10.66.13.25 |
| 04/06/2015 11:52 | Device Average Memory Usage High on 10.66.13.25 | 10.66.13.25 |
| 04/06/2015 11:51 | Port Inbound Fault High (Packet Corruption) on eyepoller.bvt.entuity.lab [... | eyepoller.bvt.entuity.lab |
| 04/06/2015 11:51 | Port Outbound Discards High (Port Congestion) on [ Gi1/0/40 ] [IR-OFF] ... | |

Event(s): 61

Overview

Status: Open

Owner:

Severity: Critical

Priority: 5 - Lowest

Class: EYE_EVENT

Monitor Category: Other

Object Monitored

Object: 10.66.13.25 : Power Supply 4

Object Class: StormWorks

Object URI: https://bvt.entuity.local/webUI/main.do?url=/webUI/objectSummary.do%3Fserver%3Df5f58c3b-35a6-4b4b-9701-b05bce8c6fae%26id%3D7318

Host of Object

Host: 10.66.13.25

Figure 187 Launching Entuity in Context

# 31 Manage Entuity Security

Management of the network infrastructure requires access and knowledge, which if not carefully controlled can lead to failures in the security of the network. An often conflicting requirement to maintaining high security is ease of management; security too complicated to maintain becomes no security.

Entuity security can be implemented to the depth that your management practices, and your Entuity implementation requires. The key components of security are:

- User authentication, which you can configure:
  - Internally, where you define user accounts on the Entuity server.
  - Externally, where user accounts are derived from a mapping of user groups in Entuity to user accounts, and or user groups, defined through an LDAP environment.
- User groups against which you can associate tool and report permissions.
- Views through which you access objects and their data managed by Entuity. You can control the role of views by configuring the content and content filters, event and incident filters and access control.
- In multi-server installations configuring trust between servers.

## Entuity User Authentication

You can configure Entuity User Authentication to run using:

- Internal authentication, where Entuity compares user sign on details with the details held for that account in the Entuity server's local security database. On successful authentication Entuity assigns user permissions derived from the user groups the user's account is associated with.
- External authentication compares user sign on details with the account details held in the external authentication system (LDAP). When successful Entuity User Authentication derives the account's network group membership and maps these to the Entuity user groups, deriving the Entuity user account permissions.

## Control User Access to Entuity Functionality

Each Entuity user is a member of one or more user groups. It is through the user group that users inherit their access rights, e.g. what views they can access, what tools they can use, reports they can create or run. This inheritance is additive. For example, where a user belongs to two user groups one which permits members access to a particular function which the other denies, then the user has access to that function.

## Control Access to the Network Using Views

Entuity can manage large, extensive networks. Views allow you to compartmentalize the network, making the network both easier to manage and easier to match to your business model. For example, views can be created to reflect the different costing groups on your network, different geographical locations of hardware or the different support teams managing the network and its services.

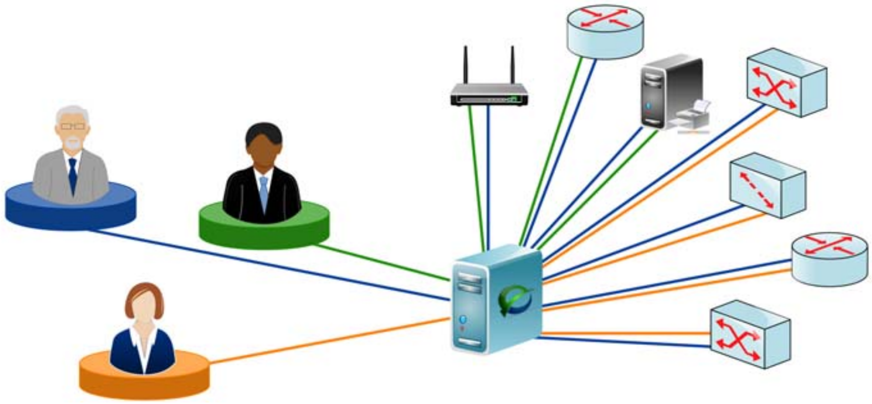


Figure 188 Users with Different View Permissions

## Set the Scope of a View

A view's target domain sets the scope of a view. Entuity provides two mechanisms for populating view content:

- Manual, where you drag and drop managed objects into a view.
- Automatic, where you select one or more views as the base for the new view.

  You can control whether the new view potentially contains all objects within its base views (union) or just those objects that are in all of its base views (intersection).

Filters determine what managed objects within that scope are displayed in the view:

- Content filters determine the network components that are displayed for a view, for example through Explorer.

  A view content filter is a defined set of rules that determines which of the network objects, e.g. devices, ports, services, potentially available in a view are actually displayed. Filters allow the content of a view to change as the objects that meet its criteria change.

- Event filters determine the events that are displayed for a view.
- Incident filters determine the incidents that are displayed for a view.

You can create content filters that restrict the view to show only the particular components of the network in which you are interested, e.g. uplink ports. You can use the same filter against a number of views.

Entuity is supplied with default filters applied to each user's My Network (*username*) view. Although you cannot change these default filters, if you have the appropriate view permission you can make copies of them and amend those copies. You can:

- Change the event and incident filters applied to a user’s My Network view but not its content filter (All Objects).
- Not change the My Network view of an administrator.

### Assigning Views to Users

Once you create a view you can associate it through user groups to users. User group settings also determine which users can create and amend views, although any user can be assigned view ownership. A view owner has administrator rights over that view.

## Entuity Multi-Server Administration

Entuity Multi-Server Administration allows you to configure trust between servers. Once established an administrator on one server, can view through the Status Summary (all servers) and Entuity Health Summary pages details of another. Administrators can also launch the client of the remote Entuity server, although they will have to login.

Within an Entuity multi-server environment an Entuity server can act as both a central server and as a remote server. A central server has access to other remote Entuity servers.

### An Example Multi-Server Configuration

Consider a network managed by four Entuity servers. You may want to grant one server, Entuity Server 1, access to the other three servers. You grant access by logging into Entuity Server 1 and entering access details for the other three servers through the Remote Entuity Servers page.

You can check this access by logging into one of the remote servers, e.g. Entuity Server 3, and through its Central Entuity Servers page confirming Entuity Server 1 is listed. From this page you can revoke the access permission of Entuity Server 1.

# 32 Views of the Managed Network

Entuity can manage large, extensive networks, and you can use views to compartmentalise the network, building a hierarchy of views to make the network both easier to manage and a better match your business model. For example, you can create views to reflect the different costing groups on your network, different geographical locations of hardware, the different teams managing the network and its services.

Once a view is created then it can be associated through user groups to users. User group settings also determine which users can create and amend views, although any user can be assigned view ownership. A view owner has an advanced set of rights over that view. The permissions a user has on a view are the same permissions they have to a map, as a map is only a visual representation of a view.

## Manage Views

Entuity views perform two roles, they:

- Determine the managed objects a user is permitted to view.

  Members of the Administrators user group have access to all views, and therefore to all content.

- Allow users to group, monitor and report on network objects. They provide the lens through which users can view the network objects to which they are permitted access.

Views allow both administrators and ordinary users to present and access the network in chunks that fit how the network should be best managed. Users can be given views that allow them to focus on the area of the network that is of interest to them, and given access rights to build their own views. As users can only view the objects in their My Network view, any views they build are within that scope. The My Network scope is determined by whether the user is:

- A member of the Administrators user group, in which case they would have access to all managed objects on a server. This is equivalent to the content of that server's All Objects view.
- Not a member of the Administrators user group, in which case they would have access to only the managed objects in the views associated with their user groups or in the views to which they are assigned ownership.

Entuity also distinguishes between those views a user can edit and those to which they only have access to view. Entuity identifies read only views by applying a padlock to the view icon in the Explorer tree.

When creating or changing views you should first set up the User Groups, and the users to be assigned to the different User Groups. When you then create views you are also ready to assign user group access. However you can always subsequently amend the user groups assigned to a view and the user assigned ownership of the view.

## All Objects View

Each Entuity server has only one All Objects view. It is a system view, (the owner is **system**) that includes all of the network objects and services under the management of that server.

By default only members of the Administrators user group have access to the All Objects view and their edit capability is limited to assigning access and edit permissions to other user groups. Those non administrator users with edit permission to the All Objects view can only edit it, i.e. assign access to other user groups, if they have the Share View permission.

To those users that have access to it is always the first in any displayed list of views, for example it is at the top of the Explorer tree and at the top of drop-down lists when defining reports. (It also has the internal view id of 1.)

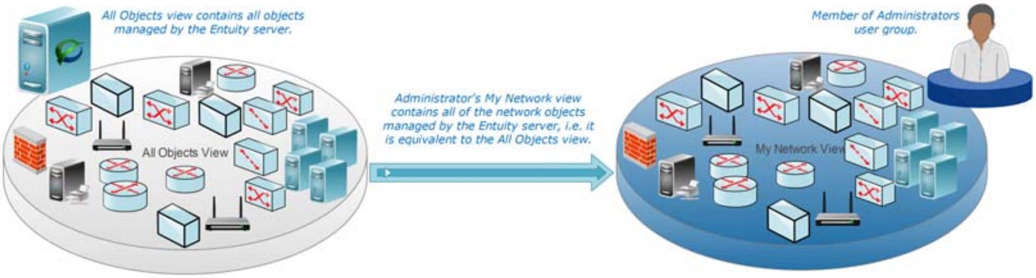

All Objects view contains all objects managed by the Entuity server.
All Objects View
Administrator's My Network view contains all of the network objects managed by the Entuity server, i.e. it is equivalent to the All Objects view.
Member of Administrators user group.
My Network View

Figure 189 System Administrator My Network View

## My Network View

Each user has their own My Network view. It contains all of the managed objects a user's permissions allow them to access; the sum of the content of all of the views to which they have access.

Every user has their own My Network view:

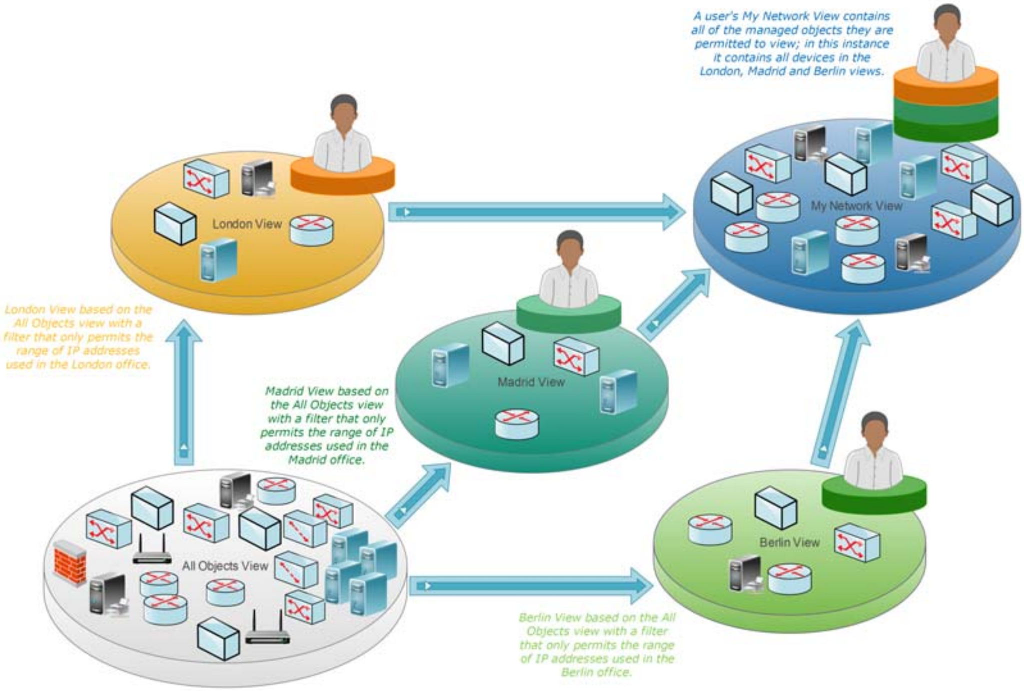
- With their user name in brackets, e.g. **My Network (jamessmith)**, **My Network (meichen)**.
- Which is their default view. The default view is configurable through user Preferences.
- That is Private to that user and cannot be accessed by non-administrators. Administrators, through the user preferences setting *Exclude other user's private Views*, can access all views.
- That is displayed after the All Objects view. When administrators can see other users' My Network views, these are sorted in alphabetical order.

My Network is a system view. Although administrator's cannot amend the content displayed in My Network views they can control the events and incidents available in the view by changing the event and incident filters.

A user who is:

- A member of the Administrators user group can view all managed objects through My Network. Although administrator's My Network view and the All Objects view have an equivalent content they have different roles, for example you:
  - Should associate any report schedules to your private My Network view and not the public All Objects view.
  - Always have access to your My Network view whereas access to the All Objects view is by default dependent on remaining a member of the Administrators user group.
- Not a member of the Administrators user group can only view through My Network the managed objects to which they are permitted access through the union of content of views to which they are permitted access.

When an administrator removes a user account from Entuity, Entuity deletes their My Network view. Entuity does not delete any other views of which they are the owner, those views remain but without an owner. When you next edit the view you must assign a new view owner.



A user's My Network View contains all of the managed objects they are permitted to view; in this instance it contains all devices in the London, Madrid and Berlin views.

London View based on the All Objects view with a filter that only permits the range of IP addresses used in the London office.

Madrid View based on the All Objects view with a filter that only permits the range of IP addresses used in the Madrid office.

Berlin View based on the All Objects view with a filter that only permits the range of IP addresses used in the Berlin office.

Figure 190 Users and My Network Views

## View Names and View Paths

When creating views you should consider their purpose and name them accordingly. In large implementations, with many Entuity servers a meaningful naming convention can assist usability.

Entuity permits most characters in view names, for example:

```
a-z, A-Z, 0-9, space, # & * ( ) < > : @ ’
```

Entuity excludes these characters from view names:

- / Forward slashes, as they are used to delimit view paths.
- \ Backslashes, to avoid confusion with file paths.
- :: double colon sequence as it is a reserved character sequence. Entuity will allow a single colon.

A naming convention should also consider that view names are case sensitive, for example **Berlin Office** and **Berlin office** are considered as two separate views. Entuity also sorts views on their name, sorting on case-insensitive alpha-numeric comparisons. Entuity therefore ignores casing during sorting and embedded integers are compared using their numeric value.

When copying a view if a view with the same name already exists at the destination Entuity automatically appends an integer enclosed in brackets to the view name. The integer is the next available integer which would usually be 1, for example **Berlin Office(1)**.

On each server a view name must be unique, or more accurately the view path must be unique. For a view created against the server root, view name and view path are the same. For a view created as a sub-view of another view, the view name does not have to be unique but its view path must be unique.

A view path is built from the view name and any parent view. For example London Office and Berlin Office are views created against the Entuity server root. They each have a sub-view called Switches, this is permitted as their view paths are unique.

| View Name | View Path |
|---|---|
| London Office | London Office |
| Berlin Office | Berlin Office |
| Switches | London Office/Switches |
| Switches | Berlin Office/Switches |

Table 42 View Names and View Paths

In multi-server environments, different servers may have views with the same view path, for example every installation is supplied with the My Network (admin) view. Also, when logged into multiple servers and operating in consolidation mode, if you create a view each Entuity server to which you are logged in attempts to create that view. Creating views in consolidation mode is the recommended approach when you want to use views with the same name across more than one server, for it ensures the:

- View names are exactly the same. Entuity is case sensitive, for example **Berlin Office** and **Berlin office** are considered as two separate views.
- View definition is the same, at least at the time it was created.

You can use the View Hierarchy report to check for consistency across servers. It is available from the Administration reports section.

## Set View Content

You can set the content of a view by defining its content scope as:

- Manual, you would then drag and drop managed objects into the view.
- Automatic based on none, one or more views:
  - Entuity includes one predefined view, All Objects, on which you can base other views. All Objects view includes all managed objects and services on the Entuity server.
  - You cannot use a My Network view as the base for another view.
  - You can base a view on other user defined views to which you have read access. However you cannot use a view as a base view to the current view if the current view acts as a base to that view. For example if Key Devices view uses Routers view as a base you cannot then amend the Routers view to use the Key Devices as a base view, Entuity prevents this type of cyclic dependency.

    A user of the derived view only requires read access to that derived view, they do not require read access to the views on which it is based. This is a key component of controlling user access to managed content.
  - A view may not have a base view, either because one was not selected when the view was configured or because its original base views have been subsequently deleted. An automatic view without a base view will be empty unless you add services or sub-views to it.

  You can control whether the new view potentially contains all objects within its base views (union) or just those objects that are in all of its base views (intersection).

You can edit a view and change it from a Manual view to an Automatic view, or from an Automatic to Manual view. However Entuity does not combine the two states, for example if you have added devices to a Manual view and then change it to an Automatic view Entuity removes all manually added devices from the view.

You can further control view content by applying a filter. A view content filter is a defined set of rules that determines which of the network objects potentially available in a view are actually displayed. Filters allow the content of a view to change as the objects that meet its criteria change. You can also set whether to include to or exclude services from the view.

Content filters apply to the content in the view directly added to the view, either through base views or manually dragged into the view. They do not apply to managed objects inherited from sub-views or through services.

There are two predefined content filters:

- All Objects includes all objects within the content scope of the view.
- Infrastructure Only displays all infrastructure ports and their associated devices, VLANs and applications. Infrastructure ports are either uplinks, i.e. ports connecting routers with switches, trunk ports, i.e. ports connecting switches together, or router ports.

You can also restrict the potential events and incidents Entuity can raise against objects within a view. By default a view’s event and incident filters allow Entuity to potentially raise any event or incident. An event or incident filter allows you to include only the event or incident types you want to be available in a view, and exclude those that you do not.

All users who are not in the Administrators user group are initially restricted to their own read only My Network view, which would be empty until their user profile is associated to user groups against which populated views are associated (or they are assigned ownership of populated views).

An additional view, All Objects by VTP, shows VLANs and devices grouped by VTP domain name. You can create this view by running `vtpDomainTool`.

The following table shows the content scope and filters of three example views:

- My Network (*username*) is a predefined read-only view that displays the managed network available to that user, which is the product of the union of all views to which the user has access. An administrator could restrict the user’s access to events and filters but in this example does not.
- New York is a user defined view. It uses the All Objects view as its base with an IP Range content filter, which filters into the view devices within the specified address range which in this example corresponds to the New York office.
- New York Managed Hosts is a user defined view. It uses a more complex filter to only include managed hosts within the IP Range, which again restricts the view to the New York office. Event and incident filters also restrict the view’s events and incidents.

| View | Base Views | Content Filter | Event Filter | Incident Filter |
|---|---|---|---|---|
| My Network (*username*) | Union of all user’s views | All Objects | All Events | All Incidents |
| New York | All Objects | IP Range | All Events | All Incidents |
| New York Managed Hosts | All Objects | Managed Hosts<br>IP Range | Selected Device Events | Selected Device Incidents |

Table 43 Predefined and User Defined Views

For more details on controlling view content see *Chapter 33 - Manage View Filters*.

## View Hierarchy

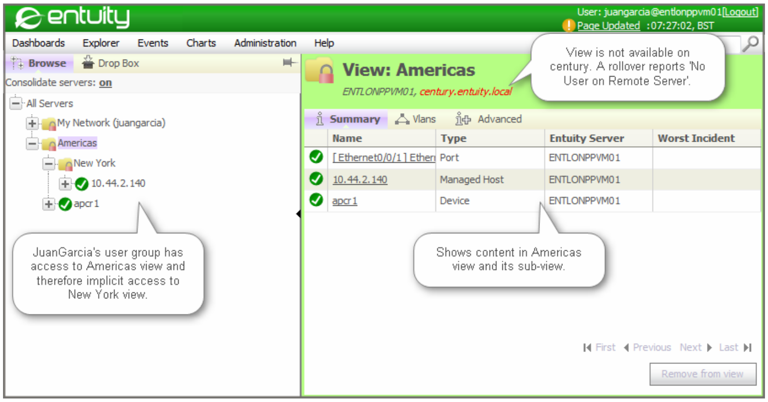
You can build a hierarchy of views. A root view sits against the Entuity server. Within it you can specify sub-views and within those sub-views more sub-views and so on.

The root view inherits the contents of all of its sub-views, similarly sub-views inherit all of their sub-view content. You can view these inherited objects, e.g. devices, ports, services, applications, through the view Summary panel, they are not displayed against the view in the Explorer Browse tree. Only objects directly added to a view, either manually or through a filter, are displayed in the Browse tree. These objects are also added to the list of managed objects displayed in the view Summary page.

When building a hierarchy of views ensure user access at each level of the view meets your requirements. If you grant a user access to a:

- Parent view the user has implicit access to all of its child views. When you create or modify a view Entuity warns you of user groups that have implicit access to the view.

  You can only remove this implicit access by modifying user access to the parent view or changing the current child view's position in the view hierarchy.



| Name | Type | Entuity Server | Worst Incident |
|---|---|---|---|
| [Ethernet0/0/1] Ethern | Port | ENTLONPPVM01 | |
| 10.44.2.140 | Managed Host | ENTLONPPVM01 | |
| apcr1 | Device | ENTLONPPVM01 | |

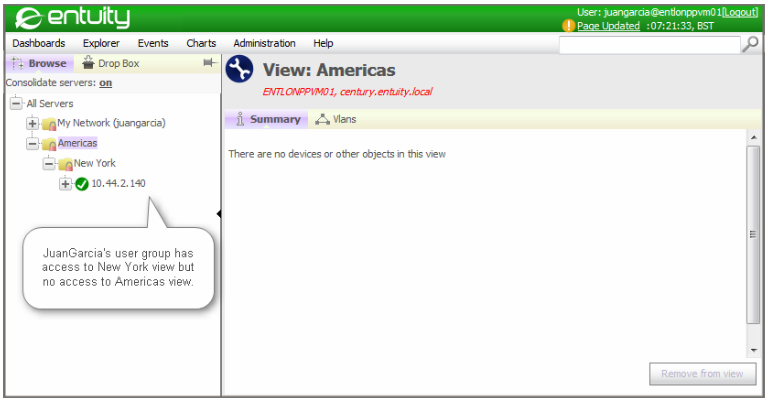
View is not available on century. A rollover reports 'No User on Remote Server'.

JuanGarcia's user group has access to Americas view and therefore implicit access to New York view.

Shows content in Americas view and its sub-view.

Figure 191 Implicit Access to a Views in a Hierarchy

- Child view (sub-view) the user does not inherit access to the content of the parent view. The parent view is available in the Explorer tree but its content is hidden from the user.



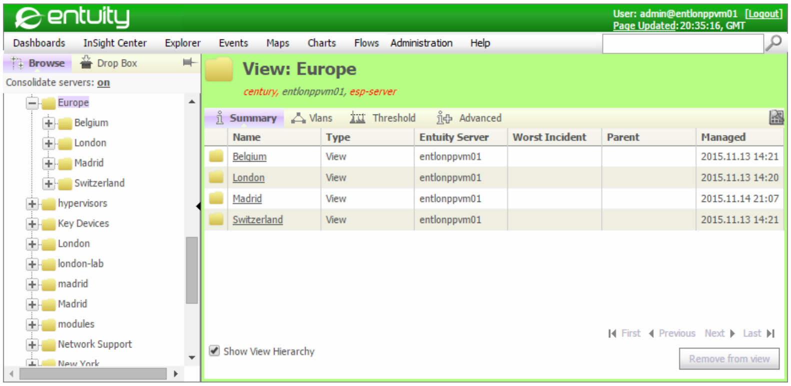
There are no devices or other objects in this view

JuanGarcia's user group has access to New York view but no access to Americas view.

Figure 192 Restricted Access to a Hierarchy of Views

## Use the Browse Tree to Navigate View Content

The Browse tree is a key tool in navigating views and their content. In multi server installations you can set *Consolidate Servers* to **on** to combine all views with the same name on currently connected remote servers.



User: admin@entlonppvm01 [Logout]
Page Updated:20:35:16, GMT

Consolidate servers: on

View: Europe

century, entlonppvm01, esp-server

| Name | Type | Entuity Server | Worst Incident | Parent | Managed |
|---|---|---|---|---|---|
| Belgium | View | entlonppvm01 | | | 2015.11.13 14:21 |
| London | View | entlonppvm01 | | | 2015.11.13 14:20 |
| Madrid | View | entlonppvm01 | | | 2015.11.14 21:07 |
| Switzerland | View | entlonppvm01 | | | 2015.11.13 14:21 |

☑ Show View Hierarchy

Figure 193 Show View Hierarchy Set to On

When you highlight a view from the Explorer tree you can:

- Use the Explorer tree to display:
  - Objects directly in the view, for example devices, services, network paths. It does not display objects inherited from child views.
  - Ports with devices in the view, but not ports inherited from sub-views.

  You would navigate down to the sub-view to see the devices and ports within them.
- Use the Explorer View Summary panel to display all objects in the view and its sub-views:
  - Devices.
  - Ports added directly to the view.
  - Services.
  - Network Paths.
  - Managed objects inherited from sub-views.
  - Orphaned ports, these are ports that do not have a device in the current view.
  - Applications.

  You can change the display of the Summary panel by selecting Show View Hierarchy. This limits the display of objects to only those objects in the view, with sub-views listed and hyperlinked allowing you to drill-down to the sub-view's content.
- Click on Maps. Entuity displays the view map.

You can access VLAN details through their association to ports, an association accessible through the port's Advanced tab.

# View Management

Administrators, and users with the appropriate permissions, can create and edit view definitions. Administrators can assign Create Views, Share Views and Edit View Filters tool permissions to user groups.

The Create View and Edit View dialogs have the same tabbed layout, each tab allowing you to configure a particular aspect of a view. View configuration tabs are:

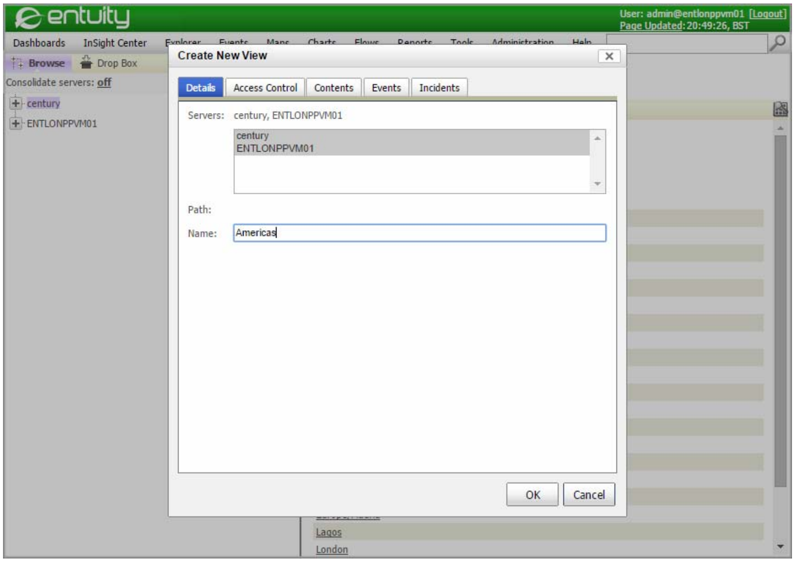
- View Details
- View Access Control
- View Content Scope
- View Event Filters
- View Incident Filters.

## View Details

Through the Details tab you can define on what servers the view is created, identify where in the view hierarchy the view sits, its view path, and set the view name.

| Attribute | Description |
|---|---|
| *Server* | Server on which you create the view.<br>When you are logged into multiple servers and have *Consolidate servers* set to **on**, it is set to **all servers**. You can click on **all servers** to view the available server and select only those on which you want to create the view. |
| *Path* | The location of the view in the view hierarchy. For example a new view with:<br>■ An empty path would be a view at the root of the hierarchy.<br>■ A path of Regions indicates it is a sub-view of Regions.<br>You cannot amend *Path*, it is determined from where in Explorer you create the view (or from the command line in what you explicitly define). |
| *Name* | View name should be unique and clearly identify its purpose. Entuity supports these characters for view names a-z, A-Z, 0-9, space, # & * ( ) < > : @ ’ |

Table 44 Set View Details



Create New View

Servers: century, ENTLONPPVM01

century
ENTLONPPVM01

Path:

Name: Americas

Figure 194 Set View Details

## View Access Control

Through the Access Control tab you can:

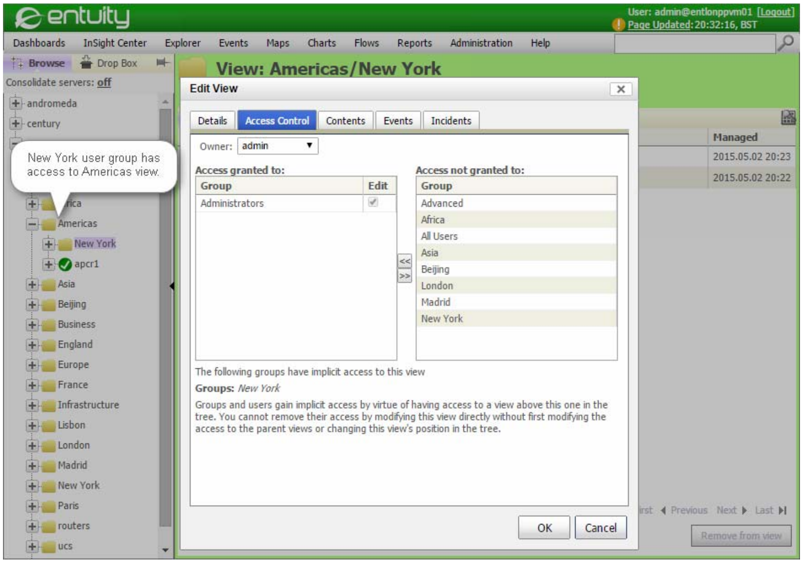
- Set the user who owns the view. In giving users view ownership you assign them more control over the view. It can also give users access to a view to which they otherwise would not have access (i.e. their user group permissions are insufficient).
- Control the user groups associated with the view, and therefore the users who have access to it.

| Attribute | Description |
|---|---|
| *Owner* | Sets the user who owns the view, which by default is the user creating the view.<br>As an administrator you can assign the view to another user, although when:<br>■ Running with consolidation on in multi-server environments the selected user must be available on all servers.<br>■ You only had access to the view because you were the owner, you may no longer see the view in Explorer. To access this now hidden view you can set your preferences to view other user’s private views.<br>**system** is the owner of the All Objects view and cannot be amended. |

Table 45 Set View Access Control

| Attribute | Description |
|---|---|
| *Access Granted to* | Sets which user groups, and therefore members of those groups, have access to the view.<br>When set to **Edit** the user can amend the view, e.g. change its name, add new content, create sub-views.<br>Entuity lists user groups and users that inherit access to the view. Inheritance is by having access to a view higher in the view hierarchy. For example if a user has access to the parent view Americas they also have access to its child view New York. You can only remove their access by modifying their access to the parent view or changing the current view's position in the view hierarchy. |

Table 45 Set View Access Control



New York user group has access to Americas view.

View: Americas/New York

Edit View

Details | Access Control | Contents | Events | Incidents

Owner: admin

Access granted to:

| Group | Edit |
|---|---|
| Administrators | ✓ |

Access not granted to:

| Group |
|---|
| Advanced |
| Africa |
| All Users |
| Asia |
| Beijing |
| London |
| Madrid |
| New York |

The following groups have implicit access to this view

**Groups:** *New York*

Groups and users gain implicit access by virtue of having access to a view above this one in the tree. You cannot remove their access by modifying this view directly without first modifying the access to the parent views or changing this view's position in the tree.

OK Cancel

Figure 195 Implicit View Access

## View Content Scope

Through the Contents tab you control the managed objects included to the view. You set the:

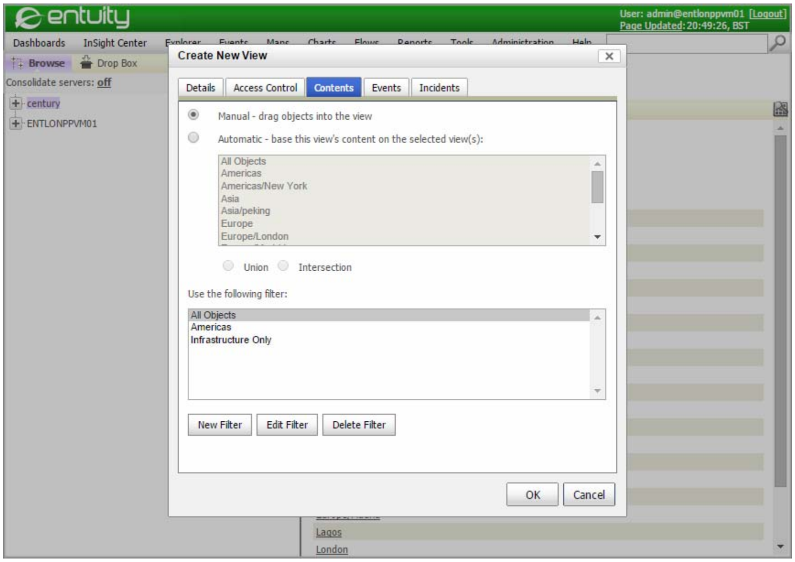
- Content scope of the view which limits what a view can potentially display. When you want a view with a:
  - Static set of managed objects, create a manual view type which through Explorer you can later drag and drop into it managed objects.
  - Dynamic set of managed objects create a view based on one or more other views. Entuity can update the content of this view if one or more of its base views change.
- Content filter which is applied to the view content scope. It only allows into the view those objects that meet the filter criteria. For example:

- All Objects filter displays all objects within the content scope.
- Infrastructure Only displays only the infrastructure ports within the view.

You can also define your own filters.

| Attribute | Description |
|---|---|
| *Manual* | Creates a view that is initially empty, you must manually add objects to it. |
| *Automatic* | Allows you to highlight one or more views on which to base the current view. A base view is one on which another view is based. All views apart from My Network views can act as a base view (although Entuity does prevent cyclic dependencies). |
| *Union / Intersection* | You can base a view on more than one view, selecting whether the content of the new view is derived from the union or intersection of objects in the selected views:<br>■ **Union**, results in a view that contains all of the objects in the selected views.<br>■ **Intersection**, results in a view that contains only the objects that are in all of the selected views. For example this allows users to implement the concept of tagging, e.g. create a view that is based on the intersection of particular services, key devices and area office views.<br>If you alter the contents of a base view or remove a view from a union or intersection definition this alters the resultant view. If you delete a base view Entuity raises a warning and lists the impacted views, Entuity does not warn if you edit a view. |
| *Use the Following Filter* | A content filter allows you to use a defined set of rules, which when an object's attributes meet those rules allows it to be included into the view. |

Table 46 Set View Contents



● Manual - drag objects into the view

○ Automatic - base this view's content on the selected view(s):

All Objects
Americas
Americas/New York
Asia
Asia/peking
Europe
Europe/London

○ Union ○ Intersection

Use the following filter:

All Objects
Americas
Infrastructure Only

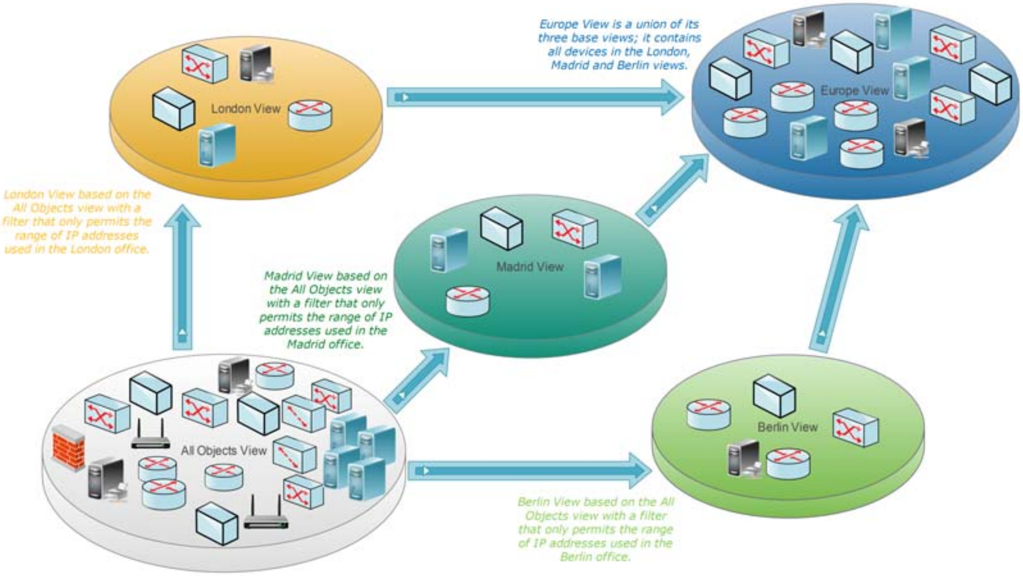
Figure 196 Set View Contents

## Union and Intersection of Views

An automatic type view is based on one or more other views. When you select multiple views you also select whether to include all of the content of the source views (**union**) or only the content that appears in all of the source views (**intersection**).

When a selected base view has child views the content of those child views is included when applying the union or intersection.

Setting the content scope of a view as the union of its base views results in a view that contains all of the objects in the selected base views. For example you may have views for each of your European offices and then create a regional view (Europe) based on the union of those offices.



Europe View is a union of its three base views; it contains all devices in the London, Madrid and Berlin views.

London View based on the All Objects view with a filter that only permits the range of IP addresses used in the London office.

Madrid View based on the All Objects view with a filter that only permits the range of IP addresses used in the Madrid office.

Berlin View based on the All Objects view with a filter that only permits the range of IP addresses used in the Berlin office.

Figure 197 View Unions

Setting the content scope of a view as the intersection of its base views results in a view that contains only the objects that are in all of the selected views. You can use view intersection to implement tagging. For example you may have three views:

- Service view showing devices involved in delivering a particular network or application service.
- Key view showing important network devices.
- New York view showing managed objects in the New York office.

You could then create an intersection view that would only include key devices in the New York office involved in delivering the specified service.

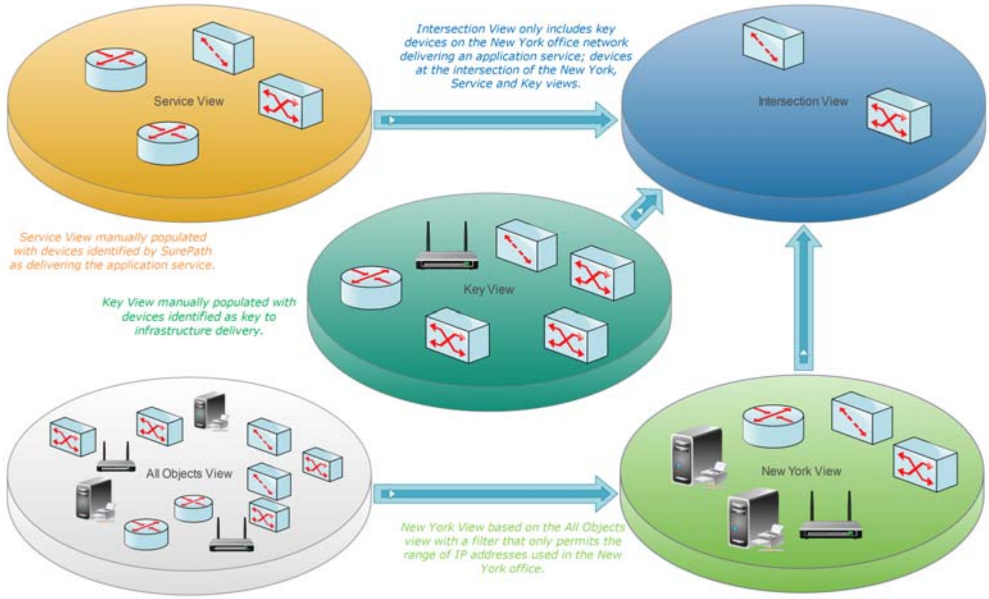

Intersection View only includes key devices on the New York office network delivering an application service; devices at the intersection of the New York, Service and Key views.
Service View
Intersection View
Service View manually populated with devices identified by SurePath as delivering the application service.
Key View
Key View manually populated with devices identified as key to infrastructure delivery.
All Objects View
New York View
New York View based on the All Objects view with a filter that only permits the range of IP addresses used in the New York office.

Figure 198 Tagging and Views

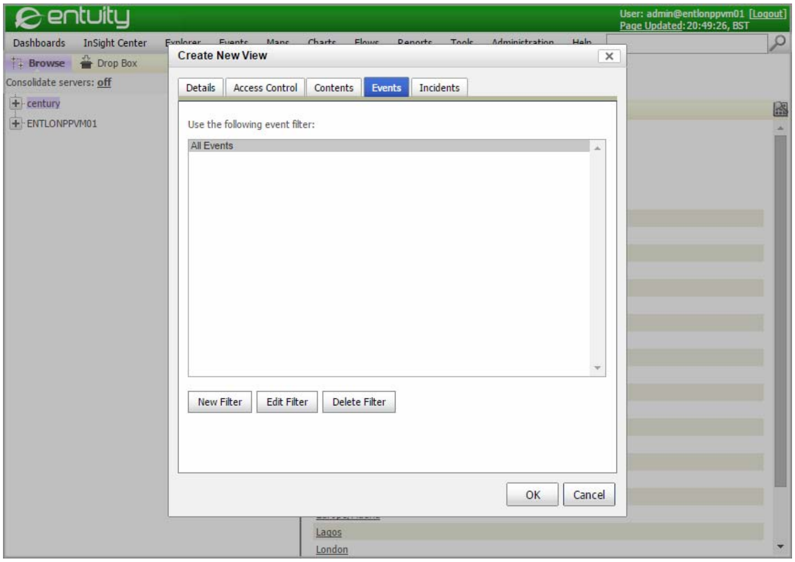
If you alter the contents of a base view or remove a view from a union or intersection definition this alters the resultant view. If you delete a base view Entuity raises a warning and lists the impacted views, Entuity does not warn you if you edit a view.

## View Event Filters

Through the Events tab you control which events Entuity can potentially raise against objects within the view. The default event filter, **All Events**, permits all events access to the view including SNMP traps and syslog events from unmanaged devices.

| Attribute | Description |
|---|---|
| *Use the following event filter* | Entuity includes one event filter, **All Events**, which potentially allows the raising of all events in the view. You can create new filters to only include the particular events that you require. |

Table 47 Set View Events



Use the following event filter:

All Events

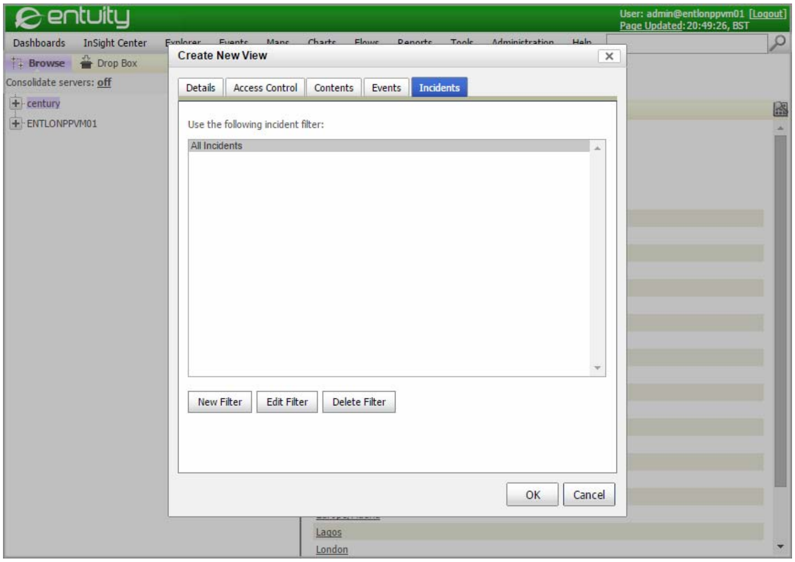
Figure 199 Set View Events

## View Incident Filters

Through the Incidents tab by selecting a filter you control which incidents Entuity can potentially raise against objects within the view. The default filter, **All Incidents**, permits all incidents access to the view. You can define new filters, or amend existing user defined filters to include to the view required incidents.

| Attribute | Description |
|---|---|
| *Use the following incident filter* | Entuity includes one incident filter, **All Incidents**, which potentially allows the raising of all incidents in the view. You can create new filters to only include the particular incidents that you require. |

Table 48 Set View Incidents



Use the following incident filter:

All Incidents

Figure 200 Set View Incidents

## Create, Amend and Delete Views

Before creating a view ensure that you are logged into Entuity as a member of the Administrators group or as a user with the Create Views, and Edit View Filters permissions.

You can create views:

- At the root of the current server.
- As a sub-view of an existing view.
- That are applied across multiple servers, both Entuity and SurePath.

  You must be logged in to all of the required servers and have set *Consolidate servers* to **on**.
- On SurePath servers for use with network paths. Network paths can only be placed within views on their SurePath server.

SurePath only uses views when accessed from a remote Entuity server. This allows you to control access to network paths in the same way you control access to other network objects, through views.

- Through the web UI, a tabbed dialog guides you through view creation.
- Through the Restful API.

## Creating Root Views

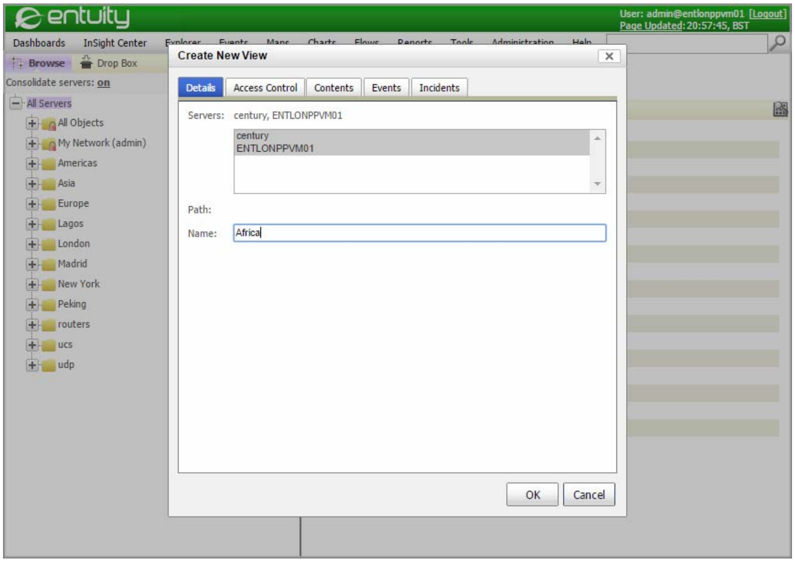
A root view sits at the top level of the view structure, a sub-view sits within a root view or another sub-view. From the Browse area of Explorer you can create a root view:

- In unconsolidated server mode by highlighting the Entuity server and from the context menu clicking **Create View**.
- In consolidated server mode by highlighting the All Servers icon and from the context menu clicking **Create View**.

To create a view:

1) From Explorer click on the All Servers icon.

2) Entuity displays the Create New View dialog through which you define the view.



Create New View

Servers: century, ENTLONPPVM01

Path:

Name: Africa

Figure 201 Create Root Views

## Creating Sub-Views

A sub-view sits within a root view or another sub-view. Before creating views you should consider who requires access to them.

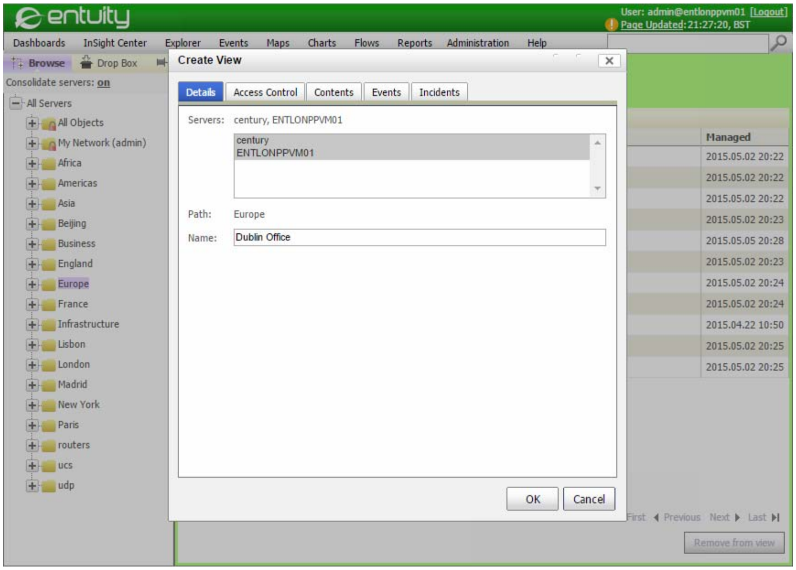
When building a hierarchy of views ensure access at each level meets your requirements, if you grant a user access to only the second or third level of a view hierarchy but not the root, that structure would be available to the user through Explorer but the content of any parent views to which they do not have access is not displayed. The user would still be able to access the views, e.g. through reports, through the server root page which lists associated views.

To create a sub-view:

1) From Explorer click on the view below which you want to create a view.

2) From the context menu click **Create View.**

3) Entuity displays the Create New View dialog through which you define the view.



Create View

Servers: century, ENTLONPPVM01

century
ENTLONPPVM01

Path: Europe

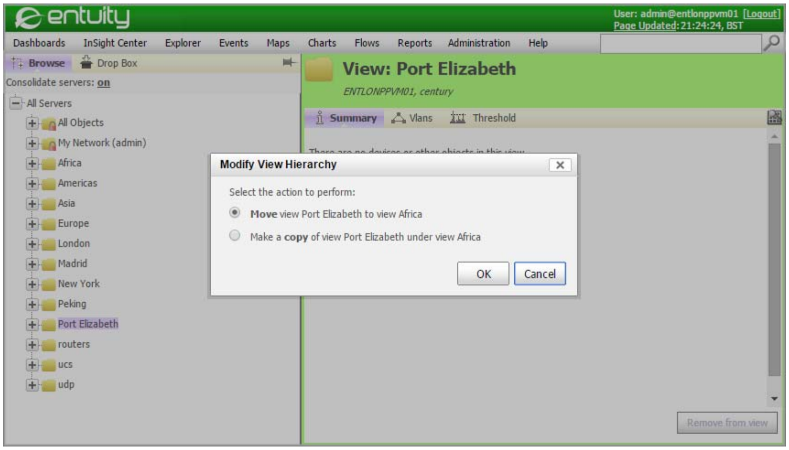
Name: Dublin Office

| Managed |
|---|
| 2015.05.02 20:22 |
| 2015.05.02 20:22 |
| 2015.05.02 20:22 |
| 2015.05.02 20:23 |
| 2015.05.05 20:28 |
| 2015.05.02 20:23 |
| 2015.05.02 20:24 |
| 2015.05.02 20:24 |
| 2015.04.22 10:50 |
| 2015.05.02 20:25 |
| 2015.05.02 20:25 |

Figure 202 Create Sub-Views

## Copying and Moving Views

You may want to re-use, or adjust your current view hierarchies.



View: Port Elizabeth

*ENTLONPPVM01, century*

Modify View Hierarchy

Select the action to perform:

● **Move** view Port Elizabeth to view Africa

○ Make a **copy** of view Port Elizabeth under view Africa

Figure 203 Modify Views

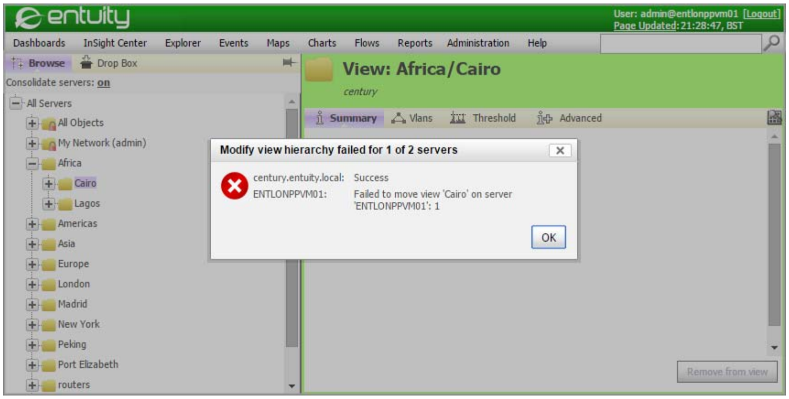
Through Explorer you can drag and drop views with the options of:

- Move, which moves the selected view, and any sub-views to the target view.

- Copy, which copies the selected view, and any sub-views to the target view.

  The original and copied views are independent of each other, changes in one do not change the other. However if the original view is based on other views, the new copy is also based on those views.

When copying and moving views in consolidated server mode Entuity checks the validity of the new view path.



Modify view hierarchy failed for 1 of 2 servers

century.entuity.local: Success
ENTLONPPVM01: Failed to move view 'Cairo' on server 'ENTLONPPVM01': 1

OK

Figure 204 Multi Server View Failure

## Creating SurePath Views

From a SurePath server you cannot view, create, edit or delete views and therefore all network paths on a SurePath server are available to all users that access that server. However you can view, create, edit and delete views on a SurePath server from its Entuity central server. When using SurePath with Entuity servers you should access SurePath only through its central Entuity server. Through views you can then control which users have access to which network paths.

It is important to recognize that a network path can only be added directly to a view that is managed by the same SurePath server as itself. You cannot for example place a network path into a view on an Entuity server. You can add a network path to a service that is in a view on another server.

When using SurePath with views you are recommended to always set to **on** the Explorer Consolidate Server setting. This combines the contents of views with the same name but managed by different servers, for example the view London on the:

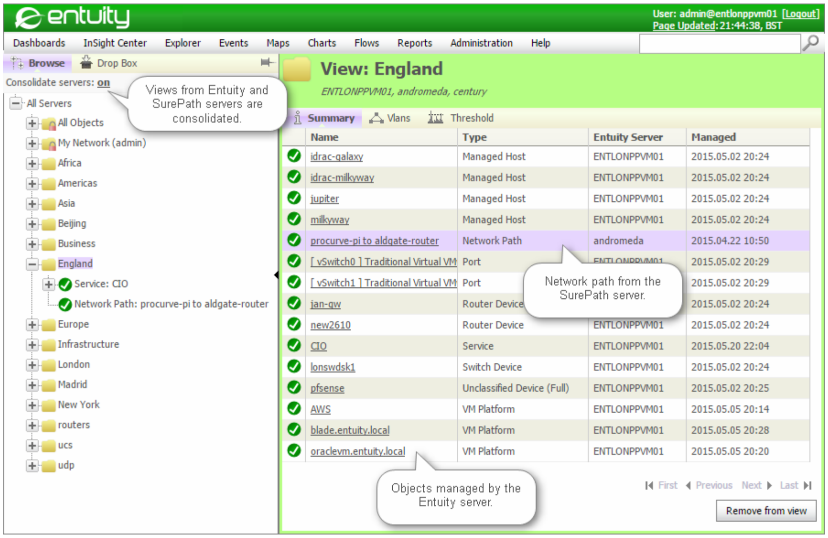
- SurePath server would contain network paths.
- Entuity server would contain at least all of the devices within the network paths defined on the SurePath server.

To create a view combining Entuity managed objects and SurePath network paths:

1) From Explorer set Consolidate Servers to **on**.

2) Create a View, for example **London**.

3) Drag devices and paths into that view. The paths are added to the SurePath view and the devices to the Entuity view.



| | Name | Type | Entuity Server | Managed |
|---|---|---|---|---|
| ✓ | idrac-galaxy | Managed Host | ENTLONPPVM01 | 2015.05.02 20:24 |
| ✓ | idrac-milkyway | Managed Host | ENTLONPPVM01 | 2015.05.02 20:24 |
| ✓ | jupiter | Managed Host | ENTLONPPVM01 | 2015.05.02 20:24 |
| ✓ | milkyway | Managed Host | ENTLONPPVM01 | 2015.05.02 20:24 |
| ✓ | procurve-pi to aldgate-router | Network Path | andromeda | 2015.04.22 10:50 |
| ✓ | [ vSwitch0 ] Traditional Virtual VM | Port | ENTLONPPVM01 | 2015.05.02 20:29 |
| ✓ | [ vSwitch1 ] Traditional Virtual VM | Port | | 2015.05.02 20:29 |
| ✓ | jan-gw | Router Device | | 2015.05.02 20:24 |
| ✓ | new2610 | Router Device | ENTLONPPVM01 | 2015.05.02 20:24 |
| ✓ | CIO | Service | ENTLONPPVM01 | 2015.05.20 22:04 |
| ✓ | lonswdsk1 | Switch Device | ENTLONPPVM01 | 2015.05.02 20:24 |
| ✓ | pfsense | Unclassified Device (Full) | ENTLONPPVM01 | 2015.05.02 20:25 |
| ✓ | AWS | VM Platform | ENTLONPPVM01 | 2015.05.05 20:14 |
| ✓ | blade.entuity.local | VM Platform | ENTLONPPVM01 | 2015.05.05 20:28 |
| ✓ | oraclevm.entuity.local | VM Platform | ENTLONPPVM01 | 2015.05.05 20:20 |

Views from Entuity and SurePath servers are consolidated.

Network path from the SurePath server.

Objects managed by the Entuity server.

Figure 205 Consolidated SurePath and Entuity Views

## Deleting Views

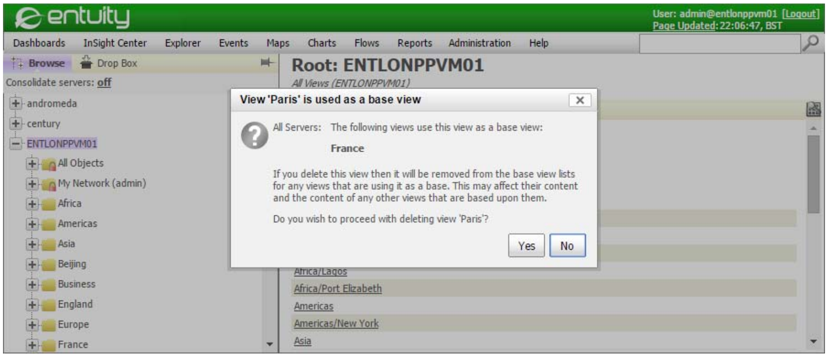
When you delete views, you are only deleting from Entuity the view, , not the managed objects within the view or services and any other configuration set-up for the view.

When using the web UI in consolidated server mode, you can delete all views with that name from all connected servers. Entuity warns you that you are deleting views and identifies the impacted servers and the impact on other views to which they act as the base view.

To delete a view:

1) From Explorer click on the view and from the context menu click **Delete View**.

2) Click **Yes** to confirm view deletion.



View 'Paris' is used as a base view

All Servers: The following views use this view as a base view:

France

If you delete this view then it will be removed from the base view lists for any views that are using it as a base. This may affect their content and the content of any other views that are based upon them.

Do you wish to proceed with deleting view 'Paris'?

Figure 206 Delete Base Views

# Managed View Content

You can populate views by basing them on existing views (see *Chapter 33 - Manage View Filters*) or by manually populating them by through dragging and dropping objects to them.

## Dragging Content into Views

You can drag and drop content between any views to which you have access:

- Administrators may copy from the All Objects view as it contains all managed objects on the server.
- All users can use their My Network view as it contains all of the objects to which they have access.

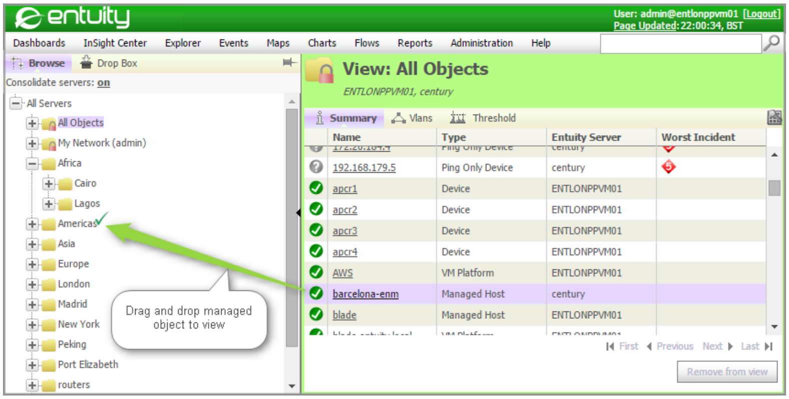
To drag objects into a view:

1) From Explorer click on All Objects. Entuity displays the details of devices in the view through the Summary tab.

2) Click on and drag the device to the target view. By holding down the Shift or Control keys you can select multiple objects.

   As you drag the device the mouse pointer either includes a red cross or green tick to indicate the validity of the destination.

3) Drop the objects when the mouse pointer includes a green tick.



Consolidate servers: on

View: All Objects

ENTLONPPVM01, century

| Name | Type | Entity Server | Worst Incident |
|---|---|---|---|
| 172.20.184.4 | Ping Only Device | century | |
| 192.168.179.5 | Ping Only Device | century | 5 |
| apcr1 | Device | ENTLONPPVM01 | |
| apcr2 | Device | ENTLONPPVM01 | |
| apcr3 | Device | ENTLONPPVM01 | |
| apcr4 | Device | ENTLONPPVM01 | |
| AWS | VM Platform | ENTLONPPVM01 | |
| barcelona-enm | Managed Host | century | |
| blade | Managed Host | ENTLONPPVM01 | |

Figure 207 Drag Objects into Views

## Delete Objects from Views

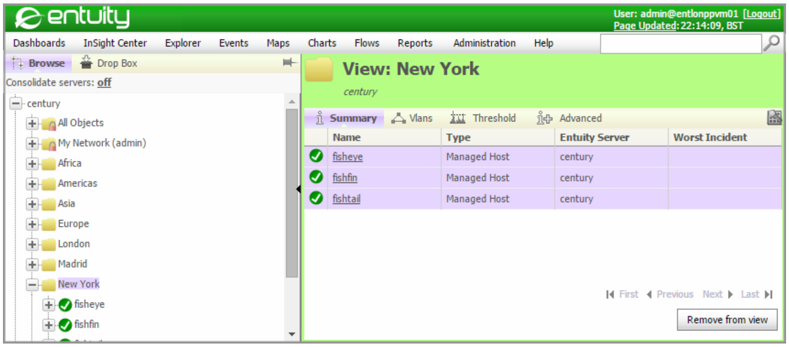
When you have dragged objects into a view, as opposed to basing content on other views, you can then remove them through Explorer using Remove from view.

To remove objects from a view:

1) From Explorer click on the required view. Entuity displays the details of managed objects in the view through the Summary tab.

2) Click on the objects to remove from the view. By holding down the Shift or Control keys you can select multiple objects.

3) Click **Remove from view**.



Consolidate servers: off

View: New York

century

| Name | Type | Entity Server | Worst Incident |
|---|---|---|---|
| fisheye | Managed Host | century | |
| fishfin | Managed Host | century | |
| fishtail | Managed Host | century | |

Figure 208 Remove Objects from a View

## Business Units and Geographic Example

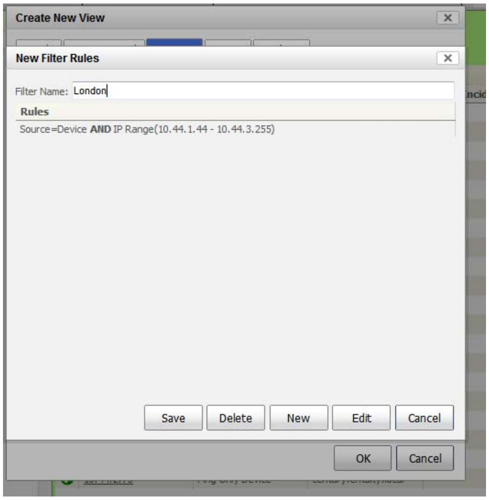
Consider how to implement access to a network that is geographically dispersed and with business units similarly dispersed. You may want some users to access:

- Only the devices in their geographic location but across all business units.
- All devices associated with a business unit across all geographic locations.

To implement a view configuration:

- Create a view for each office location and base each on the All Objects view.

  Where these offices have their own range of IP addresses you can define a content filter using IP Address Range; as new devices are added to or old ones removed from an office the content of the view automatically updates.



Filter Name: London

Rules

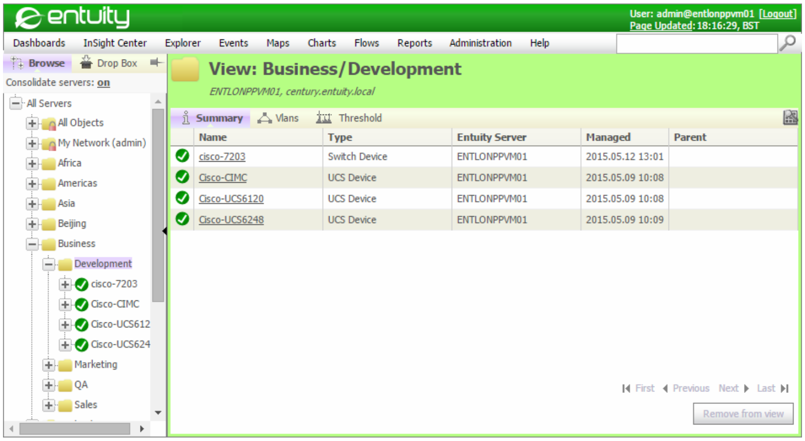
Source=Device **AND** IP Range(10.44.1.44 - 10.44.3.255)

Figure 209 IP Range Defined Filter Rules

- Assign access to this view to user groups managing those offices.
- Create a view for each business unit.

  You should drag into each business unit view all devices for that business unit, regardless of their geographic location.

  Assign access to each business unit view to user groups managing those business units.



View: Business/Development

*ENTLONPPVM01, century.entuity.local*

| | Name | Type | Entity Server | Managed | Parent |
|---|---|---|---|---|---|
| ✓ | cisco-7203 | Switch Device | ENTLONPPVM01 | 2015.05.12 13:01 | |
| ✓ | Cisco-CIMC | UCS Device | ENTLONPPVM01 | 2015.05.09 10:08 | |
| ✓ | Cisco-UCS6120 | UCS Device | ENTLONPPVM01 | 2015.05.09 10:08 | |
| ✓ | Cisco-UCS6248 | UCS Device | ENTLONPPVM01 | 2015.05.09 10:09 | |

Figure 210 Business Unit Views

# 33 Manage View Filters

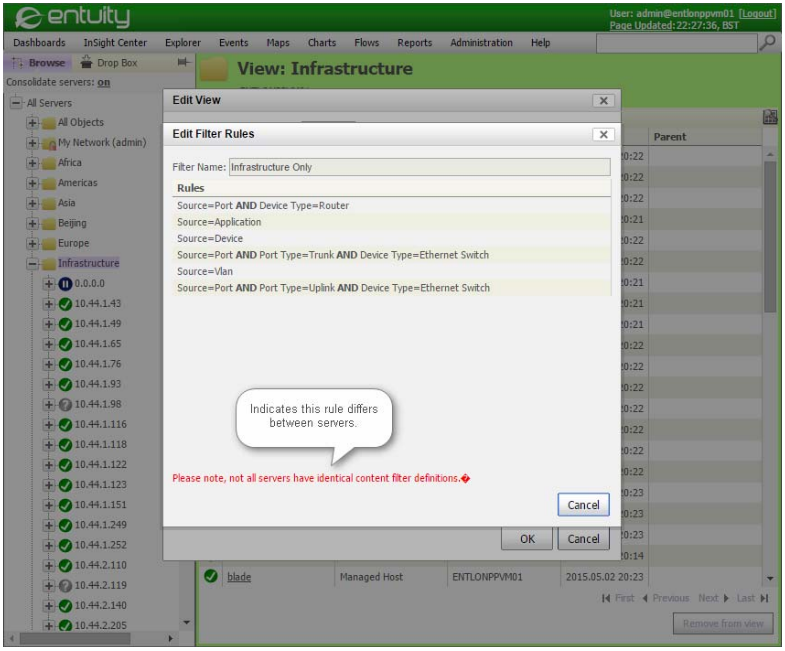
A view’s content scope determines the managed objects a view can contain. Filters applied to the view determine what managed objects within that scope are actually displayed. There are three types of filters associated with views:

- Content filters when applied determine the components that are displayed for a view. (See *Amending Content Filters*.)

  You can create views without content filters by dragging objects into an empty view.
- Event filters determine the events that are displayed for a view in Event Viewer. (See *Incident and Event Filters*.)
- Incident filters determine the incidents that are displayed for a view in Event Viewer. (See *Incident and Event Filters*.)

You can create filters that restrict the view to show only the particular components of the network you are interested in, e.g. VLANs. You can also use the same filter against a number of views.

Entuity is supplied with default filters, of which the All Objects filter is applied to the predefined All Objects view and users’ My Network views. You cannot change these default filters.



Filter Name: Infrastructure Only

| Rules |
|---|
| Source=Port **AND** Device Type=Router |
| Source=Application |
| Source=Device |
| Source=Port **AND** Port Type=Trunk **AND** Device Type=Ethernet Switch |
| Source=Vlan |
| Source=Port **AND** Port Type=Uplink **AND** Device Type=Ethernet Switch |

Indicates this rule differs between servers.

Please note, not all servers have identical content filter definitions.

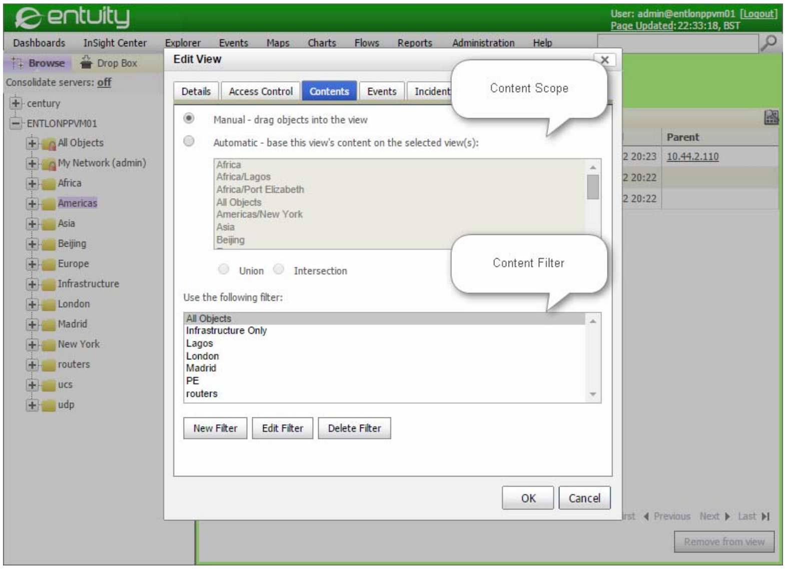
Figure 211 Content Filter Rules

# What are Content Filters?

You control how managed objects are included to a view by setting through the Edit View dialog’s Contents tab the:

- Content scope of the view, what a view can potentially display. You can set it to:
  - Manual, and then drag content into the view.
  - Automatic, which allows you to use other views to determine view content.
- Content filter which controls which objects within the content scope of the view are available through the view. You can set it to:
  - All Objects, which includes all objects within the content scope to the view.
  - Infrastructure Only, which includes only the infrastructure ports within the content scope to the view.
  - A user defined rules based content filter.

Content filters apply to the content in the view directly added to the view, either through base views or manually dragged into the view. They do not apply to managed objects inherited from sub-views or through services.



● Manual - drag objects into the view

○ Automatic - base this view's content on the selected view(s):

Africa
Africa/Lagos
Africa/Port Elizabeth
All Objects
Americas/New York
Asia
Beijing

○ Union ○ Intersection

Use the following filter:

All Objects
Infrastructure Only
Lagos
London
Madrid
PE
routers

Figure 212 Content Filter Rules

A content filter only allows through into its associated view(s) those components and types of components that are specified in its rules. They must be stated in the terms within those rules.

To identify the content filter associated with a view:

1) Highlight the view and from the context menu click **Edit View**.

2) Click the Contents tab.

## Views and Filters Best Practice

You can apply a filter to a manually populated view to further restrict the content. For example after dragging switches and routers into a view then applying a filter so that the view only shows switches. However Entuity Support recommend that you do not apply filters to manually populated views as when the filter is applied you cannot then view what you manually dragged into the view. Instead create two views, the:

- First a manual view to which you drag and drop your required devices.
- Second a view based on the first view but with a filter that only includes the required devices.

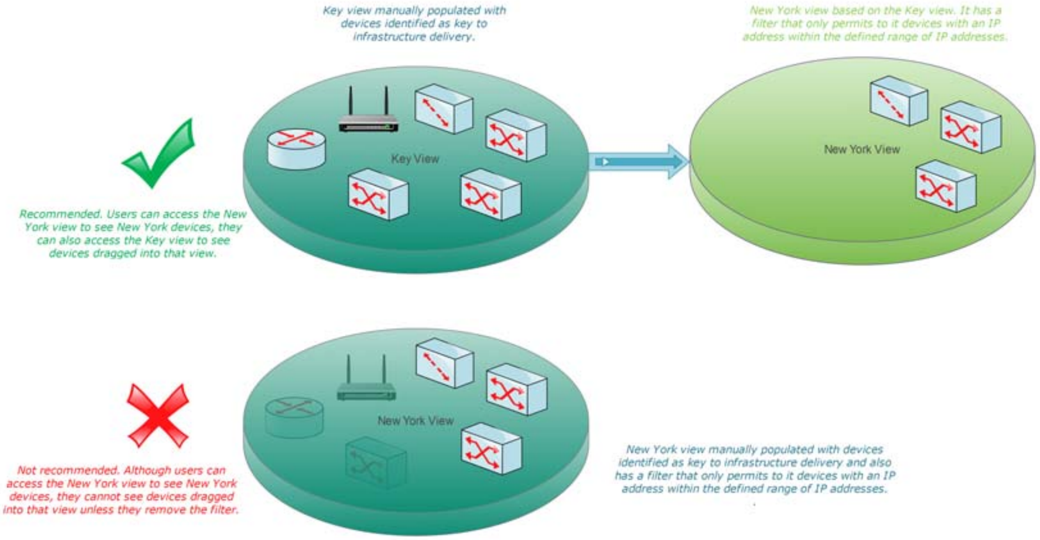

Key view manually populated with devices identified as key to infrastructure delivery.
New York view based on the Key view. It has a filter that only permits to it devices with an IP address within the defined range of IP addresses.
Key View
New York View
Recommended. Users can access the New York view to see New York devices, they can also access the Key view to see devices dragged into that view.
New York View
Not recommended. Although users can access the New York view to see New York devices, they cannot see devices dragged into that view unless they remove the filter.
New York view manually populated with devices identified as key to infrastructure delivery and also has a filter that only permits to it devices with an IP address within the defined range of IP addresses.

Figure 213 Set View Content

## All Objects and Infrastructure Only Filters

Entuity includes two predefined content filters, All Objects and Infrastructure Only. When you first create a view the default filter is All Objects. This is the filter used by My Network and All Objects views. All Objects has only one rule which allows through all objects:

```
All
```

The Infrastructure Only filter displays only those ports that are ‘uplinks’ (i.e. ports connecting routers with switches), trunk ports (i.e. ports connecting switches together), or router ports.

The Infrastructure Only filter contains six rules:

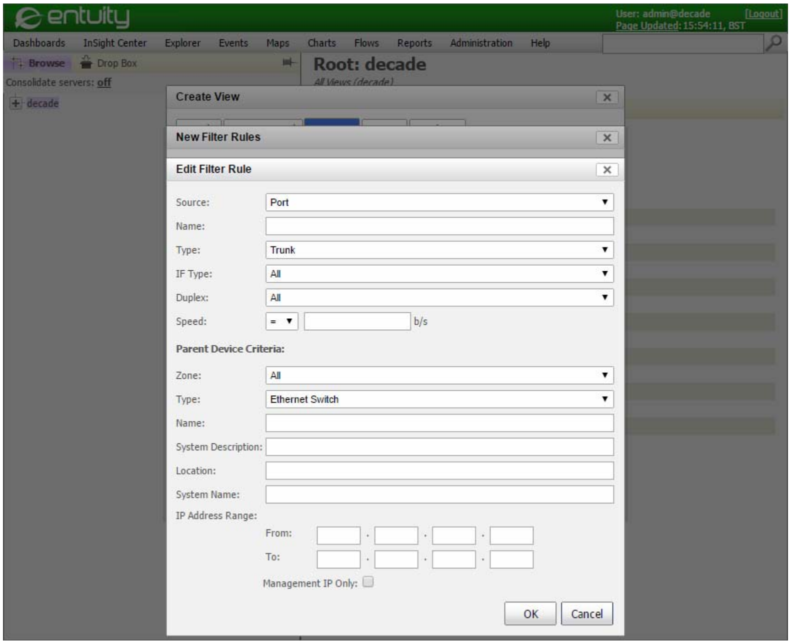
```
Source=Device AND Zone=all

Source=Port AND Port Type=Trunk AND Device Type=Ethernet Switch AND
Zone=all
```

```
Source=Port AND Port Type=Uplink AND Device Type=Ethernet Switch AND
Zone=all
```

```
Source=Application AND Zone=all
```

```
Source=Port AND Device Type=Router AND Zone=all
```

```
Source=Vlan
```



Consolidate servers: off

Source: Port

Name:

Type: Trunk

IF Type: All

Duplex: All

Speed: = b/s

Parent Device Criteria:

Zone: All

Type: Ethernet Switch

Name:

System Description:

Location:

System Name:

IP Address Range:

From: . . .

To: . . .

Management IP Only: □

Figure 214 Trunk Port Filter

All of the statements in a filter, filter required components **into** a view rather than filter them out. This means that you need to add as many rules as are needed to display the components you want to see. Each rule within a filter is combined using a logical OR.

The filter rules use the same component hierarchy as viewed through Explorer, for example a rule that filters in a port must also filter in the parent device.

Devices, applications and VLANs are filtered into the view through the first, second and fifth rules respectively. The port filters are then applied against the returned devices, applications and VLANs. Only ports which match the criteria specified in rules three, four and six are included, i.e. trunk ports, uplinks and router ports.

## Building Content Filter Rules

A filter is built from one or more rules. For example, to create a filter that only shows devices this rule is sufficient:

```
Source=Device
```

When you want to also view ports within the returned devices the filter must be amended to:

```
Source=Device
Source=Port
```

Entuity can build the rules using the source types to reflect the hierarchy of Entuity objects; views are directly linked to devices, devices to ports. This is viewable through the Explorer tree pane, i.e. devices are displayed within the view and ports are displayed against their associated device.

When a filter does not conform to this hierarchy then the returned results may not be what you expect. For example for this rule:

```
Source=Port AND Device Type=Ethernet Switch
```

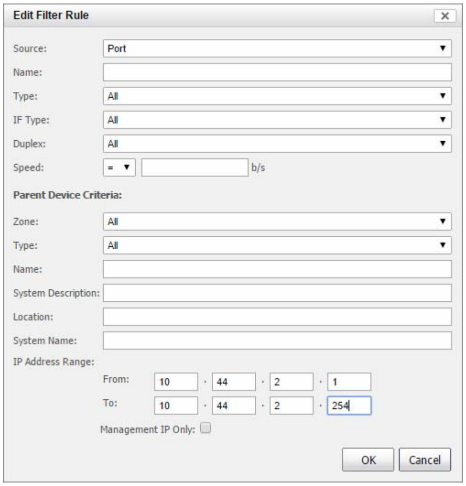
In Explorer, Entuity displays the ports of ethernet switches in the view summary page but cannot display them in the Explorer tree as you must specify the device to conform to the object hierarchy.

This filter does not include ports to the Explorer tree as in the object hierarchy there is no link between the view and the source type, port. You can check this by looking at the Component Tree pane and noticing between views and ports there are devices. Adding to the filter a rule that defines a device source type, in this example an ethernet switch, allows ports to be displayed in the view. This rule returns all of the ethernet ports:

```
Source=Device AND Device Type=Ethernet Switch
Source=Port AND Device Type=Ethernet Switch
```

To amend a content filter you can add, amend or delete these rules. The particular format of the rule varies according to the rule’s source type, i.e. VLAN, port, module or device.

To make the building of rules easier the Entuity interface only presents those options valid for the selected source type.



Edit Filter Rule

| | |
|---|---|
| Source: | Port |
| Name: | |
| Type: | All |
| IF Type: | All |
| Duplex: | All |
| Speed: | = b/s |

Parent Device Criteria:

| | |
|---|---|
| Zone: | All |
| Type: | All |
| Name: | |
| System Description: | |
| Location: | |
| System Name: | |

IP Address Range:

From: 10 . 44 . 2 . 1

To: 10 . 44 . 2 . 254

Management IP Only: □

Figure 215 Adding a Port Filter

## Application Rule Options

| Application | Description |
|---|---|
| *Application* | Select from the application to include to the view. |
| *Parent Device Criteria* | Through this section you can filter the application in the context of its device. (See *Table 50 Device Filter Rules*.) |

Table 49 Application Filter Rules

## Device Rule Options

| Device | Description |
|---|---|
| *Type* | Select:<br>■ **All** to include all types of device.<br>■ A particular device type to include only the specified device type, for example **Ethernet Switch**, **ATM Switch**, **Load Balancer**, **Router**. |
| *Zone* | Only displays when using zones. Select All to apply to all zones or select a specific zone. |
| *Name* | Enter the name of the device or leave blank (equivalent to all).<br>Device name supports filtering using regular expressions (Regex). |
| *System Description* | Manufacturer's device description.<br>The default is blank (equivalent to all). Description supports filtering using regular expressions (Regex). |
| *Location* | Text description of the physical location of the device that is contained on the device, e.g. Development Cabinet.<br>The default is blank (equivalent to all). Location supports filtering using regular expressions (Regex). |
| *System Name* | Administratively-assigned name for the chassis. By convention, this is the node's fully-qualified domain name. |
| *IP Address Range* | IP Range filter returns any managed device with ports that have an IP address in the specified range. It also returns routers with any port that has an interface with an IP address within the defined range. |
| *Management IP Only* | Select to filter devices by IP Range, where only the management IP address is considered.<br>The default is to filter by IP Range considering all device IP addresses. |

Table 50 Device Filter Rules

## Port Rule Options

| Port | Description |
|---|---|
| *Name* | Enter the name of the port or leave blank (equivalent to all).<br>Port name supports filtering using regular expressions (Regex). |

Table 51 Port Filter Rules

| Port | Description |
|---|---|
| *Type* | Select:<br>- **All** to include all types of port.<br>- To include only the specified port type, i.e. **Router**, **Server link**, **Trunk**, **Uplink** or **Other** (only includes ports that do not have a specified port type). |
| *IF Type* | Is the port interface type. Select:<br>- **All** to include all types of interface.<br>- To include only the specified port interface type, e.g. **ATM Logical**, **Gigabit Ethernet**, **PPP**, **SLDC**. |
| *Duplex* | Is the port’s duplex type. Select:<br>- **All** to include all Duplex types.<br>- **Unknown** to include no specific types.<br>- **Half** to include only Half Duplex ports.<br>- **Full** to include only Full Duplex ports.<br>- **Auto** to include only Auto Duplex ports. |
| *Speed* | Is the port’s interface speed. Enter:<br>- ***** to include ports of all speeds.<br>- <= to include only ports with interface speeds less than or equal to a specified number of bits, Kilobits or Megabits (i.e. 1,000,000 bits) per second.<br>- = to include ports with interface speeds equal to a specified number of bits, Kilobits or Megabits per second.<br>- >= to include ports with interface speeds greater than or equal to a specified number of bits, Kilobits or Megabits per second. |
| *Parent Device Criteria* | Through this section you can filter the port in the context of its device. (See *Table 50 Device Filter Rules*.) |

Table 51 Port Filter Rules

✓ To exclude ports of a particular type, e.g. trunk ports create rules that include all of the other port types; create a rule to include routers, a rule to include uplinks, a rule to include server links and a final rule to include all other non-specified port types, other.

## Service Rule

For most views you should not have to include a service rule filter. If you add a Service Filter rule to:

- An automatically populated view then all services on that Entuity server are visible in the view and therefore all components in those services are visible within that view.

  If you do not include a service rule to a view then only those services explicitly defined in the view are visible.

- A manually populated view then the service rule has no visible effect, either way only those services explicitly defined in the view are visible.

| Source | Description |
|---|---|
| *Service* | Permits into the view all services defined on that server.<br>When not specified Entuity restricts the services in a view to those explicitly added to that view. |

Table 52 VLAN Filter Rules

### VLAN Rule

| Source | Description |
|---|---|
| *VLAN* | Permits into the view events and objects related to VLANs. |

Table 53 VLAN Filter Rules

## Regular Expressions

Attributes which Entuity allows you to free type in the value also allow entry of regular expressions (Regex). When defining filter rules with regular expression consider pattern matching is case-sensitive.

| Character | Description | Character | Description |
|---|---|---|---|
| \ | Backslash | ^ | Caret |
| **$** | Dollar sign | **.** | Period (full stop or dot) |
| **\|** | Vertical bar (pipe symbol) | **?** | Question mark |
| ***** | Asterisk (star) | **+** | Plus sign |
| **(** | Opening parenthesis | **)** | Closing parenthesis |
| **[** | Opening square bracket | **{** | Opening curly brace |

Table 54 Regular Expression Special Characters

These examples show the regular expressions applied against device name to deliver the requested devices. Devices with:

- A name that includes **lon**:

  ```
  lon
  ```

- A name that start with **lon**:

  ```
  ^lon
  ```

- A name that starts with either **lon** or **par**:

  ```
  ^((lon)|(par))
  ```

- A name that ends in **1**:

  ```
  1$
  ```

- A name that ends in **a**, **b** or **c**:

```
[abc]$
```

- A name that contains at least one digit:
  ```
  [0-9]
  ```
- A name that include **s**, **t**, **u** or **v**:
  ```
  [!s-v]
  ```
- A name that include a pair of digits next to each other:
  ```
  [0-9]{2}
  ```
- A name that has **x** as the fourth character:
  ```
  ^…x
  ```
- 1 or more special characters (metacharacters) in their name require that the character is escaped. For example a name with a plus sign is escaped using the backslash:
  ```
  eol\+us
  ```

This example filter excludes all devices that include **bvt** in their name:

```
^((?!bvt).)*$
```

### Content Filters and Hierarchy of Views

When you build a view hierarchy the root view inherits the managed objects within its sub-views, and any objects those views may contain or may have inherited from their sub-views, and so on.

Inherited devices and ports are not displayed in the Explorer tree, they are displayed through the view summary pane. Similarly content filters applied against a view are not applied to inherited objects in the view summary pane.

## Amending Content Filters

There are two ways of amending a view’s content filter. You can create a new filter or edit the existing one’s rules to meet your requirements. This section includes instructions on:

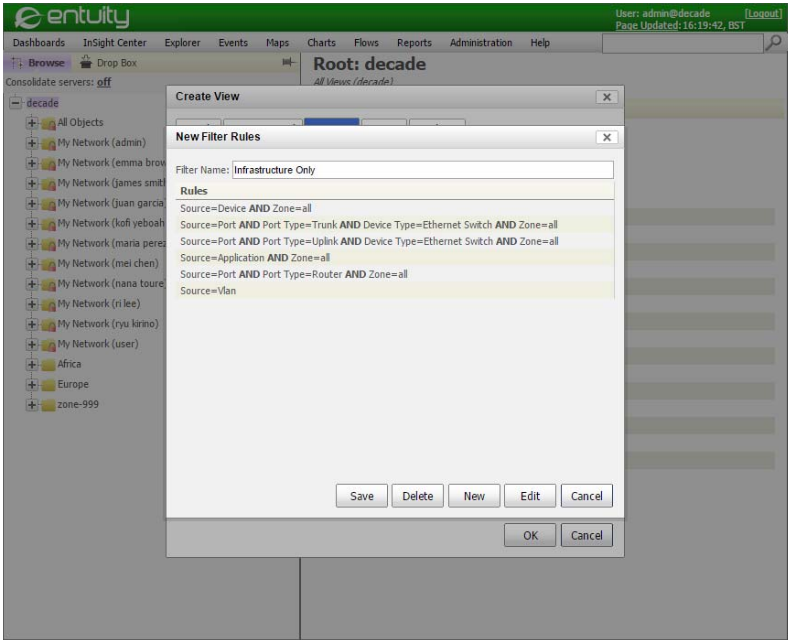
- Viewing Content Filter Rules
- Changing View Content Filters
- Adding Rules to Content Filters
- Manage IP Address Range Rules
- Editing a Content Filter Rule
- Deleting Content Filter Rules.

### Viewing Content Filter Rules

To view a content filter’s rules:

1) From Explorer highlight the view and from the context menu click **Edit View**.
2) From the Contents tab highlight the filter and click **Edit Filter**.

   Entuity prevents you from editing system only filters.



Filter Name: Infrastructure Only

Rules

Source=Device **AND** Zone=all
Source=Port **AND** Port Type=Trunk **AND** Device Type=Ethernet Switch **AND** Zone=all
Source=Port **AND** Port Type=Uplink **AND** Device Type=Ethernet Switch **AND** Zone=all
Source=Application **AND** Zone=all
Source=Port **AND** Port Type=Router **AND** Zone=all
Source=Vlan

Figure 216 Filter Rules

## Changing View Content Filters

The Edit View dialog has the same filter management functionality as the New View dialog, you can add, amend and delete filters. In addition, as you open it from a particular view, you can change which filter is associated with that view.

To amend a content filter's rules:

1) From Explorer highlight the view and from the context menu click **Edit View**.
2) From the Contents tab highlight the filter and click **Edit Filter**.

   Entuity prevents you from editing system only filters.
3) Select the required filter and amend it.
4) Click **OK**.

## Adding Rules to Content Filters

A filter is built from a series of rules. You can add new rules to a filter, the particular format of the rule varies according to the rule's source type, i.e. application, device, port, and VLAN.

To add a new term:

1) From Explorer highlight the view and from the context menu click **Edit View**.
2) From the Contents tab highlight the filter and click **Edit Filter**.
3) Click **New**. Entuity displays the Edit Filter Rule dialog.
4) Select the *Source*, i.e. **Application**, **Device**, **Port** or **VLAN**.
5) Define the new filter rule. (See *Building Content Filter Rules*.)
6) Click **OK** to create the rule. Entuity displays the new rule in the Filter Rules dialog.
7) Repeat from Step 3) until you have added all of the required rules.
8) Click **Save** to save the rule and exit the Filter Rules dialog.

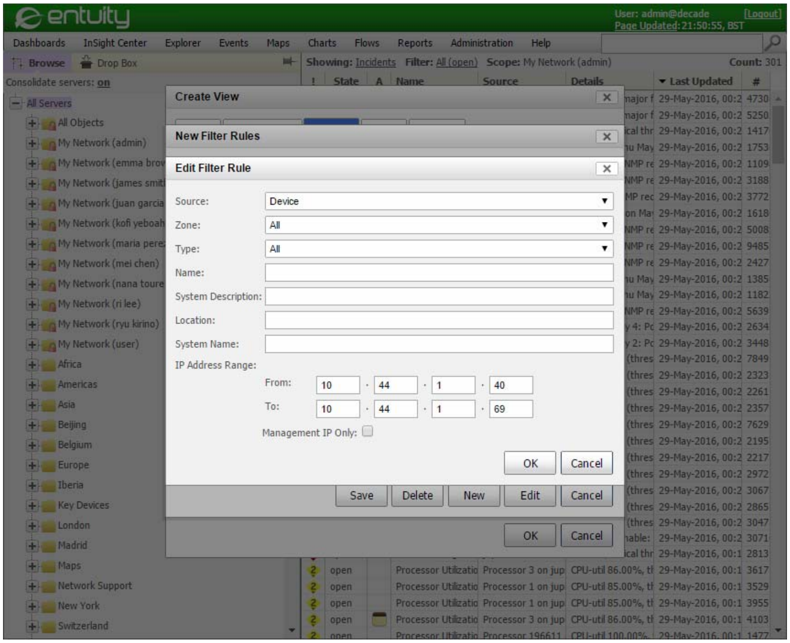
## Manage IP Address Range Rules

You can apply one or more IP address ranges against a content filter.

To manage IP ranges:

1) From Explorer highlight the view and from the context menu click **Edit View**.
2) From the Contents tab highlight the filter and click **Edit Filter**.

   Entuity displays but prevents you from editing system only filters.
3) Highlight the required filter rule and click:
   - **Edit** to amend the IP address range.
   - **Delete** for Entuity to remove filter rule.



Source: Device

Zone: All

Type: All

Name:

System Description:

Location:

System Name:

IP Address Range:

From: 10 . 44 . 1 . 40

To: 10 . 44 . 1 . 69

Management IP Only: □

Figure 217 IP Address Range Filter

4) Click **Save** to update the content filter.

## Editing a Content Filter Rule

To amend the rules of content filters:

1) From Explorer highlight the view and from the context menu click **Edit View**.

2) From the Contents tab highlight the filter and click **Edit Filter**.

3) Highlight the rule to amend and click **Edit**. Amend the terms. (See *Building Content Filter Rules*.)

4) Click **OK** and then **Save** to apply the edits to the rule and exit the Filter Rules dialog.

## Deleting Content Filter Rules

When deleting the filter’s last rule, Entuity replaces it with the default filter All.

To delete rules from content filters:

1) From Explorer highlight the view and from the context menu click **Edit View**.

2) From the Contents tab highlight the filter and click **Edit Filter**.

3) Highlight the rule to delete and select **Delete**. Entuity removes the rule.

4) Click **Save** to apply the deletion of the rule and exit the Filter Rules dialog.

✓ You can delete all rules from a filter. A view with an empty filter associated to it would not show any managed objects.

# Incident and Event Filters

The views a user has access to should always be configured to only present the information that they require. In the same way that a view should only contain the devices a user requires, the view should only present the events and incidents the user requires. Correctly configured event and incident filters prevent a user's UI from being flooded with information on network events in which they are not interested. User's with appropriately configured views will be more efficient, and the performance of their web client may also benefit.

An event filter only allows through into its associated view(s) the events of the type detailed in the event filter, i.e. you must include events to view them and exclude events to prevent them displaying.

**All Events** is the default event filter and allows through to the view all Entuity event types. You can define new event filters with appropriate descriptive names, the required set of events and support for events from devices not under management.

| Attribute | Description |
|---|---|
| *Filter Name* | Descriptive name of the event filter. |
| *Include events check box* | The **Include events from devices that are not under management** check box when selected allows Entuity to handle SNMP traps and syslog events generated from devices that are not managed by Entuity. |
| *Included Events* | Event types permitted by the rule. |
| *Excluded Events* | Event types excluded by the rule. |

Table 55 Event Filter

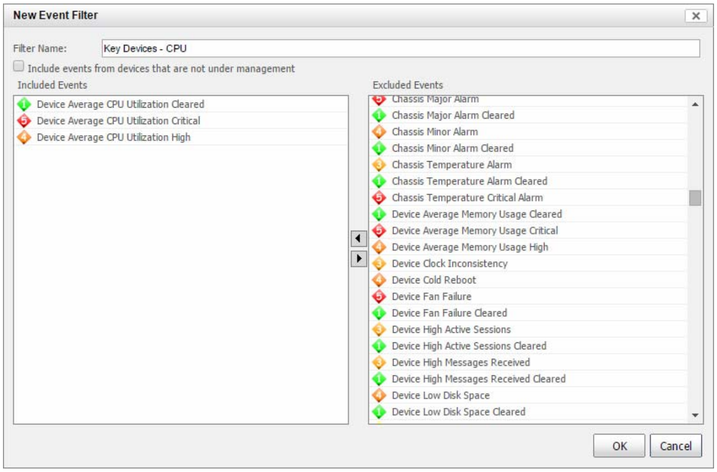
You can view and manage all of the event filters that are currently available through the Events tab and the Edit Event Filter dialog.

## Creating Event Filters

To create an event filter:

1) From Explorer highlight a view and click **Edit View**.
2) Click the Events tab. The highlighted event filter is the one currently applied to the view.
3) Click **New**.
4) Enter a descriptive event filter name and set-up its events.

   You can highlight events in one column using the shift and control keys to select multiple events. You can then use the directional arrows to move the selected events to the other column. Alternatively double-clicking on an event in one column immediately moves it to the other column.



New Event Filter

Filter Name: Key Devices - CPU

□ Include events from devices that are not under management

Included Events

- Device Average CPU Utilization Cleared
- Device Average CPU Utilization Critical
- Device Average CPU Utilization High

Excluded Events

- Chassis Major Alarm
- Chassis Major Alarm Cleared
- Chassis Minor Alarm
- Chassis Minor Alarm Cleared
- Chassis Temperature Alarm
- Chassis Temperature Alarm Cleared
- Chassis Temperature Critical Alarm
- Device Average Memory Usage Cleared
- Device Average Memory Usage Critical
- Device Average Memory Usage High
- Device Clock Inconsistency
- Device Cold Reboot
- Device Fan Failure
- Device Fan Failure Cleared
- Device High Active Sessions
- Device High Active Sessions Cleared
- Device High Messages Received
- Device High Messages Received Cleared
- Device Low Disk Space
- Device Low Disk Space Cleared

Figure 218 Create Event Filters

5) Click **OK**.

6) When you want to use the new filter for the current view, highlight the filter and click **OK**.

## Amending Event Filters

To amend a view’s event filter:

1) From Explorer highlight the view and from the context menu click **Edit View**.

2) Select the Events tab. The highlighted event filter is the one currently applied to the view.

3) Click **Edit** to view that event filter’s configuration.

   You can highlight events in one column using the shift and control keys to select multiple events. You can then use the directional arrows to move the selected events to the other column. Alternatively double-clicking on an event in one column immediately moves it to the other column.

4) Click **OK**.

## Associating Event Filters to Views

To change which event filter is associated to a view:

1) From Explorer highlight the view and from the context menu select **Edit View**.

2) Click the Events tab. The highlighted event filter is the one currently applied to the view.

3) Highlight the event filter you want to associate with the view.

4) Click **OK**.

# Zones and View Content Filter Rules

If Entuity is not managing sites with overlapping IP addresses you do not have to consider zones. When you have configured zones Entuity segregates data storage, data processing and network communication by zone. You should also configure view filters to handle zones.

To set a view's content filter:

1) From Explorer highlight the view and from the context menu click **Edit View**.

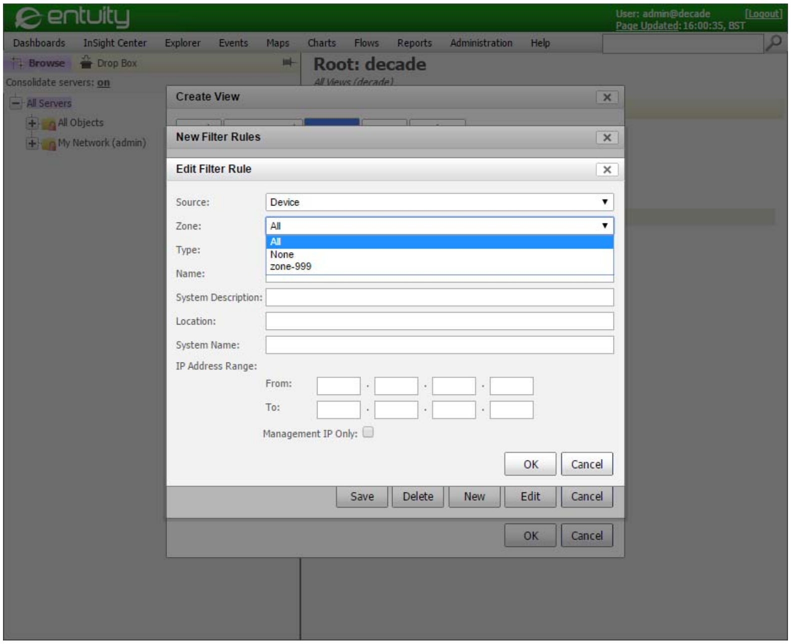
2) Select the Contents tab.

3) Highlight an existing filter and click **Edit Filter**.

4) Set the rule. (See *Figure 219 Set Zone for Content Filter Rule*.)

5) Click **Edit** to view that event filter's configuration.

6) Select a rule and click **Edit**. Assign a zone to the rule.



Source: Device

Zone: All

Type:

Name:

System Description:

Location:

System Name:

IP Address Range:

From: . . .

To: . . .

Management IP Only: □

Figure 219 Set Zone for Content Filter Rule

7) Click **OK**.

# 34 Control User Access to Views

Entuity has the following levels of view access and ownership:

- Members of the Administrator user group:
  - Have full access rights to all views.
  - Can assign ownership of a view to a new owner. By default the owner is the user who created the view.
  - Can hide the display of Private views. A Private view is one to which an administrator only has access because as an administrator they have access to all views, and not because they are the member of another user group which has access to that view.
- Owner access allows to the owner of a view:
  - Read and edit access to the view.
  - Control of access by other user groups to the view, and their permission level, i.e. read only or edit access rights.
- User group access allows members of associated user groups access to the view, with read only or read/write access rights.

Administrators can also assign to user groups additional view permissions. Through Tool Permissions you assign advanced users greater control over views:

- Create Views, allows users to create views.
- Edit View Filters, allows users to create, edit and delete filters associated with views, events and incidents.
- Share Views, allows users to share view with other user groups and control the level of permissions they have to that view.

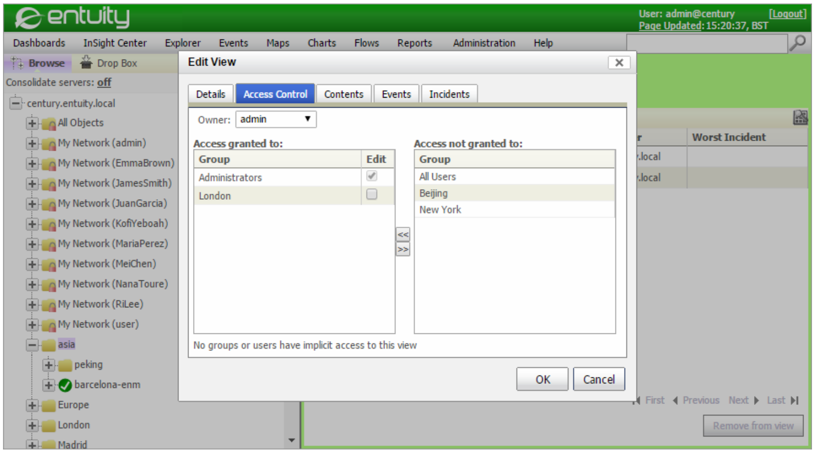
A user may also gain access to a view when that view is part of a view hierarchy. If a user has permission to access a parent view then they also have an implicit permission to access the parent's child views. Conversely a user who has permission to access a child view but not the parent can, for example through the Explorer tree, see the view but will not have access to its contents.

## Displaying View Access Controls

You can see which user and user groups are associated with a view:

1) Highlight the required view in Explorer and click **Edit View**.
2) Select the Access Control tab.

   Entuity displays the view's current access control details. The functions available, for example whether you can change or delete owners and grant access to user groups, depend upon your account permissions.



Edit View

Owner: admin

Access granted to:

| Group | Edit |
|---|---|
| Administrators | ☑ |
| London | □ |

Access not granted to:

| Group |
|---|
| All Users |
| Beijing |
| New York |

No groups or users have implicit access to this view

Figure 220 User Group Access Control

# Manage View Ownership

Assigning view ownership is useful when wanting to assign a degree of administrator privilege to a user but only for a view or a restricted set of views. Administrators can add, change or delete a view's owner. By default the owner of a view is the user that created it, however a view owner is not required.

## Changing View Ownership

By default the owner of a view is the user that created it. Administrators can change the view owner to any other user, even users that do not, through their user group, have permission to access that view. As owners of the view they inherit full owner view access rights, although to see objects within that view users must have access permissions to them.

To change the ownership of a view:

1) Highlight the required view in Explorer and click **Edit View**.

2) Click the Access Control tab.

3) From *Owner* select the user to own the view.

4) Click **OK**. Entuity closes the dialog and updates the view's owner.

If the user profile of a view owner is removed from Entuity then when you access the Edit dialog Owner is blank. You must reassign ownership before you can maker any other amendments otherwise you are warned the view owner is set to <**Invalid User**>.

# Associating Views to User Groups

By default members of the:

- All Users and Administrators user groups have access to their own My Network view.
- Administrators user group also have access to the All Objects view.

When a view is created only members of the Administrators group and the user who created the view have access to it. However you can associate user defined views with one or more user groups:

- Administrators can assign any user group to any view (excluding the private My Network views).
- Users that are a view owner, or are a member of a user group that has assign control access to a view, can assign group access to that particular view.

To associate a view to a user group:

1) Highlight the required view in Explorer and click **Edit View**.
2) Select the Access Control tab.
3) For each user group in the:
   - **Access not granted to** panel that is to have read only access, highlight it and then click on the left hand arrows button to move it to the **Access Granted** panel.
   - **Access granted to** panel that is no longer to have access, highlight it and then click on the right hand arrows button to move it to the **Access Not Granted** panel.
4) For those user groups that are granted access and which you want to allow to amend the view enable **Edit**.
5) Click:
   - **OK** to save your changes and exit the dialog.
   - **Cancel** to exit the dialog without saving your changes.

# Troubleshoot Views

## My Network View is Empty

My Network view shows the managed objects to which a user is permitted access. It is the union of all objects contained in the views to which a user has access. The My Network view may be empty if the user’s user groups are not associated to any views, or are only associated to empty views.

## A View has Disappeared

By default the owner of a view is the user that created it. Administrators can change the view owner to any other user. However, in changing view ownership if the administrator is not a member of a group that has access to that view then the administrator may no longer see the view in their Explorer. Whether an administrator can see these private views is set through Preferences.

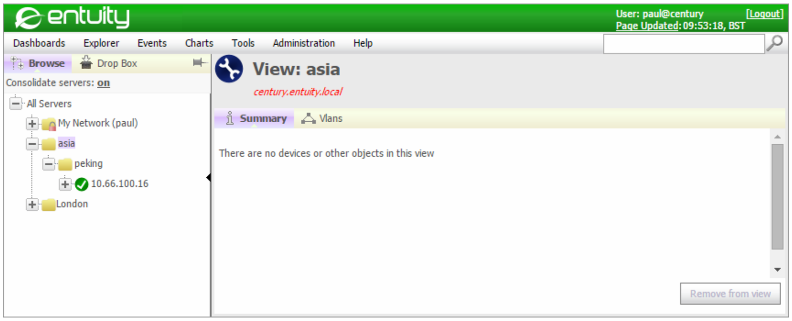
Private views are views to which only the owner and members of the administrators group have access. Private views are hidden to make the Explorer interface easier to manage, you might only make private views visible for the duration of a particular task.

To display hidden views:

1) Click **Preferences**.
2) Uncheck **Exclude Other User's Private Views**. When:
   - Selected (default), administrators only see those views to which they have access through their non-administrator user groups and view ownership settings.
   - Not selected, administrators have all views displayed in their Browse panel.
3) Click **Submit**.

## I Can See Views but not Their Content

When building hierarchies of views ensure you assign consistent access permissions throughout the hierarchy. Entuity can only display sub-views in the Explorer tree under their parent view. If a user does not have permission to view the parent view, they will still be able to see the view but will not be able to see its contents.



View: asia

century.entuity.local

There are no devices or other objects in this view

Figure 221 Inconsistent User Permissions and View Hierarchies

# 35 Manage Entuity User Groups

User groups are a major determinant of the permission level of the group members. Through associating user profiles with more than one user group, you can build profiles that match the varied requirements of different types of users.

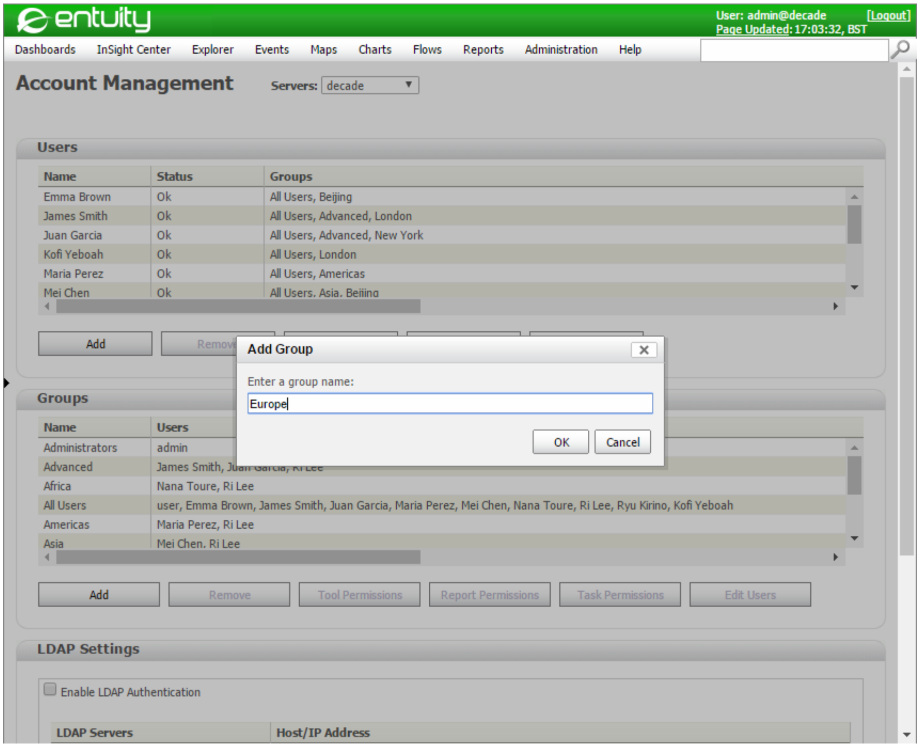
## Creating User Groups

Ensure that you log on to Entuity using an account that is a member of the Administrators user group, and then:

1) Click **Administration** > **Account Management**.

2) In multi-server environments select the server for which you want to create user groups.

3) From the Groups section click **Add**.



Servers: decade

| Name | Status | Groups |
|---|---|---|
| Emma Brown | Ok | All Users, Beijing |
| James Smith | Ok | All Users, Advanced, London |
| Juan Garcia | Ok | All Users, Advanced, New York |
| Kofi Yeboah | Ok | All Users, London |
| Maria Perez | Ok | All Users, Americas |
| Mei Chen | Ok | All Users, Asia, Beijing |

| Name | Users |
|---|---|
| Administrators | admin |
| Advanced | James Smith, Juan Garcia, Ri Lee |
| Africa | Nana Toure, Ri Lee |
| All Users | user, Emma Brown, James Smith, Juan Garcia, Maria Perez, Mei Chen, Nana Toure, Ri Lee, Ryu Kirino, Kofi Yeboah |
| Americas | Maria Perez, Ri Lee |
| Asia | Mei Chen, Ri Lee |

Enter a group name: Europe

□ Enable LDAP Authentication

| LDAP Servers | Host/IP Address |
|---|---|

Figure 222 Creating a New User Group

4) In *Group Name* enter a meaningful, unique name for the group and click **OK**.

Entuity creates the user group and displays a confirmation dialog. By default all users are excluded from the group.

5) Click **OK** to close the dialog.

## Setting User Group Membership

You can select a user and manage their assignments to groups, alternatively you can select a group and manage the users assigned to it. Ensure that you log on to Entuity, using an account that is a member of the Administrators Group.

To manage users assigned to a group:

1) Click **Administration** > **Account Management**.

2) In multi-server environments select the server for which you want to create user groups.

3) From the Groups section highlight the required group and click **Edit Users**. Entuity displays the Edit Group Members dialog.

   All the users who are currently included in the group are displayed in the left hand Members panel, whilst all those excluded are displayed in the right hand Non-members panel.

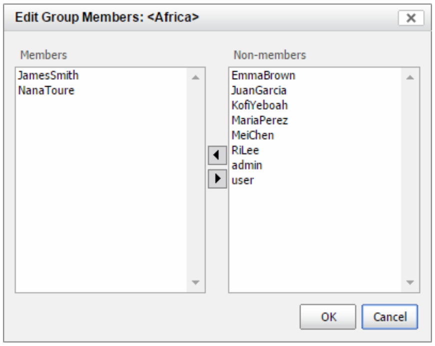


Figure 223 Modifying the Members of an User Group

4) The current members and non-members of the user group are displayed in the dialog. To

   - Include users in the group, highlight them in the Non-members panel and select the left pointing arrowhead key to move them to the Members panel.
   - Exclude users from the group, highlight them in the Members panel and select the right pointing arrowhead key to move them to the Non-members panel.

5) Click **OK** to save the amended group, and click **OK** again to confirm your updates.

## User Group Tools, Reports, Tasks and Permissions

Users that are members of the Administrators user group have full access to all of the Entuity tools, tasks and reports, and also access to all of the objects managed by Entuity. You can set up users with permissions appropriate to their role by giving their user account membership of well defined user groups.

## Tool Permissions

For each user group you can set the tools to which the associated members have access and also their permission levels to Entuity functions. As with other user profile attributes, where a user belongs to two groups with different permissions the user’s tool permissions are the sum of both.

! Entuity Configuration Management delivers a powerful tool set for managing ports and devices on your network. You are strongly advised to control user access to the Configuration Management module and fully test your scripts before applying them to your live network. The scripts provided here are only intended to illustrate the functionality and scripting techniques available with this module. Entuity accepts no liability in the event of the instructions in the documentation not being followed when using the module.

| Section | Tool | Description |
|---|---|---|
| Tools | Permissions allow you to control access to Entuity tools. | |
| | Flow Inspection | Access to Integrated Flow Analyzer dashboards and their configuration. Full access is only available to administrators. |
| | Annotation Manager | Access to the Annotation Manager tool. |
| | Application Monitor | Access to the Application Manager tool. |
| | Configuration Management Administration | Access to the Configuration Management module, all of its functionality, defined tasks, steps and schedules and histories. |
| | Configuration Monitor | Access to the Extensible menus available with Configuration Monitor module. |
| | Ticker | Access to the Ticker tool. |
| | TraceRoute | Access to Traceroute from Entuity Server. |
| | Remote Terminal | Access to the Remote Terminal tool. |
| | MIB Browser | Access to the Explorer MIB Browser. |
| Inventory | Permissions allow access to the Inventory page, the Auto Discovery option available on that page and also the Inventory Snapshot page. | |
| | Auto Discovery Administration | Permits a user to run autoDiscovery from the Inventory Administration page (a user must also have the Inventory Administration permission). |
| | Inventory Administration | Allows access to the functionality available through the Inventory Administration menu, e.g. View Devices, Add Devices, Delete Devices. |

Table 56 User Group Tool Permissions

| Section | Tool | Description |
|---|---|---|
| | Inventory Snapshots Administration | Allows users to take snapshots of the selected view's inventory, which are used with the Inventory Change report. |
| | Managed Port Administration | Allows users to unmanage from Entuity ports on a device, and to re-manage previously unmanaged ports. |
| Administrator Tools | Permissions allow access to functionality available through the web interface. Where the Administration option in the web interface section allows access to the menu, unless the functionality available in those menus is enabled here, the user will be able to use the menu but not use the functionality. | |
| | Data Export | Allows access to the functions available through the Data Export menu, e.g. import a data export job, run a data export job. |
| | Event Administration | Allows group members access to the Event Administration functions, e.g. event suppression rules, event ageout, event thresholds, trap management. |
| | Event Suppression | Allows group members to manage event suppressions that are defined through the Suppress Events dialog, available from Explorer and Event Viewer. This is a separate mechanism to suppressions defined through Event Administration. |
| | Entuity Health | Allows access to the functionality within the Entuity Health menu, e.g. License Health, Database Health, Process Health, |
| | Event Notification Administration | Allows access to configure event notifications through the Preferences page. |
| | IP SLA Administration | Allows access to the Multi-Server Remote and Central Administration pages. |
| | Multi-Server Administration | Allows access to the Multi-Server Remote and Central Administration pages. |
| | Object Editing | Allows access to the generic edit tool available in the web UI. |
| | User Defined Polling | Allows access to User Defined Polling tool. |
| | View Audit Log | Allows access to the Entuity audit log. |
| Reports | Section sets report permission levels. | |
| | Flex Reports | Allows members of the group to build Flex Reports. |
| | Reports and InSight Center | Allows members of the group to access Reports and InSight Center reports. |

Table 56 User Group Tool Permissions

| Section | Tool | Description |
|---|---|---|
| | Report Builder | Allows members of the group to build new reports. Requires Reports and InSight Center permission. |
| View Administration | Create Views | Allows members to create views at the top level of the view hierarchy. They can also edit and delete views they own, and create sub-views within views that they own. |
| | Edit View Filters | Allows members to create, edit and delete view filters. |
| | Share Views | Allows members to share views they own with members of selected user groups. |
| | Create Services | Allows members to create services and also edit and delete services that they own. |
| Menus and Links | Permissions allows you to control access to functionality enabled using Custom Menus. The options vary according to which integrations and modules are activated. | |
| | Show Remedy | Custom Menus that are available with the Entuity Remedy AR System integration. |
| | Show User Menus | Custom Menus are always available to members of the Administrators user group. When menu configurations have *toolGroups* set to **Show All Users** you can select Show User Menu to grant all members of the user group access. (See *Chapter 48 - Entuity Custom Menus*.) |

Table 56 User Group Tool Permissions

## Report Permissions

For a user to access a report they must have the appropriate Tool and Report permissions. By default members of the:

- Administrators user group have access to all reporting functionality; they have full access to the Reports UI and to all of the reports.
- All Users group do not have access to the reporting areas of the UI or to any reports.

To grant access to reports users must have complementary tool and reporting permissions:

- There are three separate reporting Tool Permissions. You can grant users access to any combination of them.
- Report Permissions you control the permissions to view, run and edit individual reports. If you grant a user access to a report you must also give them the report tool permission to access the appropriate area of the UI. For example, if you grant a user group View, Run and Schedule permission to the Service Availability report you must also give them the Reports and InSight Center tool permission otherwise they would not be able to access it.

| State | Description |
|---|---|
| **Use default** | Inherits the default report permission. |
| **No Access** | Prevents members of the user group having access to the report (unless they are members of another group with permission). |
| **View only** | Members of the user group can view generated reports. |
| **View and Run** | Members of the user group can run and view reports. |
| **View, Run and Schedule** | Members of the user group can schedule, run and view reports. |

Table 57 Report Permissions

Flex report permissions are wholly handled through the Tool Permissions dialog.

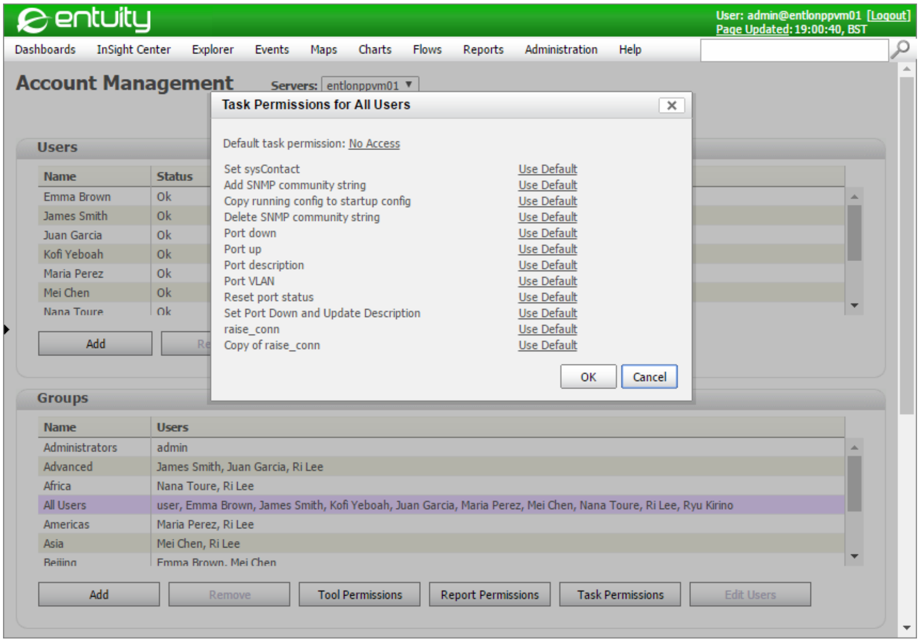
## Task Permissions

You can control user access to Configuration Management tasks on a per-task basis. By default all tasks are set to use the *Default task permission*.

| State | Description |
|---|---|
| **Use default** | Inherits the default task permission. |
| **No Access** | Prevents members of the user group having access to the task (unless they are members of another group with permission). |
| **Run** | Members of the user group can run and view tasks. |
| **Run and Schedule** | Members of the user group can schedule and run tasks. |

Table 58 Task Permissions

By default non-administrator user groups have *Default task permission* set to **No Access**. However users who have the **Configuration Management Administration** tool permission will automatically get the **Run and Schedule** task permission on all tasks. The Task Permissions dialog is updated to indicate the per-task list permissioning is replaced by user group permissioning.



Account Management

Servers: entlonppvm01

Users

| Name | Status |
|---|---|
| Emma Brown | Ok |
| James Smith | Ok |
| Juan Garcia | Ok |
| Kofi Yeboah | Ok |
| Maria Perez | Ok |
| Mei Chen | Ok |
| Nana Toure | Ok |

Task Permissions for All Users

Default task permission: No Access

| | |
|---|---|
| Set sysContact | Use Default |
| Add SNMP community string | Use Default |
| Copy running config to startup config | Use Default |
| Delete SNMP community string | Use Default |
| Port down | Use Default |
| Port up | Use Default |
| Port description | Use Default |
| Port VLAN | Use Default |
| Reset port status | Use Default |
| Set Port Down and Update Description | Use Default |
| raise_conn | Use Default |
| Copy of raise_conn | Use Default |

Groups

| Name | Users |
|---|---|
| Administrators | admin |
| Advanced | James Smith, Juan Garcia, Ri Lee |
| Africa | Nana Toure, Ri Lee |
| All Users | user, Emma Brown, James Smith, Kofi Yeboah, Juan Garcia, Maria Perez, Mei Chen, Nana Toure, Ri Lee, Ryu Kirino |
| Americas | Maria Perez, Ri Lee |
| Asia | Mei Chen, Ri Lee |
| Beijing | Emma Brown, Mei Chen |

Figure 224 Modifying Task Permissions

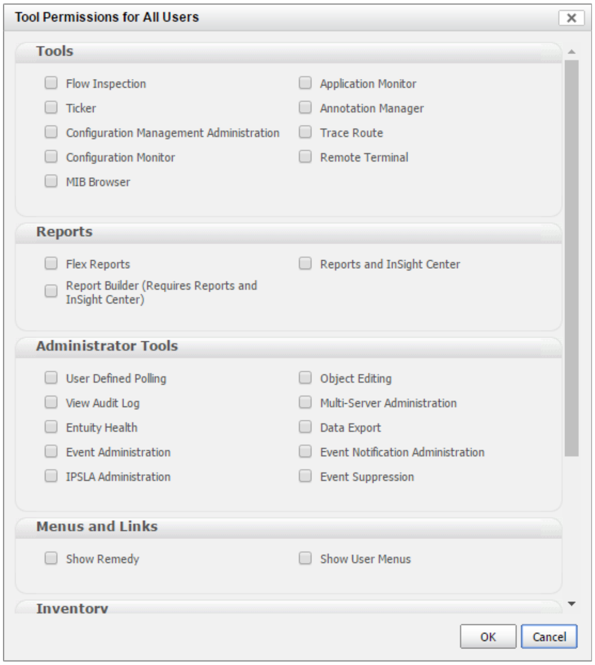
## Modifying User Group Tool, Report and Task Permissions

Ensure that you are logged into Entuity as a member of the Administrators group, and then:

1) Click **Administration** > **Account Management**.

2) In multi-server environments select the server for which you want to amend user group tool permissions.

3) From the Groups section highlight the required group and click **Tool Permissions**.



Tool Permissions for All Users

Tools

□ Flow Inspection
□ Ticker
□ Configuration Management Administration
□ Configuration Monitor
□ MIB Browser
□ Application Monitor
□ Annotation Manager
□ Trace Route
□ Remote Terminal

Reports

□ Flex Reports
□ Report Builder (Requires Reports and InSight Center)
□ Reports and InSight Center

Administrator Tools

□ User Defined Polling
□ View Audit Log
□ Entuity Health
□ Event Administration
□ IPSLA Administration
□ Object Editing
□ Multi-Server Administration
□ Data Export
□ Event Notification Administration
□ Event Suppression

Menus and Links

□ Show Remedy
□ Show User Menus

Inventory

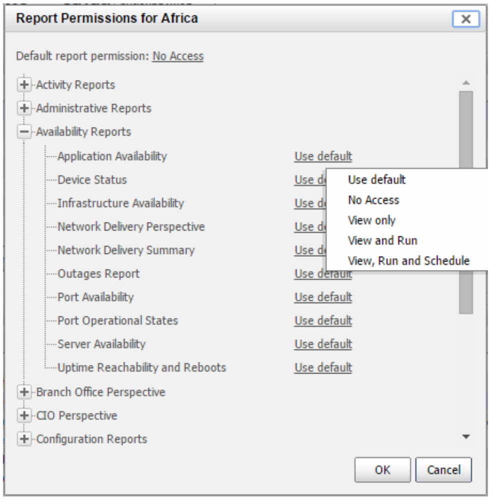
Figure 225 Modifying Tool Permissions

4) Select the check boxes of those tools to which you want members of the user group to have access, and uncheck those to which you want to prevent access.

For example, select InSight Center and Reports when you are also assigning report permissions to the user group, e.g. to view, run or manage reports.

5) Click **OK** to save the amended tool permission settings and exit from the dialog.

6) Click **Report Permissions**. Entuity displays the Report Permissions dialog, the reports are grouped by category.



Report Permissions for Africa

Default report permission: No Access

- Activity Reports
- Administrative Reports
- Availability Reports
  - Application Availability — Use default
  - Device Status — Use d
  - Infrastructure Availability — Use d
  - Network Delivery Perspective — Use d
  - Network Delivery Summary — Use d
  - Outages Report — Use default
  - Port Availability — Use default
  - Port Operational States — Use default
  - Server Availability — Use default
  - Uptime Reachability and Reboots — Use default
- Branch Office Perspective
- CIO Perspective
- Configuration Reports

Figure 226 Modifying Report Permissions

7) For each report expand its category and click on its associated permission status. Entuity displays the report permission states for you to select.

8) Click **OK** to save the amended reports permission settings and exit from the dialog.

9) Select **OK** to close the dialog.

## Deleting User Groups

You cannot delete from Entuity the predefined system user groups, Administrators and All Users. You can delete all other user groups, if you are a member of the Administrators user group.

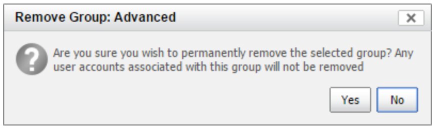
When deleting a user group, Entuity also deletes the association of user accounts to that group but does not delete the actual user accounts. All user accounts will remain a member of the All Users group.

To delete a user group, ensure that you are logged into Entuity as a member of the Administrators group, and then:

1) Click **Administration** > **Account Management**.

2) In multi-server environments select the server for which you want to amend user group tool permissions.

3) From the Groups section highlight the required group and click **Remove**. Entuity displays the Remove Group Confirmation dialog.


Remove Group: Advanced

Are you sure you wish to permanently remove the selected group? Any user accounts associated with this group will not be removed

Figure 227 Removing a User Group

4) Click **Yes** to remove the user group and then click **OK** to close the confirmation dialog.

# 36 Entuity User Profiles and User Groups

The access permissions of a user profile should be tailored to the role of the user, for example you can set which:

- Views a user can access.
- Tools they can use.
- Reports they can create or run.

Within Entuity you can indirectly assign access permissions to user profiles by assigning permissions to user groups. Each Entuity user is a member of one or more user groups, a user profile inherits its access permissions from all of the groups to which it belongs. This inheritance is additive. For example, where a user belongs to two user groups one permitting access to a function that the other denies, then the user has access to that function.

Users can own views. As owners they have read, write and delete access to the view, as well as the ability to:

- Delegate to a group the control of read, write and delete access to the view.
- Specify groups, the members of which have read only access.

You manage user groups and user accounts through the account management pages of the web UI. Also through the web UI you can create views, set view ownership manage view content and use views.

## Predefined User Profiles and User Groups

Before creating or changing views, you should set up user groups, and the user profiles to these groups. When you then create views, you can assign to them user group(s) and through the groups, users.

When you first install Entuity it has:

- Two predefined user groups, **Administrators** and **All Users.**
- Two predefined user profiles, **admin** is a member of both user groups, **user** is only a member of All Users.
- One predefined view, **All Objects** to which all administrators have access.
- Two predefined view My Network views, i.e. **My Network (admin)** and **My Network (user)**. (See *My Network View*.)

The Administrators user group allows members full access to Entuity's functionality, for example:

- Read, write and delete permissions over views.
- Create, modify and delete control over user group and user account permissions.
- Full access to Entuity's web interface, for example access to all administrator tools.

- Configure and run reports
- Full access to user menus.

You cannot delete the Administrators group from Entuity, and it must always have at least one member, initially **admin**.

All user profiles belong to the All Users group. Administrators can change the group's tools and permissions, but by default members of the All Users group have:

- Read only rights to their own predefined My Network view.
- Restricted access to Entuity tools, screens and reports.

✓ Where a user is in more than one group, then that user's access rights are the sum of all the rights of their different groups. For example, admin takes rights from the All Users and Administrators groups, and ends up with total read and write access to all of the views.

## Manage Entuity User Accounts

Account Manager is only available to members of the Administrator user group. Through the Account Manager you can:

- Create, amend and delete user groups.
- Change user group tool permissions.
- Set task permissions.
- Create new users and put them into user groups.
- Amend the passwords of individual users without knowing their previous passwords.
- Set user account security levels, e.g. force password changes, disable an account after a set number of failed logon attempts, create temporary accounts.
- Set Entuity session security, enabling automatic session logout.
- Amend your own password (provided that you know your current password).
- Remove users from the database.

When you are connected to more than one Entuity server, from Account Manager you can select the Entuity server to apply your changes. When a user is connected to more than one Entuity server, the Account Manager shows details for the server to which they first connected.

### Viewing User Account Details

You can view, create and modify user groups and user accounts for both the current Entuity server and any remote server. When you access account management, Entuity structures the information by:

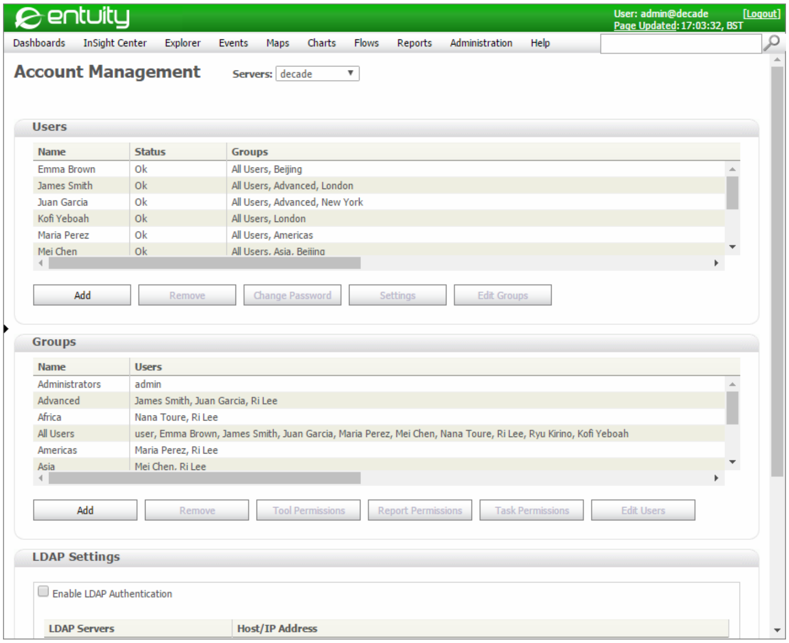
- Servers. When the current Entuity server has one or more remote servers, you can select from a drop down list which Entuity server's user account details to manage.

- Users. For the selected server Entuity displays its user accounts with summary details and access to management functions.
- Groups. For the selected server Entuity displays its user groups with summary details and access to management functions.

To check the status of a user account, for example to see which user groups it is a member of:

1) Click **Administration** > **Account Management**.

   In the Users section locate the row of the user profile. You can check its status and user group membership.


entuity
User: admin@decade [Logout]
Page Updated: 17:03:32, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help

Account Management

Servers: decade

Users

| Name | Status | Groups |
|---|---|---|
| Emma Brown | Ok | All Users, Beijing |
| James Smith | Ok | All Users, Advanced, London |
| Juan Garcia | Ok | All Users, Advanced, New York |
| Kofi Yeboah | Ok | All Users, London |
| Maria Perez | Ok | All Users, Americas |
| Mei Chen | Ok | All Users, Asia, Beijing |

Add Remove Change Password Settings Edit Groups

Groups

| Name | Users |
|---|---|
| Administrators | admin |
| Advanced | James Smith, Juan Garcia, Ri Lee |
| Africa | Nana Toure, Ri Lee |
| All Users | user, Emma Brown, James Smith, Juan Garcia, Maria Perez, Mei Chen, Nana Toure, Ri Lee, Ryu Kirino, Kofi Yeboah |
| Americas | Maria Perez, Ri Lee |
| Asia | Mei Chen, Ri Lee |

Add Remove Tool Permissions Report Permissions Task Permissions Edit Users

LDAP Settings

☐ Enable LDAP Authentication

| LDAP Servers | Host/IP Address |
|---|---|

Figure 228 Entuity User Account Management

| Attribute | Description |
|---|---|
| *Name* | The account profile login name. This username is case insensitive. |

Table 59 User Account Summary

| Attribute | Description |
|---|---|
| *Status* | The current status of the account:<br>■ **OK**, the account is running normally.<br>■ **Expired**, the account password has a time limit within which it must be changed. This period has elapsed, the password has expired and the user must enter a new password the next time they attempt to login.<br>■ **Locked**, the account is locked. When the user attempts to login they are requested to contact their administrator to unlock the account and reset the password. |
| *Groups* | List of user groups to which the user belongs. |

Table 59 User Account Summary

# 37 Manage User Profiles

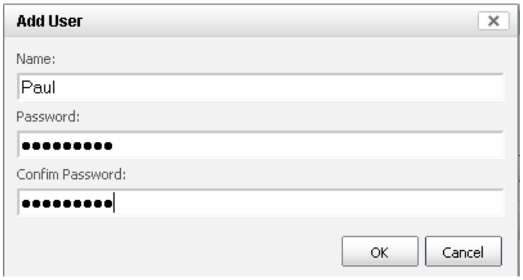
Newly created user accounts consist of a user name, password and membership of the All Users user group. Administrators can then amend user security settings and add users to additional user groups. Administrators can subsequently change user passwords and remove the user account from Entuity.

User accounts inherit their permission level from the user group(s) to which they are associated.

## Creating User Accounts

Ensure that you are logged into Entuity as a member of the Administrators Group, and then:

1) Click **Administration** > **Account Management**.
2) In multi-server environments select the server for which you want to create the user account.
3) From the Users section click **Add**.



Name: Paul

Password: ••••••••••

Confim Password: ••••••••••

Figure 229  Creating a User Account

4) In *Name* enter the Entuity login name for the user.
5) In *Password* enter the Entuity user password. For reasons of security passwords are always displayed as asterisks.
6) In *Confirm Password* enter the password again.
7) Click **OK** to save the user account, click **OK** again to close the confirmation dialog.

## Modifying Passwords

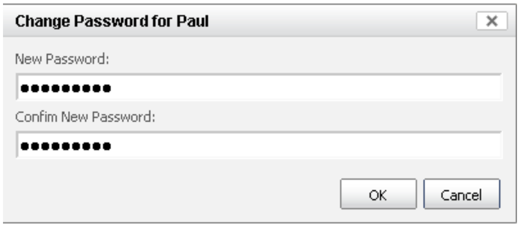
User’s with administrator rights can change both their own password and reset the password of other accounts.

Ensure that you are logged into Entuity as a member of the Administrators Group, and then:

1) Select **Administration** > **Account Management**.
2) In multi-server environments select the server for which you want to modify the user password.

3) From the Users section highlight the name of the user account who’s password you want to amend.

4) Select **Change Password**. For reasons of security passwords are always displayed as asterisks.



Change Password for Paul

New Password: ●●●●●●●●●●

Confim New Password: ●●●●●●●●●●

Figure 230 Changing Your Account Password

5) In *New Password* enter the new password.

6) In *Confirm Password* confirm the new password by re-entering it.

7) Click **OK** to save the new password, or Cancel to keep the existing password. Password changes come into effect the next time the user logs into Entuity.

   Entuity displays a confirmation dialog.

8) Select **OK** to close the dialog.

## User Account Security Settings

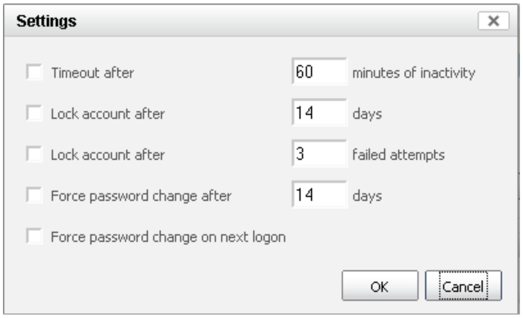
Entuity user account security may be amended to meet your requirements.

| Attribute | Description |
|---|---|
| *Time after* | Allows specification of user accounts that:<br>■ Never time out, the default option active when the check box is not selected<br>■ Are temporary user accounts<br>■ Are expired but can be re-activated. |
| *Lock account after* | Account Disable allows specification of user accounts that:<br>■ Are never disabled, the default option active when the check box is not selected<br>■ Are disabled when users make a set number of consecutive failed attempts to logon to Entuity<br>■ Are disabled but can be re-activated. |

Table 60 User Account Security Settings

| Attribute | Description |
|---|---|
| *Lock account after* | Account Disable allows specification of user accounts that:<br>■ Are never disabled, the default option active when the check box is not selected<br>■ Are disabled after a set number of days<br>■ Are disabled but can be re-activated. |
| *Force password change after* | **Password Change** allows administrators to force users to change their passwords after a set number of days. |
| *Force password change on next logon* | **Password Change** allows administrators to force users to change their passwords the next time they logon, useful when creating new accounts/ resetting passwords and wanting the users to set their own passwords. |

Table 60 User Account Security Settings


Settings

□ Timeout after 60 minutes of inactivity

□ Lock account after 14 days

□ Lock account after 3 failed attempts

□ Force password change after 14 days

□ Force password change on next logon

Figure 231 User Account Security Settings

## Changing User Account Security Settings

By default when a user session is inactive for 24 hours Entuity times out that session.

When you use the automatic refresh available with the web interface Status Summary and TopN Summary dashboards, the regular querying of the Entuity server prevents the session timing out.

To modify user account security settings ensure that you are logged into Entuity as a member of the Administrators Group, and then:

1) Click **Administration** > **Account Management**.
2) In multi-server environments select the server for which you want to create the user account.
3) From the Users section highlight the required user account.
4) From Settings amend the account security settings.
5) Click **OK** to save the new settings, or **Cancel** to keep the existing settings.

## Deleting User Accounts

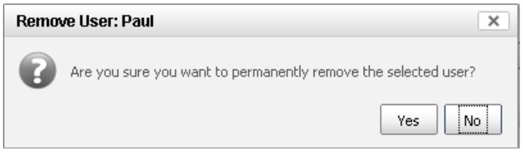
Ensure that you are logged into Entuity as a member of the Administrators Group, and then:

1) Click **Administration** > **Account Management**.

2) In multi-server environments select the server for which you want to delete the user account.

3) From the Users section highlight the user account you want to delete.

4) Highlight the user account to be deleted and select **Remove**.



Remove User: Paul

Are you sure you want to permanently remove the selected user?

Figure 232 Session Security

You cannot delete your own user account.

# 38 Manage Multiple Entuity Servers

Entuity Multi-Server Administration allows you to configure trust between servers. This allows a server to use the resources of another server (or multiple servers). For example you can set up Entuity servers to:

- Act as non-polling central servers with their remote servers polling the network. In this way you can greatly extend the network management capability of an Entuity implementation.
- Act as the license server for all of its remote servers. Although you can have more than one central licensing server, a remote server can only accept license credits from one central licensing server at any one time.
- Use the flow collection capabilities of their remote servers.
- Use the network paths discovered by SurePath (a separate Entuity product).

The trust between servers is verified through an administrator user account which must have the same credential set on all connected servers. Users, both administrators and non-administrators, can access the information on remote servers if they have user accounts on those servers. And the permission levels they have is set by their user account, i.e. although the trust between servers is set through an administrator account the capability of an individual user is set by their account permissions.

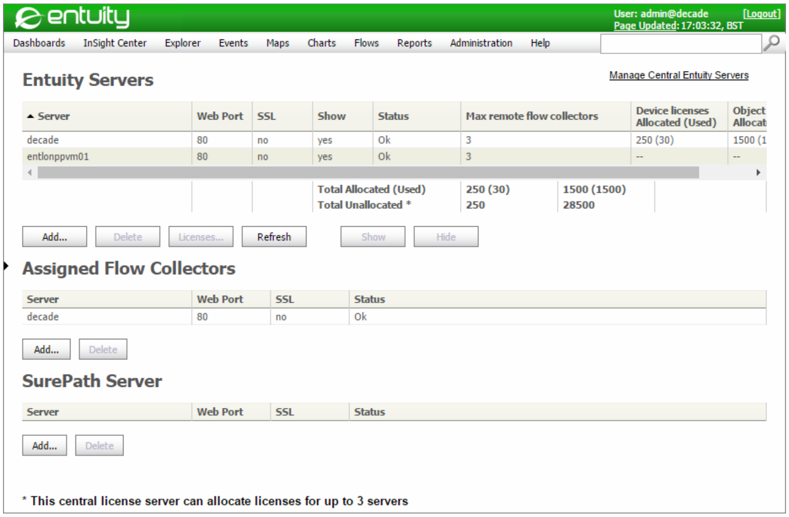
To manage Entuity server access:

1) Click **Administration** > **Multi-Server Administration**.

   Entuity servers page potentially includes three sections (depending upon what you have installed):

   - Entuity Servers section lists remote Entuity servers, servers to which the current server can already access. You can also manage these servers, add new servers and depending upon your licensing model manage their license credit allocation.

     When you click the Manage Central Entuity Servers link Entuity displays those servers that have access to the current Entuity servers. Users with the appropriate access rights on those remote servers can access information on the current Entuity server.
   - Assigned Flow Collectors. An Entuity server can receive and display flow data from the flow collectors which are assigned to it. A flow collector can only be assigned to one Entuity server at one time, although one Entuity server running IFA Premium can have as many collectors assigned to it as its license permits. (See *Assigning Flow Collectors*.)
   - SurePath servers section lists remote servers to which the Entuity server has access, for example to access network paths on SurePath servers. You can add more or remove existing servers. (See *Set Up SurePath Servers*.)



Entuity Servers

| Server | Web Port | SSL | Show | Status | Max remote flow collectors | Device licenses Allocated (Used) | Object Allocat |
|---|---|---|---|---|---|---|---|
| decade | 80 | no | yes | Ok | 3 | 250 (30) | 1500 (1 |
| entlonppvm01 | 80 | no | yes | Ok | 3 | -- | -- |

| | | | | | |
|---|---|---|---|---|---|
| | | | Total Allocated (Used) | 250 (30) | 1500 (1500) |
| | | | Total Unallocated * | 250 | 28500 |

Assigned Flow Collectors

| Server | Web Port | SSL | Status |
|---|---|---|---|
| decade | 80 | no | Ok |

SurePath Server

| Server | Web Port | SSL | Status |
|---|---|---|---|

* This central license server can allocate licenses for up to 3 servers

Figure 233 Entuity Multi-Server Administration

## Example Entuity Multi-Server Set-up

Consider a network managed by four Entuity servers. You may want to grant one server, Entuity Server 1, access to the other three servers. You grant access by logging into Entuity Server 1 and entering the details of the other three servers through the Remote Entuity Servers page.

When you login into one of these remote servers, e.g. Entuity Server 3, then through its Central Entuity Servers page you can view which Entuity servers have access to Entuity Server 3. In this example, only Entuity Server 1. You have the option of revoking the access of Entuity Server 1.

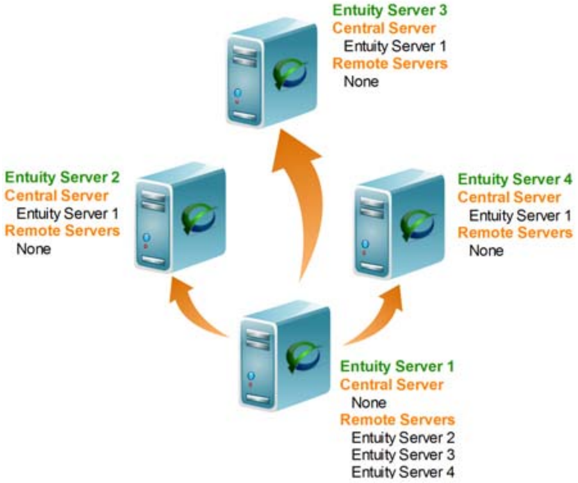


Figure 234 One Central Entuity Server Configuration

As already mentioned, an Entuity server can act as both a central and remote server. In our example four server managed network we may want to allow more than one Entuity server to access information collected by the other servers. We could allow Entuity Server 3 access to Entuity Server 1 and Entuity Server 2.

On Entuity Server 3:

- Entuity Server 1 appears as both a central and remote server, reflecting the mutual level of trust.
- Entuity Server 2 appears as only a remote server, reflecting the one way trust relationship
- Entuity Server 4 is not visible as it was not added to Entuity Server 3 as a remote server.

Entuity Server 3 is added as a central sever to Entuity Server 1 and Entuity Server 2.

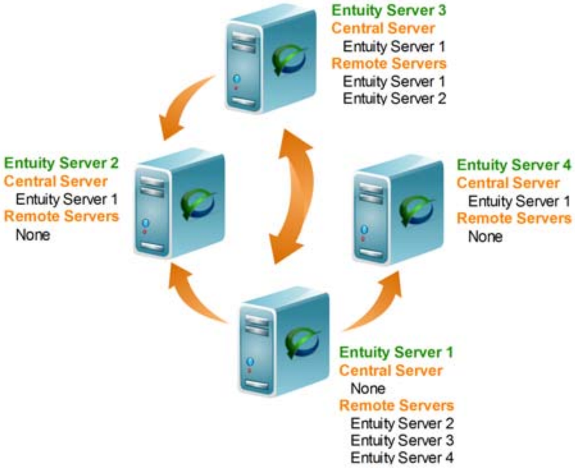


Figure 235 A Multi-Central Entuity Server Configuration

You could configure all Entuity servers to act as both remote and central servers. This allows users with the appropriate access levels to access information on all servers from any other Entuity server.

## Multi-Server Licensing

When using multiple Entuity servers to manage your network, you can assign each Entuity server its own license, tied to its host identifier which specifies the modules and integrations permitted on that server. This standalone license can also set the object and device credits available to the server. Alternatively, you can use an Entuity Central License Server to manage object and credit allocation. (See the *Entuity Getting Started Guide*.)

Using a Central License Server allows you to allocate and re-allocate licensing credits to remote servers as their requirements change. For example, you may have three servers each with local licenses that support the same number of objects. These licenses may not reflect the current loading on those servers.

| Server | License File | Managed Objects |
|---|---|---|
| Entuity Server A | 60000 objects | 45000 |
| Entuity Server B | 60000 objects | 55000 |
| Entuity Server C | 60000 objects | 25000 |

Table 61 Locally Managed Licensing

With a Central License Server you can assign fewer license credits to the lighter loaded server, and more credits to the more heavily loaded server.

| Server | License File | Managed Objects | Assigned credits |
|---|---|---|---|
| Entuity Central Server A | 180000 objects | 45000 | 60000 |
| Entuity Server B | 0 objects | 55000 | 70000 |
| Entuity Server C | 0 objects | 25000 | 40000 |

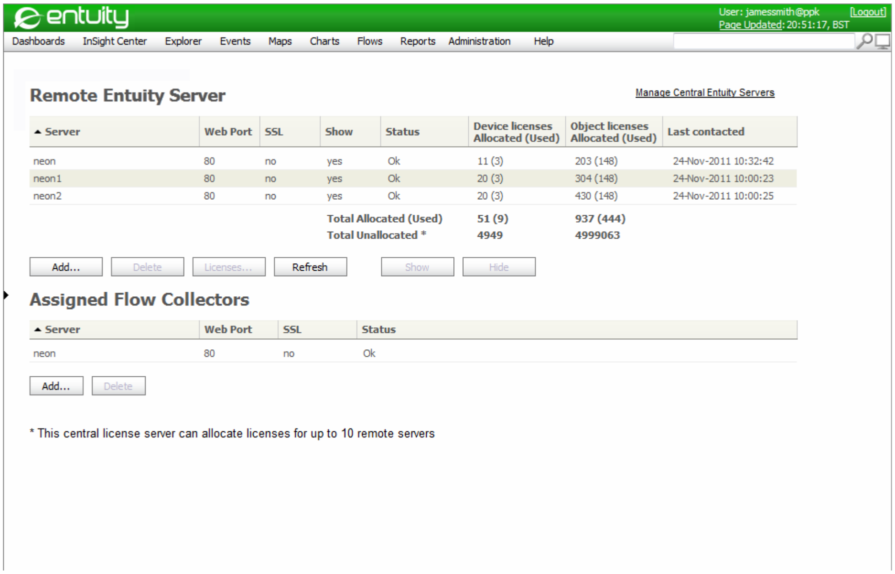
Table 62 Distributed Managed Licensing

When using a Central License Server:

- That is also a polling server you must explicitly assign license credits to that server.
- All servers require a valid license but only the licensing server includes credits for managing objects.
- A remote server can only accept license credits from one central licensing server.
- A central licensing server can only support the number of clients specified in its license file. You can check the number of remote servers the license supports from the Remote Servers page (click **Administration** > **Multi-Server Administration**).
- The central server regularly contacts its clients to confirm its presence and check license object usage. A remote server has a valid period, by default seven days, during which it will run without contact from its server.

  The License Health page reports the valid period of the object and device resources relative to its last contact with its Central Server, whereas the Entuity Expiry Core and module expiry dates refer to the license expiry date.

The license file determines which licensing model is available to you, you should therefore consult with your Entuity representative on the type of licenses you require.



Remote Entuity Server

| ▲ Server | Web Port | SSL | Show | Status | Device licenses Allocated (Used) | Object licenses Allocated (Used) | Last contacted |
|---|---|---|---|---|---|---|---|
| neon | 80 | no | yes | Ok | 11 (3) | 203 (148) | 24-Nov-2011 10:32:42 |
| neon1 | 80 | no | yes | Ok | 20 (3) | 304 (148) | 24-Nov-2011 10:00:23 |
| neon2 | 80 | no | yes | Ok | 20 (3) | 430 (148) | 24-Nov-2011 10:00:25 |
| | | | Total Allocated (Used) | | 51 (9) | 937 (444) | |
| | | | Total Unallocated * | | 4949 | 4999063 | |

Assigned Flow Collectors

| ▲ Server | Web Port | SSL | Status |
|---|---|---|---|
| neon | 80 | no | Ok |

* This central license server can allocate licenses for up to 10 remote servers

Figure 236 Remote Server License Credit Allocation

## Assigning License Credits to Entuity Servers

In multi-server environments a Central License Server can manage the license credits of its remote servers. Before you assign credits to a remote server you cannot access that server’s functionality.

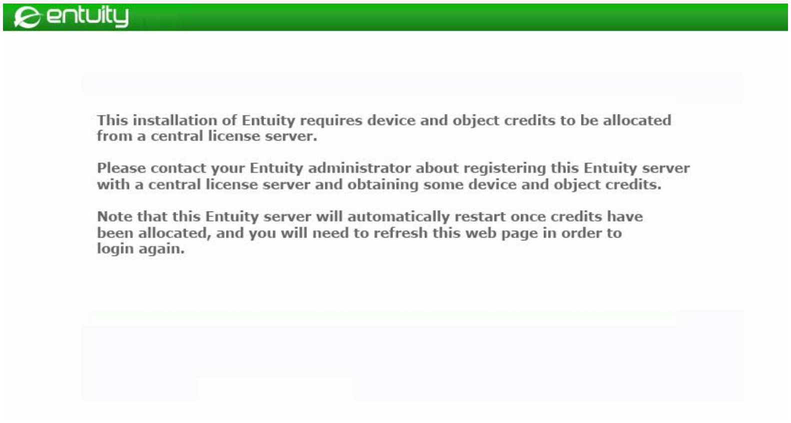
If you also want to use the Central License Server to manage and poll devices you must assign to it license credits; the Central License Server does not automatically assign itself license credits to manage network objects because:

- The server cannot know how many license credits to assign.
- You may not want the Central License Server to manage network objects.

However Entuity Support recommend a Central License Server does not manage network objects or act as a consolidation server. This is especially true in VMware Vmotion environments where the hosting virtual machine may change. For the:

- Remote servers this does not present a licensing problem.
- Central License Server its license is tied to the host identifier. If the machine changes so does the host identifier and the server fails.

You should not include the Central License Server to a VMware Vmotion setup and not use it to manage network objects or as a consolidation server. If the Central License Server fails its remote servers will continue to work for another seven days, which should be sufficient time to recover or rebuild a server.



This installation of Entuity requires device and object credits to be allocated from a central license server.

Please contact your Entuity administrator about registering this Entuity server with a central license server and obtaining some device and object credits.

Note that this Entuity server will automatically restart once credits have been allocated, and you will need to refresh this web page in order to login again.

Figure 237 Remote Server No License Credits Allocated

To assign license credits to a remote server:

1) Click **Administration** > **Multi-Server Administration**.

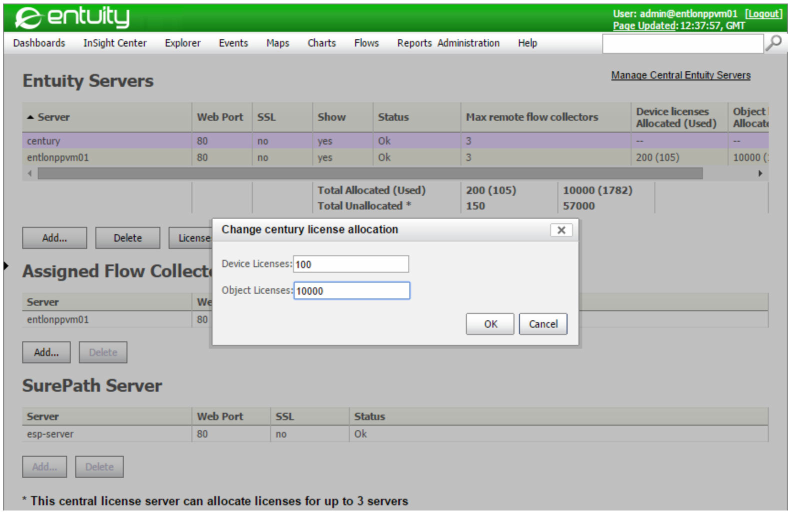
2) Highlight the remote server and then click **Edit**.

   Entuity displays the Change license allocation dialog.

3) Depending upon the license credit model you can enter the number of device and object

license credits to assign to the server.

4) Click **OK**.



Entuity Servers

| Server | Web Port | SSL | Show | Status | Max remote flow collectors | Device licenses Allocated (Used) | Object Allocat |
|---|---|---|---|---|---|---|---|
| century | 80 | no | yes | Ok | 3 | -- | -- |
| entlonppvm01 | 80 | no | yes | Ok | 3 | 200 (105) | 10000 ( |
|  |  |  | Total Allocated (Used)<br>Total Unallocated * | 200 (105)<br>150 | 10000 (1782)<br>57000 |  |  |

Change century license allocation

Device Licenses: 100

Object Licenses: 10000

Assigned Flow Collect

| Server | We |
|---|---|
| entlonppvm01 | 80 |

SurePath Server

| Server | Web Port | SSL | Status |
|---|---|---|---|
| esp-server | 80 | no | Ok |

* This central license server can allocate licenses for up to 3 servers

Figure 238 Allocating Remote Server License Credits

## Deallocating License Credits to Entuity Servers

In multi-server environments a central licensing server can manage the license credits of its remote servers.

When a remote server is unavailable you cannot deallocate its license credits, you must wait for it to be available. When a server is permanently unavailable, for example the remote server is restored from a backup to a new install, then you must wait for one week until the allocation stales. After one week Entuity frees up the license credits and they are ready for reallocation. When possible you should therefore deallocate license credits before moving a server.

To deallocate license credits to a remote server:

1) Click **Administration > Multi-Server Administration**.

2) Highlight the remote server and then click **Edit**.

3) Set the number of device and object license credits to assign to the server to zero.

4) Click **OK**.

# Managing Remote Entuity Servers

Administrators can set up central servers, servers that they use to access information held on other remote Entuity servers, for example the network objects they manage, user account profiles. To access these remote servers administrators must configure trust between the two servers by entering the access details of the remote server to the central server. When an administrator enters valid login details, which includes using a user account that is a member of an administrator group, then the local Entuity server becomes a trusted Central Server on the remote server.

Remote servers are Entuity servers that you have requested access to from the local server. When that access is granted, they have a status of OK. On the remote server if you navigate to the Central Servers page then your local server would be listed there.

| Attribute | Description |
|---|---|
| *Server* | Name of the remote Entuity server. |
| *Web Port* | Web port used by the remote Entuity server. |
| *SSL* | Indicates whether the remote Entuity server uses SSL. |
| *Show* | Indicates whether you want to show this remote server on the local server's Multi-Server Status Summary and Entuity Health pages. |
| *Status* | Current state of trust, which can be:<br>■ **OK**, the remote server considers the local server a trusted server, allowing it access.<br>■ **No Trust**, the remote server may have previously allowed the local server access but has now revoked that access.<br>■ **Service Down**, the remote Entuity server application is down, but the server machine is responding to ping.<br>■ **Communication Failure**, the remote Entuity server machine is down, i.e. not responding to ping. |

Table 63 Entuity Remote Server Details

From the Entuity Servers page you can:

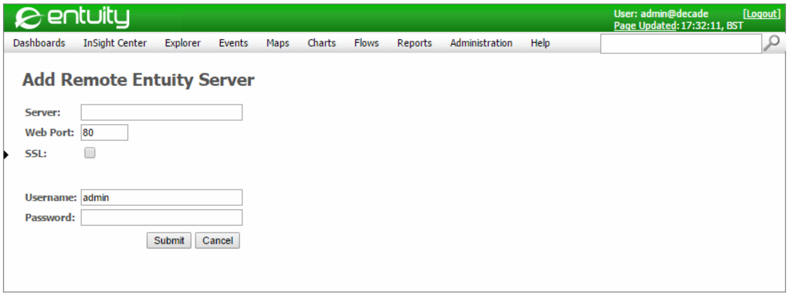
- **Delete** a server. This removes that remote server from the Multi-Server pages, and would also remove the local server from that remote server's list of Trusted Servers.
- **Show** a server. This ensures an available server's details are available in the Multi-Server pages.
- **Hide** a server. This ensures an available server's details are unavailable in the Multi-Server pages.
- **Add** a server. Add more Entuity servers to the list of servers who's details are available in the Multi-Server pages.
- Control license credit distribution through the Central License Server. The Entuity Servers page includes additional options when managing a multi-server license. (See *Multi-Server Licensing*.)

## Adding Remote Servers

To add a remote Entuity server:

1) Click **Administration > Multi-Server Administration**.

2) From the Remote Entuity Servers section click **Add**.



Add Remote Entuity Server

Server:

Web Port: 80

SSL: □

Username: admin

Password:

Figure 239 Adding Remote Servers

3) Complete the remote Entuity server details and click **Submit**.

Entuity attempts to add the remote server, failing with an appropriate warning message if the validation details are incorrect or communication with the server cannot be established.

After the Entuity central server makes a successful connection to the remote server, it displays the Available Servers page, complete with the remote server listed as available.

| Attribute | Description |
|---|---|
| *Server* | Resolved name or IP address of the remote server. |
| *Web Port* | Web port used by the Entuity remote server. |
| *SSL* | Select SSL when used by the remote Entuity server. |
| *Username* | User account on the remote Entuity server that is a member of the administration group. |
| *Password* | Valid password for the user account. |

Table 64 Add a Remote Server

# Manage Central Entuity Servers

Central Servers are remote Entuity servers that are trusted by the local Entuity server. These remote servers can display on their Multi-Server Overview pages details of this local server.

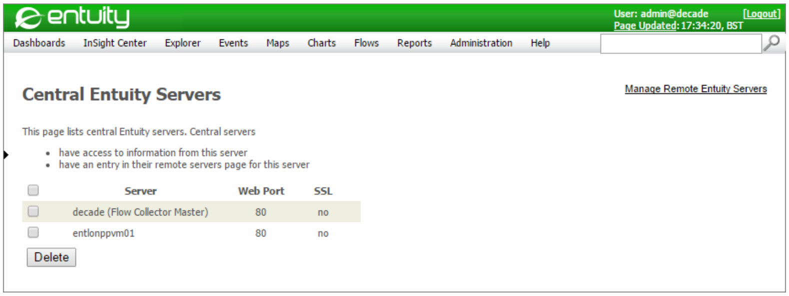
## Viewing Central Entuity Servers

To view trusted Entuity servers:

1) Click **Administration > Multi-Server Administration**.

2) Click the **Manage Central Entuity Servers** hyperlink. Entuity displays the Central Servers page.

The Central Servers page lists the remote servers that can access information on the local server for display on their Multi-Server Status Summary and Entuity Health Summary pages.



Central Entuity Servers

This page lists central Entuity servers. Central servers

- have access to information from this server
- have an entry in their remote servers page for this server

| □ | Server | Web Port | SSL |
|---|---|---|---|
| □ | decade (Flow Collector Master) | 80 | no |
| □ | entlonppvm01 | 80 | no |

Figure 240 Central Entuity Servers

### Removing Central Entuity Servers

To remove trusted Entuity servers:

1) Click **Administration > Multi-Server Administration**.

2) Click the **Manage Central Entuity Servers** hyperlink. Entuity displays the Central Servers page.

3) Use the check box to select the servers you want to remove.

4) Click **Delete**. Entuity removes those servers from the Central Entuity Servers page. On the remote servers Remote Entuity Servers page, this local server would now have a status of **No Trust**. This would prevent that remote server from displaying this local server on its Multi-Server Status Summary and Entuity Health Summary pages.

## Set Up SurePath Servers

You can use SurePath as a standalone server or integrated with other Entuity and SurePath servers. Entuity delivers a complete network management software solution, including inventory discovery and management. SurePath can remotely connect to managing Entuity servers and access their inventory and use the managing servers to poll their devices for the topology data required when building paths.

Entuity Support recommend these four installation configurations:

- SurePath standalone install. The one server both manages devices and discovers paths.
- One Entuity Server to one SurePath Server Install:
  - The SurePath server would be a central server to the Entuity server so it can use the Entuity server’s inventory when discovering paths.
  - The Entuity server would be a central server to the SurePath server to allow users access to the discovered paths from the Entuity server.
- Multiple SurePath server install:
  - One SurePath server would be a central server to the remaining SurePath servers so it can use their inventories and polling capabilities when discovering paths. It does not manage devices.
  - The remaining SurePath servers are not used to generate paths or by users to view

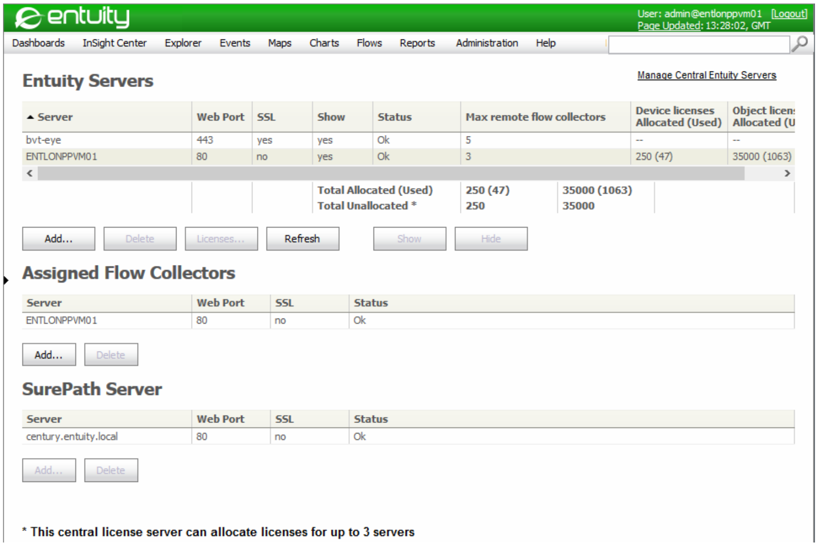
paths only to manage devices. They do not require setting up as central servers.

- One SurePath server and multiple Entuity servers install:
  - One Entuity server would be a central consolidation server, it would not poll or manage devices. It would have all of the other Entuity polling servers and the SurePath server as its remote servers.
  - One SurePath server would be a central server to the same set of Entuity servers as the Entuity consolidation server.
  - The Entuity polling servers server would provide the inventory used by the central Entuity consolidation server and the SurePath server.

To view SurePath servers:

1) Click **Administration > Multi-Server Administration**.

   SurePath Server section displays the remote server to the current server.


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 13:28:02, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
Manage Central Entuity Servers

Entuity Servers

| ▲ Server | Web Port | SSL | Show | Status | Max remote flow collectors | Device licenses Allocated (Used) | Object licen: Allocated (U |
|---|---|---|---|---|---|---|---|
| bvt-eye | 443 | yes | yes | Ok | 5 | -- | -- |
| ENTLONPPVM01 | 80 | no | yes | Ok | 3 | 250 (47) | 35000 (1063) |

| | | |
|---|---|---|
| Total Allocated (Used) | 250 (47) | 35000 (1063) |
| Total Unallocated * | 250 | 35000 |

Add... Delete Licenses... Refresh Show Hide

Assigned Flow Collectors

| Server | Web Port | SSL | Status |
|---|---|---|---|
| ENTLONPPVM01 | 80 | no | Ok |

SurePath Server

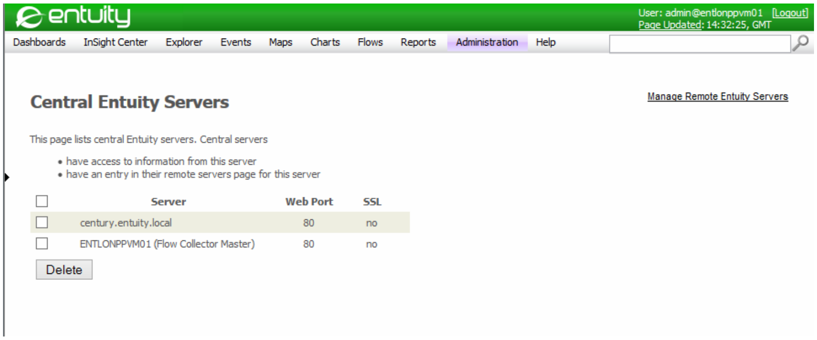
| Server | Web Port | SSL | Status |
|---|---|---|---|
| century.entuity.local | 80 | no | Ok |

* This central license server can allocate licenses for up to 3 servers

Figure 241 SurePath Servers

2) Click the **Manage Central Entuity Servers** hyperlink. Entuity displays the Central Servers page.

   The Central Servers page lists the remote servers that can access information on the local server.



Central Entuity Servers

This page lists central Entuity servers. Central servers

- have access to information from this server
- have an entry in their remote servers page for this server

| □ | Server | Web Port | SSL |
|---|---|---|---|
| □ | century.entuity.local | 80 | no |
| □ | ENTLONPPVM01 (Flow Collector Master) | 80 | no |

Figure 242 SurePath Central Servers

## Cloning Entuity Servers

When installing multiple Entuity servers system administrators may take the approach of cloning an existing install, especially where Entuity is installed to a virtual machine. You may identify an Entuity install that, for example has the required:

- View configuration
- User profiles
- Report definitions.

However the cloned install:

- May be managing devices, and usually you would not want multiple servers managing the same devices.
- Would include a license tied to the original machine. When licensing is controlled through a central licensing server then you must assign the new server a license, when assigned locally then you must obtain a new license.
- Would have the server identifier (`serverid`) of the original server.

After cloning an Entuity server that you have used when managing your network, i.e. it includes user profiles and is managing devices:

- Assign to the Entuity server its own server identifier, this is especially important in multi-server environments where Entuity servers are distinguished through their identifier.

  The Entuity server must not be running and then from the command line run:

  ```
  configure serverid new
  ```

  (for more options see the *Entuity System Administrator Reference Manual*).
- Obtain a new license from your Entuity representative.
- When you want to:
  - Retain the user permissions, view structures and report definitions but not the device inventory then from the Inventory page remove all devices.

- Start with a fresh Entuity installation then during install and configure instruct Entuity to delete the database.

# Considerations for Setting Up Multiple Entuity Servers

In Entuity multi-server environments you must determine how you want to group devices before assigning them to an Entuity server. For Entuity itself consider:

- Root cause analysis is local to each Entuity server. All hops along critical traceroute paths should be managed on the same server.
- Entuity maps only show and maintain connections between devices managed by the same Entuity server. You can include devices managed by different servers to the same map, but to show connectivity between devices managed on different servers you would have to draw the connecting line.
- Connected End Host IP address identification requires ARP cache information to be collected on the same Entuity server that is managing the switches to which the hosts are connected.

## Collecting ARP Cache Information

In multi-server environments an Entuity server may not manage routers from which it requires ARP cache information to perform end host IP address resolution on devices it does manage.

For example, when there are two separate sites and a core distribution network that joins the two, it makes sense to manage the core routers on the same server. You can then build maps to display the core distribution network. The two sites you can mange on separate Entuity servers. However, this may leave one of the servers (the one that does not manage the core) without distribution routers from which to extract ARP cache data, which is used to populate connected end host IP addresses.

Rather than have more than one Entuity server manage the same routers, through a device file you can configure `ipman` to collect ARP cache information from these routers.

By default `provost` runs `ipman` with **-f**, but does not reference a device file. You must create a device file and through `entuity.cfg` identify it to `ipman`. `ipman` can then collect ARP cache information from the routers specified in the device file.

To set ipman to collect ARP cache information from routers an Entuity server does not manage:

1) Create a tab delimited text file containing the hostname or IP address, and SNMP read community string for each router `ipman` polls.

   For example the file *entuity_home*`\etc\arp_cache_devices.cfg` contains:

   ```
   10.12.12.1 public
   rLonodon01 commstring
   ```

✓ Entuity recommend you use the example location and name of the device file to ensure it is maintained during Entuity upgrades.

2) In `entuity.cfg` specify the name of the device file, `D:\Entuity\etc\entuity.cfg`:

```
[ipman]
devicefile=D:\Entuity\etc\arp_cache_devices.cfg
```

The next time `ipman` runs it references the device file.

## Monitoring Multiple Entuity Multi-Servers

When you are monitoring multiple Entuity servers, the web UI overview pages can report on all servers for which trust is established and for which you have appropriate access rights. For example, these are pages with multi-server capability:

- Status Summary, TopN Summary and Device Metrics are available through the Dashboards menu.

  Which servers and views are available. and whether the content of those views across servers is consolidated is configurable through your Preferences.
- Health Summary, available through **Administration** > **Entuity Health**.
- Multi-Server Administration pages available through **Administration** > **Multi-server Administration**.

### Monitoring Remote Server Reachability

Entuity central server polls its remote servers to check their reachability. The polling mechanism checks all layers of the central and remote server connection. By default if the response time of any given remote server drops below the predefined timeout, then:

- The central server stops requesting information from the remote server, e.g. request are automatically disabled for the remote server’s events and incidents, managed object details. If you select the:
  - Remote server in the Explorer tree, no data is available.
  - Multi-server configuration page the remote server is reported as having a connection failure.
  - Health Summary the remote server is reported as having a connection failure.

  The central server does continue to poll all remote servers for their availability. This allows the central server to start re-polling a remote server when it is once again reachable.
- The central server's Page Status is updated. A warning icon indicates the reachability status of the unreachable remote server.

# Accessing Multi-Server Status Summary

The Status Summary dashboard provides a by view summary of the state of your network, it includes views both managed by your local server and its available remote servers. By default the page refreshes every five minutes.

Through rollovers and hyperlinks you can access more detailed information.

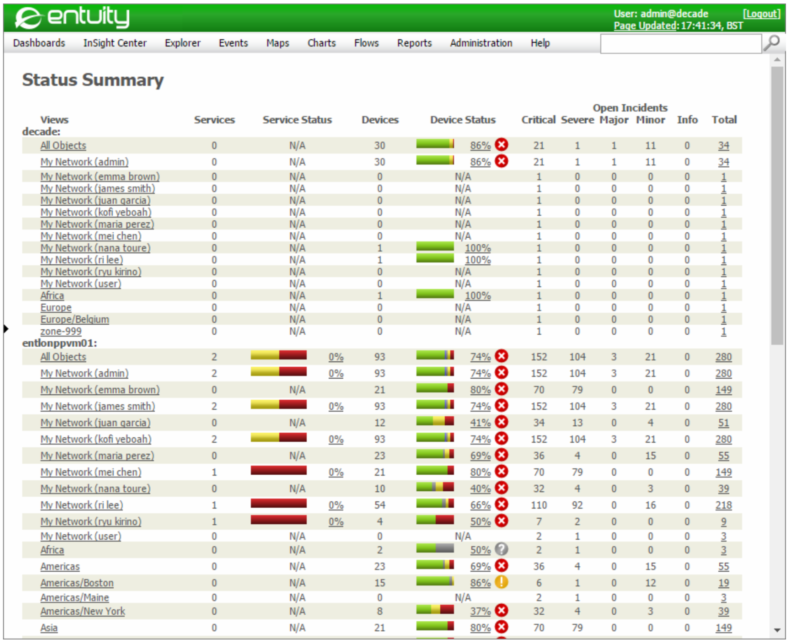
| Attribute | Description |
|---|---|
| *Views* | Name of the Entuity view. You can click on it to open Explorer with the focus on that view. |
| *Services* | Number of services associated with the view. |
| *Service Status* | The segments in the colored bar indicate the current states of services within a view. When you place the mouse over a colored segment Entuity displays a breakdown of the services in that state, e.g. **75% (6/8) Up**. Entuity displays **N/A** (Not Applicable), when there are no services in the view.<br>The percentage value represents the number of services in the view with an UP state as a percentage of the total number of services in the view. You can click through to access a summary of services in the view. |
| *Devices* | Number of devices within the view. |
| *Device Status* | Entuity determines device state by their responses to ICMP ping and/or SNMP polling, hostname resolution and system status.<br>The segments in the colored bar indicate the current states of devices within a view. When you place the mouse over a colored segment Entuity displays a breakdown of the devices in that state, e.g. for a green segment **83.2% (119/143) Ok**.<br>The percentage value represents the number of devices within the view that are OK, as a percentage of the total number of devices in the view. You can click on the hyperlink to launch the Device Status report which shows the current state of devices.<br>The device state icon represents the worst state of a device within the view. When you rollover the icon Entuity displays a breakdown of device states within the view, for example **1 device is degraded 1 device is in unknown state**. |
| *Open Incidents* | A by incident severity breakdown of incidents raised against devices in the view. You can click on the *Total* hyperlink to view the current open incidents for the view. |

Table 65 Status Summary Dashboard

To access the Status Summary dashboard:

1) Click **Dashboards > Status Summary**.

2) You can click on the hyperlinks to access the remote server. You must login, only once per browser session, but are then presented with the appropriate screen, depending on what you clicked on:



## Status Summary

| | | | | | | | Open Incidents | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Views | Services | Service Status | Devices | Device Status | Critical | Severe | Major | Minor | Info | Total |
| **decade:** | | | | | | | | | | |
| All Objects | 0 | N/A | 30 | 86% ✖ | 21 | 1 | 1 | 11 | 0 | 34 |
| My Network (admin) | 0 | N/A | 30 | 86% ✖ | 21 | 1 | 1 | 11 | 0 | 34 |
| My Network (emma brown) | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| My Network (james smith) | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| My Network (juan garcia) | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| My Network (kofi yeboah) | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| My Network (maria perez) | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| My Network (mei chen) | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| My Network (nana toure) | 0 | N/A | 1 | 100% | 1 | 0 | 0 | 0 | 0 | 1 |
| My Network (ri lee) | 0 | N/A | 1 | 100% | 1 | 0 | 0 | 0 | 0 | 1 |
| My Network (ryu kirino) | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| My Network (user) | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| Africa | 0 | N/A | 1 | 100% | 1 | 0 | 0 | 0 | 0 | 1 |
| Europe | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| Europe/Belgium | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| zone-999 | 0 | N/A | 0 | N/A | 1 | 0 | 0 | 0 | 0 | 1 |
| **entlonppvm01:** | | | | | | | | | | |
| All Objects | 2 | 0% | 93 | 74% ✖ | 152 | 104 | 3 | 21 | 0 | 280 |
| My Network (admin) | 2 | 0% | 93 | 74% ✖ | 152 | 104 | 3 | 21 | 0 | 280 |
| My Network (emma brown) | 0 | N/A | 21 | 80% ✖ | 70 | 79 | 0 | 0 | 0 | 149 |
| My Network (james smith) | 2 | 0% | 93 | 74% ✖ | 152 | 104 | 3 | 21 | 0 | 280 |
| My Network (juan garcia) | 0 | N/A | 12 | 41% ✖ | 34 | 13 | 0 | 4 | 0 | 51 |
| My Network (kofi yeboah) | 2 | 0% | 93 | 74% ✖ | 152 | 104 | 3 | 21 | 0 | 280 |
| My Network (maria perez) | 0 | N/A | 23 | 69% ✖ | 36 | 4 | 0 | 15 | 0 | 55 |
| My Network (mei chen) | 1 | 0% | 21 | 80% ✖ | 70 | 79 | 0 | 0 | 0 | 149 |
| My Network (nana toure) | 0 | N/A | 10 | 40% ✖ | 32 | 4 | 0 | 3 | 0 | 39 |
| My Network (ri lee) | 1 | 0% | 54 | 66% ✖ | 110 | 92 | 0 | 16 | 0 | 218 |
| My Network (ryu kirino) | 1 | 0% | 4 | 50% ✖ | 7 | 2 | 0 | 0 | 0 | 9 |
| My Network (user) | 0 | N/A | 0 | N/A | 2 | 1 | 0 | 0 | 0 | 3 |
| Africa | 0 | N/A | 2 | 50% ? | 2 | 1 | 0 | 0 | 0 | 3 |
| Americas | 0 | N/A | 23 | 69% ✖ | 36 | 4 | 0 | 15 | 0 | 55 |
| Americas/Boston | 0 | N/A | 15 | 86% ! | 6 | 1 | 0 | 12 | 0 | 19 |
| Americas/Maine | 0 | N/A | 0 | N/A | 2 | 1 | 0 | 0 | 0 | 3 |
| Americas/New York | 0 | N/A | 8 | 37% ✖ | 32 | 4 | 0 | 3 | 0 | 39 |
| Asia | 0 | N/A | 21 | 80% ✖ | 70 | 79 | 0 | 0 | 0 | 149 |

Figure 243 Entuity Status Summary

# 39 Entuity User Authentication

You can control access to Entuity either internally through its own security database or externally by integrating Entuity user groups and names within the LDAP environment.

## Entuity Internal Authentication

You can configure Entuity to run using internal authentication, where Entuity compares user sign on details with the details held for that account in Entuity’s local database. On successful authentication Entuity assigns user permissions derived from the user groups the user’s account is associated with.

Entuity internal authentication allows for:

- Definition of user accounts on the local server.
- Assignment of users to Entuity user groups.

  User groups are used in user authorization; when determining whether a user has the appropriate permission to perform the requested action.
- Retention of user preferences between sessions.

## Entuity External Authentication

You can configure Entuity to compare user sign on details with the account details held in the external LDAP authentication system. When successful Entuity derives the account’s network group membership and maps these to the Entuity user groups, deriving the Entuity user account permissions.

Integrating Entuity user accounts within an LDAP environment both increases the network system administrator’s control over access to Entuity and reduces the user account administrative overhead. You can set up user groups within Entuity but manage user accounts at the network level.

Entuity external authentication is implemented through LDAP servers, specifically:

- LDAPv3 (RFC 3377)
- OpenLDAP 2.3
- Active Directory for Windows 2003
- Active Directory for Windows Server 2008.

You can assign Entuity servers to more than one LDAP server and also specify their preference level, and under what conditions the Entuity server would contact a second server when login validation by the first is unsuccessful.

LDAP server configuration is outside the scope of this guide. You must know and understand your current LDAP configuration before implementing it with Entuity.

## Entuity Security Service

Entuity user authentication uses a security service that can communicate, depending upon the implementation, authentication details between external authentication system(s) and the Entuity security database. You can configure the security service, specifying the:

- Authentication content, e.g. user name, password, permission attributes
- Location of the external authentication system.

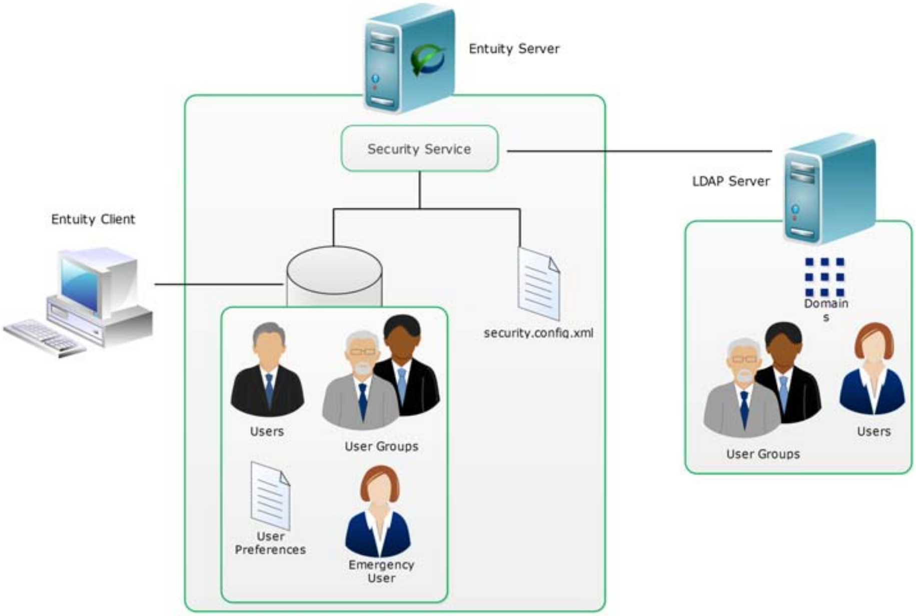


Figure 244 External Authentication Architecture

Entuity Security Service is the web service which translates external user attributes to Entuity user groups. You can specify translation rules through a configuration, access to which is available through the Account management area of the web UI.

You can configure the security service to run without external authentication, where user information is held in the local security database and is available for management through the Entuity client.

# Example Entuity User Authentication Implementations

Where multiple Entuity servers are installed, multiple security databases are also installed with the same number of security services. You can configure the Entuity servers, more specifically the security services, to use their local databases or external LDAP authentication.

✓ By default security services are configured for internal authentication. It is your responsibility to ensure all security services are consistently and appropriately configured, e.g. use the same authentication method, the appropriate mapping rules.

## Entuity and Internal Authentication

The default implementation for an Entuity server is for it act as a standalone installation, with its user authentication details held in its local security database.

When you are installing multiple Entuity servers with internal authentication each Entuity server maintains its own user accounts, user groups and user preferences. This independence allows users and user groups on different servers to share the same names but have different definitions, e.g. group permissions, user membership to groups and user preferences may all differ.

Although internal authentication is initially the easiest method to implement, where you are installing multiple Entuity servers and LDAP is already implemented the benefits of external authentication make it the recommended solution.

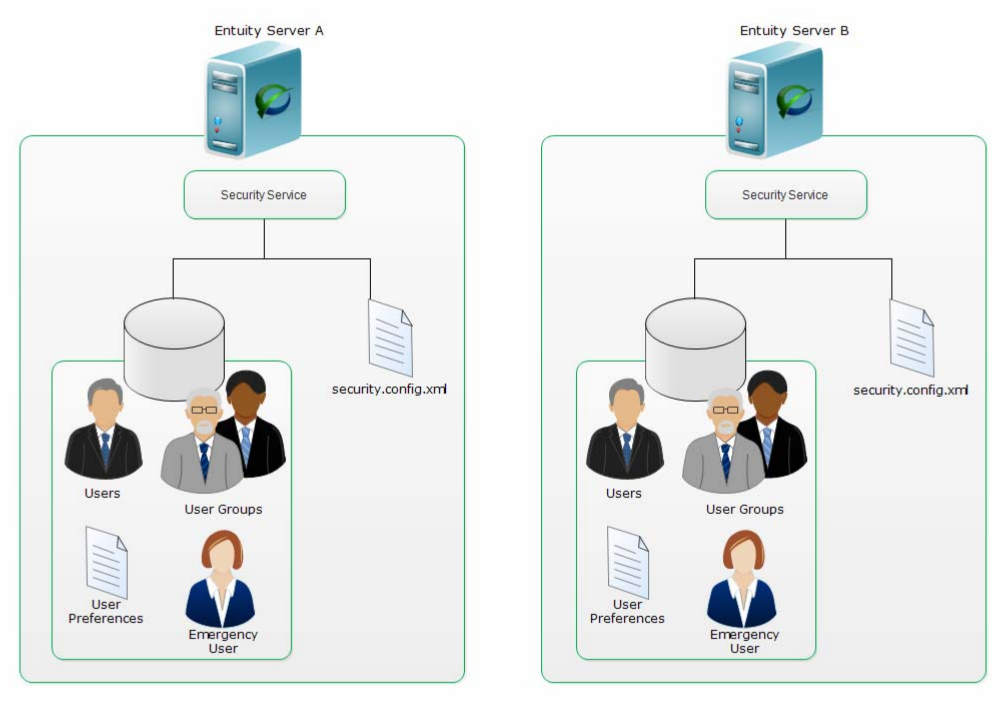


Figure 245 Entuity Servers Using Local Databases

## Entuity and LDAP Authentication

Entuity servers can be integrated into environments where LDAP authentication systems are already implemented. Entuity external authentication can work with a single Entuity server and multiple Entuity servers running local security databases.

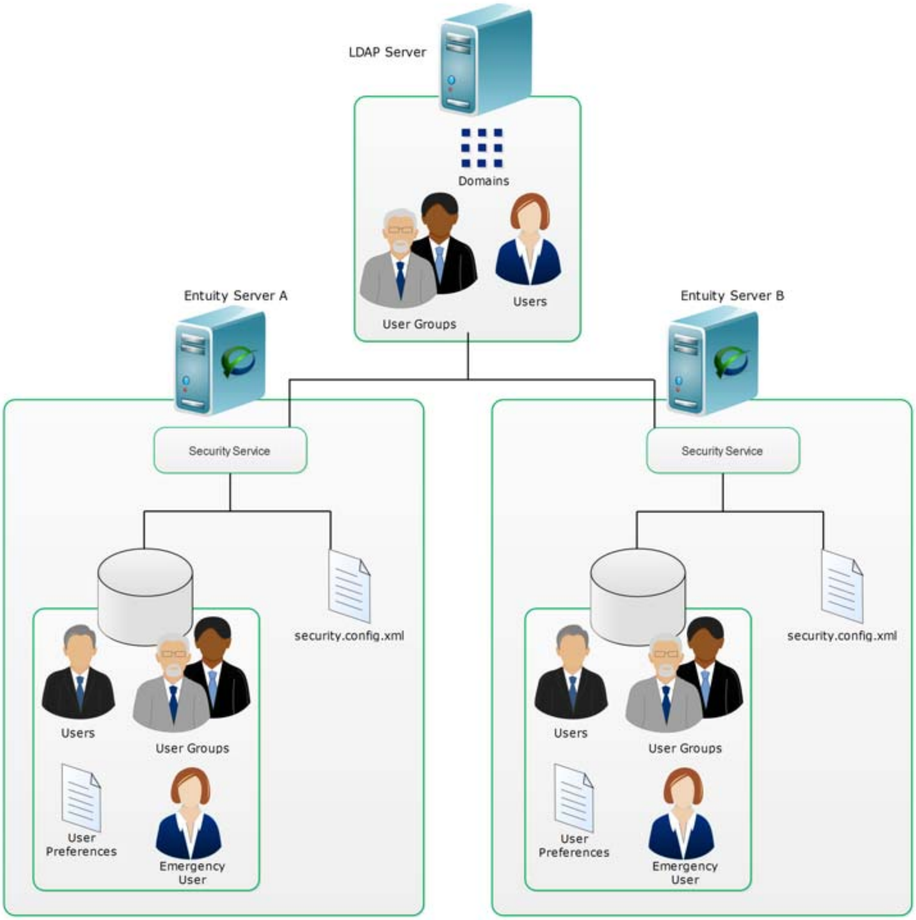


Figure 246 Entuity Servers Using External Authentication

## Set-up Entuity to use LDAP Authentication

To use an external authentication server you must:

- Have a supported LDAP environment.
- Set-up user groups on the Entuity server. You can also set-up user accounts, although Entuity would recommend only setting up user groups.
- Configure each Entuity server to work in the LDAP environment.
- Activate the LDAP configuration on the Entuity server.

Configuration and activation of LDAP authentication is through the Account Management pages of the Entuity server. Entuity web UI guides you through LDAP configuration, for which you must specify:

- LDAP server details
- LDAP group matching
- LDAP group mapping.

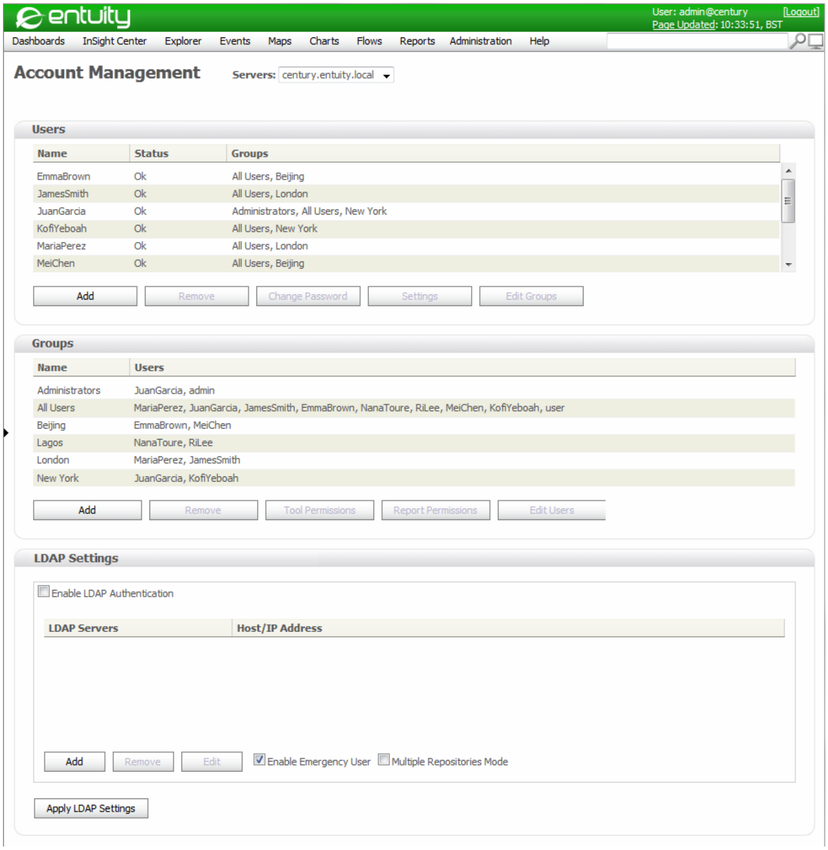
Entuity creates an XML file to hold the authentication details, *entuity_home*/`etc/security.config.xml`. When you want:

- A more complex authentication configuration than possible through the web UI, you can directly edit `security.config.xml`.
- To propagate the same configuration across multiple Entuity servers you can copy `security.config.xml` from a configured server to all other servers. You must still configure on each server the appropriate Entuity user groups.

To access the LDAP management pages when creating an LDAP server entry:

1) Click **Administration** > **Account Management**.
2) From the LDAP Settings section click **Add**.

   Entuity displays the Server Details tab.



Account Management Servers: century.entuity.local

Users

| Name | Status | Groups |
|---|---|---|
| EmmaBrown | Ok | All Users, Beijing |
| JamesSmith | Ok | All Users, London |
| JuanGarcia | Ok | Administrators, All Users, New York |
| KofiYeboah | Ok | All Users, New York |
| MariaPerez | Ok | All Users, London |
| MeiChen | Ok | All Users, Beijing |

Groups

| Name | Users |
|---|---|
| Administrators | JuanGarcia, admin |
| All Users | MariaPerez, JuanGarcia, JamesSmith, EmmaBrown, NanaToure, RiLee, MeiChen, KofiYeboah, user |
| Beijing | EmmaBrown, MeiChen |
| Lagos | NanaToure, RiLee |
| London | MariaPerez, JamesSmith |
| New York | JuanGarcia, KofiYeboah |

LDAP Settings

□ Enable LDAP Authentication

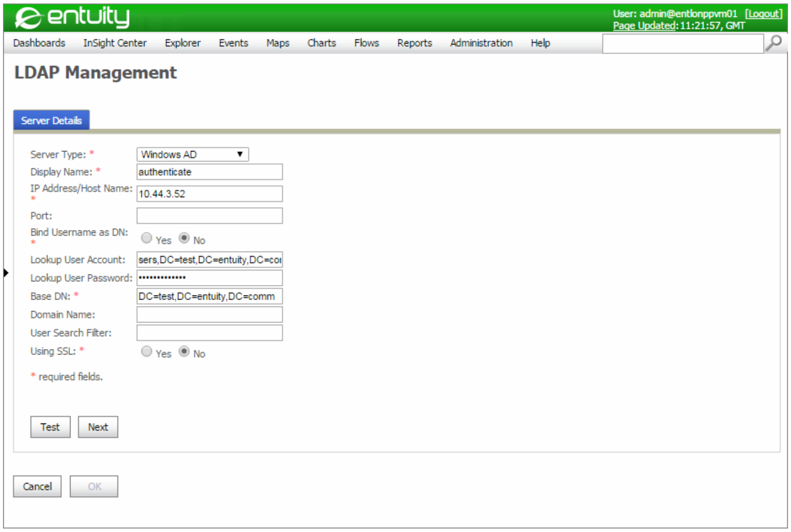
| LDAP Servers | Host/IP Address |
|---|---|

☑ Enable Emergency User □ Multiple Repositories Mode

Figure 247 LDAP Settings

## Server Details

Through the Server Details page you can specify the connection details Entuity requires to connect to the LDAP server.



LDAP Management

Server Type: * Windows AD

Display Name: * authenticate

IP Address/Host Name: * 10.44.3.52

Port:

Bind Username as DN: * ○ Yes ● No

Lookup User Account: sers,DC=test,DC=entuity,DC=coı

Lookup User Password: •••••••••••••

Base DN: * DC=test,DC=entuity,DC=comm

Domain Name:

User Search Filter:

Using SSL: * ○ Yes ● No

* required fields.

Figure 248 LDAP Management Server Details

| Attribute | Description |
|---|---|
| *Server Type* | Entuity supports two types of authentication servers:<br>■ Windows AD<br>■ OpenLDAP/LDAPv3. |
| *Display Name* | Name of the authentication server as displayed in Entuity. |
| *IP Address/Host Name* | IP address or resolved name of the authenticating LDAP server. |
| *Port* | Port used by the LDAP server, not required if using the default (389, or for SSL 636). |
| *Bind Username as DN* | Select:<br>■ **No** (default), Entuity searches the LDAP server for the username.<br>■ **Yes**, if your LDAP server only supports the bind operation using the DN format, and you can not construct a valid user DN using Entuity's expression formats, Entuity can be configured to use an alternative approach. |
| *Lookup User Account* | You must supply an account to access the LDAP server unless the server supports anonymous login.<br>The account must have READ privilege, specifically List Content. In Windows AD, everyone in the domain has READ permission in its own domain by default, other systems may have a different configuration. |
| *Lookup User Password* | Password for the account. |
| *Base DN* | Defines the starting point for searches in the LDAP directory. |

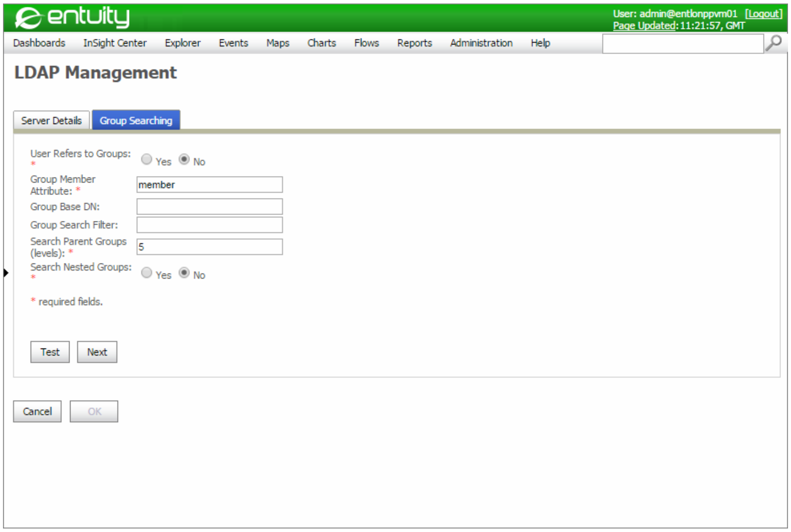
Table 66 LDAP Management Server Details

| Attribute | Description |
|---|---|
| *Username Attribute* | An OpenLAPD/LAPDv3 specific attribute. UPN is used for logging into the LAPD environment and must be unique. |
| *Domain Name* | A Windows AD specific attribute required when using domain names to distinguish between users with the same name in different domains. Enter the domain name to use as the search base. |
| *User Search Filter* | *User Search Filter* only applies when *Bind Username as DN* is set to **No**. This filter restricts the search to the user class and then compares the value to the *`sAMAccountName`* attribute.<br>Depending on the LDAP server configuration, for example if there is an index created on *objectClass*, using this filter can dramatically improve search performance. |
| *Using TLS* | Select:<br>■ **No** when not using TLS.<br>■ **Start TLS**. This is the preferred method of encrypting an LDAP connection. STARTTLS allows unencrypted and encrypted connections to be handled by the same port. It handles a non-encrypted connection by wrapping it with SSL/TLS after/during the connection process.<br>■ **LDAPS** to use SSL. |

Table 66 LDAP Management Server Details

## Group Searching

Through the Group Searching tab you can specify the LDAP filter expression for performing the group search.



LDAP Management

User Refers to Groups: * ○ Yes ● No

Group Member Attribute: * member

Group Base DN:

Group Search Filter:

Search Parent Groups (levels): * 5

Search Nested Groups: * ○ Yes ● No

* required fields.

Figure 249 LDAP Management Group Searching

| Attribute | Description |
|---|---|
| *User Refers to Groups* | When set to:<br>■ **No**, Entuity searches for groups based on Group Base DN and then which group's member contains the user.<br>■ **Yes**, Entuity searches for groups using the user's MemberOf attribute. |
| *Group Name Attribute* | An OpenLDAP/LDAPv3 attribute which sets how to search the groups. |
| *User MemberOf Attribute* | This attribute is only available when *User Refers to Groups* is set to **Yes**. The attribute used to find members of groups, by default memberOf. |
| *Group Member Attribute* | This attribute is only available when *User Refers to Groups* is set to **No**. The attribute name used to find members of groups, by default member. |
| *Group Base DN* | The domain base from which you search for groups. When the value remains empty search uses *Base DN*. |
| *Group Search Filter* | *Group Search Filter* only applies when *User Refers to Groups* is set to **No**. |
| *Search Parent Groups (levels)* | Searches for the group within the current parent group and if not found there would search within its parent-groups and so on until the set number of levels from the current group. |
| *Search Nested Groups* | Searches for the group within the current group and if not found there would search within all nested sub-groups. |

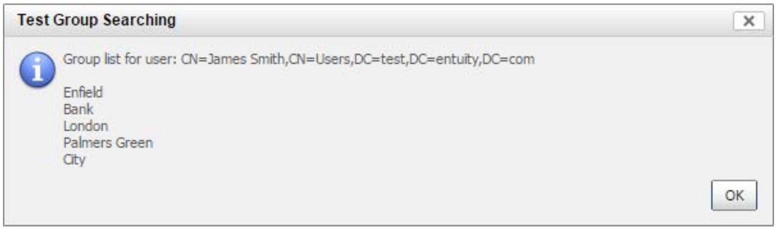
Table 67 LDAP Management Group Searching

There are two options to control group searching in the LDAP tree. Consider a very simple tree (where to be found by the search all of these groups must be under the same Group Base DN):

```
UK -> England -> London -> City -> Devonshire Square
```

The user `James Smith` is a direct member of London. *Search Parent Groups (levels)* can control the upward levels the search would go back. For example, if set to 1, then it will return England and London; and if set 0, then it will only return London.

However when *Search Nested Groups* is set to true, a search will always return all nested groups, in this case both City and Devonshire Square.



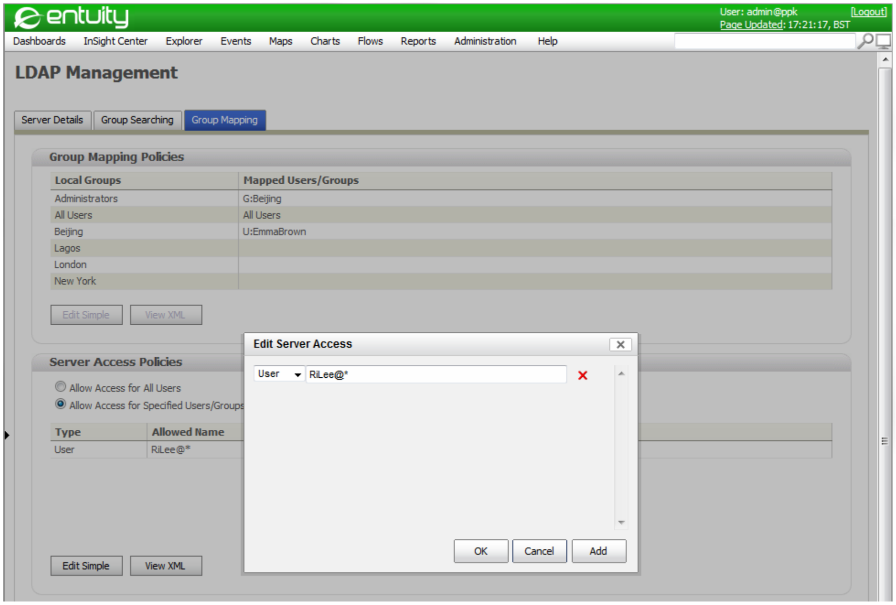
Group list for user: CN=James Smith,CN=Users,DC=test,DC=entuity,DC=com

Enfield
Bank
London
Palmers Green
City

Figure 250 Test Group Searching

## Group Mapping

Through the Group Mapping tab you can map the user groups defined in Entuity to those groups defined on the LDAP server.



LDAP Management

Group Mapping Policies

| Local Groups | Mapped Users/Groups |
|---|---|
| Administrators | G:Beijing |
| All Users | All Users |
| Beijing | U:EmmaBrown |
| Lagos | |
| London | |
| New York | |

Server Access Policies

○ Allow Access for All Users
● Allow Access for Specified Users/Groups

| Type | Allowed Name |
|---|---|
| User | RiLee@* |

Edit Server Access

User RiLee@*

Figure 251 LDAP Management Group Mapping

### Group Mapping Policies

Group Mapping Policies table lists the all of the local groups defined on the Entuity server. You can then map these local groups to LDAP user accounts and user groups.

When Mapped Users/Groups displays:

- Complex XML Content, this implies `security.config.xml` has been directly edited and contains more complex conditions than the web UI can support.
- U:*userName*, G:*groupName*, indicates LDAP user accounts and groups associated with the Entuity group.
- All Users, all LDAP users are mapped to the Entuity user group.
- Empty, there are no mapped LDAP users or user groups.

| Parameter | Description |
|---|---|
| *Local Groups* | The user groups defined on the Entuity server. |
| *Mapped Users/Groups* | The LDAP server users and groups mapped to the local group. When set through the web UI the users and user groups are additively combined |

Table 68 Group Mapping Policy Parameters

The web UI provides an interface for mapping of Entuity local groups with LDAP managed users and groups.

You can directly edit the security file when building more complex mappings. For example this mapping:

```
Administrators  U:RiLee G:Supervisors
```

associates the Entuity Administrators group with user RiLee and the Supervisors user group. This is an additive relationship for RiLee to login he must be a member of the Supervisors group. When you want to allow RiLee or any member of the Supervisors group access to Entuity then you must amend the security configuration file:

```
<condition>
           <or>
           <attr name="userName" contains="RiLee"/>
           <attr name="groups" contains="Supervisors" />
           </or>
</condition>
```

## Server Access Policies

Through the Server Access Policies section you can select how access to the Entuity server is controlled. Select:

- **Allow Access for All Users** to permit access to all users.
- **Allow Access for Specified Users/Groups** to allow access to only the specified users and user groups. User group refers to the LDAP user group and user name refers to the local Entuity user account.

  When you view the XML the first rule is to deny access to all users, subsequent rules specify the exceptions:

```
<serverAccess>
  <denyUserDomain="*" name="*">
  <allowUserDomain="*" name="RiLee">
</serverAccess>
```

## Setting up a Windows AD LDAP Server

This example setups a Windows AD LDAP server using the default configuration. At each stage you should use the Test option to validate your entered configuration details against the LDAP server.

To set-up an LDAP server:

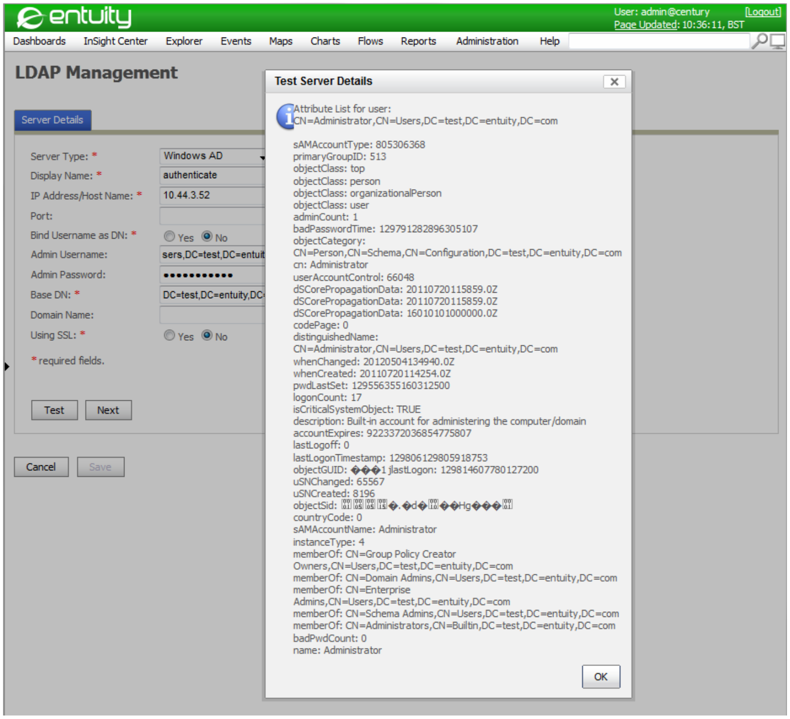
1) Click **Administration > Account Management**.

2) From the LDAP section click **Add**.

   Entuity displays the Server Details page for the LDAP Management configuration.

3) Specify LDAP server details and click **Test**.

Entuity validates these details against the specified LDAP server, and reports validation success through a dialog.



LDAP Management

Server Details

Server Type: * Windows AD
Display Name: * authenticate
IP Address/Host Name: * 10.44.3.52
Port:
Bind Username as DN: * ○ Yes ● No
Admin Username: sers,DC=test,DC=entuit
Admin Password: ••••••••••••
Base DN: * DC=test,DC=entuity,DC=
Domain Name:
Using SSL: * ○ Yes ● No

* required fields.

Test Server Details

```
Attribute List for user:
CN=Administrator,CN=Users,DC=test,DC=entuity,DC=com

sAMAccountType: 805306368
primaryGroupID: 513
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
adminCount: 1
badPasswordTime: 129791282896305107
objectCategory:
CN=Person,CN=Schema,CN=Configuration,DC=test,DC=entuity,DC=com
cn: Administrator
userAccountControl: 66048
dSCorePropagationData: 20110720115859.0Z
dSCorePropagationData: 20110720115859.0Z
dSCorePropagationData: 16010101000000.0Z
codePage: 0
distinguishedName:
CN=Administrator,CN=Users,DC=test,DC=entuity,DC=com
whenChanged: 20120504134940.0Z
whenCreated: 20110720114254.0Z
pwdLastSet: 129556355160312500
logonCount: 17
isCriticalSystemObject: TRUE
description: Built-in account for administering the computer/domain
accountExpires: 9223372036854775807
lastLogoff: 0
lastLogonTimestamp: 129806129805918753
objectGUID: ���1 jlastLogon: 129814607780127200
uSNChanged: 65567
uSNCreated: 8196
objectSid: ▯▯▯▯�.�d�▯��Hg���▯
countryCode: 0
sAMAccountName: Administrator
instanceType: 4
memberOf: CN=Group Policy Creator
Owners,CN=Users,DC=test,DC=entuity,DC=com
memberOf: CN=Domain Admins,CN=Users,DC=test,DC=entuity,DC=com
memberOf: CN=Enterprise
Admins,CN=Users,DC=test,DC=entuity,DC=com
memberOf: CN=Schema Admins,CN=Users,DC=test,DC=entuity,DC=com
memberOf: CN=Administrators,CN=Builtin,DC=test,DC=entuity,DC=com
badPwdCount: 0
name: Administrator
```

Figure 252 Test LDAP Management Server

4) Click **Next** and then enter the Group Searching details.

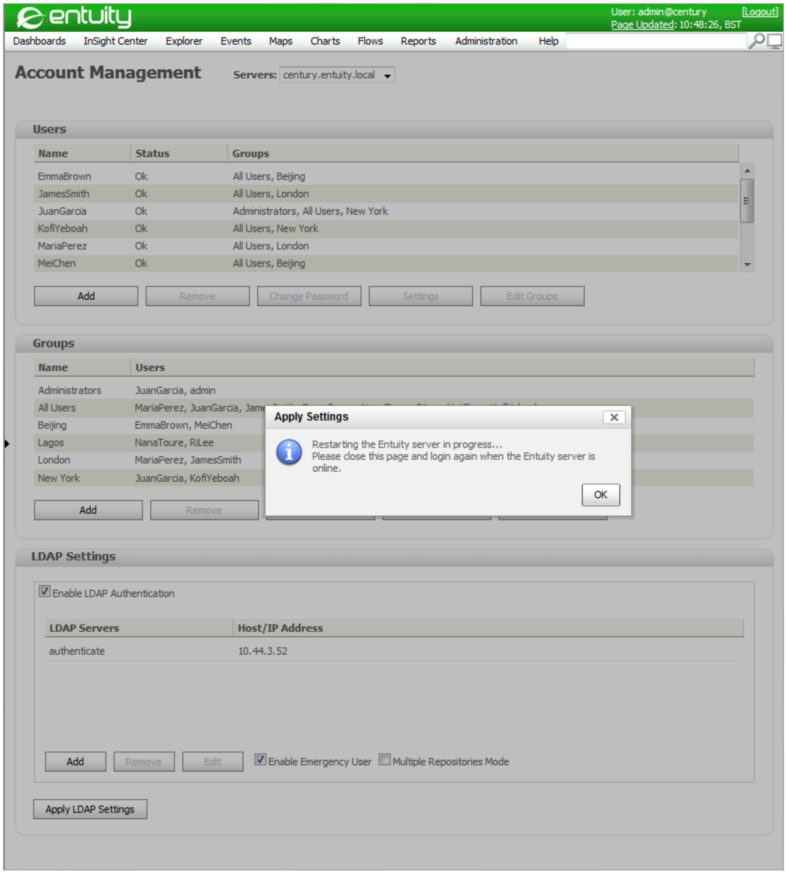
5) Click **Next** and enter Group Mapping details.

6) Click **Save**.

   Entuity displays the Account Management page and in the LDAP Settings section is the newly defined LDAP server. Where you have multiple LDAP servers the order in which they are listed is their order of priority. You can drag and drop servers to change the level of priority.

7) Click on **Enable LDAP Authentication** and then Apply LDAP Settings to activate external user authentication.

   Entuity applies these changes to the security service. This requires Apache Tomcat to stop and restart the service. You and any other users will have to re-login to Entuity.



Account Management

Servers: century.entuity.local

Users

| Name | Status | Groups |
|---|---|---|
| EmmaBrown | Ok | All Users, Beijing |
| JamesSmith | Ok | All Users, London |
| JuanGarcia | Ok | Administrators, All Users, New York |
| KofiYeboah | Ok | All Users, New York |
| MariaPerez | Ok | All Users, London |
| MeiChen | Ok | All Users, Beijing |

Groups

| Name | Users |
|---|---|
| Administrators | JuanGarcia, admin |
| All Users | MariaPerez, JuanGarcia, Jame |
| Beijing | EmmaBrown, MeiChen |
| Lagos | NanaToure, RiLee |
| London | MariaPerez, JamesSmith |
| New York | JuanGarcia, KofiYeboah |

Apply Settings

Restarting the Entuity server in progress...
Please close this page and login again when the Entuity server is online.

LDAP Settings

☑ Enable LDAP Authentication

| LDAP Servers | Host/IP Address |
|---|---|
| authenticate | 10.44.3.52 |

☑ Enable Emergency User □ Multiple Repositories Mode

Figure 253 Security Server Restart

# Managing the Security Database

Entuity user security details are held in its security database. When you are using:

- Internal authentication, you can explicitly create user accounts and user groups through Account Manager.
- External authentication, the security service dynamically creates user accounts from mapping rules. These rules match external user accounts with Entuity permissions. You cannot administer these external user accounts from Entuity.

## Manage Emergency Access Users

An Entuity emergency user profile allows you to login to an Entuity server that is configured for external LDAP authentication. When enabled the emergency user account is always available but would usually be used when Entuity cannot communicate with an LDAP server.

You can disable emergency user access through *entuity_home*`\etc\security.cfg.xml`. (See *Disabling Emergency User Access*.)

You cannot use an emergency user login when Entuity is configured to use internal authentication.

You can create and amend an emergency user login with `authtool` using the `passwd` function. The process is the same for both creating and amending an emergency user profile, you must supply valid Entuity administrator credentials before you can set the emergency user profile.

When connecting to Entuity as an emergency user, you are assigned to the Administrators group however the Change Password function is not accessible.

### Managing Emergency Users

To create or amend an emergency user:

1) From *entuity_home*`\bin` on the command line enter:

   ```
   ./authtool passwd
   ```

2) Enter the name of a local administrator user:

   ```
   admin
   ```

3) Enter the local administrator's password:

   ```
   admin
   ```

4) Enter the name of the emergency user:

   ```
   eUser
   ```

5) Enter the emergency user's password:

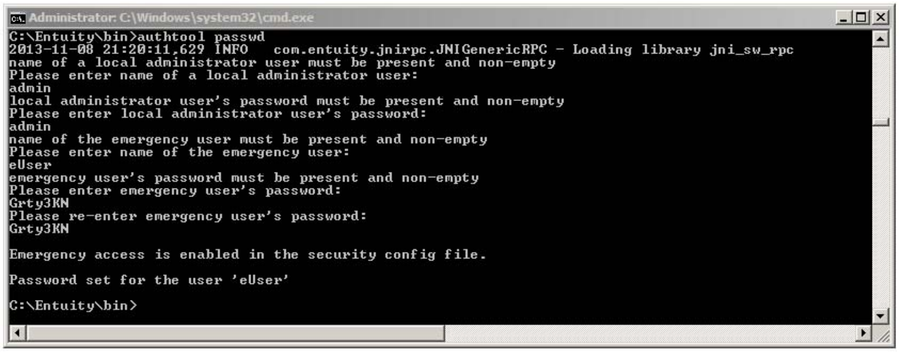
   ```
   Grty3KN
   ```

6) Re-enter the emergency user's password:

   ```
   Grty3KN
   ```

   Entuity confirms the creation, or amendment, of the emergency user profile:

   ```
   Emergency access is enabled in the security config file.
   Password set for the user 'eUser'
   ```



```
C:\Entuity\bin>authtool passwd
2013-11-08 21:20:11,629 INFO   com.entuity.jnirpc.JNIGenericRPC - Loading library jni_sw_rpc
name of a local administrator user must be present and non-empty
Please enter name of a local administrator user:
admin
local administrator user's password must be present and non-empty
Please enter local administrator user's password:
admin
name of the emergency user must be present and non-empty
Please enter name of the emergency user:
eUser
emergency user's password must be present and non-empty
Please enter emergency user's password:
Grty3KN
Please re-enter emergency user's password:
Grty3KN

Emergency access is enabled in the security config file.

Password set for the user 'eUser'

C:\Entuity\bin>
```

Figure 254 Creating an Emergency User

### Identifying Emergency Access Users

You can use the authtool list function to list the configured emergency access in the security database.

To list emergency users:

1) From *entuity_home*`\bin` on the command line enter:

```
./authtool list
```

Entuity displays the state of emergency access and the configured emergency access user profiles:

```
Emergency access is enabled in the security config file.
Users:
  eUser
  root
Total User(s) 2
```

### Deleting Emergency Users

The `authtool delete` user function allows you to delete emergency users from the security database.

To delete an emergency user:

1) From *entuity_home*`\bin` on the command line enter:

```
./authtool delete
```

2) Enter the name of the emergency user:

```
eUser
```

3) Entuity prompts you to confirm the deletion of the emergency user. Enter **Yes**.

Entuity confirms the deletion of the profile:

```
User 'eUser' deleted
```

### Disabling Emergency User Access

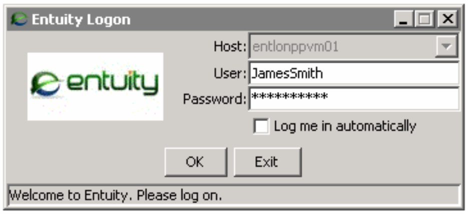
You can disable or enable emergency user access. By default this access is enabled, and Entuity recommends it remains enabled.

If you disable emergency user access you may not be able to log on to Entuity when it is configured to work with LDAP but the external authentication system is not accessible.

To disable emergency user access, in *entuity_home*`\etc\security.cfg.xml` set the value of *allowSuperUserAccess* attribute under module named `Authentication` to **false**. To enable this access, set the value to **true**.

## Log on to Entuity using Authentication

When using an external authentication server Entuity requires that the first time the user attempts to login they complete the login dialog. The user by selecting *Log on automatically* can set Entuity to automatically login.



Host: entlonppvm01
User: JamesSmith
Password: **********
□ Log me in automatically
Welcome to Entuity. Please log on.

Figure 255 Entuity Automatic Login Option

## Troubleshooting Entuity Authentication

### LDAP Authentication is Unavailable

When Entuity uses an external authentication server, access to Entuity is limited if the authentication server is unavailable. Entuity includes a special emergency access user account which does not require external authentication and can be used when the authentication server fails. This account is maintained through `authtool`. (See *Manage Emergency Access Users*.)

## authtool and Testing the Configuration

authtool is intended to assist you in the:

- Testing of external user authentication configurations.
- Testing of Server Access Configuration. (See *Testing Server Access Configuration*.)
- Management of the Entuity emergency user accounts. (See *Manage Emergency Access Users*.)

authtool is located in *entuity_home*/bin. The general syntax for this tool is:

```
authtool [-d] actionName <arguments>
```

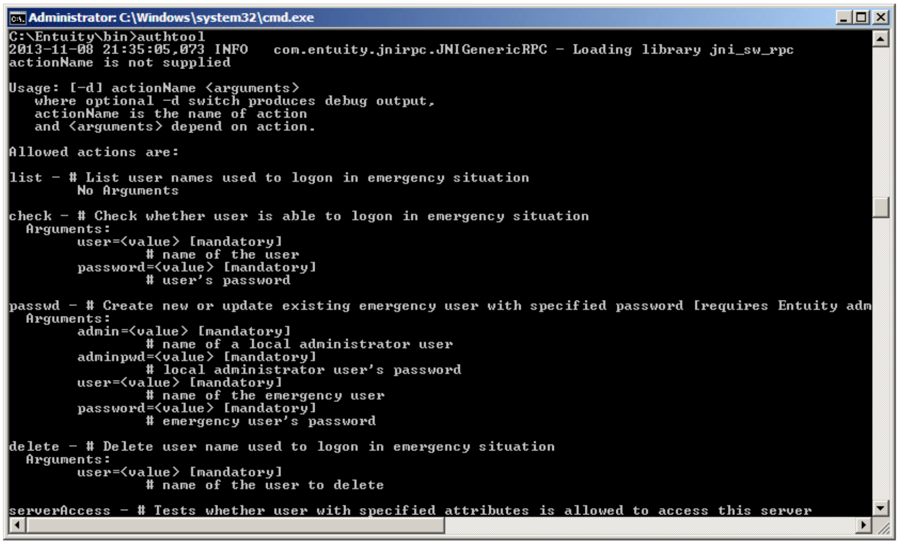
where:

- *-d* is optional and specifies verbose output.
- *actionName* is the name of action to perform.
- *arguments* specify input to that action and are specific for that action. In many cases if arguments to the action are not supplied, authtool prompts for their entry.

To get authtool help:

1) From the command line navigate to *entuity_home*`\bin` and enter `authtool`.

   `authtool` displays a full list of available actions and their arguments. `authtool` actions and arguments are also detailed in the *Entuity Reference Manual*.



Administrator: C:\Windows\system32\cmd.exe

```
C:\Entuity\bin>authtool
2013-11-08 21:35:05,073 INFO   com.entuity.jnirpc.JNIGenericRPC - Loading library jni_sw_rpc
actionName is not supplied

Usage: [-d] actionName <arguments>
   where optional -d switch produces debug output,
   actionName is the name of action
   and <arguments> depend on action.

Allowed actions are:

list - # List user names used to logon in emergency situation
        No Arguments

check - # Check whether user is able to logon in emergency situation
  Arguments:
        user=<value> [mandatory]
                # name of the user
        password=<value> [mandatory]
                # user's password

passwd - # Create new or update existing emergency user with specified password [requires Entuity adm
  Arguments:
        admin=<value> [mandatory]
                # name of a local administrator user
        adminpwd=<value> [mandatory]
                # local administrator user's password
        user=<value> [mandatory]
                # name of the emergency user
        password=<value> [mandatory]
                # emergency user's password

delete - # Delete user name used to logon in emergency situation
  Arguments:
        user=<value> [mandatory]
                # name of the user to delete

serverAccess - # Tests whether user with specified attributes is allowed to access this server
```

Figure 256 Calling authtool Help in Linux

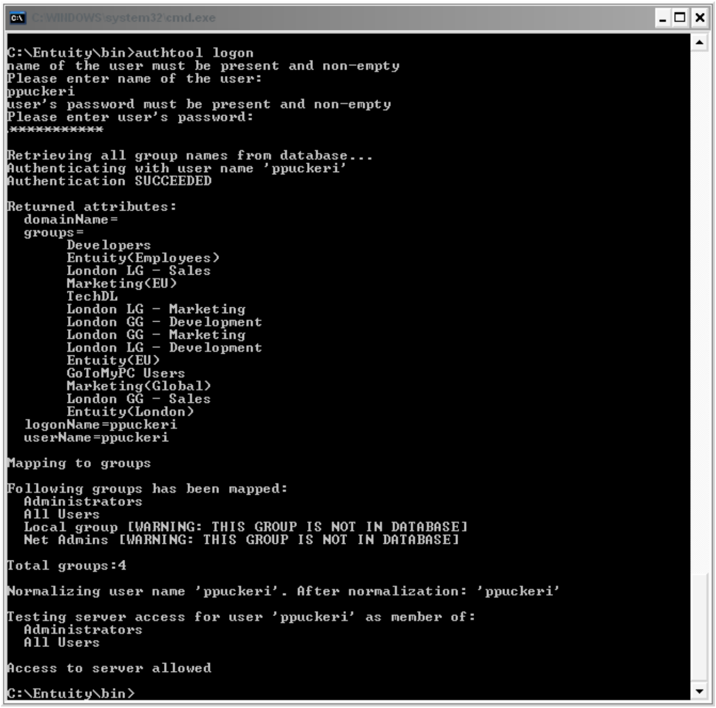
## Testing External Authentication User Logon

Once you have configured external authentication, or are in the process of doing so, you may test the user logon configuration, with *entuity_home*`\bin\authtool`:

```
authtool logon [user=username] [password=password]
```

`authtool` reports on the success or failure of the logon and when successful also reports on:

- Attributes returned from LDAP, for example domain group, groups, logon details.
- Entuity groups mapped to the logon, identifying any that are not in the database but are still included in the mapping rules.
- Testing of server access using the Entuity groups.



```
C:\Entuity\bin>authtool logon
name of the user must be present and non-empty
Please enter name of the user:
ppuckeri
user's password must be present and non-empty
Please enter user's password:
***********

Retrieving all group names from database...
Authenticating with user name 'ppuckeri'
Authentication SUCCEEDED

Returned attributes:
  domainName=
  groups=
       Developers
       Entuity(Employees)
       London LG - Sales
       Marketing(EU)
       TechDL
       London LG - Marketing
       London GG - Development
       London GG - Marketing
       London LG - Development
       Entuity(EU)
       GoToMyPC Users
       Marketing(Global)
       London GG - Sales
       Entuity(London)
  logonName=ppuckeri
  userName=ppuckeri

Mapping to groups

Following groups has been mapped:
  Administrators
  All Users
  Local group [WARNING: THIS GROUP IS NOT IN DATABASE]
  Net Admins [WARNING: THIS GROUP IS NOT IN DATABASE]

Total groups:4

Normalizing user name 'ppuckeri'. After normalization: 'ppuckeri'

Testing server access for user 'ppuckeri' as member of:
  Administrators
  All Users

Access to server allowed

C:\Entuity\bin>
```

Figure 257 authtool Logon Results

## Checking Mapping Groups

To test the mapping of a particular account you do not need to log on to the LDAP server. You can provide authtool with the list of arguments that you would expect LDAP server to return. These attributes are used as input to the mapping engine and authtool displays the mapping result.

You invoke mapping action as follows:

```
authtool mapping attributeName=attributeValue attributeName=
attributeValue
```

For example to invoke `authtool`:

```
authtool mapping userName=cwilliams groups="Network Admin"
```

You can also run authtool mapping just against the a group:

```
C:\Entuity\bin>authtool -d mapping groups=developers

Retrieving all group names from database...

15:48:21,686 DEBUG Configurator:? - Found properties file on the
classpath:app.config.properties
```

```
15:48:21,686 DEBUG Configurator:? - Testing for file existance:C:/
Entuity/etc/security.config.xml
15:48:21,686 DEBUG Configurator:? - Using configuration file:file:/C:/
Entuity/etc/security.config.xml
15:48:21,764 DEBUG Configurator:? - Found module:Authentication
15:48:21,764 DEBUG Configurator:? - Found module:CentralDB
15:48:21,764 DEBUG Configurator:? - Found module:LocalDB
15:48:21,764 DEBUG Configurator:? - Found module:ExternalAttributes-
Mapping
15:48:21,764 DEBUG Configurator:? - Found module:ldap-config
15:48:21,764 DEBUG Configurator:? - Found module:ldap-config-domain
15:48:21,764 DEBUG Configurator:? - Found module:ldap-config-sun
15:48:21,764 DEBUG Configurator:? - Found module:ldap-config-template
15:48:21,764 DEBUG Configurator:? - Found module:ServerAccess
15:48:21,764 DEBUG Configurator:? - Found module:AuthenticationService
15:48:21,764 DEBUG Configurator:? - Found module:PreferenceService
15:48:21,764 DEBUG Configurator:? - Found module:UserManagementService
15:48:21,764 DEBUG Configurator:? - Found module:TicketGrantingService
15:48:21,764 DEBUG Configurator:? - Found module:TGSConfig
Mapping with following attributes:
  groups=developers
15:48:24,748 DEBUG PrincipalAttributeMapper:? - Mapping rule
applied:Grant [AllUsers]
15:48:24,748 DEBUG PrincipalAttributeMapper:? - Mapping rule
applied:Admin groups

Following groups has been mapped:
  Administrators
  All Users
  Net Admins [WARNING: THIS GROUP IS NOT IN DATABASE]

Total groups:3
```

# 40 Advanced LDAP Authentication

You can control access to Entuity either internally through its own security database or externally by integrating Entuity user groups and names within the LDAP environment.

## Configuring User Access to Entuity Server(s)

Within multiple Entuity server installations you may want to configure access permissions at the Entuity server level, rather than the authentication service level. For example, you may want a user to have full access to one Entuity server but a more restricted access to another.

Through the ServerAccess module in `security.cfg.xml` you can set rules to specify user and group access. By having different ServerAccess module definitions on different servers you can define different user and group permissions. There are four rule types which are evaluated against submitted attributes:

- allowUser, allows user access to the server by comparing to the rule value the user's username, domain values or both.
- denyUser, denies user access to the server by comparing to the rule value the user's username, domain values or both.
- allowGroup, allows user access to the server by comparing to the rule value the user's group membership.
- denyGroup, denies user access to the server by comparing to the rule value the user's group membership.

The allowUser and denyUser rules have the structure:

```
<ruleName name="*" domain="*"/>
```

where:

- *ruleName* can be **allowUser** or **denyUser**
- *name* is the user name:
  - * indicates all users, and is the default value.
  - user name is the user name.
- *domain* is only applicable with external authentication. It is the domain associated with the network user account:
  - * indicates all domains, and is the default value.
  - domain name is the user's network domain name.

When both parameter name and domain are specified in the allowUser and denyUser rules, then the rule is only matched when both parameter values are matched (logical AND).

The allowGroup and denyGroup rules have the structure:

```
<ruleName name="*"/>
```

where:

- *ruleName* can be **allowGroup** and **denyGroup**
- *name* is the Entuity user group name:
    - * indicates the rule applies to all groups, and is the default value.
    - name is the group name.

Rule evaluation can be either case sensitive or case insensitive, which is specified through the *ignorecase* attribute of the *serverAccess* element:

```
<serverAccess ignorecase="true">
```

## Example Server Access Configuration

This example allows access only to users who are members of the Administrators group, apart from the user CharlesC:

```
<module name="ServerAccess">
  <serverAccess ignorecase="true">
    <denyUser name="*" domain="*"/>
    <allowGroup name="Administrators"/>
    <denyUser name="CharlesC"/>
  </serverAccess>
</module>
```

in detail, and in order:

- *ignoreCase* is set to true, so evaluations are case insensitive.
- *denyUser* denies access to all users in all domains. When setting a filter you must restrict access, filtering all users out before filtering the required users in.
- *allowGroup* overrides the preceding denyUser rule, allowing access to all members of the Administrators group.
- *denyUser* denies access to the user CharlesC (implicitly a member of the administrators group, otherwise the user would not need explicitly excluding).

## Testing Server Access Configuration

You can test server access configuration rules using `authtool`, which has the structure:

```
authtool serverAccess [user=username] [groups=list_of_groups]
```

where:

- `authtool` is the authentication tool which you can run from the command line to test your security configuration.
- *serverAccess* identifies the security module you are testing.
- *user* is the Entuity user.
- *groups* is one or more user groups against which the rules are applied. A list of groups would be enclosed in quotation and comma delimited.

This example tests whether CharlesC a member of the administrators group would be permitted access to the Entuity server:

```
authtool -d serverAccess user=CharlesC groups=Administrators
```

Another example is to test user access using user and domain names:

```
authtool serverAccess user=myUser@myDomain
```

## Advanced LDAP Authentication

When configuring Entuity for use with LDAP consider whether you want users to log on entering:

- Only the username.
- Both the user and domain names.

Entuity recommend enforcing domain name usage when allowing users from different domains to log on to Entuity. Entuity LDAP:

- Supports the User Principal Name (UPN) format, i.e. username@domain.
- Does not support the Universal Naming Convention (UNC) format, i.e. \\domain\username and domain\username .

From the user logon information you must be able to construct the distinguished name (DN) of the user LDAP entry on the LDAP server.

The bind name is constructed from information supplied when attempting to log on. How the bind name is constructed, and in what format, you can specify through the ldap-config module in `security.cfg.xml` in *entuity_home*/`etc`:

```
<userBindName>expression</userBindName>
<userBindNameIsDN>boolean</userBindNameIsDN>
```

where:

- *expression* constructs the bind name. This can include fixed values as well as values supplied during the log on. There are three possible variables, represented as {0}, {1} and {2}. These variables are replaced with values taken from the logon:
  - {0}, is the entered logon name, which could include both username and domain
  - {1}, is the username part of the logon
  - {2} replaced with domain part of the logon (may be empty).
- *boolean* indicates whether the constructed bind name includes a domain name (**true**), or not (**false**).

When constructed the bind name is used to authenticate (bind) against the LDAP server (together with the entered password). If the bind operation succeeds, then the user is authenticated and the login accepted, otherwise the login attempt is rejected and fails.

## Examples of LDAP Binding

Here the bind name is specified using the distinguished name (DN) format:

```
<userBindName>uid={1}, ou=People, dc=example, dc=com</userBindName>
<userBindNameIsDN>true</userBindNameIsDN>
```

Here the bind name is specified using the UPN format. The user only enters their user name, as it is combined with a predefined domain (MyCompanyDomain):

```
<userBindName>{1}@MyCompanyDomain</userBindName>
<userBindNameIsDN>false</userBindNameIsDN>
```

Here the bind name is specified using the UPN format but with the user required to enter user and domain names:

```
<userBindName>{1}@{2}</userBindName>
<userBindNameIsDN>false</userBindNameIsDN>
```

## Example of Alternative DN Construction

If your LDAP server only supports the bind operation using the DN format, and you can not construct a valid user DN using Entuity's expression formats, Entuity can be configured to use an alternative approach.

You can use an alternative method to authenticate the user:

1) The connection to the LDAP server is made with the system user name and password specified in the configuration file (this user must have enough privileges to search the directory in the specified location).
2) A search for the user entry is made on the basis of the supplied criteria.
3) If the user entry is:
   - Located, the DN of that entry is used to bind against LDAP.
   - Not found, or the bind operation fails then the log on fails.

You configure these options in the ldap-config module in `security.cfg.xml`:

```
<lookupUserBindDNAsSystemUser>true</lookupUserBindDNAsSystemUser>
            <userSearchBaseCtxDN>
            dc=example, dc=com
            </userSearchBaseCtxDN>
            <userMatchFilter>
                   (userPrincipalName={1}@{2})
            </userMatchFilter>
            <systemUserName>
                 cn=userwithsearchpriveleges, dc=example, dc=com
            </systemUserName>
```

```
<systemUserPwd>password</systemUserPwd>
```

where:

- *LookupUserBindDNAsSystemUser* when set to:
  - **true**, sets the requirement to find the user's DN before trying to bind as that user.
  - **false**, assumes you can construct a valid DN from the logon details.
- *userSearchBaseCtxDN* defines the search directory sub-tree.
- *userMatchFilter* is the criteria on which the user is identified.
- *systemUserName* is the used connect details, user name and password.

This example equates to:

1) A connection using username="cn=userwithsearchprivilieges, dc=example, dc=com" and password = "password"
2) A directory path of dc=example, dc=co
3) A search of the sub-tree for the entry whose attribute *userPrincipalName* equals username@domain
4) When the search finds:
   - A single entry, the bind operation uses the DN of that entry.
   - No matching entry the log on attempt fails.
   - Multiple entries, the log on attempt fails and logs indicate an incorrect configuration.

## Configure LDAP Group Search

When a successful user authentication (bind) operation completes, the next stage is identifying that user's groups on the LDAP server. Identification requires the user's DN, so where user authentication was through UPN it must be derived.

This example section derives user DN:

```
<userBindName>{1}@{2}</userBindName>
<userBindNameIsDN>false</userBindNameIsDN>
<lookupUserBindDNAsSystemUser>false</lookupUserBindDNAsSystemUser>
<userSearchBaseCtxDN>
            dc=example, dc=com
</userSearchBaseCtxDN>
<userMatchFilter>
            (userPrincipalName={1}@{2})
</userMatchFilter>
```

where:

- *userBindNameIsDN* is false, indicating the bind name is in UPN format.

- *lookupUserBindDNAsSystemUser* is:
  - **false**, indicating the DN search is for the current user who has sufficient privileges to search the specified folder sub-tree.
  - **true**, indicating the search should use the privileges of the system user.

- *userPrincipalName* the UPN format name on which the DN lookup is performed.

After the LDAP server finds the user’s DN, it then searches for the user’s groups. The search requires access to the relevant folders on the LDAP server. When the authenticated user does not have access you can specify whether group search must be done with system user:

```
<searchGroupsAsSystemUser>true</searchGroupsAsSystemUser>
```

Set *searchGroupsAsSystemUser* to:

- **false** when the authenticated user has the access rights to search the LDAP server for their groups.
- **true** when the authenticated user in your LDAP server does not have enough permissions to search for the groups. You must then provide system user name and password, using *systemUserName* and *systemUserPwd*.

This configuration indicates the user entry in the LDAP server contains attributes that list all distinguished names of the groups to which the user belongs, and all of these group entries contain an attribute to indicate to which group they belong (groups could be members of groups):

```
<userRefersToGroup>true</userRefersToGroup>
<userMemberOfAttrID>memberOf</userMemberOfAttrID>
<groupNameAttrID>cn</groupNameAttrID>
```

where:

- *userRefersToGroup* is:
  - **true**, indicating the user has an attribute which refer to groups this entry is member of.
  - **false**, indicating the user entry does not contain a reference to the member’s group.
- *userMemberOfAttrID* is the attribute that identifies member groups.
- *groupNameAttrID* is the name on the group attribute which identifies the group name, e.g. **cn**.

All groups specified are navigated recursively, returning all group names to which the user belongs. Where the user entry does not contain a reference to the groups it is a member of, you must use take another approach. The LDAP server can recursively search for groups that refer to the user as a member, as well as groups that refer to other user groups.

This configuration indicates the user entry on the LDAP server does not have any information on group membership, but instead group entry refers to member users or groups (or group members of groups):

```
<userRefersToGroup>false</userRefersToGroup>
```

```
<groupSearchBaseCtxDN>
            DC=example, DC=com
</groupSearchBaseCtxDN>
<groupMatchFilter>(member={3})</groupMatchFilter>
<groupSearchDepth>5</groupSearchDepth>
<groupNameAttrID>cn</groupNameAttrID>
```

where:

- *userRefersToGroup* is:
  - **true**, indicating the user has an attribute which refer to groups this entry is member of.
  - **false**, indicating the user entry does not contain a reference to the member's group.
- *groupSearchBaseCtxDN* specifies the directory path of the sub-tree where group entries could be located.
- *groupMatchFilter* specifies the matching criteria for a group to be considered as group for the user or group. The match can use variables, including {3} which is replaced by the distinguished name of the user or the group, for whom we are searching the group.
- *groupSearchDepth* sets the group recursion depth. Only increase this value when your LDAP schema has more levels of memberships.
- *groupNameAttrID* is the name on the group attribute which identifies the group name, e.g. **cn**.

## Map LDAP Groups to Entuity User Groups

When the user has been authenticated and their groups retrieved from the LDAP server, this information (attributes) must be mapped to Entuity user groups. These groups determine user permissions within Entuity. Through the *ExternalAttributesMapping* module you must define rules that map LDAP retrieved user groups to Entuity groups.

There are two types of rules: revoke and grant. Each rule may have a list of groups to which membership is granted or revoked. You can apply the rule unconditionally, or specify conditions so the rule only applies to groups that meet the set criteria.

The rules are applied in the order specified in the configuration. Rules can also be impacted by the case sensitivity of evaluated data, in environments where casing is not important use the ignorecase attribute. ignorecase applies to the user logon details as well as the retrieved attribute details.

After LDAP authentication, mapping rules can be built using these attributes:

- *logonName*, the user logon details, which includes the username and where entered the domain name.
- *userName*, the user logon name only.
- *domainName*, the domain name only, if entered when the user logged on.
- *groups*, names of the groups on the external authentication system.

revoke and grant rules have the same structure, this extract shows grant:

```
<grant name="ruleName">
            <group name="MyEntuityGroup1"/>
            <group name="MyEntuityGroup2"/>
                   <condition>
                   ...
                   </condition>
</grant>
```

where:

- **grant** is the rule type, the other rule type is **revoke**. *name* is the name of the rule, its use is optional but Entuity recommend its use to improve the readability of your configuration.
- *group* is the name of the Entuity group affected by the rule.
- *condition* specifies the tests against which the received data is evaluated. It returns either **true** or **false**.

## Set Rule Conditions

**grant** and **revoke** rules are used to map an authenticated user's LDAP groups to Entuity groups, and therefore assign them Entuity permissions. Within grant and revoke rules you can specify conditions that are tested against the LDAP groups, and only when the condition is true are the Entuity groups specified in the rule associated to the user.

Rule conditions contain attribute values that are used as test expressions These expressions can be combined using standard Boolean logic operators, AND, OR, NOT.

An attribute test expression has the structure:

```
<attr name="attrName" contains="attrValue"/>
```

where:

- *attr* indicates this is an attribute clause.
- *name* is the attribute name.
- *contains* is the test attribute value. When the named attribute contains this value the expression is considered true.

By combining these expressions with boolean operators you can increase the sophistication of the condition:

```
<grant name="Local users groups">
            <group name="administrators" />
                   <condition>
                   <or>
                   <attr name="userName" contains="rootAdmin"/>
                   <attr name="userName" contains="sysAdmin"/>
```

```
                    <attr name="userName" contains="seniorAdmin"/>
                    <and>
                    <attr name="groups" contains="seniorAnalysts" />
                    <attr name="groups" contains="seniorNetAdmins" />
                    <attr name="groups" contains="seniorNetSupport" />
                    </and>
                    </or>
             </condition>
  </grant>
```

This example is a grant rule which when true maps to the user the Entuity administrators group. The condition tests whether the user is:

- The rootAdmin user.
- The sysAdmin user.
- The seniorAdmin user.
- A member of all of the listed groups, seniorAnalysts, seniorNetAdmins and seniorNetSupport groups.

When one of these tests is:

- **true**, the condition is set to true and the user is associated to the Entuity administrators group.
- **false**, the user is not associated to the Entuity administrators group.

## Configuring LDAP Server Location and Security

The LDAP server location is configured through `security.config.xml` in ldap-config module. You can specify the protocol used when connecting to the LDAP server, facilitating a normal or secure (SSL) connection.

This has the format:

```
<property name="java.naming.provider.url" value="ldap://host:port" />
```

where:

- *property name* identifies the location as a Java URL. This should not be amended.
- *value* is the LDAP server URL which can include the server's port, for example:

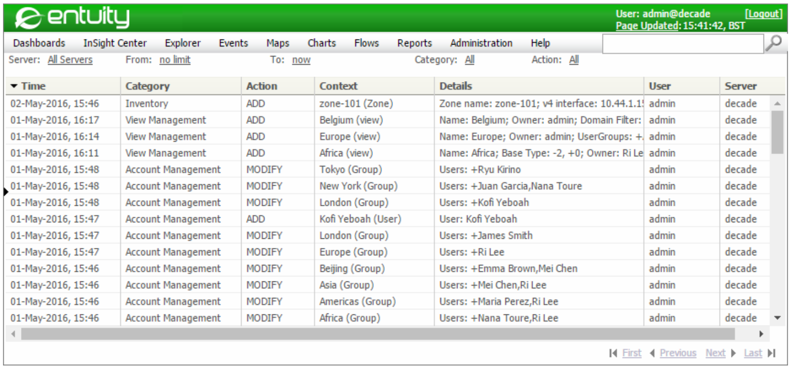
  ```
  ldaps://myhost
  ldap://myhost:12345
  ```

# 41 Audit Log

Entuity generates an extensive set of log files which are by default saved to *entuity_home*\log. You can access these log files and review them, although their number, the number of log entries within them and the depth of the technical content make it an unrealistic task unless you are troubleshooting a particular issue.

Audit Log provides a central point for reviewing and analyzing actions performed on Entuity. You can use its filters to control the display of log entries; for example you can specify a filter so Audit Log displays:

- Views created within the past week.
- New user accounts created on a particular server.
- Changes to device management.



Server: All Servers From: no limit To: now Category: All Action: All

| Time | Category | Action | Context | Details | User | Server |
|---|---|---|---|---|---|---|
| 02-May-2016, 15:46 | Inventory | ADD | zone-101 (Zone) | Zone name: zone-101; v4 interface: 10.44.1.1 | admin | decade |
| 01-May-2016, 16:17 | View Management | ADD | Belgium (view) | Name: Belgium; Owner: admin; Domain Filter: | admin | decade |
| 01-May-2016, 16:14 | View Management | ADD | Europe (view) | Name: Europe; Owner: admin; UserGroups: +. | admin | decade |
| 01-May-2016, 16:11 | View Management | ADD | Africa (view) | Name: Africa; Base Type: -2, +0; Owner: Ri Le | admin | decade |
| 01-May-2016, 15:48 | Account Management | MODIFY | Tokyo (Group) | Users: +Ryu Kirino | admin | decade |
| 01-May-2016, 15:48 | Account Management | MODIFY | New York (Group) | Users: +Juan Garcia,Nana Toure | admin | decade |
| 01-May-2016, 15:48 | Account Management | MODIFY | London (Group) | Users: +Kofi Yeboah | admin | decade |
| 01-May-2016, 15:47 | Account Management | ADD | Kofi Yeboah (User) | User: Kofi Yeboah | admin | decade |
| 01-May-2016, 15:47 | Account Management | MODIFY | London (Group) | Users: +James Smith | admin | decade |
| 01-May-2016, 15:47 | Account Management | MODIFY | Europe (Group) | Users: +Ri Lee | admin | decade |
| 01-May-2016, 15:46 | Account Management | MODIFY | Beijing (Group) | Users: +Emma Brown,Mei Chen | admin | decade |
| 01-May-2016, 15:46 | Account Management | MODIFY | Asia (Group) | Users: +Mei Chen,Ri Lee | admin | decade |
| 01-May-2016, 15:46 | Account Management | MODIFY | Americas (Group) | Users: +Maria Perez,Ri Lee | admin | decade |
| 01-May-2016, 15:46 | Account Management | MODIFY | Africa (Group) | Users: +Nana Toure,Ri Lee | admin | decade |

Figure 258 View Management Audit Log

Audit Log allows you to track who made changes and when to key Entuity features. Entuity Audit Log currently records actions performed on:

- Event Threshold Settings
- Account Management:
- Configuration Management
- Device Inventory
- Context menu port object settings: Fast util, Fast polling, Status event, manage or unmanage.
- View management
- Report scheduling.

When multi-tenanted support is configured audit log tracks the creation, deletion and modification of zones. Zone details are also included with audit log entries relating to addition/deletion of devices to the inventory.

| Category | Description |
|---|---|
| Account Management | This category includes changes to user accounts, groups and LDAP configuration. Audit Log tracks:<br>■ Creation of user accounts, deletion of user accounts, the changing of account passwords and changing of user group membership.<br>■ Creation and deletion of user groups, change in user group membership and change in associated tool permissions.<br>■ LDAP internal and external authentication enabled. |
| Configuration Management | This category includes changes to Configuration Management tasks. Audit Log tracks task modify, create task schedule, modify task schedule, delete task schedule and execute task actions. |
| Events | This category includes changes to event suppression definitions defined through Event Suppressions page (see *Event Suppression*). It identifies additions to, modifications and deletions of event suppressions. |
| Inventory | Inventory category includes changes to managed inventory, additions, deletions and modifications. Inventory logs include zone management actions. When changing inventory through the:<br>■ Inventory page *Source* is set to **Web**.<br>■ Command line *Source* is set to **proliferate**.<br>Audit log does not report on devices that Entuity fails to manage. |
| Object Settings | This category includes the enabling and disabling of port object settings initiated from the context menu:<br>■ Fast Status Polling<br>■ Fast Utilization Polling<br>■ Status Events<br>■ Manage and unmanage ports. |
| Reporting | This category logs changes to report schedules, their creation, manual deletion, suspension and resumption. |
| Threshold Settings | This category includes modifications to event thresholds, for example amending a threshold value, disabling a threshold. |
| View Management | This category logs view creation, deletion and modifications. Details include domain, event or incident filter, and group changes are also recorded. |

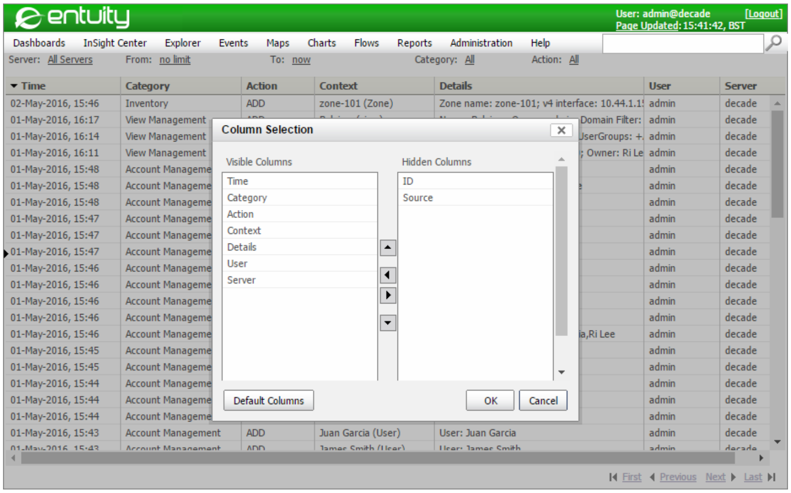
Table 69 Audit Log Categories

By default Entuity maintains audit log entries for 60 days; after 60 days Entuity deletes the entry from the audit log. You can amend this keep time for the audit log data through `entuity.cfg` and the variable `auditLogKeepTime`.

All members of the System Administrators group and users with the View Audit Log tool permission have access to Audit Log.

# Audit Log Display

You can also amend which columns to display and the order of those columns. (See *Configure Columns*.)



User: admin@decade [Logout]
Page Updated: 15:41:42, BST

Server: All Servers From: no limit To: now Category: All Action: All

| Time | Category | Action | Context | Details | User | Server |
|---|---|---|---|---|---|---|
| 02-May-2016, 15:46 | Inventory | ADD | zone-101 (Zone) | Zone name: zone-101; v4 interface: 10.44.1.1! | admin | decade |
| 01-May-2016, 16:17 | View Management | | | Domain Filter: | admin | decade |
| 01-May-2016, 16:14 | View Management | | | UserGroups: +. | admin | decade |
| 01-May-2016, 16:11 | View Management | | | ; Owner: Ri Le | admin | decade |
| 01-May-2016, 15:48 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:48 | Account Manageme | | | e | admin | decade |
| 01-May-2016, 15:48 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:47 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:47 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:47 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:46 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:46 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:46 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:46 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:46 | Account Manageme | | | ia,Ri Lee | admin | decade |
| 01-May-2016, 15:45 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:45 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:44 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:44 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:44 | Account Manageme | | | | admin | decade |
| 01-May-2016, 15:43 | Account Management | ADD | Juan Garcia (User) | User: Juan Garcia | admin | decade |
| 01-May-2016, 15:43 | Account Management | ADD | James Smith (User) | User: James Smith | admin | decade |

| Visible Columns | Hidden Columns |
|---|---|
| Time | ID |
| Category | Source |
| Action | |
| Context | |
| Details | |
| User | |
| Server | |

Figure 259 Audit Log Columns

| Column | Description |
|---|---|
| *Time* | Date and time on the Entuity server when Entuity made the audit entry. |
| *User* | This is the owner of the action. When the action is executed through:<br>■ The Web UI it is the name of the logged in Entuity user.<br>■ The command line it is set to system.<br>■ A script then the name of the user is left blank. |
| *Source* | The origin of the action. When *Source* is set to:<br>■ **Web** it indicates the action was initiated through the web interface, for example adding a device through the Inventory page.<br>■ **proliferate** it indicates the action was initiated by running `proliferate` from the command line, for example adding a device.<br>■ **DsKernelStatic** it indicates the action was performed by `DsKernelStatic`, which is usually initiated from the web interface but could also be called by RESTful API when managing views. |
| *Category* | Top level grouping of actions identify the general category to which the action is related. For example, adding a device is an Inventory action. (See *Table 69 Audit Log Categories*.) |

Table 70 Audit Log Attributes

| Column | Description |
|---|---|
| *Action* | Identifies the action type which can be one of.<br>■ **ADD**, for example creation of a new user account, taking a new device under management.<br>■ **ADD REFERENCE**, used when adding a view to another by reference.<br>■ **COPY**, used when copying a view to another view.<br>■ **DELETE**, removing a user account, deleting a report schedule.<br>■ **DELETE REFERENCE**, used when a referenced view is deleted from the view.<br>■ **MOVE**, used when moving a view to another view.<br>■ **RESUME**, resuming a suspended report schedule.<br>■ **SUSPEND**, used when suspending a report schedule. |
| *Context* | The context in which Entuity performs the action, for example if a threshold is modified then the threshold is the source context of the action. |
| *Details* | Identifies the details of the action. If the action results in changes then **-** and **+** (From and To) indicate the direction of change. For example, if a device is added to a:<br>■ View then Entuity reports the change as **+ManagedHost: saturn**<br>■ Zone then Entuity reports the change as **Zone: +zone-name**. |
| *Server* | Entuity server that performed the action. |
| *ID* | Audit entry identifier. Different rows may share the same identifier which indicates the actions were performed at the same time, for example multiple devices were selected and added into a view. |

Table 70 Audit Log Attributes

## Audit Log Filters

Through the filter options you can control what entries Audit Log displays. You can filter audit log entries by the server on which they were actioned, the user who initiated the action, the time they took place and by the category and type of action. (See *Table 71 Audit Log Filter*.) The filters only exist while you are using the Audit Log, if you navigate away from the page the filter is reset to its default state. You can also use **Clear Filter** to reset the filter.

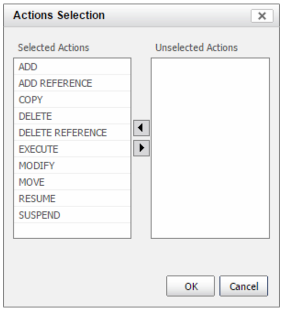


Figure 260 Audit Log Action Filter

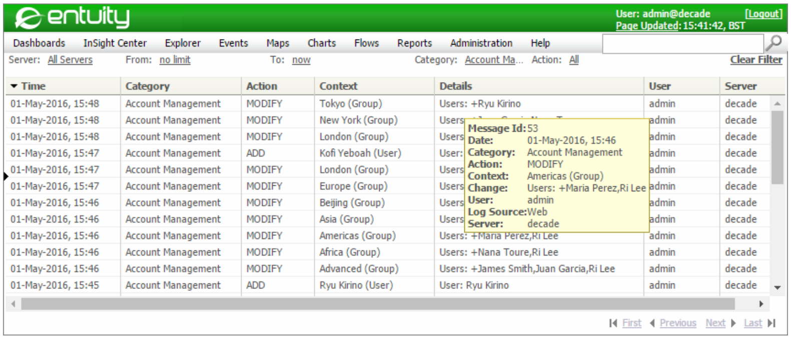
| Filter | Description |
|---|---|
| *Server* | Select:<br>■ **All** for all servers available to the current user<br>■ The specific Entuity server that performed the action. |
| *From* | Start date and time of the filter period. By default set to **no limit**, which is only restricted by the audit log retention period of 60 days (configurable through `auditLogKeepTime` in `entuity.cfg`.)<br>*From* and *To* use the same Time Period dialog. |
| *To* | End date and time of the filter period. By default set to **now**, the current data and time. The page does update |
| *Category* | Top level grouping of actions identify the general category to which the action is related. For example, adding a device is an Inventory action. (See *Table 69 Audit Log Categories*.) |
| *Action* | Identifies the action type which can be one of.<br>■ **ADD**, for example creation of a new user account, taking a new device under management.<br>■ **ADD REFERENCE**, used when adding a view to another by reference.<br>■ **COPY**, used when copying a view to another view.<br>■ **DELETE**, removing a user account, deleting a report schedule.<br>■ **DELETE REFERENCE**, used when a referenced view is deleted from the view.<br>■ **EXECUTE**, used when running a script.<br>■ **MODIFY**, used when modifying a view.<br>■ **MOVE**, used when moving a view to another view.<br>■ **RESUME**, resuming a suspended report schedule.<br>■ **SUSPEND**, used when suspending a report schedule. |
| *User* | This is the owner of the action. When the action is executed through, for example:<br>■ The Web UI it is the name of the logged in Entuity user.<br>■ The command line it is set to system.<br>■ A script then the name of the user is left blank. |

Table 71 Audit Log Filter

## Audit Log Examples

This section includes examples that illustrate Entuity Audit Log:

- Setting Event Thresholds
- Logging of Menu Driven Actions
- Log Unmanaging Ports



Server: All Servers From: no limit To: now Category: Account Ma... Action: All

| Time | Category | Action | Context | Details | User | Server |
|---|---|---|---|---|---|---|
| 01-May-2016, 15:48 | Account Management | MODIFY | Tokyo (Group) | Users: +Ryu Kirino | admin | decade |
| 01-May-2016, 15:48 | Account Management | MODIFY | New York (Group) | Users | admin | decade |
| 01-May-2016, 15:48 | Account Management | MODIFY | London (Group) | Users | admin | decade |
| 01-May-2016, 15:47 | Account Management | ADD | Kofi Yeboah (User) | User: | admin | decade |
| 01-May-2016, 15:47 | Account Management | MODIFY | London (Group) | Users | admin | decade |
| 01-May-2016, 15:47 | Account Management | MODIFY | Europe (Group) | Users | admin | decade |
| 01-May-2016, 15:46 | Account Management | MODIFY | Beijing (Group) | Users | admin | decade |
| 01-May-2016, 15:46 | Account Management | MODIFY | Asia (Group) | Users | admin | decade |
| 01-May-2016, 15:46 | Account Management | MODIFY | Americas (Group) | Users: +Maria Perez,Ri Lee | admin | decade |
| 01-May-2016, 15:46 | Account Management | MODIFY | Africa (Group) | Users: +Nana Toure,Ri Lee | admin | decade |
| 01-May-2016, 15:46 | Account Management | MODIFY | Advanced (Group) | Users: +James Smith,Juan Garcia,Ri Lee | admin | decade |
| 01-May-2016, 15:45 | Account Management | ADD | Ryu Kirino (User) | User: Ryu Kirino | admin | decade |

Message Id: 53
Date: 01-May-2016, 15:46
Category: Account Management
Action: MODIFY
Context: Americas (Group)
Change: Users: +Maria Perez,Ri Lee
User: admin
Log Source: Web
Server: decade

Figure 261 Account Management Audit Log

## Setting Event Thresholds

Entuity tracks changes in threshold settings, both changes in the status of a threshold and in its value. This example shows audit log entries for the activation of the High Mac Address Count threshold which is used with the Mac Address High Port Count event on the bsw1 device:

```
Message Id:13
Date: 27-Mar-2014, 20:54
Category: Threshold Settings
Action: MODIFY
Context: bsw1 (SwitchDevice)
Details: HighMacAddressCountThreshold Value: from 3 to 6; Enabled
User: admin
Log Source: DsKernelStatic
Server: entlonvpc01
```

## Logging of Menu Driven Actions

Audit Log can track menu driven actions on ports, for example toggling Fast Utilization Polling and Status Events. This log records the setting of Fast Status Polling for port Ethernet 8 on 10.66.33.10:

```
Message Id:12
Date: 27-Mar-2014, 20:27
Category: Object Settings
Action: MODIFY
Context: [ch1] Ethernet Interface on bsw1 (portEx)
Details: Fast Status polling: Enabled
User: admin
Log Source: DsKernelStatic
```

```
Server: entlonvpc01
```

## Log Unmanaging Ports

Entuity Audit Log tracks the management and unmanagement of ports. Entuity Audit Log distinguishes between ports unmanaged from the command line using RESTful API and those unmanaged through the web UI.

This example unmanages the **Fa0/1** ethernet interface on **10.44.1.9** using RESTful API. With RESTful API there are different methods for identifying an interface. For example you could use the interface's internal StormWorks identifier (which you can find through the port's Advanced page) or the interface description:

```
curl -u admin:admin http://entlonppvm01/api/portManagement/2/
18?unManage=y&media=json -X PUT -H "Content-Type: application/json" -d
```

To repeat the actions to generate the example audit log:

1) From the command line, navigate to *entuity_home*`\lib\tools` and enter:

```
curl -u admin:admin http://entlonppvm01/api/portManagement/2/
18?unManage=y&media=json -X PUT -H "Content-Type: application/json" -d
```

2) Click **Administration** > **Audit Log**. Entuity reports the unmanaging of the port:

```
Message Id:8
Date: 27-Mar-2016, 17:35
Category: Object Settings
Action: MODIFY
Context: [e1] Ethernet Interface on bsw1 (portEx)
Details: Port unmanage
User: system
Log Source: RESTful
Server: entlonvpc01
```

3) If you were to unmanage the same port through the web UI Entuity Audit Log identifies the web UI source.

   In Explorer highlight the port and from the context menu click **Unmanage port**.

4) Click **Administration** > **Audit Log**. Entuity reports the unmanaging of the port:

```
Message Id:17
Date: 27-Mar-2016, 21:15
Category: Object Settings
Action: MODIFY
Context: [e1] Ethernet Interface on bsw1 (portEx)
Details: Port unmanage
```

```
User: admin
Log Source: web
Server: entlonvpc01
```

If you compare the two log entries you can see Entuity distinguishes between the two methods of unmanaging ports through *Source* and *User*.

# 42 Manage Entuity and Its Database

Before running Entuity for the first time, re-installing Entuity, applying patches or re-configuring Entuity you are strongly advised to make a system backup of the installed software and data. If you then encounter a problem, for example a file system corruption, inadvertently deleting data when upgrading Entuity or misapplying a patch, you can quickly revert to the backed up implementation.

Entuity's default configuration includes a database backup that runs each evening. You should also configure your system backup tools to run nightly, backing up those folders that contain content that changes frequently, e.g. the database backup tables, configuration folders, reports folders.

! Do not run anti-virus or backup tools on the live database folder, e.g. *entuity_home*`\database`, as this type of software may lock files and cause Entuity to fail to access the database.

## Running a Full Backup and Restore of the Entuity Server

A comprehensive backup process ensures that you can quickly restore Entuity in the event of a catastrophic event, for example a file system corruption or inadvertently deleting data when upgrading Entuity. You are strongly advised to make a system backup of the installed software and data before:

- Running Entuity for the first time.
- Applying a maintenance patch.
- Upgrading Entuity to a new release.

A full installation backup is essential when applying maintenance patches or upgrading to a new Entuity release as they may include changes to the database structure which would invalidate a database only restore.

To perform a full system backup you should:

- Ensure the Entuity server is not running.
- Backup everything included within *entuity_home*.
- Check that the Entuity database is backed up. During `configure` you may have installed the database directory somewhere other than *entuity_home*/`database/data/`.
- When using Configuration Monitor backup the configuration and archive configuration file folders.

### Performing a Full System Restore

You would only have to run a full system restore:

- If you have a major incident that corrupts your Entuity database and/or software, for example the Entuity server machine has become unstable and cannot be recovered.
- To move the Entuity install to a new machine.

When using a Central License Server, you should deallocate license credits before moving a remote server. If you do not deallocate credits you would have to wait seven days until the credit allocation ages out and are available for reallocation.

To restore the Entuity server:

1) Remove any existing Entuity installation.
2) Install the last full system backup.
3) Install the last nightly backup, for example databases, configuration changes.
4) When installing to a different folder location, amend the destination configuration in `entuity.cfg`.
5) Run `configure`.
6) Perform a full system backup. You should take care not to overwrite your previous full system backup.
7) Start Entuity.

# Running a Nightly Backup

You can run a nightly backup of selected Entuity folders when Entuity is running. You should also configure your system backup tools to run nightly, backing up those folders that contain content that changes frequently, e.g. the database backup tables, configuration folders, reports folders.

These are the main components to be considered when configuring your nightly backup:

- Configuration files located in *entuity_home*`/etc`.
- Reports located in *entuity_home*`/lib/httpd/EOS/reporting`
- MIBs located in *entuity_home*/`lib/mibs`
- tftp server, the location of which is specified during `configure.`
- Database located in *entuity_home*`/database/backup/` (see *Database Management Overview*).

## Restoring from a Nightly Backup

The content of a nightly backup can be installed separately by deleting the current content and copying over the backed up content. The exception is restoring the backed up database for which you should use the Entuity restore command. (See *Restoring the Database*.)

# Database Management Overview

The Entuity database comprises a set of databases, each within their own folder (by default held under *entuity_home*`/database/data/`).

| Database | Backed Up | Description |
|---|---|---|
| **DSALPHA**, **DSPSTREAM**, **EOSdb** | Yes | Contain network management information collected and processed by Entuity. |
| **mysql** | Yes | Database users table. |
| **flowdb** | Yes | Contains data used with the Entuity Integrated Flow Analyzer. |
| **greenit** | Yes | Contains data used for the Green IT Perspective. |
| **secdb** | Yes | Contains details of Entuity user accounts, and is referenced when authenticating user logon. |
| **udadb** | Yes | Contains details of User Defined Polling. |
| **Virtualization** | No | Database used by Entuity for the initial collection of data from VM platforms. |
| **AtriumExport** | No | A module specific databases used with Entuity Integration Module for BMC® Atrium™ CMDB. |
| XMLAPIDB | No | Part of the XML Data Collector. It receives the queried XML data before it is copied into the main database. |
| **ecommerce, ReportsData, EOStrend** | No | Deprecated or not used in the current version of Entuity, database. |

Table 72 Entuity Databases

Alongside the other database folders is a temp folder used for holding temporary tables. It is not backed up.

When re-installing or re-configuring Entuity you should backup your data.

Entuity backup utility backs up the database, generating zipped backup files in directories under the Data directory. If during the `install` or `configure` process you decide to rebuild the database then all files under *entuity_home*/`database/data` are deleted. If you configured backup to save the database backup tables under that path then to preserve the backup folders move them outside of the Entuity directory tree.

For disk space reasons the Entuity backup utility does not backup those StormWorks objects specified through the StormWorks configuration as not being part of the backup.

When backing-up the Entuity database files but not using the Entuity backup utility, e.g. using standard copy and paste commands, then you should stop the Entuity database. Conversely, to use the Entuity backup utility the database must be running.

Entuity allows you to backup and restore its databases, and the MySQL users table. Two processes are involved, `backup` backs up the data and `restore` restores the backed up data.

✓ You cannot backup or restore the databases individually.

## Change the Database Backup Location

By default Entuity backups up each database to its own sub folder beneath *entuity_home*/ `database/backup`. When you rebuild the Entuity database during `install` and `configure` backups under *entuity_home*/database are also deleted. When you want to both rebuild the database and retain backups you should save the backups to a location not beneath *entuity_home*.

You can amend the default location for database backups when you run `configure`. (See the *Entuity Getting Started Guide*.)

## Backing up the Database

`backup` can run while Entuity continues to manage the network, conversely the only Entuity process `backup` requires to run is the database server `mysqld`. `backup` backs up all of the Entuity databases, and the MySQL users table to subfolders of `database\backup`.

By default `provost` schedules `backup` to run every night at 23:00. You should configure your nightly backup system tools to run after the database backup completes.

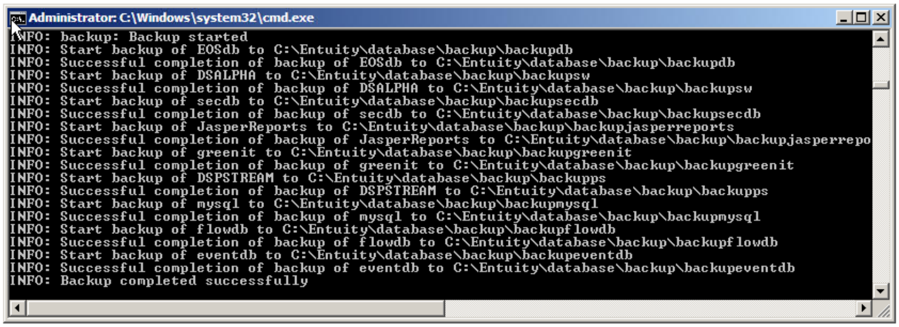
You can also manually run `backup`:

1) Ensure that you are logged on as a user with administrative privileges, and that, as a minimum, the database server `mysqld` is running.

2) From the command line run `backup`. Entuity backs up all of the databases which includes:

   - **EOSdb** database to *entuity_home*/`database/backup/backupdb.`
   - **DSALPHA** database to *entuity_home*/`database/backup/backupsw.`
   - **usadb** users table to *entuity_home*/`database/backup/backupusadb.`
   - **secdb** users table to *entuity_home*/`database/backup/backupsecdb.`
   - **greenit** database to *entuity_home*/`database/backup/backupgreenit`.
   - **DSPSTREAM** database to *entuity_home*/`database/backup/backupups.`
   - **MySQL** users table to *entuity_home*/`database/backup/backupmysql`.
   - **flowdb** database to *entuity_home*/`database/backup/backupflowdb.`
   - **eventdb** database to *entuity_home*/`database/backup/backupeventdb.`

3) As each backup completes Entuity reports the success or failure of each stage of the backup. Backup details can also be checked through the log file, `backup.log`, in the *entuity_home*/`log` directory.



```
INFO: backup: Backup started
INFO: Start backup of EOSdb to C:\Entuity\database\backup\backupdb
INFO: Successful completion of backup of EOSdb to C:\Entuity\database\backup\backupdb
INFO: Start backup of DSALPHA to C:\Entuity\database\backup\backupsw
INFO: Successful completion of backup of DSALPHA to C:\Entuity\database\backup\backupsw
INFO: Start backup of secdb to C:\Entuity\database\backup\backupsecdb
INFO: Successful completion of backup of secdb to C:\Entuity\database\backup\backupsecdb
INFO: Start backup of JasperReports to C:\Entuity\database\backup\backupjasperreports
INFO: Successful completion of backup of JasperReports to C:\Entuity\database\backup\backupjasperrepo
INFO: Start backup of greenit to C:\Entuity\database\backup\backupgreenit
INFO: Successful completion of backup of greenit to C:\Entuity\database\backup\backupgreenit
INFO: Start backup of DSPSTREAM to C:\Entuity\database\backup\backupps
INFO: Successful completion of backup of DSPSTREAM to C:\Entuity\database\backup\backupps
INFO: Start backup of mysql to C:\Entuity\database\backup\backupmysql
INFO: Successful completion of backup of mysql to C:\Entuity\database\backup\backupmysql
INFO: Start backup of flowdb to C:\Entuity\database\backup\backupflowdb
INFO: Successful completion of backup of flowdb to C:\Entuity\database\backup\backupflowdb
INFO: Start backup of eventdb to C:\Entuity\database\backup\backupeventdb
INFO: Successful completion of backup of eventdb to C:\Entuity\database\backup\backupeventdb
INFO: Backup completed successfully
```

Figure 262 Manual Running of backup

## Restoring the Database

In the event of system failure resulting in loss of data from the current databases you may have to restore the Entuity databases, and the MySQL users table, from a backup. You should use two utilities to restore and validate the database:

- `restore`, to remove the current database from the Entuity server and replace it with the database back up.
- `swmaint`, to check/repair the newly restored database. You can use `swmaint` to, for example, remove objects that have missing associations, delete stale objects, optimize tables. (See the *Entuity System Administrator Reference Manual*.)

When restoring a database backup from one server to another server then the database backup will have a different server identifier to that of the new server. After restoring the database you must change the server identifier in the restored database to that of the new server's identifier. (See *Restoring to a Different Entuity Server*.)

To restore the database:

1) Ensure that you are logged on as a user with administrative privileges.

2) Shut down Entuity.

   From the command line enter `stopeye`, or in Windows stop the Entuity service, which stops all of the Entuity services, e.g. **Entuity RPC**, **Entuity Database**, **Entuity Webserver** and **Entuity**.

3) Start the Entuity database server `mysqld`.

   From the command line run `c:\entuity\bin\start database` or in Windows restart the **Entuity Database** service.

4) From the command line run `c:\entuity\bin\restore`.

   You are prompted as follows:

   ```
   Do you really want to remove the entire Entuity database?
   If ’yes’, it will be recreated from the backup directories.
   ```

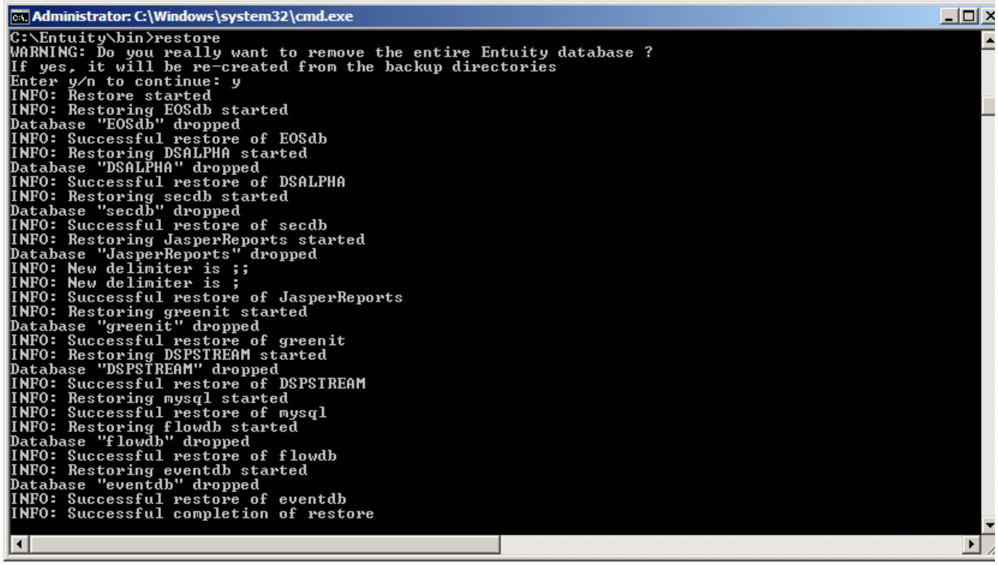
```
Type y/n to continue.
```

You can prevent Entuity from raising this prompt by using the parameter **-f**, i.e. `restore` **-f**, to force the restore.

5) Enter **y**. `restore` deletes the existing databases and tables and restores:

- **EOSdb** database from *entuity_home*/`database/backup/backupdb`.
- **DSALPHA** database from *entuity_home*/`database/backup/backupsw`.
- **usadb** users table from *entuity_home*/`database/backup/backupusadb.`
- **secdb** users table from *entuity_home*/`database/backup/backupsecdb`.
- **greenit** database from *entuity_home*/`database/backup/backupgreenit`.
- **DSPSTREAM** database to *entuity_home*/`database/backup/backupups.`
- **MySQL** users table from *entuity_home*/`database/backup/backupmysql.`
- **flowdb** database from *entuity_home*/`database/backup/backupflowdb.`
- **eventdb** database from *entuity_home*/`database/backup/backupeventdb.`

As each restore completes, Entuity reports the success or failure of each step. Restore details can also be checked through the log file, `restore.log`, in *entuity_home*/`log`.



```
C:\Entuity\bin>restore
WARNING: Do you really want to remove the entire Entuity database ?
If yes, it will be re-created from the backup directories
Enter y/n to continue: y
INFO: Restore started
INFO: Restoring EOSdb started
Database "EOSdb" dropped
INFO: Successful restore of EOSdb
INFO: Restoring DSALPHA started
Database "DSALPHA" dropped
INFO: Successful restore of DSALPHA
INFO: Restoring secdb started
Database "secdb" dropped
INFO: Successful restore of secdb
INFO: Restoring JasperReports started
Database "JasperReports" dropped
INFO: New delimiter is ;;
INFO: New delimiter is ;
INFO: Successful restore of JasperReports
INFO: Restoring greenit started
Database "greenit" dropped
INFO: Successful restore of greenit
INFO: Restoring DSPSTREAM started
Database "DSPSTREAM" dropped
INFO: Successful restore of DSPSTREAM
INFO: Restoring mysql started
INFO: Successful restore of mysql
INFO: Restoring flowdb started
Database "flowdb" dropped
INFO: Successful restore of flowdb
INFO: Restoring eventdb started
Database "eventdb" dropped
INFO: Successful restore of eventdb
INFO: Successful completion of restore
```

Figure 263 Restoring the Entuity Database

6) Once `restore` reports successful completion, run `swmaint`. For example, in:

- Default mode, `swmaint` removes object and sample data with incomplete associations. Enter:

```
swmaint
```

- Quick mode, `swmaint` does not delete or optimize object and sample data:

```
swmaint -q
```

See the *Entuity System Administrator Reference Manual* for full details on `swmaint`.

7) `swmaint` reports its progress through the command line. When it completes stop the database server `mysqld` by either:

- Invoking from the command line `stop database`, or
- In Windows stopping the **Entuity Database** service.

✓ Run `configure` before restarting the Entuity server when restoring the Entuity database to a different server, or a different location on the same server, to the one it was backed up from.

8) When restoring a database backup from one server to another you must change the server identifier in the restored database to that of the new server's identifier. (See *Restoring to a Different Entuity Server*.)

9) Restart the Entuity server.

From the command line enter `starteye`, or in Windows restart the **Entuity** service.

## Restoring to a Different Entuity Server

After restoring a database backup from one server to another, for example as part of a disaster recovery program, the restored database must be updated with the new server's identifier.

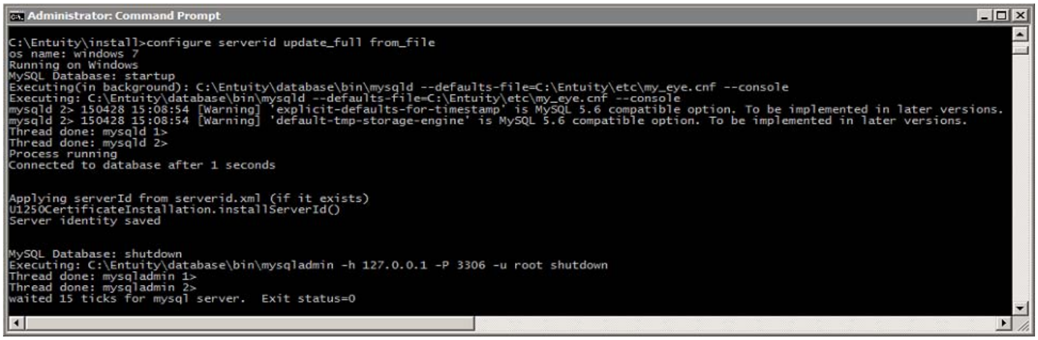
The unique server identifier is stored in *entuity_home*`\etc\serverid.xml`. You can run `configure` with the `from_file` parameter to update the restored database with the new Entuity server’s identifier.

Ensure Entuity database is not running and from the command line navigate to *entuity_home*`\install and` enter:

```
configure serverid update_full from_file
```

`update_full`, updates from `serverid.xml` the files and database with `serverid` but also dashboards, user selections and reports. When you only need to update the database you can use the `update` option.

✓ Entuity does not update the server identifiers associated with any physical connections. These connections are invalid and should be removed.



```
C:\Entuity\install>configure serverid update_full from_file
os name: windows 7
Running on Windows
MySQL Database: startup
Executing(in background): C:\Entuity\database\bin\mysqld --defaults-file=C:\Entuity\etc\my_eye.cnf --console
Executing: C:\Entuity\database\bin\mysqld --defaults-file=C:\Entuity\etc\my_eye.cnf --console
mysqld 2> 150428 15:08:54 [Warning] 'explicit-defaults-for-timestamp' is MySQL 5.6 compatible option. To be implemented in later versions.
mysqld 2> 150428 15:08:54 [Warning] 'default-tmp-storage-engine' is MySQL 5.6 compatible option. To be implemented in later versions.
Thread done: mysqld 1>
Thread done: mysqld 2>
Process running
Connected to database after 1 seconds


Applying serverId from serverid.xml (if it exists)
U1250CertificateInstallation.installServerId()
Server identity saved


MySQL Database: shutdown
Executing: C:\Entuity\database\bin\mysqladmin -h 127.0.0.1 -P 3306 -u root shutdown
Thread done: mysqladmin 1>
Thread done: mysqladmin 2>
waited 15 ticks for mysql server.  Exit status=0
```

Figure 264 Set Entuity Server Identifier

## Checking the Database

Each time Entuity starts Entuity runs `dbcheck` which checks that the database was previously correctly closed down, for example a power failure can leave some database tables open. `dbcheck` runs before the database starts and if it identifies problems that require repairing it calls `myisamchk`. The time taken to run a full check and repair of the database varies according to the size of the managed network.

# 43 Day to Day Administration

The basic administration tasks that should be performed on a regular basis include: checking permissions; checking system processes; checking disk space; monitoring port license credit availability; viewing process log files; and checking database integrity.

## Monitoring User Access

### Checking User Permissions

You should ensure that the views to which the various **User Groups** have access contain the necessary components and generate the required events. You should also ensure that any new users are added to the appropriate **Groups**, and that all **Groups** have the necessary permissions.

### Checking User Access

Each time a user logs on to Entuity a record is written to `auth.log`, held in *entuity_home*\log\. For each login attempt Entuity records:

- The login time.
- Whether the attempt was accepted or rejected.
- The user name.
- The client machine address.

Entuity also distinguishes between logging onto the server through the:

- Entuity client:

  ```
  12/14/2006 18:36:42: Accepting login: application=Entuity  host=IDD
  user=admin
  ```

- web interface using cgi scripts:

  ```
  12/15/2006 10:34:10: Accepting login: application=cgi host=10.44.1.155
  user=admin
  ```

## Checking Disk Space Availability

During the initial six months of an Entuity installation the size of the database grows appreciably. You should check that there is sufficient disk space to accommodate the increases in database size.

After the first six months of network monitoring, Entuity's database should remain approximately constant in size, growing only when new networking equipment is added to the Entuity management environment or upgrades to Entuity increase the range of objects it manages.

### Monitoring Disk Space

Corruption of the Entuity database can occur when the server runs out of disk space. To prevent this Entuity monitors the available disk space through `diskMonitor`. It compares this value against two thresholds, if it falls below the:

- First threshold, `diskMonitor` raises in Event Viewer Entuity Server Disk Space Alert events which detail the remaining disk space
- Second threshold, `diskMonitor` raises in Event Viewer an Entuity Server Shutdown event which details the remaining disk space on the server. `diskMonitor` also initiates server shutdown.

`diskMonitor` is highly configurable you can set both threshold values, the period between samples, the minimum disk space requirement, Entuity shutdown (see *Entuity Reference Manual*).

## Monitoring License Credit Usage

As more networking equipment is added to the Entuity management environment, Entuity identifies to which policy group it belongs. Each policy group has a number object credits, for example if the device credit limit is exceeded, then the ports of any newly added devices are not monitored.

There are a number of different methods you can use to check the status of Entuity license objects:

- Click **Administration** > **Entuity Health** > **License Health**, to view a breakdown of license credits.
- From the command line run `checkLicense`, which provides a detailed breakdown of license credits and weighting.
- Check `prodigy.log` for the following message:

  ```
  Insufficient credit to analyze all interfaces
  ```

If you have insufficient credits, you should increase your credit allocation by replacing your current license file.

## Checking System Log Files

`starteye` starts and restarts processes detailed in the startup configuration file; for Windows `startup_WIN32.cfg` and for Linux systems `startup_UNIX.cfg`.

The scheduling process, `provost` initiates many daily and weekly system processes to maintain topology, MAC, IP and other network-related information. The StormWorks process `DsKernelStatic` also generates log files containing information generated from the services it controls.

All of these processes generate log files in the *entuity_home*/`log` directory. The processes and their respective log files in *Table 73 Process Log Files* should be checked on a regular basis. (See *Entuity System Administrator Reference Manual* for the logs associated with processes.)

| Process name | Log file |
|---|---|
| `DsKernelStatic` | `DsKernelStatic.log` |
| `httpd` | `http.error_log`, `http.access_log` |
| `LicenseSvr` | `license.log` |
| `macman` | `macman.log` |
| `prodigy` | `prodigy.log` |
| `profluent` | `profluent.log` |
| `prole` | `prole.log` |
| `prophcap` | `prophcap.log` |
| `protean` | `protean.log` |
| `provost` | `provost.log` |
| `starteye` | `systemcontrol.log` |

Table 73 Process Log Files

✓ Many of the log files wrap to *logfile*.[1-4] when they reach a pre-determined size.

You should ensure that all the processes are completing successfully, if any process is logging this message:

```
Lack of memory
```

then there is insufficient memory (and swap space) on the management server.

## Checking Database Integrity

Each night, the devices being monitored are redistributed amongst the pollers (`proles`) by a process called `profluent`. You should check that none of the devices have been dropped as a result of this redistribution process, and that all the devices being monitored are in a consistent state. To perform this check, invoke the `probity` utility from *entuity_home*/`bin`.

If the *prole ID* field is set to ‘INVALID’ for any of the devices listed, then that device is no longer being polled. Check the `profluent` process log file, *entuity_home*/`log/prof.log`, for any diagnostic messages. Typically, the condition will be caused by the device’s SNMP polling time is considered too long to be manageable.

## Maintaining Port Peers

When Entuity monitors both ends of a circuit then it attempts to automatically match those endpoints. For ATM and Frame Relay ports Entuity first attempts to match IP addresses within DLCIs and VCCs and then between DLCIs and VCCs. For leased lines Entuity attempts to pair IP addresses of devices within the same subnet.

Occasionally this peering may not be successful, and you may have to complete the peering manually. For example, Frame Relay PVC DLCI’s are peered based on their IP address or netmask. When the device’s MIB does not contain this information then DLCI peer matching can only be completed manually.

Manual pairing of circuits is the same process whether the technology is Frame Relay, Leased Line, ATM. Entuity also allows you to use the same process to peer ports that are not used in these circuit technologies, through the Resilient Link Peering option.

## Identifying Peered Objects

You can immediately identify peered ports, Leased Lines, VCCs and DLCIs through the object icon, which for peered objects is a doubled representation to indicate a peered object.

## Managing Resilient Link Peering

Resilient links allow you to protect critical links and prevent network downtime if those links fail by having configured a standby link to immediately take over the task if the main link fails.

When two ports are linked, and you want Entuity to identify those links for reporting on using the port level Capacity Heat Maps, you can use the resilient link peering functionality.

Within Entuity you identify the two managed ports that form the resilient link. Entuity allows you to specify one resilient link per port.

### Peering Resilient Links

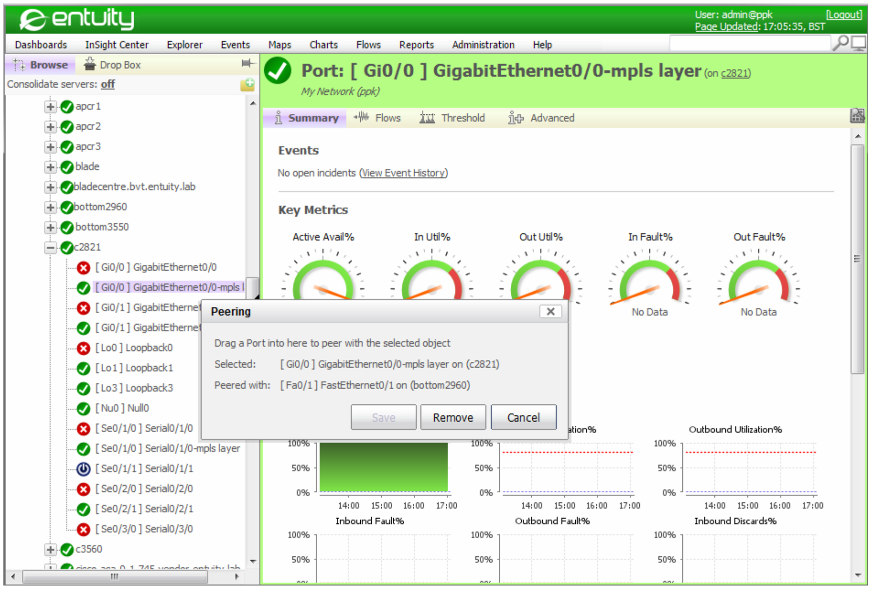
Entuity resilient peering allows you to match any Entuity managed port with any other Entuity managed port.

To peer ports:

1) From the Explorer tree highlight the device port and from the context menu click **Peering > Manage Resilient Link**.

   The Peering dialog in *From* displays the details of the selected port details.

2) From the Explorer tree find the target port and then drag it onto the open Peering dialog. Entuity updates *To*, displaying details of the newly selected port.


entuity
User: admin@ppk [Logout]
Page Updated: 17:05:35, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
Browse Drop Box
Consolidate servers: off
apcr1
apcr2
apcr3
blade
bladecentre.bvt.entuity.lab
bottom2960
bottom3550
c2821
[ Gi0/0 ] GigabitEthernet0/0
[ Gi0/0 ] GigabitEthernet0/0-mpls l
[ Gi0/1 ] GigabitEthernet
[ Gi0/1 ] GigabitEthernet
[ Lo0 ] Loopback0
[ Lo1 ] Loopback1
[ Lo3 ] Loopback3
[ Nu0 ] Null0
[ Se0/1/0 ] Serial0/1/0
[ Se0/1/0 ] Serial0/1/0-mpls layer
[ Se0/1/1 ] Serial0/1/1
[ Se0/2/0 ] Serial0/2/0
[ Se0/2/1 ] Serial0/2/1
[ Se0/3/0 ] Serial0/3/0
c3560
Port: [ Gi0/0 ] GigabitEthernet0/0-mpls layer (on c2821)
My Network (ppk)
Summary Flows Threshold Advanced
Events
No open incidents (View Event History)
Key Metrics
Active Avail% In Util% Out Util% In Fault% Out Fault%
No Data
No Data
Outbound Utilization%
Inbound Fault%
Outbound Fault%
Inbound Discards%
100%
50%
0%
14:00 15:00 16:00 17:00

Peering

Drag a Port into here to peer with the selected object

Selected: [ Gi0/0 ] GigabitEthernet0/0-mpls layer on (c2821)

Peered with: [ Fa0/1 ] FastEthernet0/1 on (bottom2960)

Figure 265 Resilient Link Peering

3) Click **Save** to peer the two selected ports. Entuity creates the link and closes the Peering dialog.

### Deleting Peered Resilient Links

Entuity resilient peering allows you to match any Entuity managed port with any other Entuity managed port. These links are maintained until they are manually deleted.

To delete resilient linked peered ports:

1) From the Explorer tree highlight the device port and from the context menu click **Peering > Manage Resilient Link**.

2) Click **Remove** and then **Yes** to the delete peering confirmation dialog.

## Managing Leased Line Peering

When two leased line ports are linked, and you want Entuity to identify those links, you can use the leased line peering functionality. Within Entuity you can identify the two managed ports that you want to link. Entuity allows you to specify one leased line peering per port.

### Peering Leased Lines

Entuity leased line peering allows you to match any Entuity managed leased line port with any other Entuity managed leased line port.

To peer leased line ports:

### Deleting Peered Leased Lines

Entuity leased line peering allows you to match any Entuity managed port with any other Entuity managed port.

### Managing Frame Relay DLCI Peering

When two DLCI ports are linked and Entuity has not already automatically linked them, you can use the DLCI peering functionality. Within Entuity you can identify the two managed ports that you want to link. Entuity allows you to specify one DLCI link per port.

#### Manual Pairing of DLCI Peers

To pair DLCI peers:

#### Deleting Peered DLCI Links

To delete peered DLCI links:

### Managing ATM VCC Peering

When two ports are linked, and you want Entuity to identify those links, you can use the resilient link peering functionality. Within Entuity you can identify the two managed ports that you want to link. Entuity allows you to specify one ATM VCC link per port.

#### Manual VCC Peering

To pair VCC peers:

#### Deleting Peered VCC Links

To delete peered VCC links:

## snmpWriteCommunity String Security

Control over writing to network devices has serious security implications. Entuity restricts application of the snmpWrite community string to certain modules, e.g. Entuity Cisco IP SLA, Entuity Configuration Monitor. Entuity presents the write community string as a series of asterisks. Only users with Entuity administrator access rights may set the snmpWrite community string. Also for security purposes Flex Reports does not access the private community string.

To set the private community string:

# 44 Performing Key Administration Tasks

Entuity Administration is available to those users that are members of the Administrator user groups or have tool permissions to one of more of the administrator functions.

To access the Entuity **Administration** options:

1) Click **Administration**.

   Entuity opens the Administration menu and displays the administration options available to you:

   - **Entuity Health**, overview of Entuity server health, process checking, reporting performance, database performance and license health. Entuity Health also includes detailed license checking, checking on Flow Collector Health and when Data Export is enabled, a data export health summary.
   - **Inventory** / **Topology**, manage devices, device attribute details and refresh view membership.
   - **Events**, manage incident ageout, suppression rules and event threshold settings. (See *Chapter 27 - Event Management System*.)
   - **Flow Collector**, manage, when enabled, Entuity Integrated Flow Analyzer settings. (See *Chapter 25 - Set-up and Manage Flow Data*.)
   - **Data Export**, export of data from the Entuity database to a database external to Entuity. (See *Chapter  - Data Export Datasets and Definitions*.)
   - User Defined Polling (See *Chapter 56 - User Defined Polling*.)
   - **Account Management**, set up and manage user profiles through user groups, tool and report permissions. Users that are not members of the Administrator user group can only amend their password.
   - **Multi-Server Administration**, manage remote and central servers. (See *Chapter 31 - Manage Entuity Security*.)
   - **Audit Log**, provides a central point for reviewing and analyzing actions performed on Entuity. (See *Chapter 41 - Audit Log*.)
   - **Preferences**, allows you to view and modify the Entuity web interface. (See *Chapter 10 - User Preferences*.)

## Monitoring the Health of the Entuity Server

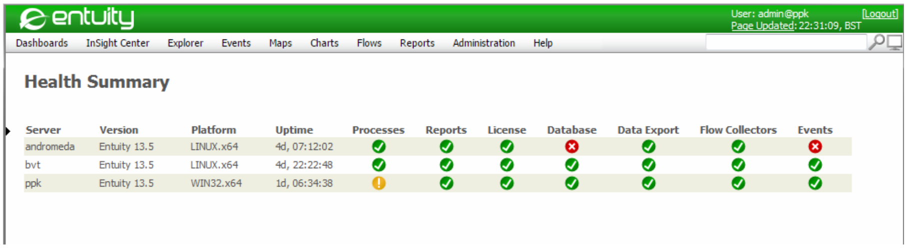
The Health Summary page presents a health summary for each of the available Entuity servers. It provides key identifying information and health metric indicators, which can have a status of OK, Warning and Severe. By clicking on an indicator you can display a detailed breakdown of that health metric for that server, which also includes a legend detailing the meaning of indicator status.

For each Entuity server, both local and remote, the Health Summary page details:

- *Server*, name of the Entuity server.

- *Version*, software version of Entuity installed to the server. Details of the last patch installed are enclosed in brackets. Where patches have been installed in the incorrect sequence, Entuity displays a warning indicator. You should always install Entuity patches in the correct sequence.
- *Platform*, operating system on which Entuity is running.
- *Uptime*, length of time since the Entuity server was last restarted (as measured using dsKernel).
- *Processes*, an indicator showing the overall health of Entuity processes. You can click on the indicator to open the Process Health page for a process by process health report.
- *Reports*, an indicator showing the overall health of Entuity reporting. You can click on the indicator to open the Reports Health page for a detailed breakdown of reporting performance.
- *License*, an indicator showing the overall health of Entuity license. You can click on the indicator to open the License Health page for a detailed breakdown of the Entuity license.
- *Database*, an indicator showing the overall health of Entuity database, as measured by the occurrence of slow queries. You can click on the indicator to open the Database Health page for a detailed breakdown of the Entuity database performance.
- *Data Export*, an indicator showing the overall health of Entuity data export jobs, as measured by the occurrence of slow jobs and job failures. You can click on the indicator to open the Data Export Health page for a detailed breakdown of the Entuity data export performance.
- *Flow Collectors*, an indicator showing the health of flow collection with:
  - Warning indicating flow data loss in the last 24 hours.
  - Severe indicating flow data loss in the last hour or the flow collector process is unresponsive.
- *Events*, an indicator showing the state of resource usage with:
  - Warning indicating resource usage has exceeded 80% of capacity but not reached 99%.
  - Severe indicating resource usage has exceeded 98% of capacity.

By default the Health Summary page refreshes every five minutes.



Health Summary

| Server | Version | Platform | Uptime | Processes | Reports | License | Database | Data Export | Flow Collectors | Events |
|---|---|---|---|---|---|---|---|---|---|---|
| andromeda | Entuity 13.5 | LINUX.x64 | 4d, 07:12:02 | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ |
| bvt | Entuity 13.5 | LINUX.x64 | 4d, 22:22:48 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ppk | Entuity 13.5 | WIN32.x64 | 1d, 06:34:38 | ! | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Figure 266 Entuity Servers Health Summary

To access the Health Summary page:

1) Click **Administration > Entuity Health > Health Summary**.

   You can click on the health metric indicators to open summary pages on that indicator.

## Checking Process Health

You can check process health using the Process Health page, and also the Entuity Server Health Summary report. The reported attributes are the same and include an overall summary of processor health through the status icon, which when set to:

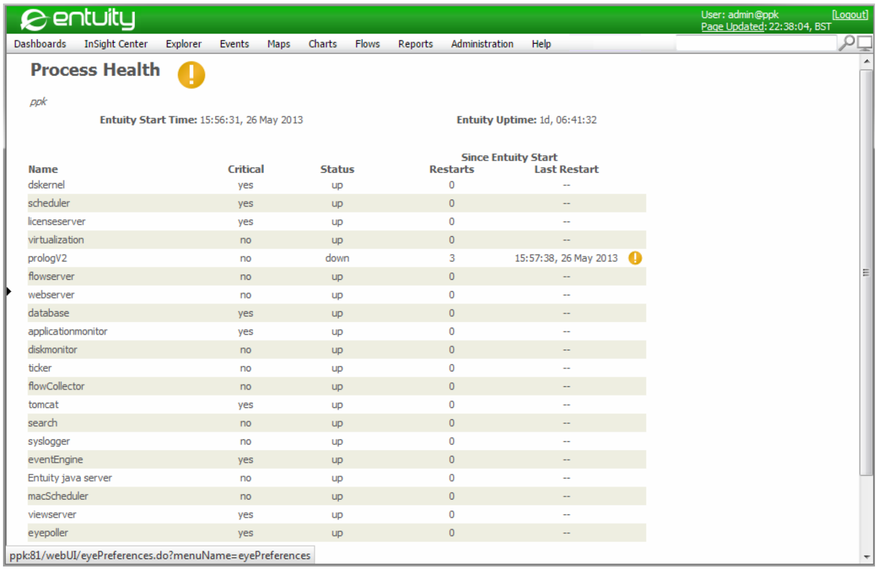
- Warning, 1 or more processes are down (permanently) no matter when that happened or 1 or more processes restarted in the last hour
- Severe, 2 or more processes are down (permanently) in the last hour or 2 or more processes restarted in the last hour.

| Name | Description |
|---|---|
| *Entuity Start Time* | Date and time of the last Entuity start up. |
| *Entuity Uptime* | The length of time the device has been up since its last start up. |
| *Name* | Name of the process. |
| *Critical* | Indicates whether the process is critical to Entuity. |
| *Status* | Current status of the process. |
| *Restarts* | Number of process restarts since Entuity started. |
| *Last restart* | Date and time the process last restarted. |

Table 74 Process Health

To run a process health check:

1) Click **Administration > Entuity Health > Process Health**.



Process Health !

ppk

**Entuity Start Time:** 15:56:31, 26 May 2013 **Entuity Uptime:** 1d, 06:41:32

| | | | Since Entuity Start | |
|---|---|---|---|---|
| **Name** | **Critical** | **Status** | **Restarts** | **Last Restart** |
| dskernel | yes | up | 0 | -- |
| scheduler | yes | up | 0 | -- |
| licenseserver | yes | up | 0 | -- |
| virtualization | no | up | 0 | -- |
| prologV2 | no | down | 3 | 15:57:38, 26 May 2013 ! |
| flowserver | no | up | 0 | -- |
| webserver | no | up | 0 | -- |
| database | yes | up | 0 | -- |
| applicationmonitor | yes | up | 0 | -- |
| diskmonitor | no | up | 0 | -- |
| ticker | no | up | 0 | -- |
| flowCollector | no | up | 0 | -- |
| tomcat | yes | up | 0 | -- |
| search | no | up | 0 | -- |
| syslogger | no | up | 0 | -- |
| eventEngine | yes | up | 0 | -- |
| Entuity java server | no | up | 0 | -- |
| macScheduler | no | up | 0 | -- |
| viewserver | yes | up | 0 | -- |
| eyepoller | yes | up | 0 | -- |

ppk:81/webUI/eyePreferences.do?menuName=eyePreferences

Figure 267 Entuity Process Health

## Checking on Reporting Performance

From the Entuity Reports Health page you can monitor the performance of the individual and overall reporting tools. You can also drill-down to detailed, temporary Flex Reports on each of the reporting tools.

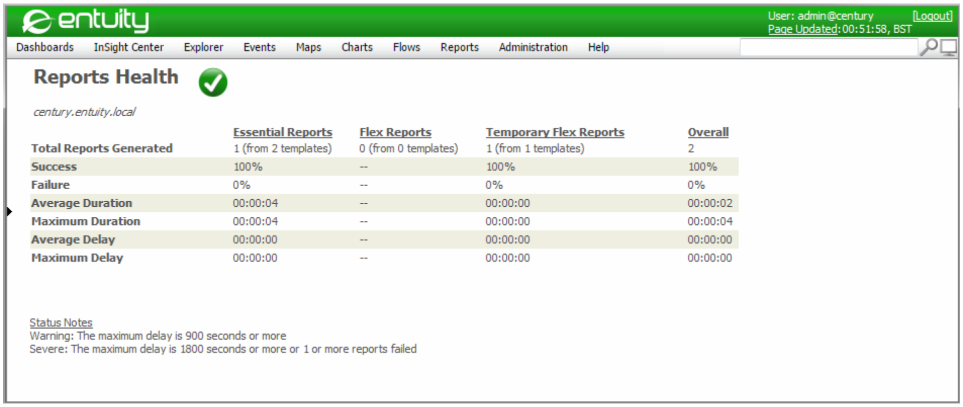
Entuity Health Reports delivers metrics against standard reports, Flex Reports, Temporary Flex Reports and an overall performance value. These Entuity Health Report metrics are calculated for the previous 24 hour period (00:00 to 23:59):

- *Total Reports Generated, number of generated reports.*
- *Success*, percentage of successfully generated reports.
- *Failure*, percentage of reports that failed to generate.
- *Average Duration*, average time taken to successfully generate reports.
- *Maximum Duration,* maximum time taken to successfully generate reports.
- *Average Delay*, average time delay between when a scheduled report was intended to run and when Entuity started to generate a report that it would successfully generate.
- *Maximum Delay*, maximum time delay between when a scheduled report was intended to run and when Entuity started to generate a report that it would successfully generate.
- *Overall Status*, summary state of Entuity reporting tools:
    - **OK**, performance is within acceptable boundaries
    - **Warning**, the maximum delay is greater than fifteen minutes
    - **Severe**, the maximum delay is greater than thirty minutes or one or more reports failed to generate.

The report headings, Reports, Flex Reports, Temporary Flex Reports and Overall are also hyperlinks to detailed Temporary Flex Reports that provide a report by report breakdown.

To access the Entuity Reports Health page:

1) Click **Administration** > **Entuity Health** > **Reports Health**.



Reports Health ✓

*century.entuity.local*

| | Essential Reports | Flex Reports | Temporary Flex Reports | Overall |
|---|---|---|---|---|
| Total Reports Generated | 1 (from 2 templates) | 0 (from 0 templates) | 1 (from 1 templates) | 2 |
| Success | 100% | -- | 100% | 100% |
| Failure | 0% | -- | 0% | 0% |
| Average Duration | 00:00:04 | -- | 00:00:00 | 00:00:02 |
| Maximum Duration | 00:00:04 | -- | 00:00:00 | 00:00:04 |
| Average Delay | 00:00:00 | -- | 00:00:00 | 00:00:00 |
| Maximum Delay | 00:00:00 | -- | 00:00:00 | 00:00:00 |

Status Notes
Warning: The maximum delay is 900 seconds or more
Severe: The maximum delay is 1800 seconds or more or 1 or more reports failed

Figure 268 Entuity Reports Health

## Checking on Database Health

You can check database health using the Database Health page, and also the Reports Server Entuity Server Health report. These health metrics are intended for Entuity representatives, or advanced users, intending to investigate performance problems or tune performance:

- *Database Uptime*, amount of time since database last start.
- *Slow Queries*, high values identify possible opportunities for database query optimization.
  - *Past Hour*, number of queries in the past hour that exceeded the slow query threshold.
  - *Average Per Hour*, hourly average since the last database restart, of queries that exceeded the slow query threshold.
  - *Past 24 Hours*, number of queries in the past twenty-four hours that exceeded the slow query threshold.
  - *Average per 24 Hours*, daily average since the last database restart, of queries that exceeded the slow query threshold.
  - *a slow query* identifies number of slow queries in past hour and past 24 hours with corresponding averages (averages are calculated since the last database start).

  A large number of slow queries corresponds to a large database load. Where there is a significant deviation of the current number of slow queries from the server’s average, this indicates an abnormal database loading that may require investigation.

Slow queries are defined as a query that takes longer the set value. The minimum and default values of long_query_time are 1 and 15 seconds, respectively.

- *Key Cache*:
  - *Size*, size of the configured key cache
  - *Hits in Past 24 Hours*, cache-hit percentage in the past 24 hours. Low hit percentage indicates the need in increasing of the cache size.
- *Table Cache*:
  - *Size*, current table cache size
  - *Tables Opened in Past 24 Hours*, daily table open rate over the previous day
  - *Average Per 24 Hours*, daily average since the last database restart, of table access

  A large number of opened tables, or an increase compared to the average indicates the need to increase the table cache.

- *Table Lock Acquisitions*:
  - *Total*, number of table lock acquisitions over the previous hour and twenty-four hours.
  - *Immediate*, number of immediate table lock acquisitions over the hour and twenty-four hours.
  - *Waited*, number of table delayed lock acquisitions over the previous hour and twenty-four hours.

  A large percentage of waited lock acquisitions indicates a large database load.

- *Threads*:
  - Non-Sleeping, number of current non-sleeping lock threads and average since the last database restart.
  - Waiting on User Lock, number of current waiting on user lock threads and average since the last database restart.

  Large numbers and higher deviations from the average indicate a higher current load.

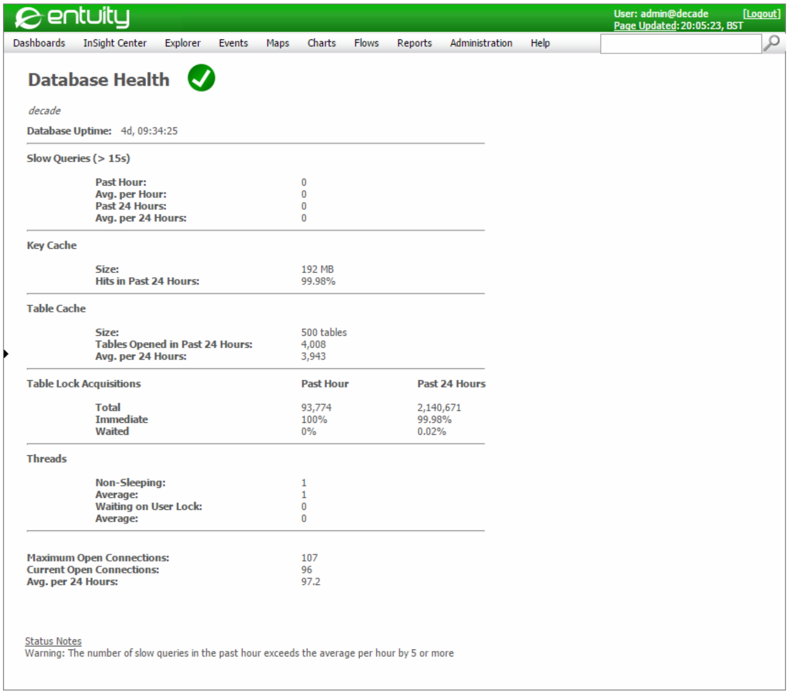
- *Maximum Open Connections*, the maximum number of open connections since the last database restart. A higher number of open connections indicates higher database utilization.
- *Current Open Connections*, the current number of open connections. A higher number of open connections indicates higher database utilization.
- *Average per 24 Hours*, the average daily number of open connections since the last database restart.

  A higher number of open connections indicates higher database utilization.

- *Overall Status*, summary state of Entuity Database Health:
  - **OK**, performance is within acceptable boundaries
  - **Warning**, the number of slow queries in the past hour is larger than the corresponding average by five or more.

To access the Entuity Database Health page:

1) Click **Administration** > **Entuity Health** > **Database Health**.



Database Health ✓

*decade*

**Database Uptime:** 4d, 09:34:25

| Slow Queries (> 15s) | | |
|---|---|---|
| | Past Hour: | 0 |
| | Avg. per Hour: | 0 |
| | Past 24 Hours: | 0 |
| | Avg. per 24 Hours: | 0 |

| Key Cache | | |
|---|---|---|
| | Size: | 192 MB |
| | Hits in Past 24 Hours: | 99.98% |

| Table Cache | | |
|---|---|---|
| | Size: | 500 tables |
| | Tables Opened in Past 24 Hours: | 4,008 |
| | Avg. per 24 Hours: | 3,943 |

| Table Lock Acquisitions | | Past Hour | Past 24 Hours |
|---|---|---|---|
| | Total | 93,774 | 2,140,671 |
| | Immediate | 100% | 99.98% |
| | Waited | 0% | 0.02% |

| Threads | | |
|---|---|---|
| | Non-Sleeping: | 1 |
| | Average: | 1 |
| | Waiting on User Lock: | 0 |
| | Average: | 0 |

| | |
|---|---|
| Maximum Open Connections: | 107 |
| Current Open Connections: | 96 |
| Avg. per 24 Hours: | 97.2 |

Status Notes
Warning: The number of slow queries in the past hour exceeds the average per hour by 5 or more

Figure 269 Entuity Database Health

### See Also

Monitoring the Health of the Entuity Server

Checking Process Health

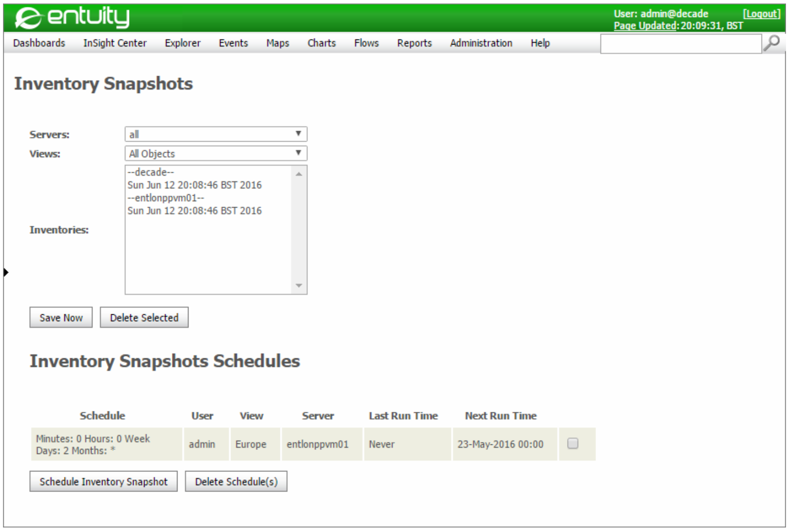
Checking on Reporting Performance

Check Event Management System Health

## Track Inventory Change

An Inventory Snapshot allows you to create, schedule and manage changes in the network inventory. Snapshots are taken on a view basis, rather than the entire inventory, so you can capture snapshots of your own root and sub-view(s). Only users with the Inventory Snapshots Administration permission can access and manage inventory snapshots.

Snapshots are stored in the Entuity database, you can then report on those snapshots through the Inventory Changes report, which is included to the Inventory Reports group. The Inventory Change report requires two snapshots.



Inventory Snapshots

Servers: all

Views: All Objects

Inventories:
--decade--
Sun Jun 12 20:08:46 BST 2016
--entlonppvm01--
Sun Jun 12 20:08:46 BST 2016

Inventory Snapshots Schedules

| Schedule | User | View | Server | Last Run Time | Next Run Time | |
|---|---|---|---|---|---|---|
| Minutes: 0 Hours: 0 Week Days: 2 Months: * | admin | Europe | entlonppvm01 | Never | 23-May-2016 00:00 | □ |

Figure 270 Inventory Snapshots

| Attributes | Description |
|---|---|
| *Servers* | Select the server(s) on which the views you want to take the snapshot are available. When you select multiple servers Entuity generates separate snapshots for the same named view on those servers. |
| *Views* | Select the view against which you want to take the inventory snapshot. |
| *Inventories* | List of saved snapshot inventories which are available to the Inventory Change report. You can highlight inventory entries and then select **Delete Selected** to remove the snapshot. |
| *Save Now* | Select to take an inventory snapshot for the selected *Servers* and *Views*. |
| *Delete Selected* | Select the inventory snapshot you want to delete from Entuity. |

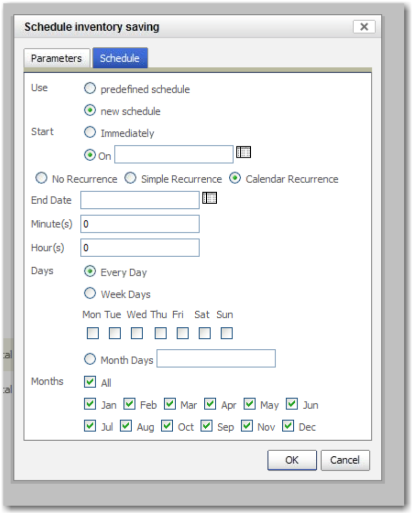
Table 75 Set-up Inventory Snapshots

| Attributes | Description |
|---|---|
| *Schedule* | Summary of the schedule. |
| *User* | Name of the user who created the inventory schedule. |
| *View* | View for which the snapshot is taken. |
| *Server* | Name of the Entuity server. |
| *Last Run Time* | Date and time the schedule last ran. |
| *Next Run Time* | Scheduled date and time of the next inventory snapshot. |

Table 76 Schedule Inventory Snapshots

## Schedule Configuration Options

For each schedule you can select an existing schedule or define a new one. Entuity includes predefined schedules that run the report Daily, Hourly, Minutely or Weekly.



Use ○ predefined schedule ● new schedule

Start ○ Immediately ● On

○ No Recurrence ○ Simple Recurrence ● Calendar Recurrence

End Date

Minute(s) 0

Hour(s) 0

Days ● Every Day ○ Week Days

Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun □

○ Month Days

Months ☑ All

☑ Jan ☑ Feb ☑ Mar ☑ Apr ☑ May ☑ Jun

☑ Jul ☑ Aug ☑ Oct ☑ Sep ☑ Nov ☑ Dec

Figure 271 Calendar Recurrence Options

| Schedules | Description |
|---|---|
| *Predefined Schedule* | |
| *Existing Schedule* | Entuity includes four predefined schedules:<br>- **weekly**, runs once a week, at midnight on Sunday<br>- **daily**, runs at midnight<br>- **hourly**, runs every hour, on the hour<br>- **minutely**, runs every sixty seconds. |
| New Schedule | |
| *No Recurrence* | Runs the schedule once. |
| Simple Recurrence | Select to display an abbreviated set of options. You can define in:<br>- Occur, for how long the report runs. Indefinitely, until a defined end date, a set number of times<br>- Every, how often the schedule runs a report, setting the number of minutes, hours, days or weeks. |

Table 77 Schedule Configuration Options

| Schedules | Description |
|---|---|
| *Calendar Recurrence* | Select to display a set of options that allow fine control over the schedule. You can define:<br>■ End Date, the end period of the report schedule.<br>■ Minutes and hours, the time when the report runs.<br>■ Days, select either every day, weekdays, one or more individual days or Month Days.<br>■ Months, select All to run every month, or one or more particular months. |

Table 77 Schedule Configuration Options

## Create Inventory Snapshots

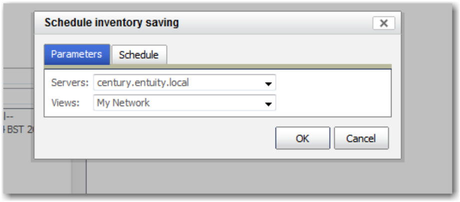
You can manually create or schedule a snapshot from the Inventory Snapshots page.

To create a snapshot schedule:

1) Click **Administration** > **Inventory** / **Topology** > **Inventory Snapshots**.

2) Select the server and view for which you want to create a schedule.

3) Select Schedule Inventory Snapshot.



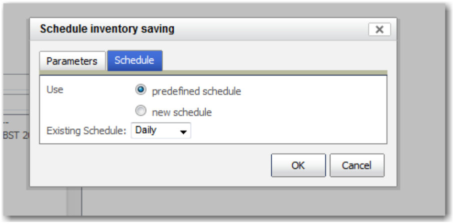
Servers: century.entuity.local

Views: My Network

Figure 272 Snapshot Schedule Server and View

4) From *Servers* select the servers for which you want to define a schedule.

5) From *Views* select the view to which you want to apply the schedule.



Use ● predefined schedule ○ new schedule

Existing Schedule: Daily

Figure 273 Select Snapshot Schedule

6) Select an existing, or define a new, schedule.

7) Click **OK**. Entuity creates the schedule. The schedule is immediately active.

### Delete an Inventory Snapshot Schedule:

To delete an inventory snapshot schedule:

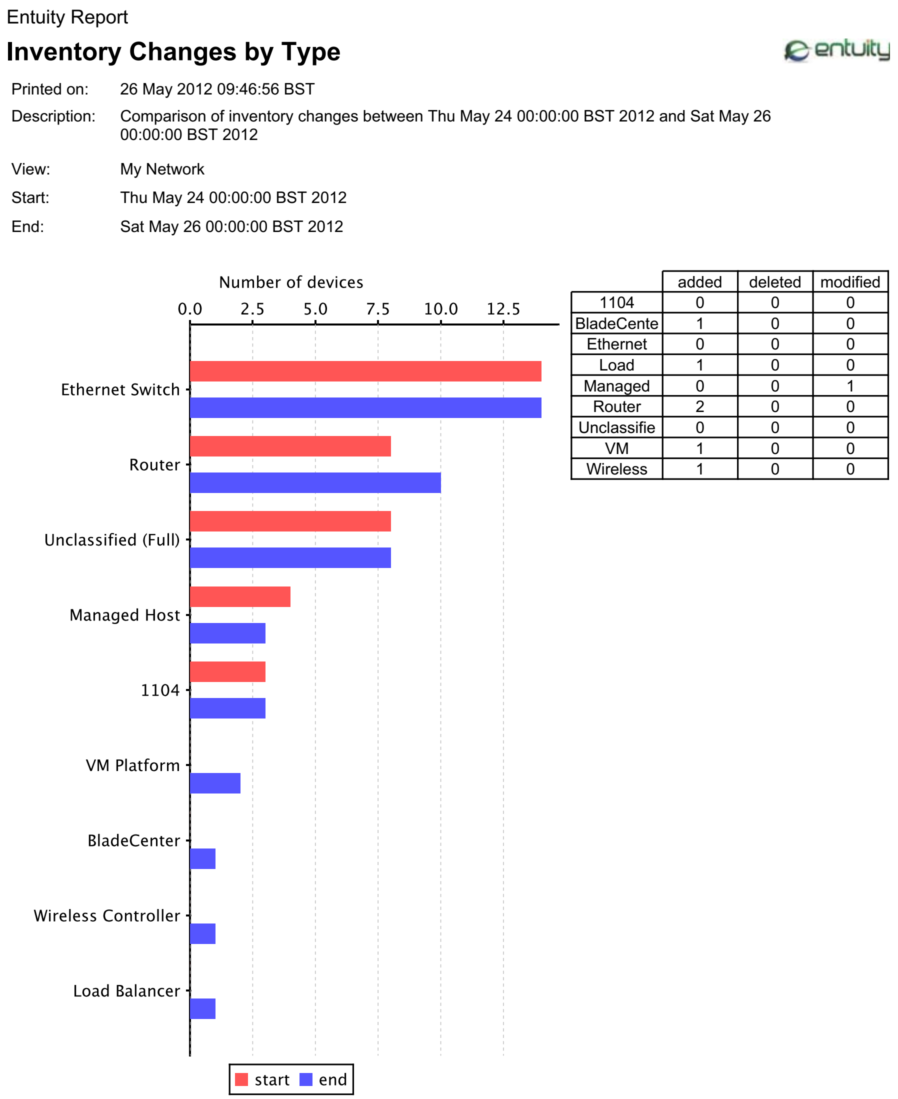
1) Click **Administration > Inventory / Topology > Inventory Snapshots**.
2) Click the check box against the schedule.
3) Click Delete Schedule(s).

### Run an Inventory Change Report

The Inventory Change report compares two inventory snapshots and identifies the changes between the two. You can configure which snapshots to use, whether to identify changes by device type, manufacturer or model, whether to include only inventory changes. Tables within the report identify the changed devices and/or attributes.

To run an Inventory Change report.

1) Click **Reports**.
2) Click **Inventory Reports**.
3) Click **Inventory Change**.
4) Define and run the report. (See the *Entuity Reports Reference Manual*.)



Entuity Report

**Inventory Changes by Type**

Printed on: 26 May 2012 09:46:56 BST

Description: Comparison of inventory changes between Thu May 24 00:00:00 BST 2012 and Sat May 26 00:00:00 BST 2012

View: My Network

Start: Thu May 24 00:00:00 BST 2012

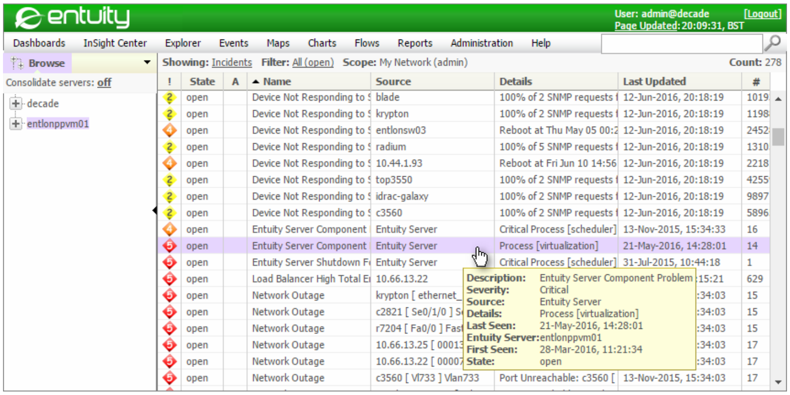
End: Sat May 26 00:00:00 BST 2012

| | added | deleted | modified |
|---|---|---|---|
| 1104 | 0 | 0 | 0 |
| BladeCente | 1 | 0 | 0 |
| Ethernet | 0 | 0 | 0 |
| Load | 1 | 0 | 0 |
| Managed | 0 | 0 | 1 |
| Router | 2 | 0 | 0 |
| Unclassifie | 0 | 0 | 0 |
| VM | 1 | 0 | 0 |
| Wireless | 1 | 0 | 0 |

Figure 274 Inventory Changes by Type Report

# Check Event Management System Health

Entuity monitors the performance of the event system. For example by default the event system supports 50000 incidents. Entuity alerts you as that limit is approached and when it is reached raises an Entuity Server Component Problem incident. You can click on the incident to view its details. An Entuity Server Component Problem incident also updates the Events indicator on the Health Summary page, from which you can click through to the Events Health page.



Showing: Incidents Filter: All (open) Scope: My Network (admin) Count: 278

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| 2 | open | | Device Not Responding to S | blade | 100% of 2 SNMP requests f | 12-Jun-2016, 20:18:19 | 1019 |
| 2 | open | | Device Not Responding to S | krypton | 100% of 2 SNMP requests f | 12-Jun-2016, 20:18:19 | 1198 |
| 4 | open | | Device Not Responding to S | entlonsw03 | Reboot at Thu May 05 00:2 | 12-Jun-2016, 20:18:19 | 2452 |
| 2 | open | | Device Not Responding to S | radium | 100% of 5 SNMP requests f | 12-Jun-2016, 20:18:19 | 1310 |
| 4 | open | | Device Not Responding to S | 10.44.1.93 | Reboot at Fri Jun 10 14:56 | 12-Jun-2016, 20:18:19 | 2218 |
| 2 | open | | Device Not Responding to S | top3550 | 100% of 2 SNMP requests f | 12-Jun-2016, 20:18:19 | 4255 |
| 2 | open | | Device Not Responding to S | idrac-galaxy | 100% of 2 SNMP requests f | 12-Jun-2016, 20:18:19 | 9897 |
| 2 | open | | Device Not Responding to S | c3560 | 100% of 2 SNMP requests f | 12-Jun-2016, 20:18:19 | 5896 |
| 4 | open | | Entuity Server Component | Entuity Server | Critical Process [scheduler] | 13-Nov-2015, 15:34:33 | 16 |
| 5 | open | | Entuity Server Component | Entuity Server | Process [virtualization] | 21-May-2016, 14:28:01 | 14 |
| 5 | open | | Entuity Server Shutdown Fa | Entuity Server | Critical Process [scheduler] | 31-Jul-2015, 10:44:18 | 1 |
| 5 | open | | Load Balancer High Total Er | 10.66.13.22 | | :15:21 | 629 |
| 5 | open | | Network Outage | krypton [ ethernet_ | | :34:03 | 15 |
| 5 | open | | Network Outage | c2821 [ Se0/1/0 ] Se | | :34:03 | 15 |
| 5 | open | | Network Outage | r7204 [ Fa0/0 ] Fast | | :34:03 | 15 |
| 5 | open | | Network Outage | 10.66.13.25 [ 00013 | | :34:03 | 17 |
| 5 | open | | Network Outage | 10.66.13.22 [ 00007 | | :34:03 | 17 |
| 5 | open | | Network Outage | c3560 [ Vl733 ] Vlan733 | Port Unreachable: c3560 [ | 13-Nov-2015, 15:34:03 | 17 |

| | |
|---|---|
| Description: | Entuity Server Component Problem |
| Severity: | Critical |
| Source: | Entuity Server |
| Details: | Process [virtualization] |
| Last Seen: | 21-May-2016, 14:28:01 |
| Entuity Server: | entlonppvm01 |
| First Seen: | 28-Mar-2016, 11:21:34 |
| State: | open |

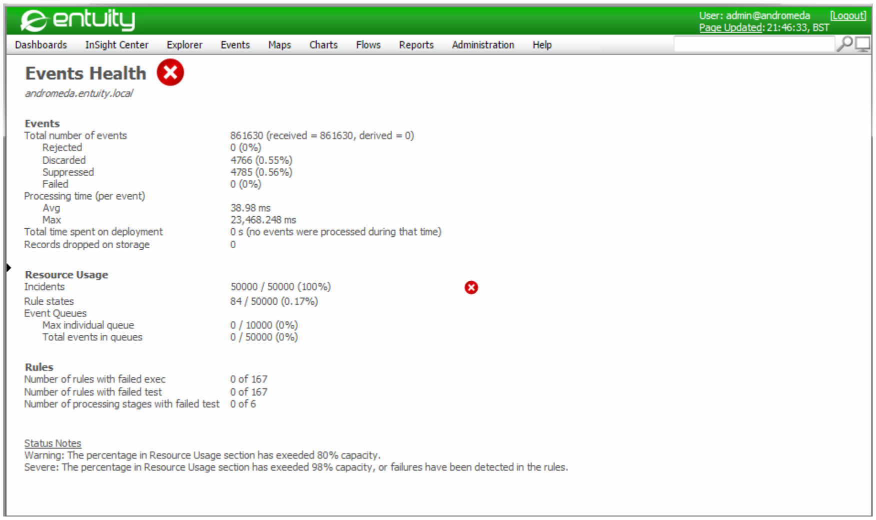
Figure 275 Entuity Server Component Problem Incident

From the Events Health page you can monitor the performance of the event system, its event handling, resource usage and rule application performance.

The events metrics are a snapshot taken at the time the report is run, the resource usage and rules generated metrics are reset at the time of the last event project deployment or the event engine was restarted, whichever is the latest.

To access the Entuity Events Health page:

1) Click **Administration** > **Entuity Health** > **Events Health**.



Events Health ✖

*andromeda.entuity.local*

| **Events** | |
|---|---|
| Total number of events | 861630 (received = 861630, derived = 0) |
| Rejected | 0 (0%) |
| Discarded | 4766 (0.55%) |
| Suppressed | 4785 (0.56%) |
| Failed | 0 (0%) |
| Processing time (per event) | |
| Avg | 38.98 ms |
| Max | 23,468.248 ms |
| Total time spent on deployment | 0 s (no events were processed during that time) |
| Records dropped on storage | 0 |
| **Resource Usage** | |
| Incidents | 50000 / 50000 (100%) ✖ |
| Rule states | 84 / 50000 (0.17%) |
| Event Queues | |
| Max individual queue | 0 / 10000 (0%) |
| Total events in queues | 0 / 50000 (0%) |
| **Rules** | |
| Number of rules with failed exec | 0 of 167 |
| Number of rules with failed test | 0 of 167 |
| Number of processing stages with failed test | 0 of 6 |

Status Notes
Warning: The percentage in Resource Usage section has exeeded 80% capacity.
Severe: The percentage in Resource Usage section has exeeded 98% capacity, or failures have been detected in the rules.

Figure 276 Events Health

| Metric | Description |
|---|---|
| **Events** | Event metrics are since the last event project deployment or the last restart of the event system, whichever is the latest. |
| *Total number of events* | The total number of events received broken down by those received into the event system and those derived within it. Total events are then categorized:<br>■ Rejected, events not accepted into the event system.<br>■ Discarded, events tested and then discarded, for example during the port state enable test.<br>■ Suppressed events, for example through n of m rules.<br>■ Failed, events that failed to be correctly processed. |
| *Processing time (per event)* | Average and maximum processing time per event. |
| *Total time spent on deployment* | The length of time taken to deploy an event project. The more deployments, the more complex the event project the greater the potential to miss events. |
| *Records dropped on storage* | Event records that could not be saved. |
| **Resource Usage** | Resource metrics are current usage values. |
| *Incidents* | The total number incidents, the maximum supported number of incidents permitted and the current usage percentage. |
| *Rule states* | Number of rules events generated through rules. |
| *Event Queues* | Number and size of event queues. |
| **Rules** | |
| *Number of rules with failed exec* | Executables can be incorporated into event actions. |
| *Number of rules with failed test* | Tests can be incorporated into event rules, invalid tests maybe caused due to incompatible data in some events. |
| *Number of processing stages with failed test* | Tests can be incorporated into event rules, invalid tests maybe caused due to incompatible data in some events. Rules are processed through stages. |

Table 78 Events Health Metrics

## Investigate Incident Resource Usage

By default the event system supports 50000 incidents and Entuity alerts you as usage hits 80% and when it passes 98% it raises an Entuity Server Component Problem incident.

To investigate incident resource usage:

1) From Event Viewer highlight the Entuity Server Component Problem incident and from the context menu click **Show Details**.

   Entuity identifies the eventEngine as the problem component. You can review the Events Health page.

2) Click **Administration** > **Entuity Health** > **Events Health**. Resource usage shows the

limit on the number of supported incidents and also the number of current incidents.

When the incident limit is reached Entuity expires out the incident with the oldest last updated date. You can manually close and expire incidents.

You should investigate whether the current incident limit is appropriate to your installation. It maybe that an anomaly has created a spike of incidents, or that the limit is too low. You can amend the limit through `maxSituationCount` in *entuity_home*\etc\`event-engine-cfg-template.properties`.

# 45 Entuity RESTful API

The Entuity implementation of a Representational State Transfer (RESTful) API provides a uniform interface for clients to access Entuity server functionality. In a RESTful API the client requests contain all the information required to process the request and the server does not store any state from previous requests.

The RESTful API is accessible via the HTTP and HTTPS communication protocols and is exposed via URLs under the `/api` path. For example you can access the information resource, depending upon your communication protocol, through

`http://`*`entuity_server`*`/api/info`

`https://`*`entuity_server`*`/api/info`

The Entuity RESTful API:

- Includes an extensive set of resources and methods. (See the *Entuity System Administrator Reference Manual*.)

| Resource | Method | Description |
|---|---|---|
| `domainFilters` | `GET` | Returns a list of the domain filters on the connected server. |
| `eventFilters` | `GET` | Returns a list of the event filters on the connected server. |
| `incidentFilters` | `GET` | Returns a list of the incident filters on the connected server. |
| `info` | `GET` | Lists server details. |
| `inventory` | `GET`<br>`POST` | Returns a list of the devices managed by the server.<br>Adds devices to the server. |
| `inventory/`*id* | `DELETE`<br>`GET`<br>`PUT` | Deletes the selected device from the server.<br>Returns details on the selected device.<br>Updates the specified attributes on the selected device. |
| `servers` | `GET` | Lists the connected server and its remote servers. |
| `servers/`*id* | `GET` | Returns details on the specified server. |
| `userGroups` | `GET` | Returns a list of the user groups on the server. |
| `users` | `GET` | Returns a list of the users on the server. |
| `version` | `GET` | Returns the Entuity implementation version of its RESTful API. |
| `views` | `GET`<br>`POST` | Returns a list of views on the server.<br>Adds views to the server. |
| `views/`*id* | `DELETE`<br>`GET`<br>`PUT` | Deletes the specified view (and any of its sub-views).<br>Returns details on the specified view.<br>Updates attributes of the specified view. |
| `views/`*id*`/objects` | `DELETE`<br>`GET`<br>`PUT` | Deletes the specified item from the specified view.<br>Returns details on the specified item in the specified view.<br>Adds the specified item to the specified view. |

Table 79 RESTful API Resources and Methods

- Allows remote running of scripts so you do not have to login and run scripts directly on the server hosting the Entuity software, e.g. through a console. Instead you can run scripts on a client machine and access the automation API through a remote procedure call with the Entuity server.
- Allows access based on Entuity user accounts. It will honor the permissions and views assigned to the logged in user (just like the web UI).
- access to all servers through a single central server. Multi-server support is similar to using the web UI in unconsolidated mode, for example:
  - In the web UI you must select the server on which you apply the operation.
  - From the Restful API you must specify the server on which to apply the operation. If you do not specify the server then the operation is applied to the local server.
- Make use of standard and modern scripting tools.

For details on the Entuity RESTful API refer to the *Entuity System Administrator Reference Manual*.

## Uniform Interface

The RESTful API provides a uniform interface using HTTP methods to interact with server resources and the HTTP method used becomes the noun in the request type.

| Method | Purpose |
|---|---|
| GET | Retrieve information. For example: `http://entuity/api/servers` would retrieve a list of servers and `http://entuity/api/servers/s1` would return details about `server` s1. |
| PUT | Update a resource on the server. For example `http://entuity/api/devices/name/Sw1` would update the device named `Sw1`. |
| POST | Create a new resource. For example `http://entuity/api/views/top/subView/subView1` would create a new view. |
| DELETE | Remove a resource. For example: `http://entuity/api/views/oldView` would delete the view `oldView`. |
| OPTIONS | Retrieve a description of the resource. Depending on the media type requested, this may be either a Web Application Description Language (WADL) or an HTML document. The output will be automatically generated and will describe the resource and it's supported HTTP methods, media types. |

Table 80 HTTP methods used to interact with the API

## Accessing Remote Servers

The RESTful API allows a client to list the servers that are accessible from the local server and direct API requests to remote servers. To list the servers accessible from a server enter:

```
http://entuity_server/api/servers
```

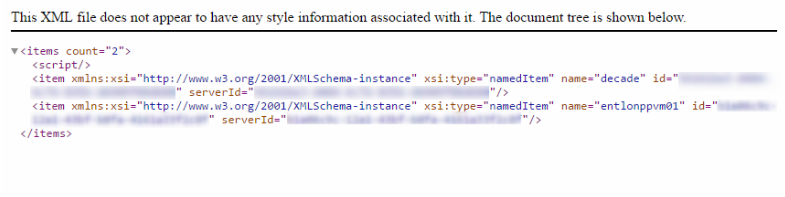
Where:

- *entuity_server* is the hostname of the Entuity server.

  If you are not logged into the server Entuity will prompt you to log in before running your query.

| Attribute | Description |
|---|---|
| xmlns:xsi= | Sets the namespace URI, identifying the schema:<br>`xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"` |
| xsi:type= | Sets the local definition of the element. |
| name= | Entuity server hostname. |
| id= | Unique Entuity server identifier. |
| serverId= | Unique Entuity server identifier. |

Table 45-1Entuity Servers API XML Response



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<items count="2">
   <script/>
   <item xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="namedItem" name="decade" id="[redacted]" serverId="[redacted]"/>
   <item xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="namedItem" name="entlonppvm01" id="[redacted]" serverId="[redacted]"/>
 </items>
```

Figure 277 Listing of Accessible Servers

API Requests can be directed to a remote server by adding either a server identifier or server name to the URI. For example to list he views on the accessed server enter:

```
http://entuity_server/api/views
```

By default HTTP methods operate on the resources local to the server you are accessing. If the server you are accessing has remote servers configured you can access any of them individually to apply an operation. You specify the server you want to apply the operation to using the `serverId` parameter. (See Table 45-1). For example the same Views request to a remote server would look like:

```
http://entuity_server/api/server/Id/4fdb4799-4ad3-4e8d-96e8-
7034bbbbba5d/views

http://entuity_server/api/server/name/remoteServer1/views
```

## Example Creating Views on Remote Servers

This example details how to use the RESTful API and curl to set up views on multiple Entuity servers:

- You should be able to access the Entuity server from a workstation with curl installed. You can run curl through an application or as a plug in for your browser.
- You will require Entuity administrator login credentials.

- The first stage is to recover the server identifiers. There are two servers in this example, `entlonppvm01` and `decade`.
- The second stage is to use the server identifiers when creating views.
- You can use this structure:

  ```
  curl -u username:password -H Content-Type:application/xml -X POST
  http://entuity_home/api/views?serverId=1234abcd-12345-123d-12ab-
  123456abcdef -d "<viewPathCreateRequest name='NE Region: County'
  parentViewPath='Customers' baseViewAggregation='NONE'/>"
  ```

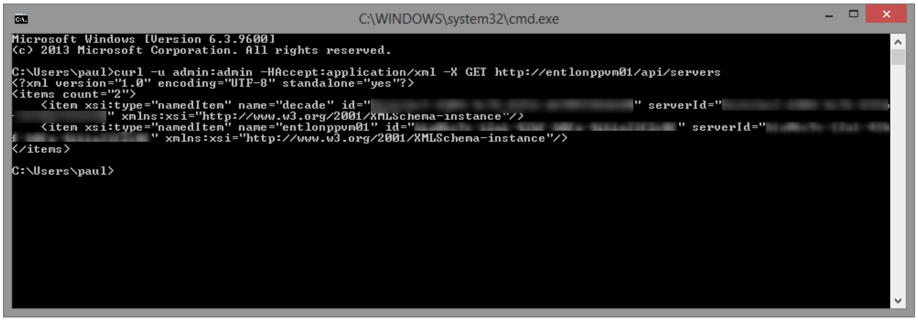
  to create the NE Region: County sub-view of Customers. You must amend the login credentials, Entuity server and *serverId*.

To retrieve the Entuity server identifiers:

1) From the command line enter:

   ```
   curl -u admin:admin -HAccept:application/xml -X GET http://
   entuity_home/api/servers
   ```

   Record the server names and identifiers.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\paul>curl -u admin:admin -HAccept:application/xml -X GET http://entlonppvm01/api/servers
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<items count="2">
    <item xsi:type="namedItem" name="decade" id="[redacted]" serverId="[redacted]
" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
    <item xsi:type="namedItem" name="entlonppvm01" id="[redacted]" serverId="[redacted]
" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
</items>

C:\Users\paul>
```

Figure 278 Listing of Accessible Servers Using curl

2) Build a curl command to create a view on a specific server, for example:

   ```
   curl -u admin:admin -H Content-Type:application/xml -X POST http://
   entuity_home/api/views?serverId=373ce3c5-9586-4e16-aa62-6d985d750445 -
   d "<viewPathCreateRequest name='NE Region: County' parent-
   ViewPath='Customers' baseViewAggregation='NONE'/>"
   ```

The use of quotes depends upon your curl setup. (See *Troubleshoot RESTful API*.)

3) You can now use these components to build a script, for example:
   - Use the list of serverId's and set up an array.
   - Use a variable to access the serverIds in the array when creating the views on each server.

# Self Documenting RESTful API

The RESTful API is self documenting using Web Application Description Language (WADL).

```
http://entuity_server/api?method=OPTIONS
```

Returns an XML describing the Entuity RESTful API, here is an example extract:

```
<?xml version="1.0" standalone="yes"?>
<?xml-stylesheet type="text/xsl" href="wadl2html.xslt"?>
<application xmlns="http://wadl.dev.java.net/2009/02">
   <doc title="Entuity API Server">Entuity API</doc>
   <resources base="http://localhost:8080/webUI/api/">
      <resource>
         <doc title="Root resource">The root resource of Entuity Rest
API</doc>
      </resource>
      <resource path="version">
         <method name="GET">
            <response>
               <representation mediaType="application/json"/>
               <representation mediaType="application/xml"/>
               <representation mediaType="text/xml"/></response>
         </method>
      </resource>
      <resource path="servers">
         <method name="GET">
            <response>
               <representation mediaType="application/json"/>
               <representation mediaType="application/xml"/>
               <representation mediaType="text/xml"/></response>
         </method>
      </resource>
```

# OPTIONS Method

You can get some simple information on resource's supported methods by issuing an OPTIONS method against a resource, or you can find all available resources by issuing an OPTIONS method against a root resource. For example, by using `curl` this command generates a lengthy output for all supported resources:

```
curl -X OPTIONS http://entuity_server/api/
```

This command generates available methods for the specified resource:

```
curl -X OPTIONS http://entuity_server/api/info
```

## Versioning of the RESTful API

All resources accessible via /api/* can also be accessed via /api/v1/*. Clients who wish to remain compatible with future versions of Entuity should use resources under the specific version: /api/v1/*. Resources without a version specifier under /api/* will contain the latest resource implementations and may be changed in future releases.

Resources under the specific version /api/v1/* may still be changed with the upgraded versions of Entuity but changes will be limited to compatible changes which are unlikely to break any integrations which make use of the api.

Compatible changes include:

- The addition of new authentication methods.
- The addition of new resources.
- The addition of new fields in resource representations returned.
- Require fewer inputs.
- Apply fewer constraints on input.

Incompatible changes will be added with a new version number, so the following URLs will be available:

- /api/v1/* will use version 1 of the API.
- /api/v2/* will use version 2 of the API which will include changes that are not compatible with previous versions.
- /api/* Will always track the latest version of the API.

Resources described in this document are described using URLs relative to their version base. For example, resource `info` can be accessed as `/api/info` or `/api/v1/info`.

## Authentication

Currently Entuity supports the basic HTTP authentication method (RFC 2617). Basic HTTP authentication is widely supported, and is completely insecure when used without SSL (password is sent in almost clear text). If you have security concerns Entuity Support recommend you use the RESTful API over HTTPS.

If using the curl tool, you can supply `-u username:password` arguments to provide authentication details.

✓ For performance reasons authentication results are cached on the server for five minutes after they are last used.

You can authenticate with any Entuity user and the resources are protected by using the Entuity permission model; users will only be able to access and modify resources that they have permission to access.

## Troubleshoot RESTful API

If you have to troubleshoot your RESTFUL API commands check:

- User account permissions. RESTful API is integrated with Entuity account management, the account credentials you use must be valid and the account must have the appropriate permission set to action your command.
- When executing POST operations that you include all the required information, for example when adding devices that you include the required information to manage a device. (See *Entuity Device Connection Attributes*.)
- For inadvertent inclusion of spaces.
- For casing issues. The RESTful API is case sensitive.
- That you are using straight quotes, curly quotes are not supported. Curly quotes may be inadvertently added to your commands if you are using a Word Processor to develop them.
- Your system's support of single and double quotes. The XML examples use double quotes enclosing single quotes, you could test whether your system is configured for single quotes enclosing double quotes. (See the *Entuity System Administrator Reference Manual*.)

✓ The curl examples included with the documentation have been verified using different versions of the generic curl install on both Windows and Linux operating systems.

# 46 Applying Entuity Maintenance Patches

Entuity Customer Support issue Release Notification and Patch Notification technical bulletins informing customers of new releases, maintenance patches and their content. These notifications are usually the trigger for updating your software.

The process to use when applying a new patch is different to that used when installing a new GA version of Entuity. A patch only includes changes that are applied to an existing installation, Entuity GA is a new ISO image.

This chapter details how to install maintenance patches. To download and install the Entuity GA ISO image see the *Entuity Getting Started Guide*.

| Name | Description |
|---|---|
| GA | The first release of a new version of Entuity, e.g. Entuity 14.0, is the General Acceptance (GA) release. It is delivered as a compressed ISO image. |
| Patches | A patch may deliver fixes to issues raised by customers, improved performance and new features. You should always apply the patches in the order they are issued, e.g. one patch may depend upon a change delivered in a previous patch. |

Table 46 Entuity ISO Image and Patches

## Patch Install Overview

Follow these steps when installing patches:

1) Check the current Entuity version, including patch level, through the Entuity Health page.

   See *Checking the Patch Level of Entuity*.

2) From the Entuity customer support site download the patch file to a temporary location.

   See *Downloading Maintenance Patches*.

3) Stop the Entuity server and take a backup.

4) Apply the patch using the patch installer, *entuity_home*`\install\installPatch`, for example:

   ```
   installPatch c:\temp\EYE2011.P01_bmc.WinNT.patch
   ```

   See *Installing Maintenance Patches*.

5) After installing the patch run `configure`. The patch is only applied once `configure` successfully completes.

6) Restart the Entuity server.

## Checking the Patch Level of Entuity

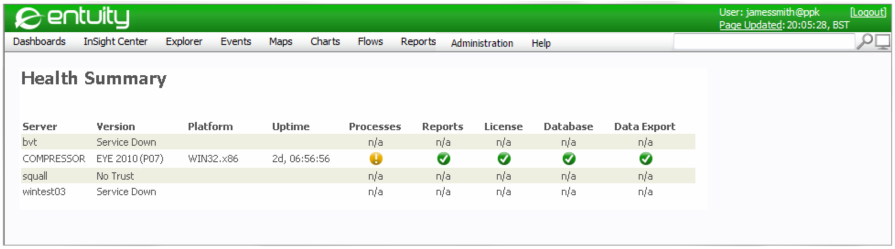
You must always install Entuity patches in the correct sequence. You should also never miss a patch, a subsequent patch may depend on a change in an earlier patch. `installPatch` does check that the patch is sequential with the current patch level of the server.

You can check the patch level of an Entuity server from the Health Summary page:

1) Click **Administration** > **Entuity Health** > **Health Summary**.

   *Version* indicates the Entuity release and patch level of the server. For example:

   - **Entuity 14.0** indicates this is the General Acceptance (GA) release, no patches are applied
   - **Entuity 13.5 (P02)** indicates 2 patches have been successfully applied



Health Summary

| Server | Version | Platform | Uptime | Processes | Reports | License | Database | Data Export |
|---|---|---|---|---|---|---|---|---|
| bvt | Service Down | | | n/a | n/a | n/a | n/a | n/a |
| COMPRESSOR | EYE 2010 (P07) | WIN32.x86 | 2d, 06:56:56 | ! | ✓ | ✓ | ✓ | ✓ |
| squall | No Trust | | | n/a | n/a | n/a | n/a | n/a |
| wintest03 | Service Down | | | n/a | n/a | n/a | n/a | n/a |

Figure 279 Entuity Maintenance Patch Level

## Downloading Maintenance Patches

Entuity Customer Support issue Patch Notifications informing customers through these technical bulletins of new maintenance patches, their content and confirmation of from where you can download them.

To download patches:

1) Login to the Entuity Customer Support site ( http://www.support.entuity.com/login.php) to view patch details, or login to the Entuity FTP site to download the patch (ftp.entuity.com).

   When you do not have an account, or have lost your account details contact your BMC representativeEntuity Customer Support.

2) Navigate to the required patch.

   Patches are stored by Entuity Release, e.g. `/Patches/13.5`Version_10_0.x/Linux`/`, `/Patches/13.0`Version_10_5.x/Windows`/`.

Entuity GA ISO image is available from the BMC Software electronic software distribution (ESD) site as compressed files.also available from the FTP site, but stored under the Images folder, e.g. `/Images/14.0/`.

3) Download to a temporary folder the required patch, associated readme and checksum files.

4) Compare the checksum of the patch against the expected hash value in checksums.txt.

   Linux operating systems include checksum utilities. In Windows environments you require a third party tool that supports SHA-1 or SHA-2 checksum calculation.

## Installing Maintenance Patches

You can install patches to Entuity from the command line using the `installPatch` utility. `installPatch` checks the patch is appropriate to the server, e.g. it's the correct Entuity version, operating system, Entuity is not running, and would raise an error if a check is failed (see *installPatch Warning and Error Messages*).

As `installPatch` applies a patch it displays its progress on screen, and reports the success or failure of its operation.

To install the downloaded maintenance patch:

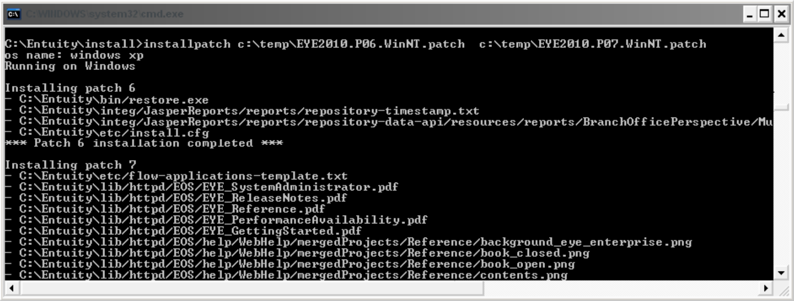
1) Stop the Entuity server and take a backup.

2) From the command line on the Entuity server run *entuity_home*`\install\installPatch` on the downloaded patch. For example with a Windows patch downloaded to the temporary folder `c:\temp`, enter:

   ```
   installPatch c:\temp\ENTUITY_13_5.P02_bmc.WinNT.patch
   ```

   Where you have more than one patch to install, you can use `installPatch` in multiple file mode. Enter the patches in sequence, using their full path with only a space between each, for example:

   ```
   installPatch c:\temp\ENTUITY_13_0.P01_bmc.WinNT.patch
   c:\temp\ENTUITY_13_0.P02_bmc.WinNT.patch
   c:\temp\ENTUITY_13_0.P03_bmc.WinNT.patch
   c:\temp\ENTUITY_13_0.P04_bmc.WinNT.patch
   ```



```
C:\Entuity\install>installpatch c:\temp\EYE2010.P06.WinNT.patch  c:\temp\EYE2010.P07.WinNT.patch
os name: windows xp
Running on Windows

Installing patch 6
- C:\Entuity\bin/restore.exe
- C:\Entuity\integ/JasperReports/reports/repository-timestamp.txt
- C:\Entuity\integ/JasperReports/reports/repository-data-api/resources/reports/BranchOfficePerspective/Mu
- C:\Entuity\etc/install.cfg
*** Patch 6 installation completed ***

Installing patch 7
- C:\Entuity\etc/flow-applications-template.txt
- C:\Entuity\lib/httpd/EOS/EYE_SystemAdministrator.pdf
- C:\Entuity\lib/httpd/EOS/EYE_ReleaseNotes.pdf
- C:\Entuity\lib/httpd/EOS/EYE_Reference.pdf
- C:\Entuity\lib/httpd/EOS/EYE_PerformanceAvailability.pdf
- C:\Entuity\lib/httpd/EOS/EYE_GettingStarted.pdf
- C:\Entuity\lib/httpd/EOS/help/WebHelp/mergedProjects/Reference/background_eye_enterprise.png
- C:\Entuity\lib/httpd/EOS/help/WebHelp/mergedProjects/Reference/book_closed.png
- C:\Entuity\lib/httpd/EOS/help/WebHelp/mergedProjects/Reference/book_open.png
- C:\Entuity\lib/httpd/EOS/help/WebHelp/mergedProjects/Reference/contents.png
```

Figure 280 Running installPatch

3) After installing the patch run `configure`. The patch is only applied once `configure` completes.

4) Restart the Entuity server.

# installPatch Warning and Error Messages

`installPatch` error and warning messages are displayed to the command line. When checking Entuity version, `installPatch` uses Entuity's internal version number, which is an abbreviated form of the release number, e.g. 8.1 corresponds to 8.0.01, 8.2 to 8.0.02. You can use the following table to identify the Entuity release number from its internal version number.

| Release Number | Internal Version Number |
|---|---|
| EYE 2008 | 6.0 |
| EYE 2009 | 7.0 |
| EYE 2009 SP1 | 7.1 |
| EYE 2010 | 8.0 |
| EYE 2010 SP1 | 8.1 |
| EYE 2010 SP2 | 8.2 |
| EYE 2011 | 9.0 |
| EYE 2012 | 10.0.0 |
| Entuity 12.5 | 12.5.0 |
| Entuity 13 | 13.0.0 |
| Entuity 13.5 | 13.5.0 |
| Entuity 14 | 14.0.0 |

Table 47 Mapping Entuity Version and Release Numbers

## Entuity installation not stopped

`installPatch` checks that the Entuity server is not running before installing the patch. If the Entuity installation has not been stopped `installPatch` displays an error message for example:

```
Port(s) 3306,3306,19191,80,20202,8080,8005 are in use
ERROR: The Entuity installation must be stopped before installing this
patch
```

## Patch already installed

If the patch has already been installed on the target Entuity server then you will be asked if you wish to re-install the patch:

```
This patch is already installed, do you wish to re-install it [yes/no]
?
```

## Patch out of sequence

If the preceding patch has not been installed on the target Entuity server then you will see an error message like this:

```
ERROR: You must install all patches up to patch number 4 before
installing this patch
```

### Later patches already installed

If patches later than the patch being installed have already been installed on the target then you will see an error message like this:

```
ERROR: This installation is already patched to level 7
```

### Patch is for different Entuity Version

If the patch being installed is for a different version of Entuity to the one installed then you will see an error message like this:

```
ERROR: This patch is for a different Entuity version, Patch is for 8.0
Installed version is 7.1
```

### Patch is for a different architecture

If the patch being installed is for a different architecture to the installation then you will see an error message like this:

```
ERROR: Incompatible patch architecture, this patch is for Linux
```

# 47 Troubleshooting System Problems

As a network management solution you can use Entuity to monitor and manage your network and identify potential and current infrastructure issues. You may also have to troubleshoot Entuity performance. Possible problems include:

- Connectivity Issues
- Device Polling Problems
- Data Missing and Problems with Database Backups
- Entuity Stops and Fails to Restart
- Device IP Address Lookup Problems
- Delay in Managed Object and Attribute Discovery
- Same Name VLANs Combined
- Incorrect Identification of Physical and Virtual Ports
- Incorrect Identification of Giant Packets as Faults
- Validating Utilization Metrics
- Linux Server Time Zones.

## Connectivity Issues

The types of connectivity problem that you may encounter include:

- Inability to communicate with the web server (see *Web Server Connectivity Problems*).
- Inability to communicate with the database (see *Database Connectivity Problems*).

### Web Server Connectivity Problems

To troubleshoot web server connectivity problems:

1) Use the `ping` utility to check connectivity to the management server at the IP layer.
2) If the server is responding to `ping`, log onto the server as the Entuity user with the requisite rights.
3) Check that there is an `httpd` web server process running on the management server. For example enter:

   ```
   ps -ef | grep httpd
   ```
4) If there is no `httpd` process running, use the `starteye` utility to start one.
5) If there is already an `httpd` process running, check the web server log files (see *Checking System Log Files*) to ascertain the cause of the problem. It may be necessary to kill the current processes, and restart them using `starteye`.

To troubleshoot web server connectivity problems if you are a Windows user:

- Use the Windows Task Manager to check that the `httpd` server is running. If it is:
  - Not running, wait a short while because it should restart automatically, otherwise use `starteye` or start the Entuity service to start one.
  - Running, check the web server log files to ascertain the cause of the problem. It may be necessary to restart Windows.

### Database Connectivity Problems

To troubleshoot database connectivity problems, proceed as follows:

1) Log into the management server as the Entuity user with the requisite rights.
2) Check that the Entuity processes are running. Click **Administration > Entuity Health > Processes**. Entuity displays the Process Health page which provides a status for each Entuity process.
3) If there are any processes not responding, check the appropriate log files and then shut down and restart Entuity.

## Device Polling Problems

You can use the `probity` utility to check whether a device has been discarded by the poller. If so, then the device polling time is deemed to be too long for management within the Entuity environment.

To troubleshoot the cause of SNMP polling failures for a device, you should interrogate the `prole` log file, *entuity_home*/`log/prole.log`, and look for any messages generated against the device name. Typical causes of SNMP polling failure include:

- Entuity could not communicate with the device via IP (caused by either a network problem or the fact that the device is down).
- An invalid SNMP read community string, e.g. the string has been changed on the device but not in Entuity.
- The SNMP access list for the device has been modified, blocking access to the management server.
- One or more SNMP response packets retrieved from the device are invalid (caused either by a bug in the device’s SNMP agent, or the corruption of UDP (User Datagram Protocol) packets by the network - turning on the UDP checksum may highlight the cause of the problem).
- The routing table of the management server indicates no route to the IP address of the device.
- The device name could not be resolved to an IP address (check the local hosts file or the applicable name service).

### SNMPv3 and End Host Discovery

Entuity may not be able to discover all end host information from devices being managed via SNMPv3 due to a lack of support for VLANs in the SNMP agent of the device. Only end hosts

(MACs) on default VLANs are discovered. This is a known limitation in several device agents, including Cisco.

The areas of Entuity that can be impacted by the lack of end-host information are:

- Maps may not be able to accurately determine uplink connections between layer 2 switches and layer 3 routers.
- End Host Configuration Changes may not be detected.

You can configure some newer SNMPv3 Cisco devices to provide VLAN information using SNMPv3 contexts, for example this command configures a device to automatically create an SNMPv3 context for each VLAN:

```
snmp-server group mygroup V3 auth context vlan- match prefix read
myread write mywrite notify mynotify
```

For older Cisco devices you can explicitly configure a context for each VLAN, for example:

```
snmp-server group mygroup v3 noauth context vlan-99
```

Consult the device documentation on which command is appropriate for a particular device.

When you have configured these devices Entuity will use SNMPv3 contexts to extract VLAN host information.

✓ If Entuity is managing a device through its SNMPv3 context then you cannot also use the SNMPv3 contexts to extract VLAN information.

You can change the **vlan-** prefix by setting `snmpVlanContextPrefix` in *entuity_home*\\`entuity.cfg`, for example:

```
snmpVlanContextPrefix=cVLAN-
```

If a device does not support SNMPv3 contexts, then to access the VLAN host information you could manage the device using SNMPv2.

## Data Missing and Problems with Database Backups

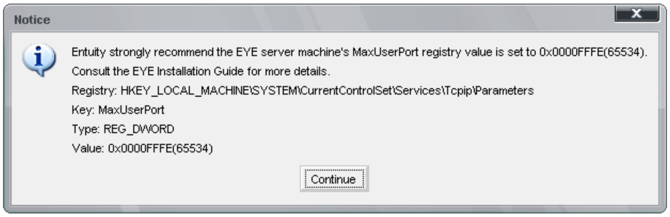
The Entuity server continually uses and releases sockets, for example when running `prole` and `fpprole`. These sockets once released only become free again after a time-out period. When running the Entuity server in a Windows environment and monitoring large networks Window's default maximum number of user ports maybe reached. Without available sockets Entuity performance is severely impacted. For example the creation of new `prole` and `fpprole` processes is prevented and so data collection becomes unreliable.

In Windows Entuity recommend the registry key value MaxUserPort is set to 0x000fffe (65534). Define the new key value as:

- *Key*: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
- *Type*: REG_DWORD
- *Value*: 0x000fffe (65534).

Care should always be taken when changing your system registry.

Entuity `configure` checks the server machine has MaxUserPort set, when it is not set, or set to a lower value than Entuity recommend, a warning notice is given. Configuration can continue past the warning notice.



Entuity strongly recommend the EYE server machine's MaxUserPort registry value is set to 0x0000FFFE(65534).
Consult the EYE Installation Guide for more details.
Registry: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Key: MaxUserPort
Type: REG_DWORD
Value: 0x0000FFFE(65534)

Figure 281 Maximum User Port Notice

## Entuity Stops and Fails to Restart

Entuity may stop and/or fail to restart when:

- The license is invalid, for example it has expired. Entuity would raise Entuity Server License Alert events warning of an imminent failure. When using a central license server Entuity raises events that identify the failing server, for example License Client License Expired.

  You should obtain a valid license file from your Entuity representative and replace the expired license. For a license with the same name you only have to stop and restart the Entuity server for the new license to take effect. (See the *Entuity Getting Started Guide.*)
- There is insufficient disk space. Entuity would generate events in Event Viewer warning of potential disk space problems on its server. Also check `diskmonitor.log` for a history of disk space usage. You should obtain a larger disk or make more space available.
- Incorrect amendments to Entuity's configuration, which may result in processes not starting or database corruption. This may only be identified through examination of Entuity log files. when unsure of why Entuity has failed contact your Entuity support desk.

## Device IP Address Lookup Problems

Entuity Search allows you to find workstations and servers in the network.

The `macman` (Media Access Control Management) process gathers MAC-related information from devices, indicating on which port a particular MAC address resides. To identify the IP address, Entuity performs a lookup of the MAC address in the ARP (Address Resolution Protocol) caches of the router ports that reside in the same IP network as the device port.

If end users are having problems resolving IP addresses:

1) Check whether Entuity has stored the MAC address of the respective workstation/server (use the Search tool).

2) If so, then check whether Entuity knows of any router ports in the same IP network as the port on which the MAC address resides.

3) If no router ports are known in this IP subnet, then you should check whether all the necessary routers have been added to the management environment.

## Delay in Managed Object and Attribute Discovery

Entuity attempts to balance discovery of network objects, the collection of data on those objects and keeping the information current against the demands this places on Entuity server resources. This balance can result in a time difference between an object, e.g. switch, being discovered, and its attributes, e.g. inventory, being fully displayed. For example if using `autoDiscovery`:

1) It (or more accurately `proliferate` which runs according to the parameters passed to it by `autoDiscovery`) discovers a switch. This may only take minutes, it depends on your network.

2) After adding the switch to its inventory the Entuity server can run object discovery on the device to determine its attributes. How quickly object discovery runs after the device is added is dependent upon the server load.

3) After the switch attributes are discovered the final stage is polling those attributes. Different attribute types have different polling schedules, for example switch inventory information is polled every 12 hours, CPU utilization every 5 minutes.

This effect is noticeable after:

- Installing Entuity the time of the initial discovery varies according to the size of the infrastructure and network. The secondary discovery completes object details, for example device links. After the Entuity discovery completes, collection of data for each of the discovered attributes depends upon their polling schedule.
- Adding an Amazon Web Service (AWS) VM Platform. The virtualization process runs every 60 minutes so there may potentially be a 60 minute delay before the Inventory Administration page displays the correct status information.
- Adding objects that Entuity had previously managed. It may take from 15 minutes upwards for the object to appear, i.e. until Entuity discovery runs. Once discovered attributes for the object will be populated only when their collectors run.

  A delay is also possible when Extended Info attributes have been reset to use discovered values through Reset User Override.

When you add a mixture of devices, some Entuity has previously managed some it has not, those it has previously managed take longer to discover than those it has never managed.

When Entuity manages thousands of objects, discovery is effectively continually running; the time between discovery cycles is shorter than the time taken to complete a discovery cycle. This is normal behavior and can explain why Entuity can take longer than the fifteen minute cycle to discover some objects.

Entuity collectors are configured to poll at rates that reflect the likely pace of attribute change, e.g. switch inventory data changes infrequently and is polled every 12 hours, router traffic data changes more frequently and by default is collected every 3 minutes.

Contact your Entuity representative if you want to amend or discuss amending polling configuration.

# Same Name VLANs Combined

When running VLAN reports you may notice Entuity has combined data from VLANs that have the same name. This combining of VLANs can occur where your network is using disparate network equipment that does not recognize the other's VLAN numbering.

Also, Entuity does not currently recognize VTP domains names. These domain names allow VLANs within different VTP domains to use the same VLAN number, but still be uniquely identified. Entuity considers devices and ports from separate, but identically named, VLANs to be from the same one.

Entuity does allow you to:

- Automate separation of VLANs by domain.
- Manually reassign ports and devices to different, or even new VLANs.

## Automatic Device to VLAN Assignment

Entuity's `vtpDomainTool` renames VLANs by combining their VLAN and VTP domain names. Devices are assigned to these renamed VLANs. `vtpDomainTool` also creates a new view, **All Objects by VTP**, which orders VLANs by domains.

`vtpDomainTool` must be run on a regular basis to maintain the accuracy of the renamed VLANs. This is best achieved through scheduling it in `provost.conf`.

## Manual Device to VLAN Assignment

You can select a VLAN associated to a device and assign it a new identifier for use within Entuity, i.e. you are not amending a value on the device only within the Entuity database. Entuity retains the original VLAN identifier which you can restore.

To reassign a device to another VLAN:

# Incorrect Identification of Physical and Virtual Ports

Entuity distinguishes between physical and virtual ports by using their interface type and then comparing it to a list of types that Entuity recognizes as physical ports. For certain port types, e.g. Frame Relay, then collectors are used to gather more information to distinguish between virtual and physical ports.

On the port's Extended Info tab *Classification* can be set to:

- Physical, for a physical port.
- Virtual, for a virtual port.

The distinction between virtual and physical ports is important when calculating spare ports, i.e. you do not want to identify a virtual port as spare. There may be occasions where the default configuration wrongly identifies the port's physical/virtual status, when this occurs for a:

- Small number of ports then you can manually set the port's *Virtual Indicator to the correct value.*
- Port type then the configuration file can be amended to correctly identify the port type. You should contact your Entuity representative to discuss configuration modification.

To amend a port's physical/virtual identification:

## Incorrect Identification of Giant Packets as Faults

The giant fault counter may be incremented for inbound packets which are not in error and which are transmitted normally. This happens on the main high end Cisco switches, for example the 6500 family. Examples of when this error occurs include:

- 802.1Q tagged packets on trunks (and other tagged ports such as certain uplinks and high-end server ports) which exceed the normal maximum transmission unit.
- 10 Gigabit ports.
- Certain Storage Area Network technologies.

Currently Cisco do not have a solution to correct this problem. You can configure `prodigy` so that it excludes giants from error calculations, i.e. events.excludeGiants in `entuity.cfg`.

Excluding giants impacts:

- Events, specifically WAN Port High Inbound Errors, Port Inbound Fault High (Packet Corruption)
- Port Fault Details report's charting of giant data.
- Inbound fault data displayed through the Fault chart tool.

## Validating Utilization Metrics

By default Entuity utilization metrics use values retrieved from managed devices to identify their capability, but these may not always be correct. For example, in Frame Relay environments port line speed and DLC CIRs are usually set within equipment that is external to the managed routers, and the values returned by the routers are manually configured by network administrators. This dependence on manually setting of device values, means there is scope for inaccuracy through administrators:

- Entering incorrect values through human error.
- Never changing the settings from their factory shipped defaults.
- Setting values once but then failing to update them as the line speeds or CIRs are changed.
- Deliberately setting bandwidth statements to values other than the real line speeds to influence routing behavior.

Entuity recommend administrators validate that line speeds Entuity discovers are a true reflection of the network, particularly WAN port and Frame Relay DLCI CIR line speeds.

## Linux Server Time Zones

When the TZ environment variable is not set on Linux servers, the servers use the default time zone, GMT. When GMT is not the server’s time zone this causes data synchronization problems in certain reports. For example running a report in EST to show port utilizations of switches from 07:00-19:00 the report would actually cover from 11:00-23:00.

# 48 Entuity Custom Menus

Custom Menus provide a mechanism to add user defined functions to Entuity, for example pinging a device, performing an SNMP walk of a device, opening a third party tool and supplying the Entuity context. You can configure Custom Menus so they are available as functions that are:

- Initiated by the user from global or context sensitive menu items for example from Event Viewer, Search.
- Automatically triggered by Entuity events.

You define Custom Menus through configuration files, which are included to the Entuity server through `sw_menu_def_site_specific.cfg` which Entuity reads during discovery.

Contact Entuity for details on how Custom Menu configuration files are constructed, the underlying concepts and an introduction to the Simple Statement Language often used to deliver the Entuity context.

## Installing and Configuring Custom Menu

Entuity includes a set of Custom Menu definitions. In `sw_menu_example.cfg` there are a set of useful example actions that can also provide the basis for more advanced customisations.

This section assumes default file names and locations were accepted during Entuity installation and configuration. When this is not the case, please adjust these instructions accordingly.

To activate Custom Menu configuration:

1) Create and save the configuration file to *entuity_home*/`etc`. Alternatively use the supplied example file, `sw_example_menu.cfg`, which is already installed to that location.

2) Include the Custom Menu configuration to Entuity. In *entuity_home*/`etc` open `sw_menu_def_site_specific.cfg` and add the name of the file containing the configuration, for example:

   ```
   !sw_menu_example.cfg
   ```

   Discovery of a new configuration can take approximately twenty minutes.

3) Open an Entuity client. As the client opens it requests the latest Custom Menu configuration.

It is only when you open the Entuity client that it checks for the latest discovered Custom Menu. Discovery that occurs when the client is open can only be viewed by closing and re-launching it.

## Defining Custom Menus

Each action is specified through its own individually named section in a configuration file. For example the Ping_Device_Client section defines a custom menu that runs from the Entuity server machine and pings the device selected from Entuity:

```
[MenuItem Ping_Device_Server]
displayName=At Server
actionMethod=simple;"ping.exe"
actionArguments=simple;
=  variable newobj=DeviceEx(getObject(head(var.objList).swObjectId));
=  [ newobj.name ]
actionLocation=Server
actionOutput=Yes
actionType=Exec
parentMenuItem=Ping_Device
supportedApps=webUI
toolGroups=Show User Menus
itemPosition=0
supportedTypes=device
selectionLimit=1
actionTimeout=30000
filter=simple;1
```

| Parameters | Description |
|---|---|
| *MenuItem* | The unique name of each menu item. *MenuItem*:<br>■ Must be unique within the Entuity server, i.e. not only in their own configuration file but in all configuration files included to Entuity.<br>■ Is a mandatory parameter.<br>■ Must not contain any spaces. |
| *displayName* | The menu item name displayed in the user interface. It should be a short but meaningful description of the action. |

Table 48 Custom Menu Parameters

| Parameters | Description |
|---|---|
| *parentMenuItem* | References the menu item below which the current menu item is displayed. You can:<br>- Leave it blank when this menu item appears against the menu root.<br>- Enter another menu item's *menuItem* value, and this menu item appears beneath that item in the menu.<br>A parent menu should not have an associated action. It must only be used to hold child menu items (to improve the organization of your menu structure). |
| *selectionLimit* | The maximum number of user interface selections supported by a single invocation of a menu item action. For example some commands e.g. ping, SNMPwalk, only act on one object at a time and so the user should only be able to select one device from the web UI. |
| *itemPosition* | The position of the menu item within the list of menu items. When two items are given the same position Entuity sorts them alphanumerically. |
| *SupportedApps* | A comma separated list of Entuity client applications for which the menu item applies, i.e. **webUI** (web interface), **Remedy**. |
| *toolGroups* | When set to:<br>- **Show User Menus** you control which user groups have access to Custom Menus through the Show User Menus tools permission. Members of the Administrators group always have access.<br>- **Admin Only** then only members of the Administrators group have access to the menu.<br>- **Show Remedy** identifies the actions as specific to the Entuity Integration for BMC® Remedy AR System. |
| *actionMethod* | The action associated with the menu item, for example the application to run, the URL called. Actions are specified using the Entuity Simple Statement Language. |
| *actionArguments* | The arguments passed to the action. Arguments are specified using the Entuity Simple Statement Language. |
| *actionLocation* | The location where the action is performed. i.e. **Server** the Entuity server machine. |
| *actionOutput* | Identifies how the output of the Entuity client is handled:<br>- **Yes**, output is displayed by Entuity<br>- **No**, output is not displayed by Entuity<br>- **Url**, output is handled as a web URL, viewed on the Entuity client workstation's default web browser. |
| *actionType* | Type of menu item action:<br>- **Class**, *ActionMethod* is an Entuity Java class that will be instantiated and a method executed on it<br>- **Exec**, *ActionMethod* requires the system **exec** function<br>- **Echo**, *ActionMethod* command string is echoed to display and is not executed. |

Table 48 Custom Menu Parameters

| Parameters | Description |
|---|---|
| *actionTimeout* | The maximum elapsed time, in milliseconds, allowed for the action to execute. Entuity terminates the action process, and releases all of the associated resources, when the timeout period is exceeded. |
| *supportedTypes* | Comma separated list of StormWorks object types supported by item and instance based menu items. Type hierarchy is taken into account such that further derived types are included unless their exclusion is specifically listed. For example, the list **port, !wanPort** includes all port types, i.e. **port, portEx, llport, frport, atmport, hiCapPort** with the exception of **wanPorts**. |
| *Filter* | Optional attribute containing StormWorks Simple Statement Language method, which controls visibility of instance based menu item. |
| *supportedEventTypes* | Comma separated list of incident and event identifiers supported by event based menu items. You can specify event types using:<br>■ `<event group>:<event id>` which includes support for wildcards. For example: `10:*, 1:9` includes all events in event group 10, but from event group 1 only event 9.<br>■ `i#` to specify the entered number as an incident identifier, for example i804 identifies the AP Antenna Host Count High incident.<br>■ `e#` to specify the entered number as an event identifier, for example e804 identifies the AP Antenna Host Count High event.<br>■ `e*` where the asterisk wild-card specifies All events.<br>■ `i*` where the asterisk wild-card specifies All incidents. |

Table 48 Custom Menu Parameters

# Define Custom Menus as Menu Items

You can access Custom Menus as menu items through the Entuity context menu or toolbar.

## Types of Menu Items

Custom Menu supports four types of menu item:

- Global, Entuity displays these items within the Advanced Actions menu, which may be available through a number of client applications. As global items they appear on the menu regardless of the current context.
- Type, these items are associated with StormWorks object types. They are only available when the selected object(s) corresponds with their supported object type list. For example, a type menu item can be configured to display only when the current context is a device.
- Instance, these items are linked to specific instances of a StormWorks object type. They are only available when the selected object(s) match the supported object(s). For example, an instance menu item can be configured to display only when the current context is that of the particular device specified.
- Event, these items are associated with specific event types. When events of those types are raised in Event Viewer and highlighted, then these Event based menu items are available.

You can arrange menu items in a hierarchical layout by specifying their parent menu items. Where you have a number of menu items it improves the clarity of the menu structure.

✓ Entuity recommend placing Instance based menu items under a parent item. Whether an Instance based item is available is dependent on the current context matching the supported objects. Applying this filter can cause a slight delay as the Entuity server must perform the check, so placing it within a parent menu item ensures it is only called when required.

## Defining Automatic Custom Menus

Automatic Custom Menus are triggered not from selecting an item on a menu but from a preset condition being met and that event triggering an action. For example, you can configure Entuity so that when it raises a device down event in Event Viewer, it also automatically raises an action request or trouble ticket, complete with relevant details, in an integrated third party system.

### Example Automatic Forwarding of Events

The Entuity Remedy AR System integration is implemented using a number of both automatic and interactive Custom Menus. For example, when Event Viewer raises events in the specified view, then, by default, Entuity automatically raises associated action requests complete with source details.

This section from the integration file, `sw_remedy_menu_def.cfg`, configures the multiple action request - event action:

- Called Raise Multiple Incidents.
- That uses the `arforward` executable provided by Entuity, specified through *actionMethod.*
- That provides event information from the Entuity server, as configured through *actionArguments.*
- To allow all event types to generate an AR, as:

  ```
  supportedEventTypes=*:*
  ```

  where ***:*** is equivalent to *EventGroupID:EventID,* indicating all event groups and all events within those groups are enabled (see the *Entuity Events Guide* for a list of event and event group identifiers).

  ```
  # Create multiple AR entries for multiple events
  [MenuItem Event_Menu1_ARMultiple_HD]
  displayName=Raise Multiple Incidents
  actionMethod=simple;variable fps=get_config_var("FPS");
  = concat(get_config_var("ENTUITY_HOME"), fps, "integ", fps, "Remedy",
  fps, "arforward")
  actionArguments=simple;
  = variable fps=get_config_var("FPS");
  ```

```
= variable proto=if(get_config_var("server.ssl_enabled") == "true",
"https", "http");
= variable cfgFile = concat(get_config_var("ENTUITY_HOME"), fps,
"etc", fps, "arhelpdsk.cfg");
= flatten(
=   [ ["-file", cfgFile],
=   flatten(
=     foreach(var.eventList,
=          variable compId = concat(objCompId.compType, ".",
objCompId.compID_1, ".", objCompId.compID_2, ".", objCompId.compID_3);
=       ["-plist",
=               "-p1", concat("Event Incident from Eye (",
(head(var.eventList)).eyeServer, ")"),
=         "-p2", concat("Event ", typeDescr, " occurred on ",
var.eyeServer,
=         ".\nSource: ", objDescr, ".\nDetails: ", eventDetails,
".\nImpacted: ", impactDescr,
=         ".\nTime: ", ftime(timeStamp), ".\nUser: ", var.userId,
"\nURL: ",
=         concat(proto, "://", eyeServer, "/EOS/cgi/EYELauncher?--
user=",var.userId, ";--start=opener;--eosObjectID=", compId))]
=       )
=     )
=   ]
= )
actionLocation=Server
actionOutput=Url
actionType=Exec
parentMenuItem=Event_Remedy_HD
supportedApps=webUI
selectionLimit=10
toolGroups=Show Remedy
filter=
itemPosition=0
supportedEventTypes=*:*
selectionLimit=10
actionTimeout=30000
```

# Example Initiating Simple Actions from Entuity

The simplest menu items are not dependent on the context for their availability, or supply contextual information as part of their action. Launching an executable or URL from Entuity is relatively straightforward to implement.

## Launching Notepad from the Entuity

This section defines a menu item:

- Called Execute Notepad.
- That opens the Notepad executable from the Entuity client.
- As executable action, through *actionOutput*.

```
[MenuItem Global_Launch_Notepad]
displayName=Execute Notepad
parentMenuItem=
itemPosition=0
toolGroups=Show User Menus
actionMethod=simple;"notepad.exe"
actionArguments=[]
actionLocation=webUI
actionOutput=No
actionType=Exec
actionTimeout=30000
supportedApps=webUI
```

## Launching a URL from the Entuity Client

This section defines a menu item:

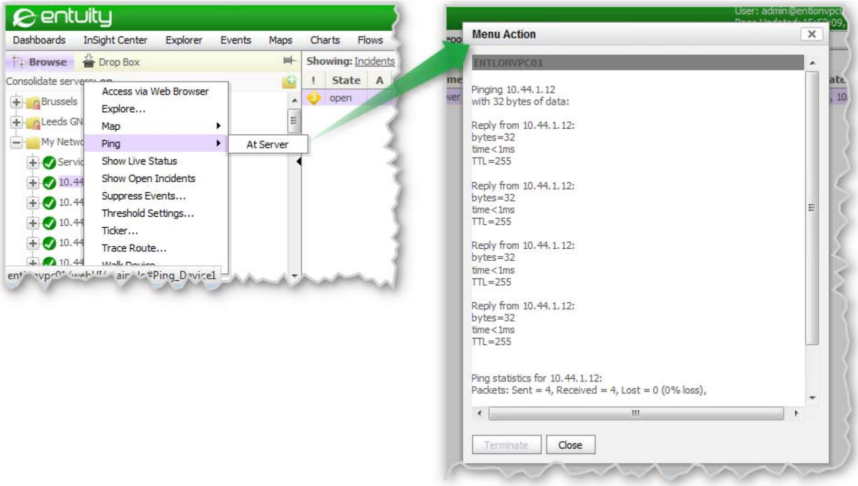
- Called Entuity Home.
- That opens the default browser on the Entuity client to view the home page of the Entuity website.
- As URL action, through *actionOutput*.

```
[MenuItem Global_Entuity_Home]
displayName=Entuity Home
parentMenuItem=
itemPosition=0
supportedApps=webUI
toolGroups=Show User Menus
actionMethod=simple;"http://www.entuity.com"
```

```
actionArguments=[]
actionLocation=Client
actionOutput=Url
actionType=Echo
actionTimeout=30000
supportedApps=webUI
```

## Example User Menu Hierarchy Using Ping Example

The Ping example from the sample configuration file includes a ping advanced action. The action is available as a menu item grouped within the parent **Ping** menu item.



```
Pinging 10.44.1.12
with 32 bytes of data:

Reply from 10.44.1.12:
bytes=32
time<1ms
TTL=255

Reply from 10.44.1.12:
bytes=32
time<1ms
TTL=255

Reply from 10.44.1.12:
bytes=32
time<1ms
TTL=255

Reply from 10.44.1.12:
bytes=32
time<1ms
TTL=255


Ping statistics for 10.44.1.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure 282 Hierarchical Custom Menu Running Ping

### Setting Parent Menu Items

This section defines a menu item that acts as the parent to the Ping action included in the sample configuration. As the parent item it:

- Does not reference its child menu items, and with *parentMenuItem* blank is set against the root menu, i.e. **Advanced Actions**.
- Does not include any actions of its own.

```
[MenuItem Ping_Device]
displayName=Ping
actionMethod=
actionArguments=
actionLocation=N/A
actionOutput=N/A
```

```
actionType=N/A
parentMenuItem=
itemPosition=0
supportedApps=WebUI
toolGroups=Show User Menus
actionTimeout=30000
supportedTypes=device
filter=simple;1
```

### Pinging the Current Device from the Entuity Server

This section defines a menu item:

- Called At Server.
- That pings the highlighted device from the Entuity server (this example is only valid when Entuity is installed in Windows environment).
- That is available from the web UI.

```
[MenuItem Ping_Device_Server]
displayName=At Server
actionMethod=simple;"ping.exe"
actionArguments=simple;
=  variable newobj=DeviceEx(getObject(head(var.objList).swObjectId));
=  [ newobj.name ]
actionLocation=Server
actionOutput=Yes
actionType=Exec
parentMenuItem=Ping_Device
supportedApps=WebUI
toolGroups=Show User Menus
itemPosition=0
supportedTypes=device
selectionLimit=1
filter=simple;1
actionTimeout=30000
```

## Example Application of Instance Custom Menu

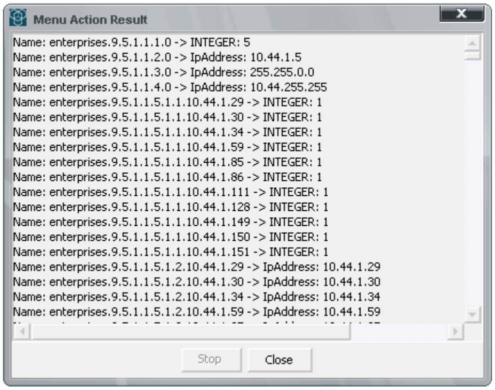
This section defines a menu item:

- Called Walk Device.

- That uses the `snmpwalk` executable with Entuity, specified through *actionMethod.*
- That provides an SNMP walk of the current device from the Entuity server, as configured through *actionArguments.*
- That is available on devices that meet the set *filter*, i.e. a system OID equal to .1.3.6.1.2.1.2.2.1.2

  You can amend the filter to another system OID or set it to apply to be available against all devices:

  ```
  filter=simple;1
  ```
- That outputs the SNMPdump results to a separate result window. As *selectionLimit* is set to 1, you cannot run another user action until it is closed, Entuity displays an appropriate information message if you attempt to do so.



```
Name: enterprises.9.5.1.1.1.0 -> INTEGER: 5
Name: enterprises.9.5.1.1.2.0 -> IpAddress: 10.44.1.5
Name: enterprises.9.5.1.1.3.0 -> IpAddress: 255.255.0.0
Name: enterprises.9.5.1.1.4.0 -> IpAddress: 10.44.255.255
Name: enterprises.9.5.1.1.5.1.1.10.44.1.29 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.1.10.44.1.30 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.1.10.44.1.34 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.1.10.44.1.59 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.1.10.44.1.85 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.1.10.44.1.86 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.1.10.44.1.111 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.1.10.44.1.128 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.1.10.44.1.149 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.1.10.44.1.150 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.1.10.44.1.151 -> INTEGER: 1
Name: enterprises.9.5.1.1.5.1.2.10.44.1.29 -> IpAddress: 10.44.1.29
Name: enterprises.9.5.1.1.5.1.2.10.44.1.30 -> IpAddress: 10.44.1.30
Name: enterprises.9.5.1.1.5.1.2.10.44.1.34 -> IpAddress: 10.44.1.34
Name: enterprises.9.5.1.1.5.1.2.10.44.1.59 -> IpAddress: 10.44.1.59
```

Figure 283 Menu Action Results Dialog

```
[MenuItem Walk_Device]
displayName=Walk Device
parentMenuItem=
itemPosition=0
supportedApps=webUI
toolGroups=Show User Menus
actionMethod=simple; concat(get_config_var("ENTUITY_HOME"), "/lib/
tools/snmpwalk")
actionArguments=simple;
=  variable devObj=DeviceEx(getObject(head(var.objList).swObjectId));
=  variable snmpCommunity=concat("-c", devObj.snmpCommunity);
=  [snmpCommunity, "-v1",  devObj.name, ".1.3.6.1.2.1.2.2.1.2" ]
actionLocation=Server
actionOutput=Yes
actionType=Exec
```

```
actionTimeout=30000
selectionLimit=1
supportedTypes=device
filter=
```

## Example Launching a User Action from an Event

This section defines a menu item:

- Called Display Event.
- That displays the device details of the highlighted event.
- That is only available in Event Viewer.

```
[MenuItem Event_Menu]
displayName=Display Event
actionMethod=simple;"The Event: "
actionArguments=simple;
=  foreach ( var.eventList, { eyeServer,eventNum,groupId,
 id,timeStamp,objCompId,priority,typeDescr,objDescr,impactType,
 impactDescr,eventDetails } )
actionLocation=Client
actionOutput=Yes
actionType=Echo
parentMenuItem=
supportedApps=WebUI
toolGroups=Show User Menus
itemPosition=0
supportedEventTypes=*:*
selectionLimit=1
actionTimeout=30000
filter=simple;1
```

# 49 Annotate Managed Objects

Through annotations you can share contact details for the staff responsible for particular incidents, keep records of irregular network behavior or acknowledge that a problem has been assigned.

Users that belong to a group that has Annotation Manager tool permission (enabled through Account Management) can add annotations by selecting the relevant component in Explorer or incident in Event Viewer. When an annotation is created, amended or deleted the change is immediately propagated to all open Entuity clients.

There are two separate sides to Entuity annotations:

- Annotations can be associated to incidents through Event Viewer.
- Annotations can be associated to network objects through their Summary tab.

## Incident Annotations

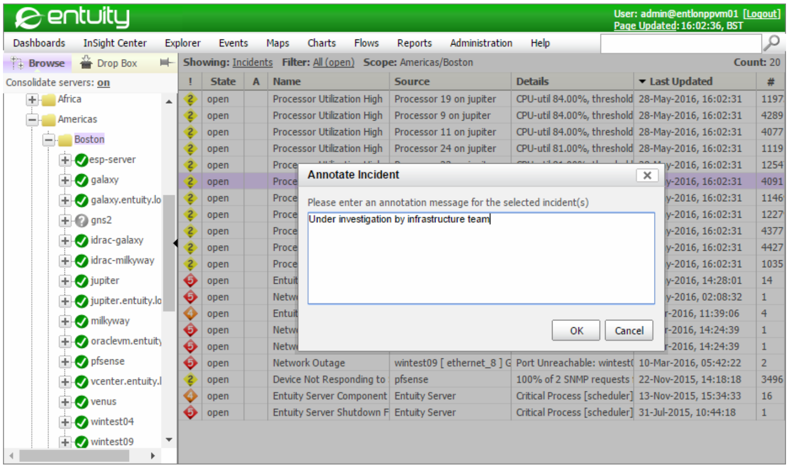
From Event Viewer you can associate annotations with the selected incident.

Event Viewer supports standard multi-select functionality; when selecting a contiguous set of events hold down the Shift key, when selecting non-contiguous events use the Control key.

To annotate an incident:

1) From Event Viewer highlight the required incident.
2) From the context menu click **Annotate**.
3) Enter an annotation, for example the course of action, who has ownership of the problem and click **OK**.

   The incident remains open but Entuity does identify it as annotated by adding an annotation icon to the incident’s annotation column, *A*.



**Showing:** Incidents **Filter:** All (open) **Scope:** Americas/Boston **Count:** 20

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| 2 | open | | Processor Utilization High | Processor 19 on jupiter | CPU-util 84.00%, threshold | 28-May-2016, 16:02:31 | 1197 |
| 2 | open | | Processor Utilization High | Processor 9 on jupiter | CPU-util 84.00%, threshold | 28-May-2016, 16:02:31 | 4289 |
| 2 | open | | Processor Utilization High | Processor 11 on jupiter | CPU-util 84.00%, threshold | 28-May-2016, 16:02:31 | 4077 |
| 2 | open | | Processor Utilization High | Processor 24 on jupiter | CPU-util 81.00%, threshold | 28-May-2016, 16:02:31 | 1119 |
| 2 | open | | Proce | | | y-2016, 16:02:31 | 1254 |
| 2 | open | | Proce | | | y-2016, 16:02:31 | 4091 |
| 2 | open | | Proce | | | y-2016, 16:02:31 | 1146 |
| 2 | open | | Proce | | | y-2016, 16:02:31 | 1227 |
| 2 | open | | Proce | | | y-2016, 16:02:31 | 4377 |
| 2 | open | | Proce | | | y-2016, 16:02:31 | 4427 |
| 2 | open | | Proce | | | y-2016, 16:02:31 | 1035 |
| 5 | open | | Entuit | | | y-2016, 14:28:01 | 14 |
| 5 | open | | Netw | | | y-2016, 02:08:32 | 1 |
| 4 | open | | Entuit | | | r-2016, 11:39:06 | 4 |
| 5 | open | | Netw | | | r-2016, 14:24:39 | 1 |
| 5 | open | | Netw | | | r-2016, 14:24:39 | 1 |
| 5 | open | | Network Outage | wintest09 [ ethernet_8 ] G | Port Unreachable: wintest( | 10-Mar-2016, 05:42:22 | 2 |
| 2 | open | | Device Not Responding to | pfsense | 100% of 2 SNMP requests | 22-Nov-2015, 14:18:18 | 3496 |
| 4 | open | | Entuity Server Component | Entuity Server | Critical Process [scheduler] | 13-Nov-2015, 15:34:33 | 16 |
| 5 | open | | Entuity Server Shutdown F | Entuity Server | Critical Process [scheduler] | 31-Jul-2015, 10:44:18 | 1 |

**Annotate Incident**

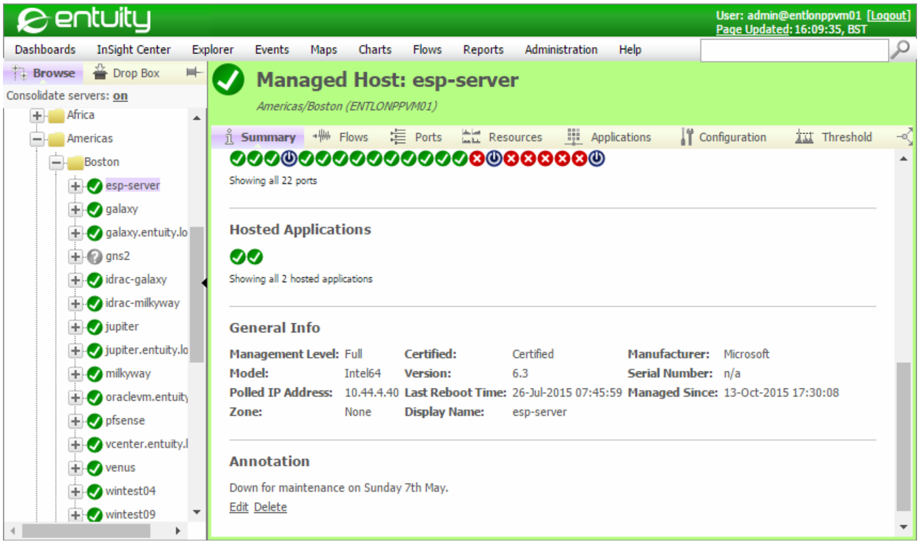
Please enter an annotation message for the selected incident(s)

Under investigation by infrastructure team

Figure 284 Event Viewer indicating Incidents with Annotations

# Network Device Annotations

Entuity associates a new annotation with the object you had selected when you started to create an annotation. Each component can only have one associated annotation. You add, view, edit and delete annotations from the Annotation section in the object’s Summary tab.



**Managed Host: esp-server**

*Americas/Boston (ENTLONPPVM01)*

Showing all 22 ports

**Hosted Applications**

Showing all 2 hosted applications

**General Info**

| | | | | | |
|---|---|---|---|---|---|
| **Management Level:** | Full | **Certified:** | Certified | **Manufacturer:** | Microsoft |
| **Model:** | Intel64 | **Version:** | 6.3 | **Serial Number:** | n/a |
| **Polled IP Address:** | 10.44.4.40 | **Last Reboot Time:** | 26-Jul-2015 07:45:59 | **Managed Since:** | 13-Oct-2015 17:30:08 |
| **Zone:** | None | **Display Name:** | esp-server | | |

**Annotation**

Down for maintenance on Sunday 7th May.

Figure 285 Device Annotations

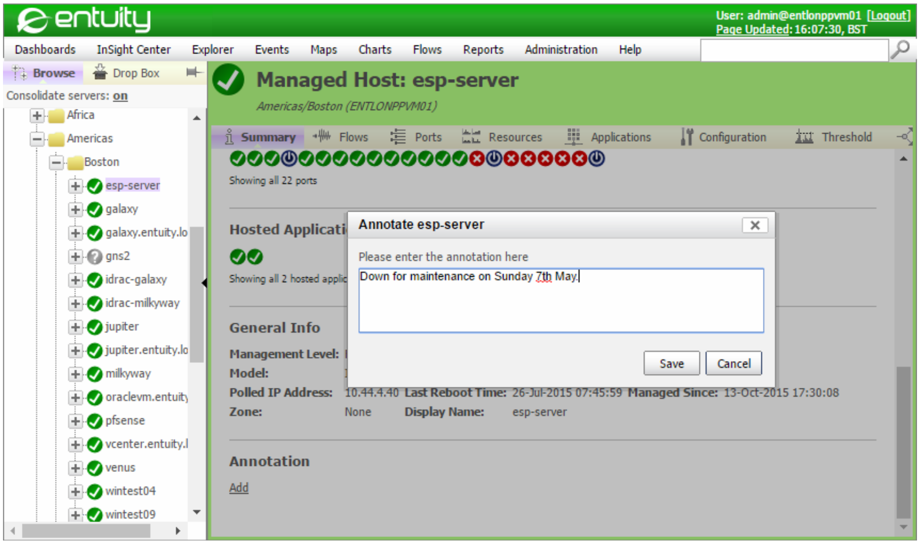
## Adding Annotations to an Object

You can associate an annotation with a component.

To add an annotation:

1) Highlight the required object.

2) From the object’s Summary tab, in the Annotation section click **Add Annotation**.



User: admin@entlonppvm01 [Logout]
Page Updated: 16:07:30, BST

Consolidate servers: on

Managed Host: esp-server
Americas/Boston (ENTLONPPVM01)

Showing all 22 ports

Showing all 2 hosted applic

Annotate esp-server

Please enter the annotation here

Down for maintenance on Sunday 7th May.

Management Level:
Model:
Polled IP Address: 10.44.4.40 Last Reboot Time: 26-Jul-2015 07:45:59 Managed Since: 13-Oct-2015 17:30:08
Zone: None Display Name: esp-server

Figure 286 Adding Annotations

3) Complete the annotation details and click **Save**.

Entuity creates the annotation and displays it in the Annotation section of the Summary tab. Entuity also includes the options to edit and delete the annotation. (See *Figure 285 Device Annotations*.)

## Amending Annotations

You can only amend an annotation, you cannot assign an annotation to another component.

To amend annotations:

1) Navigate to the Summary tab of the object with the annotation.

2) From the Annotation section click **Edit**.

3) Amend the annotation and click **Save**.

## Deleting Annotations

To delete an annotation:

1) Navigate to the Summary tab of the object with the annotation.

2) From the Annotation section click **Delete**.

3) Click **Yes** to the prompt to confirm the deletion.

Once you delete an annotation you cannot undo it.

# 50 Entuity Event Handling and Integration Overview

Entuity provides an extensive set of events, these may originate from:

- Data Entuity polls from its managed objects.
- SNMP trap data.
- Device logging data (syslog).
- Event data received from integrated third party software.
- Entuity server administration events.

Entuity displays events through its event manager, uses them to generate incidents and also makes them available for reporting. Entuity can also forward events:

- Using its own event forwarding utility, `forkevent.` (See *Chapter 54 - Forward Events*.)
- As SNMP traps, using the Send SNMP Trap action in the Event Management System. (See *Chapter 53 - SNMP Trap Forwarding*.)
- Through third party integrations.

## Incoming Network Data and Event Handling

Entuity receives network data and how it handles it depends upon its source.

### Events from Polled Data

Entuity gathers information from the network using a number of methods, for example:

- Regular SNMP polling of managed devices.
- Availability monitoring using traceroute to detect managed object availability and latency performance.
- Entuity Cisco IOS IP SLA identifies performance of routing devices by using IP SLA operations. Entuity polls the operations, against the results of which Entuity can raise events.

Whatever the polling method, how Entuity raises events against the polled data depends upon whether the event is a threshold or non-threshold event:

- Threshold events are evaluated against a set threshold, for example a device utilization high event is only raised when device utilization exceeds the set threshold. By default the majority of events, and all of those associated with modules, are deactivated.

  Threshold events are activated through Threshold Settings.
- Non-threshold events may identify state change, for example Module Ok to Module Minor Fault, or changes in inventory status for example Port Duplex Change.

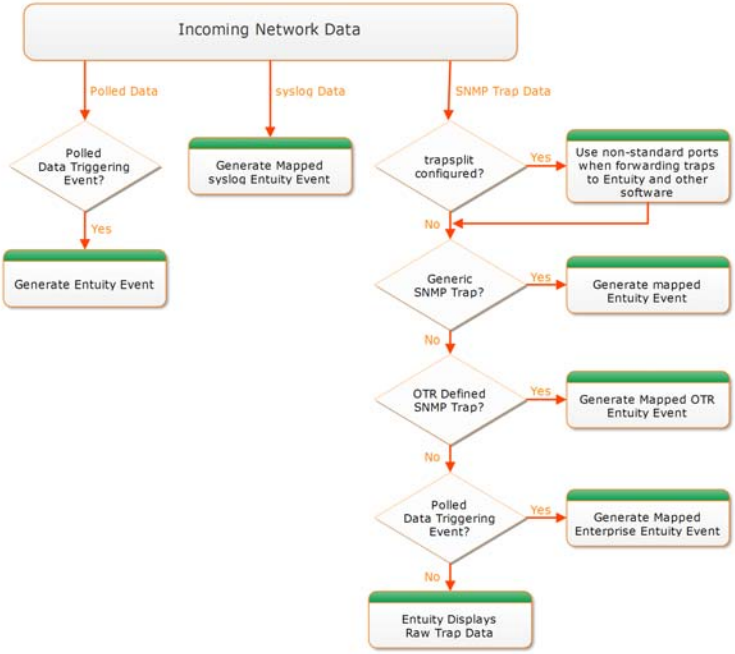

Incoming Network Data
Polled Data
syslog Data
SNMP Trap Data
Polled Data Triggering Event?
Yes
Generate Entity Event
Generate Mapped syslog Entity Event
trapsplit configured?
Yes
Use non-standard ports when forwarding traps to Entity and other software
No
Generic SNMP Trap?
Yes
Generate mapped Entity Event
No
OTR Defined SNMP Trap?
Yes
Generate Mapped OTR Entity Event
No
Polled Data Triggering Event?
Yes
Generate Mapped Enterprise Entity Event
No
Entity Displays Raw Trap Data

Figure 287 Receiving Network Data Workflow

## Entity Server Administration Events

Entity includes a number of events to assist an administrator in managing Entity, for example Entity Server Disk Space Alert, Entity Server License Alert. They are all identified by the prefix **Entity Server**.

## System Logging Events

Entity System Logger listens for device syslog alerts, and when appropriate raises syslog events. Through *entuity_home*`\etc\entuity.cfg` you can configure the conditions which would result in Entity raising syslog events, for example only for Entity managed devices and only for syslog messages of an urgency level of warning and above.

## SNMP Trap Events

Entity performs a series of checks on each received trap, attempting to take the most information from the trap. Entity checks for the most specific match first, and only when that fails attempts to match uses the next criteria. In order of precedence Entity checks whether the trap:

1) Is a generic trap, e.g. Link Up, Link Down. Entity maps generic traps to Entity events, e.g. Port Link Up, Port Link Down.

2) Has a trap definition loaded to the active event project of the Event Management System.

Only when Entuity fails to match a trap does it default to raising an Unknown Trap that displays the raw trap information. Trap receiving is highly configurable, you can for example exclude traps from devices managed by Entuity.

## Forward Incident and Event Data

You can configure Entuity to forward details of events and incidents it raises to third party software. Entuity includes a number of modules where integration with the third party software has been engineered to be specific to that integration, e.g. Entuity Remedy Action Request System Integration. These integrations are highly configurable allowing you to determine the events to forward, within the appropriate event format for that application.

You can also forward:

- Incidents and events through the Event Management System using a combination of rules, triggers and actions.

  Entuity SNMP trap forwarding allows data originally collected by Entuity to be forwarded as SNMP traps. Entuity creates appropriately structured traps, and through the Send SNMP Trap action sends them to third party software.

  Entuity SNMP trap forwarding can be used to provide two way integrations with any third party software that can handle SNMP trap data, for example as Dell Foglight, HP OpenView, IBM Tivoli Netcool.

- Events through `forkevent`.

  Entuity Event Forward Integration Module module allows Entuity to forward its events to third party software. You can configure event forwarding so it considers one or more of the event type, event source and event destination(s) when determining which events to forward.

  The details Entuity forwards for each event are also configurable, but may include the event's source, impact details and priority level.

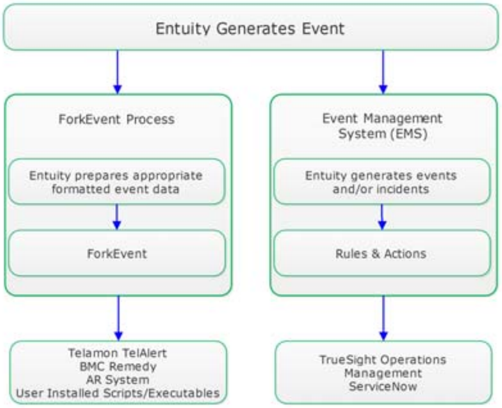

Entuity Generates Event
ForkEvent Process
Entuity prepares appropriate formatted event data
ForkEvent
Event Management System (EMS)
Entuity generates events and/or incidents
Rules & Actions
Telamon TelAlert
BMC Remedy
AR System
User Installed Scripts/Executables
TrueSight Operations Management
ServiceNow

Figure 288 Forwarding Network Data Workflow

# 51 Trap Management

Entuity trap management can receive and manage SNMPv1, SNMPv2c and SNMPv3 traps and inform requests. Entuity (`prologV2`) receives these traps and delivers them to the Event Management System where, by default, the:

- Six generic and two spanning tree traps are mapped to their respective Entuity events. (See *Receiving Generic and Spanning Tree Traps*.)
- Remaining enterprise trap types are by default handled as Unknown Trap events, which are populated with an unformatted set of information. However, through the Event Management System you can develop more intelligent handling of these enterprise traps

Entuity trap management functionality includes:

- Parsing of any SNMPv1, SNMPv2c and SNMPv3 MIB that contains trap definitions. Entuity includes an extensive set of MIBs that you can load (parse) into the Event Management System. You can also import additional MIB files and load them into the Event Management System.
- Viewing and configuring of all of the correctly parsed enterprise trap definitions.
- Creation of trap events, both manually and automatically during the parsing of the MIB and its trap definitions.
- Complete configuration of all of the trap event's properties, including severity level, time to live, and description.
- Definition of rules that control when an Unknown Trap generates an event.
- Filters you can set for Unknown Traps on a view basis.
- User defined incidents through which you can define trap event canceling through pairing of traps.
- Automatic flooding controls.

Events that are generated from traps, and incidents derived from those events, allow the same functionality as other events and incidents, for example you can add annotations.

## How Entuity Manages Traps

Entuity receives traps using `prologV2` which makes them available to the Event Management System for processing. The Event Management System performs a series of checks on each received trap. It checks:

1) For six generic and two spanning tree traps and maps them to Entuity events, e.g. Link Up and Link Down traps respectively map to the Port Link Up and Port Link Down events (see *Receiving Generic and Spanning Tree Traps*).

2) Whether a trap definition loaded to the active event project of the Event Management System. (See *Define Events for Traps*.)

Traps that are not mapped to an event Entuity raises as Unknown Trap events and incidents. (See *Receiving Generic and Spanning Tree Traps*.)

When a check is successful Entuity raises an appropriate event in the correct format. Entuity displays traps from:

- Managed devices as events against those devices; these events are only visible in views to which the devices belong.
- Unmanaged devices in all views with the exception of views that have modified IP content filters that exclude the trap source IP addresses. You can also use the Discard Unknown Trap rule to discard traps from unknown devices.

  Entuity performs additional checks when handling SNMPv3 traps from unmanaged devices (see *SNMPv3 Traps from Non-Managed Devices*).

Entuity Support recommend Entuity is installed to its own server. However, if there is another application handling traps on the same machine as Entuity, you can use trap splitter to allow both applications access to incoming SNMP traps.

Entuity handles SNMP Traps and SNMP Inform Requests using the same Event Management System mechanisms.

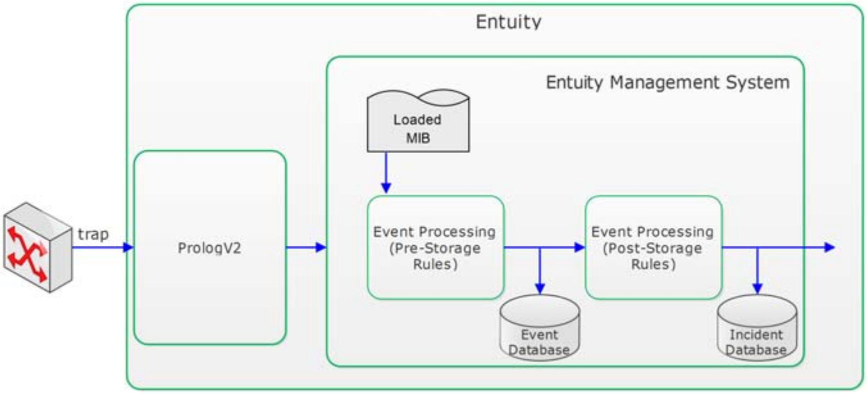

Entuity
Entuity Management System
Loaded MIB
trap
PrologV2
Event Processing (Pre-Storage Rules)
Event Processing (Post-Storage Rules)
Event Database
Incident Database

Figure 289 Trap Management Overview

## Receiving Generic and Spanning Tree Traps

Entuity's first check on receiving a trap is to test whether it is one of the eight traps for which it has mapped events and associated incidents. There are:

- Six standard traps.

| Generic Trap | Trap Name | Trap OID | Mapped Entuity Event |
|---|---|---|---|
| 0 | Cold Start | 1.3.6.1.6.3.1.1.5.1 | Device Cold Reboot |
| 1 | Warm Start | 1.3.6.1.6.3.1.1.5.2 | Device Warm Reboot |
| 2 | Link Down | 1.3.6.1.6.3.1.1.5.3 | Port Link Down |
| 3 | Link Up | 1.3.6.1.6.3.1.1.5.4 | Port Link Up |
| 4 | Authentication Failure | 1.3.6.1.6.3.1.1.5.5 | SNMP Authentication Failure |
| 5 | EGP Neighbor Loss | 1.3.6.1.6.3.1.1.5.6 | EGP Neighbor Loss |

Table 49 Generic Traps

- Two spanning tree traps.

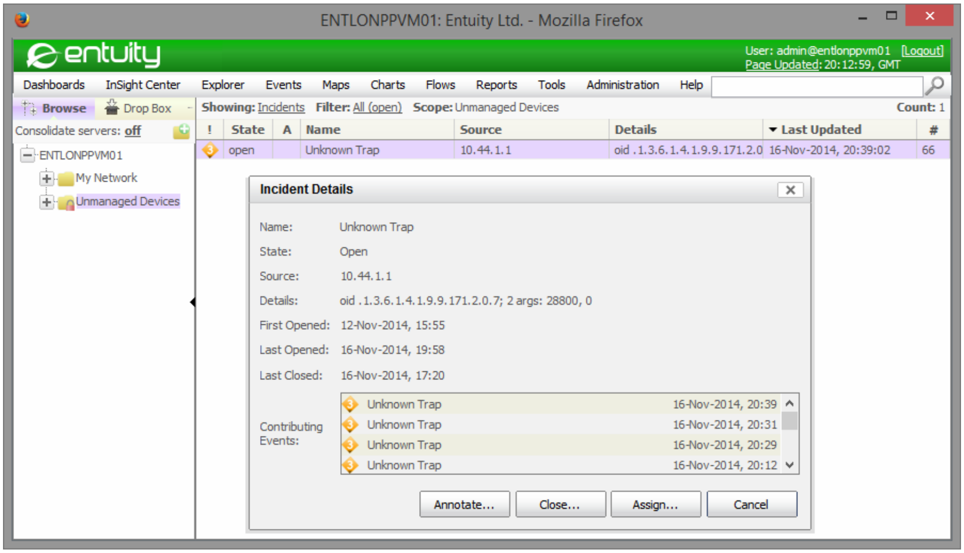
| Trap Name | Trap OID | Mapped Entuity Event |
|---|---|---|
| Spanning tree root change | 1.3.6.1.2.1.17(1) | STP New Root Device |
| Spanning tree topology change | 1.3.6.1.2.1.17(2) | STP VLAN Topology Change |

Table 50 Spanning Tree Traps

When there is a match Entuity generates the appropriate mapped event.

## Unknown Trap Events and Incidents

If a trap is not one of the six generic traps or one of the two spanning tree traps the factory default, before you have set up any trap processing, is for Entuity to raise an Unknown Trap event and incident. The Unknown Trap incident has a default ageout of 2400 seconds. You can view a longer history of traps received by viewing event history.



Showing: Incidents Filter: All (open) Scope: Unmanaged Devices Count: 1

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| 3 | open | | Unknown Trap | 10.44.1.1 | oid .1.3.6.1.4.1.9.9.171.2.0 | 16-Nov-2014, 20:39:02 | 66 |

Incident Details

Name: Unknown Trap

State: Open

Source: 10.44.1.1

Details: oid .1.3.6.1.4.1.9.9.171.2.0.7; 2 args: 28800, 0

First Opened: 12-Nov-2014, 15:55

Last Opened: 16-Nov-2014, 19:58

Last Closed: 16-Nov-2014, 17:20

Contributing Events:

| | |
|---|---|
| Unknown Trap | 16-Nov-2014, 20:39 |
| Unknown Trap | 16-Nov-2014, 20:31 |
| Unknown Trap | 16-Nov-2014, 20:29 |
| Unknown Trap | 16-Nov-2014, 20:12 |

Figure 290 Unknown Incident Details

An Unknown Trap event contains the trap OID and arguments. However, the displayed Unknown Trap event varbinds are not interpreted according to their enumerated list so the information within the trap is not easy to understand.

You can improve trap handling by creating custom events and incidents for the Event Management System to handle the trap. Trap processing interprets varbind values that rely on enumerated lists and displays varbind value names.

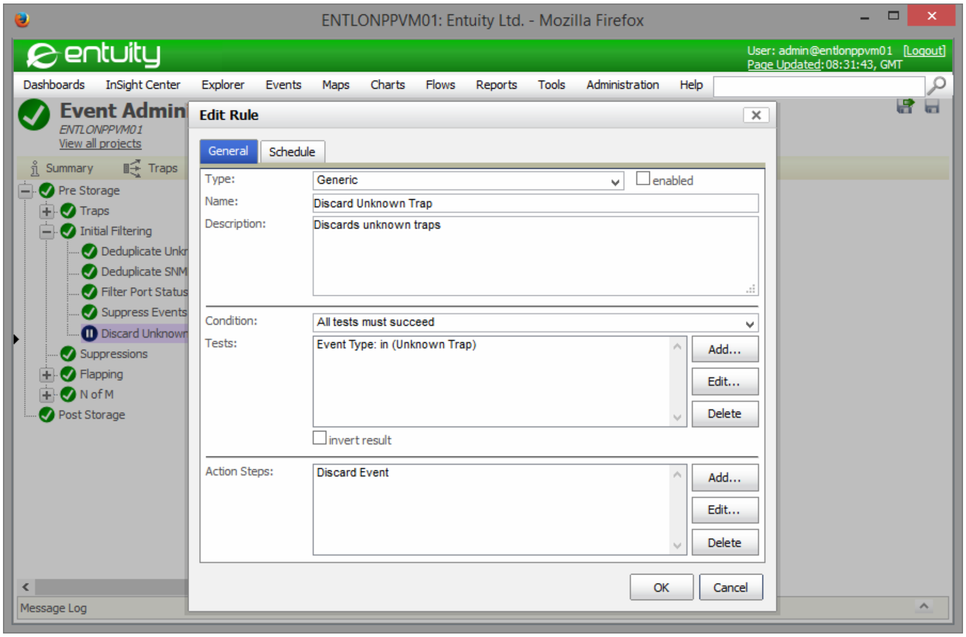
Alternatively you can prevent Entuity raising Unknown Trap events by activating the Discard Unknown Trap rule. By default this rule is part of the Initial Filtering Pre Storage stage of event processing, the stage after the Trap Processing stage. It would therefore discard all Unknown Traps.

## Discard Unknown Traps

For incoming traps for which the Event Management System does not have a specific rule and custom event Entuity generates an Unknown Trap event. You can use the Discard Unknown Trap rule for the Event Management System to discard all Unknown Trap events. By default this is a Pre Storage rule, so the events are not written to the events database.

To prevent Entuity raising Unknown Traps:

1) Click **Administration** > **Events** > **Events Administration**.
2) Click **Rules** and then from the tree click **Pre Storage** > **Initial Filtering.**
3) Highlight the **Discard Unknown Trap** rule and click **Edit**.
4) Click **Edit** and then **enabled** to activate the rule.
5) Click **Ok**.
6) Click the **Save and Deploy** icon to action the change to the rule state.



Type: Generic □ enabled

Name: Discard Unknown Trap

Description: Discards unknown traps

Condition: All tests must succeed

Tests: Event Type: in (Unknown Trap)

□ invert result

Action Steps: Discard Event

Figure 291 Discard Unknown Trap

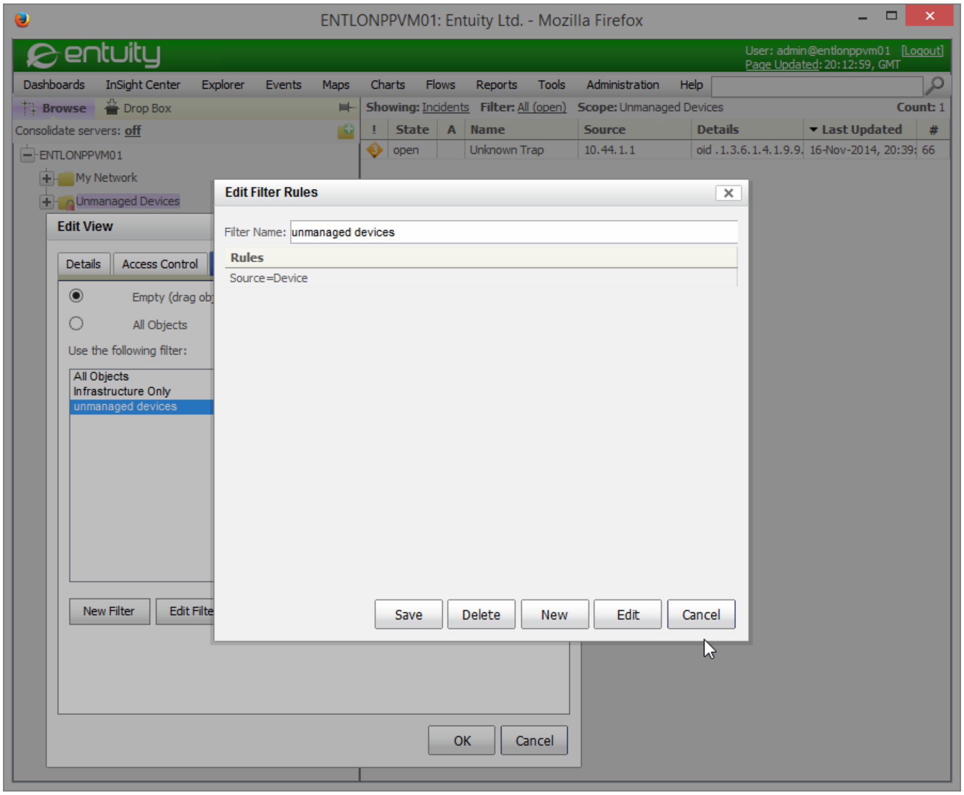
## Trap Events from Unknown Devices

Entuity can handle traps from unknown devices, an unknown device is one that is not managed by Entuity. Entuity handles traps from unknown devices in the same way as for traps sent from managed devices and interfaces:

- Six generic and two spanning tree traps are mapped to their respective Entuity events.
- All other traps Entuity raises as Unknown Trap events unless you have configured custom events.

Traps from unknown devices are displayed in all views, unless a view has an IP address filter that would exclude the device. You can find all traps from unknown devices by creating a view with:

- The content set to Empty.
- A content filter with the rule `Source=Device`.



Showing: Incidents Filter: All (open) Scope: Unmanaged Devices Count: 1

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| | open | | Unknown Trap | 10.44.1.1 | oid .1.3.6.1.4.1.9.9. | 16-Nov-2014, 20:39: | 66 |

Edit Filter Rules

Filter Name: unmanaged devices

Rules

Source=Device

Figure 292 View for Unknown Device

## Discard Traps from Unknown Devices

Entuity considers unknown devices and interfaces as devices and interfaces that are not under its management. By default traps from these devices and interfaces are handled as Unknown Trap events. Events from these unmanaged objects are visible in all views if the view’s event filter is set to include events from devices that are not under management unless a view has an IP address filter which the incoming trap fails to meet. Entuity manages incidents in the same way.

`prologV2` is the process that receives traps and forwards them to the Event Management System. Through the OTR section of *entuity_home*`\etc\entuity.cfg` you can control `prologV2`’s default behavior so that it excludes all traps from unknown devices and interfaces:

```
[OTR]
suppressUnmanagedDevices=false
suppressUnmanagedInterfaces=false
```

where

- *suppressUnmanagedDevices* controls how Entuity handles unmanaged devices. When set to:
  - **false** (default) Entuity handles traps from unmanaged devices.
  - **true**, Entuity suppresses traps from unmanaged devices.
- *suppressUnmanagedInterfaces* controls how Entuity handles unmanaged interfaces. When set to:
  - **false** (default) Entuity handles traps from unmanaged interfaces.
  - **true**, Entuity suppresses traps from unmanaged interfaces.

Changes to trap suppression and interface specific configuration may take five minutes to take effect.

## Define Events for Traps

For Entuity to handle a trap the MIB:

- With the trap definition must be imported to the Entuity server.
- Must be loaded (parsed) to the Entuity server and from that events and rules defined for the traps should be added to the live Event Management System event project.

As part of the import process Entuity can automatically generate events and rules associated with the trap definitions in the MIB. You can amend, add to and delete these rules and events.

The trap management configuration is applied through the event project. Only when the event project with your trap management configuration is saved and deployed is that configuration available for use.

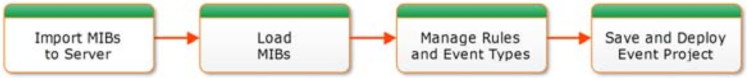


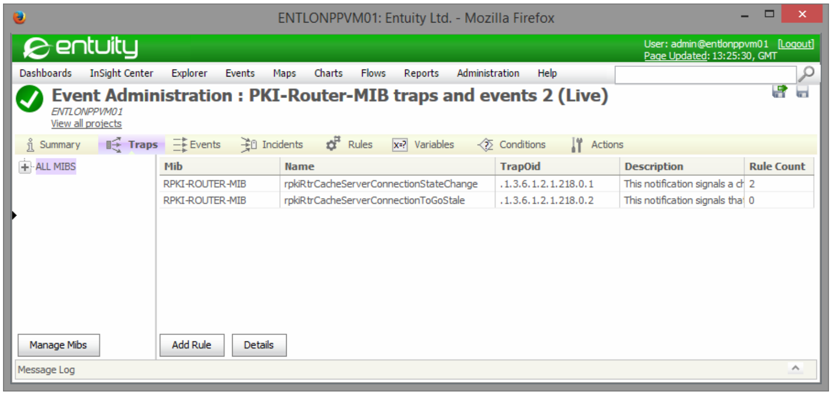
Figure 293 Trap Management Process

The Event Management System Traps page lists all MIBs and traps loaded to the Entuity server. You can also import and load MIBs to the server and edit the rules used to define how Event Management System handles traps.

To view MIBs loaded to the Entuity server:

1) Click **Administration > Events > Events Administration**.

2) Click **Traps**. The Traps page includes a tree list of all MIBs loaded to the server and a table which details all loaded trap definitions.



Event Administration : PKI-Router-MIB traps and events 2 (Live)

ENTLONPPVM01

View all projects

| Mib | Name | TrapOid | Description | Rule Count |
|---|---|---|---|---|
| RPKI-ROUTER-MIB | rpkiRtrCacheServerConnectionStateChange | .1.3.6.1.2.1.218.0.1 | This notification signals a ch | 2 |
| RPKI-ROUTER-MIB | rpkiRtrCacheServerConnectionToGoStale | .1.3.6.1.2.1.218.0.2 | This notification signals tha | 0 |

Figure 294 Imported Traps

## Importing MIB Definitions

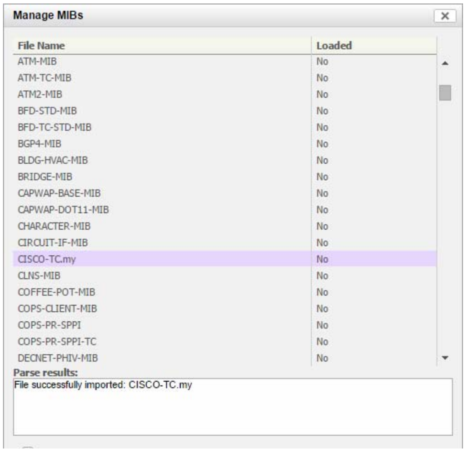
For Entuity to interpret incoming traps you must load to the server the appropriate MIBs with their trap definitions. Entuity is shipped with a set of IETF and IANA MIB files (RFC-1212, RFC-1215, RFC1155-SMI, RFC1158-MIB, RFC1213-MIB and SNMPv2-SMI MIBs) in the MIBs directory which are available for you to load (parse). You can augment these by importing additional MIBs with trap definitions.

To import MIBs to the Entuity server:

1) Click **Administration** > **Events** > **Events Administration**.

2) Click **Traps** and then **Manage MIBs**.

3) Click **Import File**. You can use the upload dialog to navigate to the folder containing the MIB to import to the server.



| File Name | Loaded |
|---|---|
| ATM-MIB | No |
| ATM-TC-MIB | No |
| ATM2-MIB | No |
| BFD-STD-MIB | No |
| BFD-TC-STD-MIB | No |
| BGP4-MIB | No |
| BLDG-HVAC-MIB | No |
| BRIDGE-MIB | No |
| CAPWAP-BASE-MIB | No |
| CAPWAP-DOT11-MIB | No |
| CHARACTER-MIB | No |
| CIRCUIT-IF-MIB | No |
| CISCO-TC.my | No |
| CLNS-MIB | No |
| COFFEE-POT-MIB | No |
| COPS-CLIENT-MIB | No |
| COPS-PR-SPPI | No |
| COPS-PR-SPPI-TC | No |
| DECNET-PHIV-MIB | No |

Parse results:

File successfully imported: CISCO-TC.my

Figure 295 Manage MIBs

When you have access to the Entuity server you can also directly upload all of the MIB files to the MIB folder, by default *entuity_home*`\lib\mibs`.

## Loading MIB Definitions

When you have imported MIBs to the Entuity server you can then also load (parse) them on the Entuity server. These loaded MIBs are then available through the Event Management System for use within event management projects. You can configure the import process to create custom events and rules for each trap definition as Entuity parses the MIBs, these events and rules are added to the event project that you are currently editing.

Entuity reports on the progress of the MIB loading and when it:

- Fails, for example if there's an error in the MIB or if it has no object definitions:

  ```
  File IPV6-TC failed to parse. (1 of 1 mibs processed)
  ```

  ```
  File IPV6-TC has no object definitions
  ```

- Succeeds and you selected the creation of custom events for the use with trap definitions, it reports the created custom events, for example:

  ```
  File BGP4-MIB successfully parsed. (1 of 1 mibs processed)
  ```

  ```
  Added custom events: bgpEstablishedNotification bgpBackwardTransNotification bgpEstablished bgpBackwardTransition
  ```

  It also warns of any MIB substitutions, for example:

  ```
  Warning: in C:\Entuity\lib\mibs\SNA-NAU-MIB: line 60:
   missing import for 'mib-2', using definition from SNMPv2-SMI
  ```

When you have access to the Entuity server you can also directly upload MIBs parsed on one Entuity server to the loaded MIBs folder of another. The default folder for loaded MIBs is *entuity_home*`\lib\mibs\parsed`. To set up the receiving server with the same configuration as the original server would also require the importing of the event project from the original to the new server. The event project contains the rules, events and incidents to use with the traps.

To load MIBs to the Entuity server:

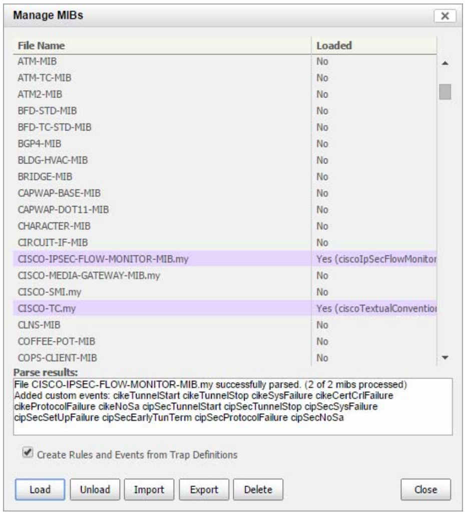
1) Click **Administration > Events > Events Administration**.

2) Click **Traps** and then **Manage MIBs**.

3) Click **Create Rules and Event from Trap Definitions** when you want Entuity to automatically create the trap processing rules and custom events to be used to handle the traps. You can subsequently amend these rules and traps.

4) From the list of MIBs highlight the MIB or MIBs to load and click **Load**.

   Entuity reports on the success or failure of each operation. Entuity updates the Loaded state of each successful load to Yes and in parenthesis includes the MIB object name.



| File Name | Loaded |
|---|---|
| ATM-MIB | No |
| ATM-TC-MIB | No |
| ATM2-MIB | No |
| BFD-STD-MIB | No |
| BFD-TC-STD-MIB | No |
| BGP4-MIB | No |
| BLDG-HVAC-MIB | No |
| BRIDGE-MIB | No |
| CAPWAP-BASE-MIB | No |
| CAPWAP-DOT11-MIB | No |
| CHARACTER-MIB | No |
| CIRCUIT-IF-MIB | No |
| CISCO-IPSEC-FLOW-MONITOR-MIB.my | Yes (ciscoIpSecFlowMonitor |
| CISCO-MEDIA-GATEWAY-MIB.my | No |
| CISCO-SMI.my | No |
| CISCO-TC.my | Yes (ciscoTextualConventio |
| CLNS-MIB | No |
| COFFEE-POT-MIB | No |
| COPS-CLIENT-MIB | No |

Parse results:

File CISCO-IPSEC-FLOW-MONITOR-MIB.my successfully parsed. (2 of 2 mibs processed)
Added custom events: cikeTunnelStart cikeTunnelStop cikeSysFailure cikeCertCrlFailure
cikeProtocolFailure cikeNoSa cipSecTunnelStart cipSecTunnelStop cipSecSysFailure
cipSecSetUpFailure cipSecEarlyTunTerm cipSecProtocolFailure cipSecNoSa

☑ Create Rules and Events from Trap Definitions

Figure 296 Load MIBs

## Imported Trap Definitions

For each imported trap you can view its definition.

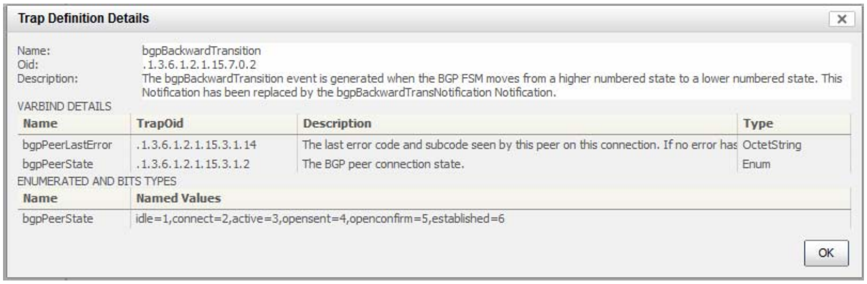
To view details of imported trap definitions:

1) Click **Administration** > **Events** > **Events Administration**.

2) Click **Traps**.

   When the page loads, its focus is on All MIBs in the MIBs tree which causes Entuity to display all of the loaded trap definitions. Alternatively, you can expand the ALL MIBs tree, highlight a MIB and view the traps imported for that MIB.

3) Highlight the trap definition and click **Details**.



Name: bgpBackwardTransition
Oid: .1.3.6.1.2.1.15.7.0.2
Description: The bgpBackwardTransition event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state. This Notification has been replaced by the bgpBackwardTransNotification Notification.

VARBIND DETAILS

| Name | TrapOid | Description | Type |
|---|---|---|---|
| bgpPeerLastError | .1.3.6.1.2.1.15.3.1.14 | The last error code and subcode seen by this peer on this connection. If no error has | OctetString |
| bgpPeerState | .1.3.6.1.2.1.15.3.1.2 | The BGP peer connection state. | Enum |

ENUMERATED AND BITS TYPES

| Name | Named Values |
|---|---|
| bgpPeerState | idle=1,connect=2,active=3,opensent=4,openconfirm=5,established=6 |

Figure 297 Trap Definition Details

| Attribute | Definition |
|---|---|
| *Trap Definition* | Name of the trap. |
| *OID* | Trap Object Identifier (OID). An example OID is **1.3.6.1.4.1.2626.1.1.0.2**, where:<br>■ **1.3.6.1.4.1.2626.1.1** is the enterprise OID.<br>■ **0** is the trap identifier, signified. 0 is always the enterprise trap identifier. |
| *Description* | Description of the trap. |
| *Varbind Details* | Details the varbinds included to the trap:<br>■ *Name*, name of the varbind.<br>■ *TrapOid*, trap OID associated to the varbind.<br>■ *Description*, description imported with the trap definition.<br>■ *Type*, type of variable together with legitimate values |
| *Enumerated and Bits Types* | Identifies named values, for example when the varbind has a *Type* of **Enum** this row:<br>■ *Name* identifies the referred to trap definition.<br>■ *Named Values* identifies the enumerated values. |

Table 51 Trap Definition Details

0 is the enterprise trap identifier for SMIv1 and SMIv2 traps, even though the standard for SMIv1 enterprise trap identification is 6.

### Unloading MIB Definitions

Unloading a MIB deletes the parsed MIB from the parsed MIB folder and therefore makes it unavailable through the Event Management System. Unloading a MIB does not remove any rules associated with the trap or custom events from the event project, as rules and events may potentially be shared by more than one MIB or trap definition. Instead when required you must separately delete custom events and trap processing rules.

Unloading a MIB does not update the event project, however Entuity would outline any events and rules within the event project that are affected by the removal of the MIB. If you delete rules and custom events associated with the MIB this does change the event project, which you have to save and then deploy for those changes to apply to your Event Management System.

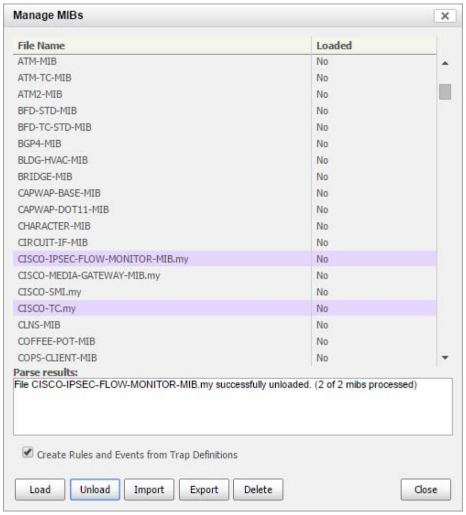
To unload MIBs from the Entuity server:

1) Click **Administration** > **Events** > **Events Administration**.

2) Click **Traps** and then **Manage MIBs**.

3) From the list of MIBs highlight the MIB or MIBs to unload and click **Unload**.

   Entuity deletes the parsed MIBs from *entuity_home*`\lib\mibs\parsed`.



| File Name | Loaded |
|---|---|
| ATM-MIB | No |
| ATM-TC-MIB | No |
| ATM2-MIB | No |
| BFD-STD-MIB | No |
| BFD-TC-STD-MIB | No |
| BGP4-MIB | No |
| BLDG-HVAC-MIB | No |
| BRIDGE-MIB | No |
| CAPWAP-BASE-MIB | No |
| CAPWAP-DOT11-MIB | No |
| CHARACTER-MIB | No |
| CIRCUIT-IF-MIB | No |
| CISCO-IPSEC-FLOW-MONITOR-MIB.my | No |
| CISCO-MEDIA-GATEWAY-MIB.my | No |
| CISCO-SMI.my | No |
| CISCO-TC.my | No |
| CLNS-MIB | No |
| COFFEE-POT-MIB | No |
| COPS-CLIENT-MIB | No |

Parse results:

```
File CISCO-IPSEC-FLOW-MONITOR-MIB.my successfully unloaded. (2 of 2 mibs processed)
```

☑ Create Rules and Events from Trap Definitions

Figure 298 Load MIBs

### Deleting MIB Definitions

Deleting a MIB deletes the loaded MIB from the parsed MIB folder and the unparsed MIB files from the Entuity server, and therefore deletes the trap definitions from the Event Management System. Deleting a MIB does not remove any rules associated with the trap or custom events from event projects, as rules and events may potentially be shared by more than one MIB or trap definition. Instead when required you must separately delete custom events and trap processing rules.

Deleting a MIB does not update the event project, however Entuity would outline any events and rules within the event project that are affected by the removal of the MIB. If you also delete rules and custom events associated with the MIB this does change the event project and would require the saving and deploying of the updated event project for those changes to affect your Event Management System.

To delete MIBs from the Entuity server:

1) Click **Administration** > **Events** > **Events Administration**.

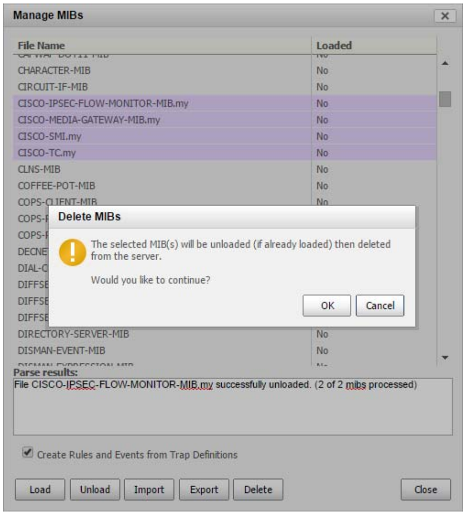
2) Click **Traps** and then **Manage MIBs**.

3) From the list of MIBs highlight the MIB or MIBs to delete and click **Delete**.

4) Entuity prompts you to confirm the deletion of the selected MIBs. Click **OK**.

   Entuity deletes for the selected MIBs:

   - Any parsed MIBs from *entuity_home*`\lib\mibs\parsed`.
   - Loaded MIBs from *entuity_home*`\lib\mibs`.



| File Name | Loaded |
|---|---|
| CHARACTER-MIB | No |
| CIRCUIT-IF-MIB | No |
| CISCO-IPSEC-FLOW-MONITOR-MIB.my | No |
| CISCO-MEDIA-GATEWAY-MIB.my | No |
| CISCO-SMI.my | No |
| CISCO-TC.my | No |
| CLNS-MIB | No |
| COFFEE-POT-MIB | No |
| COPS-CLIENT-MIB | No |
| COPS-P | |
| COPS-P | |
| DECNE | |
| DIAL-C | |
| DIFFSE | |
| DIFFSE | |
| DIFFSE | |
| DIRECTORY-SERVER-MIB | No |
| DISMAN-EVENT-MIB | No |

Delete MIBs

The selected MIB(s) will be unloaded (if already loaded) then deleted from the server.

Would you like to continue?

OK Cancel

Parse results:

File CISCO-IPSEC-FLOW-MONITOR-MIB.my successfully unloaded. (2 of 2 mibs processed)

☑ Create Rules and Events from Trap Definitions

Figure 299 Delete MIBs

## Exporting MIB Definitions

You can export MIB files from the Entuity server, for example to import to another Entuity server. If you select:

- One MIB Entuity exports it as a single MIB file with the name of that MIB.
- Multiple MIBs Entuity exports them as one compressed file named `mibs.zip`.

To export MIBs from the Entuity server:

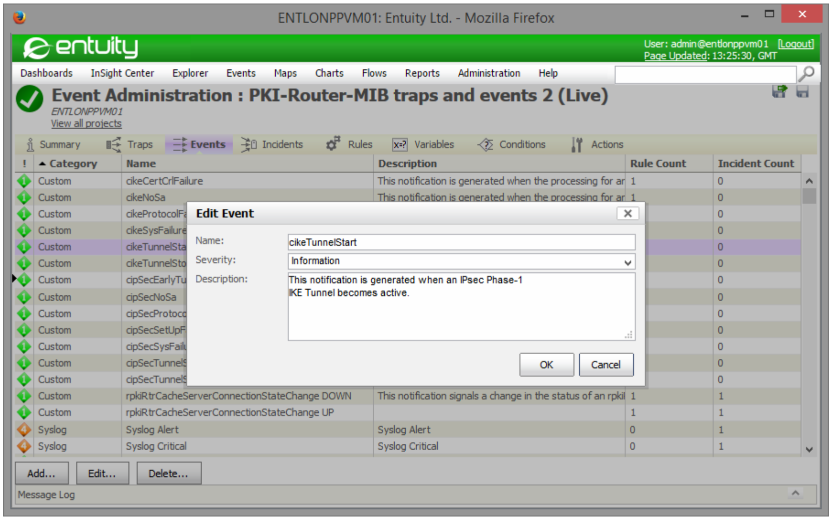
1) Click **Administration** > **Events** > **Events Administration**.
2) Click **Traps** and then **Manage MIBs**.
3) From the list of MIBs highlight the MIB or MIBs to export and click **Export**. Entuity exports the MIB file to the browser download directory.

## Custom Events to Handle Traps

When you load trap definitions you can configure Event Management System to automatically create trap processing rules and events associated with each trap. By default Event Management System sets events attributes as:

- *Category* to **Custom**. From the Events page you can sort on the Category column to group together all custom events.
- *Name* is set to the trap name.
- *Severity* is set to Information.
- *Description* is taken from the trap definition.

All of these attributes are configurable. You can also modify the associated rules and associate incidents.



Event Administration : PKI-Router-MIB traps and events 2 (Live)

*ENTLONPPVM01*

View all projects

| ! | Category | Name | Description | Rule Count | Incident Count |
|---|---|---|---|---|---|
| 1 | Custom | cikeCertCrlFailure | This notification is generated when the processing for ar | 1 | 0 |
| 1 | Custom | cikeNoSa | This notification is generated when the processing for ar | 1 | 0 |
| 1 | Custom | cikeProtocolF | | | 0 |
| 1 | Custom | cikeSysFailure | | | 0 |
| 1 | Custom | cikeTunnelSta | | | 0 |
| 1 | Custom | cikeTunnelSto | | | 0 |
| 1 | Custom | cipSecEarlyTu | | | 0 |
| 1 | Custom | cipSecNoSa | | | 0 |
| 1 | Custom | cipSecProtoco | | | 0 |
| 1 | Custom | cipSecSetUpF | | | 0 |
| 1 | Custom | cipSecSysFailu | | | 0 |
| 1 | Custom | cipSecTunnelS | | | 0 |
| 1 | Custom | cipSecTunnelS | | | 0 |
| 1 | Custom | rpkiRtrCacheServerConnectionStateChange DOWN | This notification signals a change in the status of an rpkil | 1 | 1 |
| 1 | Custom | rpkiRtrCacheServerConnectionStateChange UP | | 1 | 1 |
| 4 | Syslog | Syslog Alert | Syslog Alert | 0 | 1 |
| 4 | Syslog | Syslog Critical | Syslog Critical | 0 | 1 |

Edit Event

Name: cikeTunnelStart

Severity: Information

Description: This notification is generated when an IPsec Phase-1
IKE Tunnel becomes active.

Figure 300 Custom Events

# Trap Processing

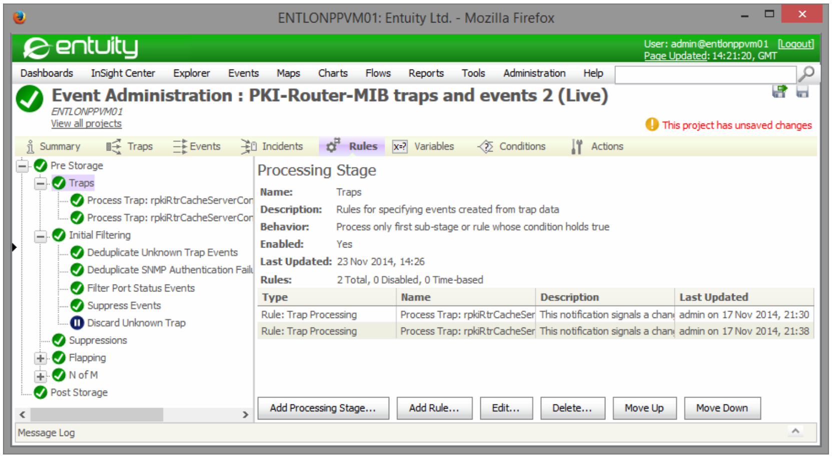
Trap handling is actioned through trap rules. Rules in the Event Management System are processed in the order they are placed in the Rules tree. The Event Management System divides rules into two stages:

- Pre Storage; before incoming event details are saved to the events database.
- Post storage; after event details are saved to the event database but before details are saved to the incident database.

Traps is the first sub-stage of the Pre Storage stage. Rules in this stage are therefore the first rules actioned. Within the Traps stage rule order is also important, rules higher in the order are processed earlier. Rule order maybe especially important when testing on varbind values.

Event Management System includes a Discard Unknown Trap rule. As part of the Initial Filtering stage when activated it is only applied after other trap processing rules are applied. It therefore only discards alerts from traps without processing rules.

You can create new stages and assign trap processing rules to those stages. However you should not delete the Traps stage as it is used to hold rules generated automatically when loading trap definitions. If you delete the stage, Entuity will recreate the stage the next time it loads MIBs and traps definitions and has to automatically generate rules.



Event Administration : PKI-Router-MIB traps and events 2 (Live)

ENTLONPPVM01

View all projects

This project has unsaved changes

Processing Stage

**Name:** Traps

**Description:** Rules for specifying events created from trap data

**Behavior:** Process only first sub-stage or rule whose condition holds true

**Enabled:** Yes

**Last Updated:** 23 Nov 2014, 14:26

**Rules:** 2 Total, 0 Disabled, 0 Time-based

| Type | Name | Description | Last Updated |
|---|---|---|---|
| Rule: Trap Processing | Process Trap: rpkiRtrCacheSer | This notification signals a chan | admin on 17 Nov 2014, 21:30 |
| Rule: Trap Processing | Process Trap: rpkiRtrCacheSer | This notification signals a chan | admin on 17 Nov 2014, 21:38 |

Figure 301 Trap Rules

## Multiple Traps Raising the Same Event Type

You can map multiple trap OIDs to the same Entuity event type. You might want to do this when:

- Some devices are using a MIB with obsolete trap definitions and other devices are using the new trap definition.
- Some devices are running SNMPv1 and others SNMPv2 which may mean using different traps to return the same information.
- Different device vendors have different MIBs but for the Entuity administrator’s purpose are returning the same information.

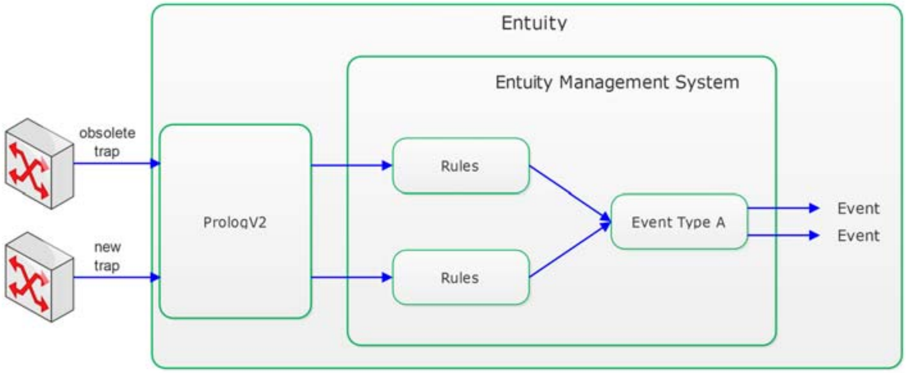


Figure 302 Two Traps One Event Type

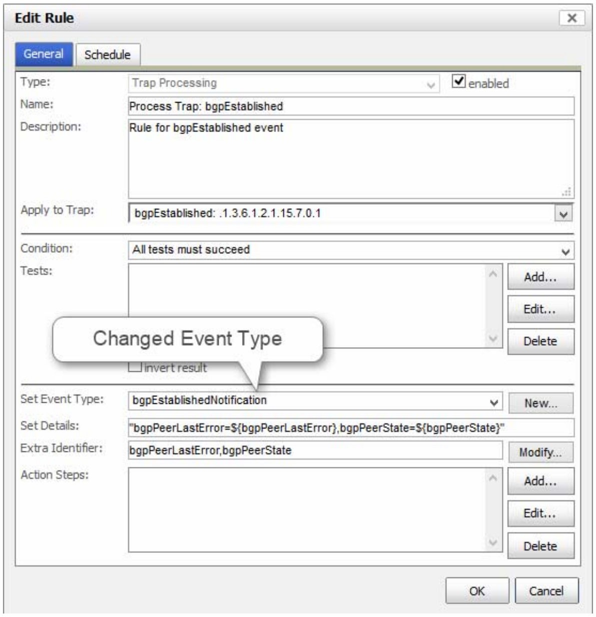
This example uses the BGP4 MIB file which includes four traps:

- Two obsolete, `bgpEstablished` and `bgpBackwardTransition`
- Two replacements for the obsolete traps, `bgpEstablishedNotification` and `bgpBackwardTransNotification`.

The initial loading of the MIB created rules and custom events for each trap. The intention is to change the rules associated with the obsolete traps so that they call the custom event type associated with the replacement traps.

To amend the trap processing rule for `bgpEstablished`:

1) Click **Administration > Events > Events Administration**.
2) Click **Rules** and then from the tree click **Pre Storage > Traps.**
3) Highlight the **Process Trap: bgpEstablished** rule and click **Edit**.
4) From *Set Event Type* select the `bgpEstablishedNotification` event type.
5) Click **Ok**.



Type: Trap Processing ☑ enabled
Name: Process Trap: bgpEstablished
Description: Rule for bgpEstablished event
Apply to Trap: bgpEstablished: .1.3.6.1.2.1.15.7.0.1
Condition: All tests must succeed
Tests:
□ invert result
Set Event Type: bgpEstablishedNotification
Set Details: "bgpPeerLastError=${bgpPeerLastError},bgpPeerState=${bgpPeerState}"
Extra Identifier: bgpPeerLastError,bgpPeerState
Action Steps:

Changed Event Type

Figure 303 Edit Rules

You can follow the same process to amend the rule for the `bgpBackwardTransition`. When the rules are adjusted the custom events associated with the obsolete trap definitions are now unused. You can delete them through the Events page.

An alternative approach to handling multiple trap OIDs that return the same type of data would be at the incident level. You can allow these traps to raise their own custom event type but associate these event types to the same incident type. The details of the incident would identify the originating trap OID.

## Using Varbind Name Values to Set Event Type

You can use varbind name values to determine the event type to raise. For example the value may determine the severity level of the raised event or signify whether an object is up or down.

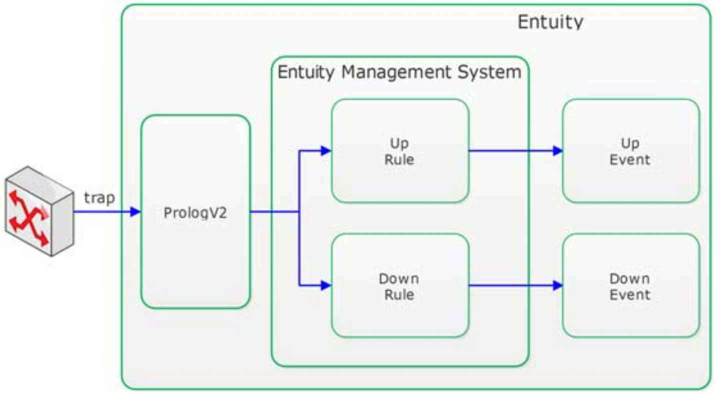
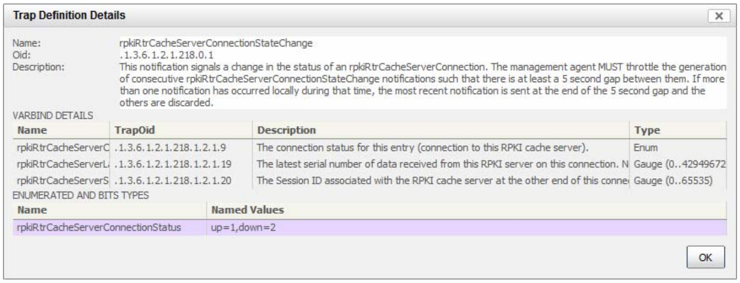


Figure 304 Varbind Name Values Determine Event Type

The initial loading of a MIB creates rules and custom events for each trap. This example:

- Loads the RPKI-Router-MIB which then generates a custom event and rule for the pkiRtrCacheServerConnectionStateChange trap.
- rpkiRtrCacheServerConnectionStatus has a value of 1 when up and 2 when down.
- Amends and renames the generated rule to signify a down connection state. The rule tests the varbind value, using the Trap Varbind Test and calls a specific custom event type.
- Creates a new rule and custom event to signify when the trap reports an up state.
- Creates an incident that is raised when the connection is in a down state and closed when it is in an Up state.



Name: rpkiRtrCacheServerConnectionStateChange
Oid: .1.3.6.1.2.1.218.0.1
Description: This notification signals a change in the status of an rpkiRtrCacheServerConnection. The management agent MUST throttle the generation of consecutive rpkiRtrCacheServerConnectionStateChange notifications such that there is at least a 5 second gap between them. If more than one notification has occurred locally during that time, the most recent notification is sent at the end of the 5 second gap and the others are discarded.

VARBIND DETAILS

| Name | TrapOid | Description | Type |
|---|---|---|---|
| rpkiRtrCacheServerC | .1.3.6.1.2.1.218.1.2.1.9 | The connection status for this entry (connection to this RPKI cache server). | Enum |
| rpkiRtrCacheServerL | .1.3.6.1.2.1.218.1.2.1.19 | The latest serial number of data received from this RPKI server on this connection. N | Gauge (0..42949672 |
| rpkiRtrCacheServerS | .1.3.6.1.2.1.218.1.2.1.20 | The Session ID associated with the RPKI cache server at the other end of this conne | Gauge (0..65535) |

ENUMERATED AND BITS TYPES

| Name | Named Values |
|---|---|
| rpkiRtrCacheServerConnectionStatus | up=1,down=2 |

Figure 305 Add Varbind Name Test

To amend the trap processing rule for `pkiRtrCacheServerConnectionStateChange`:

1) Click **Administration** > **Events** > **Events Administration**.

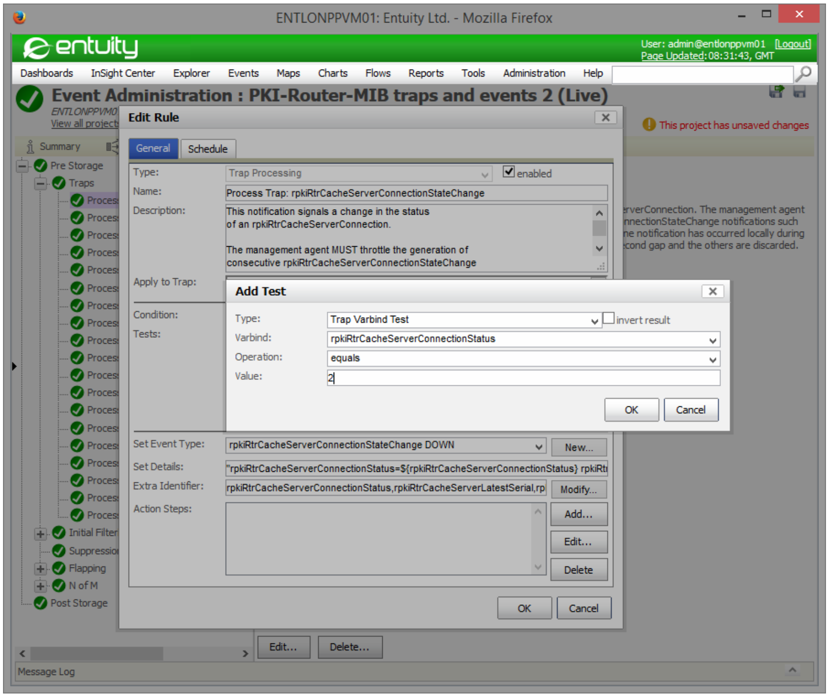
2) Click **Trap** and then **Manage MIBs**.

   Load the `RPKI-Router-MIB` and ensure **Create Rules and Events from Trap Definitions** is selected.

3) Click **Rules** and then from the tree click **Pre Storage**> **Traps.**

4) Highlight the **Process Trap: pkiRtrCacheServerConnectionStateChange** rule and click **Edit**.

5) From the Conditions section click **Add** to add a test. Set the Type to Trap Varbind Test, from Varbind select pkiRtrCacheServerConnectionStatus, set Operation to equals and value to 2.



User: admin@entlonppvm01 [Logout]
Page Updated: 08:31:43, GMT

Event Administration : PKI-Router-MIB traps and events 2 (Live)

ENTLONPPVM0
View all project

This project has unsaved changes

Edit Rule

Type: Trap Processing ☑ enabled
Name: Process Trap: rpkiRtrCacheServerConnectionStateChange
Description: This notification signals a change in the status of an rpkiRtrCacheServerConnection.

The management agent MUST throttle the generation of consecutive rpkiRtrCacheServerConnectionStateChange

Apply to Trap:
Condition:
Tests:

Add Test

Type: Trap Varbind Test □ invert result
Varbind: rpkiRtrCacheServerConnectionStatus
Operation: equals
Value: 2

Set Event Type: rpkiRtrCacheServerConnectionStateChange DOWN
Set Details: "rpkiRtrCacheServerConnectionStatus=${rpkiRtrCacheServerConnectionStatus} rpkiRt
Extra Identifier: rpkiRtrCacheServerConnectionStatus,rpkiRtrCacheServerLatestSerial,rp
Action Steps:

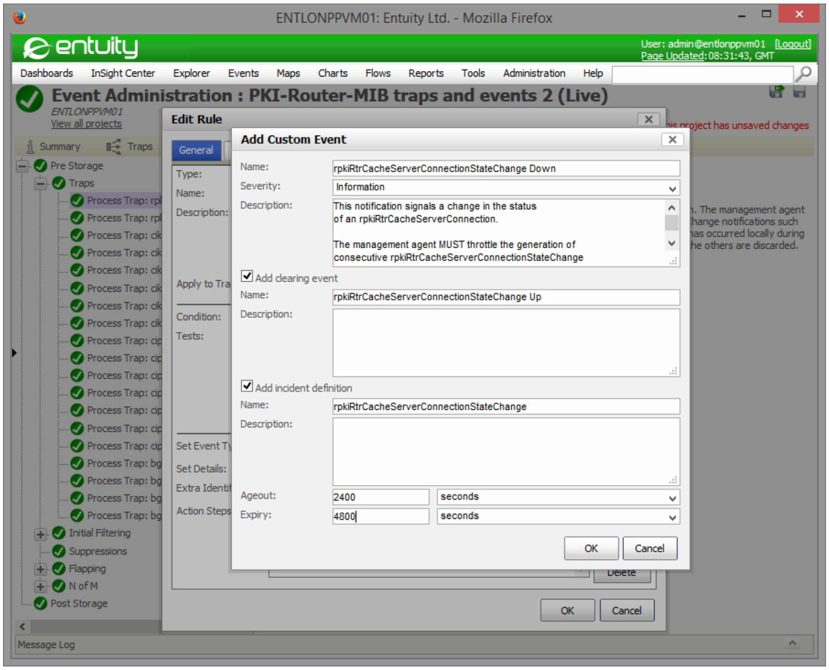
erverConnection. The management agent
nnectionStateChange notifications such
ne notification has occurred locally during
cond gap and the others are discarded.

Figure 306 Add Varbind Name Test

6) From *Set Event Type* click **New**.

   Define the new event, add the clearing event and add an incident definition. The clearing event will be called by a new processing rule that will test the trap varbind value from the up value of 1.

7) Click **OK**.


ENTLONPPVM01: Entuity Ltd. - Mozilla Firefox
entuity
User: admin@entlonppvm01 [Logout]
Page Updated:08:31:43, GMT
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Tools
Administration
Help
Event Administration : PKI-Router-MIB traps and events 2 (Live)
ENTLONPPVM01
View all projects
Summary
Traps
Edit Rule
General
This project has unsaved changes
Message Log

Add Custom Event

Name: rpkiRtrCacheServerConnectionStateChange Down

Severity: Information

Description: This notification signals a change in the status
of an rpkiRtrCacheServerConnection.

The management agent MUST throttle the generation of
consecutive rpkiRtrCacheServerConnectionStateChange

☑ Add clearing event

Name: rpkiRtrCacheServerConnectionStateChange Up

Description:

☑ Add incident definition

Name: rpkiRtrCacheServerConnectionStateChange

Description:

Ageout: 2400 seconds

Expiry: 4800 seconds

OK Cancel

Figure 307 Add Custom Event

8) Define a new trap processing rule. Highlight Traps and from the context menu click **Add**.

9) From Apply to Trap select **pkiRtrCacheServerConnectionStateChange**.

10) From the Conditions section click **Add** to add a test. Set the Type to Trap Varbind Test, from Varbind select pkiRtrCacheServerConnectionStatus, set Operation to equals and value to 1.

11) Set *Event Type* to the previously defined Up event.

12) Click **OK**.

13) Save and deploy the event project for your changes to take effect.

## Multi-Server Installations

When you have multiple Entuity servers you can set up one server with the required trap management configuration and export it to your other servers.

On the first server, the server from which you are going to export its trap management configuration:

1) Import and load to the server the required MIBs and trap definitions.

2) Define event types and trap processing rules for handling traps. You can configure Event Management System to create rules and events when traps are parsed.

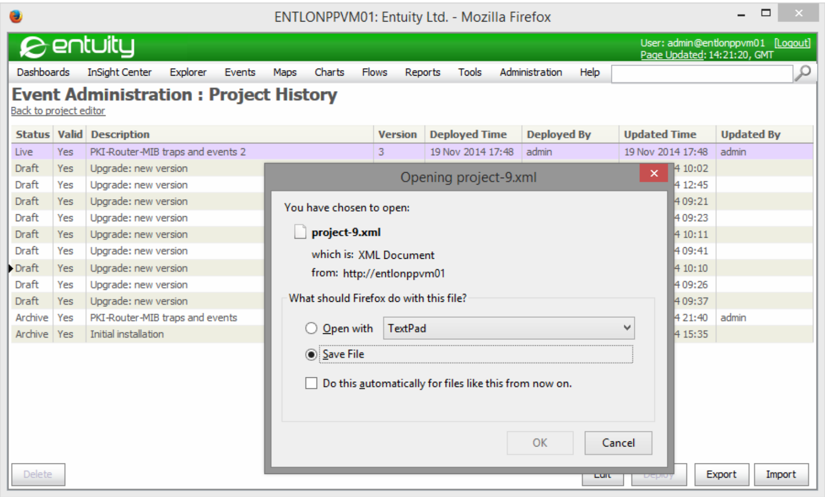
3) Amend, if required, the automatically generated rules and custom events.

4) Create any required custom events, trap processing rules and incidents.

5) When you have the event project configured ensure you have saved and deployed it.

6) Export the event project. (See *Import and Export Event Projects*)

7) Ensure the MIBs and parsed MIBs are available for you to add to subsequent servers.



Event Administration : Project History

Back to project editor

| Status | Valid | Description | Version | Deployed Time | Deployed By | Updated Time | Updated By |
|---|---|---|---|---|---|---|---|
| Live | Yes | PKI-Router-MIB traps and events 2 | 3 | 19 Nov 2014 17:48 | admin | 19 Nov 2014 17:48 | admin |
| Draft | Yes | Upgrade: new version | | | | 4 10:02 | |
| Draft | Yes | Upgrade: new version | | | | 4 12:45 | |
| Draft | Yes | Upgrade: new version | | | | 4 09:21 | |
| Draft | Yes | Upgrade: new version | | | | 4 09:23 | |
| Draft | Yes | Upgrade: new version | | | | 4 10:11 | |
| Draft | Yes | Upgrade: new version | | | | 4 09:41 | |
| Draft | Yes | Upgrade: new version | | | | 4 10:10 | |
| Draft | Yes | Upgrade: new version | | | | 4 09:26 | |
| Draft | Yes | Upgrade: new version | | | | 4 09:37 | |
| Archive | Yes | PKI-Router-MIB traps and events | | | | 4 21:40 | admin |
| Archive | Yes | Initial installation | | | | 4 15:35 | |

Opening project-9.xml

You have chosen to open:

project-9.xml

which is: XML Document

from: http://entlonppvm01

What should Firefox do with this file?

○ Open with TextPad

● Save File

□ Do this automatically for files like this from now on.

OK Cancel

Figure 308 Export Event Project

The Entuity servers receiving the trap management configuration must be set up in the same way as the original server:

1) Copy the MIBs and parse to the receiving server. By default the

- MIBs are copied to *entuity_home*`\lib\mibs`.
- MIBs are parsed to *entuity_home*`\lib\mibs\parsed`.

When MIBs are added to the Entuity server in this way it only recognizes them after you restart the server.

2) Import the event project. (See *Import and Export Event Projects*.)

3) Deploy the newly imported event project.

## SNMPv3 Traps from Non-Managed Devices

For SNMPv3 traps Entuity checks that it manages the sending device, so that it can retrieve information required to read the trap. When Entuity does not manage the device it performs a second check, this time on the SNMPv3 configuration file, `snmpV3.cfg`. To this file you should include details of all devices that Entuity does not manage but which send SNMPv3 traps that you want Entuity to handle. For each device you must include device name, device engine identifier and user name and, depending upon the level of security enabled, authentication and privacy password details.

Entuity discards SNMPv3 traps from devices which it either does not manage, or does not have an appropriate entry for in `snmpV3.cfg`.

## Handling SNMP Trap Port Conflicts

By default devices send, and `prologV2` listens for, SNMP traps on UDP port 162.

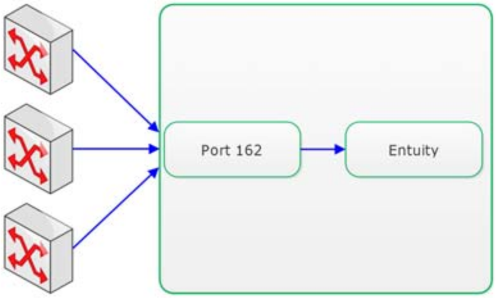


Figure 309 Receiving Traps on Port 162

Where you have installed Entuity to the same machine as another application that listens on port 162 there is a conflict. You can only have one application listening to the port.

Entuity recommend that you install Entuity to a dedicated machine.

Resolving this conflict is a two stage process:

- Configure the command line utility `trapsplit` to listen for SNMP traps on UDP port 162 (this is the default, it can listen on any port). When run it then forwards the traps to one or more specified ports.
- Change the port `prologV2` listens for SNMP traps on to the one that trapsplit is forwarding them to. This is done using the *trapportnumber* variable set in `entuity.cfg`.

Entuity's trap port conflict utility, `trapsplit`, only supports SNMPv1/SNMPv2c traps and does not support SNMPv3 traps.

For example, consider that you have two conflicting applications and decide to use trapsplit to forward traps to UDP ports 2162 and 1162:

1) Set `trapsplit` to listen on UDP port 162 for SNMP traps.

2) Through its configuration file specify the two new destinations on the same port, e.g. 2162 and 1162.

3) Adjust the listening programs to listen on the new ports rather than 162. For example, for Entuity set *trapportnumber* to 2162.

4) From the command line start `trapsplit` to forward each SNMP trap to the two ports.

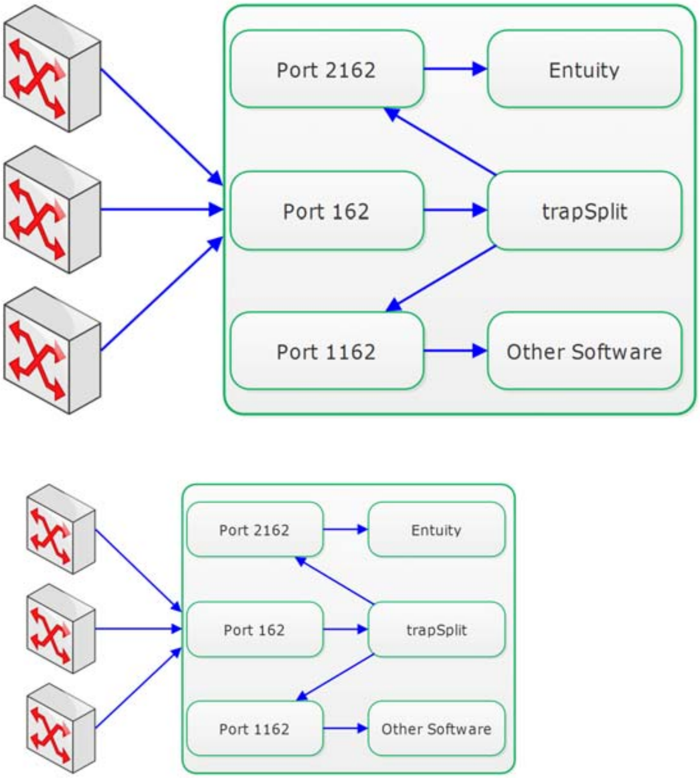


Figure 310 Example Receiving Traps

5) From UDP port 2162 `prologV2` accepts the traps. Event Viewer displays these forwarded traps as events, together with the originating agent address taken from the PDU header.

Where third party software uses SNMP libraries that ignore the PDU AGENT-ADDR field (removed from SNMPv2) and take the source from the UDP header, then the originator of the

SNMP trap appears to be the `trapsplit` host and not the original device. This is a general problem with SNMP trap forwarding and you should consult your vendor for a solution.

# 52 Device System Logging

Syslog is the standard event logging subsystem for Unix, although syslog programs are also available for windows implementations. Syslog consists of a server daemon, a client function library, and a client command line utility.

To configure your devices to send syslog messages refer to your device vendor's documentation.

Entuity System Logger reads system events generated for syslog. When events are generated by devices Entuity manages, then the System Logger generates an alarm that appears in Event Viewer. These messages are also forwarded to the syslog file, appearing as though they come from the localhost.

By default, the Entuity `syslogger` listens on port 514, which is the default for the syslog daemon (syslogd). If you want to run `syslogger` and syslogd then they cannot both listen on the same port. Instead, configure syslogd to listen on another port. When the syslogd port is different from the `syslogger` port, `syslogger` recognizes that syslogd is running and forwards syslog messages to the syslogd port.

## Monitored Syslog Messages

Syslog messages are prioritized by a combination of facility and urgency level:

- There are ten standard facilities and eight that can be configured for your use. These are monitored by the Entuity System Logger.

| Facility | Description |
|---|---|
| kern | Kernel messages. |
| user | User-level messages. |
| mail | Mail subsystem. |
| daemon | System daemons. |
| auth | Security/authorization messages. |
| syslog | Internally generated syslogd messages. |
| lpr | Printer subsystem. |
| news | Usenet news subsystem. |
| uucp | Unix to Unix Copy Program subsystem. |
| cron | Clock daemon. |
| local0 | Reserved for local use. |
| local1 | Reserved for local use. |
| local2 | Reserved for local use. |

Table 52 System Logging Error Messages

| Facility | Description |
|---|---|
| local3 | Reserved for local use. |
| local4 | Reserved for local use. |
| local5 | Reserved for local use. |
| local6 | Reserved for local use. |
| local7 | Reserved for local use. |

Table 52 System Logging Error Messages

- The various urgency levels are listed in order. When you specify a level in `entuity.cfg` you are selecting that level and all of the levels above it.

| Level | Level name | Description |
|---|---|---|
| 0 | emerg | System is unusable. |
| 1 | alert | Immediate action required. |
| 2 | crit | Critical condition. |
| 3 | err | Error condition. |
| 4 | warning | Warning condition. |
| 5 | notice | Normal but significant condition. |
| 6 | info | Informational. |
| 7 | debug | Debugging messages. |

Table 53 System Logging Message Urgency Levels

Through the syslogger section in `entuity.cfg` you can set the combination of facility source and urgency level System Logger accepts.

## Processing Monitored Messages

Syslog messages are free form text, containing five types of information:

- message text.
- machine source.
- timestamp.
- facility.
- urgency level.

`syslogger` accepts the syslog message and generates an Entuity event when the Facility and Urgency level meet the conditions specified in the syslogger section of `entuity.cfg`.

In `entuity.cfg` you can limit `syslogger` to only handle messages from devices Entuity manages.

`syslogger` takes the information from the syslog message and, where the devices are managed by Entuity, uses the Entuity database to identify the device and possibly add additional information, e.g. CPU utilization, buffer capacity and mismatches in protocol.

Syslog event details has the format:

```
tag:message
```

where:

- *tag* indicates the syslog message type, e.g.:
  - %PAGP-5-PORTFROMSTP, a spanning tree messages
  - %LINK-3-UPDOWN, a link up and down (physical)
  - %LINEPROTO-5-UPDOWN, a line up and down (layer 2)
- *message*, the content of the syslog message.

## Controlling the Display of Syslog Messages

A network can generate a large number of syslog messages, many of which may not be required for the network role that you have assigned. For example if you are troubleshooting network problems you only require a subset of syslog messages to raise incidents to notify you of where there are problems on the network. Through careful configuration of how Entuity handles Syslog messages you can control the number of messages the Event Management System handles therefore maintaining its performance.

You can use Entuity and its Event Management System to:

- Set up a Syslog input filter so that Event Management System only processes Syslog messages that are essential for trouble-shooting purposes, discarding all others before they enter the monitoring solution. Event Management System does not create events for these Syslog messages.
- Set up a Discard Syslogs filter at the Event Management System’s Post-Storage processing stage. This prevents Event Management System from raising and processing Syslog incidents. These Syslog messages did raise events and these events are still available.
- Set up a Syslog specific view. This view only presents Syslog event details to users that have specifically requested the information through the configuration of their user interface.

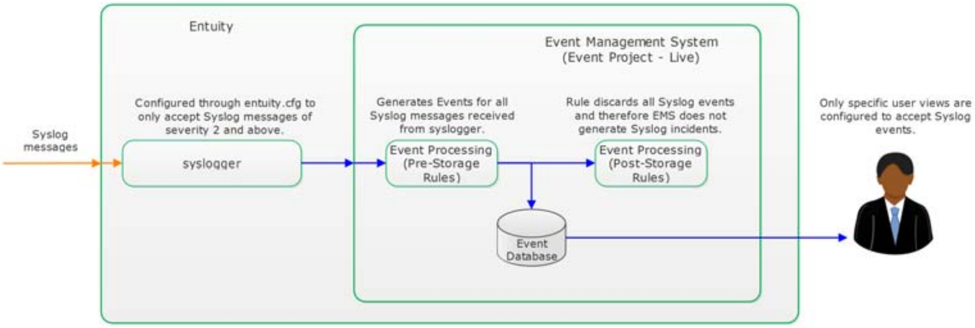


Figure 311 Syslog Filtering

## Set a syslogger Filter

Configuration of Entuity's Syslog receiver, `syslogger`, is through the syslogger section of *entuity_home*`\etc\entuity.cfg`. `syslogger` accepts Syslog messages and forwards them to the Event Management System where events and incidents are raised. You can filter the Syslog messages `syslogger` accepts by *Facility* and by *Severity*. By default `syslogger` accepts Syslog messages of all *Facilities* and of *Severity* **notice** or more severe (severities 0 to 5). Entuity Support recommend all unnecessary Syslog messages are discarded at this first filter.

This example section configures `syslogger` to only accept messages that are: from Entuity managed devices; received on port 514; either of message type mail with a log level of debug or higher, or kern with a log level of **crit** or higher.

```
[syslogger]
loglevel=crit
portnum=514
openReceiver=0
acceptfacs=mail.debug,kern.
```

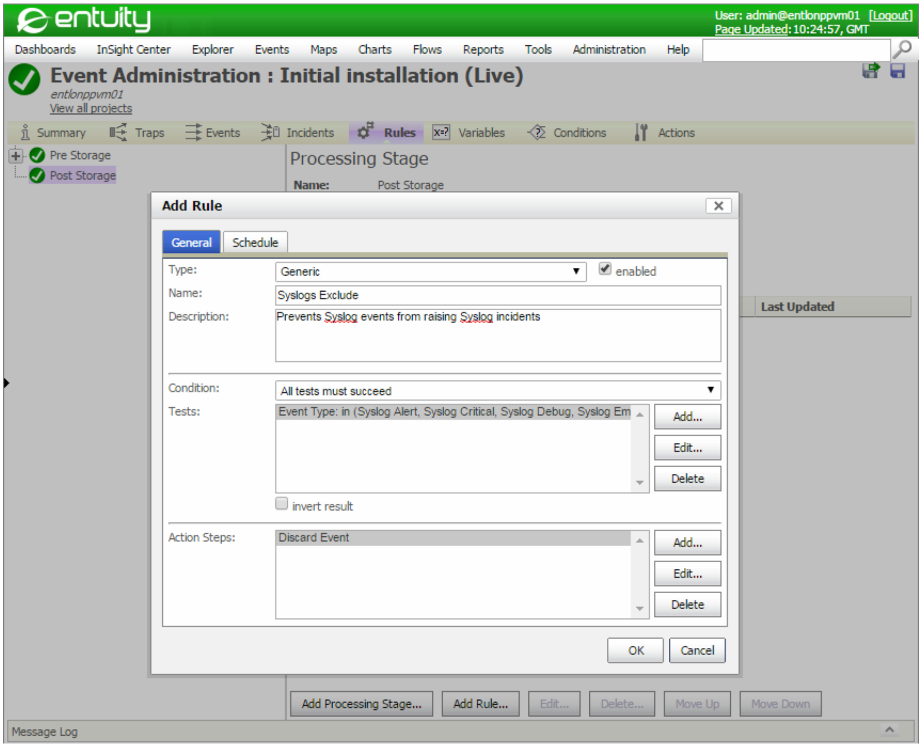
## Event Management System Post-Storage Filter

To reduce the processing performed by the Event Management System and to only deliver the required Syslog events this example prevents the raising of Syslog incidents.

The Syslogs Exclude post storage rule:

- Tests for all Syslog event types.
- Has one action, Discard Event. This does not delete the event from the Event Management System but it does prevent the event from raising an incident.

After creating the rule you must Save and Deploy the updated Event Project for it to take effect.



Name: Post Storage

Type: Generic ☑ enabled

Name: Syslogs Exclude

Description: Prevents Syslog events from raising Syslog incidents

Condition: All tests must succeed

Tests: Event Type: in (Syslog Alert, Syslog Critical, Syslog Debug, Syslog Em

□ invert result

Action Steps: Discard Event

Figure 312 Syslog Filtering Rule

## Set Up View and View Filters

The views a user has access to should always be configured to only present the information that they require. In the same way a view should only contain the devices a user requires, the view should only present the events and incidents the user requires. Correctly configured event and incident filters prevent a user’s UI from being flooded with information on network events in which they are not interested. User’s with appropriately configured views will be more efficient, as will the performance of their web client.

Entuity Support recommend:

- That by default you configure all event and incident filters to exclude Syslog events and incidents.
- That you create Syslog specific views which only includes Syslog events. This view would only be available to users monitoring Syslog messages.

To create a view that only includes Syslog events:

1) From Explorer highlight a server and click **Create View**.

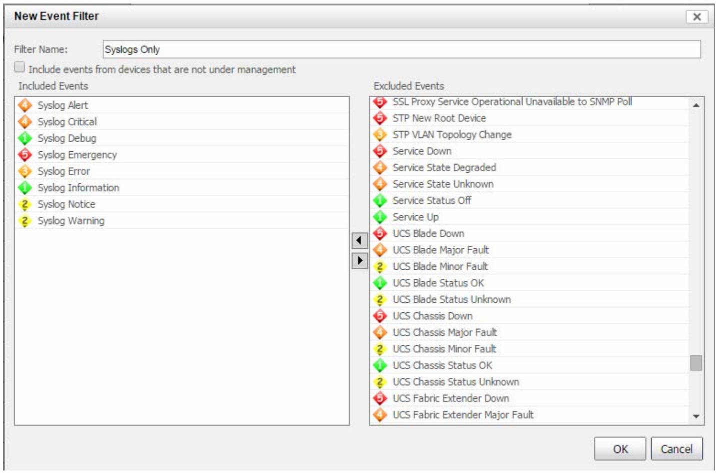
2) Set up the view content.

3) Click the Events tab. The highlighted event filter is the one currently applied to the view.

4) Click **New**.

5) Enter a descriptive event filter name, e.g. Syslogs and set-up its events. Ensure the 8 Syslog events are the only events in the Included Events column.

For all views to which you do not want to include Syslog events you must ensure that their event filters explicitly exclude Syslog events.



Filter Name: Syslogs Only

□ Include events from devices that are not under management

Included Events

- Syslog Alert
- Syslog Critical
- Syslog Debug
- Syslog Emergency
- Syslog Error
- Syslog Information
- Syslog Notice
- Syslog Warning

Excluded Events

- SSL Proxy Service Operational Unavailable to SNMP Poll
- STP New Root Device
- STP VLAN Topology Change
- Service Down
- Service State Degraded
- Service State Unknown
- Service Status Off
- Service Up
- UCS Blade Down
- UCS Blade Major Fault
- UCS Blade Minor Fault
- UCS Blade Status OK
- UCS Blade Status Unknown
- UCS Chassis Down
- UCS Chassis Major Fault
- UCS Chassis Minor Fault
- UCS Chassis Status OK
- UCS Chassis Status Unknown
- UCS Fabric Extender Down
- UCS Fabric Extender Major Fault

Figure 313 Include Syslog Event Filter

6) Click **OK**.

7) When you want to use the new filter for the current view, highlight the filter and click **OK**. You can use this filter for nay other views in which you only want to raise Syslog events.

# 53 SNMP Trap Forwarding

Through the Event Management System you can forward to third party trap receivers SNMP traps generated from Entuity events and incidents. Entuity SNMP trap forwarding can be used to provide two way integrations with any third party software that can handle SNMP trap data, for example as Dell Foglight, HP OpenView, IBM Tivoli Netcool.

You can define rules to forward events as traps and triggers to forward incidents as traps. You can control the type of events and incidents that generate traps, when they are forwarded and to where they are forwarded.

Entuity can automatically detect whether it is sending an event or an incident and then use the appropriate varbinds when building the trap. Also through the Event Management System you can generate a MIB file that details the events and incidents in the selected event project. You can then load this MIB file to the trap receiving software so it can interpret the incoming Entuity traps.

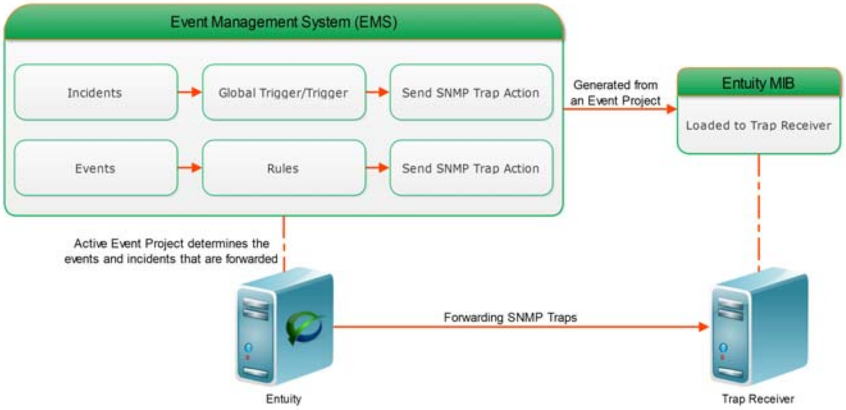


Figure 314 Send SNMP Trap Architecture

## Forward SNMP Traps

Through the Event Management System you can configure forwarding of SNMP Traps using the Send SNMP Trap action. You can forward as SNMP traps:

- Incidents by associating the Send SNMP Trap action to a Global Trigger or to triggers defined against selected incidents.
- Events by associating the Send SNMP Trap action to rules.

Entuity determines whether it is forwarding as a trap an event or incident and uses the relevant varbind list when building the trap. When associating the Send SNMP Trap action to a trigger or rule you must configure the destination details of the trap, the varbind list is usually not configurable.

The trap receiving software may handle traps in the same way regardless of whether they originated as Entuity events or incidents. Entuity Support recommends forwarding either events or incidents but not forwarding both to the same trap receiver.

## Set Send SNMP Trap Action Parameters

The Send SNMP Trap action is implemented through a Groovy Script. You must amend the script parameters to match the requirements of successfully sending traps to the trap receiver.

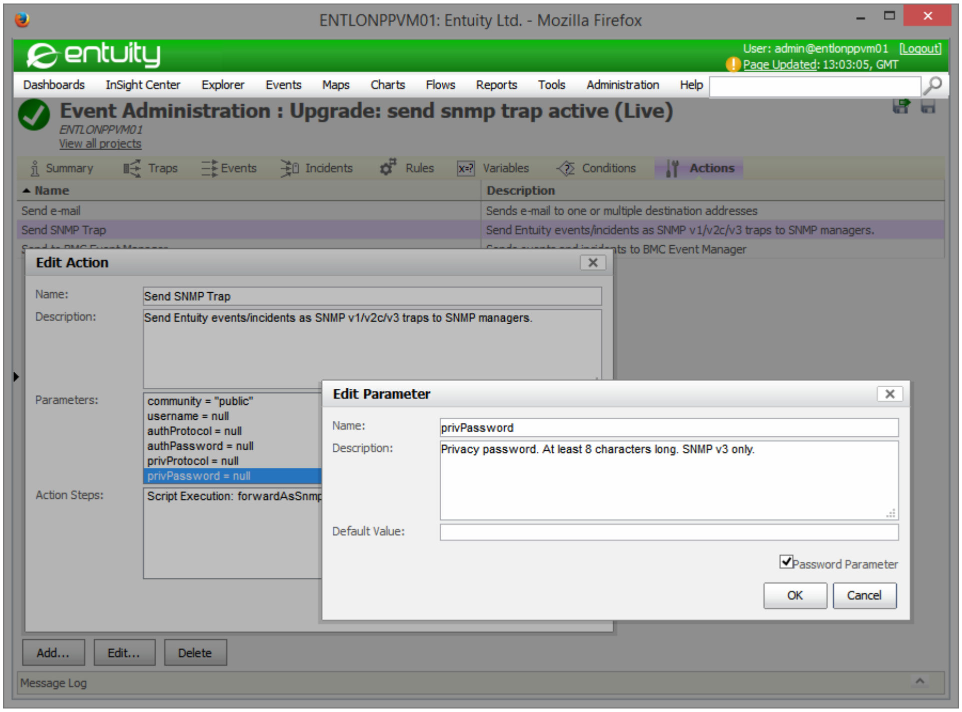
| Attribute | Description |
|---|---|
| *host* | Resolved hostname or IP address of the receiving third party software. |
| *port* | Trap receiving port of the receiving third party software. |
| *version* | SNMP trap version, i.e. 1, 2 or 3. |
| *community* | SNMPv1/v2c setting. Read community string. |
| *username* | SNMPv3 setting. Security username. |
| *authProtocol* | SNMPv3 setting. There are three levels of authentication null, MD5 or SHA. |
| *authPassword* | SNMPv3 setting. Authentication password required when *authProtocol* is set to MD5 or SHA.)<br>The password must be at least 8 characters long. The parameter value must be enclosed in quotes, so the minimum entered length is 10 characters. |
| *privProtocol* | SNMPv3 setting. There are three levels of encryption, i.e. null, DES and AES. |
| *privPassword* | SNMPv3 setting. Encryption password required when *privProtocol* is set to DES or AES.<br>The password must be at least 8 characters long. The parameter value must be enclosed in quotes, so the minimum entered length is 10 characters. |

Table 54 SNMP Trap Parameters

SNMPv3 traps require an engine identifier and by default Entuity uses its server identifier (available in `entuity.cfg` from *`server.id`*). You can override this default value through the `entuity.cfg` setting *`events`.engineIdOverwrite.* The new value must be a hexadecimal string that only uses the symbols 0-9 and A-F and is at least 5 bytes long but no more than 32 bytes.

You can configure the destination of SNMP traps, specifically:

- Amend its defaults, for example to set the hostname of the third party software.
- Set whether a parameter should be handled as a password, i.e. displayed as asterisks rather than as plain text and Triple DES (3DES) encrypted if the project is exported.



Event Administration : Upgrade: send snmp trap active (Live)

ENTLONPPVM01

View all projects

| Name | Description |
|---|---|
| Send e-mail | Sends e-mail to one or multiple destination addresses |
| Send SNMP Trap | Send Entuity events/incidents as SNMP v1/v2c/v3 traps to SNMP managers. |
| Send to BMC Event Manager | Sends events and incidents to BMC Event Manager |

Edit Action

Name: Send SNMP Trap

Description: Send Entuity events/incidents as SNMP v1/v2c/v3 traps to SNMP managers.

Parameters:

```
community = "public"
username = null
authProtocol = null
authPassword = null
privProtocol = null
privPassword = null
```

Action Steps: Script Execution: forwardAsSnmp

Edit Parameter

Name: privPassword

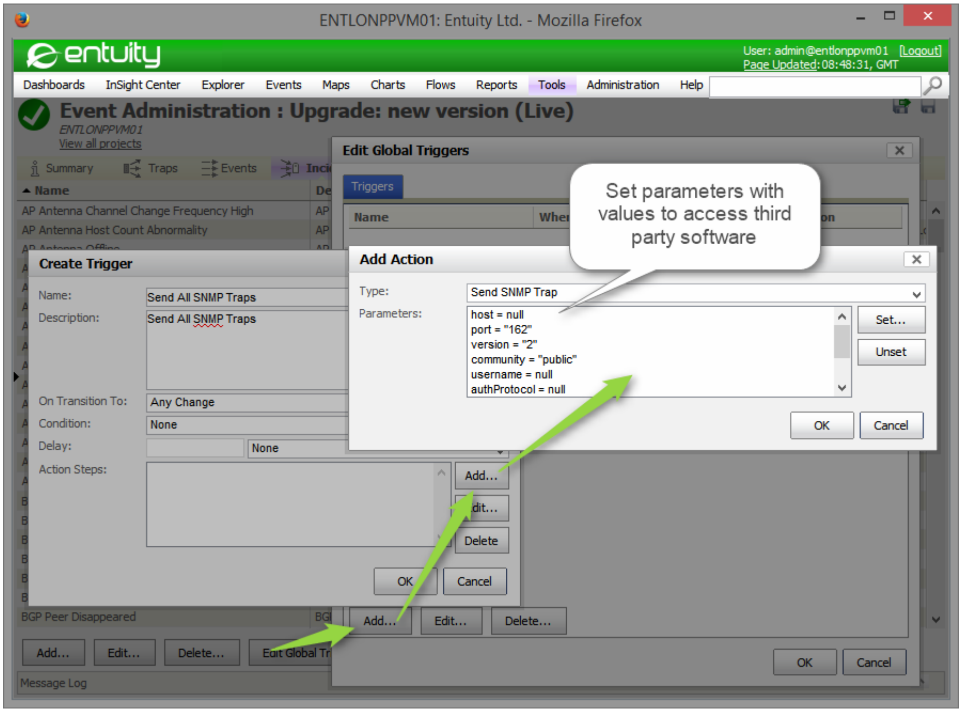
Description: Privacy password. At least 8 characters long. SNMP v3 only.

Default Value:

☑ Password Parameter

Figure 315 Edit Password Parameter

When you associate the action to a rule or trigger you can amend the parameter values used with that rule or trigger. You cannot amend the parameter type or change the varbinds. The action definition must include the address of the receiving software.



Name: Send All SNMP Traps

Description: Send All SNMP Traps

On Transition To: Any Change

Condition: None

Delay: None

Type: Send SNMP Trap

Parameters:

```
host = null
port = "162"
version = "2"
community = "public"
username = null
authProtocol = null
```

Set parameters with values to access third party software

Figure 316  Set Up a Global Trigger

## Default Event and Incident Varbind Lists

The Entuity Send SNMP Trap action includes a default list of varbinds. Entuity identifies whether the trap it is generating is based upon an Entuity event or incident and selects the relevant event or incident list of varbinds.

If you want to add custom varbinds to these SNMP traps contact Entuity Professional Services.

Each varbind element has these attributes:

- Object Identifier (OID), the object identifier that identifies the MIB instance.
- Data Type, the default varbinds are either Integer32 or String.
- Value, the value of the MIB instance.

| Default Varbinds | Description |
|---|---|
| *eDescription* | Description of the event. |
| *eDetails* | Event name. |

Table 55  Default Varbind List

| Default Varbinds | Description |
|---|---|
| *eNumHigh* | The higher 32 bits of the generated unique event number. |
| *eNumLow* | The lower 32 bits of the generated unique event number. |
| *eObjectSummaryURL* | URL of the object. It links to the object summary page on the Entuity server. |
| *eSeverity* | Event severity level. |
| *eTypeIDHigh* | The higher 32 bits of the type identifier of the event. |
| *eTypeIDLow* | The lower 32 bits of the type identifier of the event. |
| *iNumHigh* | The higher 32 bits of the generated unique incident number. |
| *iNumLow* | The lower 32 bits of the generated unique incident number. |
| *iTypeIDHigh* | The higher 32 bits of the type identifier of the incident. |
| *iTypeIDLow* | The lower 32 bits of the type identifier of the incident. |
| *iDescription* | Description of the incident. |
| *iDetails* | Name of the incident. |
| *iLastUpdateTime* | Timestamp the incident was last updated. |
| *impactDescr* | Impacted object. |
| *iObjectSummaryURL* | URL of the object. It links to the object summary page on the Entuity server. |
| *iOpenTime* | Timestamp the incident was first opened. |
| *iSeverity* | Severity of the incident. |
| *objCompID* | Internal object identifier. |
| *objDescr* | The object this incident happens on, can be a port, a device or a service. |
| *objServerID* | Entuity server identifier. |
| *objSWID* | Internal StormWorks identifier. |

Table 55 Default Varbind List

Entuity internal identifiers are 64-bit integers however the MIB only supports 32-bit integers. Therefore Entuity forwards each 64-bit integer as two separate high and low varbinds, e.g. *eNumHigh*, *eNumLow*.

## Forwarding Entuity Incidents as SNMP Traps

You can set up forwarding of incidents as SNMP traps by setting a trigger against selected incidents or by defining a global trigger.

This example forwards Entuity incidents:

- With an event severity level of Information or greater and on any change to the incident status. Depending upon the capabilities of the receiving trap software this can be used to track the opening and closing of incidents.
- Using a new Global Trigger.

- To the trap receiver 10.44.1.157.

To forward incidents as SNMP traps:

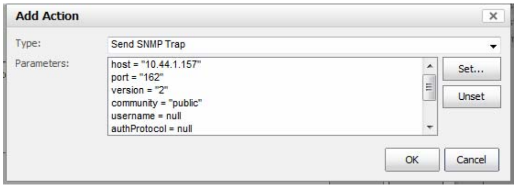
1) Click **Administration > Events > Event Administration**.

2) Click **Incidents**.

3) Click **Edit Global Triggers** and then **Add**.

4) Define the new trigger:

   - Enter a meaningful *Name* and *Description* for the trigger.
   - Set *On Transition To* to **Any Change**.
   - Set *Condition* to **None**.
   - Add to *Action Steps* the **Send SNMP Trap** action and set the host value to the IP address of the receiving software. You must enter the IP address in quotes, e.g. **"10.44.1.157"**.



Add Action

Type: Send SNMP Trap

Parameters:

```
host = "10.44.1.157"
port = "162"
version = "2"
community = "public"
username = null
authProtocol = null
```

Figure 317 Add SNMP Trap Forwarding Destination

5) Click **OK**.

6) Click the **Save and Deploy** icon. This saves your trigger changes to the current event project and then deploys the project. The new global trigger is now active.

## Forwarding Entuity Events as SNMP Traps

This example forwards Entuity events:

- In the Madrid view with an event severity level greater than Information.
- Using a new rule added to the **Pre Storage > Initial Filtering** processing stage.
- To the trap receiver 10.44.1.157.

To forward events as SNMP traps:

1) Click **Administration > Events > Event Administration**.

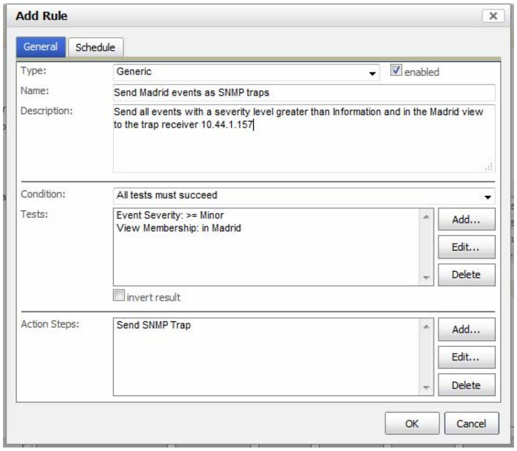
2) Click **Rules**.

3) Click **Pre Storage > Initial Filtering** and from the context menu select **Add Rule**.

4) Define the new rule:

   - Ensure *Type* is to **Generic** and *enabled* is selected.
   - Enter a meaningful *Name* and *Description* for the rule.

- Set *Condition* to **All tests must succeed** and add:
  - An **Event Severity Type** test with the *Expression* set to **Minor** or **higher**.
  - A **View Membership Test** with the view set to the required view, e.g. Madrid.
- Add to *Action Steps* the **Send SNMP Trap** action and set the host value to the IP address of the receiving software. You must enter the IP address in quotes, e.g. **"10.44.1.157"**.



Type: Generic ☑ enabled

Name: Send Madrid events as SNMP traps

Description: Send all events with a severity level greater than Information and in the Madrid view to the trap receiver 10.44.1.157

Condition: All tests must succeed

Tests: Event Severity: >= Minor
View Membership: in Madrid

□ invert result

Action Steps: Send SNMP Trap

Figure 318 Add SNMP Trap Forwarding Rule

5) Click **OK**.

   Entuity adds the new rule to the Initial Filtering processing stage.

6) Click the **Save and Deploy** icon. This saves your rule changes to the current event project and then deploys the project. The new rule is now active.

## Checking What Entuity Has Forwarded

The Action Steps of the Send SNMP Trap action are implemented through Groovy Script. When you want to check the traps Entuity is forwarding you should check the Groovy Script log file, *entuity_home*`\log\groovyEvents.log`.

Each line in the log file reports on the success or failure of forwarding an event or incident, for example:

```
03/23/2015 18:16:16 Forward 'Device Not Responding to SNMP' as SNMP
trap to 10.44.1.157:162 SUCCEEDED

03/23/2015 18:17:31 Forward 'Device Average CPU Utilization High' as
SNMP trap to 10.44.1.157:162 SUCCEEDED
```

By default log entries are chronologically ordered, the Entuity event or incident named, the receiving software clearly identified and the success of the operation detailed.

# Generate an Entuity MIB File for Trap Receivers

For the third party trap receiver to handle traps sent to it by Entuity, the trap receiver must recognize the trap's object identifiers (OIDs). You must therefore load to your trap receiver an Entuity MIB which details Entuity events and incidents.

Entuity MIBs are derived from the selected event project. An Entuity MIB includes:

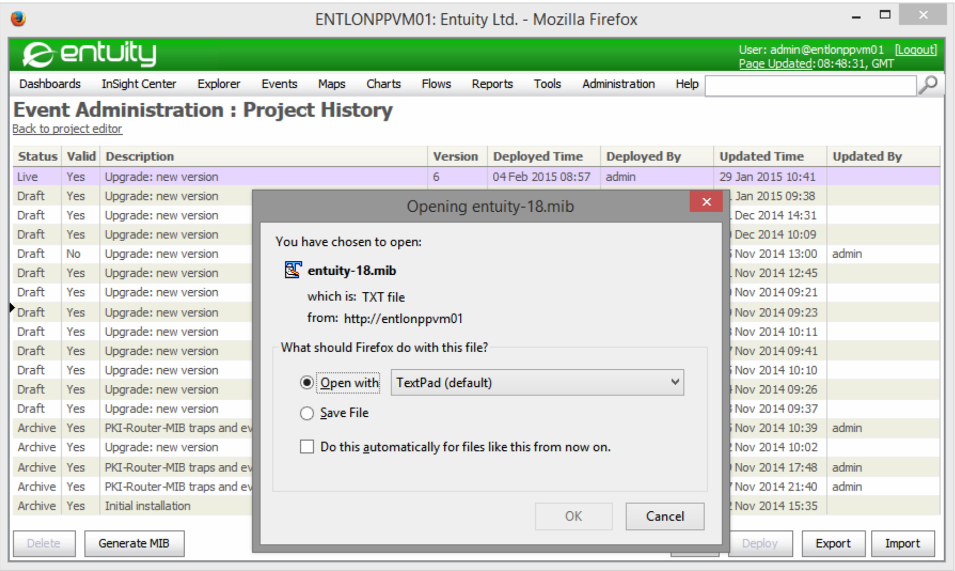
- One trap definition for each event in the event project.
- Two trap definitions, update and close, for each incident in the event project.

If you update the event project with new incidents or events that you want to forward as SNMP traps then you must generate a new Entuity MIB file and load it to the trap receiver.

To generate an Entuity MIB:

1) Click **Administration** > **Events** > **Event Administration**.
2) Click **View all projects**.
3) From the list of event projects highlight the project you want to use to generate the Entuity MIB and click **Generate MIB**.

   Entuity generates a MIB file called `entuity-[project id].mib` and opens a dialog from which you can open or download the MIB file. You can then install the MIB file to the trap handling third party software.



Event Administration : Project History

Back to project editor

| Status | Valid | Description | Version | Deployed Time | Deployed By | Updated Time | Updated By |
|---|---|---|---|---|---|---|---|
| Live | Yes | Upgrade: new version | 6 | 04 Feb 2015 08:57 | admin | 29 Jan 2015 10:41 | |
| Draft | Yes | Upgrade: new version | | | | Jan 2015 09:38 | |
| Draft | Yes | Upgrade: new version | | | | Dec 2014 14:31 | |
| Draft | Yes | Upgrade: new version | | | | Dec 2014 10:09 | |
| Draft | No | Upgrade: new version | | | | Nov 2014 13:00 | admin |
| Draft | Yes | Upgrade: new version | | | | Nov 2014 12:45 | |
| Draft | Yes | Upgrade: new version | | | | Nov 2014 09:21 | |
| Draft | Yes | Upgrade: new version | | | | Nov 2014 09:23 | |
| Draft | Yes | Upgrade: new version | | | | Nov 2014 10:11 | |
| Draft | Yes | Upgrade: new version | | | | Nov 2014 09:41 | |
| Draft | Yes | Upgrade: new version | | | | Nov 2014 10:10 | |
| Draft | Yes | Upgrade: new version | | | | Nov 2014 09:26 | |
| Draft | Yes | Upgrade: new version | | | | Nov 2014 09:37 | |
| Archive | Yes | PKI-Router-MIB traps and ev | | | | Nov 2014 10:39 | admin |
| Archive | Yes | Upgrade: new version | | | | Nov 2014 10:02 | |
| Archive | Yes | PKI-Router-MIB traps and ev | | | | Nov 2014 17:48 | admin |
| Archive | Yes | PKI-Router-MIB traps and ev | | | | Nov 2014 21:40 | admin |
| Archive | Yes | Initial installation | | | | Nov 2014 15:35 | |

Opening entuity-18.mib

You have chosen to open:

**entuity-18.mib**

which is: TXT file

from: http://entlonppvm01

What should Firefox do with this file?

● Open with TextPad (default)

○ Save File

□ Do this automatically for files like this from now on.

OK Cancel

Figure 319 Generate an Entuity MIB File

# 54 Forward Events

Event Forwarding allows Entuity to forward events to third party software. You can determine which events to forward based on one or more of the:

- Event type.
- Event source.
- Event destination. Event Forwarding allows forwarding of events to more than one third party software and more than one instance of that software.

The details Entuity forwards for each events are configurable, but may include the event's:

- Source.
- Impact details.
- priority level.

Event Forwarding is a general application suitable for use with a number of different products.

## Install Event Forwarding

Event Forwarding functionality is included with the standard Entuity installation, and is installed but not activated, on the Entuity server. Event Forwarding requires Entuity and the receiving third party software are installed and running, with permitted communication between the two.

`ForkEvent` is the main Event Forwarding executable, and is installed to:

*entuity_home*`/integ/ForkEvent/`

`forkevent.cfg` is the event forwarding configuration file, installed to:

*entuity_home*`/etc/`

## Event Forwarding Integration Architecture

The Entuity Event Forwarding integration involves:

1) Entuity collecting event data.
2) ForkEvent configured to run in either Fork or Pipe mode. Configuration is through a combination of command line and configuration file parameters.
3) When Entuity recognizes an applicable event and ForkEvent is running in:
   - Fork mode, ForkEvent starts a Fork process. This process sends the data to the third party software, and then terminates. Each event results in a new Fork process.
   - Pipe mode, ForkEvent sends the event data to the stdin of the Pipe process. The Pipe process starts running when ForkEvent is started and continues until ForkEvent is

stopped.

4) Both Fork and Pipe forward event data to the integrated software. This software must be configured to receive the Entuity event data.

5) The integrated software can now handle the event data and, for example, display it through a console.

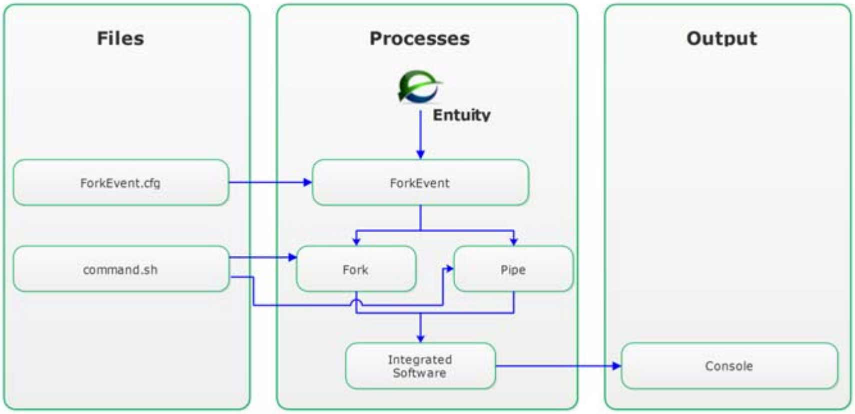


Figure 320 Entuity Event Forward Integration

## Event Forwarding Configuration File

The Event Forwarding configuration file, e.g. `forkevent.cfg`, contains details used to:

- Access the Entuity database.
- Determine whether the Event Forwarding uses the Fork or Pipe processes.
- Determine the format and order in which that event data is passed to the integrated product.

There are a number of sections, each starts with its section name, enclosed within square brackets, e.g. [connection] and [data]. All variable definitions are held within sections. These sections can be divided into three types:

- Connection section contains details required to access the Entuity database (see *Connection Section*).
- Process section determines whether the Fork or Pipe process is used, also which parameters are passed. You can specify one or more process sections, which one is used is passed as an argument when running ForkEvent (see *Process Sections*).
- Data section details the events passed to the Pipe process (see *Data Section*).

! Entuity supply an example file, ForkEvent.cfg. You should read this section and then take a backup of the file before attempting to amend it.

## Connection Section

This section details the information required to access Entuity to collect event data. This is an example section:

```
[connection]
username=admin
view=All Objects
extendedEvents=0
```

where:

- *[connection]* is the name of the section that contains the details required to access Entuity event data.
- *username* is the Entuity login name.
- *view* is the Entuity view from which events are collected. Only when an event occurs on a device within the defined view is it forwarded by ForkEvent.
- *extendedEvents* sets the maximum number of characters that forkevent forwards for the event description. Event descriptions greater than this setting are truncated. When set to:
  - 0 (default), forwards event descriptions to a maximum of 127 characters.
  - 1, forwards event descriptions to a maximum of 4095 characters. Extended event descriptions are not currently stored in the Entuity database.

## Process Sections

The process sections define:

- Which ForkEvent process, Fork or Pipe, is used.
- The arguments passed to the process.

A configuration file can have more than one process definition, although only one is used at any one time. This is passed as an argument when ForkEvent is run. (See *Run Event Forwarding*.)

This is an example section:

```
[pipe_nt]
start=H:\master\src\integration\bins\ForkEvent\ForkEventNT
args=pipe ${connection.username}
EmptyVariable=MISSING_VALUE
type=pipe
directory=H:\master\src\integration\bins\ForkEvent
```

```
loglevel=all
```

Where:

- *[pipe_nt]* is the section name. This is passed as a parameter with the ForkEvent command.
- *start* runs the specified executable. When *type* is:
  - **fork**, *start* runs when ForkEvent receives an event.
  - **pipe**, *start* runs as soon as ForkEvent runs, creating the Pipe process.

  As well as running Pipe and Fork directly, they can be run through a script or executable. For example a shell script that calls the ForkEvent process, passes arguments, or any other legitimate script instruction.
- *type* is the type of process, i.e **fork** or **pipe**.

Only *type* and *start* are mandatory parameters.

- *args* allow you to pass command line arguments with the Pipe and Fork processes. You can pass values taken from the:
  - Event data, e.g. ${event.PAPIID}.
  - Configuration file itself, e.g. ${connection.username}, where connection is the section name and username the variable name.
- *EmptyVariable* is used to enter a value in an event variable passed from Entuity that does not contain any data, i.e. to make it easier to identify in the integrated package. By default EMPTY_VARIABLE is entered, using *EmptyVariable* you can replace that with one of your choice, e.g. MISSING_VALUE.
- *directory* is the directory from which the process is run and log files are written to.
- *loglevel* is the level of logging information recorded, i.e. **errors**, **warning**, **info**, **debug** and **all**.

### Running a Script

These example section illustrate the format for invoking a script that handles the fork process. The structure for Linux (fork_unix) and Windows (fork_win) is similar:

```
[fork_unix]
start=/bin/sh
args=/Entuity/scripts/evchild.sh
   = ${event.PAPIId}
   = ${event.PAPIEventStr}
   = ${event.PAPIEventGroup}
   = ${event.PAPIDescr}
# Can include a few words from your sponsor if you like
   = Entuity Events
   = ${event.PAPIImpact}
   = ${event.PAPIImpactDescr}
   = ${event.PAPIDetails}

[fork_win]
type=fork
directory=${logdir}
start=c:\Cygwin\bin\bash
args=c:\scripts\evchild.bash
   = ${event.PAPIId}
   = ${event.PAPIEventStr}
   = ${event.PAPIEventGroup}
   = ${event.PAPIDescr}
# Can include a few words from your sponsor if you like
   = Entuity Events
   = ${event.PAPIImpact}
   = ${event.PAPIImpactDescr}
   = ${event.PAPIDetails}
```

where:

- *start* sets the executable that executes the script.
- *args* includes the:
  - Script file, e.g. evchild.bash
  - Event data, e.g. ${event.PAPIID}.

In Windows for both *start* and *args* the full path must be specified.

## Data Section

This section holds the associations between labels and Entuity event variables. These labels can be used by the Pipe process to identify and manipulate event data. There must only be one data section in an Event Forward configuration file.

The data section is only used with the Pipe process. The Pipe process runs continually and it is only through the data section that arguments can be passed for each event. The Fork process is started for each event, and so arguments are passed each time an event occurs.

This is an example section:

```
[data]
```

```
ID=${event.PAPIID}
EventGroup=${event.PAPIEventGroup}
EventId=${event.PAPIEventId}
EventString=${event.PAPIEventStr}
timeStamp=${event.PAPItimeStamp}
ID1=${event.PAPIObjectID_1}
ID2=${event.PAPIObjectID_2}
ID3=${event.PAPIObjectID_3}
ID4=${event.PAPIObjectID_4}
PRI=${event.PAPISeverity}
Attr=${event.PAPIAttr}
DESCR=${event.PAPIDescr}
Impact=${event.PAPIImpact}
ImpactDescr=${event.PAPIImpactDescr}
DETAILS=${event.PAPIDetails}
```

Where:

- *[data]* is the mandatory name of the data section.
- *${event.PAPIID}* is a numeric value specifying the current instance of the event.
- *${event.PAPIEventGroup}* is a numeric value specifying the event's group.
- *${event.PAPIEventID}* is the event identifier within the context of the event group.

✓ The combination of event group and event ID uniquely identify all Entuity event types (see *Entuity Events Reference Manual*).

- *${event.PAPIEventStr}* is the description of the event associated with the event identifier.
- *${event.PAPIObjectID_1}*, *${event.PAPIObjectID_2}* and *${event.PAPIObjectID_3}* and *${event.PAPIObjectID_4}* are internal values that indicate the origin of the event.
- *${event.PAPItimestamp}* is the time the event occurred, represented as UTC (Coordinated Universal Time, i.e. the number of seconds since 1970-01-01 00:00:00 GMT).
- *${event.PAPISeverity}* is the internal value of the event severity. (See the *Entuity Events Reference Manual.*) Entuity event severity levels are:
  - 2, Information
  - 4, Minor
  - 6, Severe
  - 8, Major
  - 10, Critical.

- *${event.PAPIDescr}* is a textual description of the managed object on which the event occurred, e.g. VLAN, device, module or port.
- *${event.PAPIDetails}* is supplemental information on the particular event, e.g. actual values of network statistics which caused a threshold event.
- *${event.PAPIImpactDescr}* is entities likely to be affected by the event, e.g. hosts, VLANs and monitored applications.

Each variable name is prefaced by *event* which identifies it as a value generated during the operation of Entuity.

## Running ForkEvent

ForkEvent must be run after the Entuity server starts or is restarted. ForkEvent accesses the Entuity database using the specified event forwarding configuration file and the specified process section within it.

When ForkEvent is run the configuration file and the required process section are passed to it. From that, ForkEvent:

1) Uses details in the [connection] section to access the Entuity database.
2) Uses details in the process section to determine whether it is running in fork or pipe mode. When running in pipe mode ForkEvent starts the Pipe process.
3) When an event occurs ForkEvent can:
   - Send the event data to the stdin of the pipe process.
   - Run a new fork process.

When there are a large number of events, Fork mode can cause a significant processing overhead. A more efficient method is using ForkEvent in Pipe mode, which only uses one process.

You can also run more than one ForkEvent process at one time, although they must use different configuration files. When running multiple ForkEvent processes when an event occurs it is handled by all of the processes.

### Fork Process

When running in Fork mode each time ForkEvent recognizes an event it generates a new Fork process. As the process is created arguments detailing the event are passed to it. You can pass these arguments through *start* or *args*.

When the data is sent the process is closed. Each event has its own Fork process.

## Pipe Process

When running in Pipe mode each time a ForkEvent recognizes an event it sends the event data to the stdin of the Pipe process. The format and structure of the event data is taken from the [data] section in the configuration file.

The Pipe continues to run until it is explicitly stopped or the Entuity server is stopped. Each time a new event occurs the same ForkEvent process is used.

In Pipe mode ForkEvent sends event data in the format:

```
VariableLabel VariableValue <CR>
BlankLine <CR>
```

where:

- *VariableLabel* is the label assigned to the event data in the [data] section, e.g. Descr in Descr=${event.PAPIDescr}.
- *VariableValue* is the event data value, extracted from the [data] section, e.g. ${event.PAPIDescr} in Descr=${event.PAPIDescr}.
- *<CR>* is the end of line marker. Each value is passed on its own line.
- *BlankLine* is automatically sent at the end of the event data to signal the end of that event.

Although the Pipe command requires more time to set up, it provides for a more efficient use of machine resources, i.e. in fork mode each new event generates a new child process in pipe mode the existing pipe process is used.

## Using scripts

You can use scripts when ForkEvent is in both Pipe and Fork mode. For example, this extract from an event forward configuration file passes three arguments to the script, command.sh:

```
[pipe_nt]
start=H:\master\src\integration\bins\command.sh
args=pipe ${connection.username} ${event.PAPIImpactDescr}
```

This is the command.sh script:

```
#!/bin/sh
FILE=/tmp/com.$$
echo "1="$1>>$FILE
echo "2="$2>>SFILE
echo "3="$3>>$FILE
while read line;do
   echo "line:" $line>>$FILE
done
```

This script takes three arguments and prints them to a file. The $ variables access the sequential attributes passed with, in this integration, event data. These variables have the format $n, where n is the positional attribute. In this example, the output file could be:

```
1=pipe
2=admin
3=HOST:  00-50-8b-af-39-67
```

## Run Event Forwarding

You can only run ForkEvent when the Entuity server is running. To run ForkEvent enter:

```
forkevent ConfigurationFile SectionName
```

Where:

- `forkevent` is the process command.
- *ConfigurationFile* is the ForkEvent configuration file, e.g. `ForkEvent.cfg`.
- *SectionName* is the section within the ForkEvent configuration file that details the method and arguments for forwarding the event data, e.g. `fork_nt`.

For example:

```
forkevent /Entuity/etc/forkevent.cfg fork_nt
```

Each time you stop and start the Entuity server you must run ForkEvent.

You can run more than one ForkEvent process at one time, although they must use different configuration files. When running multiple ForkEvent processes, when an event occurs the event details are forwarded by all processes.

### Automatic ForkEvent Startup and Shutdown

You can automate starting and stopping of ForkEvent by adding it to the start up file, e.g. `startup_UNIX_site_specific`, `startup_WIN32_site_specific`:

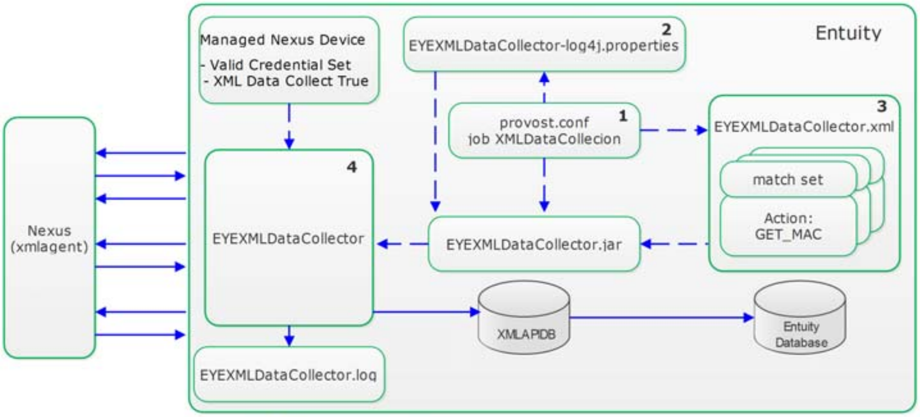
```
[forkevent]
state=normal
type=command
start=${ ENTUITY_HOME}${FPS}integ${FPS}FORKEVENT${FPS}
forkevent${ ENTUITY_HOME}{FPS}etc${FPS}forkevent.cfg fork-unix
```

# 55 XML Data Collection

Entuity can access the XML API of managed devices, query their database and integrate returned data into its database. Entuity XML Data Collection accesses the device's `xmlagent`. Although currently implemented for only Cisco devices it is extendable to other manufacturers.

Through the XML API Entuity currently retrieves the MAC addresses and interface names from the Nexus range of Cisco devices.

## XML Data Collection Implementation



**1** - provost.conf includes the job definition run by provost.
**2** - XMLDataCollector-log4j.properties sets the logging level.
**3** - XMLDataCollector.xml configures EYEXMLDataCollector.jar with the data to retrieve.
**4** - EYEXMLDataCollector creates a list of Nexus devices setup for XML data retrieval.

Figure 321 Configuration of XML Data Collection

The key components of the XML data collection implementation:

- *entuity_home*`/etc/XMLDataCollector.xml`

  Specifies how to identify a device, then apply the appropriate XML query to the device and interpret its XML reply. For example for Nexus, XML Data Collector identifies a device through its chassis identifier and system version. It can then perform the GET_MAC action with the appropriate XML configuration.

- *entuity_home*`/etc/XMLDataCollector-log4j.properties`

  Sets the level of logging applied to `EYEXMLDataCollector.jar`.

- *entuity_home*`/etc/provost.conf`

  Includes a new job `XMLDataCollection`. It runs every two hours calling the GET_MAC action.

- *entuity_home*`/lib/XMLDataCollector/EYEXMLDataCollector.jar`
  XML Data Collector jar file.
- *entuity_home*`/database/data/XMLAPIDB`
  Database used for receiving the queried XML data before it is copied into the main database. By default includes table (MacToPort) for the GET_MAC action. `macman` accesses this table when populating MAC addresses.

## Device Access for XML Data Collection

For Entuity to access the device for XML Data Collection Entuity requires:

- An appropriate set of credentials. XML Data Collection requires an SSHv2 connection to the `xmlagent` service.
- The XML Data Collection attribute on the device must be set to **True**. You can set the attribute and view its current status through the device Advanced page.

### Credential Sets

XML Data Collection uses the generic credential set mechanism also used by the Configuration Manager module. In addition to SSHv2 connections Configuration Manager also supports SSHv1 and Telnet connections which are not applicable to XML Data Collection. If you configure a credential set to use Telnet and apply it to a device on which you attempt:

- XML Data Collection, Entuity uses SSHv2.
- Configuration retrieval, Entuity uses Telnet.

In this way Entuity can support different methods of data retrieval from a device although using the same credential set.

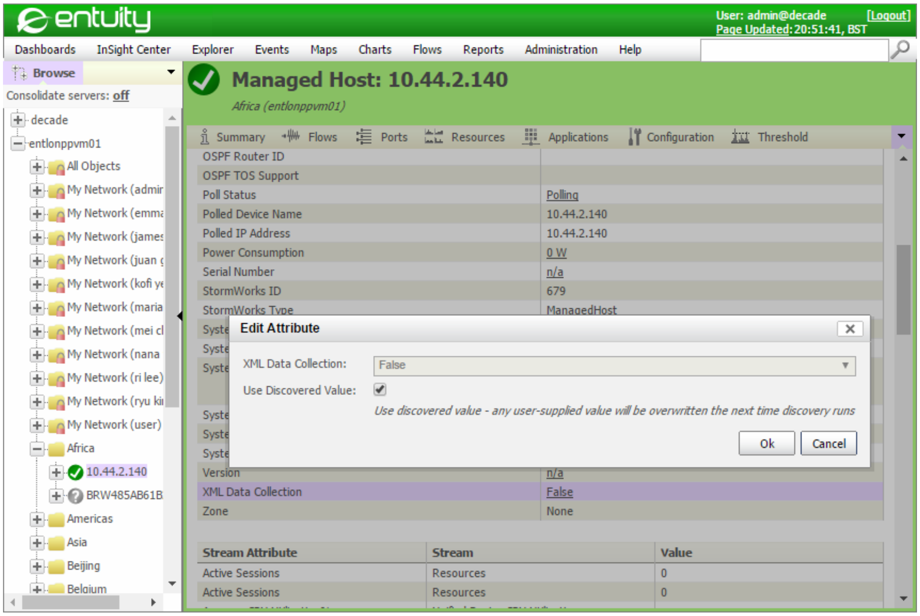
### Ready the Device for XML Data Collection

To ready a device for XML data collection set its:

- CLI access credentials.
- XML data collection to true.

You can associate a credential set and set XML data collection to **True**:

1) From the Inventory Administration page highlight a device and click Modify. (See *Modify Attributes Entuity uses to Manage a Device*.)
2) Complete the CLI Access details.
3) Click Explorer and highlight the device in the navigation tree.
4) From the device’s Advanced tab set *XML Data Collector* to **True**.



**Managed Host: 10.44.2.140**

*Africa (entlonppvm01)*

| | |
|---|---|
| OSPF Router ID | |
| OSPF TOS Support | |
| Poll Status | Polling |
| Polled Device Name | 10.44.2.140 |
| Polled IP Address | 10.44.2.140 |
| Power Consumption | 0 W |
| Serial Number | n/a |
| StormWorks ID | 679 |
| StormWorks Type | ManagedHost |
| Syste | |
| Syste | |
| Syste | |
| Syste | |
| Syste | |
| Syste | |
| Version | n/a |
| XML Data Collection | False |
| Zone | None |

**Edit Attribute**

XML Data Collection: False

Use Discovered Value: ☑

*Use discovered value - any user-supplied value will be overwritten the next time discovery runs*

| Stream Attribute | Stream | Value |
|---|---|---|
| Active Sessions | Resources | 0 |
| Active Sessions | Resources | 0 |

Figure 322 Set XML Data Collector

## NETCONF XML Message Communication

Each request and reply begins with an XML declaration indicating which version of XML and (optionally) which character set are being used. Entuity XML Data Collection connections follow a standard sequence:

- Connect to the `xmlagent` on the Device.

  XML Data Collection is through the device's `xmlagent`. Access would rely on the appropriate credential set being defined and associated with the device on the Entuity server.

- Confirm Compatible Capabilities.

  After connection to the device it first sends an XML section identifying its capabilities. Entuity responds with the same XML but removes the session identifier. This establishes the communication between Entuity and the device.

- Show Characteristics of Device.

  Entuity must identify the managed device so it can send a request in the appropriate format to retrieve its MAC addresses. The reply includes the chassis identifier and system versions string from which Entuity identifies the device (identification is through the appropriate match set section of XMLDataCollector.xml):

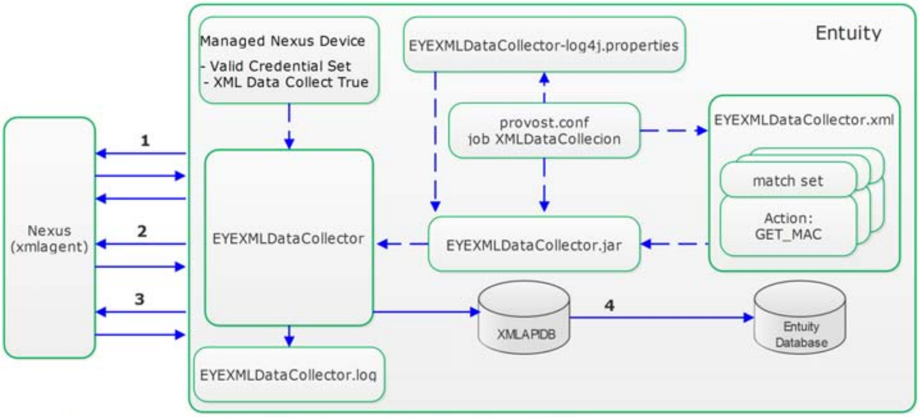
- Request Information.

  After identifying the device Entuity can configure the appropriate format for the request to retrieve MAC addresses. The device responds with an XML table of MAC addresses.

- Parse the Results, Populate XMLAPIDB and to the Entuity Database.

  Retrieved information is written to the XMLAPIDB. For the MAC Address implementation this is the PortToMac table. The standard method of integrating information from XMLAPIDB to the main database would be through StormWorks configuration and for customers this would be under the guidance of or produced by Entuity Professional Services.

  The MAC address retrieval implementation uses the non-standard method of amending a process, in this case `macman`.



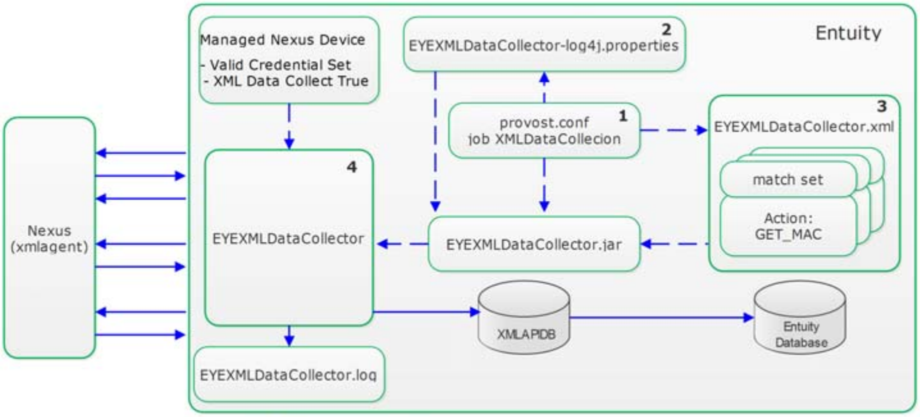
**1 -** Establish SSHv2 connection, login into xmlagent and confirm capabilities.
**2 -** Request and receive chassis and system version numbers.
**3 -** Request and receive MAC address table.
**4 -** MAC Scheme populates main Entuity database tables with MAC addresses.

Figure 323 Configuration Process of XML Data Collection

## MAC Address Retrieval

The current implementation of XML Data Collector collects MAC addresses from the Nexus range of devices. `macman` updates Entuity with the latest discovered MAC addresses. Both `macman` and the XML Data Collection jobs are scheduled through `provost.conf`. By default:

- XML Data Collector runs every 2 hours and populates the XMLAPIDB database with MAC addresses.
- `macman` runs once a day at 09:30 against every managed device and also checks for MAC addresses in the XMLAPIDB database. It also runs against individual devices every time there's a connectivity change on one of their physical ports.



**1 -** provost.conf includes the job definition run by provost.
**2 -** XMLDataCollector-log4j.properties sets the logging level.
**3 -** XMLDataCollector.xml configures EYEXMLDataCollector.jar with the data to retrieve.
**4 -** EYEXMLDataCollector creates a list of Nexus devices setup for XML data retrieval.

Figure 324 Configuration Files of XML Data Collection

## XML Data MAC Collection

Cisco Nexus 1000v devices with the sysoid `.1.3.6.1.4.1.9.12.3.1.3.840` are currently managed by Entuity using a custom device model for collecting MAC addresses from the Nexus 1000v. The XML data collection method for collecting MAC addresses supports the Nexus 1000v but is more useful when applied to other Nexus models without custom support.

Through XML data collection Entuity supports collection of MAC addresses from Nexus devices with these sysoids:

```
.1.3.6.1.4.1.9.12.3.1.3.1170
.1.3.6.1.4.1.9.12.3.1.3.1669
.1.3.6.1.4.1.9.12.3.1.3.1105
.1.3.6.1.4.1.9.12.3.1.3.719
.1.3.6.1.4.1.9.12.3.1.3.798
.1.3.6.1.4.1.9.12.3.1.3.1008
.1.3.6.1.4.1.9.12.3.1.3.612
.1.3.6.1.4.1.9.12.3.1.3.1147
.1.3.6.1.4.1.9.12.3.1.3.932
.1.3.6.1.4.1.9.12.3.1.3.777
```

When XML data collection for one of these devices is:

- Not activated then the device is managed using the existing MAC Scheme through the Bridge MIB.

- Activated but the credential sets are invalid or become invalid, the PortToMac table in the XMLAPIDB is purged of that device's entries. When `macman` runs the MAC address information is not available for that device in the XMLAPIDB and it reverts to using information collected through MAC Scheme 20.
- Activated with a valid credential set but MAC address retrieval using MAC Scheme 25 fails, for example the particular device requires a different XML query format, then Entuity again reverts to using MAC Scheme 20.
- Activated with a valid credential set and MAC address retrieval succeeds Entuity parses the retrieved information and writes it to the PortToMac table in the XMLAPIDB. `macman` would then add this information to the main database.

# 56 User Defined Polling

Entuity manages an extensive set of devices and discovers and polls a comprehensive set of attributes. However there may be occasions when you want to customize Entuity's device management, for example to:

- Provide self-service device support.

  If Entuity is managing a device that has an unusual data model and so is not collecting particular fan, power supply, memory or processor attributes then you can augment the system collectors with your own user defined collectors.

- Set up user defined attributes.

  You can define new attributes and their collectors and associate them with existing objects. For example if you want to collect additional information on all of your switch devices you can select the SwitchDevice object and create user defined attributes and collectors.

- Use predefined empty objects against which you can define attributes and collectors.

  Entuity provide 20 user defined object types (`UDComponent`*N*) that are part of the Entuity data model but are unused. As an object type is the sum of its attributes, you can configure Entuity to manage totally new components of a managed object.

✓ A collector is the mechanism for collecting data on an attribute, usually by SNMP polling of an OID. User Defined Polling is integrated with the Entuity MIB Manager through which you can import, load and browse MIBs until you select the appropriate OID for the attribute.

User Defined Polling allows you to:

- Add new attributes to existing managed objects. This applies to both:
  - System objects that are present in every Entuity installation and represent network devices, ports, modules, processors, fans and many other types of component or concept.
  - Custom objects that can be defined to represent concepts that are beyond the scope of standard Entuity discovery and monitoring support.
- Change how Entuity polls a preselected set of attributes by defining new collectors, that for example poll a manufacturer specific OID.

You can set up events against user defined attributes. You can define:

- Status events. These are events raised when the attribute value returns the set status.
- Threshold events. These are event raised when the polled attribute value is within the set ranges.

Status and threshold events have associated status and threshold incidents.

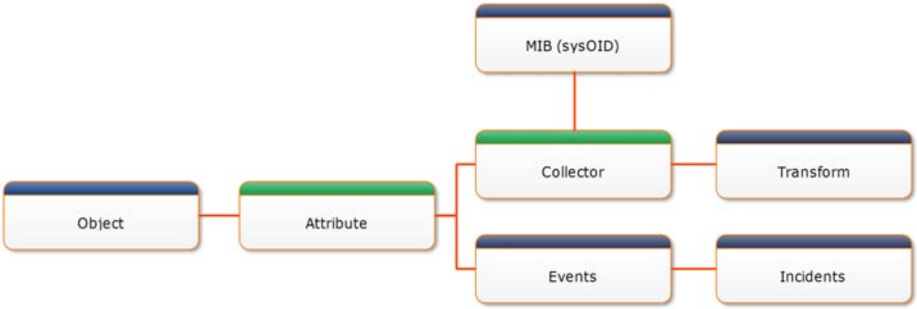


Figure 325 User Defined Polling Process

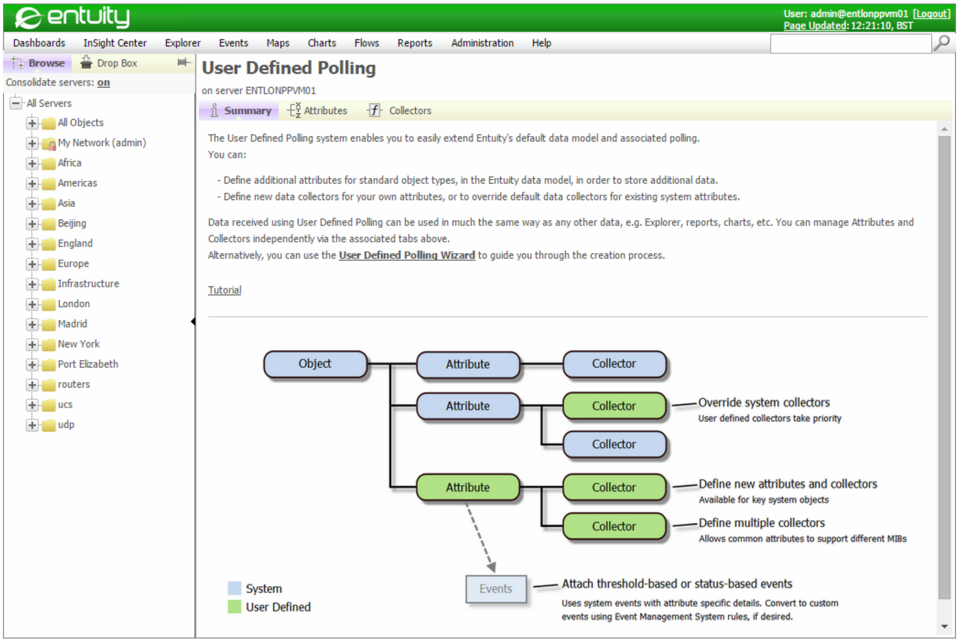
## User Defined Polling Overview

User Defined Polling is configured through the Web UI and does not usually require the running of `configure` or a system restart to implement your polling definitions.

When configuring User Defined Polling:

- Know the MIB and OID that you want to poll. User Defined Polling is integrated with the Entuity MIB Manager so you can import, load and interrogate MIBs when defining collectors.
- Select a device to set the context when defining polling through the User Defined Polling Wizard. The device should support the MIB and OIDs you are using with the collectors.

✓ Custom Polling is a separate mechanism for extending Entuity polling. Entuity Support recommend you use User Defined Polling when extending Entuity polling.



User Defined Polling

on server ENTLONPPVM01

The User Defined Polling system enables you to easily extend Entuity's default data model and associated polling.
You can:

- Define additional attributes for standard object types, in the Entuity data model, in order to store additional data.
- Define new data collectors for your own attributes, or to override default data collectors for existing system attributes.

Data received using User Defined Polling can be used in much the same way as any other data, e.g. Explorer, reports, charts, etc. You can manage Attributes and Collectors independently via the associated tabs above.
Alternatively, you can use the User Defined Polling Wizard to guide you through the creation process.

Override system collectors
User defined collectors take priority

Define new attributes and collectors
Available for key system objects

Define multiple collectors
Allows common attributes to support different MIBs

Attach threshold-based or status-based events
Uses system events with attribute specific details. Convert to custom events using Event Management System rules, if desired.

Figure 326 User Defined Polling Summary

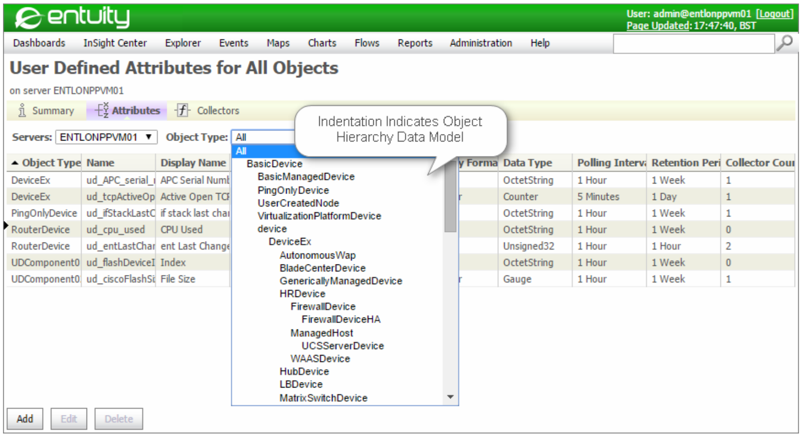
## User Defined Polling and the StormWorks Data Model

Successful implementation of User Defined Polling requires an understanding of the StormWorks data model. (See the *Entuity System Administrator Reference Manual*.) Through the User Defined Polling dialogs Entuity presents a carefully selected subset of object types and attributes.These dialogs also indent the object types to reflect the data model hierarchy.

The exact object types available depends upon your Entuity configuration, however User Defined Polling allows you to:

- Create user defined attributes for these object types and their extended types:
  - Devices
  - Ports
  - UDComponents.
- Override selected object attributes from these object types:
  - Device
  - Fan
  - Power Supply
  - UDComponents*N*
  - Memory
  - Processor.
- Override selected stream attributes from these object types:

- Fan
- Memory
- Processor.



User Defined Attributes for All Objects

on server ENTLONPPVM01

Servers: ENTLONPPVM01 ▼ Object Type: All

| ▲ Object Type | Name | Display Name | y Forma | Data Type | Polling Interv | Retention Peri | Collector Cou |
|---|---|---|---|---|---|---|---|
| DeviceEx | ud_APC_serial_ | APC Serial Numb | | OctetString | 1 Hour | 1 Week | 1 |
| DeviceEx | ud_tcpActiveOp | Active Open TCF | r | Counter | 5 Minutes | 1 Day | 1 |
| PingOnlyDevice | ud_ifStackLastC | if stack last char | | OctetString | 1 Hour | 1 Week | 1 |
| RouterDevice | ud_cpu_used | CPU Used | | OctetString | 1 Hour | 1 Week | 0 |
| RouterDevice | ud_entLastChar | ent Last Change | | Unsigned32 | 1 Hour | 1 Hour | 2 |
| UDComponent0 | ud_flashDeviceI | Index | | OctetString | 1 Hour | 1 Week | 0 |
| UDComponent0 | ud_ciscoFlashSi | File Size | r | Gauge | 1 Hour | 1 Week | 1 |

```
All
  BasicDevice
    BasicManagedDevice
    PingOnlyDevice
    UserCreatedNode
    VirtualizationPlatformDevice
    device
      DeviceEx
        AutonomousWap
        BladeCenterDevice
        GenericallyManagedDevice
        HRDevice
          FirewallDevice
            FirewallDeviceHA
          ManagedHost
            UCSServerDevice
          WAASDevice
        HubDevice
        LBDevice
        MatrixSwitchDevice
```

Indentation Indicates Object Hierarchy Data Model

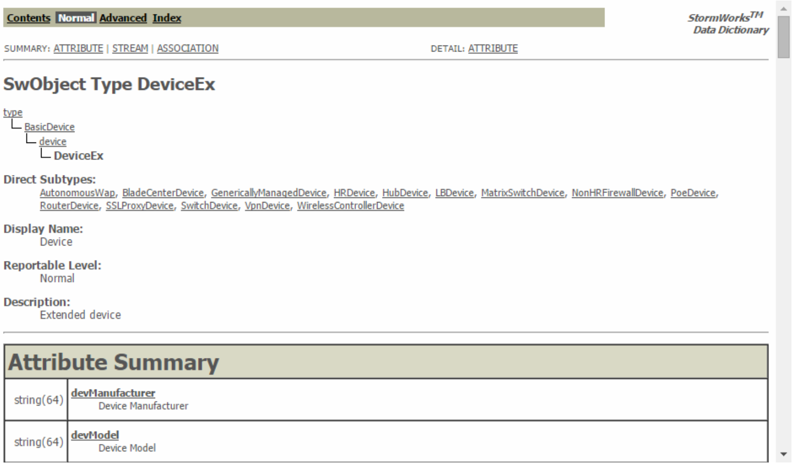
Figure 327 Object Type Hierarchy

When adding attributes you should consider the data model hierarchy when determining with which object type to associate the attribute, for example a BladeCenter specific attribute you should associate to the `BladeCenterDevice` object type and not `DeviceEx`. An attribute associated to `DeviceEx` would be available for all of its subtypes.

You can use the StormWorks Data Dictionary to interrogate the data model. To access the StormWorks Data Dictionary:

1) Click **Help** > **Contents**.

2) From the Get Started column in the Additional Documentation section click the **Entuity Data Dictionary** hyperlink.



SwObject Type DeviceEx

type
└ BasicDevice
└ device
└ DeviceEx

**Direct Subtypes:**
AutonomousWap, BladeCenterDevice, GenericallyManagedDevice, HRDevice, HubDevice, LBDevice, MatrixSwitchDevice, NonHRFirewallDevice, PoeDevice, RouterDevice, SSLProxyDevice, SwitchDevice, VpnDevice, WirelessControllerDevice

**Display Name:**
Device

**Reportable Level:**
Normal

**Description:**
Extended device

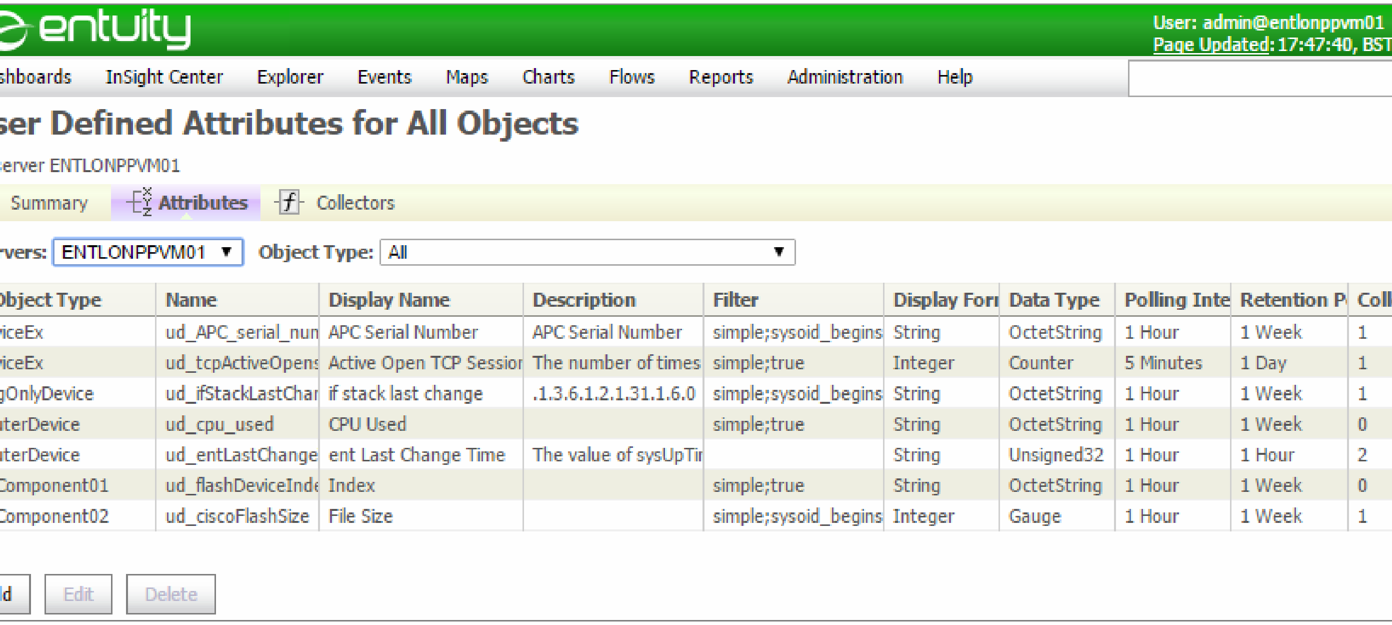
| Attribute Summary | |
|---|---|
| string(64) | **devManufacturer**<br>Device Manufacturer |
| string(64) | **devModel**<br>Device Model |

Figure 328 StormWorks Data Dictionary

## User Defined Polling of Attributes

Attributes are always associated to an object type. There are three types of attribute:

- Object, a system attribute for which a history of the attribute's values is not required as the attribute value rarely changes.
- Stream, a system attribute that is used to retain the history of the attribute's values, for example when recoding CPU utilization.
- User Defined Attribute you can use when creating new attributes. This attribute can be used both when it is important to retain the history of an attribute's values and when it is not.



User: admin@entlonppvm01
Page Updated: 17:47:40, BST

shboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help

ser Defined Attributes for All Objects

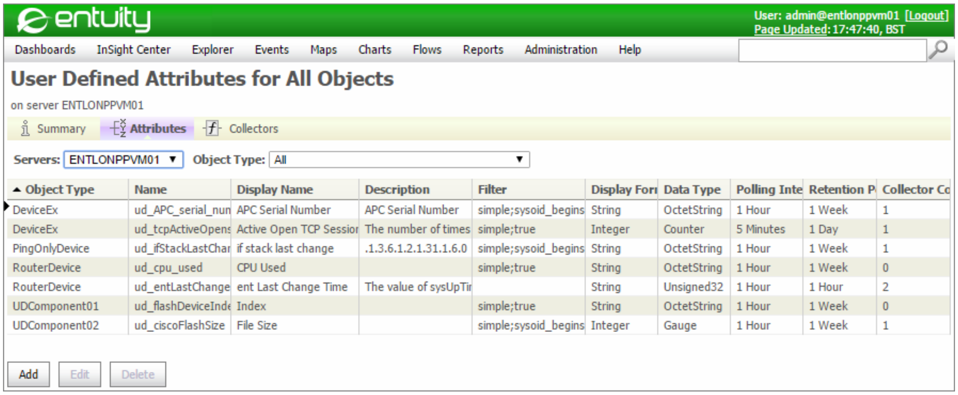
erver ENTLONPPVM01

Summary Attributes Collectors

rvers: ENTLONPPVM01 Object Type: All

| bject Type | Name | Display Name | Description | Filter | Display Fori | Data Type | Polling Inte | Retention P | Coll |
|---|---|---|---|---|---|---|---|---|---|
| iceEx | ud_APC_serial_nun | APC Serial Number | APC Serial Number | simple;sysoid_begins | String | OctetString | 1 Hour | 1 Week | 1 |
| iceEx | ud_tcpActiveOpens | Active Open TCP Sessior | The number of times | simple;true | Integer | Counter | 5 Minutes | 1 Day | 1 |
| gOnlyDevice | ud_ifStackLastChar | if stack last change | .1.3.6.1.2.1.31.1.6.0 | simple;sysoid_begins | String | OctetString | 1 Hour | 1 Week | 1 |
| terDevice | ud_cpu_used | CPU Used | | simple;true | String | OctetString | 1 Hour | 1 Week | 0 |
| terDevice | ud_entLastChange | ent Last Change Time | The value of sysUpTir | | String | Unsigned32 | 1 Hour | 1 Hour | 2 |
| Component01 | ud_flashDeviceInde | Index | | simple;true | String | OctetString | 1 Hour | 1 Week | 0 |
| Component02 | ud_ciscoFlashSize | File Size | | simple;sysoid_begins | Integer | Gauge | 1 Hour | 1 Week | 1 |

d Edit Delete



User Defined Attributes for All Objects

on server ENTLONPPVM01

Servers: ENTLONPPVM01 Object Type: All

| Object Type | Name | Display Name | Description | Filter | Display Fori | Data Type | Polling Inte | Retention P | Collector Co |
|---|---|---|---|---|---|---|---|---|---|
| DeviceEx | ud_APC_serial_nun | APC Serial Number | APC Serial Number | simple;sysoid_begins | String | OctetString | 1 Hour | 1 Week | 1 |
| DeviceEx | ud_tcpActiveOpens | Active Open TCP Sessior | The number of times | simple;true | Integer | Counter | 5 Minutes | 1 Day | 1 |
| PingOnlyDevice | ud_ifStackLastChar | if stack last change | .1.3.6.1.2.1.31.1.6.0 | simple;sysoid_begins | String | OctetString | 1 Hour | 1 Week | 1 |
| RouterDevice | ud_cpu_used | CPU Used | | simple;true | String | OctetString | 1 Hour | 1 Week | 0 |
| RouterDevice | ud_entLastChange | ent Last Change Time | The value of sysUpTir | | String | Unsigned32 | 1 Hour | 1 Hour | 2 |
| UDComponent01 | ud_flashDeviceInde | Index | | simple;true | String | OctetString | 1 Hour | 1 Week | 0 |
| UDComponent02 | ud_ciscoFlashSize | File Size | | simple;sysoid_begins | Integer | Gauge | 1 Hour | 1 Week | 1 |

Figure 329 User Defined Polling Attributes

| Attribute | Description |
|---|---|
| *Name* | When you create a new attribute or collector you must assign it a name. By default Entuity prepends the attribute or collector name with ud_ and then adds the name of the OID. You can amend the name however you should retain the ud_ prefix to avoid any future potential conflict with a system attribute or collector name.<br>If you do not follow the convention Entuity will warn you of a current naming conflict however it would not protect you against a future Entuity upgrade including an attribute or collector with the same name as one you have already defined. |
| *Display Name* | Attribute named displayed in Entuity. |
| *Description* | Description of the attribute, by default it is derived from the OID. |
| *Object Type* | StormWorks object type to which the attribute is assigned. |
| *Filter* | StormWorks filter applied to the attribute. |
| *Display Format* | Format Entuity uses to display the attribute value, e.g. Integer, String. |
| *Data Type* | Data type Entuity uses to interpret the attribute value, e.g. Counter. |
| *Polling Interval* | Interval between Entuity polling of the attribute. You should match the polling frequency to the frequency of attribute value change. |
| *Retention Period* | Period of time for which Entuity retains polled data. |
| *Transform* | Transforms are configurations used by Entuity to convert polled data into meaningful values.<br>You can click **View** to list the available transforms, and you can then select and view any transform definition. |
| *Gauge Range* | Entuity gauges are displayed on the Summary page of managed objects of the *Object Type*. You should enter appropriate minimum and maximum values to set the gauge parameters. |
| *Summary* | Determines where and how the attribute is displayed. To display the attribute on the Summary page of managed objects of the *Object Type* click:<br>■ General Info, to display the Display Name and attribute value.<br>■ Gauges, to display the attribute value in a gauge.<br>■ Charts, to display the attribute value in a chart.<br>If you do not select a check box the attribute is still available through the Advanced page of managed objects of the *Object Type*. |

Table 56 User Defined Attribute Details

Entuity attributes can support threshold and state based events and incidents. The two incident types are:

- User Defined Attribute Status incident has these contributing events:
  - User Defined Attribute State Down
  - User Defined Attribute State Disabled
  - User Defined Attribute State Other
  - User Defined Attribute State Up incident
- User Defined Attribute Value Abnormality incident has these contributing events:

- User Defined Attribute Value Critical
- User Defined Attribute Value High
- User Defined Attribute Value Warning
- User Defined Attribute Value Low
- User Defined Attribute Value Abnormality Cleared.

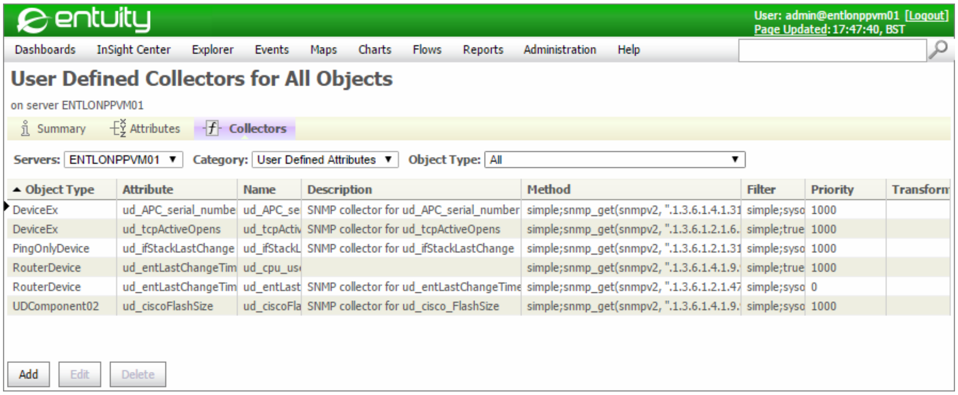
| Attribute | Description |
|---|---|
| *Threshold* | User Defined Polling includes four threshold events, and two associated incidents. For each attribute you can define four thresholds:<br>■ Critical<br>■ High<br>■ Warning<br>■ Low. |
| *Status* | User Defined Polling includes five threshold events, and two associated incidents. For each attribute you can define four thresholds:<br>■ Up<br>■ Down<br>■ Disabled<br>■ Other. |

Table 57 User Defined Attribute Events

Although Entuity uses the same set of events and incidents with all of your user defined attributes users can set suppression rules filtered on the attribute against which events are raised.

## User Defined Collectors

User Defined Collectors are assigned to attributes. The User Defined Collectors page title and table are updated to reflect the chosen category and object type. You can view existing definitions in the table and also add, amend and delete definitions.



User Defined Collectors for All Objects

on server ENTLONPPVM01

Servers: ENTLONPPVM01 Category: User Defined Attributes Object Type: All

| Object Type | Attribute | Name | Description | Method | Filter | Priority | Transform |
|---|---|---|---|---|---|---|---|
| DeviceEx | ud_APC_serial_numbe | ud_APC_se | SNMP collector for ud_APC_serial_number | simple;snmp_get(snmpv2, ".1.3.6.1.4.1.31 | simple;syso | 1000 | |
| DeviceEx | ud_tcpActiveOpens | ud_tcpActiv | SNMP collector for ud_tcpActiveOpens | simple;snmp_get(snmpv2, ".1.3.6.1.2.1.6. | simple;true | 1000 | |
| PingOnlyDevice | ud_ifStackLastChange | ud_ifStackL | SNMP collector for ud_ifStackLastChange | simple;snmp_get(snmpv2, ".1.3.6.1.2.1.31 | simple;syso | 1000 | |
| RouterDevice | ud_entLastChangeTim | ud_cpu_us | | simple;snmp_get(snmpv2, ".1.3.6.1.4.1.9. | simple;true | 1000 | |
| RouterDevice | ud_entLastChangeTim | ud_entLast | SNMP collector for ud_entLastChangeTime | simple;snmp_get(snmpv2, ".1.3.6.1.2.1.47 | simple;syso | 0 | |
| UDComponent02 | ud_ciscoFlashSize | ud_ciscoFla | SNMP collector for ud_cisco_FlashSize | simple;snmp_get(snmpv2, ".1.3.6.1.4.1.9. | simple;syso | 1000 | |

Figure 330 User Defined Collectors

| Attribute | Description |
|---|---|
| *Name* | When you create a new attribute or collector you must assign it a name. By default Entuity prepends the attribute or collector name with ud_ and then adds the name of the OID. You can amend the name however you should retain the ud_ prefix to avoid any future potential conflict with a system attribute or collector name.<br>If you do not follow the convention Entuity will warn you of a current naming conflict however it would not protect you against a future Entuity upgrade including an attribute or collector with the same name as one you have already defined. |
| *Description* | Description of the attribute, by default it is derived from the OID. |
| *Object Type* | StormWorks object type to which the attribute is assigned. |
| *Attribute* | User defined attribute name. |
| OID | OID used to poll the attribute. |
| Index | The reference for a table of instances. When the OID is a scalar *Index* is set to **None** indicating there is only one instance of it. |
| SNMP Version | SNMP version used to poll the attribute. |

Table 58 User Defined Collector Details

| Attribute | Description |
|---|---|
| Method | Contains the appropriate OID for the collector definition within the method syntax, for example:<br>`simple;snmp_get(snmpv2,".1.3.6.1.2.1.6.5.0",null)`<br>For index attributes you amend the method as Entuity uses an SNMP table walk rather than a Get operation. Click **Edit** and:<br>- Rename the function by adding `_indexes` to the end of its name.<br>- Amend the second parameter to represent the maximum number of entries that will be returned by the table walk.<br>For example:<br>`simple;snmp_get_indexes(snmpv2,".1.3.6.1.4.1.9.9.10.1.1.2.1.7",500)`<br>When you only require one item from the table you can amend the method so that it includes the index. For example to collect only the Cisco CPU busy percentage for the previous 5 seconds:<br>simple;snmp_get(snmpv2, ".1.3.6.1.4.1.9.9.109.1.1.1.1.3", null)<br>Replace null with the index:<br>simple;snmp_get(snmpv2, ".1.3.6.1.4.1.9.9.109.1.1.1.1.3", 1) |
| *Filter* | StormWorks filter applied to the collector, for example to restrict polling to devices from a selected manufacturer.. |
| *Priority* | All user defined collectors have a higher priority than system collectors. When you assign multiple collectors to the same attribute the collector with the highest priority is applied first. |
| *Transform* | Transforms are configurations used by Entuity to convert polled data into meaningful values.<br>You can click **View** to list the available transforms, and you can then select and view any transform definition. |

Table 58 User Defined Collector Details

## User Defined Polling Wizard

The User Defined Polling wizard guides you through configuring polling of a user defined attribute. The wizard always creates the attributes and collectors on the local Entuity server.

To use the User Defined Polling wizard:

1) Select a device to provide the context for the wizard. For example it sets the Entuity server on which the User Defined Polling configuration is defined, the default object type, e.g. RouterDevice.

   You can select the device from the Explorer tree.

2) Click **Administration** > **User Defined Polling** and from the User Defined Polling Summary tab click **User Defined Polling Wizard**.

3) Entuity opens the MIB Browser through which you can enter the OID to use to poll the attribute. You can also open the MIB Manager to import and load more MIBs.

   Click **Next**.

4) Define the attribute for which you want to collect data. When you selected the OID from a MIB Entuity defaults in attribute values from the OID, e.g. name, data type, description.

5) You can also define events to be potentially raised against the attribute.

   It is important that the attribute data type and value correspond to the type of event. For example a threshold event would not work with an attribute that has a string data type.

   Click **Next**.

6) Define the Collector.

## Set Up Collector for System Attributes

For each device under its management Entuity has a device data model. Occasionally an attribute on a managed device may not be polled, the system collector (or collectors) not using the OID appropriate to that device. You can define a new collector with the appropriate OID. User defined collectors take precedence over system collectors for the same device.

### Adding Used Memory Collector

The H3C switch, model H3C S7502E, was not having its used memory percentage data collected. This example:

- Creates a new collector for used memory percentage.
- Uses the OID `.1.3.6.1.4.1.2011.10.2.6.1.1.1.1.8` from the `h3c-entity-ext-mib`.
- Applies an enterprise filter to restrict the collector to H3C devices.

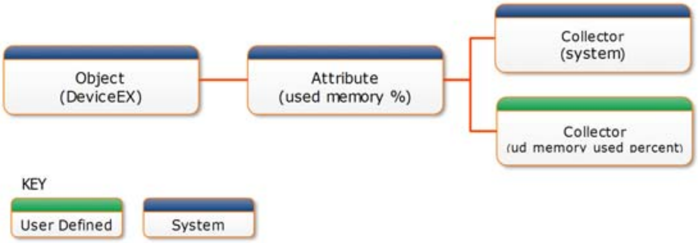
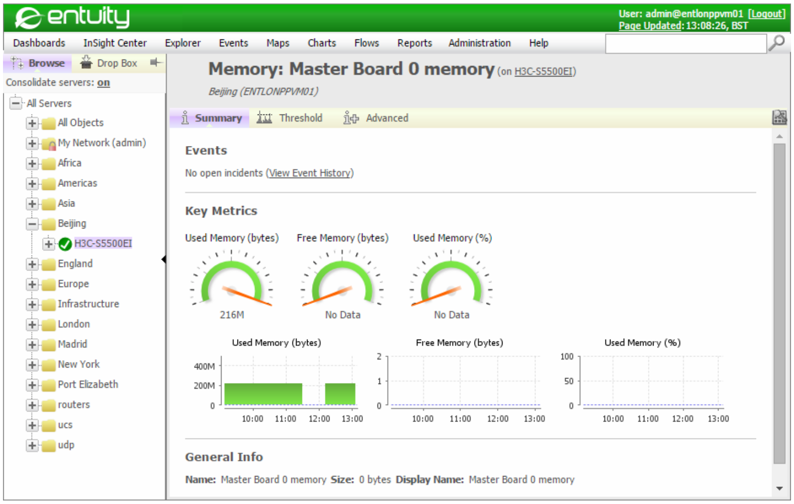


Figure 331 Define a Collector for a System Attribute

To create a new collector:

1) From the Explorer tree highlight a H3C device.

   This sets the context for when you create the collector.



Memory: Master Board 0 memory (on H3C-S5500EI)

Beijing (ENTLONPPVM01)

No open incidents (View Event History)

Name: Master Board 0 memory Size: 0 bytes Display Name: Master Board 0 memory

Figure 332 Incomplete Attribute Data Collection

2) Click **Administration > User Defined Polling** and then **Collectors**.

3) You can set the context:

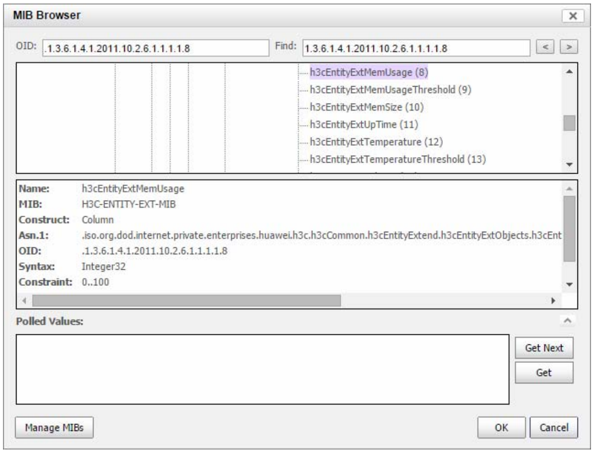
- *Servers*, in multi-server environments select the Entuity server on which to create the collector.
- *Category*, select **Stream Attributes**.
- *Object Type*, select **memory**.

Click **Add**. Entuity defaults your selections into the User Defined Collector dialog.

4) Enter a name for the collector, for example **ud_memoryUserPercentPolled**.

5) Against OID click **Browse** and then **Manage MIB**.

Import and then load (parse) `h3c-entity-ext-mib`.



MIB Browser

OID: .1.3.6.1.4.1.2011.10.2.6.1.1.1.1.8

Find: 1.3.6.1.4.1.2011.10.2.6.1.1.1.1.8

- h3cEntityExtMemUsage (8)
- h3cEntityExtMemUsageThreshold (9)
- h3cEntityExtMemSize (10)
- h3cEntityExtUpTime (11)
- h3cEntityExtTemperature (12)
- h3cEntityExtTemperatureThreshold (13)

Name: h3cEntityExtMemUsage
MIB: H3C-ENTITY-EXT-MIB
Construct: Column
Asn.1: .iso.org.dod.internet.private.enterprises.huawei.h3c.h3cCommon.h3cEntityExtend.h3cEntityExtObjects.h3cEnt
OID: .1.3.6.1.4.1.2011.10.2.6.1.1.1.1.8
Syntax: Integer32
Constraint: 0..100

Polled Values:

Figure 333 Select OID

6) Against OID click **Browse**.

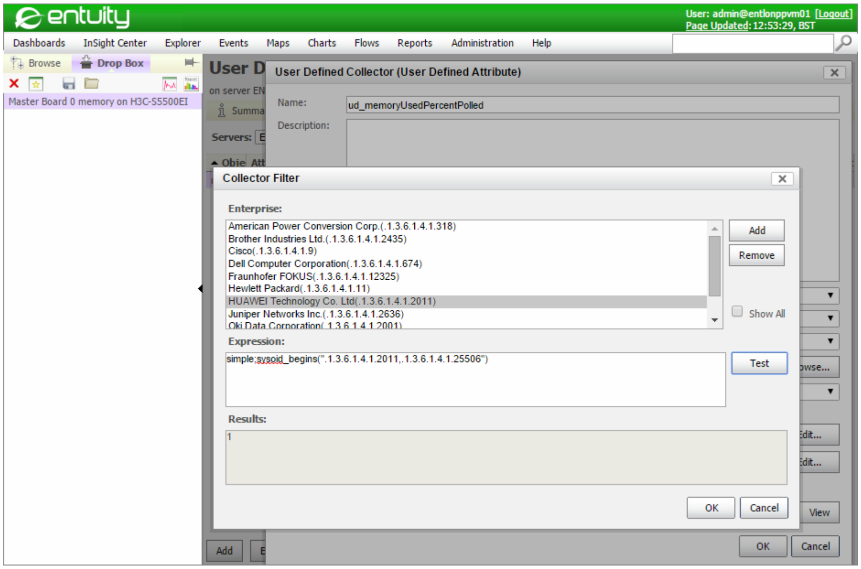
Through the MIB Browser locate the OID (`.1.3.6.1.4.1.2011.10.2.6.1.1.1.1.8`) and click **OK**.

7) From the User Defined Collector dialog in:

- *Object* select **memory**, in *Stream* select **Status** and in *Attribute* select **memoryUsedPercentPolled**.
- *Index* select **memoryFamilyAndIndex.memoryIndex**.
- *Filter* select **Edit** and then the H3C enterprise filter (or type them in)

  ```
  simple;sysoid_begins(".1.3.6.1.4.1.2011,.1.3.6.1.4.1.25506")
  ```

  If you have dragged a managed memory component to drop box you can click **Test** to test the validity of your filter.



Name: ud_memoryUsedPercentPolled

Enterprise:

American Power Conversion Corp.(.1.3.6.1.4.1.318)
Brother Industries Ltd.(.1.3.6.1.4.1.2435)
Cisco(.1.3.6.1.4.1.9)
Dell Computer Corporation(.1.3.6.1.4.1.674)
Fraunhofer FOKUS(.1.3.6.1.4.1.12325)
Hewlett Packard(.1.3.6.1.4.1.11)
HUAWEI Technology Co. Ltd(.1.3.6.1.4.1.2011)
Juniper Networks Inc.(.1.3.6.1.4.1.2636)
Oki Data Corporation(.1.3.6.1.4.1.2001)

Expression:

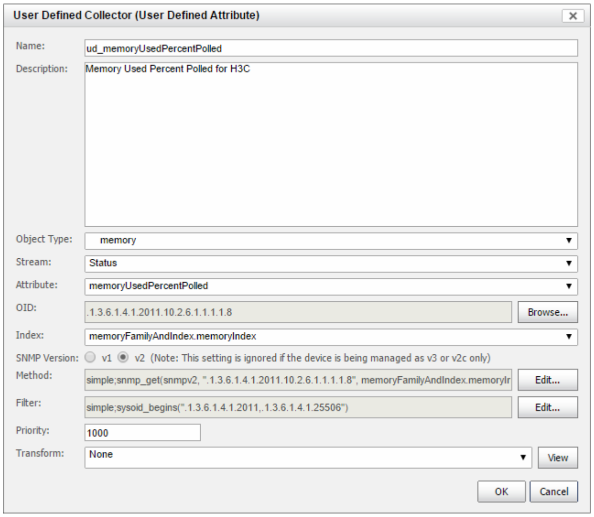
simple;sysoid_begins(".1.3.6.1.4.1.2011,.1.3.6.1.4.1.25506")

Results:

1

Figure 334 Set and Test Collector Filter

8) From the User Defined Collector dialog click **OK**.



Name: ud_memoryUsedPercentPolled

Description: Memory Used Percent Polled for H3C

Object Type: memory

Stream: Status

Attribute: memoryUsedPercentPolled

OID: .1.3.6.1.4.1.2011.10.2.6.1.1.1.1.8

Index: memoryFamilyAndIndex.memoryIndex

SNMP Version: ○ v1 ● v2 (Note: This setting is ignored if the device is being managed as v3 or v2c only)

Method: simple;snmp_get(snmpv2, ".1.3.6.1.4.1.2011.10.2.6.1.1.1.1.8", memoryFamilyAndIndex.memoryIr

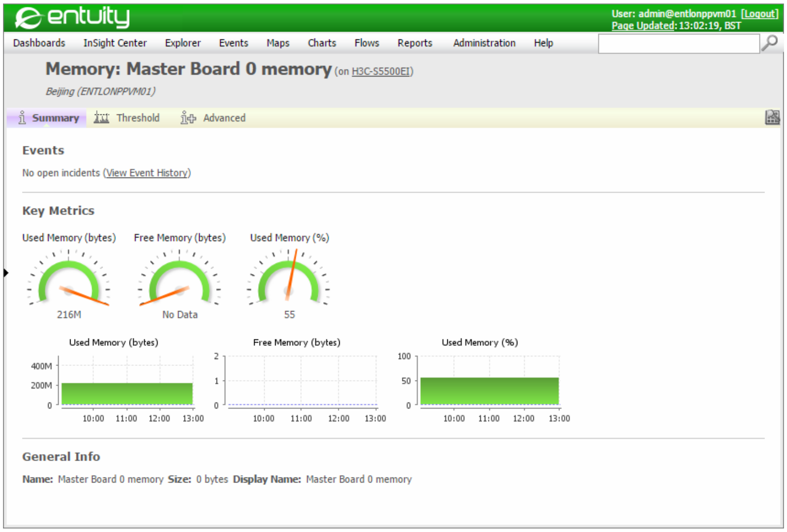
Filter: simple;sysoid_begins(".1.3.6.1.4.1.2011,.1.3.6.1.4.1.25506")

Priority: 1000

Transform: None

Figure 335 Define Collector

Entuity discovers the new collector and then polls the system attribute. This may take a few minutes or hours depending upon the size of your managed network.



Memory: Master Board 0 memory (on H3C-S5500EI)

Beijing (ENTLONPPVM01)

Events

No open incidents (View Event History)

Key Metrics

General Info

**Name:** Master Board 0 memory **Size:** 0 bytes **Display Name:** Master Board 0 memory

Figure 336 User Defined Polling Memory

# Set Up Attribute and Collector for System Objects

With User Defined Polling you can add new attributes to existing managed objects. This applies to both system objects and user defined objects. System objects are present in every Entuity installation and represent network devices, ports, modules, processors, fans and many other types of component or concept. Custom objects can be defined to represent concepts that are beyond the scope of standard Entuity discovery and monitoring support. Every different type of object has a number of attributes that each hold a specific piece of data that's relevant in the context of the component being modeled by the object.

## Adding TCP Active Sessions Attribute to Devices

The requirement is to monitor the number of open TCP connections on all managed devices. This example:

- Creates a new user defined attribute to hold the number of TCP active sessions.
- Adds the new attribute to the `DeviceEx` object type. This ensure the new attribute is available to the majority of managed devices.
- Creates a new collector to poll for TCP active sessions.
- Uses the OID `.1.3.6.1.2.1.6.5.0.` from the `TCP-MIB`.

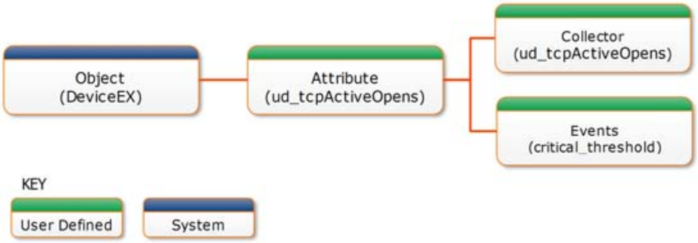
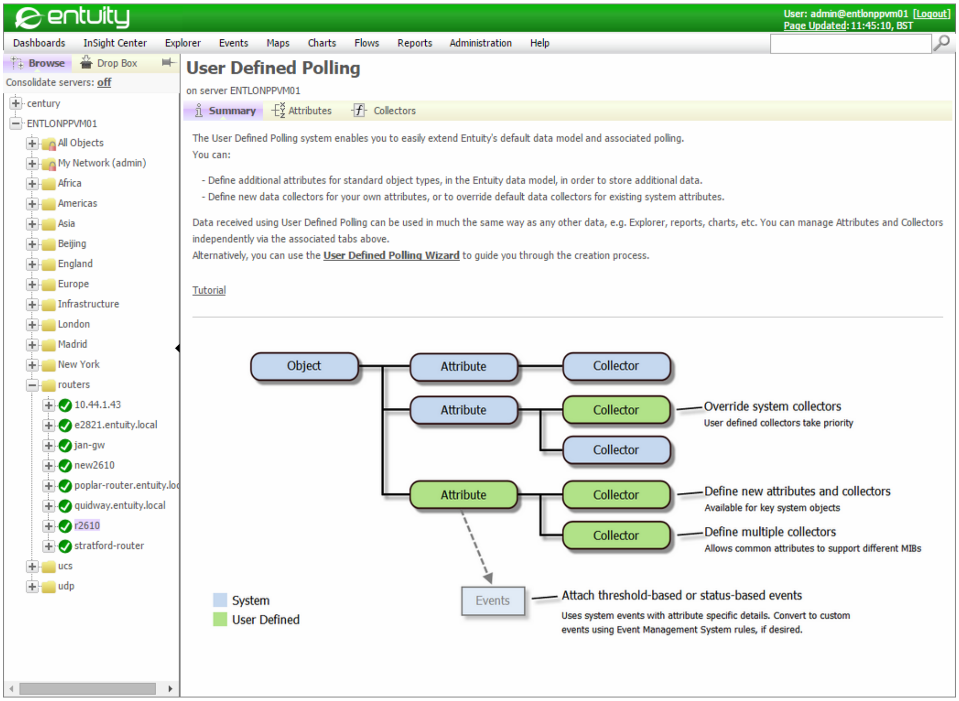


Figure 337 Define an Attribute and Collector

To create a new attribute:

1) From the Explorer tree highlight a Cisco device.

   This sets the context for when you create the attribute.



**User Defined Polling**

on server ENTLONPPVM01

The User Defined Polling system enables you to easily extend Entuity's default data model and associated polling.

You can:

- Define additional attributes for standard object types, in the Entuity data model, in order to store additional data.
- Define new data collectors for your own attributes, or to override default data collectors for existing system attributes.

Data received using User Defined Polling can be used in much the same way as any other data, e.g. Explorer, reports, charts, etc. You can manage Attributes and Collectors independently via the associated tabs above.

Alternatively, you can use the User Defined Polling Wizard to guide you through the creation process.

Tutorial

Override system collectors
User defined collectors take priority

Define new attributes and collectors
Available for key system objects

Define multiple collectors
Allows common attributes to support different MIBs

Attach threshold-based or status-based events
Uses system events with attribute specific details. Convert to custom events using Event Management System rules, if desired.

Figure 338 Select a Device

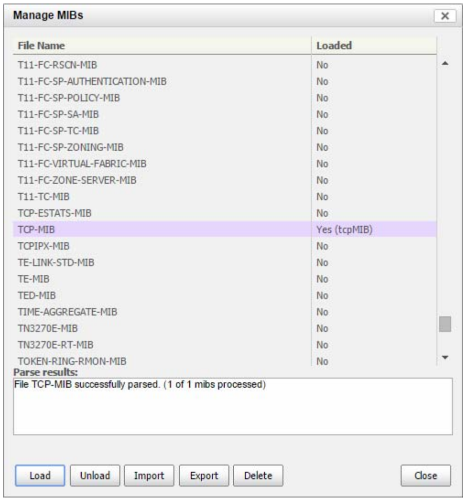
2) Click **Administration** > **User Defined Polling** and then **User Defined Polling Wizard**.

   From the SNMP MIB Browser you can enter the OID.

3) You can use the MIB Manager to import and then load (parse) required MIBs, e.g. `TCP-`

`MIB`.

Click **Close** to close the manager.



| File Name | Loaded |
|---|---|
| T11-FC-RSCN-MIB | No |
| T11-FC-SP-AUTHENTICATION-MIB | No |
| T11-FC-SP-POLICY-MIB | No |
| T11-FC-SP-SA-MIB | No |
| T11-FC-SP-TC-MIB | No |
| T11-FC-SP-ZONING-MIB | No |
| T11-FC-VIRTUAL-FABRIC-MIB | No |
| T11-FC-ZONE-SERVER-MIB | No |
| T11-TC-MIB | No |
| TCP-ESTATS-MIB | No |
| TCP-MIB | Yes (tcpMIB) |
| TCPIPX-MIB | No |
| TE-LINK-STD-MIB | No |
| TE-MIB | No |
| TED-MIB | No |
| TIME-AGGREGATE-MIB | No |
| TN3270E-MIB | No |
| TN3270E-RT-MIB | No |
| TOKEN-RING-RMON-MIB | No |

Parse results:

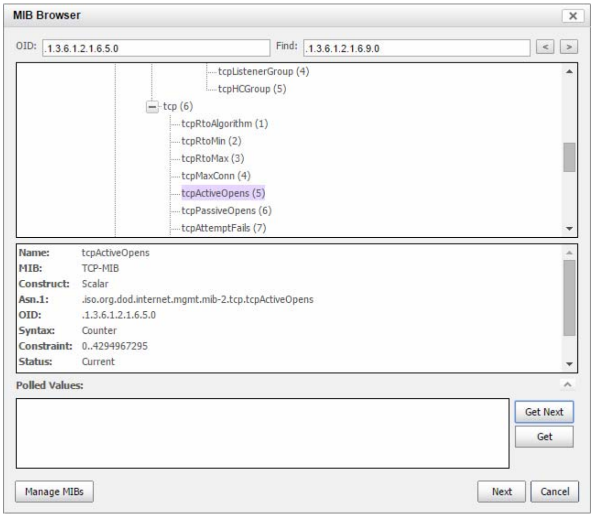
```
File TCP-MIB successfully parsed. (1 of 1 mibs processed)
```

Figure 339 Load TCP-MIB

4) From the MIB browser you can:

- Use the Find tool to locate appropriate entries in the MIB, for example enter TCP.
- Highlight an OID in the MIB tree to view its details in the MIB details panel.
- Click Get for Entuity to use the OID to get its value from the device you selected on starting the wizard.
- Click Get Next when you have selected a table in the MIB. Entuity reads the first entry in the table, subsequent Get Next requests result in reading subsequent entries in the table.

When you have selected the OID click **Next**.



OID: .1.3.6.1.2.1.6.5.0 Find: .1.3.6.1.2.1.6.9.0

```
        tcpListenerGroup (4)
        tcpHCGroup (5)
  tcp (6)
    tcpRtoAlgorithm (1)
    tcpRtoMin (2)
    tcpRtoMax (3)
    tcpMaxConn (4)
    tcpActiveOpens (5)
    tcpPassiveOpens (6)
    tcpAttemptFails (7)
```

| | |
|---|---|
| **Name:** | tcpActiveOpens |
| **MIB:** | TCP-MIB |
| **Construct:** | Scalar |
| **Asn.1:** | .iso.org.dod.internet.mgmt.mib-2.tcp.tcpActiveOpens |
| **OID:** | .1.3.6.1.2.1.6.5.0 |
| **Syntax:** | Counter |
| **Constraint:** | 0..4294967295 |
| **Status:** | Current |

**Polled Values:**

Figure 340 Select OID

5) Entuity defaults your selections into the User Defined Attribute dialog.

You can set:

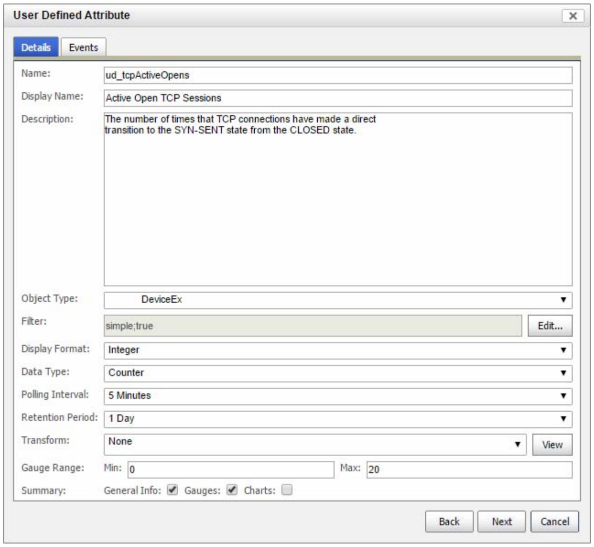
- *Object Type*, select **DeviceEx**. The current selected type is the type associated with the device.
- *Filter* may be set Cisco only devices:

  `simple;sysoid_begins(".1.3.6.1.4.1.9")`

  To make the attribute available to devices of all manufacturers amend the *Filter*:

  `simple;true`
- *Polling Interval* to 5 minutes.
- *Retention Period* to 1 Day.
- *Gauge Range* to *Min* 0 and *Max* 20.
- *Summary* leave *General Info*, *Gauges* and *Charts* as selected.

Click **Events** tab.



User Defined Attribute

Name: ud_tcpActiveOpens

Display Name: Active Open TCP Sessions

Description: The number of times that TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

Object Type: DeviceEx

Filter: simple;true

Display Format: Integer

Data Type: Counter

Polling Interval: 5 Minutes

Retention Period: 1 Day

Transform: None

Gauge Range: Min: 0 Max: 20

Summary: General Info: ☑ Gauges: ☑ Charts: ☐

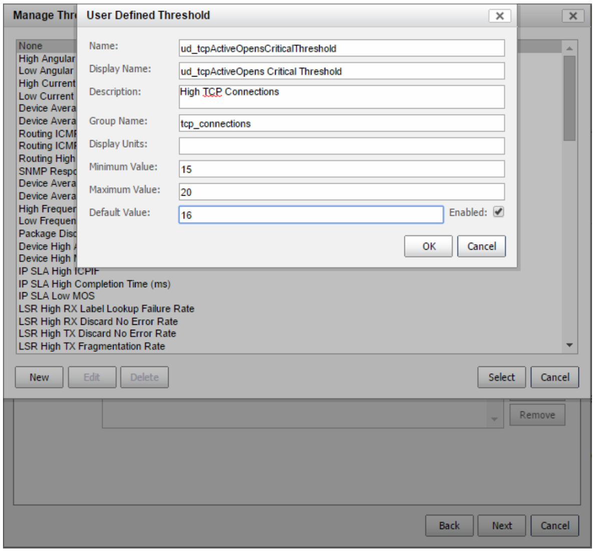
Figure 341 Define New Attribute

6) TCP active sessions is only suitable for setting threshold events.

Next to each threshold you can click the down arrow. Entuity displays the available thresholds for this object type. If your new attribute is similar to an existing attribute you might want to use the same threshold. You can also define new thresholds. If you are defining an attribute assigned to one of the UDComponent object types then initially there will not be any thresholds associated to the object and therefore available for selection.

| Attribute | Description |
|---|---|
| *Name* | Name of the threshold, by default derived from ud_, the attribute name and the threshold level. |
| *Display Name* | Name of the threshold displayed on the Threshold page. |
| *Description* | Enter a description for the threshold. |
| *Group Name* | Used on the Threshold page to group together different thresholds, for example different severity level thresholds set against the same attribute. |
| *Display Unit* | Measurement unit of the attribute. |
| *Minimum Value* | Minimum value of the threshold range. |
| *Maximum Value* | Maximum value of the threshold range. |
| *Default Value* | Default value of the threshold range. |

Table 59 User Defined Threshold



User Defined Threshold

Name: ud_tcpActiveOpensCriticalThreshold

Display Name: ud_tcpActiveOpens Critical Threshold

Description: High TCP Connections

Group Name: tcp_connections

Display Units:

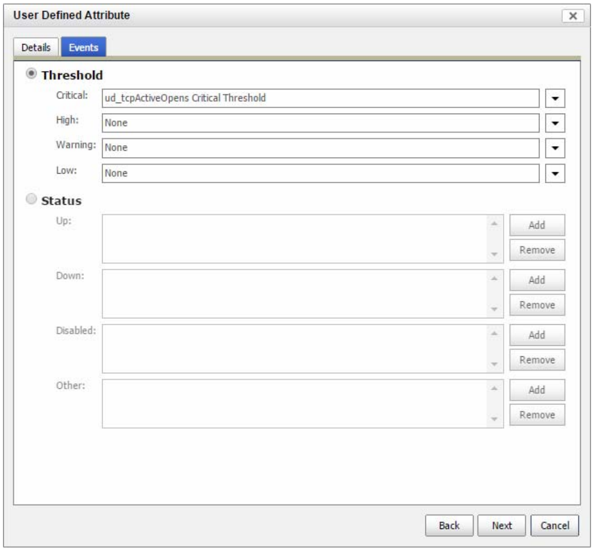
Minimum Value: 15

Maximum Value: 20

Default Value: 16 Enabled: ☑

Figure 342 Define Threshold Events

7) When you have defined threshold settings click **Next**.



User Defined Attribute

● Threshold

Critical: ud_tcpActiveOpens Critical Threshold

High: None

Warning: None

Low: None

○ Status

Up:

Down:

Disabled:

Other:

Figure 343 Define Event Thresholds

8) You can set the *Filter* so the configuration applies to all devices.

Click **Edit** and in *Expression* change:

```
simple;sysoid_begins(".1.3.6.1.4.1.9")
```

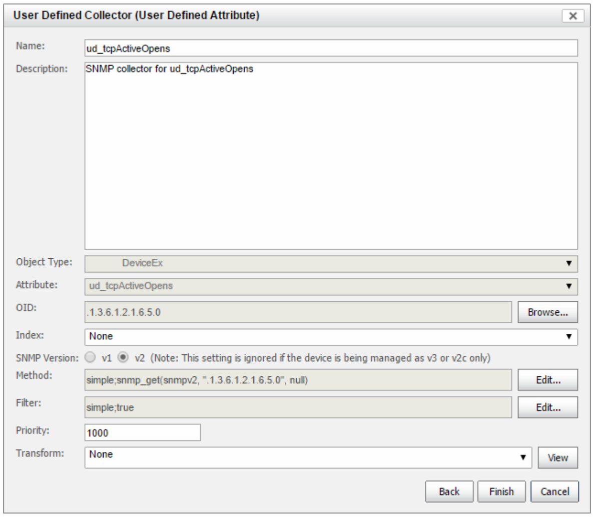
to:

```
simple;true
```

You can type in the filter or highlight enterprise and click **Add**. Entity displays the enterprise OIDs of devices under management. You can click **Select All** to view all available enterprise OIDs. A filter can support multiple sysoids.

Click **Test** to check your filter is correct. Entity applies the filter to the selected device and returns 1 if successful and 0 if it fails. If you are defining attributes against objects other than devices you can still run an evaluation. For example if defining a fan attribute go to the Advanced page of a device and drag to Drop Box a monitored fan. Then highlight the fan before evaluating the expression.

Click **OK** to accept your filter definition.



User Defined Collector (User Defined Attribute)

Name: ud_tcpActiveOpens

Description: SNMP collector for ud_tcpActiveOpens

Object Type: DeviceEx

Attribute: ud_tcpActiveOpens

OID: .1.3.6.1.2.1.6.5.0

Index: None

SNMP Version: ○ v1 ● v2 (Note: This setting is ignored if the device is being managed as v3 or v2c only)

Method: simple;snmp_get(snmpv2, ".1.3.6.1.2.1.6.5.0", null)

Filter: simple;true

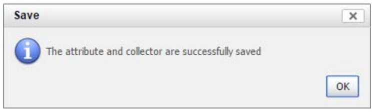
Priority: 1000

Transform: None

Figure 344 Reset Collector Filter

9) Click Finish.

Entity reports the success of the attribute and collection definition.

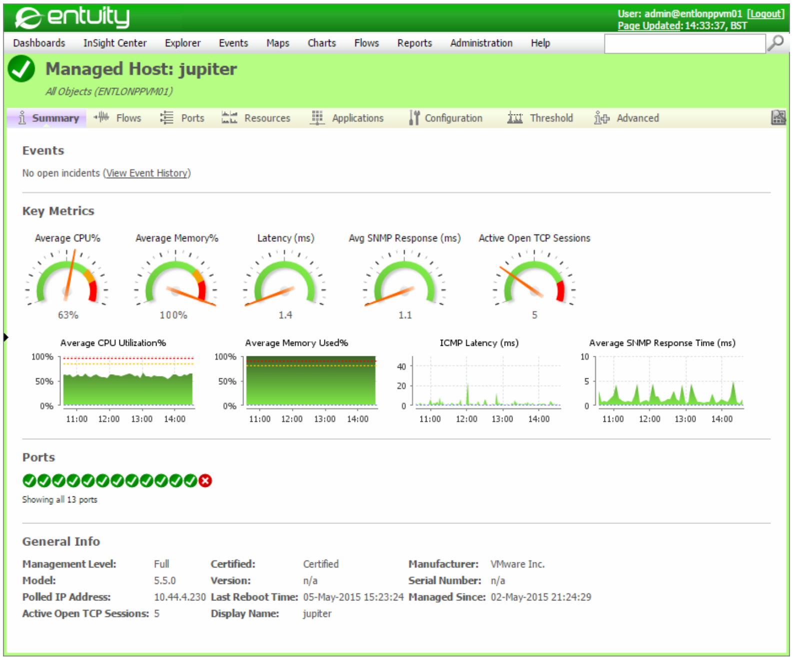


Save

The attribute and collector are successfully saved

Figure 345 Attribute and Collector Created

Entity discovers the new attribute and collector and then polls the new attribute.



Events

No open incidents (View Event History)

Ports

Showing all 13 ports

General Info

| | | | | | |
|---|---|---|---|---|---|
| **Management Level:** | Full | **Certified:** | Certified | **Manufacturer:** | VMware Inc. |
| **Model:** | 5.5.0 | **Version:** | n/a | **Serial Number:** | n/a |
| **Polled IP Address:** | 10.44.4.230 | **Last Reboot Time:** | 05-May-2015 15:23:24 | **Managed Since:** | 02-May-2015 21:24:29 |
| **Active Open TCP Sessions:** | 5 | **Display Name:** | jupiter | | |

Figure 346 Collection of New Attribute

# Set Up User Defined Polling Component

Entuity includes 20 user defined object types that you can use to model components of network devices that are not part of the standard data model. These object types include two attributes index and display name. Display name is configurable. You can then create user defined attributes to model additional attributes of the object.

## Adding Flash File Management

This example models flash file object and its attributes. The example:

- Uses the `UDComponent02` object type.
- Amends the UDComponent02 index attribute to use an integer attribute (`ciscoFlashFileEntry`) from the `ciscoFlashFileTable` table as an index to walk the table. The table index is not available (`ciscoFlashFileIndex`).
- Amends the UDComponent02 name attribute to use the Flash File name.
- Uses the User Defined Polling Wizard to configure a new attribute, Flash File Size.
- Sets three levels of threshold events against the Flash File Size attribute.
- Configures new collectors.
- Uses the `CISCO-FLASH-MIB` to identify flash file attributes for example:

```
.1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.2 cisciFlashFileSize
```

You will also have to import to the server `CISCO-SMI` and `CISCO-QOS-PIB-MIB` (they do not require loading) before loading `CISCO-FLASH-MIB`.

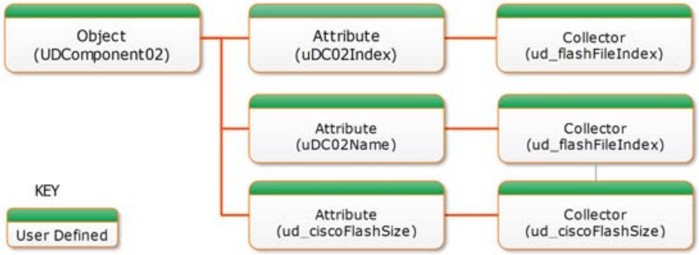


Figure 347 Extract of Flash File Definition

The example instructions are split into four stages:

1) Define the collector for the flash file index.
2) Define the collector for the flash file name.
3) Define the user defined attribute and collector for flash file size using the User Defined Polling Wizard.
4) Rename the UDComponent display name.

### Creating the Flash File Index Collector

To create a collector for the flash file index:

1) Click **Administration > User Defined Polling** and then **Collectors** tab.
2) Set the context for creating the collector. Set:
   - *Server* to the Entity server on which you want to configure the collector (only required in multi-server environments).
   - *Category* to **Object Attributes**.
   - *Object Type* to **UDComponent02**.

   Click **Add**.
3) Entity defaults in the *Object Type* as **UDComponent02** and *Attribute* as **uDC02Index**.

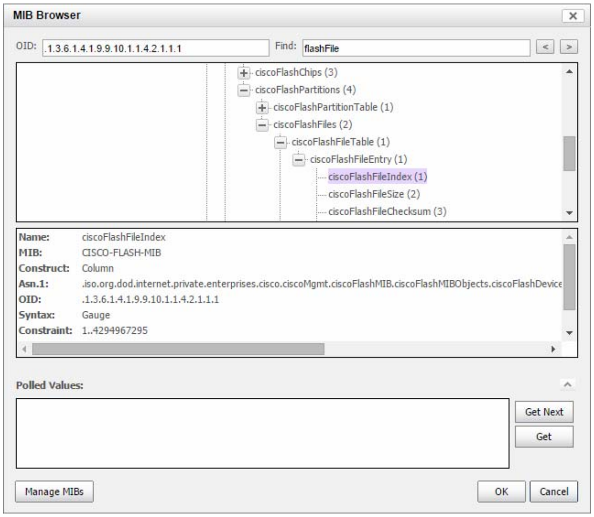
   From *OID* click **Browse**.

- From the SNMP MIB Browser you can enter the OID in *OID*.

  Alternatively you can click **MIB Manage** and use the MIB Manager to import and then load (parse) required MIBs, i.e. `CISCO-FLASH-MIB`. You will also have to import to the server `CISCO-SMI` and `CISCO-QOS-PIB-MIB` (they do not require loading).

  You can shortcut the navigation by using the Find tool, for example by entering flash. Select `ciscoFlashFileIndex` and click **Close** to close the MIB Manager.

  Click **OK** to close the MIB Browser.



OID: .1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.1
Find: flashFile

Name: ciscoFlashFileIndex
MIB: CISCO-FLASH-MIB
Construct: Column
Asn.1: .iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoFlashMIB.ciscoFlashMIBObjects.ciscoFlashDevice
OID: .1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.1
Syntax: Gauge
Constraint: 1..4294967295

Figure 348 Cisco Flash File Index OID

4) Define the collector. In:

- *Name*, enter the unique name of the collector, e.g. **ud_FlashFileIndex**.
- *Description*, enter a description of the attribute.
- *Attribute*, select the index attribute associated to the component object type, e.g. **UD02Index**.
- *Object Type*, select the component object type, e.g. **UDComponent02**.
- *OID* is the OID used by User Defined Polling as an index to the flash file table.
- *Index* is the index attribute, e.g. **UD02Index**.
- *SNMP Version* used to poll the device.
- *Method* is the instruction Entuity uses to poll for the attribute.

  For an index attribute you must change the:

  - `snmp_get` command to `snmp_get_indexes`.
  - index reference (**UD02Index**) to one that determines the maximum number of rows the `snmp_get_indexes` instruction can return, e.g. **500**.

```
simple;snmp_get_indexes(snmpv2, ".1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.2",
500)
```

- *Filter* set the filter Entuity uses to restrict creation of the object to devices that match the sysoid filter. You can set the *Filter* so the flash file configuration only applies to Cisco devices.

  Click **Edit** and in *Expression* change:

  ```
  simple;true
  ```

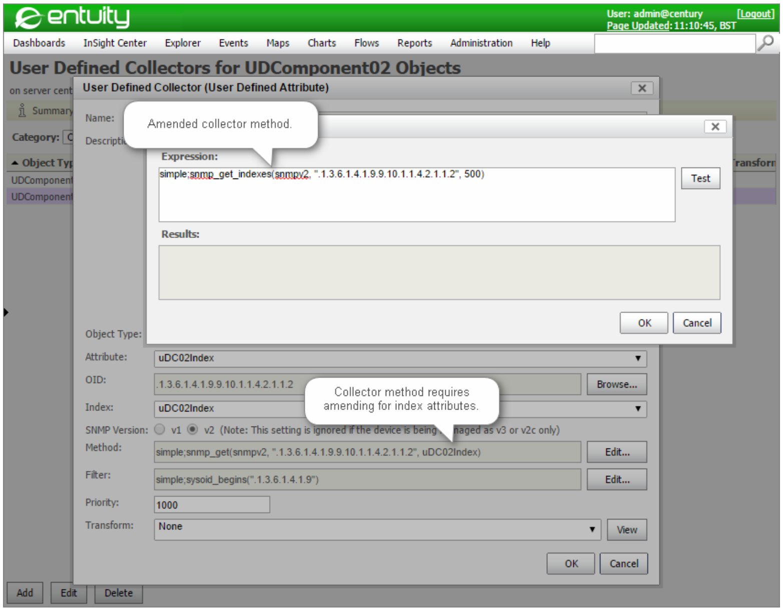
  to:

```
simple;sysoid_begins(".1.3.6.1.4.1.9")
```

You can type in the filter or highlight enterprise and click **Add**. Entuity displays the enterprise OIDs of devices under management. You can click **Select All** to view all available enterprise OIDs. A filter can support multiple sysoids.

- *Priority* is the priority level Entuity uses when comparing collectors associated to the same attribute. The higher the number the higher the priority. User Defined Polling collectors always have a higher priority than system collectors.
- *Transform* Entuity uses to interpret the data to usable information. It does not require setting for indexes.

Click **OK** to create the collector for the flash file index.



entuity
User: admin@century [Logout]
Page Updated: 11:10:45, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
User Defined Collectors for UDComponent02 Objects
on server cent
Summary
Category: C
Object Typ
UDComponent
UDComponent
Transforn
Add Edit Delete
User Defined Collector (User Defined Attribute)
Name:
Descripti
Object Type:
Test
OK Cancel
Browse...
Edit...
Edit...
View
OK Cancel

Amended collector method.

Expression:

```
simple;snmp_get_indexes(snmpv2, ".1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.2", 500)
```

Results:

Attribute: uDC02Index

OID: .1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.2

Index: uDC02Index

Collector method requires amending for index attributes.

SNMP Version: ○ v1 ● v2 (Note: This setting is ignored if the device is being naged as v3 or v2c only)

Method: simple;snmp_get(snmpv2, ".1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.2", uDC02Index)

Filter: simple;sysoid_begins(".1.3.6.1.4.1.9")

Priority: 1000

Transform: None

Figure 349 Amend Index Method

## Creating the Flash File Name Collector

To create the collector for flash file name attribute:

1) From the Explorer tree select a device with a flashcard.

   This sets the context for when you create the attribute, including in multi-server environments the Entuity server on which you creating the User Defined Polling configuration.

2) Click **Administration** > **User Defined Polling** and then **Collectors** tab.

3) Set the context for creating the collector. Set:

   - *Server* to the Entuity server on which you want to configure the collector (only required in multi-server environments).

- *Category* to **Object Attributes**.
- *Object Type* to **UDComponent02**.

Click **Add**.

4) Entuity defaults:

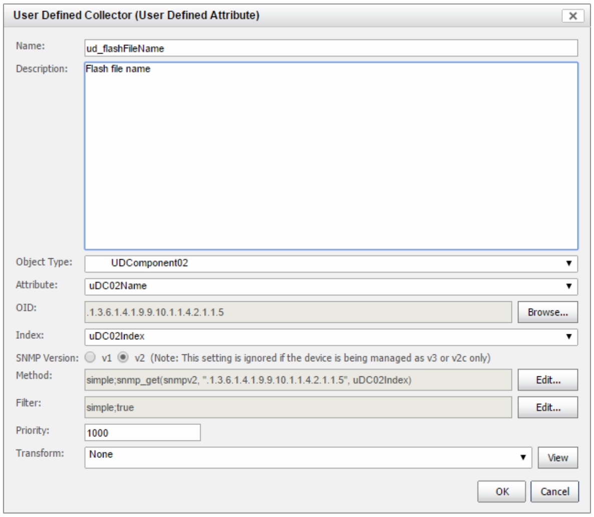
- *Name* to **ud_**. Change it to **ud_flashFileName**.
- An empty *Description*. Enter a meaningful description.
- *Object Type* to **UDComponent02**
- *Attribute* to **uDC02Index**. Change the attribute to **uDC02Name**.

From *OID* click **Browse**.

- From the SNMP MIB Browser you can enter the OID in *OID*.

  Alternatively you can click **MIB Manage** and use the MIB Manager to locate the flash file name (`.1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5`) and click **Close** to close the MIB Manager.

  Click **OK** to close the MIB Browser.



User Defined Collector (User Defined Attribute)

Name: ud_flashFileName

Description: Flash file name

Object Type: UDComponent02

Attribute: uDC02Name

OID: .1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5

Index: uDC02Index

SNMP Version: ○ v1 ● v2 (Note: This setting is ignored if the device is being managed as v3 or v2c only)

Method: simple;snmp_get(snmpv2, ".1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5", uDC02Index)

Filter: simple;true

Priority: 1000

Transform: None

Figure 350 Flash File Name

5) Complete the flash file name collector setup:

- In *Filter* set the filter Entuity uses to restrict creation of the object to devices that match the sysoid filter. You can set the *Filter* so the flash file configuration only applies to Cisco devices.

  Click **Edit** and in *Expression* change:

  ```
  simple;true
  ```

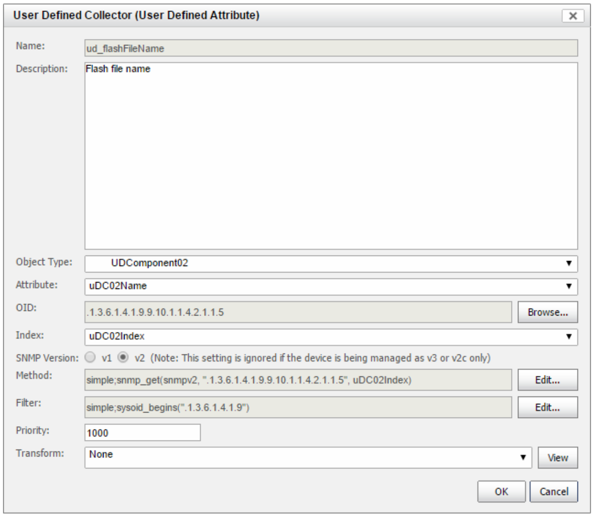
  to:

`simple;sysoid_begins(".1.3.6.1.4.1.9")`

You can type in the filter or highlight enterprise and click **Add**. Entuity displays the enterprise OIDs of devices under management. You can click **Select All** to view all available enterprise OIDs. A filter can support multiple sysoids.

- *Priority* is the priority level Entuity uses when comparing collectors associated to the same attribute. The higher the number the higher the priority. User Defined Polling collectors always have a higher priority than system collectors.
- *Transform* Entuity uses to interpret the data to usable information. It does not require setting for the name.

Click **OK** to create the collector for the flash file name.



User Defined Collector (User Defined Attribute)

Name: ud_flashFileName

Description: Flash file name

Object Type: UDComponent02

Attribute: uDC02Name

OID: .1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5

Index: uDC02Index

SNMP Version: ○ v1 ● v2 (Note: This setting is ignored if the device is being managed as v3 or v2c only)

Method: simple;snmp_get(snmpv2, ".1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5", uDC02Index)

Filter: simple;sysoid_begins(".1.3.6.1.4.1.9")

Priority: 1000

Transform: None

Figure 351 Flash File Name Collector

### Creating the Flash File Size Attribute, Collector and Events

The two collectors defined so far have been for object attributes Entuity has provided with the UDComponent02 object type. You can now define additional attributes for Entuity to poll. This example only adds one more attribute however you could add many more attributes.

To define the flash file size attribute, its collector and threshold events use the User Defined Polling Wizard:

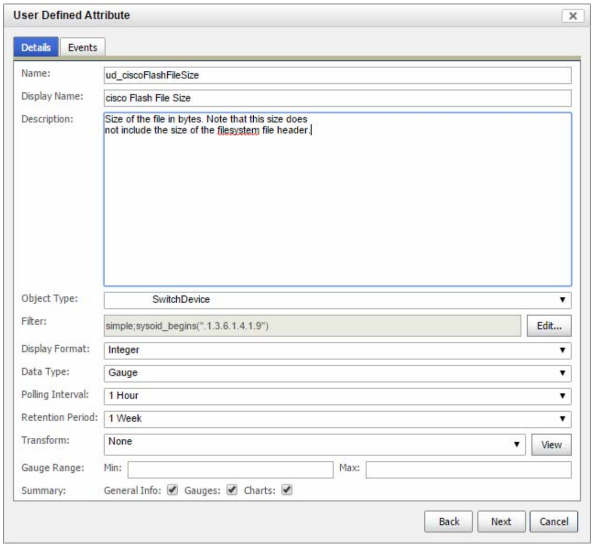
1) From the Explorer tree select a device with a flashcard.

   This sets the context for when you create the attribute, including in multi-server environments the Entuity server on which you are creating the User Defined Polling configuration.

2) Click **Administration > User Defined Polling** and then **User Defined Polling Wizard**.

   From the SNMP MIB Browser you can enter the file size OID (`.1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.2`) and click **Next**.

Entuity defaults from the MIB and your initial device selection appropriate defaults, however you may need to adjust them.



Name: ud_ciscoFlashFileSize

Display Name: cisco Flash File Size

Description: Size of the file in bytes. Note that this size does
not include the size of the filesystem file header.

Object Type: SwitchDevice

Filter: simple;sysoid_begins(".1.3.6.1.4.1.9")

Display Format: Integer

Data Type: Gauge

Polling Interval: 1 Hour

Retention Period: 1 Week

Transform: None

Gauge Range: Min: Max:

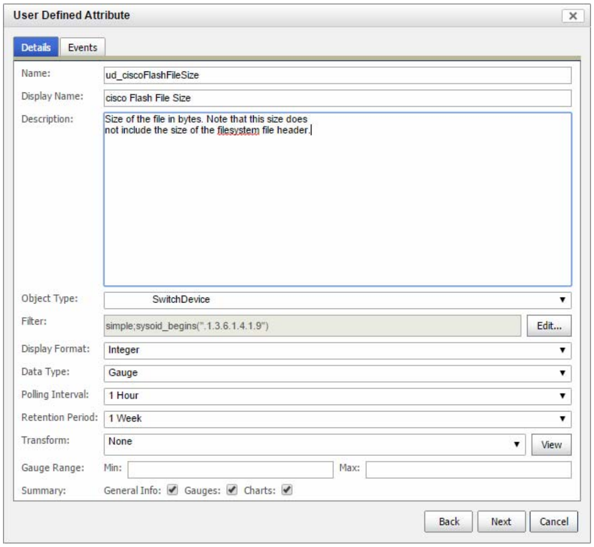
Summary: General Info: ☑ Gauges: ☑ Charts: ☑

Figure 352 Flash File Size Details

3) Set:

- *Object Type* to **UDComponent02**
- *Polling Interval* to **5 Minutes**.
- *Retention Period* to **1 Day**.
- In *Summary* select **General Info**.

And then click the **Events** tab.



User Defined Attribute

Name: ud_ciscoFlashFileSize

Display Name: cisco Flash File Size

Description: Size of the file in bytes. Note that this size does not include the size of the filesystem file header.

Object Type: SwitchDevice

Filter: simple;sysoid_begins(".1.3.6.1.4.1.9")

Display Format: Integer

Data Type: Gauge

Polling Interval: 1 Hour

Retention Period: 1 Week

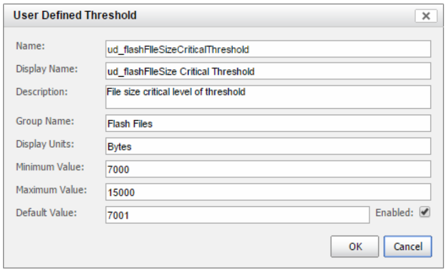
Transform: None

Gauge Range: Min: Max:

Summary: General Info: ☑ Gauges: ☑ Charts: ☑

Figure 353 Flash File Size Details

4) Select Threshold and then three severity event levels. For example click the Down arrowhead next to Critical and define the critical threshold level.



User Defined Threshold

Name: ud_flashFileSizeCriticalThreshold

Display Name: ud_flashFileSize Critical Threshold

Description: File size critical level of threshold

Group Name: Flash Files

Display Units: Bytes

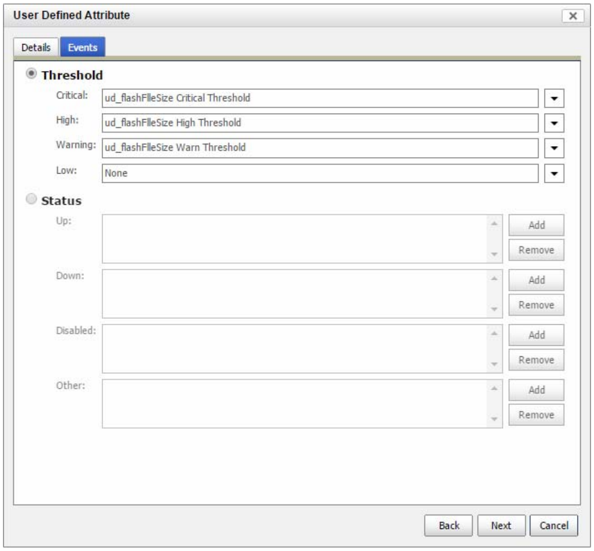
Minimum Value: 7000

Maximum Value: 15000

Default Value: 7001 Enabled: ☑

Figure 354 Define Flash File Thresholds

5) After completing the event thresholds click **Next**.



● Threshold

Critical: ud_flashFIleSize Critical Threshold

High: ud_flashFIleSize High Threshold

Warning: ud_flashFIleSize Warn Threshold

Low: None

○ Status

Up:

Down:

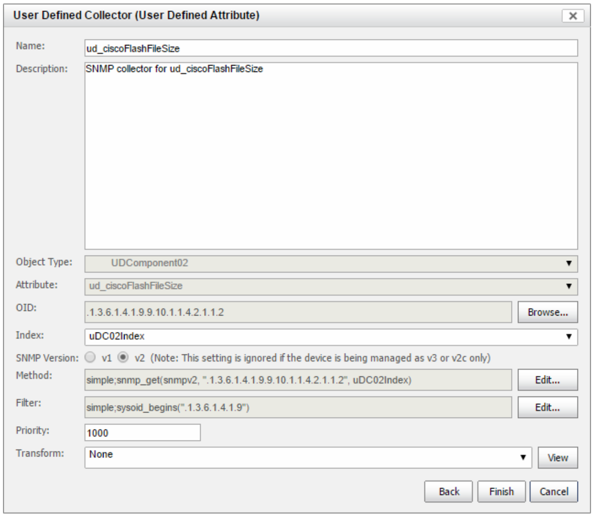
Disabled:

Other:

Figure 355 Flash File Size Event Thresholds

6) Entity defaults from the MIB and your initial device selection appropriate collector defaults, however you may need to adjust them.

Set *Index* to **uDC01Index**.



Name: ud_ciscoFlashFileSize

Description: SNMP collector for ud_ciscoFlashFileSize

Object Type: UDComponent02

Attribute: ud_ciscoFlashFileSize

OID: .1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.2

Index: uDC02Index

SNMP Version: ○ v1 ● v2 (Note: This setting is ignored if the device is being managed as v3 or v2c only)

Method: simple;snmp_get(snmpv2, ".1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.2", uDC02Index)

Filter: simple;sysoid_begins(".1.3.6.1.4.1.9")

Priority: 1000

Transform: None

Figure 356 Flash File Size Collector

7) Click **Finish** to create the configuration.

Entuity discovers the new collector, its attribute and then polls the system attribute. This may take a few minutes or hours depending upon the size of your managed network.

### Renaming the UDComponent Display Name

When you want to update the display name of the component you must make a change configuration file changes and run `configure`. For example if you have used `UDComponent02` to model a flash file object then to rename the display:

1) Copy *`entuity_home`*`\etc\sw_user_defined_components.cfg` to *`entuity_home`*`\etc\sw_user_defined_components_site_specific.cfg`.
2) In *`entuity_home`*`\etc\sw_site_specific.cfg` include the component file:

   ```
   !sw_user_defined_components_site_specific.cfg
   ```

3) Open `sw_user_defined_components_site_specific.cfg` and amend the component name. For example change:

   ```
   [Type UDComponent02]
   ClientData+=\ndisplayName=UD Component 02\n
   [Attribute uDComponents02]
   ClientData+=\ndisplayName=UDComponents02\n
   ```

   to:

   ```
   [Type UDComponent02]
   ClientData+=\ndisplayName=Flash File\n
   [Attribute uDComponents02]
   ClientData+=\ndisplayName=Flash Files\n
   ```

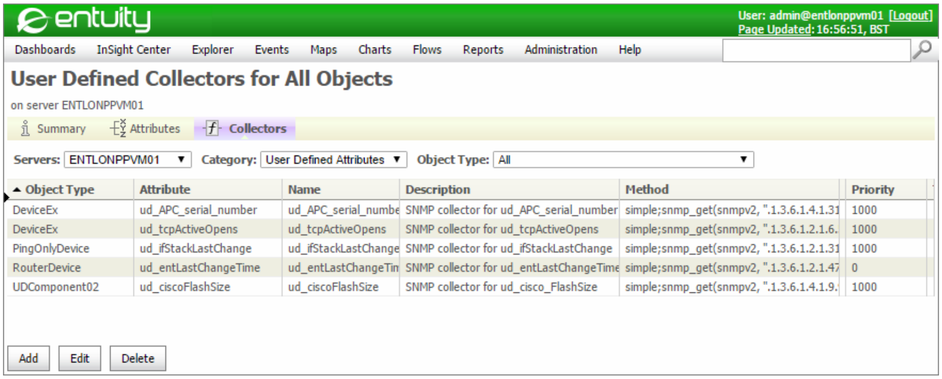
4) To apply these changes you must stop Entuity, run `configure` and then restart Entuity. For example from the command line enter:

   ```
   entuity_home\bin\stopeye
   entuity_home\install\configure defaults
   entuity_home\bin\starteye
   ```

## Multi-Server Support

When you are connected to a central server the:

- User Defined Polling Summary tab is in the context of the central server. When you then click **User Defined Polling Wizard** the attributes and collectors that you define are created on that server.
- Attributes and Collectors tabs default to the server according to alphanumeric priority. From the Servers drop-downs you can change the server.



User Defined Collectors for All Objects

on server ENTLONPPVM01

Servers: ENTLONPPVM01 Category: User Defined Attributes Object Type: All

| Object Type | Attribute | Name | Description | Method | Priority |
|---|---|---|---|---|---|
| DeviceEx | ud_APC_serial_number | ud_APC_serial_numbe | SNMP collector for ud_APC_serial_number | simple;snmp_get(snmpv2, ".1.3.6.1.4.1.31 | 1000 |
| DeviceEx | ud_tcpActiveOpens | ud_tcpActiveOpens | SNMP collector for ud_tcpActiveOpens | simple;snmp_get(snmpv2, ".1.3.6.1.2.1.6. | 1000 |
| PingOnlyDevice | ud_ifStackLastChange | ud_ifStackLastChange | SNMP collector for ud_ifStackLastChange | simple;snmp_get(snmpv2, ".1.3.6.1.2.1.31 | 1000 |
| RouterDevice | ud_entLastChangeTime | ud_entLastChangeTin | SNMP collector for ud_entLastChangeTime | simple;snmp_get(snmpv2, ".1.3.6.1.2.1.47 | 0 |
| UDComponent02 | ud_ciscoFlashSize | ud_ciscoFlashSize | SNMP collector for ud_cisco_FlashSize | simple;snmp_get(snmpv2, ".1.3.6.1.4.1.9. | 1000 |

Figure 357 Multi-Server Support

# Manage MIBs

For Entuity to poll attributes you must load to the server the appropriate MIBs. Entuity is shipped with a set of IETF and IANA MIB files (RFC-1212, RFC-1215, RFC1155-SMI, RFC1158-MIB, RFC1213-MIB and SNMPv2-SMI MIBs) in the MIBs directory which are available for you to load (parse). You can augment these by importing and then loading any additional MIBs that you require.

Entuity allows you to browse the loaded MIBs for the required sysOID; Browse MIB is the first step in the User Defined Polling wizard and it is also available when defining a collector. If the required MIB is not available you can open the MIBs manager through which you can control the MIBs available on your server.

When configuring trap forwarding through Event Management System you can also manage MIBs and in addition create rules and events from trap definitions.

## Importing MIB Definitions

You should only import to the Entuity server those MIBs that you require. Also you should not import multiple versions of the same MIB definition, as this would potentially cause confusion if you have to do any subsequent troubleshooting of that MIBs behavior. For example you could import ostensibly the same MIB through two files that have different file extensions. When you load (parse) those MIB files the result will be one loaded MIB but it would not be possible to determine which MIB file it was based on.

When you have access to the Entuity server you can directly add all of your required MIB files to the MIB folder, by default *entuity_home*`\lib\mibs`. Alternatively you can import them through the MIB manager which you can access through the Browse MIB dialog, opened when start the User Defined Polling wizard or when selecting an OID for a collector.

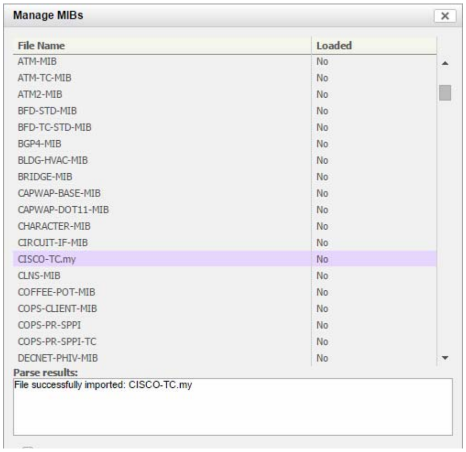
To import MIBs to the Entuity server when using the User Defined Polling wizard:

1) Click **Administration > User Defined Polling**.

2) Click **User Defined Polling wizard**.

3) From the Browse MIBs dialog click **Manage MIBs**.

4) Click **Import File**. You can use the upload dialog to navigate to the folder containing the MIB to import to the server.



| File Name | Loaded |
|---|---|
| ATM-MIB | No |
| ATM-TC-MIB | No |
| ATM2-MIB | No |
| BFD-STD-MIB | No |
| BFD-TC-STD-MIB | No |
| BGP4-MIB | No |
| BLDG-HVAC-MIB | No |
| BRIDGE-MIB | No |
| CAPWAP-BASE-MIB | No |
| CAPWAP-DOT11-MIB | No |
| CHARACTER-MIB | No |
| CIRCUIT-IF-MIB | No |
| CISCO-TC.my | No |
| CLNS-MIB | No |
| COFFEE-POT-MIB | No |
| COPS-CLIENT-MIB | No |
| COPS-PR-SPPI | No |
| COPS-PR-SPPI-TC | No |
| DECNET-PHIV-MIB | No |

Parse results:

File successfully imported: CISCO-TC.my

Figure 358 Manage MIBs

## Loading MIB Definitions

After you have imported MIBs to the Entuity server you must load (parse) them to the server.

When you have access to the Entuity server you can also directly upload MIBs parsed on one Entuity server to the loaded MIBs folder of another. The default folder for loaded MIBs is *entuity_home*`\lib\mibs\parsed`.

If through the Event Management System you have created events and rules from a MIB's trap definitions then the event project contains the rules, events and incidents to use with the traps. To set up the receiving server with the same configuration as the original server would also require the importing of the event project from the original to the new server and not just the transfer of MIB files.

To load MIBs to the Entuity server:

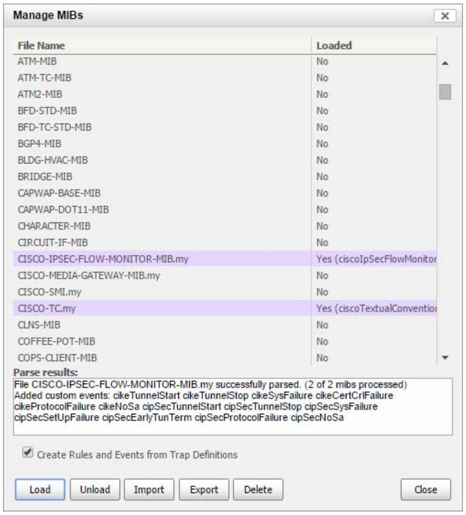
1) Click **Administration > User Defined Polling**.

2) Click **User Defined Polling wizard**.

3) From the Browse MIBs dialog click **Manage MIBs**.

4) From the list of MIBs highlight the MIB or MIBs to load and click **Load**.

   Entuity reports on the success or failure of each operation. Entuity updates the Loaded state of each successful load to Yes and in parenthesis includes the MIB object name.



| File Name | Loaded |
|---|---|
| ATM-MIB | No |
| ATM-TC-MIB | No |
| ATM2-MIB | No |
| BFD-STD-MIB | No |
| BFD-TC-STD-MIB | No |
| BGP4-MIB | No |
| BLDG-HVAC-MIB | No |
| BRIDGE-MIB | No |
| CAPWAP-BASE-MIB | No |
| CAPWAP-DOT11-MIB | No |
| CHARACTER-MIB | No |
| CIRCUIT-IF-MIB | No |
| CISCO-IPSEC-FLOW-MONITOR-MIB.my | Yes (ciscoIpSecFlowMonitor |
| CISCO-MEDIA-GATEWAY-MIB.my | No |
| CISCO-SMI.my | No |
| CISCO-TC.my | Yes (ciscoTextualConventio |
| CLNS-MIB | No |
| COFFEE-POT-MIB | No |
| COPS-CLIENT-MIB | No |

Parse results:

```
File CISCO-IPSEC-FLOW-MONITOR-MIB.my successfully parsed. (2 of 2 mibs processed)
Added custom events: cikeTunnelStart cikeTunnelStop cikeSysFailure cikeCertCrlFailure
cikeProtocolFailure cikeNoSa cipSecTunnelStart cipSecTunnelStop cipSecSysFailure
cipSecSetUpFailure cipSecEarlyTunTerm cipSecProtocolFailure cipSecNoSa
```

☑ Create Rules and Events from Trap Definitions

Figure 359 Load MIBs

## Unloading and Deleting MIB Definitions

Unloading a MIB deletes the parsed MIB from the parsed MIB folder. It does not remove any rules associated with the trap or custom events from the event project, as rules and events may potentially be shared by more than one MIB or trap definition. Instead when required you must separately delete custom events and trap processing rules.

Unloading a MIB does not update the event project. However if you also delete rules and custom events associated with the MIB this does change the event and would change the saving and deploying of the updated event project.

To unload MIBs from the Entuity server:

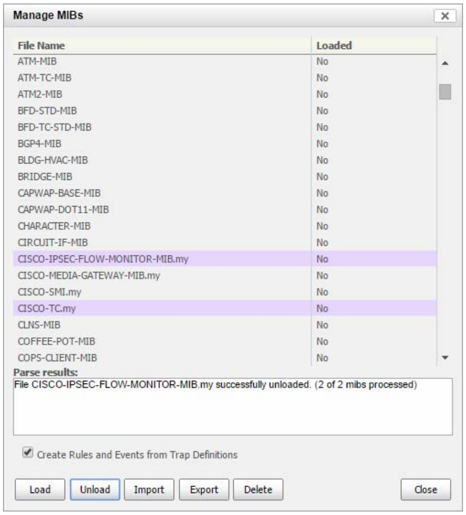
1) Click **Administration > User Defined Polling**.

2) Click **User Defined Polling wizard**.

3) From the Browse MIBs dialog click **Manage MIBs**.

4) From the list of MIBs highlight the MIB or MIBs to unload and click **Unload**.

   Entuity deletes the parsed MIBs from *entuity_home*`\lib\mibs\parsed`.



| File Name | Loaded |
|---|---|
| ATM-MIB | No |
| ATM-TC-MIB | No |
| ATM2-MIB | No |
| BFD-STD-MIB | No |
| BFD-TC-STD-MIB | No |
| BGP4-MIB | No |
| BLDG-HVAC-MIB | No |
| BRIDGE-MIB | No |
| CAPWAP-BASE-MIB | No |
| CAPWAP-DOT11-MIB | No |
| CHARACTER-MIB | No |
| CIRCUIT-IF-MIB | No |
| CISCO-IPSEC-FLOW-MONITOR-MIB.my | No |
| CISCO-MEDIA-GATEWAY-MIB.my | No |
| CISCO-SMI.my | No |
| CISCO-TC.my | No |
| CLNS-MIB | No |
| COFFEE-POT-MIB | No |
| COPS-CLIENT-MIB | No |

Parse results:

File CISCO-IPSEC-FLOW-MONITOR-MIB.my successfully unloaded. (2 of 2 mibs processed)

☑ Create Rules and Events from Trap Definitions

Figure 360 Load MIBs

## Deleting MIB Definitions

Deleting a MIB removes the trap definitions from the event project and deletes the loaded MIB from the parsed MIB folder and the unparsed MIB files from the Entuity server. It does not remove any rules associated with the trap or custom events from the event project, as rules and events may potentially be shared by more than one MIB or trap definition. Instead when required you must separately delete custom events and trap processing rules.

Deleting a MIB does not update the event project. However if you also delete rules and custom events associated with the MIB this does change the event and would change the saving and deploying of the updated event project.

To delete MIBs from the Entuity server:

1) Click **Administration** > **User Defined Polling**.

2) Click **User Defined Polling wizard**.

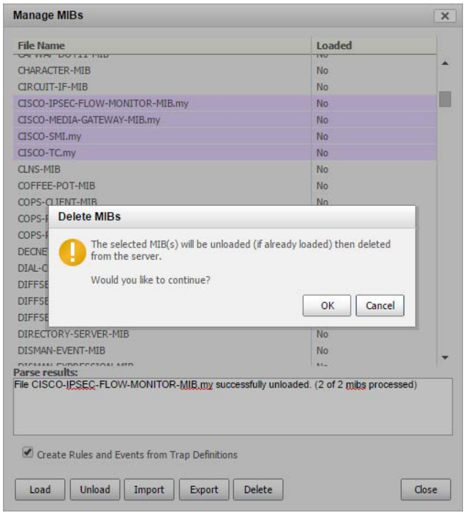
3) From the Browse MIBs dialog click **Manage MIBs**.

4) From the list of MIBs highlight the MIB or MIBs to delete and click **Delete**.

5) Entuity prompts you to confirm the deletion of the selected MIBs. Click **OK**.

   Entuity deletes for the selected MIBs:

   - Any parsed MIBs from *entuity_home*`\lib\mibs\parsed`.
   - Loaded MIBs from *entuity_home*`\lib\mibs`.



| File Name | Loaded |
|---|---|
| CHARACTER-MIB | No |
| CIRCUIT-IF-MIB | No |
| CISCO-IPSEC-FLOW-MONITOR-MIB.my | No |
| CISCO-MEDIA-GATEWAY-MIB.my | No |
| CISCO-SMI.my | No |
| CISCO-TC.my | No |
| CLNS-MIB | No |
| COFFEE-POT-MIB | No |
| COPS-CLIENT-MIB | No |
| COPS-F | |
| COPS-F | |
| DECNE | |
| DIAL-C | |
| DIFFSE | |
| DIFFSE | |
| DIFFSE | |
| DIRECTORY-SERVER-MIB | No |
| DISMAN-EVENT-MIB | No |

Delete MIBs

The selected MIB(s) will be unloaded (if already loaded) then deleted from the server.

Would you like to continue?

Parse results:

File CISCO-IPSEC-FLOW-MONITOR-MIB.my successfully unloaded. (2 of 2 mibs processed)

☑ Create Rules and Events from Trap Definitions

Figure 361 Delete MIBs

## Exporting MIB Definitions

You can export MIB files from the Entuity server, for example to import to another Entuity server. If you select:

- One MIB Entuity exports it as a single MIB file with the name of that MIB.
- Multiple MIBs Entuity exports them as one compressed file named `mibs.zip`.

To export MIBs from the Entuity server:

1) Click **Administration** > **User Defined Polling**.
2) Click **User Defined Polling wizard**.
3) From the Browse MIBs dialog click **Manage MIBs**.
4) From the list of MIBs highlight the MIB or MIBs to export and click **Export**. Entuity exports the MIB file to the browser download directory.

# 57 Entuity Cisco IOS IP SLA Module

Entuity Cisco IOS IP SLA module includes:

- Full support for 10 IP SLA operation types.
- Discovery and monitoring of all IP SLA operation types on devices, both created by Entuity and by third party tools.
- MPLS support for those IP SLA operation types that support MPLS.
- Control of both operation specification and automatic operation creation.
- Extensive Cisco IOS IP SLA event support, including configuration, availability and performance events and incidents to the Cisco IOS IP SLA operations.
- IP SLA Echo and IP SLA Details reports. IP SLA information is also reported on through the Branch Office Perspective and Network Summary report.

This allows, for example:

- Measurement of end-to-end metrics e.g. client-server latency and availability.
- Measurement of jitter, for streaming audio/video/ VoIP.
- Identification of slow or unreliable hops along a path.

## What are Cisco IOS IP SLA Measures?

Cisco IOS IP SLAs is an intelligent active agent available on Cisco devices with routing capabilities. Cisco IOS IP SLAs takes advantage of facilities already deployed (the Cisco IOS) and does not require any further hardware deployment (these are software operations). With Entuity Cisco IOS IP SLAs you are leveraging your current investment in Cisco devices and IOS.

Cisco IOS IP SLAs provides layer three and above monitoring. Its applications include web site monitoring and infrastructure troubleshooting. Metrics include response time, availability, jitter, connect time, packet loss and application performance.

Cisco IOS IP SLAs per-class traffic monitoring, enabled through TOS/DSCP, allows easy application of metrics to key Service Level Agreements (SLA). For example UDP jitter operation measures one-way latency, round-trip latency, jitter and packet loss all useful when monitoring infrastructure circuit quality and behavior.

## Entuity Cisco IOS IP SLA Module

Entuity Cisco IOS IP SLA is a licensable module available with Entuity. Activation of Entuity Cisco IOS IP SLA does not require additional software installation. You must acquire an appropriate license and then run Entuity `configure` to include the module. (See the *Entuity Getting Started Guide.*)

Entuity Cisco IOS IP SLA details are placed into views within Entuity and access permissions granted based on that view membership according to the standard Entuity security model.

### Entuity Cisco IOS IP SLA Data Management

IP SLA Operations are defined through the web UI and are instantiated as part of the Entuity discovery cycle, the length of which is dependent upon the characteristics of the network under management but would usually be within 24 hours.

By default all Entuity Cisco IOS IP SLA metrics are polled once every 300 seconds. Information, for which an historical record is kept, have their polled values retained, and available for reporting on, for 28 days.

### Command Line and Automated IP SLA Management

From the IP SLA tab you can manage IP SLA operations on the selected device. You can also manage IP SLA operations using the Entuity RESTful API. (See the *Entuity System Administrator Reference Manual*.)

You can use the:

- RESTful API `GET` function to view details of existing IP SLA operations on a device.
- RESTful API `PUT` function to create IP SLA operations and amend the parameters of existing IP SLA operations.
- RESTful API `DELETE` function to delete the IPSLA operation on the device for the given IPSLA creator name and type.

Management of IP SLA operations through a combination of RESTful API and the web UI is fully supported. However to manage IP SLA operations from web UI you must have the appropriate permissions within Entuity, to use the RESTful API you must have access to, and appropriate permissions on, the Entuity server.

## Managing and Monitoring Operations

Entuity separates the management of IP SLA operations, e.g. their definition, creation and destruction, from the monitoring of the data they return. This separation of management from polling tasks allows Entuity to accept data from operations created by third party tools, including from types of operations not directly supported by Entuity.

### Managing IP SLA Operations

You can create, amend and delete IP SLA operations. You can access operation type definitions from the device’s IP SLA tab in Explorer. There are a number of crucial attributes in managing devices. (For a full list see *Appendix D - IP SLA Operation Type Attributes*.)

| Attribute | Description |
|---|---|
| *Operation Index* | Unique identifier of the operation created by Entuity on the device. When creating more than 1 IP SLA operation on a device then you must set *Operation Index* to a unique value, as by default *Operation Index* is always set to 1.<br>For example when 2 operations share the same index Entuity would create an operation from the first definition, later it would compare the operation to the second operation definition, determine that they are different and recreate the operation. This loop would continue on the next discovery as the operation would now not match the first definition. |
| *Lifetime* | How long the operation exists on the device, by default **forever**. |
| *Owner* | Creator of the operation. All Entuity operations have an owner of EYE, this is user configurable. |

Table 60 Manage IP SLA Operations

Entuity checks that for each operation it manages on a device there is a current operation on that device, and that each operation on a device with a known owner, usually EYE, has a current definition in Entuity.

In detail, every five minutes for each operation on a device with an owner of **EYE,** Entuity checks that it has an IP SLA operation definition, i.e. through the *Operation Index*. When an *Operation Index* exists:

- On a device and in Entuity, this would be the usual case when you have *Lifespan* set to **forever**. This also implies that when you want to delete or suspend operations on a device you should do so from Entuity.

  Entuity then compares the definition with the operation on the device. When the definition and operation are:

  - The same, Entuity does not take any action.
  - Different, Entuity sends an instruction to delete the operation on the device.
- On a device but not on Entuity, Entuity sends an instruction to delete the operation on the device. This case would usually occur after you have deleted the operation definition from Entuity.
- In Entuity but not on a device, Entuity sends an instruction to create the operation on the device. This would usually occur after you have first created a definition, or after an amendment to the definition in Entuity that on the previous check resulted in the deletion of the operation. When you have amended *Lifespan*, for example to one day then each day the operation would terminate and Entuity would recreate it.

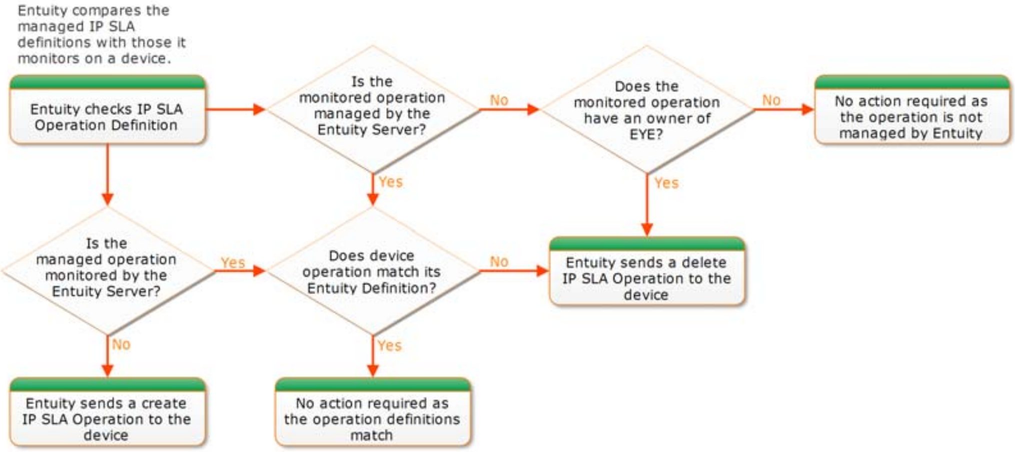
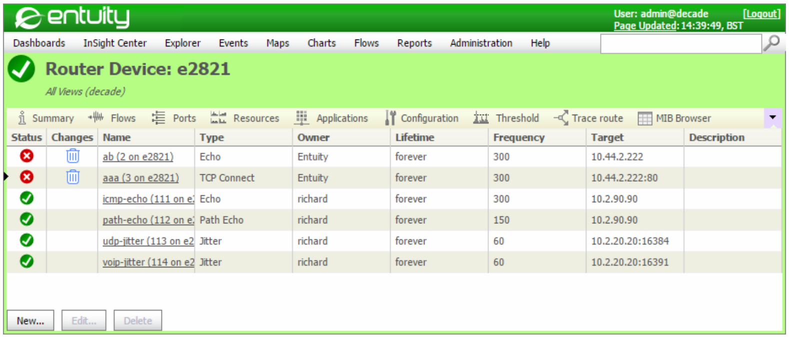

Entuity compares the managed IP SLA definitions with those it monitors on a device.
Entuity checks IP SLA Operation Definition
Is the monitored operation managed by the Entuity Server?
No
Does the monitored operation have an owner of EYE?
No
No action required as the operation is not managed by Entuity
Yes
Yes
Is the managed operation monitored by the Entuity Server?
Yes
Does device operation match its Entuity Definition?
No
Entuity sends a delete IP SLA Operation to the device
No
Yes
Entuity sends a create IP SLA Operation to the device
No action required as the operation definitions match

Figure 362 Managing IP SLA Operations

When Entuity creates an operation it checks to identify whether the create operation is successful, raising appropriate events:

- IP SLA Creation Failure, the operation failed to create, for example the SNMP write community string is not correct in Entuity.
- IP SLA Creation Succeeded, operation succeeded.


entuity
User: admin@decade [Logout]
Page Updated: 14:39:49, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
Summary Flows Ports Resources Applications Configuration Threshold Trace route MIB Browser
New... Edit... Delete

Router Device: e2821

*All Views (decade)*

| Status | Changes | Name | Type | Owner | Lifetime | Frequency | Target | Description |
|---|---|---|---|---|---|---|---|---|
| ✖ | 🗑 | ab (2 on e2821) | Echo | Entuity | forever | 300 | 10.44.2.222 | |
| ✖ | 🗑 | aaa (3 on e2821) | TCP Connect | Entuity | forever | 300 | 10.44.2.222:80 | |
| ✓ | | icmp-echo (111 on e2 | Echo | richard | forever | 300 | 10.2.90.90 | |
| ✓ | | path-echo (112 on e2 | Path Echo | richard | forever | 150 | 10.2.90.90 | |
| ✓ | | udp-jitter (113 on e2 | Jitter | richard | forever | 60 | 10.2.20.20:16384 | |
| ✓ | | voip-jitter (114 on e2 | Jitter | richard | forever | 60 | 10.2.20.20:16391 | |

Figure 363 IP SLA Operations

## Monitoring IP SLA Operations

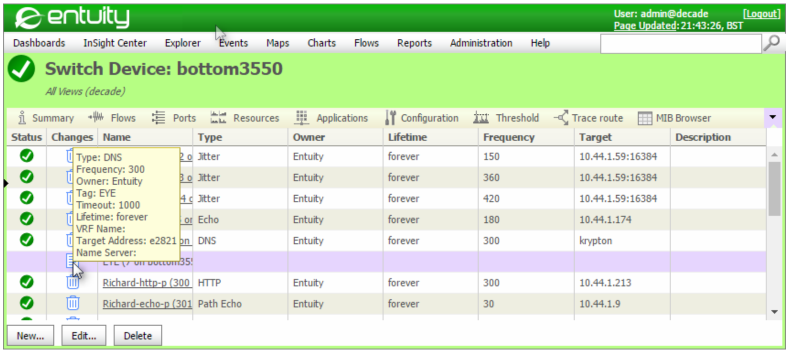
By default Entuity polls IP SLA operations every five minutes (300 seconds). Through Entuity you can monitor the returned statistics, the statistics vary according to the operation type. Entuity can also monitor operations created by other tools and/or of operation types different to those it formally supports.

Entuity includes four event types for monitoring operation performance:

- IP SLA Test Failed indicates the operation was created but data was not returned, for example the target device is not responding.

  IP SLA Test Succeeded indicates the operation was failing to return data, but is now working correctly.
- IP SLA Test High Latency indicates the operation is reporting latency above its set threshold. IP SLA Test High Latency Cleared indicates the operation is now reporting latency below its set threshold.
- IP SLA Low MOS is specific to the UDP Jitter VoIP operation, and indicates a MOS value lower than the set threshold. IP SLA Low MOS Cleared indicates the operation is now reporting MOS value above its set threshold.
- IP SLA High ICPIF is specific to the UDP Jitter VoIP operation, and indicates an ICPIF value greater than the set threshold. IP SLA High ICPIF Cleared indicates the operation is now reporting ICPIF value below its set threshold.

You can access operation type definitions from the device’s IP SLA tab. (See *Figure 364 IP SLA Operation Details*.)



Switch Device: bottom3550

*All Views (decade)*

| Status | Changes | Name | Type | Owner | Lifetime | Frequency | Target | Description |
|---|---|---|---|---|---|---|---|---|
| ✓ | | 2 o | Jitter | Entuity | forever | 150 | 10.44.1.59:16384 | |
| ✓ | | 3 o | Jitter | Entuity | forever | 360 | 10.44.1.59:16384 | |
| ✓ | | 4 c | Jitter | Entuity | forever | 420 | 10.44.1.59:16384 | |
| ✓ | | or | Echo | Entuity | forever | 180 | 10.44.1.174 | |
| ✓ | | on | DNS | Entuity | forever | 300 | krypton | |
| | | EYE (7 on bottom35 | | | | | | |
| ✓ | | Richard-http-p (300 | HTTP | Entuity | forever | 300 | 10.44.1.213 | |
| ✓ | | Richard-echo-p (301 | Path Echo | Entuity | forever | 30 | 10.44.1.9 | |

Type: DNS
Frequency: 300
Owner: Entuity
Tag: EYE
Timeout: 1000
Lifetime: forever
VRF Name:
Target Address: e2821
Name Server:

Figure 364 IP SLA Operation Details

# 58 IP SLA Operations

Entuity Cisco IOS IP SLA allows you to configure IP SLA operations, assisting you through their setup with sensible default values. IP SLA operations are set against a routing device, being configured on the source device but aimed at the target device.

Only users with administrator or IP SLA Management access rights can create Cisco IP SLA operations.

## Managing IP SLA Operations

IP SLA operations require:

- The device to have its SNMP write community string set.
- Their definition to be assigned to the device.

Entuity can also monitor IP SLA operations that it has not created, i.e. they were created either by other Entuity servers or third party tools. To monitor these operations Entuity does not require the SNMP write community string. Monitored operations can also be different from those Entuity formally supports, Entuity returns a useful set of data but it may not be complete for all types.

### Supported Cisco IOS IP SLA Operation Types

Entuity currently fully supports 10 Cisco IOS IP SLA operation types:

- DHCP
- HTTP
- ICMP Echo
- TCP Connect
- UDP Jitter
- DNS
- HTTP Raw
- ICMP Path Echo
- UDP Echo
- UDP Jitter VoIP.

For IP SLA operation type details see *Appendix D - IP SLA Operation Type Attributes* and *Appendix E - Operation Configuration Attributes*.

### Setting Device SNMP Write Community

Control over writing to network devices has serious security implications. To allow the successful configuration of IP SLA operations Entuity must be enabled to write to those devices. SNMPwrite is enabled through an attribute of the device.

Entuity allows you to define the configuration for operations on devices for which *SNMP Write Community* is not set, or is incorrectly set. When Entuity attempts to create an operation on the device without the correct authentication, then the first time the create operation fails

Entuity raises an IP SLA Creation Failure event. Another indication that the operation has failed is the absence of statistical data for the operation.

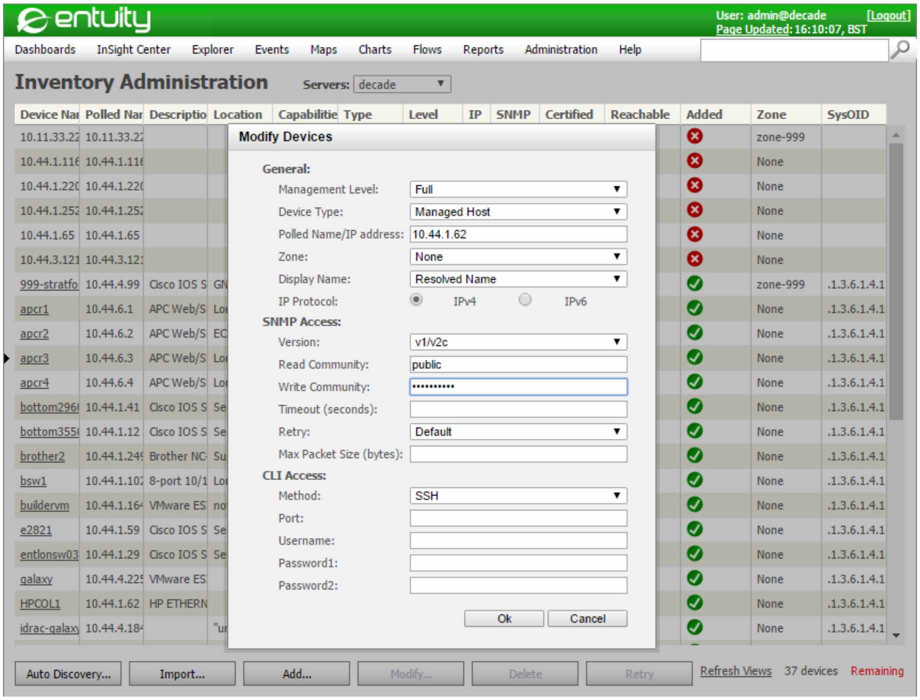
To set the SNMP write community string, ensure you are logged in as a user who is a member of the Administrator's group and:

1) Click **Administration** > **Inventory** / **Topology** > **Inventory Administration**.

2) Highlight the required device and click **Modify**.

3) In *Write Community* enter the write community string.

4) Click **OK**.



Inventory Administration

Servers: decade

| Device Nai | Polled Nai | Descriptio | Location | Capabilitie | Type | Level | IP | SNMP | Certified | Reachable | Added | Zone | SysOID |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.11.33.22 | 10.11.33.22 | | | | | | | | | | ✗ | zone-999 | |
| 10.44.1.116 | 10.44.1.116 | | | | | | | | | | ✗ | None | |
| 10.44.1.220 | 10.44.1.220 | | | | | | | | | | ✗ | None | |
| 10.44.1.252 | 10.44.1.252 | | | | | | | | | | ✗ | None | |
| 10.44.1.65 | 10.44.1.65 | | | | | | | | | | ✗ | None | |
| 10.44.3.121 | 10.44.3.121 | | | | | | | | | | ✗ | None | |
| 999-stratfo | 10.44.4.99 | Cisco IOS S | GN | | | | | | | | ✓ | zone-999 | .1.3.6.1.4.1 |
| apcr1 | 10.44.6.1 | APC Web/S | Lo | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| apcr2 | 10.44.6.2 | APC Web/S | EC | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| apcr3 | 10.44.6.3 | APC Web/S | Lo | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| apcr4 | 10.44.6.4 | APC Web/S | Lo | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| bottom296 | 10.44.1.41 | Cisco IOS S | Se | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| bottom355 | 10.44.1.12 | Cisco IOS S | Se | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| brother2 | 10.44.1.249 | Brother NC- | Su | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| bsw1 | 10.44.1.102 | 8-port 10/1 | Lo | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| buildervm | 10.44.1.164 | VMware ES | no | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| e2821 | 10.44.1.59 | Cisco IOS S | Se | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| entlonsw03 | 10.44.1.29 | Cisco IOS S | Se | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| galaxy | 10.44.4.225 | VMware ES | | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| HPCOL1 | 10.44.1.62 | HP ETHERN | | | | | | | | | ✓ | None | .1.3.6.1.4.1 |
| idrac-galaxy | 10.44.4.184 | | "ur | | | | | | | | ✓ | None | .1.3.6.1.4.1 |

Modify Devices

General:

Management Level: Full

Device Type: Managed Host

Polled Name/IP address: 10.44.1.62

Zone: None

Display Name: Resolved Name

IP Protocol: ● IPv4 ○ IPv6

SNMP Access:

Version: v1/v2c

Read Community: public

Write Community: ••••••••••

Timeout (seconds):

Retry: Default

Max Packet Size (bytes):

CLI Access:

Method: SSH

Port:

Username:

Password1:

Password2:

Figure 365 Private Community String

## Creating IP SLA Operations

When creating an operation assign a meaningful name.

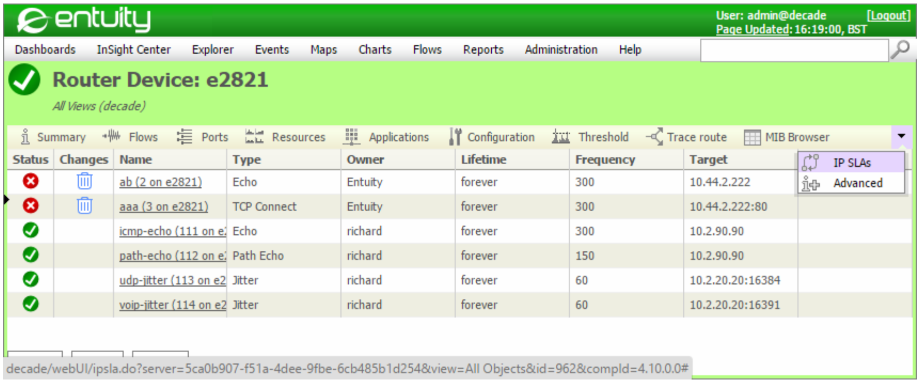
| Attribute | Description |
|---|---|
| *DeviceID* | Name or address of the device on which the operation is set. |
| *operationType* | IP SLA operation type. |
| *Target* | Target device. |

Table 61 Creating IP SLA Operations

To create IP SLA operations:

1) Through Explorer navigate to the device’s IP SLA tab.

   If the IP SLA tab is not visible you can extend the browser windows or select a tab by clicking the tab down arrow. (See *Figure 366 Navigating to Hidden IP SLA tab*.)



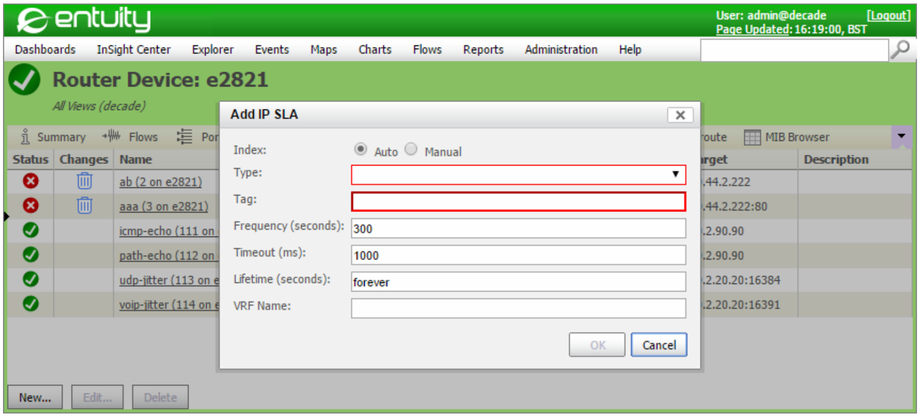
| Status | Changes | Name | Type | Owner | Lifetime | Frequency | Target |
|---|---|---|---|---|---|---|---|
| ✗ | 🗑 | ab (2 on e2821) | Echo | Entuity | forever | 300 | 10.44.2.222 |
| ✗ | 🗑 | aaa (3 on e2821) | TCP Connect | Entuity | forever | 300 | 10.44.2.222:80 |
| ✓ | | icmp-echo (111 on e: | Echo | richard | forever | 300 | 10.2.90.90 |
| ✓ | | path-echo (112 on e: | Path Echo | richard | forever | 150 | 10.2.90.90 |
| ✓ | | udp-jitter (113 on e2 | Jitter | richard | forever | 60 | 10.2.20.20:16384 |
| ✓ | | voip-jitter (114 on e2 | Jitter | richard | forever | 60 | 10.2.20.20:16391 |

decade/webUI/ipsla.do?server=5ca0b907-f51a-4dee-9fbe-6cb485b1d254&view=All Objects&id=962&compId=4.10.0.0#

Figure 366 Navigating to Hidden IP SLA tab

2) Click **New**.

   Entuity displays the Add IP SLA dialog and highlights in red the mandatory attributes. When you select the IP SLA Type the dialog will display the attributes specific to that type.



Add IP SLA

Index: ● Auto ○ Manual

Type:

Tag:

Frequency (seconds): 300

Timeout (ms): 1000

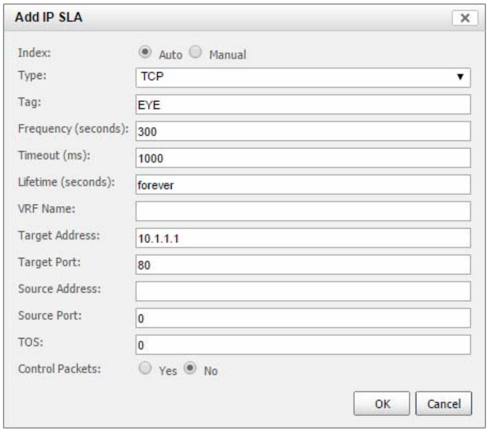
Lifetime (seconds): forever

VRF Name:

OK Cancel

Figure 367 Navigating to Hidden IP SLA tab

3) Define the operation, the attributes vary according to the operation type (see *Appendix D - IP SLA Operation Type Attributes*). Always assign the operation a meaningful name.



Add IP SLA

| | |
|---|---|
| Index: | ● Auto ○ Manual |
| Type: | TCP |
| Tag: | EYE |
| Frequency (seconds): | 300 |
| Timeout (ms): | 1000 |
| Lifetime (seconds): | forever |
| VRF Name: | |
| Target Address: | 10.1.1.1 |
| Target Port: | 80 |
| Source Address: | |
| Source Port: | 0 |
| TOS: | 0 |
| Control Packets: | ○ Yes ● No |

Figure 368 Defining IP SLA TCP Operations

4) Click **OK**.

Entuity saves the operation configuration and creates the first operation on the device.

## Checking IP SLA Operation Creation

An operation can fail because it was never created on the source device, or the operation failed to deliver information from the target device. Entuity includes two IP SLA management events and associated incidents:

- IP SLA Creation Failure, indicates the creation of an operation has failed on the source device. There may be access restrictions on the device, you may not have set the correct SNMP write community string, or have an invalid configuration.
- IP SLA Test Failed, indicates the operation was successfully created but it failed to connect to the target device. The target device may be unavailable, check firewall settings and that the device can respond to the operation.

## Deleting IP SLA Operations

From Entuity you can delete the IP SLA operation definition from which Entuity generates the operation. Entuity regularly checks that operations with an owner of EYE on a device have a managed definition. When there is not a definition, e.g. you have deleted it, then Entuity sends an instruction to the device to delete the operation.

To delete IP SLA operations from Entuity:

1) Through Explorer navigate to the device’s IP SLA tab.

If the IP SLA tab is not visible you can extend the browser windows or select a tab by clicking the tab down arrow. (See *Figure 366 Navigating to Hidden IP SLA tab*.)

2) Select the row of the IP SLA operation that you want to delete.

3) Click Delete and from the context menu click **Delete**.

On the next check of operations that Entuity manages on that device it removes those operations that no longer have a definition in Entuity.

When you are removing all operations from a device, and no longer require that the SNMP write community string is set in Entuity, do not immediately remove the community string. You must wait until all of the Entuity operations are deleted from the device.

## Monitoring IP SLA Operations

Entuity can monitor operations managed by itself, by other Entuity servers and third party tools. The table will be automatically refreshed after any user action (i.e. a successful create, edit or delete operation). The table will also schedule automatic updates at 5 minute intervals (the same frequency at which the IP SLA Poller watchdog and IP SLA Creator manager operations run) which should provide suitable resolution to observe state changes for the IP SLAs in the table.

When Entuity manages the operation you can click on the operation name and drill-down to the IPSLA poller definition.

| Attribute | Description |
|---|---|
| *Status* | 🔧 Awaiting creation and discovery of IP SLA on host device.<br>? Unable to poll host device.<br>✓ Host device reports that IP SLA is operational.<br>✗ Host device reports that last IP SLA operation was unsuccessful.<br>? Host device reports that last IP SLA was not started or completed for unknown reasons. |
| *Changes* | Absence of an icon indicates a change to the operator setup is not imminent. When the icon is:<br>📄 Indicates that this is the initial attempt to apply changes to IP SLA on this device and confirmation has not yet been received.<br>📄✗ At least one attempt to apply changes to the IP SLA operator has failed because, for example an invalid IP SLA configuration or this device is currently unreachable.<br>🗑 Indicates the IP SLA operation is due to be removed from this device. |

Table 58-1Monitor IP SLA Operations

| Attribute | Description |
|---|---|
| *Name* | User designated string to label the operation. It also acts as a hyperlink to the Explorer's Summary tab for the associated IP SLA Base Poller object (for IP SLAs which have been discovered on the device), or will be shown as plain text if only an IP SLA Creator object exists without an associated Poller object (e.g. Entuity has not yet created this IP SLA on the device, or it has not yet been discovered, or it defines an invalid IP SLA). |
| *Type* | IP SLA operation type. Entuity supports ten operation types which are DHCP, DNS, HTTP, HTTP Raw, Echo, TCP, Echo Path, Jitter, UDP and VoIP operations. |
| *Owner* | Name of the operation owner. By default, all operations created by Entuity will use EYE. |
| *Lifetime* | Integer specifying a period of time in seconds for which IP SLA will be active or the string 'forever' if the lifetime is unbounded. |
| *Frequency* | Integer value specifying interval between polling events in seconds. |
| *Target* | IP address or hostname for target device, or a target URL for IP SLAs with a HTTP probe. |
| *Description* | String specifying operation type dependent configuration data. |

Table 58-1Monitor IP SLA Operations

The operation’s Summary tab provides details of the configuration, together with collected and rolled up statistics tabs. (For details on the statistics collected for each operation see *Appendix D - IP SLA Operation Type Attributes*.)

## Monitoring Unsupported Operation Types

Entuity can discover and monitor operation types that are not one of the set it fully supports, by utilizing its root IP SLA definition. This root definition holds all of the attributes for the operations it formally supports. When Entuity discovers an operation outside of this set, Entuity still applies this root definition. Entuity can only display those attributes for the unsupported operation that correspond to an attribute for a supported operation.

Data from unsupported operations is monitored using the same processes as supported operations.

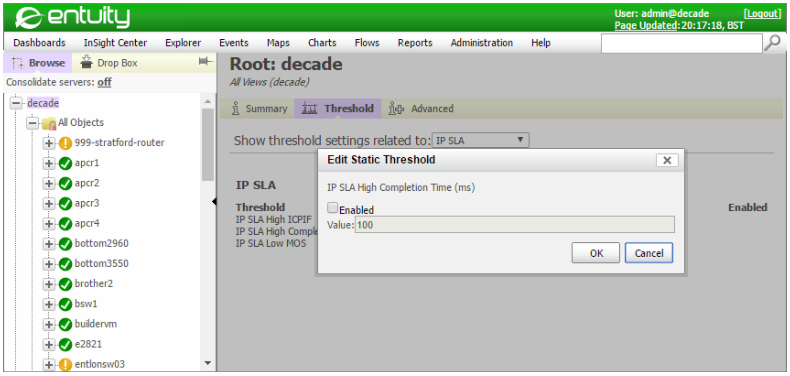
## Checking Operation Performance

Entuity Cisco IOS IP SLA is a key module in monitoring services where high latency would impact the user experience. Entuity includes three threshold events for monitoring network performance:

- IP SLA Low MOS and IP SLA High ICPIF are specific to the UDP Jitter VoIP operation. (See *Chapter 60 - Using Entuity IP SLA as a VoIP Solution*)
- IP SLA Test High Latency, indicates the operation is reporting latency between the source and target device above the set threshold for the operation.

  You can check the performance of the target device, where Entuity is managing the target there may be other raised events.

You can set the threshold on the IP SLA Test High Latency event against the Entuity server or the device.



Show threshold settings related to: IP SLA

IP SLA High Completion Time (ms)

☐ Enabled

Value: 100

Figure 369 Setting Thresholds Against All Devices

## Entuity Cisco IOS IP SLA Incidents

Entuity Cisco IOS IP SLA incidents are configured through the event project and managed through the event system. You can add annotations, assign incidents to users, close incidents and investigate incident details. Entuity includes a default set of Entuity Cisco IOS IP SLA incidents, details of which are in the *Event Reference Manual*:

- IP SLA Creation Failure Incident
- IP SLA High ICPIF Incident
- IP SLA Low MOS Incident
- IP SLA Test Failed
- IP SLA Test High Latency Incident.

# 59 Report on Performance Using IP SLA

Graphing and reporting of IP SLA attributes is available using Attribute Grapher, Change History, module reports and the InSight Center Branch Office Perspective.

## Gathering IP SLA Statistics

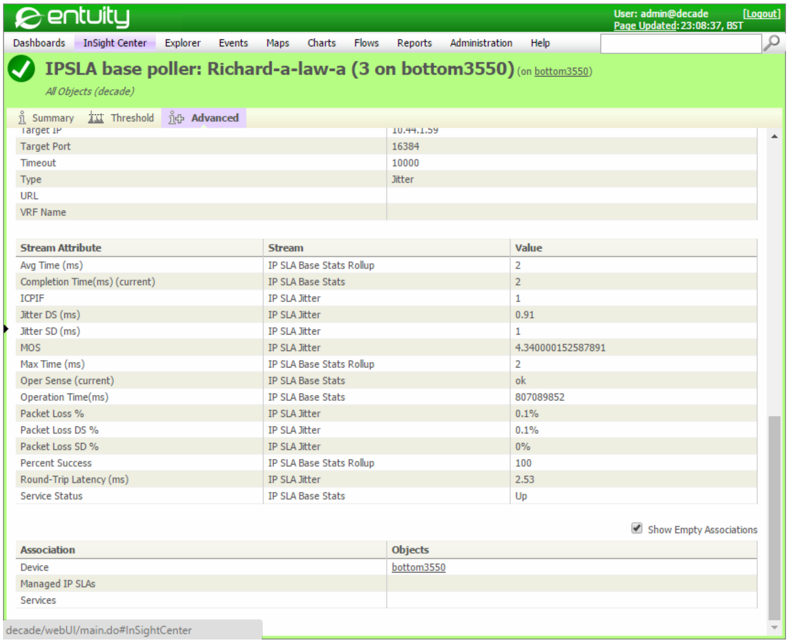
Different Cisco IP SLA operations share a core set of attributes, e.g. index, tag, type and return a core set of statistics, e.g. operation sense, completion time. By recognizing core attributes and statistics Entuity can monitor operations it does not formally support. For those operations it does formally support, Entuity recognizes the operation type and collects the data accordingly. (For details on the statistics collected for each operation see *Appendix D - IP SLA Operation Type Attributes*.)

By default, Entuity polls all monitored IP SLA operations every five minutes (300 seconds). Entuity retains the polled time-series data for seventy-two hours. This is data that we require for a history to be kept, for example ICMP Echo completion time. You can access the polled statistics through the operation's Advanced tab.

Entuity rolls up this data, i.e. extracts the most meaningful information and saves it in a form that can be efficiently used to graph and report on over a longer period, by default twenty-eight days. For example rather than keeping five minute completion times, Entuity rolls up the data into twenty minute samples and saves three completion time values for that sample the maximum time in milliseconds, percent success and average time in milliseconds. You can access the rolled-up statistics, through the operation's Advanced tab.

| Statistic | Description |
|---|---|
| *Maximum* | Maximum value of the attribute in the twenty minute rollup sample, e.g. *Max Time(ms)* is the highest completion in the polled values that were rolled up. |
| *Average* | Average value of the attribute in the twenty minute rollup sample, e.g. *Avg Time(ms)* is the average completion time calculated from the polled values that were rolled up. |
| *Percentage* | Percentage value of the attribute in the twenty minute rollup sample, e.g. for the echo path operation, *Percent Success* is the number of successful operations as a percentage of total number of operations in the rolled up sample. |
| *Delta* | The difference in value on the polled statistics since the last poll. |

Table 59 Types of Polled and Rollup Statistics



IPSLA base poller: Richard-a-law-a (3 on bottom3550) (on bottom3550)

*All Objects (decade)*

| | |
|---|---|
| Target IP | 10.44.1.59 |
| Target Port | 16384 |
| Timeout | 10000 |
| Type | Jitter |
| URL | |
| VRF Name | |

| Stream Attribute | Stream | Value |
|---|---|---|
| Avg Time (ms) | IP SLA Base Stats Rollup | 2 |
| Completion Time(ms) (current) | IP SLA Base Stats | 2 |
| ICPIF | IP SLA Jitter | 1 |
| Jitter DS (ms) | IP SLA Jitter | 0.91 |
| Jitter SD (ms) | IP SLA Jitter | 1 |
| MOS | IP SLA Jitter | 4.340000152587891 |
| Max Time (ms) | IP SLA Base Stats Rollup | 2 |
| Oper Sense (current) | IP SLA Base Stats | ok |
| Operation Time(ms) | IP SLA Base Stats | 807089852 |
| Packet Loss % | IP SLA Jitter | 0.1% |
| Packet Loss DS % | IP SLA Jitter | 0.1% |
| Packet Loss SD % | IP SLA Jitter | 0% |
| Percent Success | IP SLA Base Stats Rollup | 100 |
| Round-Trip Latency (ms) | IP SLA Jitter | 2.53 |
| Service Status | IP SLA Base Stats | Up |

☑ Show Empty Associations

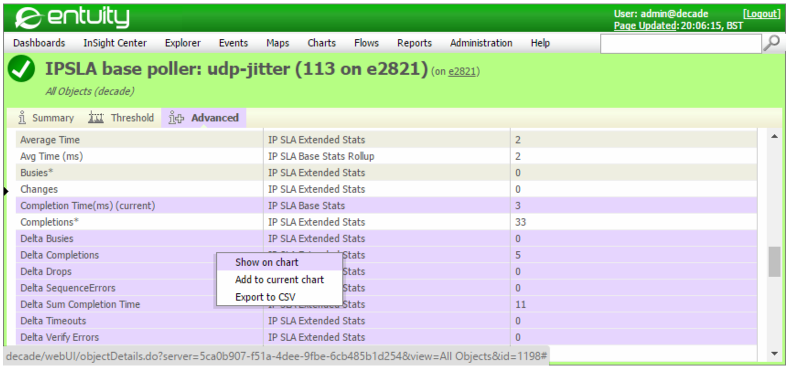
| Association | Objects |
|---|---|
| Device | bottom3550 |
| Managed IP SLAs | |
| Services | |

decade/webUI/main.do#InSightCenter

Figure 370 Jitter Statistics

## Reporting in Real-time on IP SLA Statistics

You can graph polled statistics in real-time through the Charts tool.



IPSLA base poller: udp-jitter (113 on e2821) (on e2821)

*All Objects (decade)*

| | | |
|---|---|---|
| Average Time | IP SLA Extended Stats | 2 |
| Avg Time (ms) | IP SLA Base Stats Rollup | 2 |
| Busies* | IP SLA Extended Stats | 0 |
| Changes | IP SLA Extended Stats | 0 |
| Completion Time(ms) (current) | IP SLA Base Stats | 3 |
| Completions* | IP SLA Extended Stats | 33 |
| Delta Busies | IP SLA Extended Stats | 0 |
| Delta Completions | Stats | 5 |
| Delta Drops | Stats | 0 |
| Delta SequenceErrors | Stats | 0 |
| Delta Sum Completion Time | Stats | 11 |
| Delta Timeouts | IP SLA Extended Stats | 0 |
| Delta Verify Errors | IP SLA Extended Stats | 0 |

decade/webUI/objectDetails.do?server=5ca0b907-f51a-4dee-9fbe-6cb485b1d254&view=All Objects&id=1198#

Figure 371 Echo Path Change History

To graph attributes:

1) Through Explorer navigate to the device’s IP SLA tab.

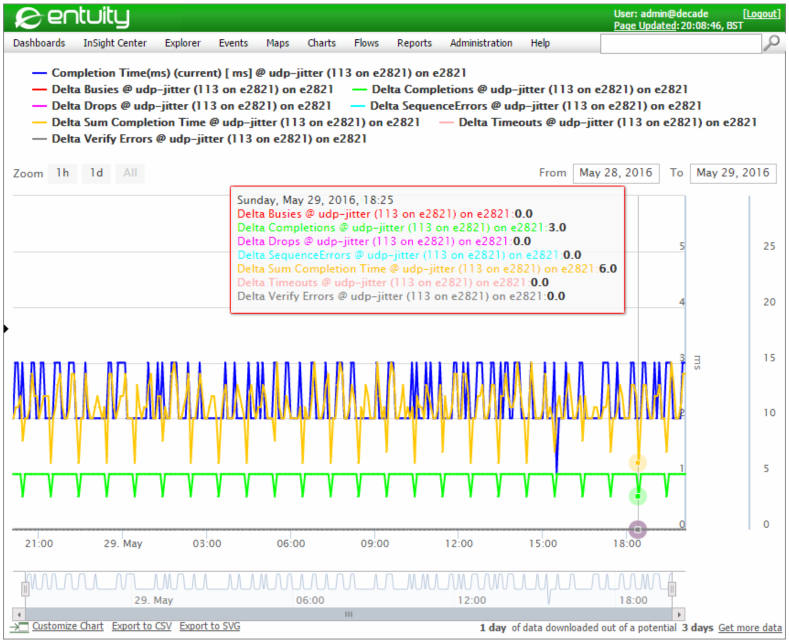
If the IP SLA tab is not visible you can extend the browser windows or select a tab by clicking the tab down arrow. (See *Figure 366 Navigating to Hidden IP SLA tab*.)

2) Click the name of the IP SLA operation.

3) Click the poller’s Advanced tab.

4) Highlight the attributes to include to the chart.

5) From the context menu click **Show on chart** to graph the attribute in a new grapher, or **Add to current chart** to add the attribute to an existing graph.


entuity
User: admin@decade [Logout]
Page Updated: 20:08:46, BST
Dashboards
InSight Center
Explorer
Events
Maps
Charts
Flows
Reports
Administration
Help
Zoom 1h 1d All
From May 28, 2016 To May 29, 2016
ms
0 1 2 3 4 5
0 5 10 15 20 25
21:00 29. May 03:00 06:00 09:00 12:00 15:00 18:00
29. May 06:00 12:00 18:00
Customize Chart
Export to CSV
Export to SVG
1 day of data downloaded out of a potential 3 days Get more data

— Completion Time(ms) (current) [ ms] @ udp-jitter (113 on e2821) on e2821
— Delta Busies @ udp-jitter (113 on e2821) on e2821
— Delta Completions @ udp-jitter (113 on e2821) on e2821
— Delta Drops @ udp-jitter (113 on e2821) on e2821
— Delta SequenceErrors @ udp-jitter (113 on e2821) on e2821
— Delta Sum Completion Time @ udp-jitter (113 on e2821) on e2821
— Delta Timeouts @ udp-jitter (113 on e2821) on e2821
— Delta Verify Errors @ udp-jitter (113 on e2821) on e2821

Sunday, May 29, 2016, 18:25
Delta Busies @ udp-jitter (113 on e2821) on e2821: **0.0**
Delta Completions @ udp-jitter (113 on e2821) on e2821: **3.0**
Delta Drops @ udp-jitter (113 on e2821) on e2821: **0.0**
Delta SequenceErrors @ udp-jitter (113 on e2821) on e2821: **0.0**
Delta Sum Completion Time @ udp-jitter (113 on e2821) on e2821: **6.0**
Delta Timeouts @ udp-jitter (113 on e2821) on e2821: **0.0**
Delta Verify Errors @ udp-jitter (113 on e2821) on e2821: **0.0**

Figure 372 Graphing Attribute Data

## Reporting IP SLA Performance

You can report on the information provided by the Entuity Cisco IOS IP SLA module using the:

- IP SLA Echo and IP SLA Details reports provided with the module, available from the Activity area of the Report Center.
- Branch Office Perspective available through the InSight Center. It provides an overview of the health of the network equipment at the selected branch office. Where multiple IP SLA operations are configured for a branch office their results are listed separately. You can drill down to the Branch Office Details report.

  The Branch Office Details report displays detailed time series charts for the WAN ports, monitored device Reachability and IP SLA operations. Various drill downs are available, a click on an IP SLA color ribbon opens the IP SLA Details report and displays that specific IP SLA operation with the selected time sample, zoomed in 10 fold.
- Network Summary report is a management level summary report, the type useful for

‘Monday morning’ reviewing of network availability and performance. It uses utilization and availability data collected as part of Entuity’s normal functioning, but can also use information collected by the Entuity Cisco IOS IP SLA module.

For more details on reports see the *Entuity Reports Reference Manual*.

# 60 Using Entity IP SLA as a VoIP Solution

Entuity Cisco IOS IP SLA can simulate VoIP traffic across the IP network, using three standard CODECs, and then measures network performance. Entuity reports on consistent voice quality scores (MOS and IPCIF) between Cisco IOS devices. Entuity Cisco IOS IP SLA's UDP Jitter VoIP solution is useful, for example, as a due diligence tool for administrators determining whether the network is ready for a full VoIP installation.

## IP SLA Based ICPIF and MOS Measurements

Both Impairment / Calculated Planning Impairment Factor (ICPIF) and Mean Opinion Score (MOS) are derived from metrics collected by the UDP Jitter VoIP operation type:

- ICPIF attempts to quantify the key impairments to voice quality that are encountered in the network. ICPIF values are expressed in a typical range of 5 (very low impairment) to 55 (very high impairment). ICPIF values numerically less than 20 are generally considered adequate. While intended to be an objective measure of voice quality, the ICPIF value is also used to predict the subjective effect of combinations of impairments.
- MOS is a common benchmark used to determine the quality of sound produced by specific CODECs. A wide range of listeners have judged the quality of voice samples sent using particular CODECs, on a scale of 1 (poor quality) to 5 (excellent quality). The opinion scores are averaged to provide the mean for each sample.

### Synchronizing Device Clocks

Unidirectional latency, ICPIF and VoIP metrics all require clock synchronization between the source and destination devices. When synchronization fails these metrics are not returned and gaps appear in the data. Use NTP (Network Time Protocol) to synchronize device clocks.

## Background to ICPIF

ICPIF originated in ITU-T recommendation G.113 (1996). It is used to quantify impairments to voice quality encountered across a network. ICPIF identifies and rates five types of impairment, and also a user expectation factor:

```
Icpif = Io + Iq + Idte + Idd + Ie - A
```

| Attribute | Description |
|---|---|
| *Io* | Impairments caused by non-optimal loudness rating or high noise, |
| *Iq* | Impairments caused by PCM type quantizing distortion, |
| *Idte* | Impairments caused by talker echo, |
| *Idd* | Impairments caused by one way transmission times (one way latency), |

Table 60 ICPIF Impairments

| Attribute | Description |
|---|---|
| *Ie* | Impairments caused by equipment effects, e.g. type of CODEC, packet loss. |
| *A* | Advantage factor (user expectation factor). |

Table 60 ICPIF Impairments

ICPIF values range from 0 to 55, with 0 considered a perfect score.

| ICPIF Upper Limit | Speech Communication Quality |
|---|---|
| 5 | Very Good |
| 10 | Good |
| 20 | Adequate |
| 30 | Limiting Case |
| 45 | Exceptionally Limiting Case |
| 55 | Customers likely to react strongly |

Table 61 ICPIF and Perceived Call Quality

## Equipment Impairment Factors (Ie)

The G.711 CODEC delivers a better quality of service than G.729a, but both operate within a packet environment. The actual impairment depends on the CODEC used and packet loss. The greater the packet loss, the greater the impairment. Cisco has measured voice quality with PSQM (ITU P.861) at discrete packet loss levels. Entuity uses this scale to translate packet loss levels for given CODECs into voice distortion values.

| Packet Loss (%) | G.711 Codec | G.729a Codec |
|---|---|---|
| 0 | o | 10 |
| 2 | 12 | 20 |
| 4 | 22 | 30 |
| 6 | 28 | 38 |
| 8 | 32 | 42 |

Table 62 Cisco Equipment Impairment Factor

## Transmission Delay Impairment(Idd)

The Idd value represents one way latency, times translated into values using the table taken from the ITU-T recommendation G.113.

| Latency (ms) | Idd | Latency (ms) | Idd |
|---|---|---|---|
| 150 | 0 | 400 | 25 |
| 200 | 3 | 500 | 30 |

Table 63 Transmission Delay Impairment (Idd)

| Latency (ms) | Idd | Latency (ms) | Idd |
|---|---|---|---|
| 250 | 10 | 600 | 35 |
| 300 | 15 | 700 | 40 |
| 350 | 20 | 800 | 40 |

Table 63 Transmission Delay Impairment (Idd)

### Advantage Factor

Delivery of service is about matching customer perception with their expectation of voice quality. Expectations vary according to the communication service, landline users have higher expectations than cell phone users. The Advantage Factor allows this expectation factor to be included in the ICPIF calculation, G113 provided expectation factors for typical networks. The default Advantage Factor for IP SLAs VoIP UDP jitter operations is always zero.

| Communication Service | Maximum A |
|---|---|
| Landline | 0 |
| Wireless (in building) | 5 |
| Cellular outside/moving vehicle | 10 |
| Difficult Location, multi-hop satellite link | 20 |

Table 64 Advantage Factor (A)

## Background to MOS

MOS provides a scale for the subjective experience of speech. Different CODECs deliver different quality levels of VoIP transmission. For each CODEC listeners have judged the quality of voice samples (which have known degrees of impairment), using a scale from 1 (poor) to 5 (excellent). These opinion scores were then averaged, providing a mean for each sample.

MOS is used by knowing the used CODEC, monitoring the level of transmission impairment and then deriving the MOS value. This MOS value indicates the user’s subjective experience of voice transmission.

## Combining ICPIF and MOS

Combining ICPIF and MOS measurements, combines both objective and subjective VoIP quality of service measurements.

| ICPIF | MOS | Interpretation |
|---|---|---|
| 0-3 | 4-5 | Excellent |
| 4-13 | 3-4 | Just Perceptible, not annoying |

Table 65 ICPIF to MOS (ITU G.113)

| ICPIF | MOS | Interpretation |
|---|---|---|
| 14-23 | 2-3 | Perceptible, slightly annoying |
| 24-33 | 1-2 | Annoying, not objectionable |
| 34-43 | 0-1 | Very annoying, objectionable |

Table 65 ICPIF to MOS (ITU G.113)

## IP SLA ICPIF and MOS Events

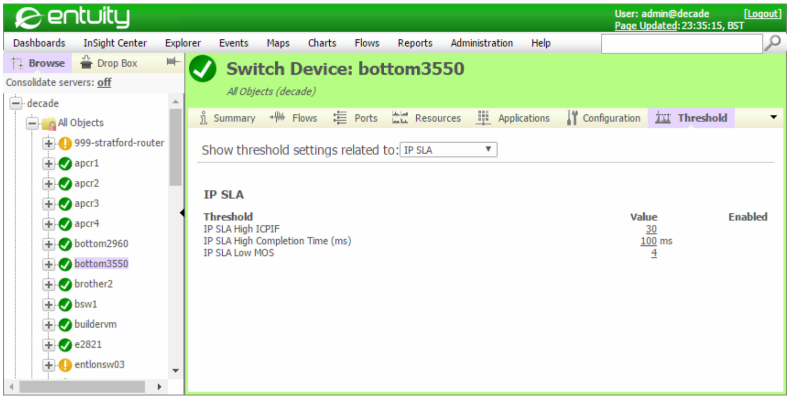
There are four events associated with ICPIF and MOS:

- IP SLA High ICPIF, default threshold 30
- IP SLA High ICPIF Cleared
- IP SLA Low MOS, default threshold 4.
- IP SLA Low MOS Cleared.

The IP SLA High ICPIF and IP SLA High ICPIF Cleared events are the opening and closing events respectively for the IP SLA High ICPIF incident. The IP SLA Low MOS and IP SLA Low MOS Cleared events are respectively the opening and closing events for the IP SLA Low MOS incident.

You can activate these events and amend the ICPIF and MOS event thresholds at the Entuity server and device level. To amend a device’s IP SLA threshold:

1) Highlight the device and from the context menu click **Threshold Settings**.
2) From *Show threshold settings* click **IP SLA**.
3) Amend and activate the threshold settings.



Switch Device: bottom3550

*All Objects (decade)*

Show threshold settings related to: IP SLA

IP SLA

| Threshold | Value | Enabled |
|---|---|---|
| IP SLA High ICPIF | 30 | |
| IP SLA High Completion Time (ms) | 100 ms | |
| IP SLA Low MOS | 4 | |

Figure 373 Setting VoIP Event Thresholds

# 61 Troubleshooting IP SLA Performance

You should always consult the Cisco IP SLA documentation for details on enabling and managing IP SLA operations. This troubleshooting section covers:

- *Operations Are Not Being Created*
- *Operations Failing to Create After Configuring the Source Port*
- *IP SLA and Firewalls*
- *Enabling the IP SLA Responder on Operation Targets*.

## Operations Are Not Being Created

When Entuity Cisco IOS IP SLA fails to create operations:

1) Check that you have set the SNMP write community string for the device.

   Entuity would raise IP SLA Creation Failure events and incidents indicating the creation of an operation has failed on the source device. There may be access restrictions on the device, you may not have set the correct SNMP write community string, or have an invalid configuration.

2) Consider whether you have waited long enough for Entuity to discover the operation definition. The length of the Entuity discovery cycle is dependent upon the network it is managing, you may have to wait for 24 hours.

## Operations Failing to Create After Configuring the Source Port

When you specify a particular port, ensure that it is the only operation on that device to use that port. For example, to emulate VoIP traffic you may use the source port 16834. However do not assign a second UDP Jitter operation to that device using the same source port otherwise the operation may fail.

Same source port failure can occur across all operation types, but it is more likely when the conflict involves an operation that take a greater time to complete, e.g. UDP Jitter.

Entuity recommend the port on the source device used by an operation should not be shared with other operations. When source port is set to 0 (the default for most operation types) the operation automatically selects any available port, and avoids any potential conflict.

## IP SLA and Firewalls

When using IP SLA with firewalls always consider which ports and commands must be allowed through the firewall.

### Entuity to Device Firewalls

When you have configured firewalls to perform deep packet inspection, you usually need only permission through snmpGet for Entuity to poll devices. The Entuity Cisco IOS IP SLA module requires that snmpSet commands also be permitted. When not allowed these commands fail. The initial reaction may be to check that the correct snmpWriteCommunity string is set, but also check firewall command permissions.

### Device to Device Firewalls

When source and target devices are separated by a firewall, the firewall must be open to ports used by Entuity Cisco IOS IP SLA. You should consider:

- When using *Control Packets* that the control protocol uses port 1967. The IP SLA source can specify which port the responder should listen to for a particular operation.
- *Target port* should always be open.
- *Source port* should be defined to allow responses through firewalls. When not defined, the default state for many operation types, then responses will not pass through the firewall.

## Enabling the IP SLA Responder on Operation Targets

The IP SLA Responder is a feature which allows the use of UDP and TCP operations. The IP SLA Agent Responder code must exist on target devices to support operations which use non-native services such as the UDP echo and the TCP connection operation types.

Consult the Cisco IP SLA documentation for details on enabling IP SLA responders.

# 62 Entuity Cisco Unified Communications Manager

Entuity CUCM module manages Cisco® Unified Communications Manager (CUCM). All of the CUCM information is integrated within Entuity's business management database. This comprehensive data allows improved CUCM performance, as reliability is dependent on correct configuration and operation of associated components. Entuity CUCM generates, where appropriate, both performance and availability events. All CUCM information is available for reporting.

The Entuity CUCM module can also be implemented as part of a VoIP solution. (See *QoS Monitoring of VoIP Traffic*.)

## Cisco Unified Communications Manager (CUCM)

CUCM is an IP telephony system, placing calls over the IT network. The phones that CUCM manages use the same IP network as other network services. The Entuity CUCM module allows you to manage CUCM as part of the network infrastructure.

CUCM is the controlling software for a Cisco VoIP deployment, managing and/or monitoring:

- A range of devices and device types
- Users
- Phone directory (i.e. phone MAC:extension:user:IP)
- Enables call placement
- Other CUCMs
- Time zones
- Supports redundancy.

## Entuity CUCM Integration

Entuity manages CUCMs as an application on a managed host device. Entuity does not automatically discover these devices, by default, but instead you manually add them. (See *Entuity CUCM Discovery*.) Once under it management Entuity can then discover further CUCM details. Entuity polls CUCMs using SNMP.

CUCM management is integrated into Entuity with inventory data displayed through its tabbed interface, events and incidents through Event Viewer and data being available to reports.

Entuity CUCM presents all of the data in the CUCM MIB, including:

- Device pools, e.g. time zones, TFTP servers, regions and inter-region bandwidths.
- Configuration and status (history) for IP phones, Gateways, Gatekeepers, Voice-Mail devices, Media devices, CTI devices, H.323 devices.
- CUCM status, e.g. number of each device type (registered, rejected, active), memory and CPU usage, uptime, process count.

Entuity's event manager raises:

- CUCM process monitoring events, against CPU and memory utilization, indicating reduced performance or increased risk of failure.
- Availability events for changes in managed device status.
- Resource events against the CUCM managed host, e.g. disk space, total memory usage.

You can report on CUCM managed host devices, on CUCMs through the CUCM Inventory report and all CUCM data is also available for reporting on through Flex Reports.

# Activating Entuity CUCM

Activation of Entuity CUCM does not require additional software installation. You must acquire an appropriate license, include its configuration and then run Entuity `configure`. Entuity CUCM also requires that the Entuity Managed Hosts module is activated.

## Module Licensing

Entuity components are licensed by type. To run the full Entuity CUCM module the license must include the CUCM type (see the *Entuity Getting Started Guide*). The Managed Hosts type is included with all Entuity licenses.

## Module Availability

The Entuity CUCM module is available with Entuity in all supported environments (see the *Entuity Getting Started Guide*).

## Module Security

CUCMs are placed into views within Entuity and access permissions granted based on that view membership according to the standard Entuity security model.

## Entuity CUCM Data Management

All Entuity CUCM metrics for which an historical record is kept have their polled values retained, and available for reporting on, for 28 days.

# Entuity CUCM Discovery

Entuity recommend, and have set as the default, configuring AutoDiscovery so it does not discover CUCMs. AutoDiscovery configuration file, `autodisc.cfg`, excludes the relevant sysoids:

```
-excludesysoids=1.3.6.1.4.1.311.1.1.3.1.2,1.3.6.1.4.1.2.3.1.2.1.1.3,1.
3.6.1.4.1.8072.3.2.10,1.3.6.1.4.1.8072.3.2.3,1.3.6.1.4.1.311.1.1.3.1.1
,1.3.6.1.4.1.311.1.1.3.1.3
```

### Discovering Managed Host Packages

Entuity CUCM is enabled through the Managed Hosts module. The packages on the managed host are not, by default, discovered. Knowledge of these packages can be useful when troubleshooting a CUCM installation.

To discover managed host packages:

1) Highlight the managed host for which you want to discover packages.
2) From its **Thresholds** page select Managed Hosts.
3) Enable Package Discovery and set the number of packages Entuity can discover. When set to 0 Entuity discovers all of the packages on the device.
4) Click **OK** to enable discovery.

## QoS Monitoring of VoIP Traffic

VoIP traffic requires a certain level of network resource for the user to receive an acceptable level of voice quality. Quality of Service (QoS) is designed to ensure VoIP traffic receives the necessary level of preferential treatment reducing or eliminating the delay of voice packets that travel across a network.

The Entuity Cisco IOS IP SLA module allows monitoring of VoIP through a number of metrics, including both Impairment / Calculated Planning Impairment Factor (ICPIF) and Mean Opinion Score (MOS) which are derived from IP SLA UDP Jitter Operation metrics:

- ICPIF attempts to quantify the key impairments to voice quality that are encountered in the network. ICPIF values are expressed in a typical range of 5 (very low impairment) to 55 (very high impairment). ICPIF values numerically less than 20 are generally considered adequate. While intended to be an objective measure of voice quality, the ICPIF value is also used to predict the subjective effect of combinations of impairments.
- MOS is a common benchmark used to determine the quality of sound produced by specific codecs. A wide range of listeners have judged the quality of voice samples sent using particular codecs, on a scale of 1 (poor quality) to 5 (excellent quality). The opinion scores are averaged to provide the mean for each sample.

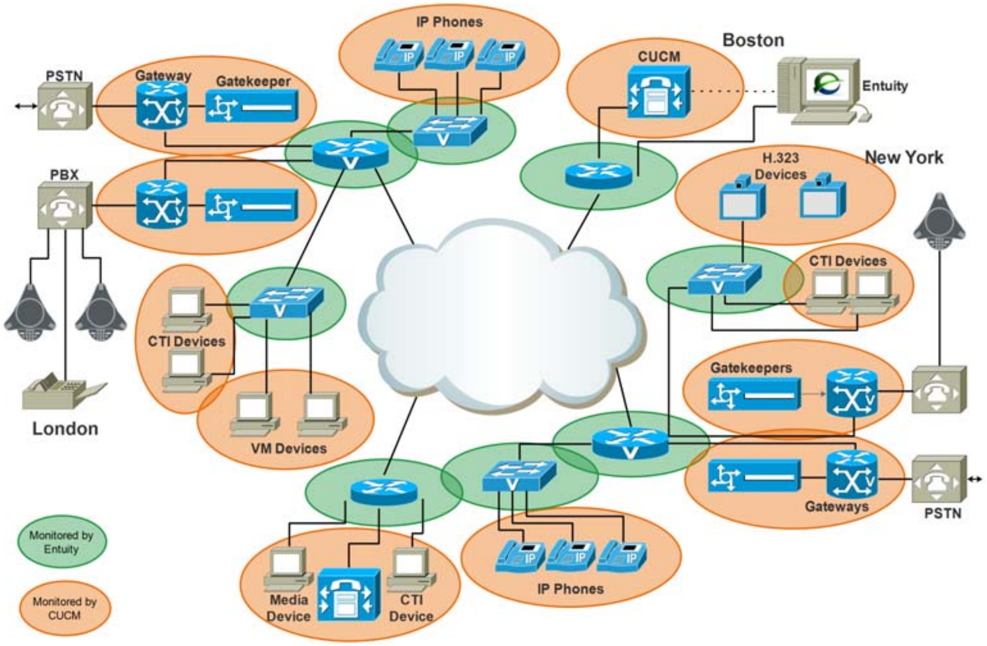


Figure 374 Entuity CUCM module as part of a VoIP Solution

# 63 Cisco Wide Area Application Services

Entuity WAAS module manages Cisco wide area application services (WAAS) devices.

## Cisco WAAS Overview

Cisco Systems developed WAAS to optimize the performance of TCP-based applications operating in a secure wide area network (WAN) environment. WAAS combines WAN optimization, acceleration of TCP-based applications, and Cisco's Wide Area File Services (WAFS) in a single appliance or blade.

WAAS technology usually involves a pair of devices that reside each end of a WAN link, one configured as the Core Server, the second as the Edge Client.

## Entuity WAAS Module

Entuity WAAS manages Cisco WAAS devices using Entuity to display information, statistics and alerts that are specific to them.

Entuity WAAS manages WAAS devices as a separate device type, discovering general device details (e.g. name, description, polled IP address), and also Central Server Host attributes, WAAS Device Type (Core Server or Edge).

Entuity WAAS displays information through he web UI. The exact layout depends on how the device has been configured (Server or Edge):

- WAAS Connection, for each connection between the managed device and its corresponding peer Entuity WAAS details:
  - Inbound Compression Ratio
  - Outbound Compression Ratio
  - Total Inbound Kbs
  - Total Outbound Kbs
  - Total Inbound Messages
  - Total Outbound Messages.

  These are polled every hour. Hourly data is kept for one week while daily data is kept for six months.
- Status, indicates for:
  - Edge devices, whether the Edge Component is running.
  - Core Servers, whether the Core Server component is running.

  These are polled every five minutes and this data is kept for one week.
- Cache Statistics, providing details of:
  - Max Cache Volume
  - Current Cache Volume

  - Max Cache Resources
  - Current Cache Resources
  - Resources Evicted Number
  - Last Evicted Time
  - Volume High Watermark
  - Volume Low Watermark
  - Volume Percentage High Watermark
  - Volume Percentage Low Watermark.

  These are polled every hour. Hourly data is kept for 1 week while daily data is kept for six months.

- CIFS Statistics, providing details of:
  - Total Bytes Read
  - Total Bytes Written
  - Remote Request Count
  - Local Request Count
  - Total Remote Time
  - Total Local Time
  - Connected Session Count
  - Open Files Count.

  These are polled every hour. Hourly data is kept for one week while daily data is kept for six months.

## Licensing

Entuity components are licensed by type. To run the full Entuity WAAS module the license must include the WAAS device type. Entuity installations that do not include the license display only the most high level details of the discovered WAAS, i.e. through the General tab.

## Security

Entuity WAAS management conforms to the standard Entuity security model, with permissions being granted through View membership.

## Availability

The Entuity WAAS module is available with Entuity in all supported environments.

# 64 Entuity QoS Module

Entuity® QoS module supports Cisco® QoS Modular CLI (QMC). It provides a detailed inventory of your QoS configuration, together with monitoring in real-time of each interface's performance. This information is also available for reporting on through Flex Reports and Report Builder.

Entuity QoS is available as a separate, licensed module enabled through `configure`.

## Why use Cisco IOS QoS?

The Cisco IOS® includes already installed QoS features to allow control over, and predictable service of, different networked applications and traffic types.Entuity QoS improves:

- Control over resources, with visibility into which resources (bandwidth, equipment, wide-area facilities, and so on) are being used. For example, you can limit the bandwidth consumed over a backbone link by FTP transfers or give priority to an important database access.
- Increased efficient usage of network resources, you will know what your network is being used for and that you are servicing the most important traffic to your business.
- Monitoring of tailored services through knowledge of traffic classes.
- Delivery of services through close monitoring of the applications that are most important to your business, e.g. bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available, and that other applications using the link get their fair service without interfering with mission-critical traffic.

QoS management helps to set and evaluate QoS policies and goals. A common methodology involves:

1) Using Entuity to identify the performance and traffic characteristics of the network.
2) Deploying Entuity QoS to the targeted devices.
3) Using Entuity QoS to test and evaluate service delivery. As your network changes, so will your QoS requirements and constant monitoring of both is essential.

Entuity QoS returns extensive QoS configuration details, presenting policy maps, class maps, access groups and their relationships. Entuity QoS includes extensive drilldown capabilities, exposing the often complex, nested relationships involved with QoS implementations.

Entuity allows reporting on inventory and performance data. You can also build reports having extensive access to QoS data, allowing reporting on inventory, performance, e.g. busiest class, traffic profiling, compare pre and post performance statistics.

# QoS Data Collection

By default Entuity QoS restricts collection of QoS data to infrastructure ports, this restriction controls the load QoS data collection places on your Entuity server. For infrastructure ports Entuity QoS sets *QoS Enabled* to **Yes** and for all other ports sets it to **No**. Entuity identifies an infrastructure port as one with a *VIP Status* of **Router**, **Trunk**, **Uplink** or **Server Link**.

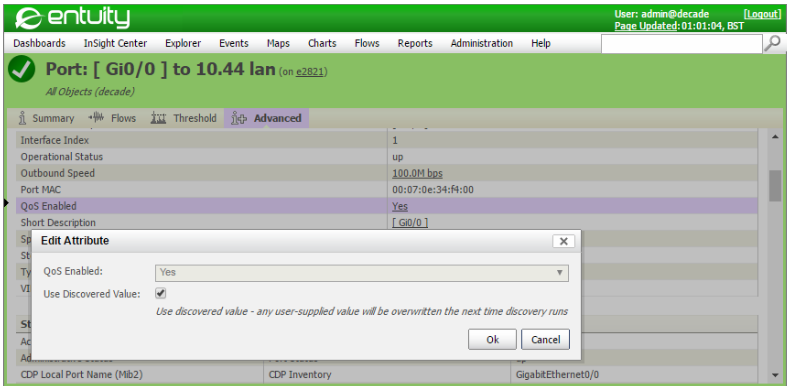
When you want to override the default QoS behavior of a port you amend *QoS Enabled*. For example, to activate QoS data collection on a port that does not have the appropriate *VIP Status*:

1) From the web UI Explorer select the port.

2) Click **Advanced**.

3) Set *QoS Enabled* to **Yes**.

When you want to disable QoS collection for a port set it to **No**.



Port: [ Gi0/0 ] to 10.44 lan (on e2821)

All Objects (decade)

| | |
|---|---|
| Interface Index | 1 |
| Operational Status | up |
| Outbound Speed | 100.0M bps |
| Port MAC | 00:07:0e:34:f4:00 |
| QoS Enabled | Yes |
| Short Description | [ Gi0/0 ] |

Edit Attribute

QoS Enabled: Yes

Use Discovered Value: ☑

*Use discovered value - any user-supplied value will be overwritten the next time discovery runs*

| | | |
|---|---|---|
| CDP Local Port Name (Mib2) | CDP Inventory | GigabitEthernet0/0 |

Figure 375 Enabling QoS Collection on a Port

Entuity QoS data is gathered from `Cisco-Class-Based-QOS-MIB.my`, with Entuity QoS polling *QoS Enabled* ports every 15 minutes. All Entuity QoS metrics for which an historical record is kept have their polled values retained and available for reporting on for eight days.

Entuity QoS also delivers extensive real-time performance data, presented by default as rate data, but also available as absolute and delta. This information is securely held with it placed into views within Entuity and access permissions granted based on that view membership according to the standard Entuity security model.

# Simple QoS Example

This QoS example identifies three types of traffic through match statements - telnet, SNMP and ICMP. These named access lists are placed in class maps, in this simple example one access list to each class map. These class maps are built into the traffic profile policy map. This policy map can then be applied to the ethernet interface.

```
!match traffic flows
access-list TELNET permit tcp any eq telnet any
access-list SNMP permit udp any any eq snmp
access-list ICMP permit icmp any any

!Use access-lists to build class maps
class-map match-all icmp-only
  match access-group ICMP
class-map match-all snmp-only
  match access-group SNMP
class-map match-all telnet-only
  match access-group TELNET

!use class maps to build policy map
policy-map traffic-profile
  class telnet-only
  class snmp-only
  class icmp-only

!apply policy map to interface
interface Ethernet0/0
 ip address 192.168.3.34 255.255.255.0
 service-policy input traffic-profile
```

## QoS Components

QoS comprises of four components:

- Traffic identification, enabled through match statements (access-lists).
- Class maps, collections of access-lists.
- Policy maps, collections of paired class-maps and action.
- Service policy, application of policy maps to interfaces. One policy map for the ingress and egress of each interface.

Entuity advise using named access lists, both as best practice and as Entuity QoS does not present the lowest level match statements.

### Traffic Identification through Access Groups

Through access lists devices can classify packets by physical port, source or destination IP address, application port, IP Protocol type, MAC address and so on. Entuity displays access lists:

- Ordering them in the same sequence as they are configured, and therefore the same order as they are applied.
- Pre- and post- policy traffic performance statistics.

✓ Entuity QoS identifies access lists through their access groups, so it is important these groups are given meaningful, descriptive names.

### Traffic Management through Class Maps

Classification and admission control are always performed at the network edge, ensuring traffic conforms to the internal network policy. Packets can be marked with special flags (colors), which are used inside the network for QoS management.

For each class Entuity displays traffic management configuration and pre- and post-policy performance statistics.

### Managing Policy Maps

Policy maps are applied to the interface as service policies. Each interface has a maximum of two service policies, one for inbound traffic, one for outbound. Entuity details the classes associated with the policy map.

### QoS Traffic Policing

Traffic policing allows you to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels or classes of service (CoS).

Using Entuity's Business Views you can monitor the traffic policing configuration on interfaces at the edge of your network. Typically, conforming traffic is transmitted and traffic that exceeds is sent with a decreased priority or dropped.

Through Entuity providing detailed QoS configuration information and extensive statistics on port performance, you can amend the configuration to meet changing network requirements.

## QoS Management

### Managing Congestion through Queues

Queue management is an important congestion tool, for example for avoiding tail drops, where the possibility exists of high priority packets being dropped because they cannot be added to the router’s queue and therefore identified. Queues are associated with classes, one queue per class. A low priority class can be assigned smaller queue depth, high priority classes greater resources reducing the probability of losing high priority packets.

Entuity details both queue configuration and current performance, for example current queue depth and number of discarded packets. You can check queues associated with high priority classes are assigned greater resources, reducing the probability of losing high priority packets, than those associated with lower priority classes.

## Managing Congestion Avoidance

Congestion avoidance can be achieved through packet dropping. Cisco IOS QoS allows Class-Based Weighted Fair Queuing Configuration (CBWFQ) with Weighted Random Early Detection (WRED). Entuity allows you to appropriately modify congestion management through displaying class configuration and its performance, for example:

- Whether explicit congestion notification is enabled for the class, precedence thresholds for the service profiles.
- performance statistics such as number of transmitted packets, tail dropped packets, random packets.

## Monitoring QoS Packet Marking

Packet marking allows you to partition your network into multiple priority levels or classes of service (CoS). QoS Packet Marking can be implemented through:

- Marking packets by setting the IP precedence bits or the IP differentiated services code point (DSCP) in the Type of Service (ToS) byte.
- Associate a QoS group value with a packet.

After setting the IP precedence bits or the IP DSCP, packets are classified by their IP precedence bit or IP DSCP value. These classifications are then used to apply user-defined differentiated QoS services to the packet.

Associating a packet with a QoS group allows users to associate a group ID with a packet. The group ID can be used to classify packets into QoS groups based on prefix, autonomous system, and community string.

A user can assign up to eight IP precedence values, sixty-four IP DSCP markings, and one hundred QoS groups.

Entuity QoS identifies the packet marking method applied on the parent class map and displays its configuration details.

## Managing QoS Traffic Shaping

Traffic shaping attempts to control the volume of traffic sent into a network, and the rate at which the traffic is sent. Therefore traffic shaping is implemented at the network edges, and may involve separating traffic into traffic flows and individually shaping each of these flows, smoothing the peaks and troughs of data transmission.

Entuity QoS can show the separated traffic flows and the individual shaping of each, indicating where the current configuration can be improved to better manage the current traffic.

# 65 QoS Events and Reports

QoS events are managed by Entuity's event manager, which allows the standard customization options, e.g. add annotations, modify threshold levels, event suppression. Default event thresholds are held at the root level, but can be overridden at the individual interface class and queue levels.

All events are generated via polling.

## Entuity QoS Incidents

Entuity QoS incidents are configured through the event project and managed through the event system. You can add annotations, assign incidents to users, close incidents and investigate incident details. Entuity includes a default set of Entuity QoS incidents, details of which are in the *Entuity Events Reference Manual*:

- QoS Bandwidth Problem Incident
- QoS Class Bit Rate High Incident
- QoS Class Drop Bit Rate High Incident
- QoS Class Drop Packet Rate (Buffer Shortage) High Incident
- QoS Queue Drop Bit Rate High Incident.

## Managing QoS Class Events

Entuity monitors traffic management performance through class maps, with events being raised against three metrics:

- high bit rate
- bit drop rate
- drop packet hourly rate (buffer shortage).

By default these events are not enabled. You can enable them and set the threshold level at the Entuity server root level, or against the individual classes associated with an interface.

Identification of what the event is raised against is through the event's data fields.

| Attribute | Description |
|---|---|
| *Source* | The class against which the event is raised, either by Name or IP Address. |
| *Impacted* | The particular interface against which the event is raised. |

Table 66 Managing QoS Class Events

| Attribute | Description |
|---|---|
| *Details* | Identifies the:<br>- correct voltage value, i.e. the rail against which the event is raised,<br>- actual traffic value,<br>- threshold value, where values above that indicate performance problems and Entuity should raise an event. |

Table 66 Managing QoS Class Events

High Bit Rate, High Bit Drop Rate and Drop Packet Rate events are cleared from Event Viewer's Open Events view either after ten minutes have elapsed, or when Entuity raises a Clearing event, i.e. the next poll is within the threshold boundaries.

### Class Thresholds

Setting class thresholds follows the same rules as setting other event thresholds. For example, thresholds can be set at these different levels:

- Global level, i.e. using the Global View on the Entuity server.
- Component level, e.g. selecting a particular component, a class defined against an interface.

The process for setting a class threshold is the same, regardless of the particular metric. These class thresholds are available to set interfaces:

- In *Class Bit Rate High Threshold*, select *Enabled* to turn on the threshold, and accept or amend the default bit rate of 500000. A polled post policy bit rate value greater than this threshold and Entuity raises an QoS Class Bit Rate High.
- In *Class Bit Drop Rate High Threshold*, select *Enabled* to turn on the threshold, and accept or amend the default bit rate of 100000. A polled drop bit rate value greater than this threshold and Entuity raises an QoS Class Drop Bit Rate High.
- In *Class Drop Packet Hourly Rate (Buffer Shortage) High Threshold*, select *Enabled* to turn on the threshold, and accept or amend the default dropped packet rate of 10. A Dropped Packets value greater than this threshold and Entuity raises a QoS Class Drop Packet Hourly Rate (Buffer Shortage) High.

## Managing the Queue Event

Entuity monitors interface congestion, which is managed through defining queues for different classes of traffic.

By default the Qos Queue event is not enabled. You can enable it and set the threshold level at the Entuity server root level, or against the individual queues associated with an interface's classes.

Identification of what the event is raised against is through the event's data fields.

| Attribute | Description |
|---|---|
| *Source* | The queue against which the event is raised, either by Name or IP Address. |
| *Impacted* | The particular interface class against which the event is raised. |
| *Details* | The queue performance and its thresholds. |

Table 67 Managing the Queue Event

High Class Queue Bit Drop Rate event is cleared from Event Viewer’s Open Events view either after ten minutes have elapsed, or when Entuity raises a Clearing event, i.e. the next poll is within the threshold boundaries.

## Queue Thresholds

Setting the queue thresholds follows the same rules as setting other event thresholds. For example, thresholds can be set at these different levels:

- Global level, i.e. using the Global View on the Entuity server.
- Component level, e.g. selecting a particular component, a queue defined against an interface’s class.

To set the queue threshold in *Queue Bit Drop Rate High Threshold*, select *Enabled* to turn on the threshold, and accept or amend the default bit rate of 100000. When number of packets dropped by the router when traffic exceeds *Max Queue Depth* is greater than this threshold, Entuity raises an QoS Class Drop Packet Rate (Buffer Shortage) High.

# 66 Manage and Monitor Network Device Configuration

The Entuity Configuration Management module adds configuration monitor and management functions to Entuity. Entuity can retrieve and archive network device configurations, detect, alert and report on changes to both running and saved configurations.

## Entuity Configuration Monitor Functionality

When you are an administrator or a user with the Configuration Monitor tool permission you can use Entuity Configuration Management to:

- Retrieve and archive device configuration files. You can initiate a configuration retrieval from the web UI, schedule a retrieval or configure a retrieval to occur when there is a detected change in the startup or running device configuration files.
- Alert to changes in device configuration files.
- Alert to changes to firmware versions and the automatic retrieval of device configuration.
- Warn of unsaved changes in device configuration files.
- Enable detailed comparison of device configuration files.
- Allow you to identify trivial changes in device configuration files which Entuity Configuration Monitor can exclude when identifying differences between files.
- Check device configuration files for best practice. You can define different mandated policy statements, Entuity Configuration Monitor associates them to devices by matching them on their sysOID.
- Access devices using Telnet and SSH.
- Transport device configurations using FTP, TFTP, SCP and RCP protocols.
- Integrate with Entuity's permissions system.
- Track configuration performance through Entuity interface, e.g. configurable, events raised in its web UI, reports available.
- Integrate with Entuity reports and includes Entuity Configuration Monitor module reports.
- View archived configuration files.
- Manage device configuration from the command line and through the Entuity RESTful API. You can use `RESTful API ConfigManagement` to apply configuration management settings for the specified target device(s).

## Entuity Configuration Management Module

Entuity Configuration Management is included with all standard Entuity installations, but it is not activated by default. Activation requires a valid Entuity license and inclusion of Entuity Configuration Management during `configure`.

## Module Licensing

Entuity components are licensed by type. To run the full Entuity Configuration Management module the license must include the Entuity Configuration Management type. (See the *Entuity Getting Started Guide*.)

When Entuity Configuration Management is disabled, none of the features are visible to the end user; however, any configuration files archived during a previous licensed run of Entuity Configuration Management are retained on the file system.

Device configuration files are owned by Entuity and protected by the permissions system of the operating system. You can access these files outside of Entuity Configuration Management with a user account that has the necessary permissions.

## Module Availability

The Entuity Configuration Management module is available with Entuity in all supported environments. (For details on Entuity's technical specification see the *Entuity Getting Started Guide*.)

## Module Security

Retrieved configuration details are associated with their device in Entuity, so access permissions are granted based on that view membership according to the standard Entuity security model.

The current and archived files are saved to the Entuity server, with access to those folders outside of Entuity controlled by the operating system permissions.

## Remote and Transport Protocols

Entuity Configuration Management can use Telnet and Secure Shell (SSHv1 and SSHv2) to access devices for monitoring their configuration. All required executables are included in the package and preinstalled in the appropriate location. No additional installation steps are required to use either Telnet or SSH.

Entuity Configuration Management can use FTP, TFTP, SCP and RCP servers for the retrieval of configuration files. For configuration retrieval to work the specified transfer server type must be running on the Entuity server.

## User Group Tools and Permissions

Users that are members of a user group with:

- Configuration Monitor access can view and set all parameters including the list of devices to monitor, the frequency of monitoring, the number of files to archive as well as ignore patterns and policy patterns.
- Configuration Management access can set up configuration management tasks and steps.

Users that are not members of user groups with either configuration tool permission can:

- View configuration events in Event Viewer, but cannot navigate from there to view the underlying device configuration.

- Have permissions assigned for each individual Configuration Management task.

### Permissions in Multi-Server Deployment

The Configuration Management module is checked for on the Entuity server on which the user is logged in to (e.g. the central server, in the case on a multi-server deployment). However, the tool permission are checked against the Entuity server where the associated device/view is being managed (which may be a remote server). Furthermore, if a remote server does not have the module enabled, then Entuity considers the permission as disabled on that serve for all users.

### Device Configuration Retrieval

Entuity Configuration Management can attempt device configuration retrieval for a device:

- Entuity is managing, regardless of its management level, e.g. Full, Ping Only, Basic.
- For which there is a retrieval script file associated either with its device or vendor sysOid. Full Entuity Configuration Management functionality is only available if there are also mapped policy and exclusion files.

### Command Line and Automated Configuration Retrieval

From Entuity you can apply configuration changes to the selected device. You can also use the RESTful API to apply configuration management settings to one or more specified devices. You can use RESTful API within scripts to automate the management of device configuration retrieval. (See the *Entuity System Administrator Reference Manual*.)

## Setting Up Entuity Configuration Management

Before you activate Entuity Configuration Management read this user documentation and prepare your mandated policy statements and exclude pattern files. Entuity provide sample versions of both types of file, but it is likely that they will require customisation. When you customize a file you should rename it, otherwise Entuity upgrades would overwrite your changes. You can also specify additional files for use with other manufacturer’s devices or for specific device models (as defined by their sysOID).

Entuity Configuration Management requires:

- An appropriate Entuity license.
- Available remote shell protocols, for example Telnet and Secure Shell (SSHv1 and SSHv2). You would require device login credentials.
- A running transfer server, i.e. FTP, TFTP, SCP or RCP server.
- Activation of configuration monitoring on required devices.

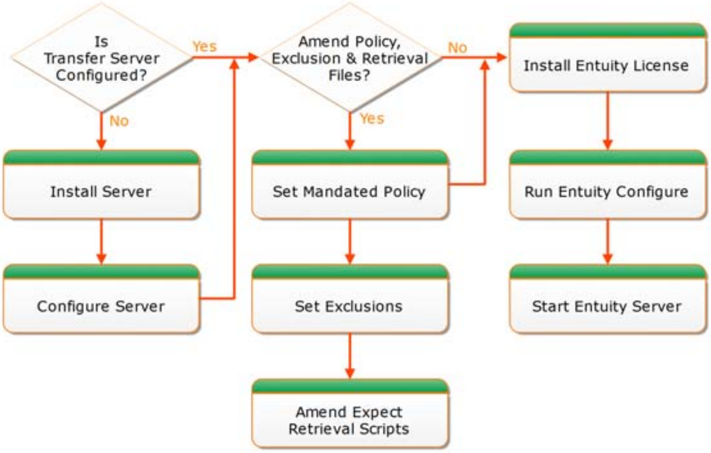


Figure 376 Install and Configure Entuity Configuration Management

## Example Entuity Configuration Management Installation

This example provides an overview of an Entuity Configuration Management installation using the:

- Provided TFTP server.
- Sample policy, exclusion and retrieval files.

To set up Entuity Configuration Management with its sample configuration:

1) Configure and start the TFTP server.

   The transfer directory you specify here must be the same as set during `configure`.

2) Accept the sample setup of the mandated policy, exclusion and retrieval script files.

   In practice it is likely that you would want to amend the supplied files, in which case you should rename them to prevent them being overwritten during Entuity upgrades, and/or create your own.

3) Ensure you have an Entuity license with the Entuity Configuration Management module enabled and then run `configure`.

   You should set the transfer directory to the same directory as specified for the TFTP server.

4) Start Entuity.

   To activate configuration management you:

   - Must wait for Entuity `discovery` to complete one cycle, only then is Entuity Configuration Management fully available.

- Can initiate a configuration retrieval from the web UI, schedule a retrieval or configure a retrieval to occur when there is a change in the startup or running configuration files.

5) For each device you can:
   - Assign CLI credentials. These credentials are used when Entuity Configuration Management initiates the command line access with the device, using Telnet or SSH.
   - Associate configuration management tasks.

## Activating Entuity Configuration Management

You include to Entuity the Entuity Configuration Management module by running `configure`. You must also acquire and install an appropriate license.

Activation of the Entuity Configuration Management is only one part of enabling the module. It is important to consider developing tasks, customizing associated configuration files, device access and transfer servers.

To activate the Entuity Configuration Management module:

1) Acquire a valid license from your Entuity representative. Add the new license file to *entuity_home*`\etc`, the default location.

2) Stop the Entuity server.

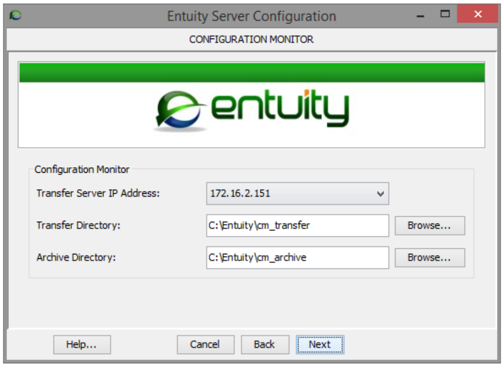
3) Run `configure`, and from the Module Select page enable Configuration Management.

   Only when you have activated the Entuity Configuration Management module does `configure` display its configuration page. Configure the module.

| Attribute | Description |
|---|---|
| *Server IP Address* | The IP address of the Entuity server used for the transfer of device configuration. Where the server has more than one address, for example it has IPv4 and IPv6 addresses, you can select the required address from the drop-down list. |
| *Transfer Directory* | The initial location for the retrieved configuration files, by default *entuity_home*`\cm_transfer`. Retrieved configurations are placed here before they are moved to the Archive directory.<br>The transfer directory should be the same as the home directory specified, for example in the TFTP server initialization file. |
| *Archive Directory* | The location for the archived configuration files, by default *entuity_home*`\cm_archive`. |

Table 68 Entuity Configuration Management Configure Attributes

4) Once you have specified Entuity Configuration Management click **Next**.



Configuration Monitor

Transfer Server IP Address: 172.16.2.151

Transfer Directory: C:\Entuity\cm_transfer Browse...

Archive Directory: C:\Entuity\cm_archive Browse...

Figure 377 Entuity Configuration Management Configuration

5) Start the Entuity server.

# 67 Prepare Configuration Management Files

Before using Entuity Configuration Management to monitor network device configurations you should amend its policy and pattern matching behavior to meet your requirements. Set up policy and pattern matching through:

- Generic exclusions files. These specify text patterns that Entuity Configuration Management can safely ignore when trying to identify important configuration changes, e.g. timestamp changes. Entuity Configuration Management includes example generic exclusions files, e.g. `cisco-generic-exclusions.cfg`.
- Policy files. These specify configuration lines that good and bad practice configurations should conform to. So, a device configuration that does not include a configuration setting defined in the include section of its associated policy file would cause Entuity Configuration Management to raise a CM Configuration Missing Policy Mandated Statement event.

  Entuity supply example generic policy files for Cisco, HP and Juniper devices. You can amend their content to meet your requirements. (See *Appendix G - Entuity Configuration Management Files*.)

When amending exclusion and policy files you should also rename them to ensure your changes are not overwritten during your next Entuity upgrade.

It is through a device's Configuration page that you can view and change the default associations of exclusion and policy. Each time Entuity Configuration Management performs an ignore pattern or policy violation check, it references these files (or rather their representation in the Entuity database). Changes to rules in these exclusion and policy files impact Entuity Configuration Management behavior after the next discovery cycle.

## Identifying Device Configuration Change

When you retrieve device configuration information, Entuity Configuration Management compares the retrieved file with the previously retrieved file. To avoid flagging trivial changes in the configuration file, e.g. timestamp changes, Entuity Configuration Management includes an ignore pattern matching function.

Through exclusion files that define patterns to ignore, for example `cisco-generic-exclusions.cfg`, you can specify default patterns that Entuity Configuration Management must ignore. (See *Appendix G - Entuity Configuration Management Files*.)

The pattern matching file is parsed when saved to the device. It takes one discovery cycle for changes to be included to Entuity. The patterns are stored in the Entuity database, although updates must be amended in the pattern matching file.

Different configuration changes made to any line or group of lines that match one of the ignore patterns are not be considered a change to the configuration file being analyzed. Entuity Configuration Management considers these changes as trivial.

Where the only differences between a newly retrieved configuration file and the last archived one are trivial, the newly retrieved file is treated as though it were an exact copy of the archived one and discarded. Entuity does not raise a change event.

The pattern matching rules are global and applied to both network device startup configurations and running configurations.

## Identifying Policy Violations

From the Configuration page you can configure Entuity Configuration Management to check configuration files for policy violations. Policy checking is on a per device basis.

Entuity Configuration Monitor includes example policy files for these device types, Cisco, HP, Juniper. You can amend these files, you can also create new files. Policy violations are identified through two sections in the file:

- Include patterns, which identifies patterns that must be included to a configuration file.
- Exclude patterns, which identifies patterns that must be excluded from a configuration file.

You amend policy files through a text editor, external to Entuity.

When Entuity Configuration Management identifies policy violations it can invoke Policy Violation events. Each policy definition includes a policy name, and when violated the policy name is included in the policy violation event.

When the policy violation is of a device configuration file missing a pattern defined in the:

- Must include section, Entuity Configuration Management alerts the user through a CM Configuration Violation Missing Policy Mandated Statement event. Entuity Configuration Management raises the event on the first match of a particular violation.
- Must exclude file, Entuity Configuration Management raises a CM Configuration Include Policy Exclusion event.

Policy Violation Events have configurable expiry times. They also have corresponding clearing events raised when the configuration is found to have been edited to fix the violation.

# 68 Set and Run Transfer Servers

The initial communication between Entuity and a device is through Telnet, and SSH using a command line access credential set specified in Entuity. All required executables are included in the package and installed in the appropriate location. No additional installation steps are required. However, configuration retrieval is through a separate transfer mechanism, using FTP, SCP, RCP or TFTP. The mechanism details are specified through a Step definition in the task.

The Entuity server must be running the transfer server and a device must have the credentials to access that server. You can use multiple types of transport servers at the same time, they must also use the same transfer directory. This directory must also be the same as that set during `configure`.

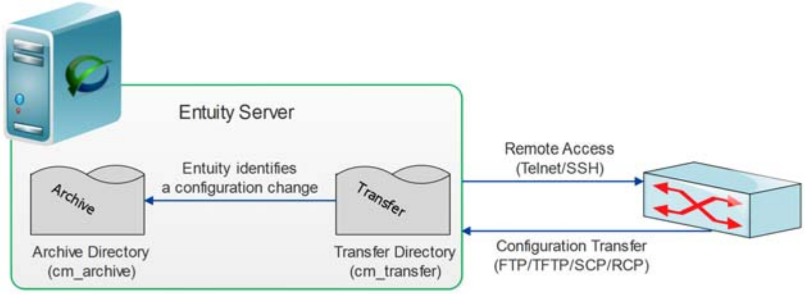

Entuity Server
Entuity identifies a configuration change
Archive
Transfer
Archive Directory (cm_archive)
Transfer Directory (cm_transfer)
Remote Access (Telnet/SSH)
Configuration Transfer (FTP/TFTP/SCP/RCP)

Figure 378 Transfer and Archive Configuration Files

Entuity recommend devices monitored by Entuity Configuration Management are configured with encrypted passwords. Files are transferred in clear text.

## Retrieving Configurations with TFTP Servers

Before you can use Entuity Configuration Management a transfer server must be configured and running. Entuity Configuration Management can be used with the leading TFTP servers.

In Linux environments consult with your system administrator on a suitable TFTP server. In Windows environments the Entuity ISO image includes a suitable open source TFTP server, OpenTFTPServer. OpenTFTPServer is not installed by Entuity `configure` (see *Appendix F - TFTP Server Configuration*).

TFTP does not have an authentication mechanism, and the configuration files require global read and write permissions. Placing the TFTP root directory under the web root is a security risk and Entuity advise against doing this.

The open source TFTP server included with the Entuity installation is also available from `http://sourceforge.net/projects/tftp-server/`. You can use other TFTP servers. In either case always consult the TFTP server documentation.

## Setting Up OpenTFTPServer

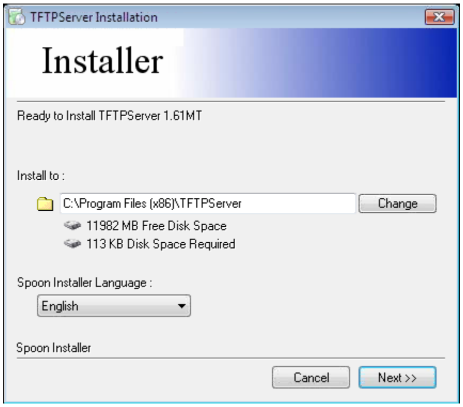
To set up the supplied TFTP server on a Windows server:

1) Install the TFTP server to the same machine as the Entuity server.

   From *entuity_home*`\integ\TFTPServer` double-click on `TFTPServerMTInstallerv1.61.exe`.

2) Through the wizard specify the location of the TFTP server and click **Next**.

   The Installer displays the GNU General Public License.



TFTPServer Installation

Installer

Ready to Install TFTPServer 1.61MT

Install to : C:\Program Files (x86)\TFTPServer

11982 MB Free Disk Space

113 KB Disk Space Required

Spoon Installer Language : English

Figure 379 Install TFTP Server

3) Click **Next** to accept the license terms and install the server. The installer displays the install complete dialog.

4) Configure the TFTP server.

   Navigate to the TFTP server folder and edit `TFTPServerMT.ini`. In the:

   - `[HOME]` section, set the directory to which the TFTP server does the initial saving of the configuration file. This must be the same as the *Transfer Directory* defined through `configure`, for example `c:\entuity\cm_transfer`. When not set the TFTP server writes these files to the same folder as the TFTP server executable.
   - `[TFTP-OPTIONS]` section set the file operation permissions to allow writing to these folders.

   For more details see *Appendix F - TFTP Server Configuration*.

# Setting up an FTP Server

Entuity Configuration Management does not include an FTP server, but would work with the leading FTP servers, e.g. Microsoft IIS FTP (Windows), vsftpd (Linux). When using an FTP server it must be configured to place device configurations in the same transfer directory as specified during `configure`. The FTP server must have full access rights to the directory.

When you have a running FTP server on the Entuity server machine, you must ensure each device from which you want to retrieve its configuration can access the FTP server.

## Preconfiguring Cisco Devices for FTP Access

Before you can use FTP on devices that require command line delivery of credentials you must configure the device. For example:

```
R837#config terminal
R837(config)#ip ftp username EYEAccess
R837(config)#ip ftp password EYEPassword
R837(config)#end
```

## Managing FTP Access to Non-Cisco Devices

FTP server credentials are specified through the lcm section of `entuity.cfg`, and apply to non-Cisco devices. The default settings are:

```
[lcm]
FTPUsername=EYEAccess
FTPPassword=EYEPassword
```

where:

- *[lcm]* is the section name.
- *FTPUsername* identifies the FTP server account, by default **anonymous.**
- *FTPPassword* identifies the account password, by default **EYE**.

# Running Transfer Servers

Although Entuity Configuration Management is configured to work with the specified transfer server it does not check that the server is running when attempting a retrieval. If the server is not running the retrieval fails and Entuity raises a CM Running Configuration Retrieval Failed and CM Startup Configuration Retrieval Failed events.

The Entuity server must also support the mechanism used to access the device, e.g. Telnet, SSH.

## Running OpenTFTPServer

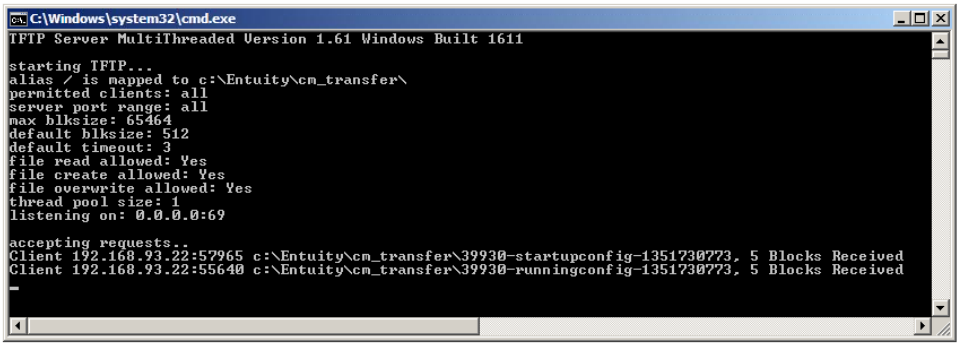
You can install and run OpenTFTPServer as a standalone process or as a service:

- When first installing and testing Entuity Configuration Management you may want to run OpenTFTPServer as a standalone process to easily view its command line information and error messages.
- In a production environment running OpenTFTPServer as a service ensures it runs when Entuity runs, for example that it is available after restarting the server machine.

To run OpenTFTPServer as a standalone process:

1) From `\Program Files (86)\TFTPServer\RunStandaloneMT.bat`.

   OpenTFTPServer displays a summary of its configuration and its state of accepting requests. OpenTFTPServer also displays the receiving of configuration files.



```
TFTP Server MultiThreaded Version 1.61 Windows Built 1611

starting TFTP...
alias / is mapped to c:\Entuity\cm_transfer\
permitted clients: all
server port range: all
max blksize: 65464
default blksize: 512
default timeout: 3
file read allowed: Yes
file create allowed: Yes
file overwrite allowed: Yes
thread pool size: 1
listening on: 0.0.0.0:69

accepting requests..
Client 192.168.93.22:57965 c:\Entuity\cm_transfer\39930-startupconfig-1351730773, 5 Blocks Received
Client 192.168.93.22:55640 c:\Entuity\cm_transfer\39930-runningconfig-1351730773, 5 Blocks Received
_
```

Figure 380 Run OpenTFTPServer

# 69 Device Configuration Retrieval

Entuity Configuration Management allows you to schedule, or manually, retrieve device configurations. You can access a device's Configuration page to see the status of configuration retrieval, initiate retrievals and view and manage retrieved configuration files for that device.

Management and user functionality is available from the Configuration page of the device:

- It provides access to the management functions of configuration monitoring. For example setting up the transfer method, setting the policy rules, configuring retrieval schedules.
- Allows you to view and compare archived configuration files, identify their name and paths allowing you to access them using third party tools, and initiate manual retrieval of device configuration files.

## Discovery and Configuring Device Configuration

Entuity Configuration Monitor retrieves and interprets device configuration files through three types of configuration:

- Retrieval task
- Exclude differences
- Policy rules.

Entuity associates device and vendor sysOids to the appropriate retrieval script, excluded differences and policy rule files, e.g.:

```
cisco-generic-exclusions.cfg(.1.3.6.1.4.1.9)
.
.
cisco-generic-policies.cfg(.1.3.6.1.4.1.9)
hp-generic-policies.cfg(.1.3.6.1.4.1.11)
```

Devices that support configuration retrieval are then discovered as part of Entuity's standard discovery process.

Entuity first attempts to match on the specific device sysOID, and if that fails on a vendor sysOID and if that fails a configuration file is not associated with the device. Through Entuity you can amend the default association although care must be taken to avoid making an invalid association.

Entuity Configuration Management cannot immediately retrieve device configuration after discovery has run:

- You must set CLI credentials for each device.
- Changed based retrieval is enabled by default, but you may also want to enable Nightly Retrieval.

- You can amend default values associated against the device’s configuration monitor attributes, for example, number of archive files.

| Attribute | Description |
|---|---|
| *Transfer Method* | Select from TFTP, FTP, SCP and RCP. |
| *Retrieval Task* | The task used to retrieve configuration from the device. |
| *Exclude File* | This file identifies patterns of configuration Entuity Configuration Monitor can safely ignore when identifying non-trivial changes in the device’s configuration. |
| *Policy Rules* | This file specifies good and bad configuration which a device’s configuration should, respectively include and exclude. |
| *Nightly Retrieval* | By default set to **Off**, but when set to **On** it enables scheduled retrieval. Each night at 02:00 Entuity retrieves configuration files from the first device, and then at one minute intervals initiates configuration retrieval for each device with this setting enabled,<br>Scheduled and change-based (timestamp) initiated configuration retrievals are independent of this process, although Entuity would not activate a configuration retrieval when one is already underway. |
| *Changed Based Retrieval* | When set to **On** (default) it allows Entuity to check, by default every five minutes, for changes in either the startup or running configuration files timestamp. A change in a timestamp indicates a change in the device configuration. Entuity does not immediately initiate configuration retrieval as the configuration may still be being edited. Entuity continues to poll the device and when the timestamp remains unchanged for two consecutive polls then Entuity waits a set period checks the timestamp from the latest poll and if that remains unchanged then initiates retrieval of the configuration.<br>Scheduled and user initiated configuration retrievals are independent of this process, although Entuity would not activate a configuration retrieval when one is already underway. |
| *Number of Archives* | The number of versions of the device configuration files in the Archive folder. There is a separate count for startup and running configuration files. The default is four. |

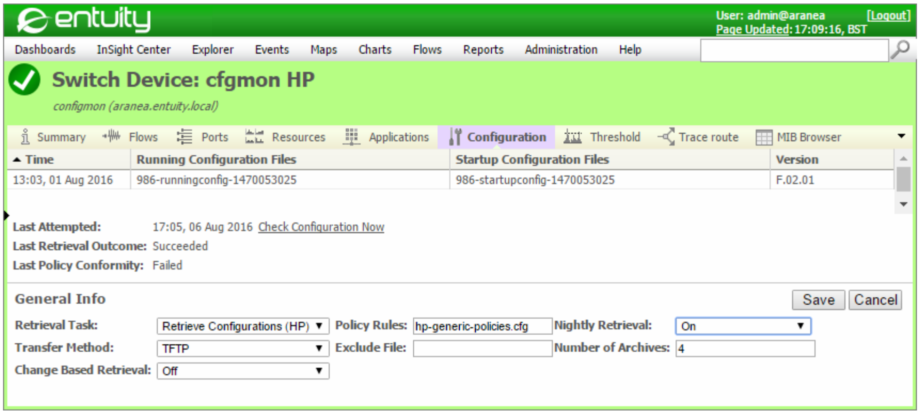
Table 69 Configuration Retrieval Setup

To configure device configuration retrieval settings:

1) From the Explorer tree highlight the device and click the Configuration tab.

2) Click **Edit**.

3) Amend the configuration settings and click **Save**.


entuity
User: admin@aranea [Logout]
Page Updated: 17:09:16, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
Summary Flows Ports Resources Applications Configuration Threshold Trace route MIB Browser
Save Cancel

Switch Device: cfgmon HP

configmon (aranea.entuity.local)

| Time | Running Configuration Files | Startup Configuration Files | Version |
|---|---|---|---|
| 13:03, 01 Aug 2016 | 986-runningconfig-1470053025 | 986-startupconfig-1470053025 | F.02.01 |

Last Attempted: 17:05, 06 Aug 2016 Check Configuration Now
Last Retrieval Outcome: Succeeded
Last Policy Conformity: Failed

General Info

Retrieval Task: Retrieve Configurations (HP)
Transfer Method: TFTP
Change Based Retrieval: Off
Policy Rules: hp-generic-policies.cfg
Exclude File:
Nightly Retrieval: On
Number of Archives: 4

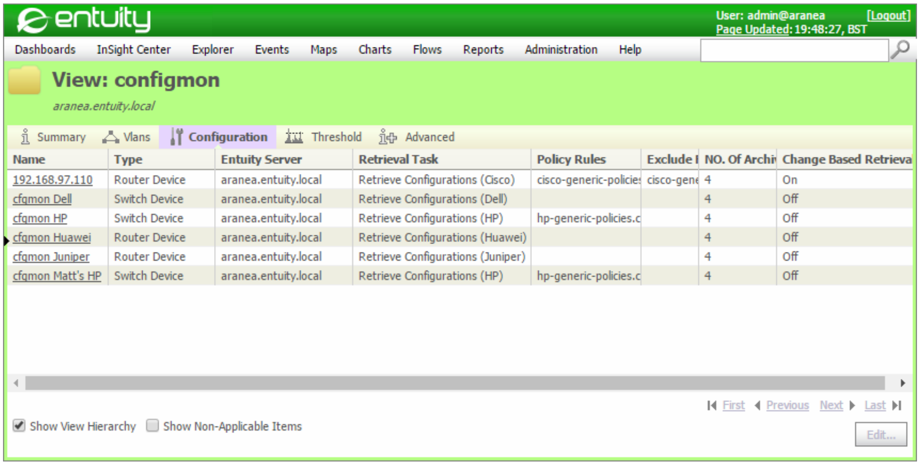
Figure 381 Set up Device Configuration Retrieval

# Device Configuration by View

To view a summary of the configuration management setup of devices in a view:

1) From the Explorer tree select the view and click the Configuration tab.

Each row in the column details the configuration management setup of a device.


entuity
User: admin@aranea [Logout]
Page Updated: 19:48:27, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
Summary Vlans Configuration Threshold Advanced
First Previous Next Last
Edit...

View: configmon

aranea.entuity.local

| Name | Type | Entuity Server | Retrieval Task | Policy Rules | Exclude I | NO. Of Archi | Change Based Retrieva |
|---|---|---|---|---|---|---|---|
| 192.168.97.110 | Router Device | aranea.entuity.local | Retrieve Configurations (Cisco) | cisco-generic-policies | cisco-gene | 4 | On |
| cfgmon Dell | Switch Device | aranea.entuity.local | Retrieve Configurations (Dell) | | | 4 | Off |
| cfgmon HP | Switch Device | aranea.entuity.local | Retrieve Configurations (HP) | hp-generic-policies.c | | 4 | Off |
| cfgmon Huawei | Router Device | aranea.entuity.local | Retrieve Configurations (Huawei) | | | 4 | Off |
| cfgmon Juniper | Router Device | aranea.entuity.local | Retrieve Configurations (Juniper) | | | 4 | Off |
| cfgmon Matt's HP | Switch Device | aranea.entuity.local | Retrieve Configurations (HP) | hp-generic-policies.c | | 4 | Off |

☑ Show View Hierarchy □ Show Non-Applicable Items

Figure 382 Device Configuration Summary by View

| Attribute | Description |
|---|---|
| *Name* | Display name of the device and a hyperlink to its Explorer Summary tab. |

Table 69-1Summary of Configuration Settings for Devices in a View

| Attribute | Description |
|---|---|
| *Type* | Device type. |
| *Entuity Server* | Entuity server running the configuration management task. |
| *Retrieval Task* | Name of the retrieval task. |
| *Policy Rules* | Name of the policy rules file applied by the task to the retrieved configurations. |
| *Nightly Retrieval* | By default set to **Off**, but when set to **On** it enables scheduled retrieval. Each night at 02:00 Entuity retrieves configuration files from the first device, and then at one minute intervals initiates configuration retrieval for each device with this setting enabled |
| *Transfer Method* | Transfer method used by the task, i.e. TFTP, FTP, SCP or RCP. |
| *Exclude File* | Name of the exclude file applied by the task to retrieved configurations. |
| *No. of Archives* | The number of versions of the device configuration files in the Archive folder. There is a separate count for startup and running configuration files. The default is four |
| *Change Based Retrieval* | When set to **On** (default) it allows Entuity to check, by default every five minutes, for changes in either the startup or running configuration files timestamp. |

Table 69-1Summary of Configuration Settings for Devices in a View

## Retrieving and Archiving Device Configurations

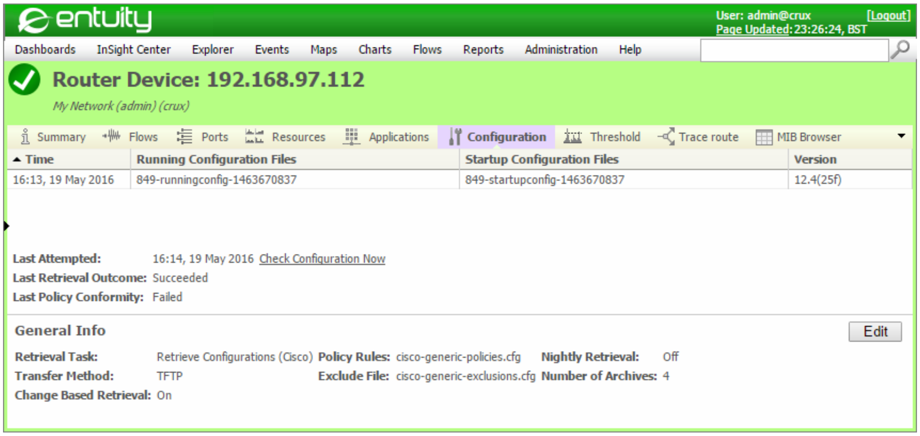
Entuity Configuration Management can retrieve the running and startup configuration files of devices managed by Entuity and for which Entuity has the appropriate CLI credential set, including authorization to use the transfer server.

Entuity Configuration Management provides three mechanisms through which you can retrieve device configuration:

- Manual retrieval, where you can select a device through the web UI and initiate a configuration check.
- Scheduled retrieval, where you can schedule a daily configuration check of a device.
- Change-based retrieval, where you configure a configuration retrieval when Entuity identifies a change in the timestamp of the running or startup configuration files of a device.

Change-based, scheduled and user initiated configuration retrievals are independent of each other, although Entuity would not activate a configuration retrieval when one is already underway.

You can check the current status of scheduled and change base retrieval through the Explorer Configuration tab, from which you can also initiate a manual retrieval.


entuity
User: admin@crux [Logout]
Page Updated: 23:26:24, BST
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
Summary Flows Ports Resources Applications Configuration Threshold Trace route MIB Browser
Edit

Router Device: 192.168.97.112

My Network (admin) (crux)

| Time | Running Configuration Files | Startup Configuration Files | Version |
|---|---|---|---|
| 16:13, 19 May 2016 | 849-runningconfig-1463670837 | 849-startupconfig-1463670837 | 12.4(25f) |

Last Attempted: 16:14, 19 May 2016 Check Configuration Now
Last Retrieval Outcome: Succeeded
Last Policy Conformity: Failed

General Info

Retrieval Task: Retrieve Configurations (Cisco)
Transfer Method: TFTP
Change Based Retrieval: On
Policy Rules: cisco-generic-policies.cfg
Exclude File: cisco-generic-exclusions.cfg
Nightly Retrieval: Off
Number of Archives: 4

Figure 383 Archived Configuration Files

Entuity Configuration Management only archives retrieved configurations that indicate configuration change.

| Attribute | Description |
|---|---|
| *Timestamp* | Data and time the configuration was retrieved. |
| *Running Configuration Files* | Name of the archive file derived from StormWorks identifier of the device, the configuration file type and a unique number, for example: `66-runningconfig-1194533283` |
| *Startup Configuration Files* | Name of the archive file derived from StormWorks identifier of the device, the configuration file type and a unique number: `66-startupconfig-1194533329` |
| *Version* | Software version running on the device. |

Table 70 Archived Configuration Files

## Scheduled Device Configuration Retrieval

By default, Entuity Configuration Management does not activate scheduled retrieval of device configuration. When it is enabled, Entuity Configuration Management retrieves configuration files daily at 02.00. Entuity Configuration Management creates a queue and then, at one minute intervals, retrieves the configuration files from each monitored device in turn.

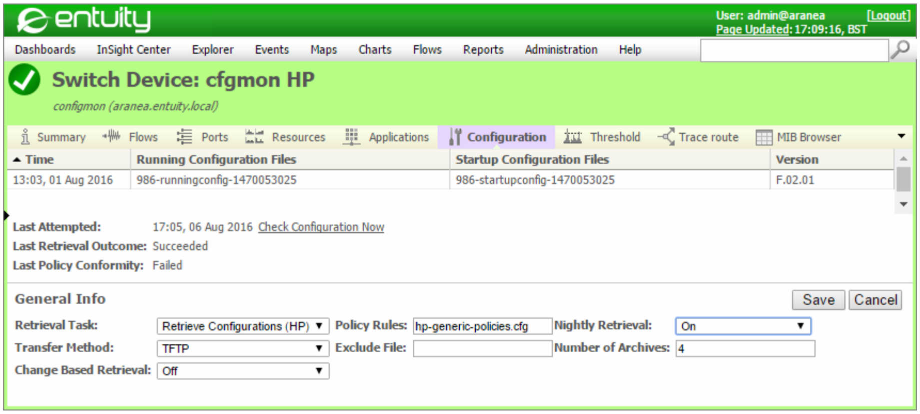
To activate scheduled device configuration:

1) Through Explorer navigate to the device’s Configuration tab.

   If the tab is not visible you can extend the browser window or select a tab by clicking the tab down arrow and selecting Configuration from the drop-down list.

2) Click **Edit**.

3) Set *Nightly Retrieval* to **On**.



Switch Device: cfgmon HP

cfgmon (aranea.entuity.local)

| Time | Running Configuration Files | Startup Configuration Files | Version |
|---|---|---|---|
| 13:03, 01 Aug 2016 | 986-runningconfig-1470053025 | 986-startupconfig-1470053025 | F.02.01 |

Last Attempted: 17:05, 06 Aug 2016 Check Configuration Now
Last Retrieval Outcome: Succeeded
Last Policy Conformity: Failed

General Info

Retrieval Task: Retrieve Configurations (HP)
Policy Rules: hp-generic-policies.cfg
Nightly Retrieval: On
Transfer Method: TFTP
Exclude File:
Number of Archives: 4
Change Based Retrieval: Off

Figure 384 Nightly Retrieval

## Change-Based Device Configuration Retrieval

You can configure Entuity to check, by default every five minutes, for changes in either the startup or running configuration files' timestamps. A change in the timestamp indicates a change in the device configuration. After identifying a timestamp change:

1) Entuity waits until two consecutive polls return unchanged timestamps.
2) Entuity then waits a set period as defined through *lcm.SNMPTriggerHoldOffTime* in `entuity.cfg`.
3) After the hold time elapses Entuity Configuration Management checks the latest poll of the device. If the timestamp remains unchanged, which indicates updates to the configuration are complete, Entuity then initiates a configuration retrieval.

To activate change-based device configuration:

1) Through Explorer navigate to the device's Configuration tab.

   If the tab is not visible you can extend the browser window or select a tab by clicking the tab down arrow and selecting Configuration from the drop-down list.

2) Set *Changed Base Retrieval* to **On**.

## Manual Device Configuration Retrieval

When Entuity Configuration Management successfully retrieves configuration files it can:

- Check for configuration changes.
- Check for policy violations.
- Archive or discard the configuration files.
- Raise events when appropriate.

If retrieval of configuration files fails, Entuity raises a Configuration Retrieval Failed event in Event Viewer.

To manually retrieve device configuration files:

1) From the web UI Explorer select the device.
2) Click **Configuration** .
3) In the Archived Configurations section click **Check Configuration Now**.

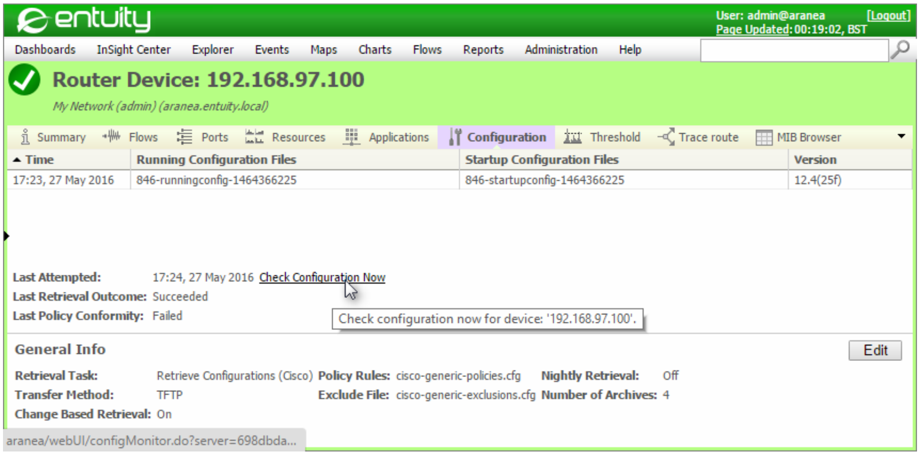
   Entuity initiates device configuration retrieval and displays an information dialog. This dialog informs you as to whether the action was successfully initiated or not, it does not imply the configuration retrieval request was successful.
4) Click **Close** to close the dialog. The retrieval request may take a couple of minutes.

When the configuration check:

- Fails, Entuity raises an appropriate event in Event Viewer.

  In the device Configuration page *Last Attempted* displays the time of the failed retrieval attempt and *Last Retrieval Outcome* is set to **Failed**. From the Configuration Management History page you can drill down to view the Diagnostic Data and debug the full conversation details between the Entuity server and the target device.
- Succeeds and identifies a configuration change, Entuity raises an appropriate event in Event Viewer.
- Succeeds but does not identify a configuration change, Entuity updates *Last Attempted* and *Last Outcome* to the time of the retrieval and to **Succeeded**, respectively.

When the retrieval successfully completes Entuity Configuration Management only archives the files if they include a non-trivial change when compared to the previously archived files. Newly archived files appear as a new row in the device’s Web UI Archived Configuration Files table.



Router Device: 192.168.97.100

My Network (admin) (aranea.entuity.local)

| Time | Running Configuration Files | Startup Configuration Files | Version |
|---|---|---|---|
| 17:23, 27 May 2016 | 846-runningconfig-1464366225 | 846-startupconfig-1464366225 | 12.4(25f) |

Last Attempted: 17:24, 27 May 2016 Check Configuration Now
Last Retrieval Outcome: Succeeded
Last Policy Conformity: Failed

Check configuration now for device: '192.168.97.100'.

General Info

Retrieval Task: Retrieve Configurations (Cisco) Policy Rules: cisco-generic-policies.cfg Nightly Retrieval: Off
Transfer Method: TFTP Exclude File: cisco-generic-exclusions.cfg Number of Archives: 4
Change Based Retrieval: On

aranea/webUI/configMonitor.do?server=698dbda...

Figure 385 Check Configuration Now

## How Retrieved Configuration Files Are Archived

When Entuity Configuration Management retrieves configuration files it checks against the last archived configuration files for that device for:

- Significant changes. These are specified by regular expressions in the exclusions file. By default changes to the "! Last configuration change at " and "ntp clock-period " lines are ignored although this can be overruled by changing the ignore patterns file.
- Policy violations, specified in the policy file.

Device configuration files that:

- Do not include policy violations, or significant changes, are discarded.
- Include significant changes are archived, and events may be raised.

By default Entuity Configuration Management retains a maximum of four archived configuration versions, including the current configuration. You can amend this number, setting it to a value between one and ten.

Entuity automatically monitors free disk space on the management station as part of its standard functionality. All archived configuration files include a timestamp.

Entuity Configuration Monitor uses this structure when determining where to store the files containing retrieved configuration:

```
$ARCHIVEDIR/$DEVICE_ID/$CONFIG_TYPE/$CONFIG_FILE
```

| Attribute | Description |
|---|---|
| $ARCHIVEDIR | Directory chosen for the archives during ***Configure.*** |

Table 71 Configuration Structure

| Attribute | Description |
|---|---|
| $DEVICE_ID | Numeric StormWorks identifier. Each device's identifier is available on its web UI Advanced Details page. |
| $CONFIG_TYPE | Either running or startup |
| $CONFIG_FILE | The file itself. |

Table 71 Configuration Structure

A configuration file has the format:

```
$DEVICE_ID_$CONFIG_TYPE_$TIMESTAMP
```

where $TIMESTAMP is the time configuration was triggered.

### Setting the Number of Archived Device Configuration Files

By default Entuity Configuration Management archives for each device the last four versions of its combined startup and running configurations. You can amend this number, on a per device basis:

1) From the Explorer tree highlight the device and click the Configuration tab.

2) Click **Edit**.

3) Amend the *Number of Archives* value.

You can check the current number of archive files through the device Configuration panel in the web UI.

### Handling Failures in Configuration Retrieval

If a device signals an error condition during an attempted configuration check, Entuity Configuration Monitor raises CM Startup Configuration Retrieval Failed and CM Running Configuration Retrieval Failed incidents and event. The details string identifies the device and the configuration file.

If the retrieval failure is a symptom of other problems with the network or the device itself, other components of Entuity should alert the user to the probable cause.

## Viewing Configuration Changes

Entuity Configuration Monitor allows you to open and compare the results of configuration retrieval where configuration changes have been identified. You can view the changes through a default browser, or take the path and name of the configuration files and compare them in a third party tool.

From the web UI you can select from the context menu the files that you want to compare. From Event Viewer, the type of comparison you can make is determined by the event. For example, if Entuity Configuration Monitor raises a CM Running Configuration Changed event, and the context menu allows you to view the current and previously retrieved running configurations for the device.

## Understanding the Compare Configuration File Page

From Entuity you can select to compare the current startup and running configuration files, any two archived startup configuration files, or any two archived running configuration files. Entuity Configuration Monitor identifies all differences between the two selected files; any ignore patterns configured through the exclude patterns file are not applied. (See *Figure 387 Inline Comparison of Configuration Files*.)

Entuity Configuration Monitor displays comparison results through a HTML page, titled Compare Configuration Files. Beneath the title Entuity Configuration Monitor identifies the compared files.

| Attribute | Description |
|---|---|
| *Filename* | Name of the archived file. The name indicates whether the configuration is a startup or running configuration. |
| *Device* | Name of the device as identified in Entuity. |
| *Last Changed* | Date the configuration was last changed. Entuity Configuration Monitor discards retrieved configurations that are the same as the previously retrieved configurations, so this is not necessarily the same as the time of the last successful configuration retrieval. |

Table 72 Comparison of Configuration Files

Entuity Configuration Monitor uses color coded highlights to identify the differences between the two files. There is a legend at the foot of the comparison HTML page.

| Highlight Color | Type of Difference |
|---|---|
| *Yellow* | Change to an existing line |
| *Green* | New line. |
| *Red* | Deleted line. |
| *Grey* | Missing line when compared to the original. |

Table 73 Compare Configuration Color

By default Entuity Configuration Monitor displays both files in their entirety side-by-side. You can configure the display to view the configuration files inline, where lines that are the same in the two files are displayed only once.

You can also configure the context. By default Entuity Configuration Monitor displays the complete files, however in long files you may only want to view a few lines before and after the differing lines to gain the context.

## Changing the Compare Configuration File Page

To change the Compare Configuration Files presentation:

1) On the Compare Configuration Files page click **Change View Format**. This hyperlink jumps to the foot of the page.

2) To alter the file display:

- Select *Inline* to view the changed lines one under another.
- In *Context* enter the number of lines around the differenced lines that you want to display. To display all the lines in a file leave blank.

3) Click **Reload**. This applies the stylesheet, reloads the page and updates the display to your new requirements.

## Comparing Startup and Running Configuration Files

In the web UI you can view each device’s archived configuration files, comparing their startup and running configurations. Each row in the Archived Configurations section indicates a configuration change in either the startup or running configuration files, when compared to the previously archived files.

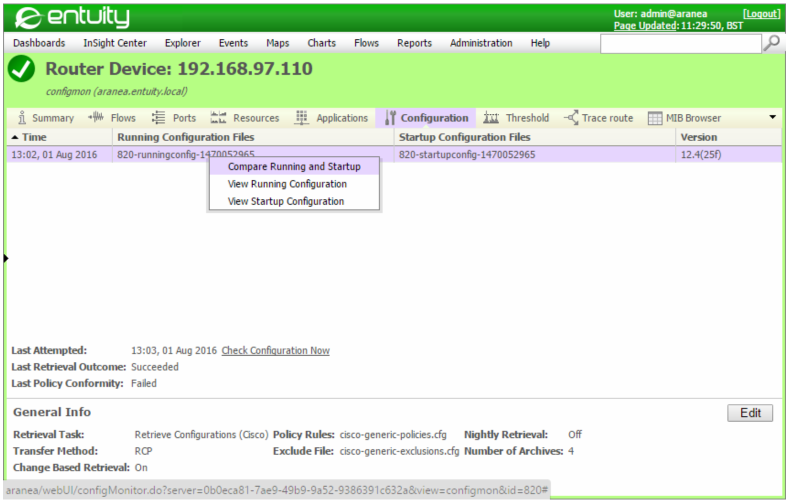
To compare startup and running configurations for a device:

1) From Explorer select the device.

2) Click **Configuration** .

3) In the Archived Configurations section highlight the row that contains the configurations you want to compare.

4) From the context sensitive menu click **Compare Running and Startup**.



Router Device: 192.168.97.110

*configmon (aranea.entuity.local)*

| Time | Running Configuration Files | Startup Configuration Files | Version |
|---|---|---|---|
| 13:02, 01 Aug 2016 | 820-runningconfig-1470052965 | 820-startupconfig-1470052965 | 12.4(25f) |

**Last Attempted:** 13:03, 01 Aug 2016
**Last Retrieval Outcome:** Succeeded
**Last Policy Conformity:** Failed

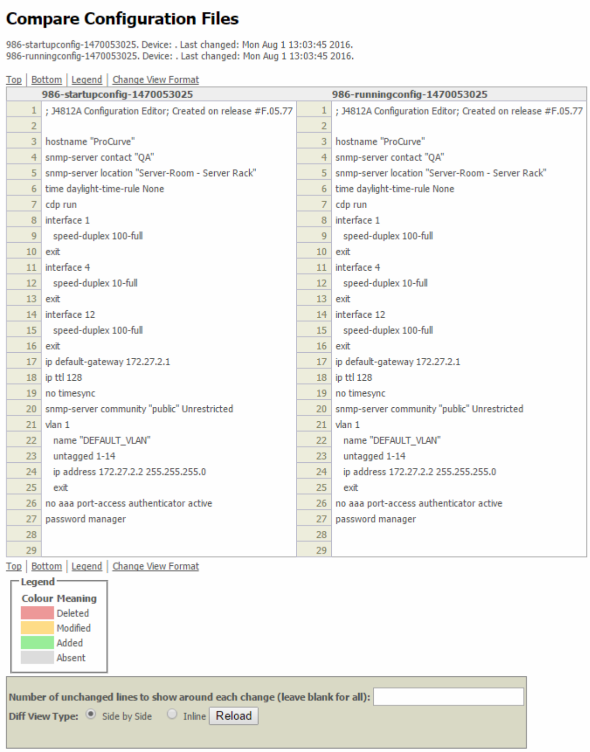
General Info

**Retrieval Task:** Retrieve Configurations (Cisco) **Policy Rules:** cisco-generic-policies.cfg **Nightly Retrieval:** Off
**Transfer Method:** RCP **Exclude File:** cisco-generic-exclusions.cfg **Number of Archives:** 4
**Change Based Retrieval:** On

aranea/webUI/configMonitor.do?server=0b0eca81-7ae9-49b9-9a52-9386391c632a&view=configmon&id=820#

Figure 386 Archived Configuration Files

Entuity generates a Compare Configuration Files page, displaying it in your default browser. You can adjust the display to best fit your requirements.



**Compare Configuration Files**

986-startupconfig-1470053025. Device: . Last changed: Mon Aug 1 13:03:45 2016.
986-runningconfig-1470053025. Device: . Last changed: Mon Aug 1 13:03:45 2016.

Top | Bottom | Legend | Change View Format

| | 986-startupconfig-1470053025 | | 986-runningconfig-1470053025 |
|---|---|---|---|
| 1 | ; J4812A Configuration Editor; Created on release #F.05.77 | 1 | ; J4812A Configuration Editor; Created on release #F.05.77 |
| 2 | | 2 | |
| 3 | hostname "ProCurve" | 3 | hostname "ProCurve" |
| 4 | snmp-server contact "QA" | 4 | snmp-server contact "QA" |
| 5 | snmp-server location "Server-Room - Server Rack" | 5 | snmp-server location "Server-Room - Server Rack" |
| 6 | time daylight-time-rule None | 6 | time daylight-time-rule None |
| 7 | cdp run | 7 | cdp run |
| 8 | interface 1 | 8 | interface 1 |
| 9 | speed-duplex 100-full | 9 | speed-duplex 100-full |
| 10 | exit | 10 | exit |
| 11 | interface 4 | 11 | interface 4 |
| 12 | speed-duplex 10-full | 12 | speed-duplex 10-full |
| 13 | exit | 13 | exit |
| 14 | interface 12 | 14 | interface 12 |
| 15 | speed-duplex 100-full | 15 | speed-duplex 100-full |
| 16 | exit | 16 | exit |
| 17 | ip default-gateway 172.27.2.1 | 17 | ip default-gateway 172.27.2.1 |
| 18 | ip ttl 128 | 18 | ip ttl 128 |
| 19 | no timesync | 19 | no timesync |
| 20 | snmp-server community "public" Unrestricted | 20 | snmp-server community "public" Unrestricted |
| 21 | vlan 1 | 21 | vlan 1 |
| 22 | name "DEFAULT_VLAN" | 22 | name "DEFAULT_VLAN" |
| 23 | untagged 1-14 | 23 | untagged 1-14 |
| 24 | ip address 172.27.2.2 255.255.255.0 | 24 | ip address 172.27.2.2 255.255.255.0 |
| 25 | exit | 25 | exit |
| 26 | no aaa port-access authenticator active | 26 | no aaa port-access authenticator active |
| 27 | password manager | 27 | password manager |
| 28 | | 28 | |
| 29 | | 29 | |

Top | Bottom | Legend | Change View Format

Legend

| Colour | Meaning |
|---|---|
| 🟥 | Deleted |
| 🟨 | Modified |
| 🟩 | Added |
| ⬜ | Absent |

**Number of unchanged lines to show around each change (leave blank for all):**

**Diff View Type:** ● Side by Side ○ Inline

Figure 387 Inline Comparison of Configuration Files

## Viewing Startup and Running Configuration Files

From the web UI you can view each device’s archived configuration files. Each row in the Archived Configurations section indicates a configuration change in either the startup or running configuration files, when compared to the previously archived files.

To view startup and running configurations for a device:

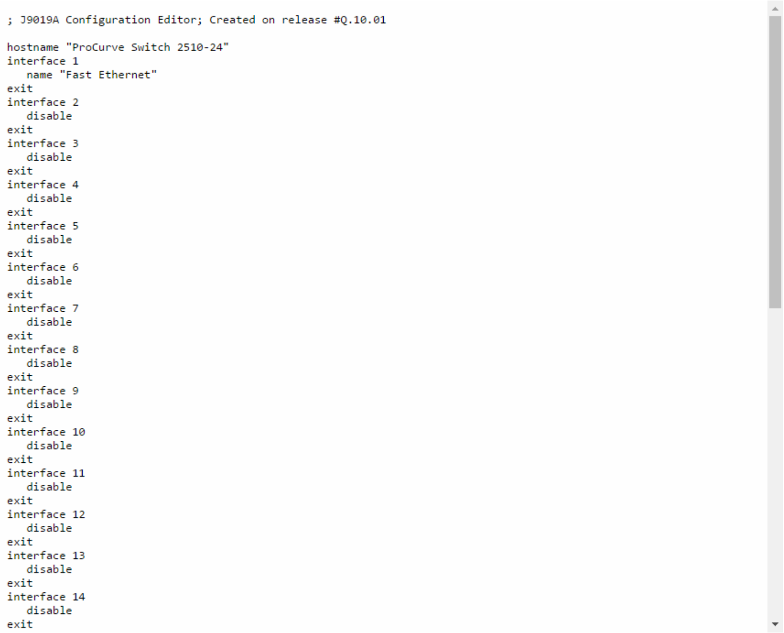
1) From Explorer select the device.

2) Click **Configuration** .

3) In the Archived Configurations section highlight the row that contains the configuration you want to view.

4) From the context sensitive menu click:

- **View Running Configuration**. Entuity displays the configuration file(s) in your default browser.
- **View Startup Configuration**. Entuity displays the configuration file(s) in your default browser.



```
; J9019A Configuration Editor; Created on release #Q.10.01

hostname "ProCurve Switch 2510-24"
interface 1
   name "Fast Ethernet"
exit
interface 2
   disable
exit
interface 3
   disable
exit
interface 4
   disable
exit
interface 5
   disable
exit
interface 6
   disable
exit
interface 7
   disable
exit
interface 8
   disable
exit
interface 9
   disable
exit
interface 10
   disable
exit
interface 11
   disable
exit
interface 12
   disable
exit
interface 13
   disable
exit
interface 14
   disable
exit
```

Figure 388 Viewing Configuration Files

## Identifying Configuration File Changes

In the web UI you can view each device’s archived configuration files, comparing their startup and running configurations. Each row in the Archived Configurations section indicates a configuration change in either the startup or running configuration files, when compared to the previously archived files.

To view changes in configurations for a device:

1) From Explorer select the device.
2) Click **Configuration**.
3) In the Archived Configurations section highlight the two rows that contain the configurations you want to compare.
4) From the context sensitive menu click:
   - **Compare Running Configurations**. Entuity generates a Compare Configuration Files page highlighting the differences between the two selected running configurations.
   - **Compare Startup Configurations**. Entuity generates a Compare Configuration Files page highlighting the differences between the two selected startup configurations.

# 70 Manage Entuity Configuration Monitor

Entuity Configuration Monitor includes a set of events through which you can monitor configuration retrieval. When you find a problem, for example failure to retrieve configuration from a device, you can interrogate Diagnostic Data.

## Entuity Configuration Monitor Events

Entuity Configuration Monitor includes events through which you can track changes in device configuration and also failures in configuration retrieval.

| Events | Description |
|---|---|
| CM Configuration Includes Policy Exclusion | An archived configuration file for a device matches one or more of the bad practice rules. |
| CM Configuration Missing Policy Mandated Statement | An archived configuration file for a device fails to conform to all of the good practice rules. |
| CM Firmware Version Changed | Change in the device firmware. Entuity Configuration Monitor also initiates a device configuration retrieval. |
| CM Previously Unsaved Configuration Saved | The current running and startup device configuration files are now the same. |
| CM Running Configuration Changed | The last running-configuration file retrieved by Entuity Configuration Monitor for a specified device does not match the last previously archived copy. |
| CM Running Configuration Retrieval Failed | Entuity Configuration Monitor failed to retrieve a configuration file from a monitored device. |
| CM Startup Configuration Changed | The last startup-configuration file retrieved by Entuity Configuration Monitor for a specified device does not match the last previously archived copy. |
| CM Startup Configuration Retrieval Failed | Entuity Configuration Monitor failed to retrieve a configuration file from a monitored device. |
| CM Unsaved Configuration | The running-configuration file retrieved by Entuity Configuration Monitor for a specified device does not match the startup-configuration file for that device. |

Table 74 Device Configuration Monitor Events

### Entuity Configuration Monitor Incidents

Entuity Configuration Monitor incidents are configured through the event project and managed through the event system. You can add annotations, assign incidents to users, close incidents and investigate incident details. Entuity includes a default set of Entuity Configuration Monitor incidents, details of which are in the *Entuity Event Reference Manual*:

- CM Configuration Includes Policy Exclusion Incident
- CM Configuration Missing Policy Mandated Statement Incident

- CM Firmware Version Changed Incident
- CM Running Configuration Changed Incident
- CM Running Configuration Retrieval Failed Incident
- CM Startup Configuration Changed Incident
- CM Startup Configuration Retrieval Failed Incident
- CM Unsaved Configuration Incident.

## Managing Entuity Configuration Monitor Events

Entuity Configuration Monitor events are fully integrated into Entuity, are managed using the same tools as standard events and require the user to have the same permission level, administrator, to change their configuration.

By default Entuity Configuration Monitor events are enabled for all devices where Entuity Configuration Monitor attempts to retrieve device configuration.

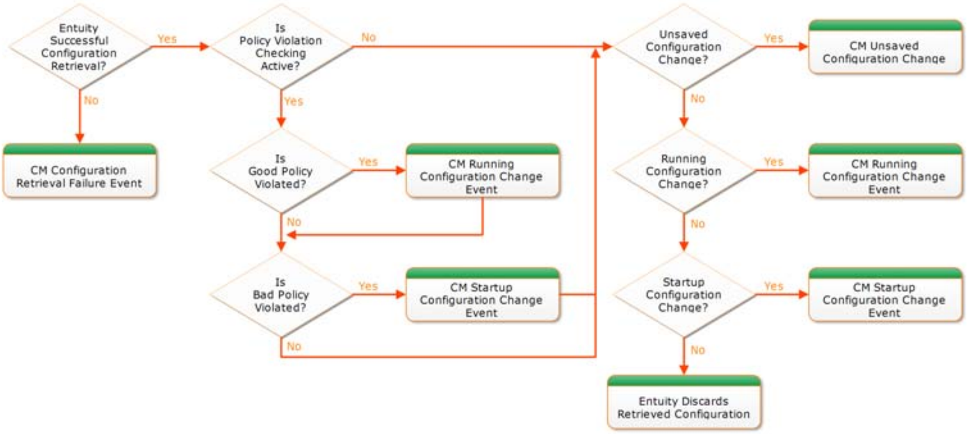
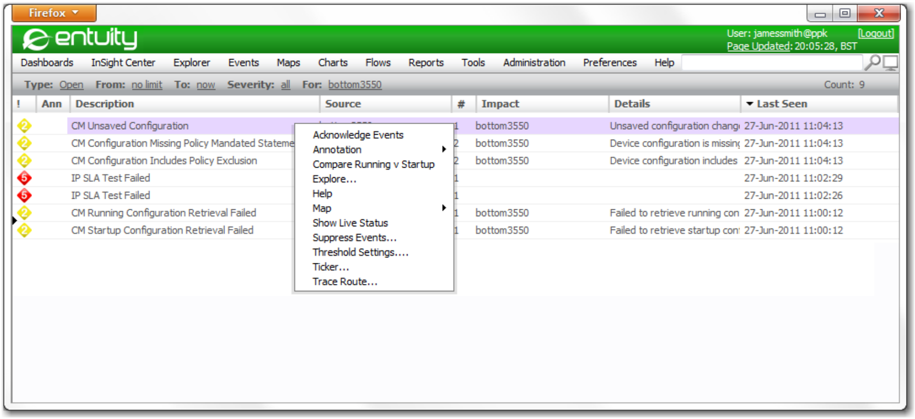

Entuity Successful Configuration Retrieval?
Yes
No
CM Configuration Retrieval Failure Event
Is Policy Violation Checking Active?
No
Yes
Is Good Policy Violated?
Yes
No
CM Running Configuration Change Event
Is Bad Policy Violated?
Yes
No
CM Startup Configuration Change Event
Unsaved Configuration Change?
Yes
No
CM Unsaved Configuration Change
Running Configuration Change?
Yes
No
CM Running Configuration Change Event
Startup Configuration Change?
Yes
No
CM Startup Configuration Change Event
Entuity Discards Retrieved Configuration

Figure 389 Entuity Configuration Monitor Event Process

## Investigating Configuration Events

From Event Viewer, the type of comparison you can make is determined by the type of event. For example, if Entuity Configuration Monitor raises a CM Running Configuration Changed event, then the context menu allows you to view the current and previously retrieved running configurations for the device.



Type: Open From: no limit To: now Severity: all For: bottom3550 Count: 9

| ! | Ann | Description | Source | # | Impact | Details | Last Seen |
|---|---|---|---|---|---|---|---|
| 2 | | CM Unsaved Configuration | | 1 | bottom3550 | Unsaved configuration chang | 27-Jun-2011 11:04:13 |
| 2 | | CM Configuration Missing Policy Mandated Stateme | | 2 | bottom3550 | Device configuration is missin | 27-Jun-2011 11:04:13 |
| 2 | | CM Configuration Includes Policy Exclusion | | 2 | bottom3550 | Device configuration includes | 27-Jun-2011 11:04:13 |
| 5 | | IP SLA Test Failed | | 1 | | | 27-Jun-2011 11:02:29 |
| 5 | | IP SLA Test Failed | | 1 | | | 27-Jun-2011 11:02:26 |
| 2 | | CM Running Configuration Retrieval Failed | | 1 | bottom3550 | Failed to retrieve running con | 27-Jun-2011 11:00:12 |
| 2 | | CM Startup Configuration Retrieval Failed | | 1 | bottom3550 | Failed to retrieve startup con | 27-Jun-2011 11:00:12 |

Figure 390 Entuity Configuration Monitor Events in Event Viewer

# Troubleshoot Configuration Retrieval

When retrieval of a device configuration fails Entuity raises the CM Running Configuration Retrieval Failed or CM Startup Configuration Retrieval Failed event against that device. You can troubleshoot retrieval:

1) Check for other events raised against the device, for example Network Outage, to identify whether retrieval failure is a symptom of a more widespread problem or whether it is the real issue.

2) Identify whether this event is raised against one or more devices.

   When the event is raised against many devices:

   - Check the transfer servers. Although Entuity Configuration Monitor is configured to work with the specified server it does not check that the server is running when attempting a retrieval. If the server is not running the retrieval will fail.
   - Check the specified transfer and archive folders exist and permit your transport servers to write to them.
   - Check CLI credential sets are still valid.

   When this event is raised against one device then it may be an issue specific to the device, for example the device is down, although if you have initiated a manual retrieval it may be a more widespread issue that is yet to show itself.

## Use Transfer Server Logs

Transfer servers, including OpenTFTPserver, can be configured to run in logging mode. You can then use the transfer server log files to identify the success of file uploads and troubleshoot any issues.

# Report on Entuity Configuration Monitor

Entuity Configuration Monitor includes Configuration Monitor Settings, Device Configuration Settings and Device Configuration Summary reports (see the *Entuity Reports Reference Manual*):

- The Configuration Monitor Settings report summarizes the current configuration monitor settings of devices.
- The Device Configuration Status report details the last attempt at configuration retrieval.
- The Device Configuration Summary report summarizes the device configuration of the reporting period.

Entuity Configuration Monitor data is also available for you to develop your own reports and dashboards.

# 71 Entuity Configuration Management

The Entuity Configuration Management module allows you to configure devices and ports from Entuity, by running scripts through an Expect like API on those target devices if the appropriate CLI credential sets have been established. You can for example set a port to admin down or change a device community string.

Entuity Configuration Management uses a combination of the Entuity information database, an Expect API and Groovy scripts to allow you to specify configuration tasks. A task usually has a specific objective, often the configuration of a device or port. It comprises of a number of steps. For example, a simple three step task might be:

1) Log in to a device.
2) Perform an action.
3) Log out of a device.

The login and logout steps are quite generic and could be used by many tasks, which illustrates the efficiency in building tasks from a number of re-usable steps.

When you run a task it becomes a job, and if this job is running against a number of objects then each object has its own sub-job. In this way the success or failure of a sub-job on one object (device or port) does not impact on the processing of another sub-job. As this implies you can apply a task to many objects.

You can run tasks from context menus and also schedule them.

The Configuration Management module:

- Requires a valid license.
- Is activated through `configure`.
- Users must either be members of the Administrators group or be assigned the Configuration Management Administration tool permission.

Entuity Configuration Management delivers a powerful tool set for managing ports and devices on your network. You are strongly advised to control user access to the Configuration Management module and fully test your scripts before applying them to your live network. The scripts provided here are only intended to illustrate the functionality and scripting techniques available with this module. Entuity accepts no liability in the event of the instructions in the documentation not being followed when using the module.

# Configuration Management Process

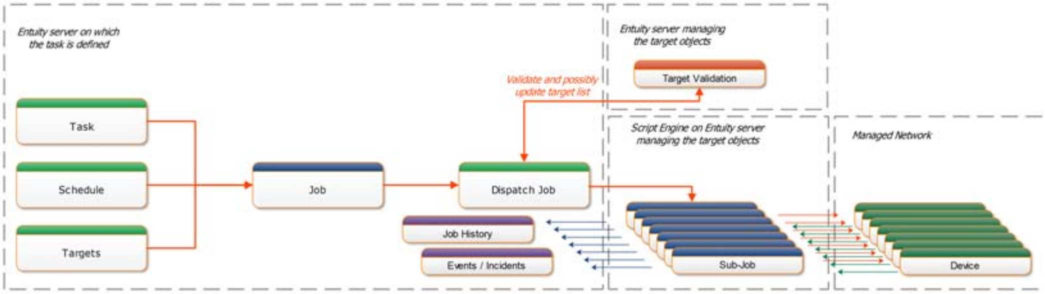

Entuity server on which the task is defined
Task
Schedule
Targets
Job
Dispatch Job
Job History
Events / Incidents
Validate and possibly update target list
Entuity server managing the target objects
Target Validation
Script Engine on Entuity server managing the target objects
Sub-Job
Managed Network
Device

Figure 391 Configuration Management Device Task Process

The configuration management process:

1) The starting point is the running of a task applied to a set of targets, which can either be devices or ports on devices. The running of a task may be initiated from a context menu or through the scheduler.

   When the task runs it is a job.

2) The Entuity server identifies and validates the target objects. (See *Target Validation*.) Where the target objects are managed by remote Entuity servers this involves checking with those servers and potentially amending the list of targets the job runs against.

3) The Entuity server creates a dispatch job to send to the Script Engine of the Entuity server managing the target objects. The dispatch job contains one sub-job for each target. When these targets are managed by different servers Entuity creates a dispatch job for each server.

As jobs may be defined on a central server but run on a remote server it is important central and remote servers are running the same version of Entuity.

4) The Script Engine runs the sub-jobs, performing the specified task on the target device or port.

   Through the Job History page you can view the progress of a job. Drilling down to a sub-job you can view its progress.

   When tasks are configured for events then Entuity can raise events and incidents reporting the success or failure of the job.

| Term | Description |
|---|---|
| Task | A task is the definition of the configuration management operation. It comprises of one or more steps.<br>A task is defined on one Entuity server and all of its history, audit logs and schedules are retained there, even though the task may be applied to objects on remote Entuity servers. |
| Step | A step is a discrete part of a task. The step action is configured through a Groovy Script. The same step may be used by more than one task. |
| Job | A job consists of its task definition and run time settings, for example when it is to be run, which objects it is run against, and as such only exists when it is running. |
| Sub-Job | When a job runs Entuity creates a sub-job for each object it runs against. For example if the job is to run against six devices Entuity creates six self-contained sub-jobs. These sub-jobs are run by the Script Engine on the Entuity server that manages the target object which may be different from the Entuity server on which the job was run. |
| Dispatch Job | When Entuity runs a job it creates the sub-jobs and then submits them all to the Script Engine as one dispatch job. If the sub-jobs are being run on a number of Entuity servers then Entuity creates one dispatch job for each server.<br>If the Script Engine is busy then the dispatch job may be queued, i.e. submitting a dispatch job does not imply the immediate execution of its first sub-job. |
| Script Engine | Script Engine runs the sub-job. Sub-jobs are run by the Script Engine of the Entuity server that is managing the target object (device or port). |

Table 75 Entuity Configuration Management Terms

## Target Validation

Before Entuity creates sub-jobs and submits them to the script engine it validates the proposed target objects.

Validation tests applied by Entuity before dispatching the job:

- Is the task still available. Entuity may attempt to run a job even after the associated task has been deleted.
- Is the current version of the task the same as that associated with the job, for example one user may call a task while another user is updating it. This check is only applicable to tasks called from context menus.
- Validates the Groovy script.
- Are the user permissions of the job owner sufficient to run the job.
- Applies the filter to derive the target objects.

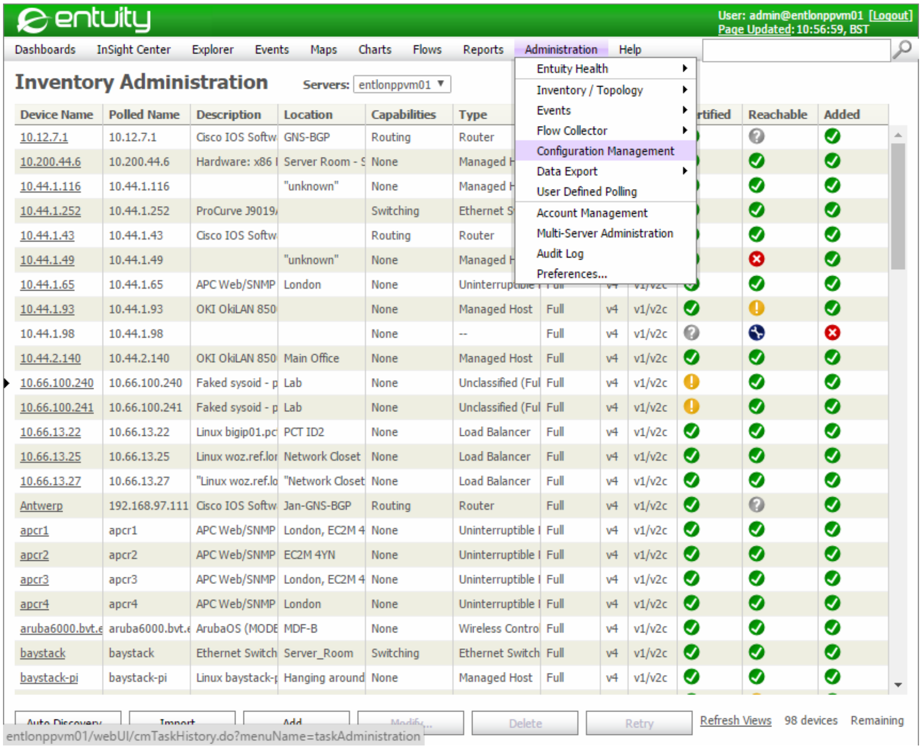
Entuity checks the credential sets required for accessing the target objects when running the sub-job.

# Configuration Management Administration

Administrators have full access to the Configuration Management module. Users that are members of user groups with the Configuration Management tool permission also have full access. (See *Tool Permissions*.)

Access to the Configuration Management task administration and history pages is through the same administration menu:

1) Click **Administration > Configuration Management**.



Inventory Administration

Servers: entlonppvm01

| Device Name | Polled Name | Description | Location | Capabilities | Type | | | | rtified | Reachable | Added |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.12.7.1 | 10.12.7.1 | Cisco IOS Softw | GNS-BGP | Routing | Router | | | | ✓ | ? | ✓ |
| 10.200.44.6 | 10.200.44.6 | Hardware: x86 I | Server Room - S | None | Managed H | | | | ✓ | ✓ | ✓ |
| 10.44.1.116 | 10.44.1.116 | | "unknown" | None | Managed H | | | | ✓ | ✓ | ✓ |
| 10.44.1.252 | 10.44.1.252 | ProCurve J9019/ | | Switching | Ethernet S | | | | ✓ | ✓ | ✓ |
| 10.44.1.43 | 10.44.1.43 | Cisco IOS Softw | | Routing | Router | | | | ✓ | ✓ | ✓ |
| 10.44.1.49 | 10.44.1.49 | | "unknown" | None | Managed H | | | | ✓ | ✗ | ✓ |
| 10.44.1.65 | 10.44.1.65 | APC Web/SNMP | London | None | Uninterruptible I | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.44.1.93 | 10.44.1.93 | OKI OkiLAN 850 | | None | Managed Host | Full | v4 | v1/v2c | ✓ | ! | ✓ |
| 10.44.1.98 | 10.44.1.98 | | | None | -- | Full | v4 | v1/v2c | ? | 🔧 | ✗ |
| 10.44.2.140 | 10.44.2.140 | OKI OkiLAN 850 | Main Office | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.66.100.240 | 10.66.100.240 | Faked sysoid - p | Lab | None | Unclassified (Ful | Full | v4 | v1/v2c | ! | ✓ | ✓ |
| 10.66.100.241 | 10.66.100.241 | Faked sysoid - p | Lab | None | Unclassified (Ful | Full | v4 | v1/v2c | ! | ✓ | ✓ |
| 10.66.13.22 | 10.66.13.22 | Linux bigip01.pc | PCT ID2 | None | Load Balancer | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.66.13.25 | 10.66.13.25 | Linux woz.ref.lor | Network Closet | None | Load Balancer | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| 10.66.13.27 | 10.66.13.27 | "Linux woz.ref.lo | "Network Closet | None | Load Balancer | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| Antwerp | 192.168.97.111 | Cisco IOS Softw | Jan-GNS-BGP | Routing | Router | Full | v4 | v1/v2c | ✓ | ? | ✓ |
| apcr1 | apcr1 | APC Web/SNMP | London, EC2M 4 | None | Uninterruptible I | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| apcr2 | apcr2 | APC Web/SNMP | EC2M 4YN | None | Uninterruptible I | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| apcr3 | apcr3 | APC Web/SNMP | London, EC2M 4 | None | Uninterruptible I | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| apcr4 | apcr4 | APC Web/SNMP | London | None | Uninterruptible I | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| aruba6000.bvt.e | aruba6000.bvt.e | ArubaOS (MODE | MDF-B | None | Wireless Contro | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| baystack | baystack | Ethernet Switch | Server_Room | Switching | Ethernet Switch | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |
| baystack-pi | baystack-pi | Linux baystack-p | Hanging around | None | Managed Host | Full | v4 | v1/v2c | ✓ | ✓ | ✓ |

entlonppvm01/webUI/cmTaskHistory.do?menuName=taskAdministration

Figure 392 Entuity Configuration Management

The Task Administration page consists of tabs that reflect the major components of Entuity Configuration Management:

- Tasks. (See *Task Administration*.)
- Steps. (See *Task Steps*.)

  A step is a discrete part of a task. The step action is configured through a Groovy Script. A task comprises of one or more steps. The same step may be used by more than one task.

  Through the Steps administration page users can create, edit and delete steps.
- Schedules. (See *Task Schedules*.)

For each schedule Entuity identifies its component, including when it last run and when it will next run.

Through the Schedules administration page users can edit, delete, suspend and resume schedules.

- History. (See *Task History*.)

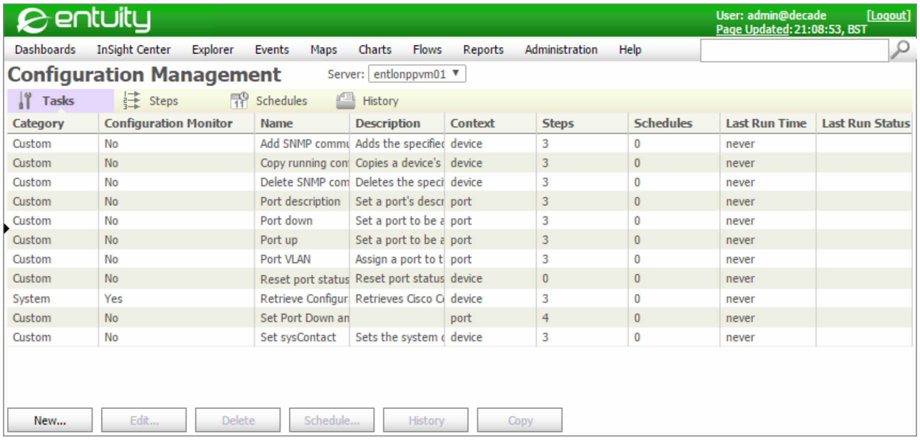
Task, steps and schedules are saved to the selected Entuity server. In multi-server environments you can set up configuration management on the central server but the objects they run against can be on remote servers. Task history is always held on the server on which the task is defined.

## Task Administration

A task contains all of the instructions required to complete the designated configuration management or monitor task. Depending upon the configuration you can manually run tasks by selecting target objects (e.g. devices or ports) from context menus or by scheduling the task against a view. A running task is a job, and when it runs against a target it is a sub-job.

Through the Task administration page you can create, edit and delete tasks. This would involve assigning steps to tasks and potentially creating new steps. It might also involve assigning schedules to tasks. You can also access the task history.

All users that can access Configuration Management administration have access to all of the tasks, steps, schedules and histories.



User: admin@decade

Page Updated: 21:08:53, BST

Configuration Management

Server: entlonppvm01

| Category | Configuration Monitor | Name | Description | Context | Steps | Schedules | Last Run Time | Last Run Status |
|---|---|---|---|---|---|---|---|---|
| Custom | No | Add SNMP commu | Adds the specifiec | device | 3 | 0 | never | |
| Custom | No | Copy running con | Copies a device's | device | 3 | 0 | never | |
| Custom | No | Delete SNMP com | Deletes the speci | device | 3 | 0 | never | |
| Custom | No | Port description | Set a port's descr | port | 3 | 0 | never | |
| Custom | No | Port down | Set a port to be a | port | 3 | 0 | never | |
| Custom | No | Port up | Set a port to be a | port | 3 | 0 | never | |
| Custom | No | Port VLAN | Assign a port to t | port | 3 | 0 | never | |
| Custom | No | Reset port status | Reset port status | device | 0 | 0 | never | |
| System | Yes | Retrieve Configur | Retrieves Cisco C | device | 3 | 0 | never | |
| Custom | No | Set Port Down an | | port | 4 | 0 | never | |
| Custom | No | Set sysContact | Sets the system c | device | 3 | 0 | never | |

Figure 393 Task Administration

| Attribute | Description |
|---|---|
| *Category* | Entuity Configuration Management supports System and Custom task types. You can not modify system tasks however you can copy them and modify the resulting custom task. Entuity is shipped with these Configuration Monitor system tasks:<br>■ Retrieve Configuration (Cisco)<br>■ Retrieve Configuration (Dell)<br>■ Retrieve Configuration (Juniper)<br>■ Retrieve Configuration (HP)<br>■ Retrieve Configuration (Huawei).<br>Custom tasks are user defined. You cannot create a custom task with a name matching an existing task. However, if Entuity introduces a system task whose name conflicts with a custom task, then both tasks will be considered as valid. The custom task's display name will be qualified by appending **(custom)** to the end (except for the Tasks and Steps tabs where the Category column qualifies the tasks). |
| *Configuration Monitor* | Set to Yes for a Configuration Monitor level task and to No for a Configuration Management level task.<br>Configuration Monitor tasks:<br>■ Do not appear in the Task Permissions dialog. Instead, if a user has Configuration Monitor tool permission, then they will implicitly have permission to run and view the history of all related Configuration Monitor tasks.<br>■ Can only be executed with the Configuration Monitor feature, i.e. automatically by the Configuration Monitor tool, or manually via the **Check Configuration Now** menu option or a link inside the associated Explorer tab. They cannot be scheduled via the Configuration Management scheduler page.<br>■ Must be defined on each server on which they will be used. |
| *Name* | String to identify a task which must be unique on the selected server (case insensitive comparison). |
| *Description* | Task description (optional). |
| *Context* | Identifies the context in which the task can run, i.e. **Device** or **Port**. |
| *Steps* | Number of steps in the task. When you do a mouse over Entuity displays a list of the names of steps used in the task. |
| *Schedules* | Number of scheduled jobs for this task. |
| *Last Run Time* | Timestamp of the last execution of the task. |
| *Last Run Status* | If the task:<br>■ Has an associated job that is running then *Status* indicates the current state of jobs associated with the task, for example **2 IN PROGRESS, 3 QUEUED**. This is also a hyperlink to the job History tab.<br>■ Does not have an associated job that is running then *Status* shows the state of the previously completed job, i.e. Succeeded or Failed. |

Table 76 Task Administration

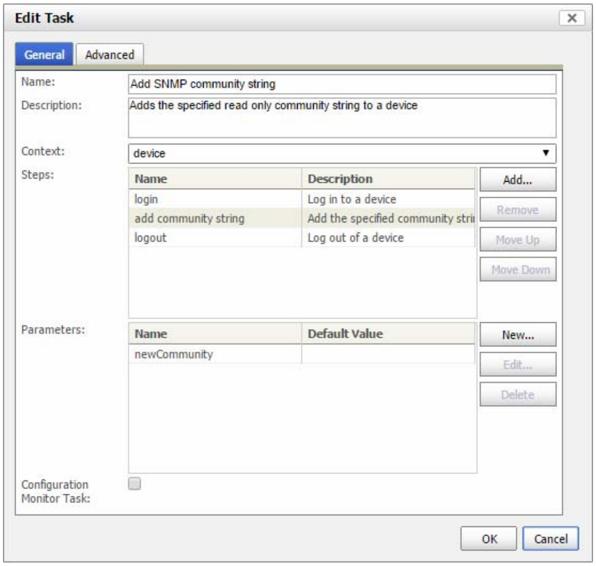
| Button | Description |
|---|---|
| **New** | Click to create a task. (See *New and Edit Task dialog*.) |
| **Delete** | Click to delete the selected task or tasks. |
| **History** | Click to view the history of the selected task or tasks.<br>Entuity retains the task history for 30 days This includes task jobs run from both the context menu and scheduler. (See *Task History*.) |
| **Edit** | Click to edit the selected task. (See *New and Edit Task dialog*.) |
| **Schedule** | Click to schedule a task. |
| **Copy** | Creates a copy of the highlighted task. The name of the copy is Copy of added to the original name |

Table 77 Task Actions

## New and Edit Task dialog

The Create Task and Edit Task dialogs are essentially the same, comprising of two tabs, General and Advanced.

The General tab includes the name and description of the task. It is also where you associate steps to the tasks and define any parameters. The parameters you define for a task are available to all of the steps in the task. (See *Task Parameters*.)



Name: Add SNMP community string

Description: Adds the specified read only community string to a device

Context: device ▼

Steps:

| Name | Description |
|---|---|
| login | Log in to a device |
| add community string | Add the specified community stri |
| logout | Log out of a device |

Parameters:

| Name | Default Value |
|---|---|
| newCommunity | |

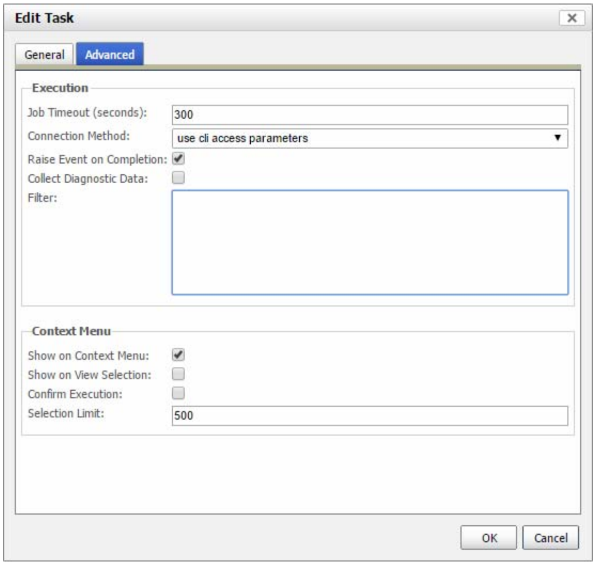
Configuration Monitor Task: ☐

Figure 394 Task General

| Attribute | Description |
|---|---|
| *Name* | A unique name (case insensitive comparison) to identify the task on the selected server. |
| *Description* | A description of the task. (Optional.) |
| *Context* | Sets the type of target that the task can run against:<br>■ **Device** (default) the task can only run against a device.<br>■ **Port** which limits the task to only run against a port.<br>These contexts apply regardless of whether the task is called from the scheduler or a context menu. |
| *Steps* | A valid task must contain at least one step. A task can contain the same step more than once and the same step can be included to multiple tasks.<br>You can click:<br>■ **Add** to create a new step or select from existing steps.<br>■ **Remove** to delete the selected step or steps from the task. Entuity allows you to select multiple steps and then delete them (Entuity does not prompt you to confirm deletion of the steps from the task.)<br>You can also reorder the steps within a task by using the Move Up and Move Down buttons. |
| *Parameters* | Groovy Script parameter format, i.e. **String**, **Integer**, **Float**.<br>You can click:<br>■ **New** to create a new parameter.<br>■ **Edit** to replace the selected parameter with a new one.<br>■ **Delete** to delete the selected parameter, or parameters from the task. Entuity allows you to select multiple parameters and then delete them (Entuity does not prompt you to confirm deletion of the parameters from the task.) |
| *Configuration Monitor Task* | When selected Entuity Configuration Management handles the task as a configuration monitor task. Configuration monitor tasks:<br>■ Do not appear in the Task Permissions dialog. Instead, if a user has the Configuration Monitor tool permission, then they have permission to run and view the history of all Configuration Monitor tasks.<br>■ Cannot be scheduled. These tasks can be run automatically by the Configuration Monitor tool, or manually via the Check Configuration Now menu option or link inside the associated Explorer tab.<br>■ Must be defined on the Entuity server on which they are used, i.e. on the server managing the device against which the task is run. In contrast configuration management tasks can be run from a central server and applied to devices managed by remote servers. |

Table 78 Tasks General Options

The Advanced tab includes settings that control how the task is run, for example whether it is available from context menus, its job timeout settings, against how many objects it can run.



Execution

Job Timeout (seconds): 300

Connection Method: use cli access parameters

Raise Event on Completion: ☑

Collect Diagnostic Data: ☐

Filter:

Context Menu

Show on Context Menu: ☑

Show on View Selection: ☐

Confirm Execution: ☐

Selection Limit: 500

Figure 395 Task Advanced

| Attribute | Description |
|---|---|
| *Job Timeout (seconds)* | Time, in seconds, assigned for Entuity to execute the task after which the task will timeout and terminate. The timeout period starts when Entuity starts to execute the job.<br>The default is 300 (5 minutes) and the maximum value is 32767 (9 hours approximately). |
| *Connection Method* | Method of connecting to the object. When set to:<br>■ **use cli access parameters** (default) Entuity uses the connection method defined in the credential set to connect to devices. If a credential set is not specified than Entuity ignores the connection request and records this failure in the Task History.<br>■ **use connection parameters** Entuity prompts the user for credential details before executing the task.<br>■ **none** Entuity does not require a connection to complete the task, for example SNMP Get/Set only tasks. |
| *Raise Event on Completion* | When selected Entuity raises a Config Mgmt Job Succeeded or Config Mgmt Job Failed event (and potentially an associated incident) when Entuity respectively considers the job to have completed successfully or failed.<br>When not selected Entuity cannot raise configuration management events. |
| *Collect Diagnostic Data* | Script Engine retains the conversation data between itself and the device for each task (which can be turned off in `entuity.cfg`). There is a limit (configurable in `entuity.cfg`) of the total size of these diagnostic data that can be stored in Script Engine's log file, *entuity_home*`\log\expect.log`. |

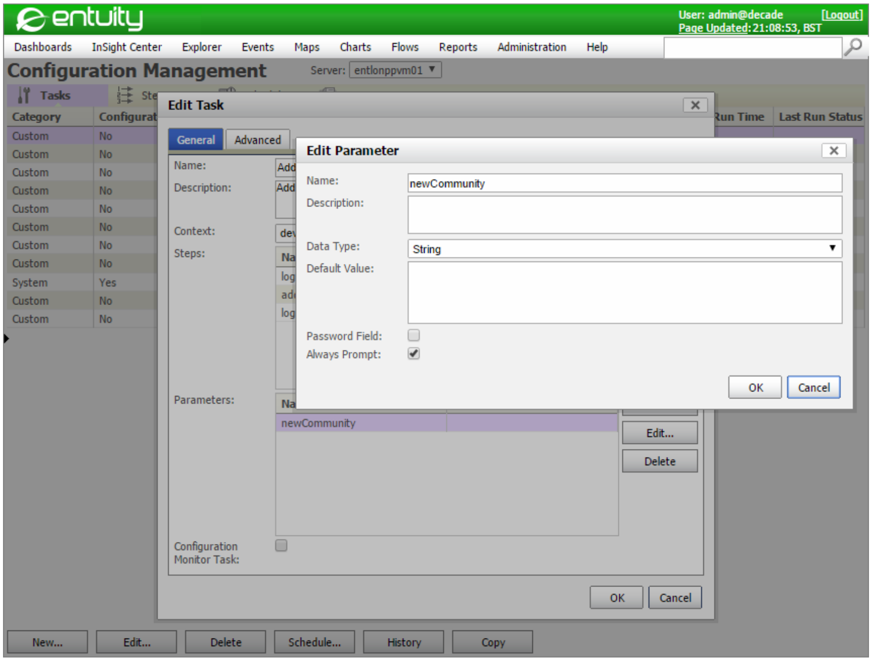
Table 79 Task Advanced Options

| Attribute | Description |
|---|---|
| *Filter* | Object filter specifies the object against which the task can legitimately run, for example you can filter on the device SysOid:<br>`simple; device.sysOid==”1.3.6.1.2.1.1.3” \|\| device.sysOid==”1.3.6.1.2.1.1.4”`<br>In multi-server environments if the selected object is on a remote server, the filter is sent to the remote server for evaluation. The result is returned to the central server.<br>For context menus a filter is evaluated when you open the menu, so if the selected object does not meet the filter then the context menu task is not displayed.<br>For scheduled jobs the filter is always evaluated when the scheduled job is run. |
| *Show on context menu* | When selected the task can be run from the context menu, when not selected it can only be scheduled. |
| *Show on View Selection* | When *Show on context menu* and *Show on View selection* are:<br>■ Both selected the task can be run from the view-level context menu. The task is always available from the context menu. When running the task Entuity applies the filter so the job only runs against appropriate objects.<br>■ Not both selected (default) the task is not available through the view context menu. |
| *Confirm Execution* | When *Show on context menu* and *Confirm Execution* are selected the user must confirm the running of the job. The default is unselected. |
| *Selection Limit* | When *Show on context menu* is selected you can enter the maximum number of objects that can be selected when you run the task from the context menu. When set to:<br>■ **1** (default) the task is only available from the context menu when 1 object is selected.<br>■ *N* the task is only available from the context menu when *N* or a fewer number of objects are selected. Only one of the selected objects must match the *Filter* for Entuity to display the task on the context menu (when running the task Entuity applies the filter so the job only runs against appropriate objects).<br>The maximum value is 500. The exception is when you run a task from a view. Then there is no limit on the number of objects against which you can run the task. |

Table 79 Task Advanced Options

## Task Parameters

Parameters are stored locally to the task and are only saved when you save the task. Parameters are available to all steps in the task. You can set parameter values when defining the task or when running the job.



| Category | Configurat |
|---|---|
| Custom | No |
| Custom | No |
| Custom | No |
| Custom | No |
| Custom | No |
| Custom | No |
| Custom | No |
| Custom | No |
| System | Yes |
| Custom | No |
| Custom | No |

Edit Parameter

Name: newCommunity

Description:

Data Type: String

Default Value:

Password Field: □

Always Prompt: ☑

OK Cancel

Parameters: newCommunity

Configuration Monitor Task: □

Figure 396 Task Parameters

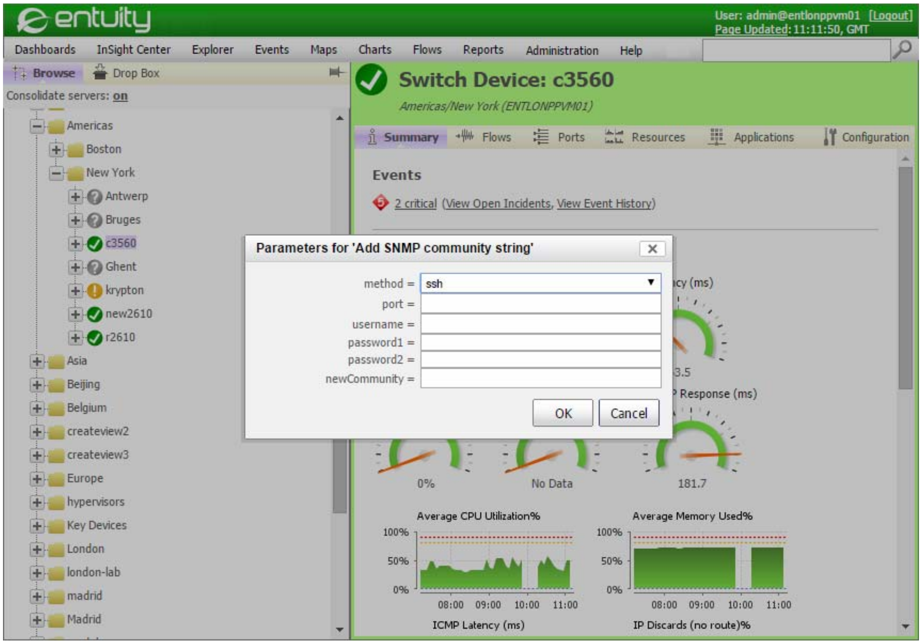
| Attribute | Description |
|---|---|
| *Name* | It must be a valid Groovy variable name and unique for each task.<br>Entuity validates the value when you click **OK**. |
| *Description* | Description of the parameter, for example its purpose or usage (optional). |
| *Data Type* | Parameter data type, i.e. **String** (default), **Integer** or **Float**. |
| *Default Value* | A default value is optional. When it is:<br>■ Specified then it must be a valid Groovy expression.<br>■ Not specified Entuity assigns a null to the variable.<br>Entuity validates the value when you click **OK**. |
| *Password Field* | When the check box is selected characters are masked as they are entered, i.e. instead of the characters entered Entuity displays asterisks. This is useful with Password fields. When not selected (default) then the characters are displayed as entered. |
| *Always Prompt* | When:<br>■ Selected Entuity always prompts the user to enter a value.<br>■ Not selected (default) Entuity does not prompt for a value unless the default value is not set. |

Table 80 Parameter Attributes

Entuity stores connection details as task parameters.

If you set the *Connection Method* to **use connection parameters**, then Entuity automatically creates hidden credential parameters for the task but requires you to set the parameter values. When the task is:

- Called from the context menu Entuity raises a dialog and prompts for entry of the credential details and any other parameters that require values.



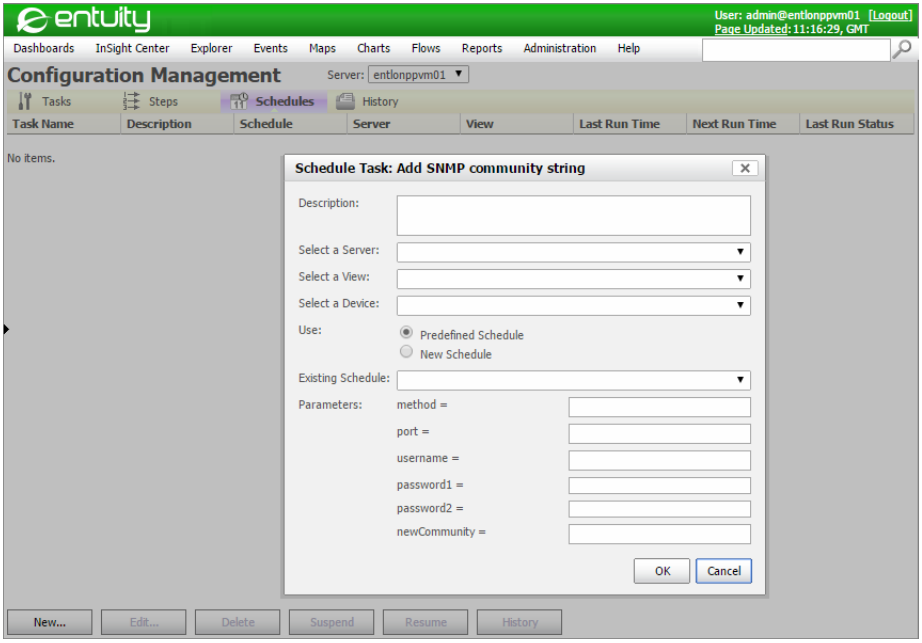
Parameters for 'Add SNMP community string'

method = ssh
port =
username =
password1 =
password2 =
newCommunity =

OK Cancel

Figure 397 Set Task Parameters

- Scheduled you are prompted to complete the credential and any other parameter values when scheduling the task.



Schedule Task: Add SNMP community string

Description:

Select a Server:

Select a View:

Select a Device:

Use: ● Predefined Schedule ○ New Schedule

Existing Schedule:

Parameters: method = port = username = password1 = password2 = newCommunity =

OK Cancel

Figure 398 Set Task Parameters

| Parameter | Description |
|---|---|
| *method* | Method of accessing the target command line interface, i.e. **telnet** or **ssh**. |
| *port* | Port used by the telnet (default port 23) or ssh (default port 22) applications to access the target. If a value is not entered Entuity uses the application default. Optional parameter. |
| *username* | Username required to access the target. |
| *password1* | Password required to access the target. |
| *password2* | *Password2* can be used with ssh connections. Optional parameter. |

Table 81 Task Parameters

## Create Tasks

This example creates a task that takes a port down and updates the port short description. It uses steps included as part of the example tasks:

1) Logs in into a device.

2) Sets a port to down.

3) Updates the system contact to James Smith.

4) Logs out of the device.

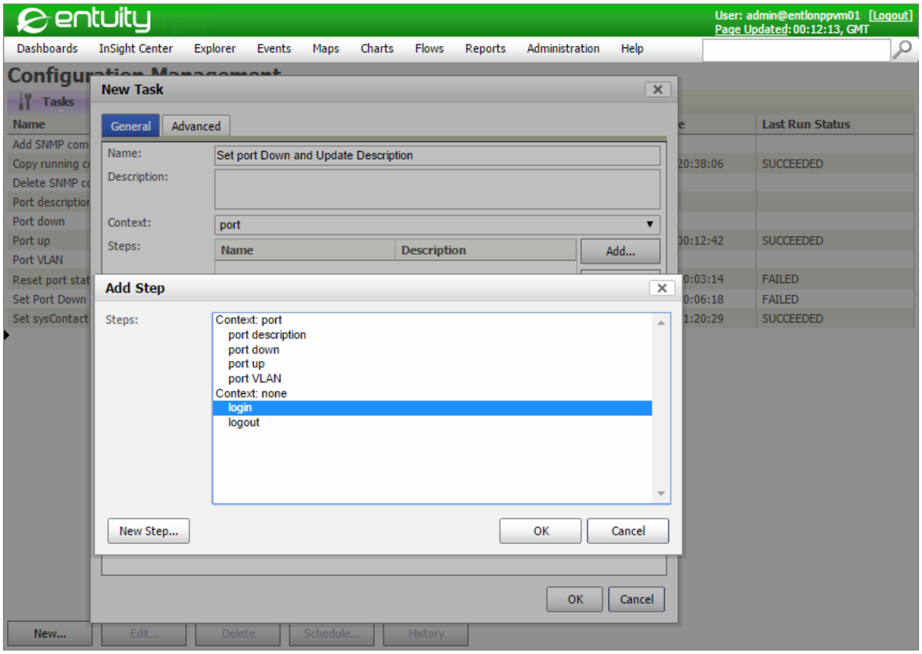
To create a task:

1) Select **Administration** > **Configuration Management**.

2) Click **New**.

3) In the Steps section click **Add**.

   Users can select an existing step or create a new one. If the user has already selected a task context then Entuity only displays steps valid for that context, otherwise steps are grouped by context.



| Name | e | Last Run Status |
|---|---|---|
| Add SNMP com | | |
| Copy running c | 20:38:06 | SUCCEEDED |
| Delete SNMP c | | |
| Port descriptio | | |
| Port down | | |
| Port up | 00:12:42 | SUCCEEDED |
| Port VLAN | | |
| Reset port stat | 0:03:14 | FAILED |
| Set Port Down | 0:06:18 | FAILED |
| Set sysContact | 1:20:29 | SUCCEEDED |

Name: Set port Down and Update Description

Description:

Context: port

Steps:

| Name | Description |
|---|---|

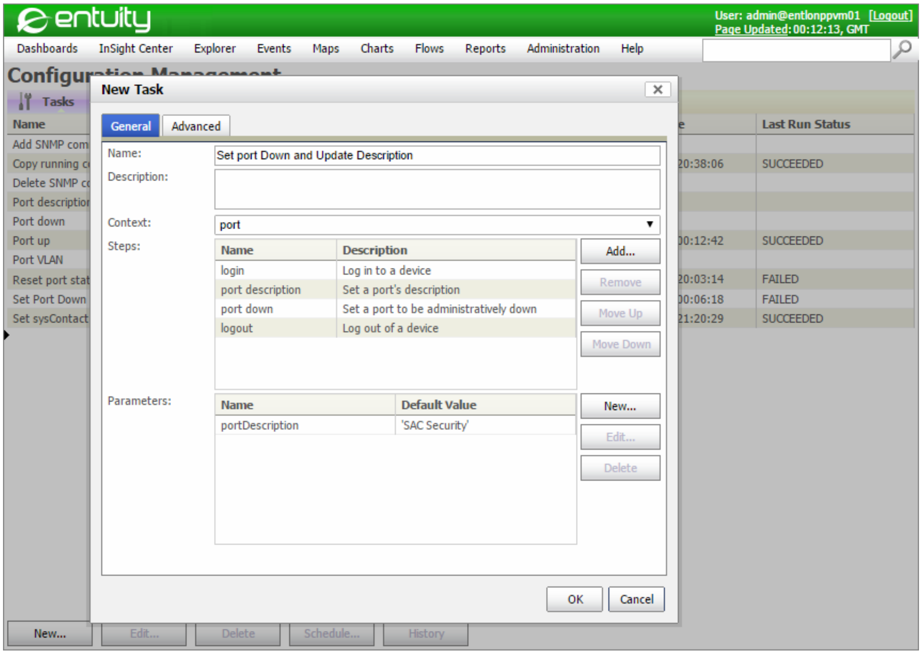
Steps:

Context: port
- port description
- port down
- port up
- port VLAN

Context: none
- login
- logout

Figure 399 New Task General

4) In the Steps section click **OK**.



New Task

Name: Set port Down and Update Description

Description:

Context: port

Steps:

| Name | Description |
|---|---|
| login | Log in to a device |
| port description | Set a port's description |
| port down | Set a port to be administratively down |
| logout | Log out of a device |

Parameters:

| Name | Default Value |
|---|---|
| portDescription | 'SAC Security' |

| Name | e | Last Run Status |
|---|---|---|
| Add SNMP com | | |
| Copy running c | 20:38:06 | SUCCEEDED |
| Delete SNMP c | | |
| Port descriptio | | |
| Port down | | |
| Port up | 00:12:42 | SUCCEEDED |
| Port VLAN | | |
| Reset port stat | 20:03:14 | FAILED |
| Set Port Down | 00:06:18 | FAILED |
| Set sysContact | 21:20:29 | SUCCEEDED |

Figure 400 New Task with 4 Steps

## Delete Tasks

When a task is deleted Entuity also deletes the scheduled jobs and all of their histories.

To delete tasks:

1) Select **Administration** > **Configuration Management.**

2) From the Tasks tab highlight one or more tasks.

3) Click **Delete**.

4) Entuity displays a delete warning dialog and prompts you to confirm the deletion.

# Task Steps

A task is made up of steps. From the Configuration Management Steps tab you can select:

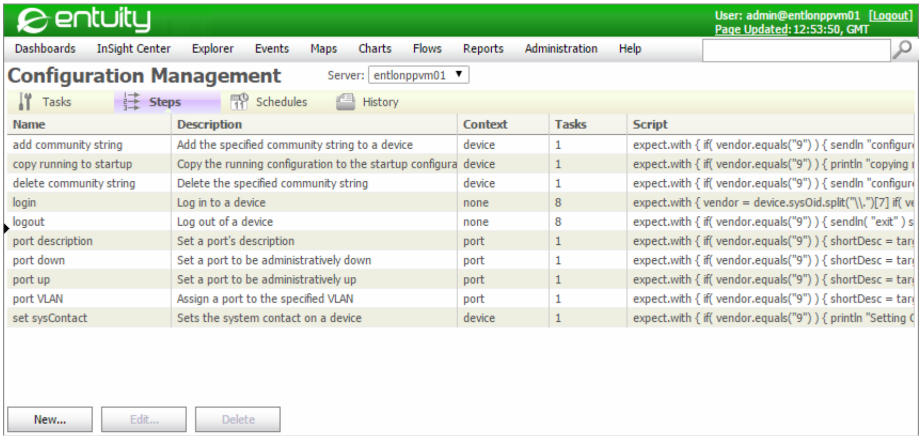
- **New** to define a new step.
- **Edit** to edit an existing step.
- **Delete** to delete a selected step.

The Configuration Management Steps tab lists all of the available steps. You can sort the table on any of the step attributes by clicking on its column heading. Steps can be part of one or more tasks. The *Tasks* column identifies in how many tasks the step is used.

Entuity allows the saving of steps with syntax errors, in part to allow users to save scripts as they are developed. You can still run and schedule invalid tasks but Entuity reports the syntax errors as run time errors in the task's history.

To access a list of available steps:

1) Select **Administration** > **Configuration Management** and then the Steps tab.



| Name | Description | Context | Tasks | Script |
|---|---|---|---|---|
| add community string | Add the specified community string to a device | device | 1 | expect.with { if( vendor.equals("9") ) { sendln "configur |
| copy running to startup | Copy the running configuration to the startup configura | device | 1 | expect.with { if( vendor.equals("9") ) { println "copying |
| delete community string | Delete the specified community string | device | 1 | expect.with { if( vendor.equals("9") ) { sendln "configur |
| login | Log in to a device | none | 8 | expect.with { vendor = device.sysOid.split("\\.")[7] if( ve |
| logout | Log out of a device | none | 8 | expect.with { if( vendor.equals("9") ) { sendln( "exit" ) s |
| port description | Set a port's description | port | 1 | expect.with { if( vendor.equals("9") ) { shortDesc = tar |
| port down | Set a port to be administratively down | port | 1 | expect.with { if( vendor.equals("9") ) { shortDesc = tar |
| port up | Set a port to be administratively up | port | 1 | expect.with { if( vendor.equals("9") ) { shortDesc = tar |
| port VLAN | Assign a port to the specified VLAN | port | 1 | expect.with { if( vendor.equals("9") ) { shortDesc = tar |
| set sysContact | Sets the system contact on a device | device | 1 | expect.with { if( vendor.equals("9") ) { println "Setting C |

Figure 401 Steps Tab

| Attribute | Description |
|---|---|
| *Name* | Unique name (case insensitive comparison) on the selected server |
| *Description* | Optional description of the step. |
| *Context* | If the step *Context* is:<br>■ Device or Port then the step can be used with, respectively, Device and Port tasks.<br>■ None then this step can be used with device and port tasks. |
| *Script* | The entire Groovy script. |
| *Tasks* | Number of tasks using this step. A mouse-over displays a list of tasks using this step. |

Table 82 Step Definition

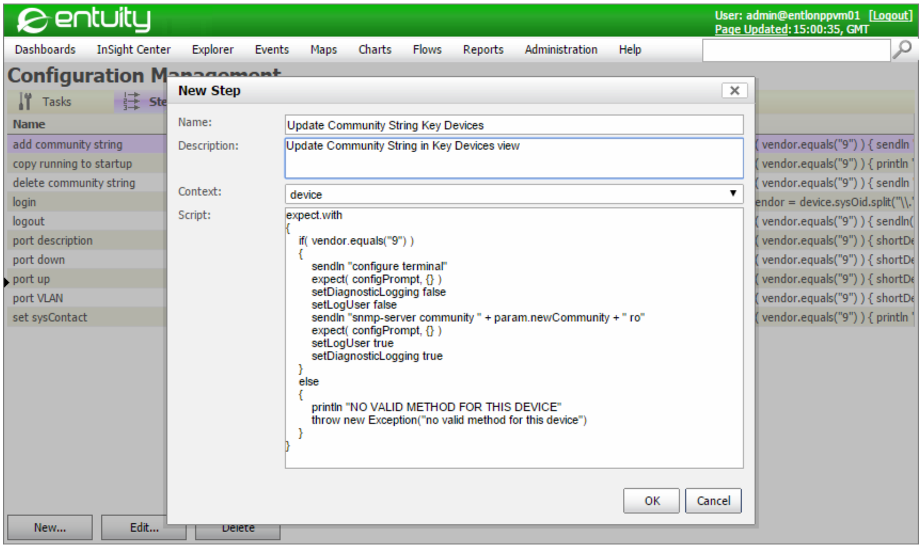
## Create and Edit Steps

To create a step:

1) Select **Administration** > **Configuration Management**.

2) Click **Steps**.

3) Click **New**.



Name: Update Community String Key Devices

Description: Update Community String in Key Devices view

Context: device

Script:

```
expect.with
{
   if( vendor.equals("9") )
   {
      sendln "configure terminal"
      expect( configPrompt, {} )
      setDiagnosticLogging false
      setLogUser false
      sendln "snmp-server community " + param.newCommunity + " ro"
      expect( configPrompt, {} )
      setLogUser true
      setDiagnosticLogging true
   }
   else
   {
      println "NO VALID METHOD FOR THIS DEVICE"
      throw new Exception("no valid method for this device")
   }
}
```

Figure 402 Create Step

| Attribute | Description |
|---|---|
| *Name* | Each step must have a unique name (case insensitive comparison) on the selected server |
| *Description* | Optional description of the step. |
| *Context* | Device is selected by default, other context options are Port and None. If:<br>■ Device or Port are selected then the step can be used with, respectively, Device and Port tasks.<br>■ None is selected then this step can be used with device and port tasks. |
| *Groovy Script* | An example use of Groovy Script would be to associate a step with at least one sysOID, for example:<br>If(device.sysOid.equals(”1.3.6.1.2.1.1.3”))<br>*then do this*<br>else if (device.sysOid.equals(”1.3.6.1.2.1.1.4”))<br>*then do that*<br>In this way a task can be launched on all devices, but certain parts of the scripts will be executed dependent upon the device sysOid. |

Table 83 Step Definition

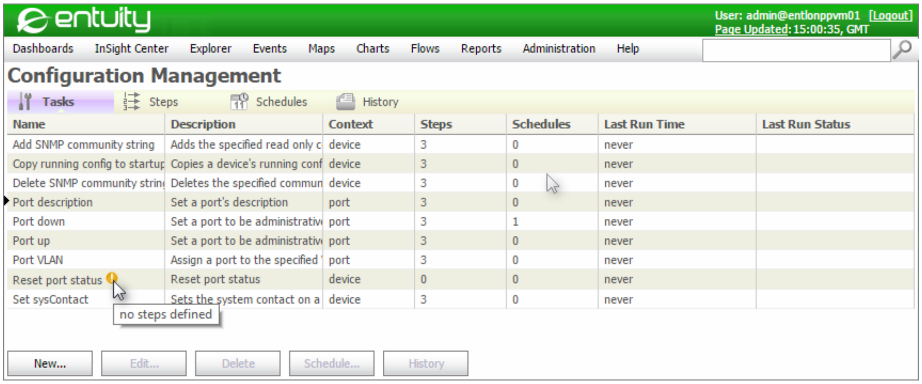
## Delete Steps

When deleting a step Entuity displays a warning message that lists by name any tasks that the step(s) are associated with, and which would therefore be affected by the deletion. Users can continue with or cancel the delete request.

On deleting a step Entuity updates associated tasks by removing that step from the task. Entuity does not delete tasks that no longer contain any steps. However it does identify the tasks as invalid with a warning icon. Entuity also marks as invalid Schedules that call invalid tasks. Entuity can run invalid tasks and schedules.

To delete steps:

1) Select **Administration** > **Configuration Management**.
2) Select the Steps tab and highlight one or more steps.
3) Click **Delete**.
4) Entuity displays a delete warning dialog and prompts you to confirm the deletion.



Configuration Management

| Name | Description | Context | Steps | Schedules | Last Run Time | Last Run Status |
|---|---|---|---|---|---|---|
| Add SNMP community string | Adds the specified read only c | device | 3 | 0 | never | |
| Copy running config to startup | Copies a device's running conf | device | 3 | 0 | never | |
| Delete SNMP community strin | Deletes the specified commun | device | 3 | 0 | never | |
| Port description | Set a port's description | port | 3 | 0 | never | |
| Port down | Set a port to be administrativ | port | 3 | 1 | never | |
| Port up | Set a port to be administrativ | port | 3 | 0 | never | |
| Port VLAN | Assign a port to the specified | port | 3 | 0 | never | |
| Reset port status | Reset port status | device | 0 | 0 | never | |
| Set sysContact | Sets the system contact on a | device | 3 | 0 | never | |

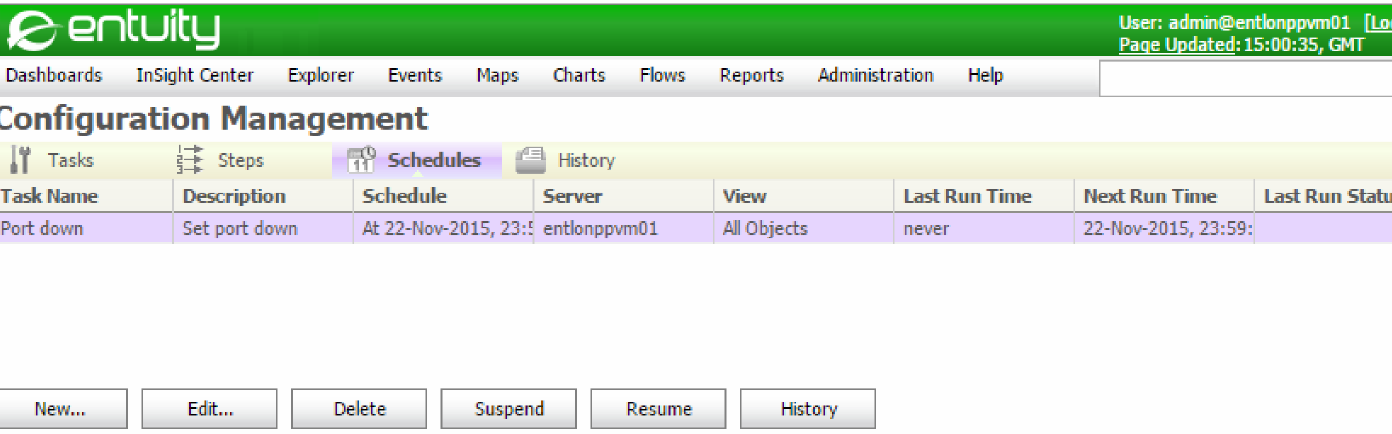
Figure 403 Task without Steps

## Task Schedules

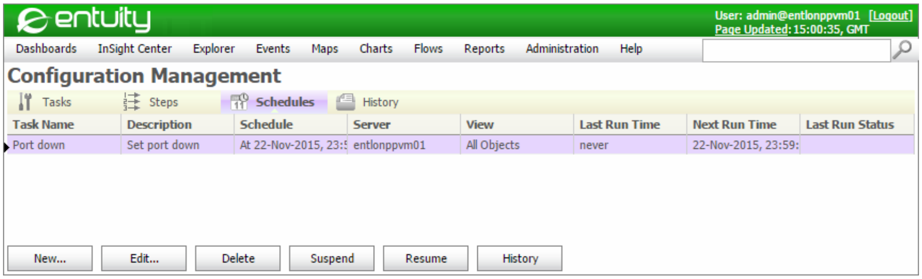
Scheduled jobs are listed in the Schedules tab from where you can:

- Create, edit and delete schedules.
- Suspend and resume scheduled jobs.
- Open the History tab in the context of the selected schedule.

Multiple scheduled jobs for the same task are allowed.



| Task Name | Description | Schedule | Server | View | Last Run Time | Next Run Time | Last Run Statu |
|---|---|---|---|---|---|---|---|
| Port down | Set port down | At 22-Nov-2015, 23:5 | entlonppvm01 | All Objects | never | 22-Nov-2015, 23:59: | |


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 15:00:35, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
Configuration Management
Tasks Steps Schedules History

| Task Name | Description | Schedule | Server | View | Last Run Time | Next Run Time | Last Run Status |
|---|---|---|---|---|---|---|---|
| Port down | Set port down | At 22-Nov-2015, 23:5 | entlonppvm01 | All Objects | never | 22-Nov-2015, 23:59: | |

New... Edit... Delete Suspend Resume History

Figure 404 Schedules Tab

| Attribute | Description |
|---|---|
| *Name* | Task schedule name. |
| *Description* | Description for this scheduled definition. |
| *Schedule* | Details of the schedule. |
| *Server* | Name of the Entuity server on which the schedule is defined. |
| *View* | View against which the schedule is run. |
| *Last Run Time* | Date and time the schedule was last run. |
| *Next Run Time* | Date and time the job is next scheduled to run. |
| *Status* | Status of the last execution; completed/running/suspended. |

Table 84 Schedule Attributes

| Button | Description |
|---|---|
| **Edit** | Select a schedule in the table to amend. Apart from the schedule name all schedule parameters can be amended. |

Table 85 Schedule Actions

| Button | Description |
|---|---|
| **Delete** | Deletes the selected schedule(s). Entuity displays a delete confirmation dialog. |
| **New** | Create schedules. When clicked Entuity displays a list of tasks from which the user can select one to associate with the schedule which they can then define. |
| **Suspend** | You can select one or more schedules and then click **Suspend** to suspend those schedules. |
| **Resume** | You can select one or more suspended schedules and then click **Resume** to resume those schedules. |
| **History** | Click to view the history of the selected schedule, or schedules in the History tab.<br>Entuity retains the task history for 30 days, this includes task jobs ran from both the context menu and scheduler. (See *Task History*.) |

Table 85 Schedule Actions

## Schedule Tasks

To schedule a task:

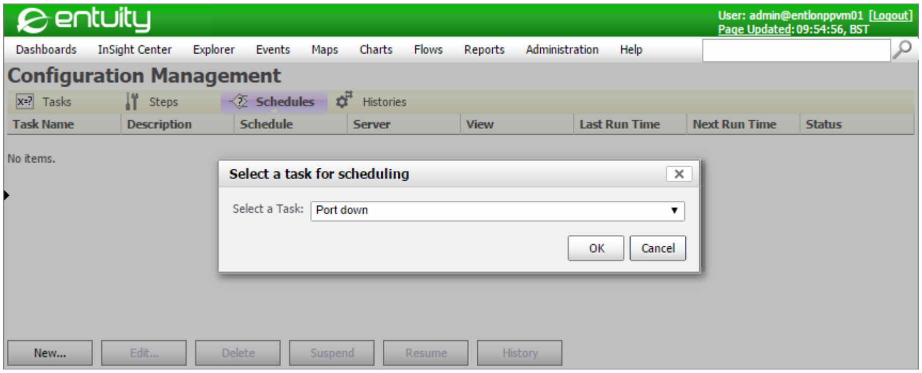
1) Select **Administration** > **Configuration Management**.

2) From the Administration tab highlight a task.

3) Click **Schedule**.

4) Click **New**.

5) Select the task you want to schedule and click **OK**.



User: admin@entlonppvm01 [Logout]
Page Updated: 09:54:56, BST

Configuration Management

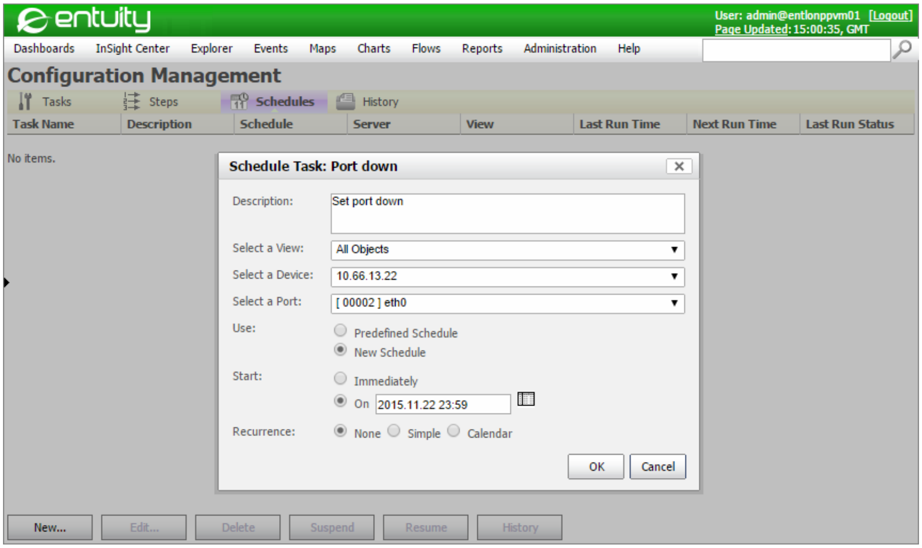
No items.

Select a task for scheduling

Select a Task: Port down

Figure 405 Select a Task to Schedule

6) Define the schedule and click **OK**.



Schedule Task: Port down

Description: Set port down

Select a View: All Objects

Select a Device: 10.66.13.22

Select a Port: [ 00002 ] eth0

Use: ○ Predefined Schedule ● New Schedule

Start: ○ Immediately ● On 2015.11.22 23:59

Recurrence: ● None ○ Simple ○ Calendar

OK Cancel

Figure 406 Schedule Task

| Attribute | Description |
|---|---|
| *Description* | Display name for the scheduled task. |
| *Server* | Only available when the server you have logged into has remote servers. You can select:<br>■ **All Servers** to run the task against the current server and its remote servers. This also places views into consolidate servers mode.<br>■ A single server. |
| *View* | Select a single view. |
| *Device* | If the task *Context* is **device** then you can select an individual device or **All Devices**. |
| *Port* | If the task *Context* is **port** then you can select an individual port or **All Ports**. |
| *Parameters* | Entuity only displays this section if there are parameters (including automatically generated ones) defined in the task. The inputs will be checked against its data type. |
| *Use & Start* | Same as the report scheduler.<br>The recurrence options at the bottom of the dialog should be presented like this:<br>Recurrence: (*) None ( ) Simple ( ) Calendar |

Table 86 Schedule Task

## Delete Schedules

To delete a schedule:

1) Select **Administration** > **Configuration Management**.

2) From the Administration tab highlight one or more schedules.

3) Click **Delete**.

4) Click **Yes** to delete the schedule.

# Task History

Through the task History page Entuity Configuration Management details when a job was run. Each job is a separate row in the task history table. You can highlight a job and then click Details to view a summary of each sub-job. You can drill down further and view the details of the sub-job.

Although the target objects may be on remote servers and the sub-jobs may run on remote servers, the complete history of the task is always stored to the originating server's task history.

By default Entuity retains for 30 days the task history for all run jobs. This is configurable through `entuity.cfg`. (See the *Entuity System Administrator Reference Manual*.) Each night Entuity removes records which are more than 30 days old.

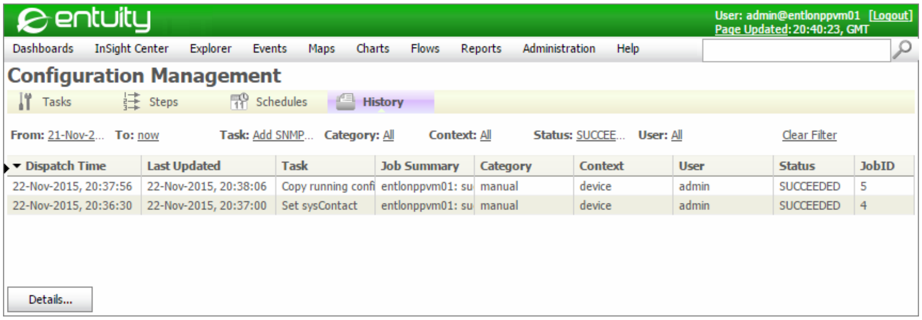
The Task History tab:

- Includes a filter to allow you to focus on the particular tasks in which you are interested.
- Table can be sorted by column, allowing you to order task histories by, for example task, when they ran, on which server they are defined.
- Refreshes every 60 seconds. Entuity also polls every three minutes for the status of current sub-jobs. When drilling down and viewing the progress of sub-jobs Entuity updates sub-job status every 20 seconds.

## Accessing Task History

You can access task history from a number of locations:

- Click **Administration** > **Configuration Management** and click the **History** tab.
- After calling a job from a context menu. When the job is submitted Entuity displays an information dialog that includes a link to the Task History page. When you click on the link it opens the Task History page and displays the newly submitted job (and only that job).
- From the Tasks and Schedules tabs clicking History displays a history of the tasks and scheduled jobs respectively.



User: admin@entlonppvm01 [Logout]
Page Updated: 20:40:23, GMT

Configuration Management

From: 21-Nov-2... To: now Task: Add SNMP... Category: All Context: All Status: SUCCEE... User: All Clear Filter

| Dispatch Time | Last Updated | Task | Job Summary | Category | Context | User | Status | JobID |
|---|---|---|---|---|---|---|---|---|
| 22-Nov-2015, 20:37:56 | 22-Nov-2015, 20:38:06 | Copy running confi | entlonppvm01: su | manual | device | admin | SUCCEEDED | 5 |
| 22-Nov-2015, 20:36:30 | 22-Nov-2015, 20:37:00 | Set sysContact | entlonppvm01: su | manual | device | admin | SUCCEEDED | 4 |

Figure 407 Task History

| Attribute | Description |
|---|---|
| *Server* | Server on which the task is defined. |
| *From* | Time when the job was dispatched to the Script Engine. The job may then be executed or it may be queued. |
| *To* | Time of the last update from a server processing a sub-job associated with the job. Entuity checks on sub-job progress every five minutes. When the job is finished it will also be the time the last sub-job of the job finished executing. |
| *Category* | How the job was initiated. When set to:<br>■ **Manual** - filters in jobs initiated from a context menu.<br>■ **Scheduled** - filters in jobs initiated through a scheduler.<br>■ **All** - filters in jobs initiated through a scheduler or from a context menu. |
| *Task* | Filters in all jobs associated with the selected task or tasks. |
| *Context* | Filters on the target object of the task. When set to:<br>■ **Device -** filters in jobs run against devices.<br>■ **Port** - filters in jobs run against ports.<br>■ **All** - filters in jobs run against ports or devices. |
| *User* | User who ran the task. Select one or more user names. |
| *Status* | Status of the job, i.e. **DISPATCHING**, **QUEUED**, **IN_PROGRESS**, **FAILED**, **SUCCEEDED**. |

Table 87 Task History Filter Attributes

| Attribute | Description |
|---|---|
| *Dispatch Time* | Time when the job was dispatched to the Script Engine. The job may then be executed or it may be queued. |
| *Last Updated* | Time of the last update from a server processing a sub-job associated with the job. Entuity checks on sub-job progress every five minutes. When the job is finished it will also be the time the last sub-job of the job finished executing. |

Table 88 Task History

| Attribute | Description |
|---|---|
| *Category* | Indicates how the job was called:<br>■ **Manual**, called from a context menu.<br>■ **Scheduled**, called through the task scheduler. |
| *Task* | Task name. |
| *Job Summary* | Additional information on the job status, for example details on why a job may have failed. |
| *Context* | Context against which the job is run, i.e. Device or Port. |
| *User* | User who initiated the running of the job. |
| *Status* | Status of the job, i.e. **DISPATCHING**, **IN PROGRESS**, **FAILED**, **SUCCEEDED**. |
| *JobID* | Unique identifier of the run job for that particular Entuity server. This column is hidden by default but can be added to the table through the Config Column dialog. |
| *Server* | Server from which the job was run. This column is hidden by default but can be added to the table through the Config Column dialog. |
| *Targets* | The number of targets (and therefore sub-jobs) of the job. This column is hidden by default but can be added to the table through the Config Column dialog. |

Table 88 Task History

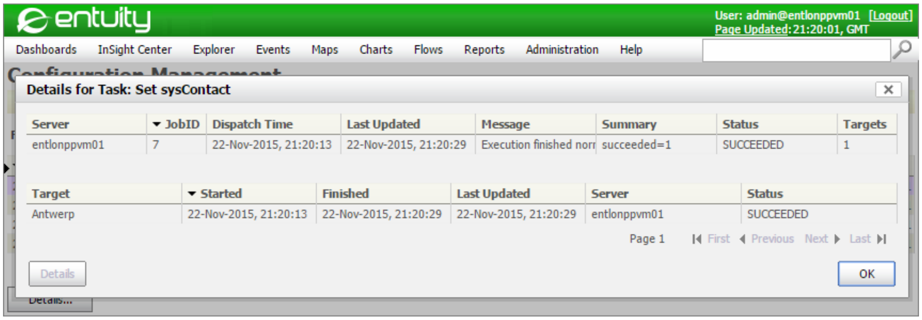
## Job and Sub-Job Details

Each row in the Task History page is a summary of a particular job. Entuity retains the history of each sub-job. To access these details you can:

1) Highlight a row and click **Details**.

   The Details for Task dialog comprises of two tables:

   - Each row of the top table contains a summary of a selected job.
   - Each row of the bottom table shows the sub-jobs associated with the job selected in the top table.
   - Entuity considers a job as failed if one or more of its sub-jobs has failed.



| Server | JobID | Dispatch Time | Last Updated | Message | Summary | Status | Targets |
|---|---|---|---|---|---|---|---|
| entlonppvm01 | 7 | 22-Nov-2015, 21:20:13 | 22-Nov-2015, 21:20:29 | Execution finished norr | succeeded=1 | SUCCEEDED | 1 |

| Target | Started | Finished | Last Updated | Server | Status |
|---|---|---|---|---|---|
| Antwerp | 22-Nov-2015, 21:20:13 | 22-Nov-2015, 21:20:29 | 22-Nov-2015, 21:20:29 | entlonppvm01 | SUCCEEDED |

Figure 408 Job and Sub-Job Details

| Attribute | |
|---|---|
| *Target* | Entuity identifier, for example device display name of the object (device or port) against which the sub-job is run. |
| *Started* | Time the sub-job started. |
| *Finished* | Time the sub-job completed. |
| *Last Updated* | Time of the last update from a server processing a sub-job associated with the job. Entuity checks on sub-job progress every five minutes. When the job is finished it will also be the time the last sub-job of the job finished executing. |
| *Server* | Entuity server on which the sub-job is run. A sub-job is run on the server that manages the target object, i.e. device or port. |
| *Status* | Status of the sub-job, i.e. **IN_PROGRESS**, **FAILED**, **SUCCEEDED**. |
| *Output* | Returned feedback from the interaction. For example:<br>`Server: bvt; View: My Network(admin); Device: e2821; Begin Time: 02-Jul-2015, - 16:21; End Time: 02-Jul-2015, 16:22; Connection Method: auto; [Output/Error:…];`<br>*Output* is available when you select a row and from the context menu click **Show Details**. |
| *Errors* | Details of sub-job failure, for example an error in the Groovy Script or credentials.<br>*Errors* is available when you select a row and from the context menu click **Show Details**. |

Table 89 Sub-Job History

## Check Job Progress

From the Task History page you can view completed and running jobs and their current status. For a running job Entuity updates job status every 10 seconds. Entuity also polls every 10 seconds for the status of current sub-jobs. When drilling down and viewing the progress of sub-jobs Entuity updates sub-job status every 10 seconds.

You can check the progress of a job:

- After manually calling it from a context menu Entuity displays confirmation that the job has been submitted and includes a link to the Task History page from which you can track the progress of the job and its sub-jobs.
- By clicking **Administration > Configuration Management** and then selecting the **History** tab.
- Initiated from a schedule by highlighting the task in the Schedules tab of the Task Administration page and then clicking **History**. Entuity displays the details of the currently running instance of the job or if it is not running then of the last job execution.

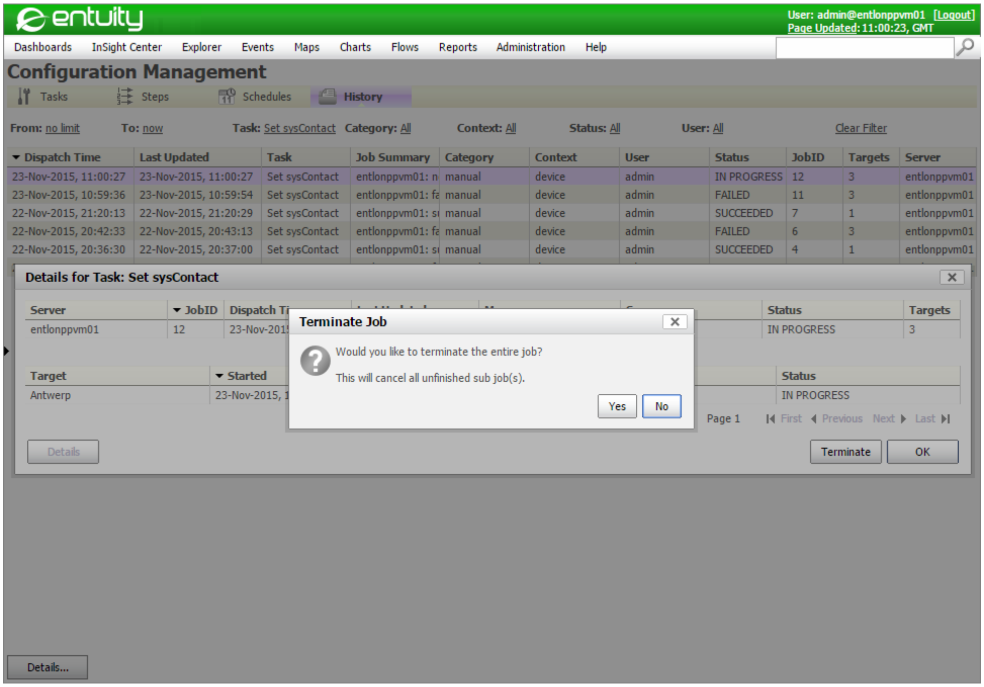
Administrators and users with the Configuration Management permission can view all jobs.

| Job Status | Description |
|---|---|
| **DISPATCHING** | Indicates the dispatch job has been sent to the Script Engine. |
| **QUEUED** | Tomcat has not submitted the tasks due to the number of submitted jobs already reaching the maximum number of permitted concurrent jobs. This count is shared by all users on the local server. Default is 10. |
| **FAILED** | Indicates one or more of the sub-jobs associated to the job have failed. If you terminate a job Entuity also reports this as a failed job. |
| **SUCCEEDED** | Indicates all sub-jobs of the current job have finished. |

Table 90 Task Job Status

To stop a running job:

1) Select **Administration > Configuration Management**.
2) Click **History**.
3) Highlight the job that is in progress and click **Details**.
4) Click **Terminate** to terminate all unfinished sub-jobs of the current job.
5) Click **Yes** to confirm job termination.



From: no limit To: now Task: Set sysContact Category: All Context: All Status: All User: All Clear Filter

| Dispatch Time | Last Updated | Task | Job Summary | Category | Context | User | Status | JobID | Targets | Server |
|---|---|---|---|---|---|---|---|---|---|---|
| 23-Nov-2015, 11:00:27 | 23-Nov-2015, 11:00:27 | Set sysContact | entlonppvm01: n | manual | device | admin | IN PROGRESS | 12 | 3 | entlonppvm01 |
| 23-Nov-2015, 10:59:36 | 23-Nov-2015, 10:59:54 | Set sysContact | entlonppvm01: fa | manual | device | admin | FAILED | 11 | 3 | entlonppvm01 |
| 22-Nov-2015, 21:20:13 | 22-Nov-2015, 21:20:29 | Set sysContact | entlonppvm01: su | manual | device | admin | SUCCEEDED | 7 | 1 | entlonppvm01 |
| 22-Nov-2015, 20:42:33 | 22-Nov-2015, 20:43:13 | Set sysContact | entlonppvm01: fa | manual | device | admin | FAILED | 6 | 3 | entlonppvm01 |
| 22-Nov-2015, 20:36:30 | 22-Nov-2015, 20:37:00 | Set sysContact | entlonppvm01: su | manual | device | admin | SUCCEEDED | 4 | 1 | entlonppvm01 |

Details for Task: Set sysContact

| Server | JobID | Dispatch Ti | Status | Targets |
|---|---|---|---|---|
| entlonppvm01 | 12 | 23-Nov-2015 | IN PROGRESS | 3 |

| Target | Started | Status |
|---|---|---|
| Antwerp | 23-Nov-2015, 1 | IN PROGRESS |

Terminate Job

Would you like to terminate the entire job?

This will cancel all unfinished sub job(s).

Figure 409 Job and Sub-Job Details

| Sub-Job Status | Description |
|---|---|
| **IN PROGRESS** | The sub-job is being executed by Script Engine.<br>Users can click the red cross icon next to an unfinished sub-job to terminate that sub-job. Because of the delay in transmission, the sub-job could actually finish before receiving the termination request. In this case the Script Engine will just ignore the request and return the succeeded/failed status. |
| **QUEUED** | The job is queued by Script Engine. There could be two causes:<br>■ Script Engine allows only one task running per device. So any new tasks on the same device will have to wait for the running task to finish first. This also means if the task is running on multiple ports from the same device, they will actually be executed serially.<br>■ Script Engine also has a `maxConcurrentTask` count which can be overwritten in `script_engine.properties.cfg`. |
| **SUCCEEDED** | All steps of the task have completed successfully. |
| **FAILED** | One of the steps has completed with an error, the remaining steps (if any) for this particular object will not be executed. |
| **DISPATCHING** | Entuity (Tomcat) has submitted the job to Script Engine. |

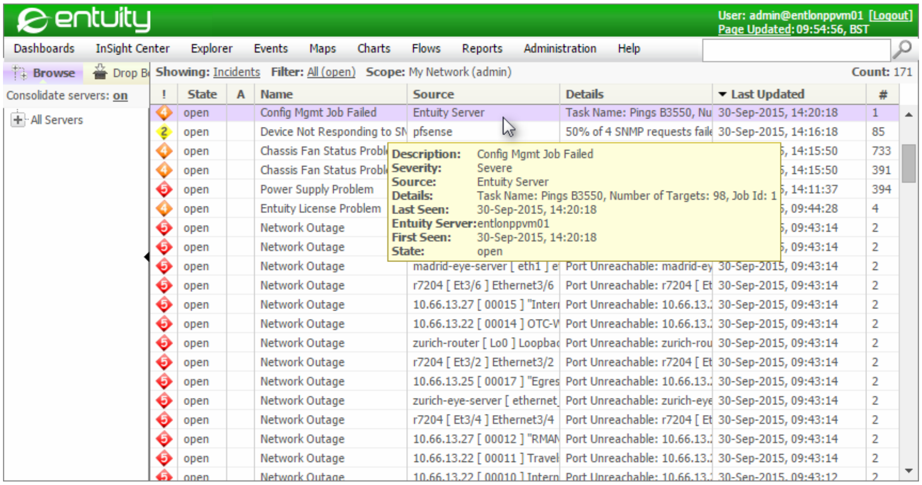
Table 91 Task Sub-Job State

# Configuration Management Events and Incidents

Entuity raises events and incidents against configuration management jobs as they complete, reporting on their failure or success. There are two events:

- Config Mgmt Job Succeeded which indicates the identified job successfully completed and therefore all of its sub-jobs successfully completed.
- Config Mgmt Job Failed which indicates one or more of the sub-jobs associated with the identified job failed. The event details include information on the cause of the job failure.

These two events respectively trigger the Config Mgmt Job Succeeded and Config Mgmt Job Failed incidents.



Showing: Incidents Filter: All (open) Scope: My Network (admin) Count: 171

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| 4 | open | | Config Mgmt Job Failed | Entuity Server | Task Name: Pings B3550, Nu | 30-Sep-2015, 14:20:18 | 1 |
| 2 | open | | Device Not Responding to SN | pfsense | 50% of 4 SNMP requests faile | 30-Sep-2015, 14:16:18 | 85 |
| 4 | open | | Chassis Fan Status Probl | | | 5, 14:15:50 | 733 |
| 4 | open | | Chassis Fan Status Probl | | | 5, 14:15:50 | 391 |
| 5 | open | | Power Supply Problem | | | 5, 14:11:37 | 394 |
| 4 | open | | Entuity License Problem | | | 5, 09:44:28 | 4 |
| 5 | open | | Network Outage | | | 5, 09:43:14 | 2 |
| 5 | open | | Network Outage | | | 5, 09:43:14 | 2 |
| 5 | open | | Network Outage | madrid-eye-server [ eth1 ] e | Port Unreachable: madrid-ey | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | r7204 [ Et3/6 ] Ethernet3/6 | Port Unreachable: r7204 [ Et | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | 10.66.13.27 [ 00015 ] "Interı | Port Unreachable: 10.66.13.: | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | 10.66.13.22 [ 00014 ] OTC-V | Port Unreachable: 10.66.13.: | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | zurich-router [ Lo0 ] Loopbac | Port Unreachable: zurich-rou | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | r7204 [ Et3/2 ] Ethernet3/2 | Port Unreachable: r7204 [ Et | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | 10.66.13.25 [ 00017 ] "Egres | Port Unreachable: 10.66.13.: | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | zurich-eye-server [ ethernet_ | Port Unreachable: zurich-eye | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | r7204 [ Et3/4 ] Ethernet3/4 | Port Unreachable: r7204 [ Et | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | 10.66.13.27 [ 00012 ] "RMAN | Port Unreachable: 10.66.13.: | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | 10.66.13.22 [ 00011 ] Travel | Port Unreachable: 10.66.13.: | 30-Sep-2015, 09:43:14 | 2 |
| 5 | open | | Network Outage | 10.66.13.22 [ 00010 ] Intern | Port Unreachable: 10.66.13.: | 30-Sep-2015, 09:43:12 | 2 |

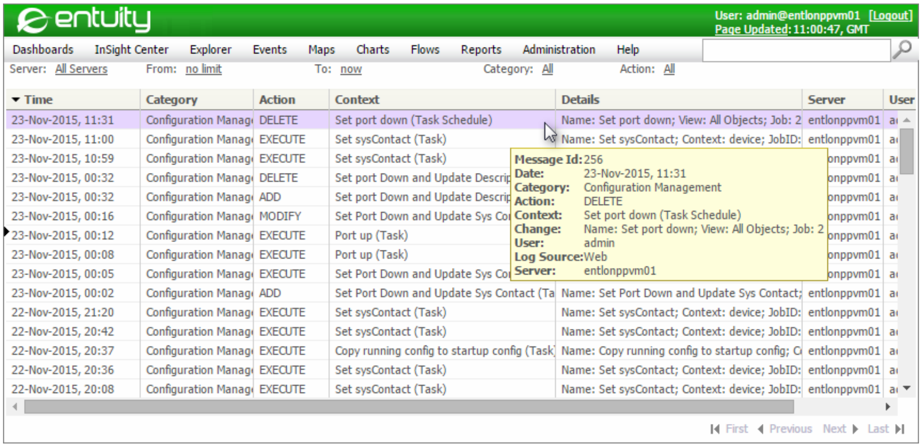
**Description:** Config Mgmt Job Failed
**Severity:** Severe
**Source:** Entuity Server
**Details:** Task Name: Pings B3550, Number of Targets: 98, Job Id: 1
**Last Seen:** 30-Sep-2015, 14:20:18
**Entuity Server:** entlonppvm01
**First Seen:** 30-Sep-2015, 14:20:18
**State:** open

Figure 410 Configuration Management Job Failed Incident

# Configuration Management Audit Log

Configuration Management actions are included in the audit log, specifically:

- Create a task.
- Edit a task and save the changes.
- Delete a task.
- Create a job schedule.
- Edit job schedule and save the changes.
- Delete a Scheduled Job
- Edit/Delete a Step if it is being used by a Task.



User: admin@entlonppvm01 [Logout]
Page Updated: 11:00:47, GMT

Server: All Servers From: no limit To: now Category: All Action: All

| Time | Category | Action | Context | Details | Server | User |
|---|---|---|---|---|---|---|
| 23-Nov-2015, 11:31 | Configuration Manag | DELETE | Set port down (Task Schedule) | Name: Set port down; View: All Objects; Job: 2 | entlonppvm01 | a |
| 23-Nov-2015, 11:00 | Configuration Manag | EXECUTE | Set sysContact (Task) | Name: Set sysContact; Context: device; JobID: | entlonppvm01 | a |
| 23-Nov-2015, 10:59 | Configuration Manag | EXECUTE | Set sysContact (Task) |  | onppvm01 | a |
| 23-Nov-2015, 00:32 | Configuration Manag | DELETE | Set port Down and Update Descrip |  | onppvm01 | a |
| 23-Nov-2015, 00:32 | Configuration Manag | ADD | Set port Down and Update Descrip |  | onppvm01 | a |
| 23-Nov-2015, 00:16 | Configuration Manag | MODIFY | Set Port Down and Update Sys Co |  | onppvm01 | a |
| 23-Nov-2015, 00:12 | Configuration Manag | EXECUTE | Port up (Task) |  | onppvm01 | a |
| 23-Nov-2015, 00:08 | Configuration Manag | EXECUTE | Port up (Task) |  | onppvm01 | a |
| 23-Nov-2015, 00:05 | Configuration Manag | EXECUTE | Set Port Down and Update Sys Co |  | onppvm01 | a |
| 23-Nov-2015, 00:02 | Configuration Manag | ADD | Set Port Down and Update Sys Contact (Ta | Name: Set Port Down and Update Sys Contact; | entlonppvm01 | a |
| 22-Nov-2015, 21:20 | Configuration Manag | EXECUTE | Set sysContact (Task) | Name: Set sysContact; Context: device; JobID: | entlonppvm01 | a |
| 22-Nov-2015, 20:42 | Configuration Manag | EXECUTE | Set sysContact (Task) | Name: Set sysContact; Context: device; JobID: | entlonppvm01 | a |
| 22-Nov-2015, 20:37 | Configuration Manag | EXECUTE | Copy running config to startup config (Task) | Name: Copy running config to startup config; C | entlonppvm01 | a |
| 22-Nov-2015, 20:36 | Configuration Manag | EXECUTE | Set sysContact (Task) | Name: Set sysContact; Context: device; JobID: | entlonppvm01 | a |
| 22-Nov-2015, 20:08 | Configuration Manag | EXECUTE | Set sysContact (Task) | Name: Set sysContact; Context: device; JobID: | entlonppvm01 | a |

**Message Id:** 256
**Date:** 23-Nov-2015, 11:31
**Category:** Configuration Management
**Action:** DELETE
**Context:** Set port down (Task Schedule)
**Change:** Name: Set port down; View: All Objects; Job: 2
**User:** admin
**Log Source:** Web
**Server:** entlonppvm01

Figure 411 Configuration Management Audit Log

# 72 Entuity Data Export

Entuity Data Export allows export of Entuity data from its business management database to a separate user definable target database. By exporting data to a database that contains only the data you require in a structure that you can readily identify, Entuity's data becomes readily available to third party software. For example, Entuity supply integration modules, e.g. Entuity Integration Module for BMC® Atrium™ CMDB, and enhanced reporting functionality that use Data Export.

Where you have multiple Entuity servers installed, more than one server can write to the same database, allowing you to combine data from across your Entuity managed network. You can then directly query and report on this data without having to access Entuity.

Entuity Data Export allows:

- Export of Entuity data to a separate target database, currently the same version of the database as used by the Entuity server (see the *Entuity Getting Started Guide*).
- Users to query, and report on data collected from more than one Entuity server.
- Export to the same database from multiple Entuity servers, and even to the same tables within that database.

Data Export is configured through the web interface. You define the data you want in Dataset Definitions and group these definitions together into scheduled or manually run jobs.

Data Export includes a data reference reporting tool, which you can use to discover details on data gathering to help you appropriately configure data export, for example polling time, polling interval, ageout time.

Entuity recommend the target database is installed to a separate machine to the one to which the Entuity server is installed. This prevents third party tools' usage of the target database impacting the general performance of the Entuity server.

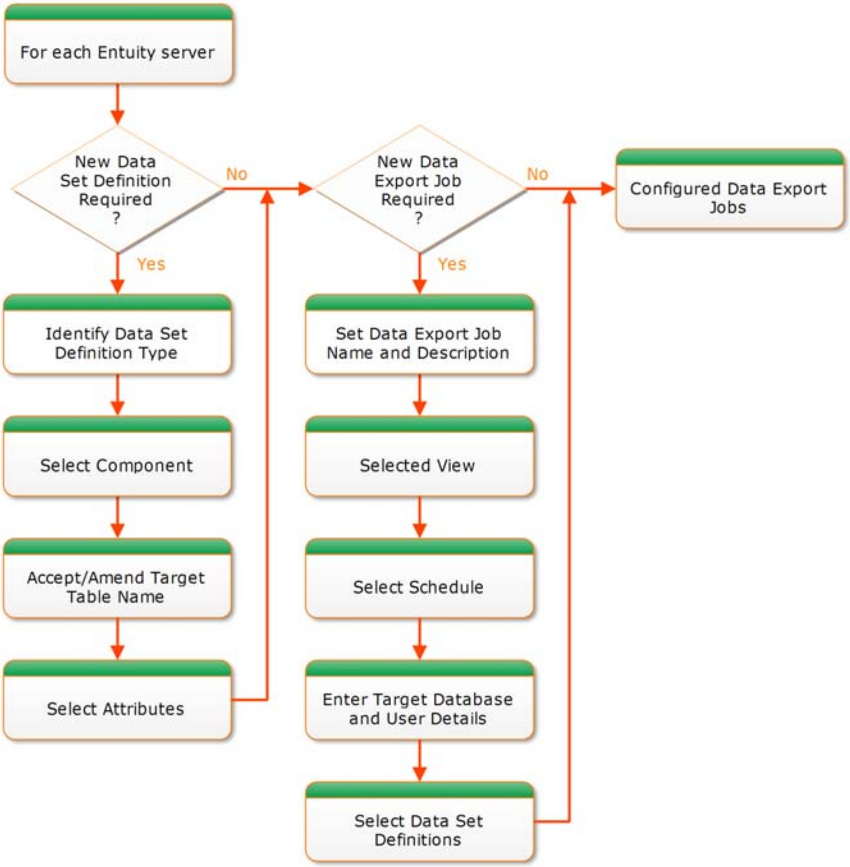

For each Entuity server
New Data Set Definition Required ?
No
Yes
Identify Data Set Definition Type
Select Component
Accept/Amend Target Table Name
Select Attributes
New Data Export Job Required ?
No
Yes
Set Data Export Job Name and Description
Selected View
Select Schedule
Enter Target Database and User Details
Select Data Set Definitions
Configured Data Export Jobs

Figure 412 Entuity Data Export Overview

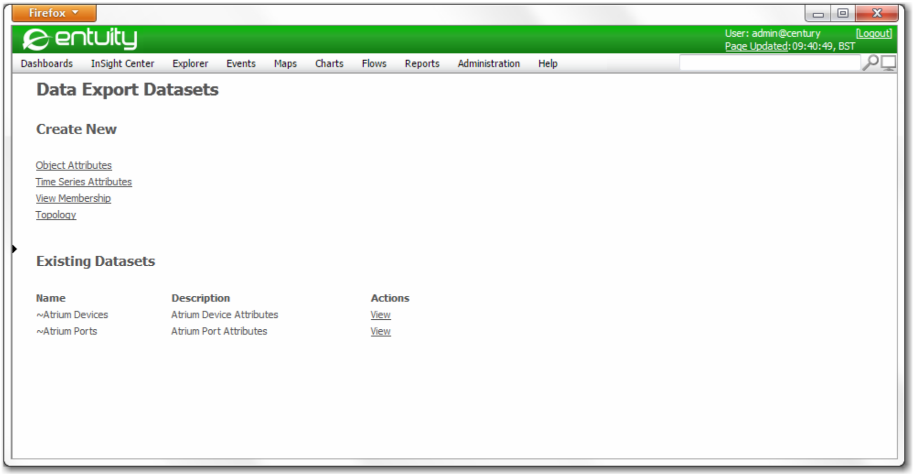
## Data Export Datasets and Definitions

A dataset definition defines the data to extract from the Entuity database. You can then associate one or more dataset definitions with a data export job, which when run exports Entuity data to the target database.

Entuity Data Export includes four types of dataset definitions, each definition type is associated with data structure used by Entuity:

- Object Attributes identifies data for which Entuity does not maintain an historic record, usually attributes which seldom change their value, for example device name, or for which a change history is not required, for example community string.
- Time Series identifies attributes for which Entuity maintains an historic record, for example port utilization data.

- Topology identifies associations between managed Entuity objects.
- View Membership identifies which components are in the selected view. This allows more efficient export of component to view information. For example you could create an Object Attributes Dataset Definition that is configured to collect device details from the All Objects view. You could then create View Membership Dataset Definitions for each view, configured to collect device membership details. This is more efficient than exporting Object Attributes details for each view.



Data Export Datasets

Create New

Object Attributes
Time Series Attributes
View Membership
Topology

Existing Datasets

| Name | Description | Actions |
|---|---|---|
| ~Atrium Devices | Atrium Device Attributes | View |
| ~Atrium Ports | Atrium Port Attributes | View |

Figure 413 Dataset Definitions

The Dataset Definitions page is available from **Administration > Data Export > Datasets**. From this page you can:

- Create new datasets.
- Maintain existing datasets.
- View predefined datasets which are signified with a tilda prefix, e.g. ~Atrium Ports. Those Entuity modules that require Data Export also include predefined datasets for use or as samples that can be copied.

## Target Table and Column Naming

Each dataset definition is exported to one table. Data Export generates the target table name, with a prefix derived from the dataset type and the main body of the name derived from the selected component. For example an object attribute table for an ATM port has the default name `swo_atmPort`.

Each column within the table also has a compound name, the prefix identifies the attribute type and the main body of the name is derived from the underlying attribute name. For example Inbound Speed has the name `swc_portInSpeed`.

You can amend export table names, including removing the default prefix. However, each table can only receive data from one data type so the prefix performs a useful function in identifying the data type. You cannot amend the default attribute names.

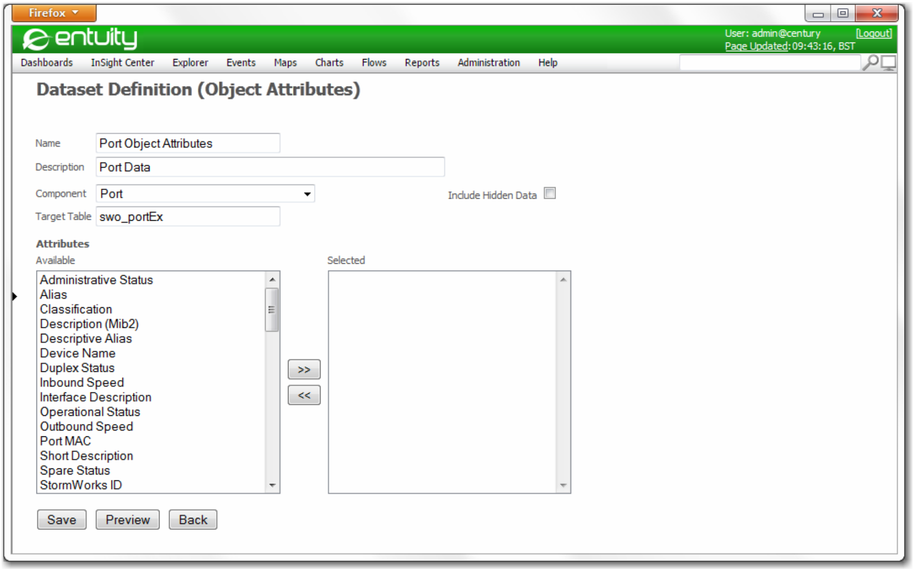
| Prefix | Description |
|---|---|
| *swo_* | Default prefix for tables holding object attribute data. |
| *swt_* | Default prefix for tables holding topology data. |
| *swv_* | Default prefix for tables holding view membership data. |
| *sws_* | Default prefix for tables holding time series attribute data. |
| *swc_* | Default prefix for attribute data. |
| *swsc_* | Default prefix for secondary object attribute data. |

Table 92 Table and Column Data Export Prefixes

## Create Object Attribute Datasets

Object Attribute datasets allow for the export of data for which Entuity does not maintain an historic record, e.g. device name, community string, location. This is data Entuity considers is relatively unchanging, and when it does change the requirement to capture that change within the system is not considered of high value.

By default Entuity displays those attributes likely to be of most interest to you and hides the rest.



Dataset Definition (Object Attributes)

Name: Port Object Attributes

Description: Port Data

Component: Port

Include Hidden Data □

Target Table: swo_portEx

Attributes

Available:
Administrative Status
Alias
Classification
Description (Mib2)
Descriptive Alias
Device Name
Duplex Status
Inbound Speed
Interface Description
Operational Status
Outbound Speed
Port MAC
Short Description
Spare Status
StormWorks ID

Selected:

Figure 414 Object Attribute Dataset Definition

### Object Attribute Dataset Definitions

| Attribute | Description |
|---|---|
| *Name* | Unique name for the Dataset Definition. |
| *Description* | Here should be entered a meaningful Dataset Definition description. This is displayed in the web interface. |
| *Component* | List of StormWorks component types. This is the same list as shown in Flex Reports, and by default does not show hidden components. Display names are used, e.g. DeviceEx is displayed as Device, PortEx as Port. |
| *Include Hidden Data* | Displays data usually hidden from Data Export. By default Data Export, and Flex Reports, only display those dataset objects and attributes that are considered of most interest for network management.<br>By including hidden data you can view the whole Entuity database, however much of the tables and attributes are only used by Entuity when managing the network. |
| *Target Table* | Entuity Data Export derives a name using the dataset definition type and the component name. sw_o_, is prefixed for object data.<br>For example with the component type Port being exported as object data, Entuity generates a default name of swo_PortEx (as it uses the real name of the component and not the display name). You can amend this default table name. |
| *Attributes* | List that includes:<br>■ Attributes of that component<br>■ Attributes of component types to which the component has a one-to-one association<br>■ Attributes of component types that it has a one-to-many association, where the selected component type is the 'one'. For example when you select the Port component Entuity also displays the attributes of its device<br>Attributes of associated component types are clearly identified by prefixing the attribute name with its component type, using the convention (component type) -> attribute name, for example:<br>(Device) -> Serial Number<br>Entuity does not display the StormWorks identifier for the selected component as it is always included to the export. Entuity does display the StormWorks identifier of associated components.<br>*Attributes* is only available with Object, Time Series and Topology dataset definitions. |

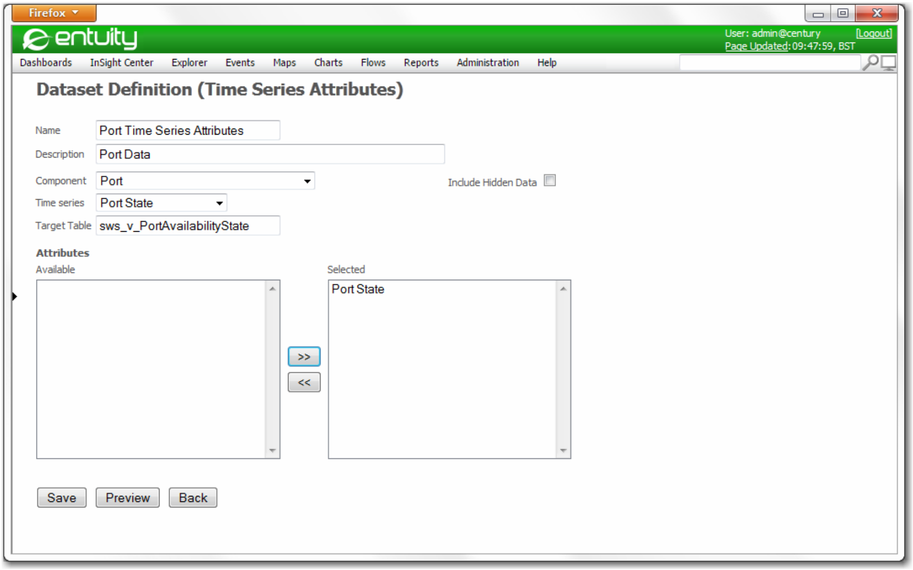
Table 93 Object Attribute Dataset Definition

## Create Time Series Datasets

Time Series datasets allow for the export of data for which Entuity maintains an historic record, e.g. port utilization, latency measures, CPU utilization. This is data Entuity expects to change frequently and considers a history of change to be important.

By default Entuity displays those attributes likely to be of most interest to you, and hides those of less interest. For example, Entuity often converts raw polled data into more meaningful units of measurement.

Entuity polling frequency varies according to the characteristics of the data being polled, e.g. its criticality to system performance, its rate of change. Polled values are rolled up into more manageable chunks, e.g. five minute polled data is rolled up into twenty minute chunks, which can then be rolled up into hourly, then daily. When choosing data to export you should consider the required granularity of that data.



Dataset Definition (Time Series Attributes)

Name: Port Time Series Attributes
Description: Port Data
Component: Port
Include Hidden Data □
Time series: Port State
Target Table: sws_v_PortAvailabilityState

Attributes
Available:
Selected: Port State

Figure 415 Time Series Attribute Dataset Definition

## Time Series Dataset Definitions

| Attribute | Description |
|---|---|
| *Name* | Must be a unique name for the Dataset Definition. |
| *Description* | Should be a meaningful Dataset Definition description. This is displayed in the web interface. |
| *Component* | List of StormWorks component types. This is the same list as shown in Flex Reports, and by default does not show hidden components. Display names are used, e.g. DeviceEx is displayed as Device, PortEx as Port. |

Table 94 Time Series Dataset Definitions

| Attribute | Description |
|---|---|
| *Include Hidden Data* | Displays data usually hidden from Data Export. By default Data Export, and Flex Reports, only display those dataset objects and attributes that are considered of most interest for network management.<br>By including hidden data you can view the whole Entuity database, however much of the tables and attributes are only used by Entuity when managing the network. |
| *Time Series* | List of data types for the selected *Component* for which Entuity maintains an historic record. |
| *Target Table* | Entuity Data Export derives a name from the dataset definition type and the selected *Time Series*, value. For example, where the table name is:<br>sws_v_PortAvailability<br>where:<br>■ sws_v, identifies the table as holding time series data<br>■ PortAvailability identifies the table as holding port availability data.<br>You can amend the table name. |
| *Attributes* | List that includes:<br>■ Attributes of that component<br>■ Attributes of component types to which the component has a one-to-one association<br>■ Attributes of component types that it has a one-to-many association, where the selected component type is the 'one'. For example when you select the Port component Entuity also displays the attributes of its device.<br>Attributes of associated component types are clearly identified by prefixing the attribute name with its component type, using the convention (component type) -> attribute name, for example:<br>(Device) -> Serial Number<br>Entuity does not display the StormWorks identifier for the selected component as it is always included to the export. Entuity does display the StormWorks identifier of associated components. |

Table 94 Time Series Dataset Definitions

# Create Topology Datasets

Topology datasets allow for export of the relationships Entuity has identified between managed objects. Entuity identifies many relationships between objects, by default Data Export displays those relationships likely to be of most interest, e.g. associations between devices, and hides those of less interest, e.g. associations within devices.

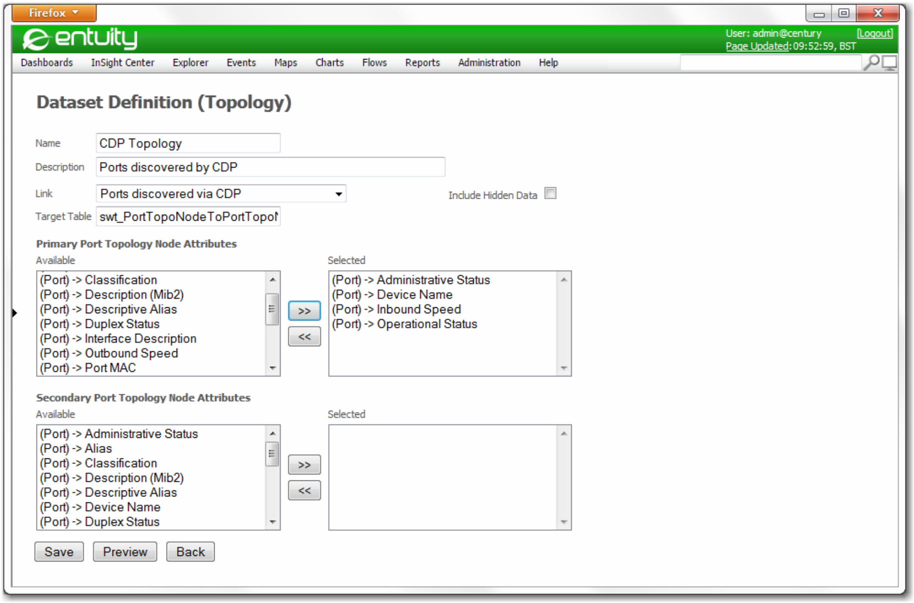
Entuity identifies peering between devices at the interface level, and allows you to select relationships within the context of the technology used to discover the relationship, e.g. Frame Relay, IP peering, CDP.

When you create a topology dataset, you must specify the attributes you want to export for both sides of the relationship. For IP Peering the list of available attributes are those against the:

- Port
- Topology node.

This reflects how Entuity holds the association between the port and its topology node. The peering information is held within the topology node. By default the only information displayed on the topology node is its StormWorks identifier.

Data Export only displays those attributes likely to be of most interest, the rest are hidden.



User: admin@century [Logout]
Page Updated: 09:52:59, BST

Dataset Definition (Topology)

Name: CDP Topology

Description: Ports discovered by CDP

Link: Ports discovered via CDP

Include Hidden Data □

Target Table: swt_PortTopoNodeToPortTopol

Primary Port Topology Node Attributes

Available:
(Port) -> Classification
(Port) -> Description (Mib2)
(Port) -> Descriptive Alias
(Port) -> Duplex Status
(Port) -> Interface Description
(Port) -> Outbound Speed
(Port) -> Port MAC

Selected:
(Port) -> Administrative Status
(Port) -> Device Name
(Port) -> Inbound Speed
(Port) -> Operational Status

Secondary Port Topology Node Attributes

Available:
(Port) -> Administrative Status
(Port) -> Alias
(Port) -> Classification
(Port) -> Description (Mib2)
(Port) -> Descriptive Alias
(Port) -> Device Name
(Port) -> Duplex Status

Selected:

Figure 416 Defining Topology Dataset definitions

## Topology Dataset Definitions

| Attribute | Description |
|---|---|
| *Name* | Unique name for the Topology Dataset Definition. |
| *Description* | Here should be entered a meaningful Dataset Definition description. This is displayed in the web interface. |

Table 95 Topology Dataset Definitions

| Attribute | Description |
|---|---|
| *Link* | List of association types between managed objects Entity can discover. By default Data Export displays associations discovered through different technologies:<br>ATM VCC to ATM VCC, discovered through IP peering<br>ATM VCC to Frame Relay DLCI, discovered through IP Peering<br>Frame Relay DLCI to ATM VCC, discovered through IP Peering<br>Frame Relay DLCI to Frame Relay DLCI, discovered through IP peering<br>Port to Port, discovered through CDP<br>Port to Port, discovered through Spanning Tree<br>Port to Port, discovered through IP peering<br>Port to Port, discovered through uplink detection.<br>By default *Link* does not show hidden components. Display names are used, e.g. DeviceEx is displayed as Device, PortEx as Port. |
| *Include Hidden Data* | Displays data usually hidden from Data Export. By default Data Export only display those links that are considered of most interest for network management.<br>By including hidden data you can view all of the topology associations types available within Entuity, however many of these links are only used by Entuity when managing the network. |
| *Target Table* | Entuity Data Export derives a name using the dataset definition type and the component name. `swt_` identifies the target table as holding topology data. |
| *Primary Attributes* | List of attributes available from the source of the link. |
| *Secondary Attributes* | List of attributes available from the end of the link. |

Table 95 Topology Dataset Definitions

For both *Primary Attributes* and *Secondary Attributes* topology information is held within Entuity within a topology node. For example with a port to port connection, the source port is associated to its node, which is associated to the topology node of the end link, which is associated to its port. By default the only node information displayed is its StormWorks identifier. Of more interest for export purposes is the information on its associated interface.

Attributes of associated component types are clearly identified by prefixing the attribute name with its component type, using the convention (component type) -> attribute name, for example:

```
(port) -> Serial Number
```

Entuity does not display the StormWorks identifier for the selected component. as it is always included to the export. Entuity does display the StormWorks identifier of associated components.

## View Membership Datasets and Optimizing Data Export

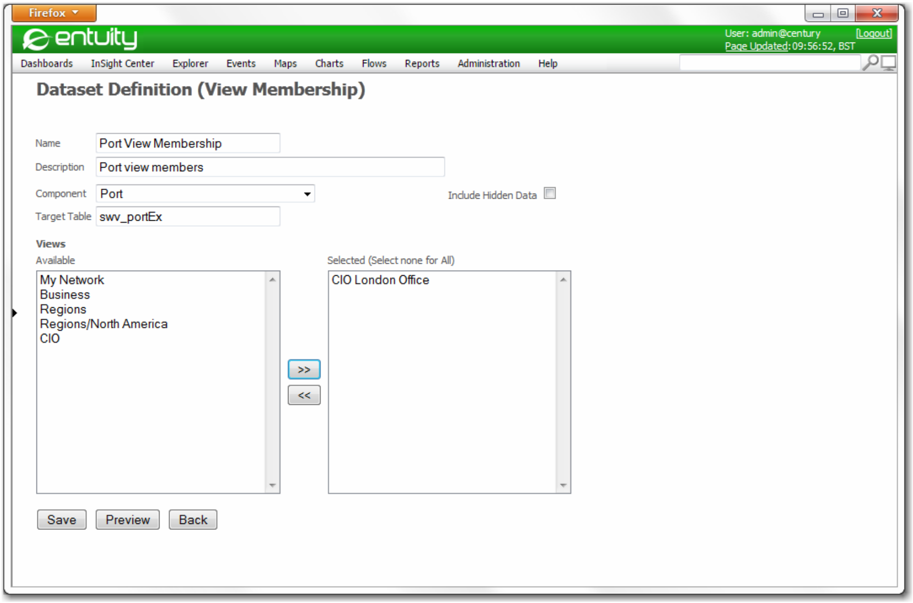
Export of View Membership data identifies which components are in the selected view, allowing more efficient export of component to view information. For example you could:

1) Create an Object Attributes Dataset Definition that is configured to collect device details from the All Objects view.

2) Create View Membership Dataset Definitions for each view configured to collect device membership details.

This is more efficient than exporting Object Attributes details for each view.

To identify a view in the exported table Entuity uses its full path and not just its name. For example the London and New York views each may have a sub-view called Routers, in the export table they are identified as **London**/**Routers** and **New York**/**Routers**.



Dataset Definition (View Membership)

Name: Port View Membership

Description: Port view members

Component: Port

Include Hidden Data ☐

Target Table: swv_portEx

Views

Available:
My Network
Business
Regions
Regions/North America
CIO

Selected (Select none for All):
CIO London Office

Figure 417 View membership Dataset Definition

## View Membership Dataset Definitions

| Attribute | Description |
|---|---|
| *Name* | Text box, in which must be entered a unique name for the Dataset Definition. |
| *Description* | Here should be entered a meaningful Dataset Definition description. This is displayed in the web interface. |
| *Component* | List of StormWorks component types. This is the same list as shown in Flex Reports, and by default does not show hidden components. Display names are used, e.g. DeviceEx is displayed as Device, PortEx as Port. |

Table 96 View membership Dataset Definition

| Attribute | Description |
|---|---|
| *Target Table* | Entuity Data Export derives a name using the dataset definition type and the component name. swv_, for view membership. |
| *Views* | List that includes available and selected Views. |

Table 96 View membership Dataset Definition

## Exporting Port Data Example

1) Click **Administration** > **Data Export** > **Datasets**.

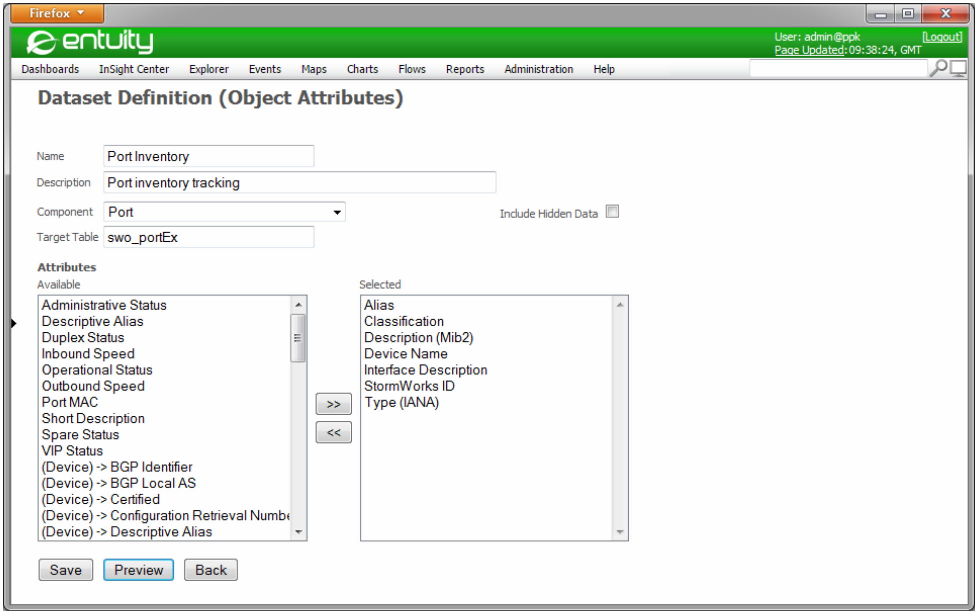
2) Click **Object Attributes**. Entuity displays the Dataset Definition (Object Attributes) page.

3) Enter a meaningful name, description and select from *Component*, **Port**. Entuity defaults a Target Table name and displays a list of available port attributes.

4) From *Attributes* select the required attributes to export. You can:

- Highlight the attribute in the left column and then use the direction keys to move the attributes to the right column.
- Double-click on the attribute.
- Standard multi-select options are available (mouse and control/shift key combinations).

Attribute order does not reflect the final database table column order.



Dataset Definition (Object Attributes)

Name: Port Inventory

Description: Port inventory tracking

Component: Port

Include Hidden Data □

Target Table: swo_portEx

Attributes

Available:
Administrative Status
Descriptive Alias
Duplex Status
Inbound Speed
Operational Status
Outbound Speed
Port MAC
Short Description
Spare Status
VIP Status
(Device) -> BGP Identifier
(Device) -> BGP Local AS
(Device) -> Certified
(Device) -> Configuration Retrieval Numb
(Device) -> Descriptive Alias

Selected:
Alias
Classification
Description (Mib2)
Device Name
Interface Description
StormWorks ID
Type (IANA)

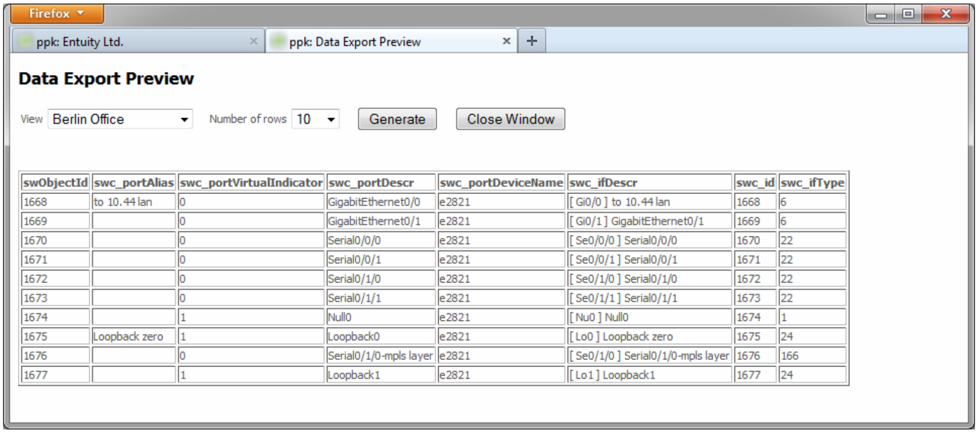
Figure 418 Example Object Attribute Dataset Definition

5) Click **Preview**. Entuity displays the Data Export Preview page in a new Window. This shows the structure of the data export but does not contain any data.

6) Select:

- A view, ideally one with a small number of devices so the preview runs quickly
- The number of rows to display.
- **Generate**. Entuity displays the data that meets the dataset definition for that view.

Alternate between the two windows until you have the required data structure.



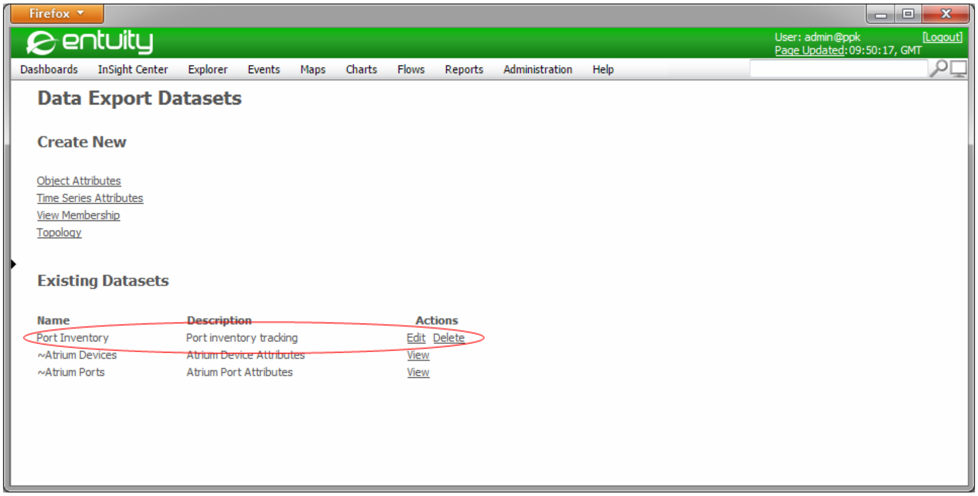
Data Export Preview

View: Berlin Office
Number of rows: 10

| swObjectId | swc_portAlias | swc_portVirtualIndicator | swc_portDescr | swc_portDeviceName | swc_ifDescr | swc_id | swc_ifType |
|---|---|---|---|---|---|---|---|
| 1668 | to 10.44 lan | 0 | GigabitEthernet0/0 | e2821 | [ Gi0/0 ] to 10.44 lan | 1668 | 6 |
| 1669 |  | 0 | GigabitEthernet0/1 | e2821 | [ Gi0/1 ] GigabitEthernet0/1 | 1669 | 6 |
| 1670 |  | 0 | Serial0/0/0 | e2821 | [ Se0/0/0 ] Serial0/0/0 | 1670 | 22 |
| 1671 |  | 0 | Serial0/0/1 | e2821 | [ Se0/0/1 ] Serial0/0/1 | 1671 | 22 |
| 1672 |  | 0 | Serial0/1/0 | e2821 | [ Se0/1/0 ] Serial0/1/0 | 1672 | 22 |
| 1673 |  | 0 | Serial0/1/1 | e2821 | [ Se0/1/1 ] Serial0/1/1 | 1673 | 22 |
| 1674 |  | 1 | Null0 | e2821 | [ Nu0 ] Null0 | 1674 | 1 |
| 1675 | Loopback zero | 1 | Loopback0 | e2821 | [ Lo0 ] Loopback zero | 1675 | 24 |
| 1676 |  | 0 | Serial0/1/0-mpls layer | e2821 | [ Se0/1/0 ] Serial0/1/0-mpls layer | 1676 | 166 |
| 1677 |  | 1 | Loopback1 | e2821 | [ Lo1 ] Loopback1 | 1677 | 24 |

Figure 419 Generated Data Export Preview

7) Click **Save**. Entuity saves the new dataset definition and adds it to the list of existing datasets. You can now associate the definition with a Data Export job.



User: admin@ppk [Logout]
Page Updated: 09:50:17, GMT

Data Export Datasets

Create New

Object Attributes
Time Series Attributes
View Membership
Topology

Existing Datasets

| Name | Description | Actions |
|---|---|---|
| Port Inventory | Port inventory tracking | Edit Delete |
| ~Atrium Devices | Atrium Device Attributes | View |
| ~Atrium Ports | Atrium Port Attributes | View |

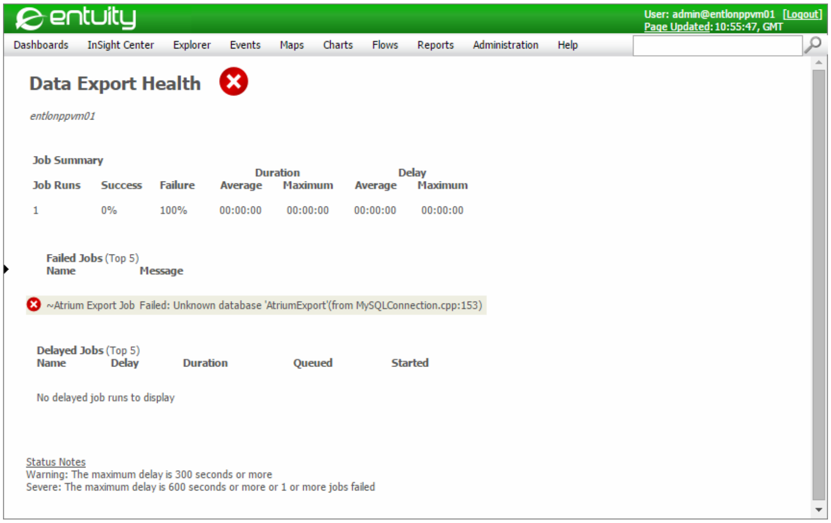
Figure 420 New Dataset Added to Existing Datasets List

# 73 Check on Data Export Health

From the Entuity Data Export Health page you can monitor the performance of the data export module. It delivers both a summary of overall data export performance, two TopN tables one that lists the top five failing data export jobs and the second the most delayed data export jobs. Entuity Data Export metrics are calculated for the previous 24 hour period, the stat point of which is the time at which the page is loaded.

To check the performance of the Entuity Data Export:

1) Click **Administration** > **Entuity Health** > **Data Export Health**. Entuity displays the Data Export Health page.



Data Export Health ✗

*entlonppvm01*

Job Summary

| | | | Duration | | Delay | |
|---|---|---|---|---|---|---|
| Job Runs | Success | Failure | Average | Maximum | Average | Maximum |
| 1 | 0% | 100% | 00:00:00 | 00:00:00 | 00:00:00 | 00:00:00 |

Failed Jobs (Top 5)

| Name | Message |
|---|---|
| ✗ ~Atrium Export Job | Failed: Unknown database 'AtriumExport'(from MySQLConnection.cpp:153) |

Delayed Jobs (Top 5)

| Name | Delay | Duration | Queued | Started |
|---|---|---|---|---|

No delayed job runs to display

Status Notes
Warning: The maximum delay is 300 seconds or more
Severe: The maximum delay is 600 seconds or more or 1 or more jobs failed

Figure 421 Entuity Data Export Health

The Overall Status indicator provides summary state of Entuity data export performance. You can move your mouse pointer over the icon to reveal a tooltip summary of the state.

| Status | Description |
|---|---|
| ✓ *OK* | Performance is within acceptable boundaries. |
| ! *Warning* | Maximum delay is greater than five minutes. |
| ✗ *Severe* | Maximum delay is greater than ten minutes, or one or more jobs failed to complete. |

Table 97 Overall Status Indicator

The Job Summary table includes the total number of export jobs run over the previous 24 hours, including both scheduled and manually generated. It also includes a percentage breakdown of the success and failure of those export jobs. You can reference the Failed Jobs table to see the most recent failures, or review the export history of an individual job.

| Attribute | Description |
|---|---|
| *Job Runs* | Total number of data export jobs run. |
| *Success* | Percentage of successfully completed data export jobs. |
| *Failure* | Percentage of data export that failed to complete. |
| *Average Duration* | Average time taken to successfully complete data export jobs. |
| *Maximum Duration* | Maximum time taken to successfully complete data export jobs. |
| *Average Delay* | Average time delay between when a scheduled data export job was intended to run and when Entuity started to run the data export job that would successfully complete. |
| *Maximum Delay* | Maximum time delay between when a scheduled data export job was intended to run and when Entuity started to run the data export job that would successfully complete. |

Table 98 Job Summary

The Failed Jobs table lists the top five failing export jobs. You can use the Data Export Job History page to investigate further. (See *Viewing the Data Export Job History*.)

| Attribute | Description |
|---|---|
| *Name* | Name of the data export job. |
| *Message* | Error message generated when the data export job failed. |

Table 99 Failed Jobs Table

The Delayed Jobs table lists for the top five delayed export jobs (sorted by *Delay*). The Status Notes at the foot of the page indicate the warning and severe threshold settings, which by default are:

- Warning: The maximum delay is 300 seconds or more
- Severe: The maximum delay is 600 seconds or more or 1 or more jobs failed.

| Attribute | Description |
|---|---|
| *Name* | Name of the data export job. |
| *Delay* | Time delay between when a scheduled data export job was intended to run and when Entuity started to run the data export job that would successfully complete. |
| *Duration* | *T*ime taken to successfully complete data export jobs. |
| *Queued* | Number of jobs currently queued. |
| *Started* | Time the data export job started. |

Table 100 Delayed Jobs Table

# 74 Target Databases and Export Jobs

Entuity Data Export exports data from its database to the specified target database; the Entuity and target database must be the same version of the database. Entuity Support recommend you first set up the target database and user access permissions, for example from the target database command line, before creating the data export jobs from within Entuity. A data export job includes the necessary connection parameters to access the target database, if you set up the target database first you can test the connection as you configure the data export job.

A data export job also includes any defined export schedule, the selected dataset definitions and the view against which they are applied. The first time Entuity Data Export runs a particular export job it creates the required tables within the target database before populating them. With subsequent runs Entuity Data Export can backfill missing data and remove data that has aged out.

## Manage the Target Database

Entuity recommend the target database is installed to a separate machine to the Entuity server. This target database must be configured to allow the user accounts defined within the Data Export Jobs full access privileges. The Data Export Jobs can create tables and columns within tables, however creation of the target database, and the appropriate user account, is a process external to Entuity.

The user account Entuity uses to access the target database must allow it to:

- Create new tables.
- Amend existing table structures by adding new columns.
- Update existing data within the tables.

The data structure of a table in the Target database is derived from the attributes in the Dataset Definition. When an attribute is removed from a Dataset Definition, subsequent data exports do not include data for that attribute's associated database column. Instead Entuity writes a null value. Data Export does not delete columns from Target database tables.

This section provides an overview for creating a target database, a user account for use with Data Export and adjustment of the authentication protocol. You should always consult the appropriate database documentation.

### Creating a Target Database

Data Export Jobs require that their target database exists before they attempt to export data. To create a database:

1) From the command line login to the database:

```
mysql -h host -u user -p
```

| Attribute | Description |
|---|---|
| *host* | Server name or IP address. |
| *user* | User name. |

Table 101 Creating a Target Database

2) Database prompts you for a password, enter the password.

3) Check that the database you want to create does not already exist:

```
SHOW DATABASES;
```

4) When the required database does not exist, create the database:

```
CREATE DATABASE targetDatabase;
```

5) To exit the database enter:

```
QUIT
```

## Granting Entuity Server Access to the Database

You must configure the target database to accept database connections from Entuity. You can grant permission to Data Export to access the export database using the syntax:

```
grant all on targetDatabase.* to user@address identified by 'password';
```

| Attribute | Description |
|---|---|
| *targetDatabase* | Name of the database to which Entuity exports data |
| *user* | Account name used by Data Export to establish a connection with the target database |

Table 102 Database Access

To add a user for Data Export:

1) Log on to the server hosting the target database.

2) From the bin directory of the database installation using a local connection connect to the database, for example:

```
./mysql -u root -h 127.0.0.1
```

3) Grant permission to the Entuity server to access the *targetDatabase* database. For example, from the prompt enter:

```
grant all on targetDatabase.* to EYEuser@10.44.1.149 identified by 'xyz1234';
```

## Testing Data Export Access

After you have set up the Data Export user account on the target database, and adjusted the authentication protocol, you should test the connection.

From the Entity server you can test the connection, for example from the command line enter:

```
./mysql -uEYEuser -pxyz1234 -h10.44.1.1 -DtargetDatabase -P3306
```

where 10.44.1.1 is the IP address of the remote server.

You can also test the connection from the Data Export Job page:

1) Click **Administration** > **Data Export** > **Jobs**.
2) From the Target Database section of the page enter the database details.
3) Click **Test Connection**. Entuity uses these credentials to test the connection to the database.

| Attribute | Description |
|---|---|
| *Server* | IP address or resolved name of the server. When the target database is installed to the same server as Entuity you should still enter an IP address or resolved name and not enter Localhost. |
| *User Name* | User account granted access to the target database. |
| *DB Name* | Target name. |
| *Password*, | User account password. |

Table 103 Target Database Access

## Data Export Job Definitions

It is through Data Export Jobs that you control what data is exported, where it is exported to and when. A data export job specifies the:

- Datasets to export. A data export job can include one or more dataset definitions.
- View against which the dataset definitions are applied.
- Export schedule, for example whether an export automatically runs every hour, day, week.
- Target database to receive the exported data. The export job definition includes the necessary connection parameters.
- Data management of the target database; through *backfill* how to handle missing data and through *ageout* the amount of data retention.

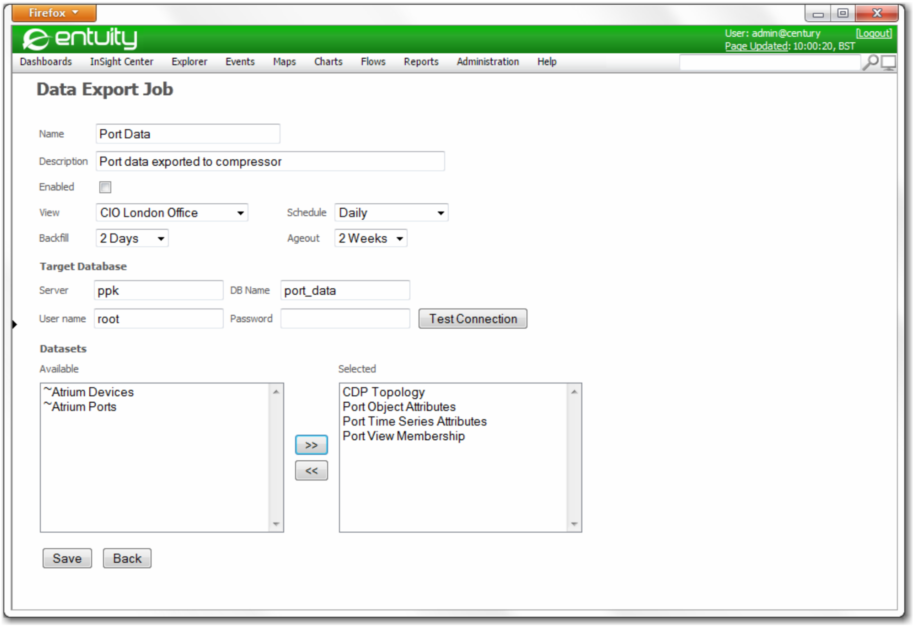
You must separately specify each Data Export Job.

| Attribute | Description |
|---|---|
| *Name* | Must be a unique name for the Data Export Job. Once saved this name cannot be amended. |
| *Description* | Meaningful Data Export Job description which is displayed in the web interface. |

Table 104 Data Export Job Definitions

| Attribute | Description |
|---|---|
| *View* | Entuity view against which the export is run. By selecting **All Views** you can select all available views. |
| *Schedule* | Data export schedule. You can run data export jobs on demand or scheduled.<br>Data Export Job schedules are the same as those used for Flex Reports.<br>When an existing schedule does not meet your requirements use the Flex Report Create Schedule mechanism to create an appropriate one.<br>Entuity only runs one Data Export Job at one time. This avoids resource overload and database conflict. The Data Export queue is separate from other queues, e.g. Flex Reports and a Data Export job can run at the same time. |
| *Backfill* | How far back Entuity should go when attempting to replace missing data in the target database. For example, if a data export job is scheduled to run three hourly but fails to run for a day a backfill value of **2 Days** would allow the data export job to export the missing data. |
| *Ageout* | How long data in the target database should be retained. For example, with an ageout value of **2 weeks**, each time the data export job runs it would delete from the target database data older than two weeks. |
| *Server* | Name of the server on which the database export is hosted. |
| *DB Name* | Name of the export database. |
| *User Name* | User account used to access the export database. |
| *Password* | Password used to access the export database |
| *Datasets* | List of datasets available to be assigned to the data export job. |

Table 104 Data Export Job Definitions



Data Export Job

Name: Port Data

Description: Port data exported to compressor

Enabled: ☐

View: CIO London Office

Schedule: Daily

Backfill: 2 Days

Ageout: 2 Weeks

Target Database

Server: ppk

DB Name: port_data

User name: root

Password:

Datasets

Available:
~Atrium Devices
~Atrium Ports

Selected:
CDP Topology
Port Object Attributes
Port Time Series Attributes
Port View Membership

Figure 422 Dataset Export Job

## Exporting Port Data Jobs Example

1) Click **Administration > Data Export > Jobs**.

2) Click **New Job**. Entuity displays the Data Export Job page.

3) Enter a meaningful name and description.

4) In *View* select the Entuity view against which the export is run. By selecting All Views you can select all available views.

5) In *Schedule* select the data export schedule.

6) Click *Enabled* to allow the report to be scheduled. When not selected you can run the report manually but its schedule is not active and so it is not automatically run.

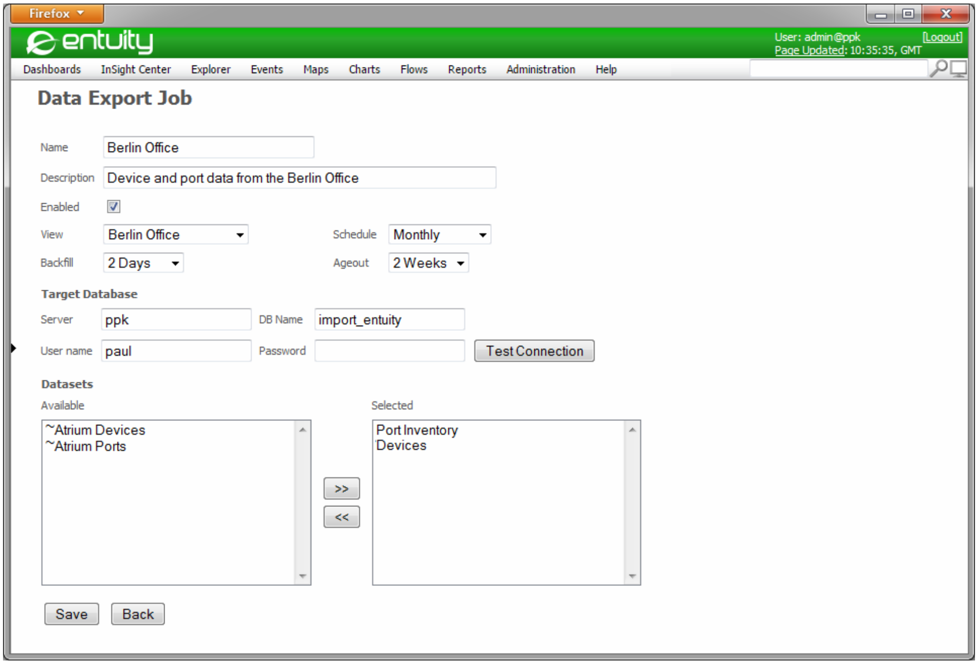
7) In *Backfill* enter a value that relates to the selected schedule. For example, if you have a daily export schedule you may want the capability of a 5 day backfill, i.e. each time the job is run Entuity would insert any missing data, going back up to five days.

8) In *Ageout* select for how long data should be retained in the target database.

9) Specify for the Target Database, *Server*, *DB Name*, *User Name*, and *Password*.

   Click **Test Connection** to test the database connection.

10) Select the *Datasets* to be assigned to the data export job.


Firefox
entuity
User: admin@ppk [Logout]
Page Updated: 10:35:35, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help
>>
<<
Test Connection
Save
Back

## Data Export Job

Name: Berlin Office

Description: Device and port data from the Berlin Office

Enabled: ☑

View: Berlin Office

Schedule: Monthly

Backfill: 2 Days

Ageout: 2 Weeks

**Target Database**

Server: ppk

DB Name: import_entuity

User name: paul

Password:

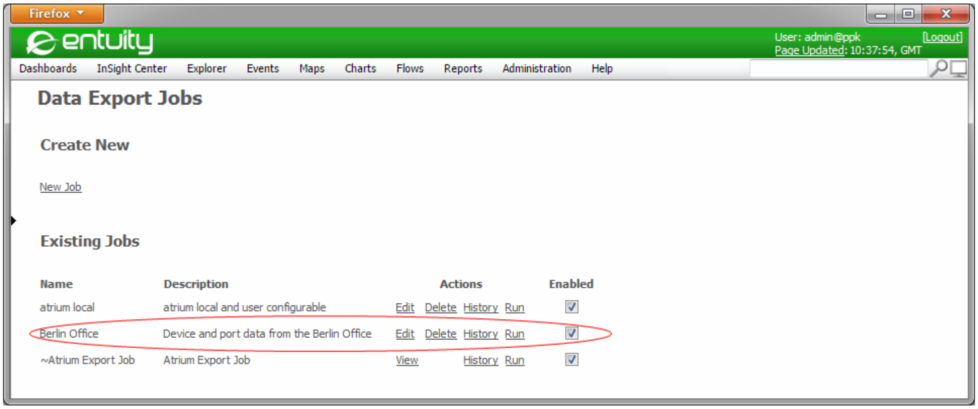
**Datasets**

Available:
~Atrium Devices
~Atrium Ports

Selected:
Port Inventory
Devices

Figure 423 Data Export Job Definition

11) Click **Save**. Only when a Dataset Export Job is saved can it be run.


Firefox
entuity
User: admin@ppk [Logout]
Page Updated: 10:37:54, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Administration Help

## Data Export Jobs

**Create New**

New Job

**Existing Jobs**

| Name | Description | Actions | Enabled |
|---|---|---|---|
| atrium local | atrium local and user configurable | Edit Delete History Run | ☑ |
| Berlin Office | Device and port data from the Berlin Office | Edit Delete History Run | ☑ |
| ~Atrium Export Job | Atrium Export Job | View History Run | ☑ |

Figure 424 Saved Data Export Job

# Export Data From Multiple Entuity Servers

You can configure data export on more than one Entuity server. You can set those servers to export data to the same database, even to the same database tables. Data Export ensures data from different Entuity servers is correctly identified through the `swExportjob` table.

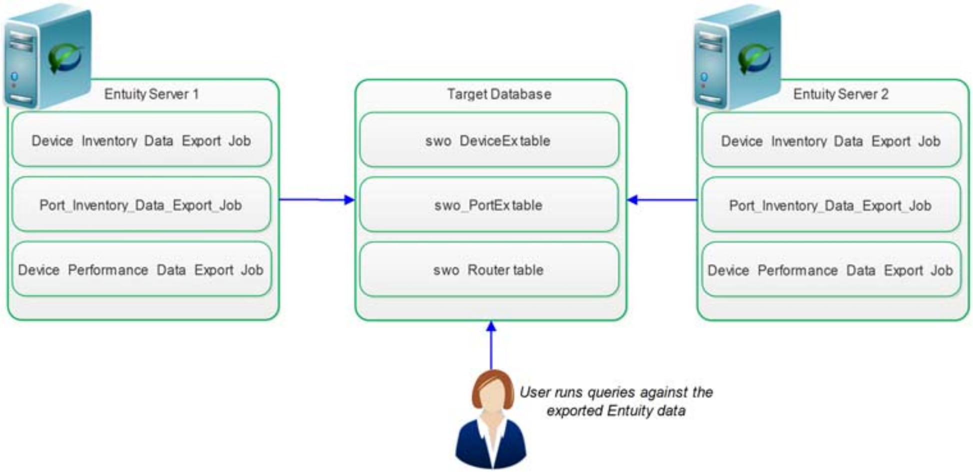

Entuity Server 1
Device Inventory Data Export Job
Port_Inventory_Data_Export_Job
Device Performance Data Export Job
Target Database
swo DeviceExtable
swo_PortExtable
swo Router table
Entuity Server 2
Device Inventory Data Export Job
Port_Inventory_Data_Export_Job
Device Performance Data Export Job
User runs queries against the exported Entuity data

Figure 425 Entuity Data Export Process

`SwExportjob` holds:

- swJobId, unique identifier of each data export job.
- Entuity server name.
- Data Export Job name.

Each exported database table includes a column for each data item that you have specified.

| Attribute | Description |
|---|---|
| *swJobId* | Unique identifier of each data export job. |
| *swObjectId* | Unique internal Entuity identifier for each Entuity component. StormWorks identifiers are unique within each Entuity server.<br>The combination of swJobId and swObjectId uniquely identifies each row of data. |
| *swCreateTime* | Time the row was created |
| *swModifyTime* | Time the row was last amended |
| *swDeleteTime* | Time of the data export during which the component was identified as not present. This maybe because the object has timed out, or has been removed from the view. If Entuity restarts collecting data on the component, the delete time is removed. *SwModifyTime* is updated. |

Table 105 Entuity Data Export Process

Each row within a table contains a record of when that component was created, amended and deleted. Data Export also includes an audit table, from which you can determine when data jobs run, how many updates, how many deletes.

## Viewing the Data Export Job History

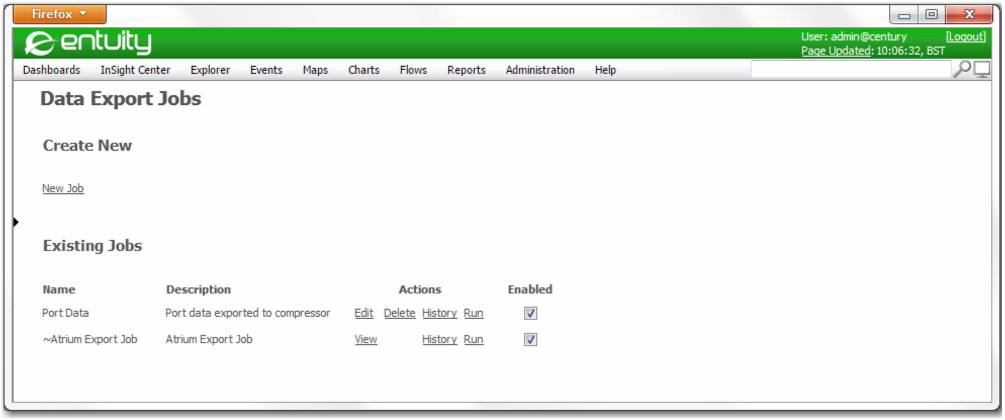
The data export history report provides a detailed breakdown of each time an export job was run. By default the report defaults to show the jobs run over the previous two days, however you can amend the reporting period.

| Attribute | Description |
|---|---|
| *Job Name* | Name of the data export job. |
| *Period* | Reporting period of the report. By default set to 2 days, but selectable periods include 1 hour, 2 hours, 3 hours, 6 hours, 12 hours, 1 day, 2 days 5 days, 1 week, 2 weeks, 1 month, 6 months. You should select a reporting period appropriate to how often the data export job is run. On amending the reporting period Entuity automatically updates the report. |
| *Date* | Date the data export job ran. |
| *Queued* | Time the data export job was scheduled to run. |
| *Started* | Time Entuity started the scheduled data export job. Data export jobs are assigned a priority and only run when there is available processing capacity. |
| *Finished* | Time the data export job completed. |
| *Duration* | Time in seconds from the data export job starting to completing. |
| *Status* | Success or failure of the data export job. |

Table 106 Data Export Job History Report Details

To run the Data Export Job History report:

1) Click **Administration > Data Export > Jobs**. Entuity displays a list of existing jobs.



Data Export Jobs

Create New

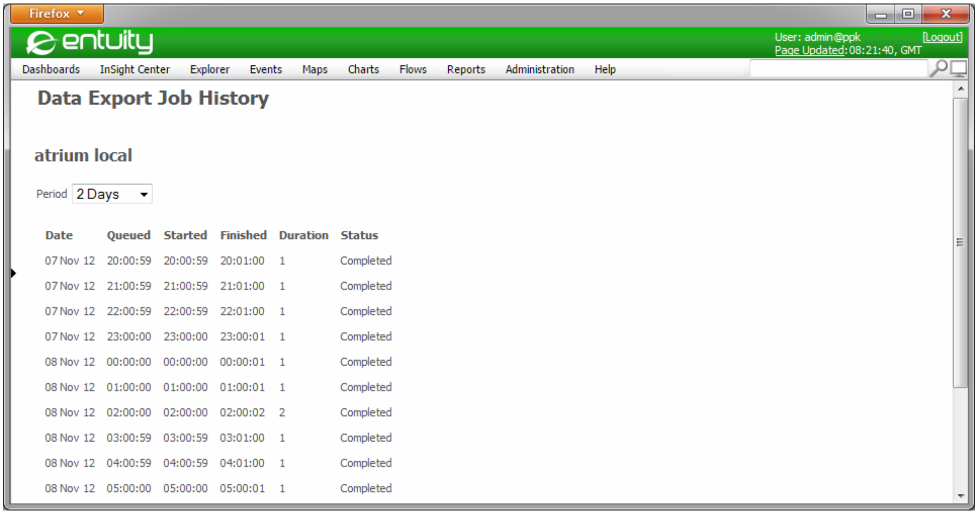
New Job

Existing Jobs

| Name | Description | Actions | Enabled |
|---|---|---|---|
| Port Data | Port data exported to compressor | Edit Delete History Run | ☑ |
| ~Atrium Export Job | Atrium Export Job | View History Run | ☑ |

Figure 426 Data Export Job History

2) Click **History** from the row containing the data export job in which you are interested. Entuity displays the Data Export Job History for the selected job, defaulting to a reporting period of the last two days. Amend *Period* and Entuity automatically updates the report, using the new reporting period.



Data Export Job History

atrium local

Period 2 Days

| Date | Queued | Started | Finished | Duration | Status |
|---|---|---|---|---|---|
| 07 Nov 12 | 20:00:59 | 20:00:59 | 20:01:00 | 1 | Completed |
| 07 Nov 12 | 21:00:59 | 21:00:59 | 21:01:00 | 1 | Completed |
| 07 Nov 12 | 22:00:59 | 22:00:59 | 22:01:00 | 1 | Completed |
| 07 Nov 12 | 23:00:00 | 23:00:00 | 23:00:01 | 1 | Completed |
| 08 Nov 12 | 00:00:00 | 00:00:00 | 00:00:01 | 1 | Completed |
| 08 Nov 12 | 01:00:00 | 01:00:00 | 01:00:01 | 1 | Completed |
| 08 Nov 12 | 02:00:00 | 02:00:00 | 02:00:02 | 2 | Completed |
| 08 Nov 12 | 03:00:59 | 03:00:59 | 03:01:00 | 1 | Completed |
| 08 Nov 12 | 04:00:59 | 04:00:59 | 04:01:00 | 1 | Completed |
| 08 Nov 12 | 05:00:00 | 05:00:00 | 05:00:01 | 1 | Completed |

Figure 427 Data Export Job History

# 75 Entuity HA Compatibility Module

While the availability and performance of every network is mission-critical to its organization, management challenges and business risk increases as networks expand and become decentralized. With Entuity, failover capabilities keep your network management system available protecting mission-critical business service delivery and satisfying even the largest of enterprises.

The Entuity HA Compatibility Module offers a custom agent for Veritas™ Cluster Server (VCS) from the The Carlyle Group on the Microsoft Windows and Linux platforms.

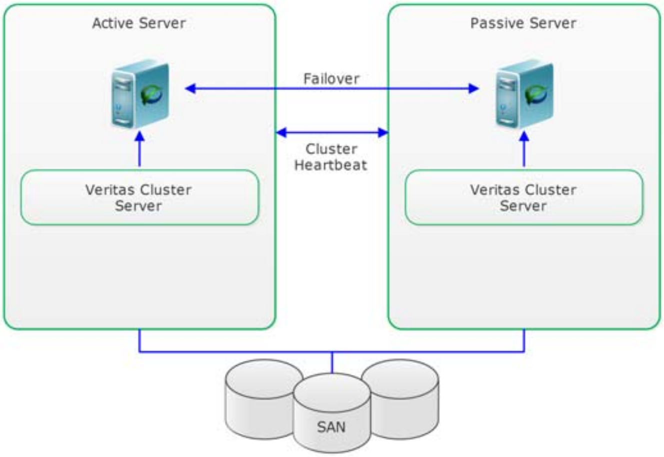


Figure 428 Veritas Cluster Server Configuration

Entuity has also been validated against Neverfail® from Artisan Infrastructure on the Microsoft Windows platform, requiring no additional adapter.

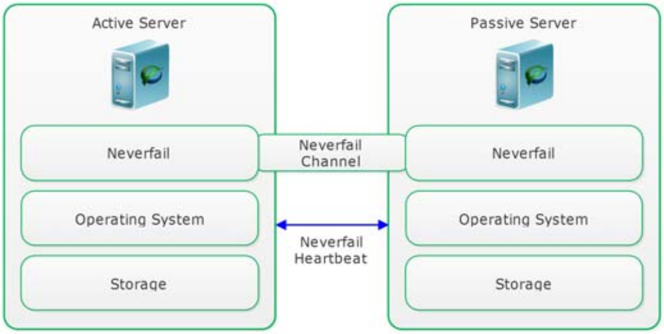


Figure 429 Neverfail Configuration

Both solutions offer a range of capabilities for high-availability to meet a variety of needs and budgets. Both third party software products must be purchased directly from the respective manufacturer and installed separately.

### Licensing

To run this module with VCS you require an appropriate license for each server to which you install Entuity.

For Neverfail a High Availability Compatibility module license is not required. However you will require an Entuity license for each server.

> You must provide your Entuity contact with the host identifier of each server to which you want to install Entuity. The host identifier is used to generate a unique license for each server. (See the *Entuity Getting Started Guide* for licensing details.)

### Availability

Entuity High Availability Compatibility module supports these Veritas applications:

- Veritas Storage Foundation™ and High Availability Solutions 5.1 MP3 for Windows
- Veritas Storage Foundation™ and High Availability Solutions 5.0 MP3 for Linux.

Entuity High Availability Compatibility module supports Neverfail heartbeat 5.5.2153 and Neverfail 6.

## Neverfail Configuration Overview

With Neverfail, high availability of the Entuity server is maintained during a service failure by transferring the Entuity server identity from the primary server to the backup server. The Entuity server identity includes its host identifier, IP address, hostname and all of its registry settings.

When a server has failed and Entuity is running on the backup server, Entuity is unaware that it is now running on a different machine. Neverfail also ensures only one server, initially the primary server and then the backup server, is visible to the network at any one time.

When using Neverfail to deliver High Availability:

1) Neverfail should be installed to its primary and backup servers.
2) Install Entuity to the primary server.
3) Through Neverfail, an exact copy of the Entuity install on the primary server, is made to the backup server.
4) Run Entuity on the primary server.
5) Neverfail intercepts every disk I/O request and sends it to the backup server, where it is also written to the backup server’s hard disk.
6) If the primary server goes down, Neverfail on the backup server detects this failure and:

- Starts Entuity on the backup server. Entuity's startup process ensures the database is valid.
- Ensures that the IP address is swapped to the backup server. This switch is transparent to the user, with the only sign being a short outage period.

## VCS Overview

In a Veritas HA cluster storage is shared (or replicated) and in a failover only the IP address moves between nodes. Therefore, Entuity is configured to use a floating IP address which Veritas moves between machines. The DNS name for this IP address is not the same as the host name of the machine Entuity is running on. All clients will need to be configured to use this floating IP address and all managed devices will also need to be configured to send traps to the floating IP address.

When using VCS to deliver High Availability:

1) VCS should be installed to its primary and backup servers.
2) Provide a separate shared storage area to which both primary and backup servers have access.
3) Install Entuity to shared storage.
4) Configure Entuity on each server to use a common path (e.g. same name location) on the shared storage.
5) Configure the primary and backup VCS servers to:
    - Know about and communicate with each other.
    - Work with the Entuity agent (to startup, monitor, shutdown Entuity).
    - Understand the components that are required on each server for Entuity to work (e.g. access to SAN, Entuity itself).
6) Instruct VCS to start Entuity on the primary server (via their console). VCS uses our agent to start Entuity, and Entuity uses the SAN to store its data.
7) If VCS detects any required Entuity component on the primary server has failed, then it:
    - Shuts down Entuity on the primary server.
    - Ensures that IP and DNS resolution is swapped to the backup server. Users are unawares of the switch (except for a short outage period).
    - Sends a message to the backup server to start Entuity.
8) On the backup server Entuity loads the data from the shared database on the SAN.

## Entuity and VCS High Availability

Veritas Cluster Server (VCS) is high-availability cluster software, which supports all Entuity platforms, i.e. Linux and Microsoft Windows. Entuity HA Compatibility module allows Entuity to take advantage of the VCS application cluster capabilities.

## Before You Start

Before you install and configure Entuity:

- Set Up your VCS Environment.
- Check the Veritas Application.
- Check Your Entuity Licenses.

### Set Up your VCS Environment

Setting up VCS is outside the scope of this document. If you require assistance in implementing Entuity High Availability under VCS, contact Entuity Professional Services.

### Check the Veritas Application

Entuity is verified to work with these versions of Veritas applications:

- Veritas Storage Foundation™ and High Availability Solutions 5.1 for Windows.
- Veritas Storage Foundation™ and High Availability Solutions 5.0 for Linux.

When installing to a different version, the installation and configuration instructions may vary from the example given here.

### Check Your Entuity Licenses

For each node within the cluster that you may potentially have to run Entuity, you must have an Entuity license locally installed to that machine. Entuity licenses are not transferable between servers. For your Entuity supplier to generate a valid license in you must provide the host identifier.

Consult the *Entuity Getting Started Guide* and your Entuity representative when determining your licensing requirements.

## Entuity and VCS Overview

In a Veritas HA cluster storage is shared (or replicated) and in a failover only the IP address moves between nodes. This means that we have to configure Entuity to use a floating IP address which Veritas moves between machines. The DNS name for this IP address will not be the same as the host name of the machine Entuity is running on. All clients will need to be configured to use this floating IP address and all managed devices will also need to be configured to send traps to the floating IP address.

When using VCS to deliver High Availability:

1) VCS should be installed to the primary and backup servers.
2) Provide a separate shared storage area to which both primary and backup servers have access.
3) Install Entuity to the shared storage area.
4) Configure Entuity on both servers to use a common path (e.g. same name location) on the shared storage.
5) Configure the primary and backup VCS servers to:

- Know about and communicate with each other.
- Work with the Entuity agent (to startup, monitor, shutdown Entuity).
- Understand the components that are required on each server for Entuity to work (e.g. access to SAN, Entuity itself).

6) Instruct VCS to start Entuity on the primary server (via the console). VCS uses our agent to start Entuity, and Entuity uses the SAN to store its data.

7) If VCS detects any required Entuity component on the primary server has failed, then it:

   - Shuts down Entuity on the primary server.
   - Ensures that IP and DNS resolution is swapped to the backup server. Users are unawares of the switch (except for a short outage period).
   - Sends a message to the backup server to start Entuity.

8) On the backup server Entuity loads the data from the shared database on the SAN.

### Configuring Entuity Services in Windows

In Windows environments the Entuity server runs through a number of services. Entuity `configure` creates these services, so you must run `configure` on each node in the VCS. In Linux environments services are not created and `configure` only needs to be run on one node in the cluster.

In all environments each node that runs Entuity must have a locally installed Entuity license that is valid on that machine. During `configure` you must also define the host name that has been set up in DNS for the floating IP address.

## Configuring Entuity for Veritas

The instructions for installing and configuring Entuity High Availability are specific to the operating system and the version of Veritas Storage Foundation™ and High Availability Solutions.

### Linux Installation Example

These instructions assume you install to our recommended locations. If these locations are different in your configuration, then substitute the paths appropriately in the following instructions.

| Location | Description |
|---|---|
| *entuity_home*/integ/VCS | Location of the configuration files and scripts to be installed into the Veritas directories and configuration. |
| /opt/VRTSvcs | Location of the Veritas Cluster software. |
| /share/EYE | Location of the Entuity software which is mounted on shared storage accessible from all nodes in the cluster that will be running Entuity. |
| /local/EYE_license | Location of the Entuity license file on each node in the cluster. |

Table 107 VCS Linux Folders

To install and configure Entuity in a Veritas Cluster:

1) Create a directory for the Entuity Veritas agent scripts under /opt/VRTSvcs/bin:

```
cd /opt/VRTSvcs/bin
mkdir EYE
```

2) Create a symbolic link to the Veritas script agent:

```
cd /opt/VRTSvcs/bin/EYE
ln -s ../Script50Agent ./EYEAgent
```

3) Copy the agent scripts to the Entuity agent directory:

```
cd /share/EYE/integ/VCS/
cp online offline monitor clean /opt/VRTSvcs/bin/EYE
```

4) Copy the Entuity type configuration to the Veritas configuration directory

```
cp EYEtypes.cf /etc/VRTSvcs/conf/config
```

5) Indicate to the Veritas cluster that you are about to make a change to the configuration:

```
/opt/VRTSvcs/bin/haconf -makerw
```

6) Add the following line to the file `/etc/VRTSvcs/conf/config/main.cf`

```
include "EYEtypes.cf"
```

7) Edit the file `/etc/VRTSvcs/conf/config/main.cf` and add the Entuity installation to the cluster configuration.

See the example configuration in the file `/share/EYE/integ/VCS/EYEmain.cf`

8) Indicate to the Veritas cluster that you have finished making changes to the configuration.

```
/opt/VRTSvcs/bin/haconf -dump -makero
```

9) Log in to the Veritas GUI process, check the configuration and start Entuity.

### Windows Installation Example

These instructions assume you install to our recommended locations. If these locations are different in your configuration, then substitute the paths appropriately in the following instructions.

| Location | Description |
|---|---|
| *entuity_home*`/integ/VCS` | Location of the configuration files and scripts to be installed into the Veritas directories and configuration. |
| %VCS_HOME% | Location of the Veritas Cluster software. |
| `/share/EYE` | Location of the Entuity software which is mounted on shared storage accessible from all nodes in the cluster that will be running Entuity. |
| `/local/EYE_license` | Location of the Entuity license file on each node in the cluster. |

Table 108 Windows Default Folders

To install and configure Entuity in a Veritas Cluster:

1) Configure Entuity.
2) Run `hostIdent` on each node in the cluster to discover the host identifier, and get a license for each node.
3) Place an Entuity license file on the same path on each node:

   ```
   Copy license.dat C:\local\license.dat
   ```

4) Run `configure` on each node in the cluster.

`configure` is run on each node to ensure that the Entuity services are installed on each node.

5) Create an Entuity directory under %VCS_HOME%\bin:

   ```
   cd %VCS_HOME%\bin
   mkdir EYE
   ```

6) Copy the Veritas script agents dynamic link library into the Entuity directory:

   ```
   cd EYE
   copy ..\default50agent.dll .\EYE.dll
   ```

7) Copy the agent scripts to the agent directory.

   ```
   cd %ENTUITY_HOME%\integ\VCS
   copy online.pl offline.pl monitor.pl %VCS_HOME%\bin\EYE
   ```

8) Copy the Entuity type definition to the Veritas configuration directory.

   ```
   copy EYEtypes.cf %VCS_HOME%\conf\config
   ```

9) Add the following line at the top of the file `%VCS_HOME%\conf\config\main.cf`

   ```
   include "EYEtypes.cf
   ```

10) Edit the `main.cf` file to add the Entuity installation to the cluster.

    See the example configuration in the file *entuity_home*`\integ\VCS\EYEmain.cf`

## Entuity and Neverfail High Availability

Entuity has been validated against Neverfail® Heartbeat 5.5.2153 and Neverfail 6 from Artisan Infrastructure on the Microsoft Windows platform, requiring no additional adapter.

Consult the Neverfail documentation and your Entuity representative before installing Entuity as part of a High Availability solution.

### Overview of the Neverfail Configuration

Neverfail requires two servers, on the primary (active) server Entuity runs and manages the network. On the backup (passive) server Neverfail maintains a copy of the primary server's Entuity install, regularly updating the secondary install with changes in the primary's dynamic data, e.g. reports, database, log files.

Neverfail maintains high availability of the Entuity server during a service failure by transferring the Entuity server identity from the primary server to the backup server. The Entuity server identity includes its IP address, hostname and all registry settings.

Post transfer Entuity is unaware that it is now running on a different machine. Neverfail also ensures only one server, initially the primary server and then the backup server, is visible to the network at any one time.

### Check Your Entuity Licenses

For each server which may potentially have to run Entuity you must have an Entuity license locally installed to that machine. Entuity licenses are not transferable between servers. For your Entuity supplier to generate a valid license you must provide the host identifier.

Consult the *Entuity Getting Started Guide* and your Entuity representative when determining your licensing requirements.

### Neverfail Configuration Process

When using Neverfail to deliver High Availability:

1) The primary and secondary servers should have the same hardware specification. Run a scope report on both machines as part of your pre-installation process.
2) Set up Entuity with a static IP address, which is not assigned from a DHCP server.
3) Ensure the DNS configuration can fully convert this static IP address to a fully qualified name.
4) Neverfail should be installed to its primary and backup servers. Configure Neverfail to exclude the Entuity license file from the duplication process.
5) A third IP address, the Management Client Connection Point, is for the active server to receive pings from the passive server. When Neverfail does not receive a response to the ping, Entuity is considered down.
6) Install Entuity to the primary server, including its license file.
7) Through Neverfail, an exact copy of the Entuity install on the primary server is made to the backup server.
8) Install the backup server's Entuity license.
9) Run Entuity on the primary server.
10) Neverfail intercepts every disk I/O requests and sends it to the backup server, where it is also written to the backup server's hard disk.
11) If the primary server goes down, Neverfail on the backup server detects this failure and:
    - Starts Entuity on the backup server. Entuity's startup process detects that the database on the primary server did not shutdown properly and initiates the database repair process. The larger the database the longer it will take to complete the process during which time Entuity cannot poll for data.
    - Ensures that the IP address and DNS resolution is swapped to the backup server. This switch is transparent to the user, with the only sign being a short outage period.
12) After the installation has been replicated the file system filters should be set to only replicate dynamic data:

- *entuity_home*\Database\data
- *entuity_home*\Database\backup
- *entuity_home*\etc
- *entuity_home*\flowrepos
- *entuity_home*\lib\httpd\EOS\reporting\reports
- *entuity_home*\maps
- *entuity_home*\log\mysqld.error.log (this may be configured to be somewhere other than under *entuity_home*)

✓ The mysqld.error.log file requires replication as it is checked by dbcheck at Entuity startup to determine the state of the database server when it was last shut down.

- *entuity_home*\reports.

# Appendix A Object States

For every network object Entuity manages it identifies and assigns a state. Entuity groups these states, using color coded icons to represent the state. A tooltip available from the icon indicates the underlying cause of the object status.

Entuity uses a combination of methods to identify the object state, for:

- Devices and ports Entuity can use a combination of ICMP ping and SNMP polling to identify their current state. `applicationMonitor` manages ICMP ping as part of the Entuity availability monitor root cause analysis functionality. System administrators can configure `applicationMonitor`, for example to exclude from its monitoring a range of IP addresses.

> If you attempt to exclude the management IP address of a Ping Only device from `applicationMonitor`, Entuity ignores the setting and continues to manage the device through its IP address.

- Applications Entuity uses the response to a TCP connect request.
- Objects that are not polled directly but are part of a managed object, for example a power supply unit, a fan, their object status is derived through SNMP polling of their managed object.

## Object States By State Level

The following tables outline the states Entuity can assign to managed objects. The short description given with each icon is also available as a tooltip.

| Icon | Tooltip / Description |
|---|---|
| ✓ | Ok |
| | The device or port is successfully responding to ICMP ping and SNMP polling, an application successfully responds to a TCP connect request. For objects other than devices and ports, for example applications, extra information about the object state is not retrieved. |
| ✓ | ICMP responding (SNMP disabled) |
| | Device only status. A device managed as ping-only is responding correctly to ICMP ping. |
| ✓ | SNMP responding (ICMP disabled) |
| | Entuity availability monitoring (`applicationMonitor`) excludes the port or device from ICMP ping. The port or device is responding to SNMP polling. |

Table 109 Object States - OK

| Icon | Tooltip / Description |
|---|---|
| ⏸ | ICMP and SNMP disabled |
|  | Device only status. The device has both ICMP ping and SNMP polling disabled:<br>■ It has been set as non-polling by editing its *Poll Status* attribute.<br>■ It is a ping-only device with a management IP address that is outside of the range of IP addresses Entuity availability monitoring (`applicationMonitor`) is configured to ping. (See *Set Up ICMP Monitoring.*) |
| ⏸ | Unmanaged |
|  | Port only status. Entuity is not currently managing the port. An option to remanage the port is available from the context menu. (See *Managing and Unmanaging Ports*.) |

Table 110 Object States - Non-Polling

| Icon | Tooltip / Description |
|---|---|
| ⏻ | Admin down |
|  | Port only status. SNMP polling of the port determines it is set to Admin Down. Entuity considers this an administrative choice and therefore the port is not considered as operationally unavailable; port operational availability is set to 100%. |
| ⏻ | Admin down (ICMP disabled) |
|  | Port only status. Entuity availability monitoring (`applicationMonitor`) excludes the port or device from ICMP ping.<br>SNMP polling of the port determines it is set to Admin Down. Entuity considers this an administrative choice and therefore the port is not considered as operationally unavailable; port operational availability is set to 100%. |

Table 111 Object States - Admin Down

| Icon | Tooltip / Description |
|---|---|
| 🔧 | Pending full object discovery |
|  | This state is usually a temporary state, discovery has started but full discovery of all of its attributes is not complete. |
| 🔧 | Status Not Available |
|  | This state is usually a temporary state, for example a device may have this state after it is taken under Entuity management but before discovery of is attributes. |
| 🔧 | Unrecognized status |
|  | This state is usually a temporary state, assigned when the object state does not meet the conditions for any of the other state categories. |

Table 112 Object States - Uninitialized

| Icon | Tooltip / Description |
|---|---|
| ! | ICMP not responding (not root cause) |
| | The managed object is not responding to ICMP ping, but it is not the root cause. The managed object is responding to SNMP polling. |
| ! | ICMP not responding |
| | The device or port is not responding to ICMP ping, although it did respond to the last SNMP poll. Entuity availability monitoring (`applicationMonitor`) has determined this object to be the root cause of the failure.<br>Entuity assigns a port this state when this set of conditions is met:<br>■ Device that the port is on is responding to ICMP ping and SNMP polling.<br>■ Port does not respond to ICMP ping, for example because of a firewall configuration, and is therefore identified as the root cause. |
| ! | Management IP not responding to ICMP |
| | Device only status. The device management IP address is not responding to ICMP ping but other IP addresses are responding. The device also responds to SNMP polling. |
| ! | Management IP not responding to ICMP (SNMP Disabled) |
| | Device only status. The device management IP address is not responding to ICMP ping but other IP addresses are responding. SNMP polling of the device is disabled. |
| ! | Management IP not responding to ICMP, SNMP not responding |
| | Device only status. The device management IP address is not responding to ICMP ping but other IP addresses are responding. The device is not responding to SNMP polling. |
| ! | SNMP not responding |
| | The device or port is not responding to SNMP polling but it is responding to ICMP ping. |
| ! | Degraded |
| | A managed object is in a degraded state, for example a Frame Relay DLCI. |

Table 113 Object States - Warning

| Icon | Tooltip / Description |
|---|---|
| ✖ | ICMP & SNMP not responding |
| | The device or port is not responding to ICMP ping and SNMP polling. Entuity availability monitoring (`applicationMonitor`) has determined this object to be the root cause of the failure. |
| ✖ | ICMP not responding, root cause (Port Down) |
| | The port is not responding to ICMP ping, although it did respond to the last SNMP poll reporting the port as operationally down. Entuity availability monitoring (`applicationMonitor`) has determined this object to be the root cause of the failure. |

Table 114 Object State - Critical

| Icon | Tooltip / Description |
|---|---|
| ⊗ | ICMP not responding (SNMP disabled) |
| | Device only status. The ping-only device is not responding to ICMP ping, and Entuity availability monitoring (`applicationMonitor`) has determined this object to be the root cause of the failure. |
| ⊗ | Port down |
| | Port only status. Entuity availability monitoring (`applicationMonitor`) excludes the port or device from ICMP ping. SNMP polling of the port determines the port is operationally down. |
| ⊗ | Port down (ICMP disabled) |
| | Port only status. Entuity availability monitoring (`applicationMonitor`) excludes the port or device from ICMP ping. SNMP polling of the port determines the port is operationally down. |
| ⊗ | SNMP not responding (ICMP disabled) |
| | Entuity availability monitoring (`applicationMonitor`) excludes the port or device from ICMP ping. SNMP polling of the port determines the port is operationally down. |
| ⊗ | Down |
| | The managed object is the root cause of the network failure. |

Table 114 Object State - Critical

| Icon | Tooltip / Description |
|---|---|
| ❔ | ICMP & SNMP not responding (not root cause) |
| | The device or port is not responding to ICMP ping and SNMP polling. Entuity availability monitoring (`applicationMonitor`) has determined this object is not the root cause of the failure. |
| ❔ | ICMP not responding (SNMP disabled) |
| | Device only status. A ping-only device is not responding correctly to ICMP ping. Entuity availability monitoring (`applicationMonitor`) identifies this device as not the root cause of the failure. |
| ❔ | Parent down |
| | Entuity has set the application or port to the Unknown state as their parent device is down. |
| ❔ | Parent polling disabled |
| | Entuity has set the application or port to the Unknown state as the parent device has polling disabled. |
| ❔ | Parent unreachable |
| | Entuity has set the application or port to the Unknown state as the parent device is unreachable to Entuity. |

Table 115 Object State - Unknown

| Icon | Tooltip / Description |
|---|---|
| ? | Unable to resolve hostname to IP |
| | Device only status. Entuity cannot resolve the device name to an IP address for a ping-only device. This could indicate an invalid device name or a problem with DNS. |
| ? | Unable to resolve hostname to IP (SNMP disabled) |
| | Device only status. Entuity cannot resolve the device name to an IP address for a ping-only device. This could indicate an invalid device name or a problem with DNS. |
| ? | Unable to resolve hostname to IP (ICMP disabled) |
| | Device only status. Entuity availability monitoring (`applicationMonitor`) excludes the port or device from ICMP ping. Entuity cannot resolve the device name to an IP address for a ping-only device. This could indicate an invalid device name or a problem with DNS. |
| ? | Unknown |
| | The state is not known. This could be because it has not been polled yet or because of failures in the polling process.<br>Device status may be unknown when:<br>■ A device has been added recently, and Entuity (`DSKernelStatic`) has not yet completed creation and population of the associated streams. The amount of time this takes will depend on the size of the install, whether `DSKernelStatic` has recently restarted and how many objects have recently been modified or created.<br>■ Entuity availability monitoring (`applicationMonitor`) has failed.<br>■ Entuity availability monitoring cannot map a monitored IP address to a device. This can happen if a device has been added to the inventory twice. One will have the correct status, and the other will always be shown as Unknown (Entuity can only map an IP address to one device instance at a time). You should delete one of the entries to resolve the issue.<br>Port status may be unknown when:<br>■ A port has been recently added and Entuity has not yet completed creation and population of associated streams. The amount of time this takes depends on the size of the install, whether DSKernelStatic has recently been restarted and how many objects have recently been modified or created.<br>■ The administration status is disabled.<br>■ An SNMP failure has occurred, including authentication or access control issues, preventing Entuity from determining the port state. For example the device is not responding to SNMP, or the port has been removed from the device but discovery has not yet detected this and updated the inventory. As such, SNMP requests for information about the port are unsuccessful. |

Table 115 Object State - Unknown

## Network Path States

| Icon | Tooltip / Description |
|---|---|
| ✓ | Ok |
| | The path is available. |
| ● | Unitialized |
| | This state is usually a temporary state, discovery has started but full discovery of all of its attributes is not complete. |
| ? | Unknown |
| | The state is not known. This could be because the service has not been polled yet or because of failures in the polling process. |
| ! | Impacted |
| | The actual path has changed from the reference path. The service may still be available indicate |
| ✕ | Down |
| | The managed object is the root cause of the network failure. |

Table 116 Network Path States

## Application States

Application states are determined by Entuity monitoring the responses to TCP connect requests against two thresholds:

- Application Timeout threshold determines how long Entuity waits for a response from the application before timing it out. You can set the application timeout threshold through a section in *entuity_home*`\etc\entuity.cfg`:

  ```
  [applicationmonitor]
  ```

  ```
  appTimeout=8
  ```

  Where *appTimeout* defines the system wide application timeout in seconds, by default set to five seconds.

- Application Latency threshold determines how Entuity interprets the time taken to receive a response from the application. You can set threshold levels through the Thresholds page.

| Icon | Tooltip / Description |
|---|---|
| ✓ | Ok |
| | The application is available. |
| ● | Unitialized |
| | This state is usually a temporary state, discovery has started but full discovery of all of its attributes is not complete. |

Table 117 Application States

| Icon | Tooltip / Description |
|---|---|
| ? | Unknown |
|  | If an application does not respond to Entuity within the time frame set by the Application Timeout threshold and is not the root cause. |
| ! | Degraded |
|  | If an application does not respond to Entuity within the time frame set by the Application Latency threshold and is not the root cause of the problem. |
| ✖ | Down |
|  | If an application does not respond to Entuity within the time frame set by the Application Timeout threshold and is the root cause of the problem. |

Table 117 Application States

# Appendix B  Connectivity Discovery Technologies

The network topology delivered through maps is the product of a number of discovery technologies:

- Layer 3:
  - IP Peering
  - Trace Route - Ping State
- Layer 2:
  - Cisco Discovery Protocol - CDP
  - Link Layer Discovery Protocol - LLDP
  - Spanning Tree
  - SynOptics Network Management Protocol - SONMP
  - Physical Address Matching
- Routing (part of the Routing Protocols module):
  - Border Gateway Protocol - BGP
  - Enhanced Interior Gateway Routing Protocol - EIGRP
  - Intermediate System to Intermediate System - IS-IS
  - Open Shortest Path First - OSPF
- Other:
  - Host Detection
  - User Defined Connections
  - Hypervisor Detection
  - IPv6 ND (part of the IPv6 module)
  - VM Detection.

Maps can combine these technologies to provide a clear view of the network topology. This view is limited by your user permissions.

## Discovery and Polling Considerations

When you first install Entuity you would have noticed the incremental nature of its discovery process, for example some device details appear when you can first view the device, but other details are only available after a number of hours, i.e. a number of StormWorks discoveries. By default StormWorks discovery runs every two hours.

Maps operate within this environment, seeing a new device in a map does not mean all of its connectivity is discovered. Similarly changes in network topology are recognized in maps only after discovery has subsequently run and you have refreshed the current map, or opened a new one.

If you define and enable physical connections Entuity then creates the association between the source and destination devices, this creation also uses the discovery process. There will therefore be a delay between defining a connection and Entuity displaying it in a map.

In running StormWorks discovery every two hours Entuity is balancing the reporting of changes in your network topology with the load involved in discovering that information. Discovery is also impacted by the load placed on the server, more objects under management potentially the longer the discovery cycle and the relative priority of those objects. However, changes in device state are likely to be more frequent than changes in network topology, and maps reports these changes in almost realtime. Device and link state are derived from data returned from Entuity polling devices and handling events. By default the client refreshes state information every twenty seconds.

## Border Gateway Protocol - BGP

The Border Gateway Protocol (BGP) is the core routing protocol of the Internet. It works by maintaining a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional IGP metrics, but makes routing decisions based on path, network policies and/or rulesets.

Entuity supports BGP through the Routing Protocols module which is activated through `configure`.

## Cisco Discovery Protocol - CDP

CDP is a proprietary layer 2 protocol that exchanges information about neighboring devices. It works on the majority of Cisco devices by default, and is a licensed technology available with some other manufacturer’s devices.

Entuity gathers CDP from the CDP MIBs, providing a complete and fully accurate layer 2 and layer 3 topology. This relies on the:

- Devices all being under Entuity management.
- CDP is enabled globally and on each interface. Including the detail parameter allows the display of the layer 3 addressing configured on the neighbor.
- CDP is of compatible versions.
- MIB population working.

## Enhanced Interior Gateway Routing Protocol - EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary routing protocol. EIGRP is an advanced distance-vector routing protocol, with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router.

Entuity supports EIGRP through the Routing Protocols module which is activated through `configure`.

## Host Detection

Entuity detects managed hosts through the host resources MIB and identifies their network connections.

## Hypervisor Detection

Entuity detects connections between servers running hypervisors and the appropriate switch/router port on the physical network.

## IPv6 ND

The IPv6 Neighbor Discovery (ND) protocol facilitates the discovery of neighboring devices. Both regular hosts and routers in an IPv6 environment use the IPv6 ND protocol when exchanging information necessary for proper internetwork operation.

Entuity supports IPv6 ND through the IPv6 module which is activated through `configure`.

## IP Peering

IP Peering provides visibility into your WAN links, i.e. leased line, Frame Relay DLCIs, ATM VCCs, using subnet masking. It also reflects any manual IP pairings you may have made in Entuity.

## Intermediate System to Intermediate System - IS-IS

IS-IS is a link-state interior gateway protocol. Each IS-IS enabled router maintains its own database of the network topology, from which it computes the best path for each packet it forwards.

IS-IS uses the same algorithm as another routing protocol, OSPF, for computing the best path through the network.However IS-IS is an OSI network protocol and therefore does not use IP addressing. However the Entuity map route protocols implementation is for IPv4 addressing, although IS-IS may appear to identify links between IPv6 devices the peering is not through the IPv6 addressing but through the device's MAC addresses.

Entuity supports IS-IS through the Routing Protocols module which is activated through `configure`.

## Link Layer Discovery Protocol - LLDP

The IEEE 802.1AB Link Layer Discovery Protocol (LLDP), provides a solution for the configuration issues caused by expanding LANs. It runs over the data link layer and specifically defines a standard method for Ethernet network devices to advertise information about themselves to other nodes on the network and store the information they discover. LLDP is available as a technology link type on the Entuity maps.

## Open Shortest Path First - OSPF

The Open Shortest Path First (OSPF) protocol is a hierarchical interior gateway protocol (IGP) for routing in Internet Protocol, using a link-state in the individual areas that make up the hierarchy. OSPF version 2 supports IPv4.

A link state database (LSDB) is constructed as a tree-image of the network topology, and identical copies of the LSDB are periodically updated on all routers in each OSPF-aware area. By convention, area 0 represents the core or "backbone" region of an OSPF-enabled network, and other OSPF area numbers may be designated to serve other regions of an enterprise (large, business) network - however every additional OSPF area must have a direct or virtual connection to the backbone OSPF area. The backbone area has the identifier 0.0.0.0. Inter-area routing goes via the backbone.

Routers in the same broadcast domain or at each end of a point-to-point telecommunications link form adjacencies when they have detected each other. This detection occurs when a router "sees" itself in a hello packet. This is called a two way state and is the most basic relationship. The router select a designated router (DR) and a backup designated router (BDR) which act as a hub to reduce traffic between routers. OSPF uses both unicast and multicast to send "hello packets" and link state updates. Multicast addresses 224.0.0.5 (all SPF/link state routers) and 224.0.0.6 (all Designated Routers) are reserved for OSPF. In contrast to the Routing Information Protocol (RIP) or the Border Gateway Protocol (BGP), OSPF does not use TCP or UDP but uses IP directly, via IP protocol 89. OSPF handles its own error detection and correction, therefore negating the need for TCP or UDP functions.

Entuity supports OSPF through the Routing Protocols module which is activated through `configure`.

## Physical Address Matching

Physical Address Matching includes connections involving ports with *VIP Status* of Server link or Uplink.

Entuity considers an uplink as trunking on a connection to a single port on a router or layer 3 switch. When the port is on a firewall, load balancer or managed host the uplink is considered a Server link, unless the device has routing capability.

You can amend the uplink detection algorithm through the `topology` and `vipman` sections in `entuity.cfg`. You can configure Entuity to, for example:

- Identify device types that should be considered as servers, by default load balancers, firewalls and managed hosts.
- Amend the detection algorithm to consider analysis of MAC information.
- Amend the maximum number of links for an uplink, by default set to 1.

Topology discovery is done by StormWorks discovery and the original topology and changes to that topology take the time of discovery cycle to appear in the topology. Status is shown much quicker.

For the best performance of this link technology:

- MACs must be gathered from the switches.

- Entuity should manage all intermediate devices.
- Where trunks are not detected and the router is the only MAC that appears on some of the switch to switch links. In this case the uplink detection suppresses the links to these ports - as it sees more than one device with ports with a single MAC address on that is the router MAC address.

## Spanning Tree

Spanning tree provides a vendor neutral technology for visibility into your network. When correctly implemented Entuity discovers bridge links, switch to switch relationships, through polling the Bridge MIB. Complete spanning tree connectivity relies on a contiguous set of Entuity managed devices.

A device’s spanning tree details are available through its Explorer Advanced tab.

Spanning tree shows trunk connectivity, and also includes uplinks when spanning tree is enabled, i.e. they are "router on a stick" or layer 3 switch connections - fast ethernet connections which can route between VLANS.

Spanning tree will not show uplinks in other cases, and these are then detected using uplink detection.

This technology can be disabled by setting the following in `entuity.cfg`:

```
[Topology]
EnableSpanningTree=0
```

## SynOptics Network Management Protocol - SONMP

SONMP is also known as the Nortel Discovery Protocol (NDP), a Data Link Layer network protocol for discovery of Nortel (Avaya and Ciena) devices. It is available as a technology link type for the Entuity maps.

## Trace Route - Ping State

Trace Route - Ping State technology shows layer 3 connectivity between mapped objects using information from Entuity availability monitoring. Entuity by default performs traceroutes every ten minutes, and pings IP addresses within a route every two minutes. Entuity:

- Can return information on devices, including their status, even when intermediate devices are not under its management.
- Does not include to a Trace Route - Ping State map devices with an IP address that is administratively down.
- Does not support networks where load sharing is implemented.

Entuity excludes devices and interfaces that return ping information but are not truly layer 3 objects, for example switches that only have a layer 3 management address. However you can amend these device and interface settings through the topology section of `entuity.cfg`. (See the *Entuity System Administrator Reference Manual*.)

## User Defined Connections

If Entuity does not discover all connections between devices, for example a cable connection between devices, you can define a physical connection. This connection is automatically available within maps to which the source and destination devices are included.

User defined connections are made through the **Administration > Inventory** / **Topology > Physical Connections**.

## VM Detection

Entuity detects virtual machines (VMs) that run on managed hypervisors, virtual machines that Entuity also independently manages as Managed Host or Ping Only devices. Entuity maps these virtual machines to their hypervisors through their virtual NIC.

# Appendix C Entuity URLs

The Entuity web UI uses frames to display different types of information within the same page, the content of each frame within the page has its own URL. You can access these URLs through the web browser, and copy and amend them to suit your own purposes, for example to open a saved map, a filtered view of incidents, a flow chart, a report.

You can then use these URLs to:

- Launch the Entuity web UI in a context defined within the URL.
- Add content to custom dashboards.

## How to discover the information required to generate a URL

There are a number of techniques for accessing these URLs:

- Use a browser's Properties dialog to identify the source of the frame.
- Open frame content in its own browser window and then copy from its navigation bar the URL. For interactive charts use **Open this chart in new page,** which opens the chart in a new page with its URL available from the browser address bar.

### Recovering a URL

The easiest method of generating a URL is to copy it from the Entuity web UI. For example to get the URL that would display the Summary tab for a particular port:

1) From Entuity use Explorer to display the Summary details tab for the port.
2) Click on the tab, this sets the focus of the browser to that frame within the window.
3) Display the browser context menu, and then when using the web browser:
   - Internet Explorer, click **Properties**.
   - Firefox click **This Frame** > **View Frame Info**.
4) From Address highlight and copy the URL. Ensure you select the full URL.

   You can test the URL by pasting it to your browser's address field. When you are:

   - Not logged into the Entuity server, you are first prompted to login and then redirected to the object page. This page appears within a frame, the web UI's header and Explorer frames are also displayed.
   - Logged into the Entuity server, the URL displays only the launched object page, as in the following screen capture.

### Entuity Server Identifiers

Each Entuity server has its own unique server identifier. The identifier is included in the URLs it generates and restricts application of the URL to the objects managed by the specified server. It is a mandatory parameter.

The server identifier is present in most URLs and can also be viewed on the Entuity server through *entuity_home*`\etc\serverid.xml`. For legacy reasons the server identifier has three parameter names each used exclusively in its area of Entuity:

- *eyeServer*, used for generating reports.
- *server*, launching web UI pages.
- *serverId*, launching charts, events.

When copying dashboard configurations between Entuity servers you should check if any server identifiers require amending.

## Using URLs to call the Entuity Web UI

By specifying a URL you can launch the Entuity web UI's Summary and Advanced tabs within the context of a specified object managed by the identified Entuity server.

For example, this URL displays the Summary tab for the specified port on the Entuity server century:

```
http://century/webUI/objectSummary.do?menuName=Explorer
&server=81050284-2aec-418d-a9ba-6f2355f98295&view=My%20Network&id=877
```

This example URL displays the Advanced tab for the specified port on the Entuity server century:

```
http://century/webUI/objectDetails.do?server=81050284-2aec-418d-a9ba-
6f2355f98295&view=My%20Network&id=877
```

### URL Syntax for Web UI Launch

`http://`*EntuityServer*`/webUI/`*pageName*`.do?server=`*serverIdentifier*`&view=`*Entuityview*`&id=`*ObjectID*`&compId=`*CompID*

where:

- *EntuityServer*, is the resolved host name or IP address of the Entuity server.
- *pageName*, is the name of the web UI tab. Entuity currently supports two tabs for URL launching:
  - Summary, objectSummary.do
  - Advanced, objectDetails.do.
- *server*, is the unique identifier of the Entuity server. (See *Entuity Server Identifiers*.)
- *view*, is the name of the Entuity business view. This is an optional field.
- *id*, is the unique StormWorks identifier of the managed object.
- *CompID*, relates the object to its associated events. It is not required with the Advanced and Summary tabs, although it may be appended to a URL that is copied from the web UI. For example:

  ```
  http://ppk/webUI/objectDetails.do?server=18ef37ae-1538-4ee0-b0ae-
  f83e3d8bf8a1&view=London&id=609&compId=4.1.0.0
  ```

# Use URLs with Custom Dashboards

The content of each pane of a custom dashboard is derived from a fully qualified URL, i.e. http://*entuity_server*, https://*entuity_server*. When you edit a custom dashboard you can see, and amend these URLs although they should remain fully qualified.

You should ensure the homepage URL uses the same protocol, HTTP or HTTPS, as the Entuity server. By default browsers block mixed content to prevent unencrypted content being included in pages with encrypted content. You can change this default behavior, for example in FireFox click on the small shield in the URL bar that indicates mixed content is blocked.

## Configuring Chart URLs for Custom Dashboards

You can add charts to custom dashboards by dragging and dropping to the Custom Dashboard Editor:

- Charts from the Entuity web UI.
- A chart's URL using the chart's icon.

This example URL generates a flow top listeners chart:

```
http://ppk/webUI/flowSummary.do?style=bar&period=LAST_1_HOUR
&topN=5&width=150&height=200&label=0&serverId=045de6eb-0894-4357-aa31-
a4a6947360e9&deviceId=1&selop=AND(EQ(%22if%22,%221%22))&view=My%20Netw
ork&id=1087&compId=1.1.1.0&showTree=0&fixedInterface=1&groups=srcIP
```

where:

- *webUI/flowSummary.do*, identifies the Entuity server and the flow summary interface. When the, as here, the server is not explicitly identified only the flow chart is displayed and not the tabulated data.
- *style*, is the chart style, bar, stack, line.
- *period*, chart reporting period.
- *topN*, top number of flows.
- *width* and *height* of the chart.
- *serverId*, unique identifier of the Entuity server. (See *Entuity Server Identifiers*.)
- *view*, name of the view against which the chart is run.
- *deviceId*, *id* and *compId* are Entuity internal identifiers for the charted object.
- *label*, controls when the chart label is displayed, 1 to display and 0 to hide.
- *showTree*, controls when the dashboard panel includes the port banner with a link to the device summary, 1 to display and 0 to hide.
- *fixedInterface* the graphed interface.
- *srcIP* the source IP address for the flow.

## Configuring Event and Incident URLs for Custom Dashboards

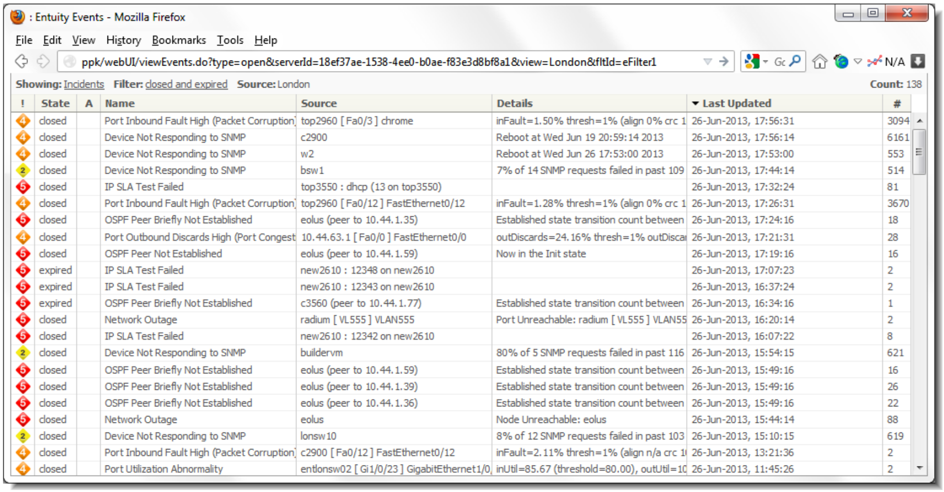
You can add events and incidents to a custom dashboard. You should have already defined the event and incident filter, the URL syntax allows you to reference existing filters not define them. There are two event and incident specific parameters:

- *type* sets the view to events or incidents:
  - **open**, incidents
  - **historical**, events.
- *fltId* identifies the event and incident filter through its internal name, `eFilter`*n*. (See *Recovering a URL*.)

  To use the default filter **All (open)** do not include this parameter to the URL.

This example URL displays incidents raised on the specified server within the London view for the user defined filter **eFilter1** (the filter display name is **closed and expired**):

```
http://ppk/webUI/viewEvents.do?type=open&serverId=18ef37ae-1538-4ee0-
b0ae-f83e3d8bf8a1&view=London&fltId=eFilter1
```



ppk/webUI/viewEvents.do?type=open&serverId=18ef37ae-1538-4ee0-b0ae-f83e3d8bf8a1&view=London&fltId=eFilter1

**Showing:** Incidents **Filter:** closed and expired **Source:** London **Count:** 138

| ! | State | A | Name | Source | Details | Last Updated | # |
|---|---|---|---|---|---|---|---|
| 4 | closed | | Port Inbound Fault High (Packet Corruption) | top2960 [ Fa0/3 ] chrome | inFault=1.50% thresh=1% (align 0% crc 1 | 26-Jun-2013, 17:56:31 | 3094 |
| 4 | closed | | Device Not Responding to SNMP | c2900 | Reboot at Wed Jun 19 20:59:14 2013 | 26-Jun-2013, 17:56:14 | 6161 |
| 4 | closed | | Device Not Responding to SNMP | w2 | Reboot at Wed Jun 26 17:53:00 2013 | 26-Jun-2013, 17:53:00 | 553 |
| 2 | closed | | Device Not Responding to SNMP | bsw1 | 7% of 14 SNMP requests failed in past 109 | 26-Jun-2013, 17:44:14 | 514 |
| 5 | closed | | IP SLA Test Failed | top3550 : dhcp (13 on top3550) | | 26-Jun-2013, 17:32:24 | 81 |
| 4 | closed | | Port Inbound Fault High (Packet Corruption) | top2960 [ Fa0/12 ] FastEthernet0/12 | inFault=1.28% thresh=1% (align 0% crc 1 | 26-Jun-2013, 17:26:31 | 3670 |
| 5 | closed | | OSPF Peer Briefly Not Established | eolus (peer to 10.44.1.35) | Established state transition count between | 26-Jun-2013, 17:24:16 | 18 |
| 4 | closed | | Port Outbound Discards High (Port Congest | 10.44.63.1 [ Fa0/0 ] FastEthernet0/0 | outDiscards=24.16% thresh=1% outDiscai | 26-Jun-2013, 17:21:31 | 28 |
| 5 | closed | | OSPF Peer Not Established | eolus (peer to 10.44.1.59) | Now in the Init state | 26-Jun-2013, 17:19:16 | 16 |
| 5 | expired | | IP SLA Test Failed | new2610 : 12348 on new2610 | | 26-Jun-2013, 17:07:23 | 2 |
| 5 | expired | | IP SLA Test Failed | new2610 : 12343 on new2610 | | 26-Jun-2013, 16:37:24 | 2 |
| 5 | expired | | OSPF Peer Briefly Not Established | c3560 (peer to 10.44.1.77) | Established state transition count between | 26-Jun-2013, 16:34:16 | 1 |
| 5 | closed | | Network Outage | radium [ VL555 ] VLAN555 | Port Unreachable: radium [ VL555 ] VLAN55 | 26-Jun-2013, 16:20:14 | 2 |
| 5 | closed | | IP SLA Test Failed | new2610 : 12342 on new2610 | | 26-Jun-2013, 16:07:22 | 8 |
| 2 | closed | | Device Not Responding to SNMP | buildervm | 80% of 5 SNMP requests failed in past 116 | 26-Jun-2013, 15:54:15 | 621 |
| 5 | closed | | OSPF Peer Briefly Not Established | eolus (peer to 10.44.1.59) | Established state transition count between | 26-Jun-2013, 15:49:16 | 16 |
| 5 | closed | | OSPF Peer Briefly Not Established | eolus (peer to 10.44.1.39) | Established state transition count between | 26-Jun-2013, 15:49:16 | 26 |
| 5 | closed | | OSPF Peer Briefly Not Established | eolus (peer to 10.44.1.36) | Established state transition count between | 26-Jun-2013, 15:49:16 | 22 |
| 5 | closed | | Network Outage | eolus | Node Unreachable: eolus | 26-Jun-2013, 15:44:14 | 88 |
| 2 | closed | | Device Not Responding to SNMP | lonsw10 | 8% of 12 SNMP requests failed in past 103 | 26-Jun-2013, 15:10:15 | 619 |
| 4 | closed | | Port Inbound Fault High (Packet Corruption) | c2900 [ Fa0/12 ] FastEthernet0/12 | inFault=2.11% thresh=1% (align n/a crc 1( | 26-Jun-2013, 13:21:36 | 2 |
| 4 | closed | | Port Utilization Abnormality | entlonsw02 [ Gi1/0/23 ] GigabitEthernet1/0, | inUtil=85.67 (threshold=80.00), outUtil=10 | 26-Jun-2013, 11:45:26 | 2 |

Figure 430 Incidents URL with eFilter1

## Configuring Report URLs for Custom Dashboards

You can add reports to custom dashboards. You can retrieve a report's URL through a web browser and then amend the generated URL to meet your requirements. You should only use the report's web UI to generate the report, and therefore URL, that you require and not attempt to create a report URL outside of this mechanism. You should limit amendments to report URLs to:

- Removing a report's generation identifier
- Hiding the framework that surrounds a generated report.

This example URL generates a Device Latency report in HTML format:

```
http://century/webUI/jasperReport.do?reportGenera-
tionId=1320703828618&report=%2Freports%2FActivity%2FDeviceL-
atency&format=html&eyeServer=aa2287e3-19ac-4d2c-876a-
b1e7b6-
fa059e&view=My%20Network&topNCount=10&timeFrame=prev%3A24h&secondary-
TimeFrame=&primeTime=Sun%3ASun%400%3A0&autoRun=1

http://ppk/webUI/jasperReport.do?reportGenera-
tionId=1320703828618&report=%2Freports%2FActivity%2FDeviceL-
atency&format=html&eyeServer=18ef37ae-1538-4ee0-b0ae-
f83e3d8bf8a1&view=My%20Network&topNCount=10&timeFrame=prev%3A24h&secon
daryTimeFrame=&primeTime=Sun%3ASun%400%3A0&autoRun=1&framework=0
```

This version of the URL is amended for use within a custom dashboard, *reportGenerationId* is removed and the framework parameter is included and set to hide:

```
http://century/webUI/jasperReport.do?reportGenera-
tionId=1320703828618&report=%2Freports%2FActivity%2FDeviceL-
atency&format=html&eyeServer=aa2287e3-19ac-4d2c-876a-
b1e7b6fa059e&view=My%20Network&topNCount=10&timeFrame=prev%3A24h&secon
daryTimeFrame=&primeTime=Sun%3ASun%400%3A0&autoRun=1&framework=0
```

The particular parameters available for each report URL vary according to that report's definition Report Options. The key components of report URL syntax are:

```
http://EntuityServer/webUI/jasperReport.do?reportGenera-
tionId=reportId&report=reportId&format=formatName&eyeServer=serverID&v
iew=Entuityview&topNCount=number&report-
Period=timeframe&autoRun=1&framework=0
```

where:

- *http://EntuityServer/webUI/*, identifies the Entuity server and its interface.
- *jasperReport.do*, identifies the underlying technology through which Entuity generates reports.
- *reportGenerationId*, uniquely identifies the generated report.

  When you are using a copied URL to generate a new report each time it is run, you should remove this parameter. If you leave this value in you may get a cached version of the report with this identifier, and not a newly generated report.
- *report*, identifies the report type, for example an Activity report, specifically Device Latency.
- *format*, the output format of the report, e.g. HTML, PDF.
- *eyeServer*, internal identifier of the Entuity server on which the report is run. (See *Entuity Server Identifiers*.)
- *view*, name of the view against which the report is run.
- *topNCount*, limits the number of devices included to the report, for example the ten devices with the highest latency.
- *reportperiod*, sets the period over which the report reports, for example:

  - *timeFrame*, sets the time frame of the report, e.g. the previous twenty-four hours.
  - *secondaryTimeFrame*, allows reports to chart stream data from more than one time period. It is only used with reports designed using Report Builder.
  - *primeTime*, sets the prime time period.
- *autoRun*, when set to 1 Entuity automatically runs the URL and generates a report when it is loaded.
- *framework*, controls the display of the framework that surrounds a generated report in the web UI, for example the different output report icons, sidebar margins, whether all pages are displayed. When set to:
  - **1** (default), Entuity displays the framework with the generated report.
  - **0**, Entuity hides the framework, i.e. hides report output and format headings, reduces the size of the page margins, displays all report pages (rather than only the first). You might hide the framework when displaying reports in a custom dashboard.

## Reports Not Displaying Consistently in Custom Dashboards

For each user Entuity, more accurately Apache Tomcat, caches objects used in the last report a user accessed during their current Entuity session. Caching improves the performance of report display. However, where you are using custom dashboards with more than one report, Entuity may not consistently display the content of those reports, e.g. logos, charts. You can amend the size of the cache, so it maintains more reports. This setting applies to all users, it may therefore potentially significantly increase the memory requirements of Apache Tomcat on the Entuity server.

Configuration of the report cache is through the *Jasper.maxCachedReportsPerSession* in *entuity_home*`\etc\entuity.cfg`, for example:

```
[Jasper]

maxCachedReportsPerSession=2
```

where:

- *maxCachedReportsPerSession*, sets the number of reports Apache Tomcat caches for the duration of each users Entuity session.

# Appendix D  IP SLA Operation Type Attributes

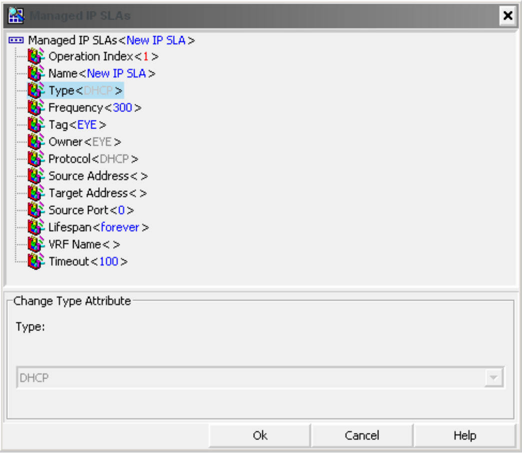
Entuity discovers the supported IP SLA operation types on all monitored devices. Polled attributes use the RTTMON MIB, attributes vary according to the operation type. This appendix lists the operation configuration and operation polling attributes:

- DHCP Operation
- DNS Operation
- HTTP Operation
- HTTP Raw Operation
- ICMP Echo Operation
- TCP Connect Operation
- UDP Echo Operation
- UDP Jitter Operation
- UDP Jitter VoIP Operation.

## DHCP Operation

The DHCP operation measures the Round Trip Time (RTT) taken to discover a DHCP Server and obtain a lease from it. After obtaining an IP Address, Cisco IOS IP SLA releases the IP address that was leased by the server.

The DHCP operation is useful for cable and DSL (Digital Subscriber Lines) providers that use DHCP for dynamic address allocation.



Managed IP SLAs<New IP SLA>
- Operation Index<1>
- Name<New IP SLA>
- Type<DHCP>
- Frequency<300>
- Tag<EYE>
- Owner<EYE>
- Protocol<DHCP>
- Source Address< >
- Target Address< >
- Source Port<0>
- Lifespan<forever>
- VRF Name< >
- Timeout<100>

Change Type Attribute

Type: DHCP

Figure 431  Configuring DHCP Operations

| Attribute | Description |
|---|---|
| Operation Index | Unique identifier of the operation. |
| Name | IP SLA operation name. |
| Type | The type of operation to be performed. |
| Frequency | Sets the duration between initiating each operation. You should not set to a value which is of a shorter duration than *Timeout*.<br>The minimum allowed value is 10 seconds. |
| Tag | A descriptive string used by Entuity to identify the operation target. |
| Owner | Identifies the creator of the operation, i.e. EYE. |
| Protocol | Protocol used by the operation. |
| Source Address | Specifies the IP address of the source. |
| Target Address | Specifies the IP address of the destination. |
| Source Port | The port on the source device used by the operation. When set to:<br>■ 0 (default) allows the operation to automatically select any available port.<br>■ a specific port number, ensures the operation uses that port. Take care that other operations on the same device do not use the same port, as the conflict can cause operations to fail. This is especially true when the conflict involves an operation that take a greater time to complete, e.g. UDP Jitter. |
| Lifespan | IP SLA operation interval, by default **forever**, i.e. once created it exists forever on the device unless deleted by Entuity. You can enter a limited lifespan, by entering a value in seconds. When this time elapses the operation and Entuity has to recreate it. |
| VRF Name | Name of the MPLS IP VPN VRF. |
| Timeout | Length of time, in seconds, Entuity waits for a response from the IP SLA operation before marking it as timed-out. You should not set to a value which is of a greater duration than *Frequency*. |

Table 118 DHCP Operation Attributes

| Object Name | Attribute and Description |
|---|---|
| rttMonLatestRttOperCompletionTime | *Completion Time*. The latest completion time of RTT operations which complete successfully. |
| rttMonLatestRttOperSense | *Sense*. The latest completion time of any RTT operation which completes successfully. |

Table 119 DHCP Operation Time-Series Attributes

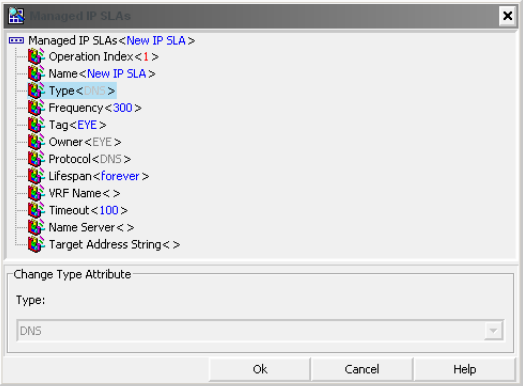
## DNS Operation

Domain Name System (DNS) response time is measured as the difference between the time taken to send a DNS request and receiving the reply. When *Address to Resolve* specifies:

- An IP Address, the operation resolves the hostname.

- A hostname, the operation resolves the IP address.

The DNS operation is useful for checking DNS performance, an important element for user perception of network performance.



Managed IP SLAs<New IP SLA>
Operation Index<1>
Name<New IP SLA>
Type<DNS>
Frequency<300>
Tag<EYE>
Owner<EYE>
Protocol<DNS>
Lifespan<forever>
VRF Name< >
Timeout<100>
Name Server< >
Target Address String< >

Change Type Attribute
Type:
DNS

Figure 432 Configuring DNS Operations

| Attribute | Description |
|---|---|
| Operation Index | Unique identifier of the operation. |
| Name | IP SLA operation name. |
| Type | The type of operation to be performed. |
| Frequency | Sets the duration between initiating each operation. You should not set to a value which is of a shorter duration than *Timeout*. |
| Tag | A descriptive string used by Entuity to identify the operation target. |
| Owner | Identifies the creator of the operation, i.e. EYE. |
| Protocol | Protocol used by the operation. |
| Lifespan | IP SLA operation interval, by default **forever**, i.e. once created it exists forever on the device unless deleted by Entuity. You can enter a limited lifespan, by entering a value in seconds. When this time elapses the operation and Entuity has to recreate it. |
| VRF Name | Name of the MPLS IP VPN VRF. |
| Timeout | Length of time, in seconds, Entuity waits for a response from the IP SLA operation before marking it as timed-out. You should not set to a value which is of a greater duration than *Frequency*. |
| Target Address String | Address to resolve. |
| Name Server | IP address of name server. |

Table 120 DNS Operation Attributes

| Object Name | Attribute and Description |
|---|---|
| rttMonLatestRttOperCompletionTime | *Completion Time*. The latest completion time of RTT operations which complete successfully. |
| rttMonLatestRttOperSense | *Sense*. The latest completion time of any RTT operation which completes successfully. |

Table 121 DNS Operation Time-Series Attributes

## HTTP Operation

Entuity's HTTP operation supports the HTTP GET operation. It measures the Round Trip Time (RTT) taken to connect and access data from an HTTP server. This HTTP operation involves three stages:

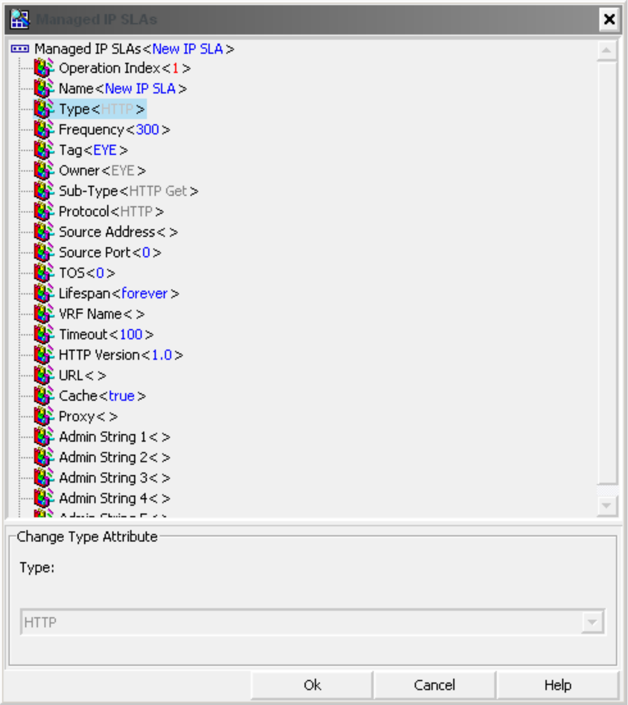
- A DNS operation measuring the DNS RTT.
- A TCP Connect operation using the domain name to connect to the appropriate HTTP server measuring the RTT for this operation.
- An HTTP Get request measuring the RTT to retrieve the specified HTML page from the HTTP server.

A total HTTP RTT is the sum of the DNS RTT, the TCP Connect RTT, and the HTTP RTT.

| Attribute | Description |
|---|---|
| *DNS Time* | The RTT taken to perform domain name look up. |
| *TCP Time* | The RTT taken to perform a TCP connect to the HTTP Server. The TCP connect is performed after the DNS operation. |
| *HTTP Time* | The RTT taken to send a request and receive a response from the HTTP Server (the operation retrieves the base HTML page only). |

Table 122 HTTP Server Response Time Measurements

The results of an HTTP operation are useful in monitoring your web server performance levels by determining the RTT taken to retrieve a web page.



Managed IP SLAs

Managed IP SLAs<New IP SLA>
- Operation Index<1>
- Name<New IP SLA>
- Type<HTTP>
- Frequency<300>
- Tag<EYE>
- Owner<EYE>
- Sub-Type<HTTP Get>
- Protocol<HTTP>
- Source Address< >
- Source Port<0>
- TOS<0>
- Lifespan<forever>
- VRF Name< >
- Timeout<100>
- HTTP Version<1.0>
- URL< >
- Cache<true>
- Proxy< >
- Admin String 1< >
- Admin String 2< >
- Admin String 3< >
- Admin String 4< >

Change Type Attribute

Type: HTTP

Figure 433  Configuring HTTP Operations

| Attribute | Description |
|---|---|
| Operation Index | Unique identifier of the operation. |
| Name | IP SLA operation name. |
| Type | The type of operation to be performed. |
| Frequency | Sets the duration between initiating each operation. You should not set to a value which is of a shorter duration than *Timeout*. |
| Tag | A descriptive string used by Entuity to identify the operation target. |
| Owner | Identifies the creator of the operation, i.e. EYE. |
| Sub-Type | A code that represents the specific type of RTT operation, i.e. HTTP Get. |
| Protocol | Protocol used by the operation. |
| Source Address | Specifies the IP address of the source. |

Table 123 HTTP Operation Attributes

| Attribute | Description |
|---|---|
| Source Port | The port on the source device used by the operation. When set to:<br>■ 0 (default) allows the operation to automatically select any available port.<br>■ a specific port number, ensures the operation uses that port. Take care that other operations on the same device do not use the same port, as the conflict can cause operations to fail. This is especially true when the conflict involves an operation that take a greater time to complete, e.g. UDP Jitter. |
| TOS | Defines the IP Type of Service (TOS) byte for request packets. This attribute may also be used as a Differentiated Services Code Point (DSCP). |
| Lifespan | IP SLA operation interval, by default **forever**, i.e. once created it exists forever on the device unless deleted by Entuity. You can enter a limited lifespan, by entering a value in seconds. When this time elapses the operation and Entuity has to recreate it. |
| VRF Name | Name of the MPLS IP VPN VRF. |
| Timeout | Length of time, in seconds, Entuity waits for a response from the IP SLA operation before marking it as timed-out. You should not set to a value which is of a greater duration than *Frequency*. |
| HTTPVersion | HTTP Version e.g. "1.0". |
| URL | URL to retrieve. |
| AdminCache | Boolean - if true - download cached pages. |
| Proxy | URL of the proxy server. |

Table 123 HTTP Operation Attributes

| Object Name | Attribute and Description |
|---|---|
| rttMonLatestRttOperCompletionTime | *Completion Time*. The latest completion time of RTT operations which complete successfully. |
| rttMonLatestHTTPOperDNSRTT | *DNS Time*. Round Trip Time taken to perform DNS query within the HTTP operation. |
| rttMonLatestHTTPOperTransactionRTT | *TCP Time*. Round Trip Time taken to connect to the server. |
| rttMonLatestHTTPOperTCPConnectRTT | *HTTP Time*. Round Trip Time taken to connect to the HTTP server. |
| rttMonLatestHTTPOperMessageBodyOctets | *Octets*. The size of the message body received as a response to the HTTP request. |
| rttMonLatestHTTPOperSense | *State*. An application specific sense code for the completion status of the latest RTT operation. |
| rttMonLatestHTTPErrorSenseDescription | *Sense*. A sense description for the completion status of the latest RTT operation. |

Table 124 HTTP Operation

## HTTP Raw Operation

Entuity's HTTP operation supports the HTTP Raw operation. For HTTP Raw requests IP SLAs require the entire content of the HTTP request. HTTP Raw requests are more flexible than HTTP Get requests, allowing more configuration and access through proxy servers.

This HTTP operation involves three stages:

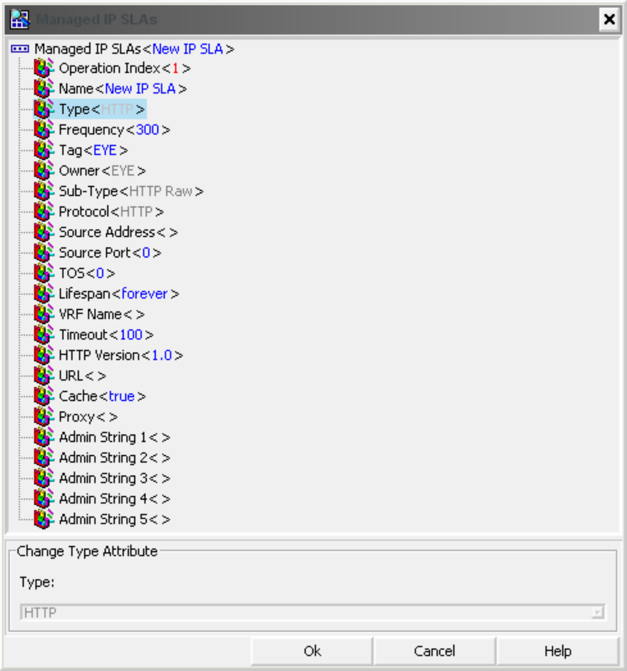
- A DNS operation measuring the DNS RTT.
- A TCP Connect operation using the domain name to connect to the appropriate HTTP server measuring the RTT for this operation.
- An HTTP Get request measuring the RTT to retrieve the specified HTML page from the HTTP server.

A total HTTP RTT is the sum of the DNS RTT, the TCP Connect RTT, and the HTTP RTT.

| Attribute | Description |
|---|---|
| *DNS Time* | The RTT taken to perform domain name look up. |
| *TCP Time* | The RTT taken to perform a TCP connect to the HTTP Server. The TCP connect is performed after the DNS operation. |
| *HTTP Time* | The RTT taken to send a request and receive a response from the HTTP Server (the operation retrieves the base HTML page only). |

Table 125 HTTP Server Response Time Measurements

The results of a Raw HTTP operation are useful in monitoring your web server performance levels by determining the RTT taken to retrieve a web page.



Managed IP SLAs

Managed IP SLAs<New IP SLA>
- Operation Index<1>
- Name<New IP SLA>
- Type<HTTP>
- Frequency<300>
- Tag<EYE>
- Owner<EYE>
- Sub-Type<HTTP Raw>
- Protocol<HTTP>
- Source Address< >
- Source Port<0>
- TOS<0>
- Lifespan<forever>
- VRF Name< >
- Timeout<100>
- HTTP Version<1.0>
- URL< >
- Cache<true>
- Proxy< >
- Admin String 1< >
- Admin String 2< >
- Admin String 3< >
- Admin String 4< >
- Admin String 5< >

Change Type Attribute

Type: HTTP

Figure 434 Configuring HTTP RAW Operations

| Attribute | Description |
|---|---|
| Operation Index | Unique identifier of the operation. |
| Name | IP SLA operation name. |
| Type | The type of operation to be performed. |
| Frequency | Sets the duration between initiating each operation. You should not set to a value which is of a shorter duration than *Timeout*. |
| Tag | A descriptive string used by Entuity to identify the operation target. |
| Owner | Identifies the creator of the operation, i.e. EYE. |
| Sub-Type | A code that represents the specific type of RTT operation, i.e. HTTP Raw. |
| Protocol | Protocol used by the operation. |
| Source Address | Specifies the IP address of the source. |

Table 126 HTTP Raw Operation Attributes

| Attribute | Description |
|---|---|
| SourcePort | The port on the source device used by the operation. When set to:<br>■ 0 (default) allows the operation to automatically select any available port.<br>■ a specific port number, ensures the operation uses that port. Take care that other operations on the same device do not use the same port, as the conflict can cause operations to fail. This is especially true when the conflict involves an operation that take a greater time to complete, e.g. UDP Jitter. |
| Source Port | The port on the source device used by the operation. When set to:<br>■ 0 (default) allows the operation to automatically select any available port.<br>■ a specific port number, ensures the operation uses that port. Take care that other operations on the same device do not use the same port, as the conflict can cause operations to fail. This is especially true when the conflict involves an operation that take a greater time to complete, e.g. UDP Jitter. |
| TOS | Defines the IP Type of Service (TOS) byte for request packets. This attribute may also be used as a Differentiated Services Code Point (DSCP). |
| Lifespan | IP SLA operation interval, by default **forever**, i.e. once created it exists forever on the device unless deleted by Entuity. You can enter a limited lifespan, by entering a value in seconds. When this time elapses the operation and Entuity has to recreate it. |
| VRF Name | Name of the MPLS IP VPN VRF. |
| Timeout | Length of time, in seconds, Entuity waits for a response from the IP SLA operation before marking it as timed-out. You should not set to a value which is of a greater duration than *Frequency*. |
| HTTPVersion | HTTP Version e.g. "1.0". |
| URL | URL to retrieve. |
| AdminCache | Boolean - if true - download cached pages. |
| Proxy | URL of the proxy server. |
| Admin String 1 to 5 | Strings stores the content of HTTP raw request, when the request cannot fit into String1 then it is split and put in Strings 1 through 5. |

Table 126 HTTP Raw Operation Attributes

| Object Name | Attribute and Description |
|---|---|
| rttMonLatestRttOperCompletionTime | *Completion Time*. The latest completion time of RTT operations which complete successfully. |
| rttMonLatestHTTPOperDNSRTT | *DNS Time*. Round Trip Time taken to perform DNS query within the HTTP operation. |

Table 127 HTTP Operation

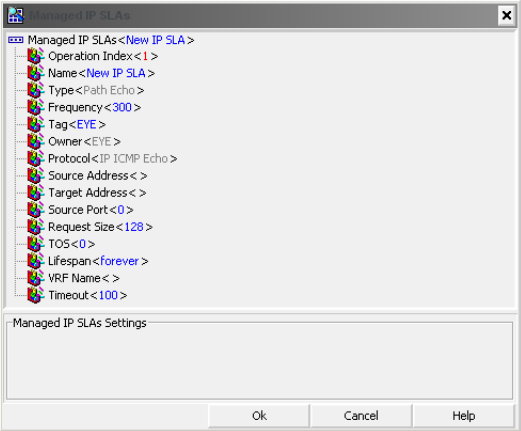
| Object Name | Attribute and Description |
|---|---|
| rttMonLatestHTTPOperTransactionRTT | *TCP Time*. Round Trip Time taken to connect to the server. |
| rttMonLatestHTTPOperTCPConnectRTT | *HTTP Time*. Round Trip Time taken to connect to the HTTP server. |
| rttMonLatestHTTPOperMessageBodyOctets | *Octets*. The size of the message body received as a response to the HTTP request. |
| rttMonLatestHTTPOperSense | *State*. An application specific sense code for the completion status of the latest RTT operation. |
| rttMonLatestHTTPErrorSenseDescription | *Sense*. A sense description for the completion status of the latest RTT operation. |

Table 127 HTTP Operation

## ICMP Echo Operation

The IP SLAs ICMP Path Echo operation records statistics for each hop along the path that the IP SLAs operation takes to reach its destination. The ICMP Path Echo operation determines this hop-by-hop response time between a Cisco router and any IP device on the network by discovering the path using the traceroute facility. Response times are measured as the difference between the time taken to send a Path Echo request and receiving the replies.

Using the statistics recorded for the response times and availability, the ICMP Path Echo operation can identify a hop in the path that is causing a bottleneck. It provides a useful indicator of user perception of network performance.



Managed IP SLAs<New IP SLA>
Operation Index<1>
Name<New IP SLA>
Type<Path Echo>
Frequency<300>
Tag<EYE>
Owner<EYE>
Protocol<IP ICMP Echo>
Source Address< >
Target Address< >
Source Port<0>
Request Size<128>
TOS<0>
Lifespan<forever>
VRF Name< >
Timeout<100>

Figure 435 Configuring ICMP Path Echo Operations

| Attribute | Description |
|---|---|
| Operation Index | Unique identifier of the operation. |

Table 128 ICMP Echo Operation Attributes

| Attribute | Description |
|---|---|
| Name | IP SLA operation name. |
| Type | The type of operation to be performed. |
| Frequency | Sets the duration between initiating each operation. You should not set to a value which is of a shorter duration than *Timeout*. |
| Tag | A descriptive string used by Entuity to identify the operation target. |
| Owner | Identifies the creator of the operation, i.e. EYE. |
| Protocol | Protocol used by the operation. |
| Source Address | Specifies the IP address of the source. |
| Target Address | Specifies the IP address of the destination. |
| Source Port | The port on the source device used by the operation. When set to:<br>■ 0 (default) allows the operation to automatically select any available port.<br>■ a specific port number, ensures the operation uses that port. Take care that other operations on the same device do not use the same port, as the conflict can cause operations to fail. This is especially true when the conflict involves an operation that take a greater time to complete, e.g. UDP Jitter. |
| RequestPacketSize | Sets the protocol data size in the payload of the operation's request packet. |
| TOS | Defines the IP Type of Service (TOS) byte for request packets. This attribute may also be used as a Differentiated Services Code Point (DSCP). |
| Lifespan | IP SLA operation interval, by default **forever**, i.e. once created it exists forever on the device unless deleted by Entuity. You can enter a limited lifespan, by entering a value in seconds. When this time elapses the operation and Entuity has to recreate it. |
| VRF Name | Name of the MPLS IP VPN VRF. |
| Timeout | Length of time, in seconds, Entuity waits for a response from the IP SLA operation before marking it as timed-out. You should not set to a value which is of a greater duration than *Frequency*. |

Table 128 ICMP Echo Operation Attributes

| Object Name | Attribute and Description |
|---|---|
| rttMonLatestRttOperCompletionTime | *Completion Time*. The latest completion time of RTT operations which complete successfully. |
| rttMonLatestRttOperSense | *Sense*. The completion status of the last RTT operation which completes successfully. |
| rttMonStatsCaptureCompletions | *Completions*. Number of successful echo operations. |

Table 129 ICMP Echo Operation Time-Series Attributes

| Object Name | Attribute and Description |
|---|---|
| rttMonStatsCollectNumDisconnects | *Disconnects*. Number of operations that did not occur because the connection to the target was lost. |
| rttMonCtrlAdminTimeout | *Timeouts*. Number of timeout operations and a completion was not time recorded. |
| rttMonStatsCollectBusies | *Busies*. Number of operations that did not occur because a previous operation was still outstanding. |
| rttMonStatsCollectNoConnections | *No Connections*. Number of operations that did not occur because no connection (session) exists with the target. |
| rttMonStatsCollectDrops | *Drops*. Number of times the operation did not occur due to a lack of internal resource. |
| rttMonStatsCollectSequenceErrors | *Sequence Errors*. Number of times a completed operation did not contain the correct sequence identifier. The completion time is not recorded. |
| rttMonStatsCollectVerifyErrors | *Verify Errors*. Number of times a completed operation was received, but the data it contained did not match the expected data; no completion time recorded. |
| rttMonStatsCaptureCompletionTimeMax | *Max RTT.* Maximum round trip time. |
| rttMonStatsCaptureCompletionTimeMin | *Min RTT.* Minimum round trip time. |
| rttMonStatsCaptureSumCompletionTime / rttMonStatsCaptureCompletions | *Average RTT.* Average of successful round trip times. |

Table 129 ICMP Echo Operation Time-Series Attributes

## TCP Connect Operation

The Transmission Control Protocol (TCP) Connection operation discovers the time it takes to connect to the target device. This operation is useful for testing virtual circuit or application availability. The measured connection time is the difference between the time Entuity sends the ACK and the initial SYN.

When the target is a Cisco device with an enabled responder then the operation makes a TCP connection to any known port number. When the destination is a non-Cisco IP host, then the target port number must be specified. This operation is useful in simulating connection times, for example to Telnet, SSH, SQL, HTTP.

Figure 436 Configuring TCP Connect Operations

| Attribute | Description |
|---|---|
| Operation Index | Unique identifier of the operation. |
| Name | IP SLA operation name. |
| Type | The type of operation to be performed. |
| Frequency | Sets the duration between initiating each operation. You should not set to a value which is of a shorter duration than *Timeout*. |
| Tag | A descriptive string used by Entuity to identify the operation target. |
| Owner | Identifies the creator of the operation, i.e. EYE. |
| Protocol | Protocol used by the operation. |
| Source Address | Specifies the IP address of the source. |
| Target Address | Specifies the IP address of the destination. |
| Source Port | The port on the source device used by the operation. When set to:<br>■ 0 (default) allows the operation to automatically select any available port.<br>■ a specific port number, ensures the operation uses that port. Take care that other operations on the same device do not use the same port, as the conflict can cause operations to fail. This is especially true when the conflict involves an operation that take a greater time to complete, e.g. UDP Jitter. |
| Target Port | This object represents the target's port number. |
| TOS | Defines the IP Type of Service (TOS) byte for request packets. This attribute may also be used as a Differentiated Services Code Point (DSCP). |

Table 130 TCP Connect Operation Attributes

| Attribute | Description |
|---|---|
| Control Packets | When enabled (**true**) the operation sends control messages to a responder, residing on the target device to respond to the data request packets being sent by the source device. |
| Lifespan | IP SLA operation interval, by default **forever**, i.e. once created it exists forever on the device unless deleted by Entuity. You can enter a limited lifespan, by entering a value in seconds. When this time elapses the operation and Entuity has to recreate it. |
| VRF Name | Name of the MPLS IP VPN VRF. |
| Timeout | Length of time, in seconds, Entuity waits for a response from the IP SLA operation before marking it as timed-out. You should not set to a value which is of a greater duration than *Frequency*. |

Table 130 TCP Connect Operation Attributes

| Object Name | Attribute and Description |
|---|---|
| rttMonLatestRttOperCompletionTime | *Completion Time*. The latest completion time of RTT operations which complete successfully. |
| rttMonLatestHTTPOperSense | *State*. An application specific sense code for the completion status of the latest RTT operation. |

Table 131 TCP Connect Operation Time-Series Attributes

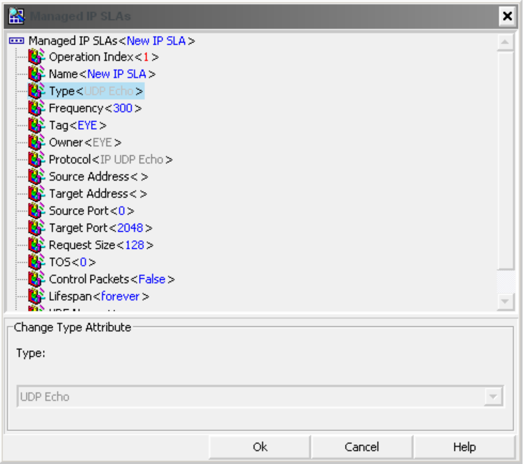
## UDP Echo Operation

The User Datagram Protocol (UDP) Echo operation calculates UDP response times between a Cisco device and any IP enabled device. Response time is computed by measuring the time taken to send a datagram and receive a response from the destination device.

When the target is a Cisco router with an active responder, then Cisco IOS IP SLA can send a UDP datagram to any specified port number. When the destination is a non-Cisco IP host, then a port must be specified.

By default the Echo operation uses UDP port 7, although another port may be specified.

For accurate measurements UDP Echo requires clock synchronization between source and destination and an available Cisco IOS IP SLA responder on the destination device.



Managed IP SLAs

Managed IP SLAs<New IP SLA>
- Operation Index<1>
- Name<New IP SLA>
- Type<UDP Echo>
- Frequency<300>
- Tag<EYE>
- Owner<EYE>
- Protocol<IP UDP Echo>
- Source Address< >
- Target Address< >
- Source Port<0>
- Target Port<2048>
- Request Size<128>
- TOS<0>
- Control Packets<False>
- Lifespan<forever>

Change Type Attribute

Type: UDP Echo

Figure 437  Configuring UDP Echo Operations

| Attribute | Description |
|---|---|
| Operation Index | Unique identifier of the operation. |
| Name | IP SLA Operation name. |
| Type | The type of operation to be performed. |
| Frequency | Sets the duration between initiating each operation. You should not set to a value which is of a shorter duration than *Timeout*. |
| Tag | A descriptive string used by Entuity to identify the operation target. |
| Owner | Identifies the creator of the operation, i.e. EYE. |
| Protocol | Protocol used by the operation. |
| Source Address | Specifies the IP address of the source. |
| Target Address | Specifies the IP address of the destination. |
| Source Port | The port on the source device used by the operation. When set to:<br>■ 0 (default) allows the operation to automatically select any available port.<br>■ a specific port number, ensures the operation uses that port. Take care that other operations on the same device do not use the same port, as the conflict can cause operations to fail. This is especially true when the conflict involves an operation that take a greater time to complete, e.g. UDP Jitter. |
| Target Port | This object represents the target's port number. |
| TOS | Defines the IP Type of Service (TOS) byte for request packets. This attribute may also be used as a Differentiated Services Code Point (DSCP). |

Table 132 UDP Echo Operation Attributes

| Attribute | Description |
|---|---|
| Control Packets | When enabled (**true**) the operation sends control messages to a responder, residing on the target device to respond to the data request packets being sent by the source device. |
| Lifespan | IP SLA operation interval, by default **forever**, i.e. once created it exists forever on the device unless deleted by Entuity. You can enter a limited lifespan, by entering a value in seconds. When this time elapses the operation and Entuity has to recreate it. |
| VRF Name | Name of the MPLS IP VPN VRF. |
| Timeout | Length of time, in seconds, Entuity waits for a response from the IP SLA operation before marking it as timed-out. You should not set to a value which is of a greater duration than *Frequency*. |
| Interval | IP SLA Operation interval |

Table 132 UDP Echo Operation Attributes

| Object Name | Attribute and Description |
|---|---|
| rttMonLatestRttOperCompletionTime | *Completion Time*. The latest completion time of RTT operations which complete successfully. |
| rttMonLatestRttOperSense | *Sense*. The latest completion time of any RTT operation which completes successfully. |

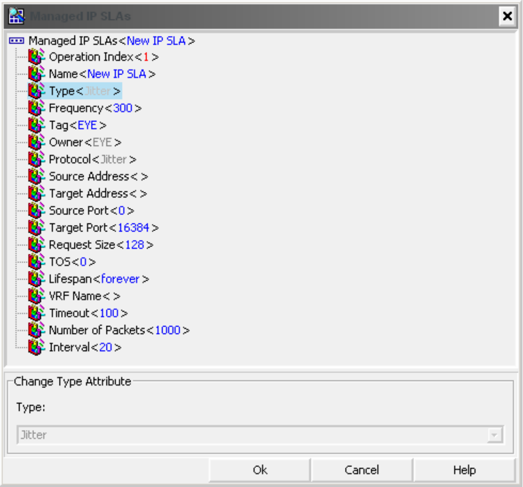
Table 133 UDP Echo Operation

## UDP Jitter Operation

The Jitter operation measures delay specifically inter-packet delay variance. Packet loss is a critical element in SLAs and Jitter statistics are useful for analyzing traffic in a VoIP network.

The UDP Jitter operation is a superset of the UDP echo operation, measuring UDP RTT and per-direction delay variance (jitter).

✓ For accurate measurements UDP Jitter requires clock synchronization between source and destination. There must be an available Cisco IOS IP SLA responder on the destination device.



```
Managed IP SLAs<New IP SLA>
    Operation Index<1>
    Name<New IP SLA>
    Type<Jitter>
    Frequency<300>
    Tag<EYE>
    Owner<EYE>
    Protocol<Jitter>
    Source Address< >
    Target Address< >
    Source Port<0>
    Target Port<16384>
    Request Size<128>
    TOS<0>
    Lifespan<forever>
    VRF Name< >
    Timeout<100>
    Number of Packets<1000>
    Interval<20>
```

Change Type Attribute

Type: Jitter

Figure 438 Configuring UDP Jitter Operations

| Attribute | Description |
|---|---|
| Operation Index | Unique identifier of the operation. |
| Name | IP SLA operation name. |
| Type | The type of operation to be performed. |
| Frequency | Sets the duration between initiating each operation. You should not set to a value which is of a shorter duration than *Timeout*. |
| Tag | A descriptive string used by Entuity to identify the operation target. |
| Owner | Identifies the creator of the operation, i.e. EYE. |
| Protocol | Sets the protocol to be used to perform the operation. |
| Source Address | Specifies the IP address of the source. |
| Target Address | Specifies the address of the target. |
| Source Port | The port on the source device used by the operation. When set to:<br>■ 0 (default) allows the operation to automatically select any available port.<br>■ a specific port number, ensures the operation uses that port. Take care that other operations on the same device do not use the same port, as the conflict can cause operations to fail. This is especially true when the conflict involves an operation that take a greater time to complete, e.g. UDP Jitter. |
| Target Port | This object represents the target's port number. This object is applicable to udpEcho, tcpConnect and jitter probe |
| RequestPacketSize | Sets the protocol data size in the payload of the operation's request packet. |

Table 134 UDP Jitter Operation Attributes

| Attribute | Description |
|---|---|
| TOS | Defines the IP Type of Service (TOS) byte for request packets. This attribute may also be used as a Differentiated Services Code Point (DSCP). |
| Lifespan | IP SLA operation interval, by default **forever**, i.e. once created it exists forever on the device unless deleted by Entuity. You can enter a limited lifespan, by entering a value in seconds. When this time elapses the operation and Entuity has to recreate it. |
| VRF Name | Name of the MPLS IP VPN VRF. |
| Timeout | Length of time, in seconds, Entuity waits for a response from the IP SLA operation before marking it as timed-out. You should not set to a value which is of a greater duration than *Frequency*. |
| Interval | Interval between packets. |
| Number Of Packets | Number of packets. |

Table 134 UDP Jitter Operation Attributes

| Object Name | Attribute and Description |
|---|---|
| rttMonLatestRttOperCompletionTime | *Completion Time*. The latest completion time of RTT operations which complete successfully. |
| rttMonLatestJitterOperSumOfNegativesDS | *Jitter Dest-Src*. The sum of RTT's of all negative jitter values from packets sent from destination to source. |
| rttMonLatestJitterOperMaxOfPositivesSD | *Max. Jitter Src-Dest*. The maximum of all positive jitter values from packets sent from source to destination. |
| rttMonLatestJitterOperSumOfNegativesSD | *Jitter Src-Dest*. The sum of all negative jitter values from packets sent from source to destination. |
| rttMonLatestJitterOperMaxOfPositivesDS | *Max Jitter Dest-Src*. The maximum of all positive jitter values from packets sent from destination to source. |
| rttMonLatestJitterOperOWSumSD | *Delay Src-Dest*. The sum of one way latency from source to destination. |
| rttMonLatestJitterOperOWSumDS | *Delay Dest-Src*. The sum of one way latency from destination to source. |
| rttMonLatestJitterOperOWSumSD | *Sum Src-Dest*. The sum of one way latency from source to destination. |
| rttMonLatestJitterOperOWSumDS | *Sum Dest-Src*. The sum of one way latency from destination to source. |
| rttMonLatestJitterOperNumOfOW | *One Ways*. The number of successful one way latency measurements. |
| rttMonLatestJitterOperRTTSum | *RTT*. The sum of Jitter RTT's that are successfully measured. |

Table 135 UDP Jitter Operation

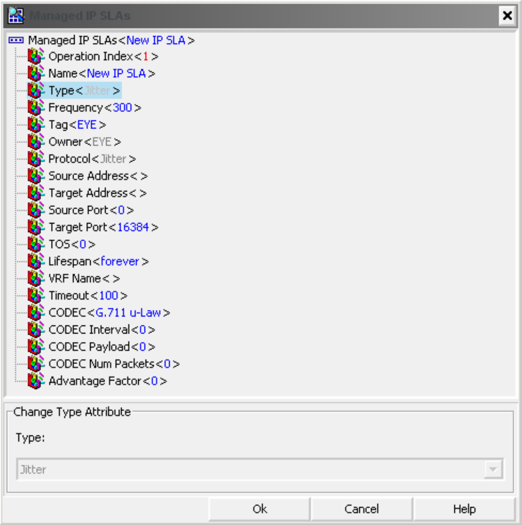
| Object Name | Attribute and Description |
|---|---|
| rttMonLatestJitterOperRTTSum | *Sum RTTs*. The sum of Jitter RTT's that are successfully measured. |
| rttMonLatestJitterOperNumOfRTT | *Round Trips*. The number of RTT's that were successfully measured. |

Table 135 UDP Jitter Operation

## UDP Jitter VoIP Operation

The IP SLAs UDP jitter VoIP operation accurately simulates VoIP traffic, using common CODECs.The operation derives MOS and ICPIF voice quality scores between Cisco IOS devices on the network. You can set thresholds against MOS and ICPIF values, directly against an IP SLA definition, a device or the Entuity server root.

For accurate measurements UDP Jitter VoIP requires clock synchronization between source and destination. There must be an available Cisco IOS IP SLA responder on the destination device.



Managed IP SLAs<New IP SLA>
- Operation Index<1>
- Name<New IP SLA>
- Type<Jitter>
- Frequency<300>
- Tag<EYE>
- Owner<EYE>
- Protocol<Jitter>
- Source Address< >
- Target Address< >
- Source Port<0>
- Target Port<16384>
- TOS<0>
- Lifespan<forever>
- VRF Name< >
- Timeout<100>
- CODEC<G.711 u-Law>
- CODEC Interval<0>
- CODEC Payload<0>
- CODEC Num Packets<0>
- Advantage Factor<0>

Change Type Attribute

Type: Jitter

Figure 439 Configuring Jitter VoIP Operations

| Attribute | Description |
|---|---|
| Operation Index | Unique identifier of the operation. |
| Name | IP SLA operation name. |
| Type | The type of operation to be performed. |

Table 136 UDP Jitter VoIP Operation Attributes

| Attribute | Description |
|---|---|
| Frequency | Sets the duration between initiating each operation. You should not set to a value which is of a shorter duration than *Timeout*. |
| Tag | A descriptive string used by Entuity to identify the operation target. |
| Owner | Identifies the creator of the operation, i.e. EYE. |
| Protocol | Protocol used by the operation. |
| Source Address | Specifies the IP address of the source. |
| Target Address | Specifies the IP address of the destination. |
| Source Port | The port on the source device used by the operation. When set to:<br>■ 0 (default) allows the operation to automatically select any available port.<br>■ a specific port number, ensures the operation uses that port. Take care that other operations on the same device do not use the same port, as the conflict can cause operations to fail. This is especially true when the conflict involves an operation that take a greater time to complete, e.g. UDP Jitter. |
| Target Port | This object represents the target's port number. |
| TOS | Defines the IP Type of Service (TOS) byte for request packets. This attribute may also be used as a Differentiated Services Code Point (DSCP). |
| Lifespan | IP SLA operation interval, by default **forever**, i.e. once created it exists forever on the device unless deleted by Entuity. You can enter a limited lifespan, by entering a value in seconds. When this time elapses the operation and Entuity has to recreate it. |
| VRF Name | Name of the MPLS IP VPN VRF. |
| Timeout | Length of time, in milliseconds, Entuity waits for a response from the IP SLA operation before marking it as timed-out. You should not set to a value which is of a greater duration than *Frequency*. |
| CODEC | Specifies the CODEC type to be used with the jitter operation. The options are:<br>■ **G.711 u-law**<br>■ **G.711 a-law**<br>■ **G.729A**. |
| CODEC Interval | Represents the inter-packet delay between packets and is in milliseconds. This object is applicable when *CODEC* is set. |
| CODEC Payload | Represents the number of octets that needs to be placed into the Data portion of the message. This object is applicable when *CODEC* is set. |
| CODEC Num Packets | This value represents the number of packets that need to be transmitted. This object is applicable when *CODEC* is set. |
| Advantage Factor | The user Advantage Factor (also known as the access Expectation Factor) used when calculating ICPIF. It places a value on the quality level a user expects from a particular type of service. By default it is set to zero. |

Table 136 UDP Jitter VoIP Operation Attributes

| Object Name | Attribute and Description |
|---|---|
| rttMonLatestRttOperCompletionTime | *Completion Time*. The latest completion time of RTT operations which complete successfully. |
| rttMonLatestJitterOperSumOfNegativesDS | *Jitter Dest-Src*. The sum of RTT's of all negative jitter values from packets sent from destination to source. |
| rttMonLatestJitterOperMaxOfPositivesSD | *Max. Jitter Src-Dest*. The maximum of all positive jitter values from packets sent from source to destination. |
| rttMonLatestJitterOperSumOfNegativesSD | *Jitter Src-Dest*. The sum of all negative jitter values from packets sent from source to destination. |
| rttMonLatestJitterOperMaxOfPositivesDS | *Max Jitter Dest-Src*. The maximum of all positive jitter values from packets sent from destination to source. |
| rttMonLatestJitterOperOWSumSD | *Delay Src-Dest*. The sum of one way latency from source to destination. |
| rttMonLatestJitterOperOWSumDS | *Delay Dest-Src*. The sum of one way latency from destination to source. |
| rttMonLatestJitterOperOWSumSD | *Sum Src-Dest*. The sum of one way latency from source to destination. |
| rttMonLatestJitterOperOWSumDS | *Sum Dest-Src*. The sum of one way latency from destination to source. |
| rttMonLatestJitterOperNumOfOW | *One Ways*. The number of successful one way latency measurements. |
| rttMonLatestJitterOperRTTSum | *RTT*. The sum of Jitter RTT's that are successfully measured. |
| rttMonLatestJitterOperRTTSum | *Sum RTTs*. The sum of Jitter RTT's that are successfully measured. |
| rttMonLatestJitterOperNumOfRTT | *Round Trips*. The number of RTT's that were successfully measured. |

Table 137 UDP Jitter VoIP Operation

# Appendix E  Operation Configuration Attributes

Entuity sets default values for IP SLA operation configuration attributes. Some of these values may be amended through web UI and RESTful API. (See *Entuity System Administrator Reference Manual*.)

## Implemented Commands

This section matches the IP SLA commands with Entuity's attribute names.

### Control Packets

**Description:** The IP SLA control protocol is a proprietary protocol for initial exchange between the IP SLA source and the responder. This must be enabled for use with IP SLA responders.

**Attribute Name:** *operationNameControlEnable*, where *operationName* is the name of the operation, e.g. TCPControlEnable.

**Default:** disabled

### Interval

**Description:** Sets how often the operation should send a operation out to gather statistics. This command applies to all operation types.

**Attribute Name:** *operationInterval*.

**Default:** 300 seconds

### owner

**Description:** Configures the SNMP owner of the operation. This command applies to all operation types.

**Default:** EYE

### request-data-size

**Description:** This command applies to the following operation types: ICMP Echo, ICMP path echo, UPD Echo, Jitter, DLSw, and frame relay.

**Default:** Varies according to operation type but always set in bytes.

### response-data-size

**Description:** This command applies only to SNA Echo operations.

**Default:** Varies according to operation type but always set in bytes.

### tag

**Description:** Logically links operations together in a group. This command applies to all operations.

**Default:** Entuity

### timeout

**Description:** Sets the amount of time the operation waits for a response from its request packet. This command applies to all operations.

**Default:** 100 seconds.

### tos number

**Description:** Defines the IP ToS byte for request packets. IP precedence uses the left-most three bits of the ToS byte.

When implementing DiffServ, precedence is still set using the left-most three bytes. Addtional priority is configured using the next three bytes. This option is useful for monitoring per-class traffic.

Bits six and seven are reserved for future use.

The tos command applies to the following operation types: HTTP, ICMP echo, ICMP path echo, ICMP path jitter, TCP connect, UDP echo and UDP jitter.

**Attribute Name:** *operationname*TOS

**Default:** 0

### vrf

**Description:** Allows monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using Cisco IOS IP Service Level Agreements (SLAs) operations.

This command applies to the following operation types in the Entuity Cisco IOS IP SLA: ICMP Echo, ICMP Path Echo, ICMP Path Jitter, UDP Echo and UDP Jitter.

**Attribute Name:** *vrf*

**Default:**

## Commands Not Implemented

This section lists the IP SLA commands not yet implemented in Entuity Cisco IOS IP SLA.

### lsr-path

**Description:** Loose Source Routing (LSR) allows specifying of a path for monitoring.

### threshold

**Description:** Set the rising threshold (hysteresis) that generates a reaction event and stores history information for the operation. This command applies to all operations.

### verify-data

**Description:** Checks each operation response for corruption. This command applies to the following operation types: ICMP Echo, ICMP path echo, ICMP path jitter, UDP echo, UDP jitter and UDP VoIP.

# Appendix F TFTP Server Configuration

This section is specific to the 32-bit TFTP server provided with Entuity when installed to Windows environments. In Solaris and Linux environments consult with your system administrator.

Entuity includes to *entuity_home*`\integ\TFTPServer`:

- License file.
- `tftpserver.ini`, this is an example initialization file.
- `TFTPServerMTInstallerv1.61.exe`, this is the TFTP server installer executable.

When you run the installer you can configure to where the TFTP server is installed, but the default location is `c:\Program Files (x86)\TFTPServer`. The installer installs:

- `ReadMeMT.txt`
- `RunStandAloneMT.bat`
- `TFTPServerMT.exe`
- `TFTPServerMT.ini`
- `TFTPServerMT.log`
- `TFTPServerMTInstallService.exe`
- `TFTPServerMTRemoveService.exe`.

The `TFTPServerMT.exe` and `TFTPServerMT.ini` files must remain in the same folder. You should amend the INI file to:

- Specify a home directory that is the same as that specified during Entuity `configure.`
- Permit TFTP server write and overwrite operations.

There are other configuration options available that you can use to amend TFTP server performance.

Always consult the TFTP server documentation.

## Example TFTP Server File Configuration

TFTP server can be configured through `TFTPServerMT.ini`, and is only required when not accepting the default TFTP server behavior. `TFTPServerMT.ini` must be in the same folder as the TFTP server executable, `TFTPServerMT.exe`.

This extract provides a simple `TFTPServerMT.ini`:

```
[LISTEN-ON]

[HOME]
```

```
c:\Entuity\cm_transfer\

[LOGGING]
Errors

[ALLOWED-CLIENTS]
10.44.1.0-10.44.1.11
10.44.1.13-10.44.1.255

[TFTP-OPTIONS]
```

where

- LISTEN-ON section, is used when you have more than one NIC card on your server and/or want to the card/interface used to listen for TFTP requests. The default listening port is 69. TFTP server can support up to 8 interfaces. The default is all interfaces, this specifies interface 49:

  ```
  69.254.185.131:49
  ```

- HOME section must be specified and is also specified during Entuity `configure`. Entuity recommend an explicit definition of drive and folder name, e.g.:

  ```
  c:\Entuity\cm_transfer\
  ```

- LOGGING, determines level of logging, e.g. **None**, **All**, **Errors** (default). **All** is resource intensive and not recommended. `TFTPServer.log` is created in the same directory as the TFTP executable. Logging only runs when TFTP server is run as a Windows Service.
- ALLOWED-CLIENTS section specifies permitted clients for TFTP Access. By default all clients are permitted. Through IP ranges you can control allowed clients, this range effectively disallows 10.44.1.12:

  ```
  10.44.1.0-10.44.1.11
  10.44.1.13-10.44.1.255
  ```

- [TFTP-OPTIONS] section through which you can further configure the TFTP server behavior:
  - *port-range*, port range on which TFTP server would respond from (default is any free port). When operating with a firewall you may like to restrict this to a suitable range, e.g.:

  ```
  port-range=30000-30100
  ```

  - *ThreadPoolSize*, number of threads ready for handling server requests, by default 1. Range is between 0 and 100. When there are not enough ready threads to handle requests, TFTP server creates and after usage deletes additional threads.

  ```
  ThreadPoolSize=5
  ```

  - *timeout*, default timeout, in seconds, per interval. Default is three seconds, although valid range is from 1 to 120.

  ```
  timeout=30
  ```

  - *blksize*, is the maximum block size on client request. The default is 512, unless overridden by the client, with a maximum of 65464.

```
blksize=65464
```

- *write*, a flag for allowing, or disallowing, writing of files on the server. The default is disallowed, **N**. It should be set to **Y** to allow the creation of new files on the server.

```
write=Y
```

- *overwrite*, a flag for allowing, or disallowing, overwriting of files on the server. The default is disallowed, **N**. It should be set to **Y** to allow the overwriting of files on the server.

```
overwrite=Y
```

## Example TFTPServerMT.ini

```
[LISTEN-ON]
#if you have more than one NIC card on your server
#can specify which cards will listen TFTP requests
#Specify the Interface you would like server to listen
#default listening port is 69, but can be overridden here
#up to 8 interfaces can be specified
#Default is All Interfaces
'128.254.185.131
'69.254.185.131:69

[HOME]
#You should specify home directory(s) here
#The home directory can be specified
#in two different ways, with alias or
#bare names without aliases. Using alias you
#can specify up to 8 directories like
#routers=c:\RouterImages\Images
#boot=d:\PXEBoot\Images
#installs=d:\PXEBoot\Images
#without aliases, only one directory can
#be specified, which will become root
#directory for tftp.
#mix-up of bare names and aliases not allowed
'c:\Installs
'routers=c:\RouterImages\Images
```

```
'boot=d:\PXEBoot\Images
'installs=c:\installs
c:\Entuity\cm_transfer\

[LOGGING]
#Logging is done in TFTPServer.log, in directory where exe is.
#Logging will be done only if run as NT Service.
#default is Errors
#Logging "All" is resources intensive, should not be normally used.
'None
Errors
'All

[ALLOWED-CLIENTS]
#These are permitted clients for TFTP Access.
#Hosts having IP address within these ip ranges
#only will be responded to DNS requests.
#32 ranges can be specified.
#If none is specified, then all are allowed
'192.168.0.1-192.168.0.254
'10.0.0.1-10.255.255.254
#block 10.44.1.12
10.44.1.0-10.44.1.11
10.44.1.13-10.44.1.255

[TFTP-OPTIONS]
#First Option is server port range on which tftpserver
#would respond from, if you have firewall
#issues, you may like to restrict this
#range. default is any free port
#do not use reserve ports less than 1024
#The Multithreaded TFTP Server listens the
#requests on port 69 but responds on any free
#port within these ranges, these are server
#ports not client ports, client can use any port
#if there is a fire wall issue, it should be
#opened for server ip for these ports.
'port-range=30000-30100
```

```
#Next is Thread Pool Size
#value of 0 means there is no thread pool
#threads will be created just in time and
#killed after serving requests.
#if simultaneous request are more than
#thread pool size, extra threads will be
#created and killed after serving requests
#but ready threads will never be less than this value
#min is 0, max can be 100, default is 1
'ThreadPoolSize=1

#Next is default timeout per interval
#if not overridden by client
#min is 1, max can be 120, default is 3 secs.
'timeout=3

#Next is max block size, allowed
#on client request. Max is 65464
#if not overridden by client
#it is always 512
'blksize=65464

#Next are the file operation permissions
#Clients can only read files if read is
#set to Y, default is Y
read=Y
#Clients can only create new files if write is
#set to Y, default is N
write=Y
#Clients can only overwrite existing files if
#overwrite is #set to Y, default is N
overwrite=Y
```

# Appendix G Entity Configuration Management Files

This section details components of the Entuity Configuration Management setup, together with example policy and pattern matching files that are included with the module.

When amending exclusion and policy files you should also rename them to ensure your changes are not overwritten during your next Entuity upgrade. These files are included to Entuity through sw_cm_transforms.cfg, you must therefore update this file with any filename changes or new files.

## Entuity Configuration Management Setup Summary

| Item | Description |
|---|---|
| **Configuration Files** | |
| Exclusions files | Specify text patterns that Entuity Configuration Management can safely ignore when trying to identify important configuration changes, e.g. timestamp changes. Entuity Configuration Management includes example generic exclusions files, e.g. cisco-generic-exclusions.cfg. |
| Policy files | Specify configuration lines that good and bad practice configurations should conform to. So, a device configuration that does not include a configuration setting defined in the include section of its associated policy file would cause Entuity Configuration Management to raise a CM Configuration Missing Policy Mandated Statement event.<br>Entuity supply example generic policy files for Cisco, HP and Juniper devices: cisco-generic-policies.cfg, hp-generic-policies.cfg.<br>You can amend their content to meet your requirements. |
| Retrieval Tasks | Entuity Configuration Management includes retrieval tasks for Cisco, Juniper, HP and Huawei devices. |
| entuity.cfg | entuity.cfg settings and defaults:<br>[lcm]<br>scriptDir=ENTUITY_HOME/integ/SCRAPE<br>expectProg=ENTUITY_HOME/integ/SCRAPE/expect(.exe)<br>FTPUsername=anonymous<br>FTPPassword=EYE<br>tftpServerIP=set via configure     <- this is the IP for FTP and TFTP<br>diffDir=ENTUITY_HOME/integ/etc |
| **configure Attributes** | |

Table 138 Configuring Entuity Configuration Management

| Item | Description |
|---|---|
| *Server IP Address* | The IP address of the Entuity server used by TFTP and/or FTP servers. Where the server has more than one address, for example it has IPv4 and IPv6 addresses, you can select the required address from the drop-down list. |
| *Transfer Directory* | The initial location for the retrieved configuration files. Retrieved configurations are placed here before they are moved to the Archive directory.<br>For example, with the supplied TFTP server the transfer directory should be the same as the home directory specified in the TFTP server initialization file.<br>Entuity recommend this is outside of the Entuity server directory structure, otherwise the directory could be deleted during Entuity upgrades. |
| *Archive Directory* | The location for the archived configuration files. Entuity strongly recommend this is outside of the Entuity server directory structure, otherwise the directory could be deleted during Entuity upgrades. |
| License file | Contains Entuity license details, including Entuity server version, licensed modules. You can temporarily use the evaluation license. |
| **Credential Sets created for each Device** | |
| Credentials | Credential are configured against each device. From the Inventory Administration page you can modify one or more device setups.They are used for accessing a device through Telnet or SSH. |
| **Configuration** | |
| *Configuration Retrieval Transfer Method* | Select from TFTP and FTP. |
| *Configuration Retrieval Excluded Differences File* | This file identifies configuration patterns for the device that Entuity Configuration Management can safely ignore. |
| *Configuration Retrieval Policy Rules* | This file specifies good and bad configuration which a device’s configuration should, respectively include and exclude. |
| *Configuration Retrieval Scheduled* | When set to True it enables scheduled retrieval. By default this is performed each night at 02.00.<br>User initiated monitoring, from the user action menu, is independent of scheduled retrieval. Entuity Configuration Management ensures only one request is processed at one time. |
| *Configuration Retrieval Number of Archives* | The number of versions of the device configuration files in the Archive folder. There is a separate count for startup and running configuration files. The default is four. |
| *Configuration Retrieval Debug Mode* | Enable debug mode when you are troubleshooting configuration retrieval. Debug provides greater detail on the processing of Entuity Configuration Management, displayed through events. |
| **TFTP Server Configuration (supplied TFTP server)** | |

Table 138 Configuring Entuity Configuration Management

| Item | Description |
|---|---|
| `TFTPServerMT.ini` | In the:<br>■ [HOME] section<br>set the directory to which the TFTP server does the initial saving of the configuration file. This must be the same as the Transfer Directory defined through `configure`, for example `c:\entuity\cm_transfer` When not set the TFTP server writes these files to the same folder as the TFTP server executable.<br>■ [TFTP-OPTIONS] section<br>set the file operation permissions to allow writing to these folders. |
| **FTP Server Configuration** | |
| `entuity.cfg` | Set when FTP credentials are set on the command line (see earlier section). |
| Preconfigure devices | Preconfigure devices on which Entuity uses FTP to retrieve device configuration:<br>`R837(config)#ip ftp password who-cares-its-anonymous`<br>`R837(config)#do sh run \| incl ftp`<br>`ip ftp username anonymous`<br>`ip ftp password`<br>`7 13121F1D460F05382E37653A21315E06180C0F4F54574647`<br>`R837(config)#` |

Table 138 Configuring Entuity Configuration Management

## Excluded Differences From Pattern Matching Files

When comparing configurations returned from a device, you are only interested in meaningful differences. For example, you know timestamps will differ between the two files, and for Entuity Configuration Management to raise an event would not be meaningful. Instead through a pattern matching file you can identify trivial changes, such as timestamps, that Entuity Configuration Management will not then raise events for.

You can identify to Entuity trivial changes by specifying them through a pattern matching file. Entuity Configuration Monitor includes an exclusions file for Cisco devices, `cisco-generic-exclusions.cfg`.

This extract includes two ignore pattern lines. The first ignores a changing timestamp, the second a clock change.

```
#---------------------------------------------------------------------

# Ignore patterns

#---------------------------------------------------------------------

# Ignore timestamps

! Last configuration change at.*

#Ignore ntp clock change

ntp clock-period.*
```

In pattern matching files:

- Lines starting with a hash, #, are considered as comments and are ignored.
- Patterns that span several lines should use \n (escape n) to signal a newline.
- Lines ending with a dot asterisk, **.***, include the wildcard character. This is used to allow matching on the parts of the line that vary from retrieval to retrieval. Matches must be otherwise exact. For example the pattern:

  ```
  service timestamps
  ```

  matches only the first of the following three lines

  ```
  service timestamps
  service timestamps debug uptime
  service timestamps log datetime
  ```

  This pattern:

  ```
  service timestamps.*
  ```

  matches each of the three lines.

All pattern matching is against the original text never against transformed text. Where a line matches one or more patterns, the line is handled the same as though it matched only one.

## Policy Mandated Statement Files

Policy Mandated Statement files allow you to specify good configuration that administrators should include to, and bad configuration that administrators should exclude from, the configuration of devices under their control. Entuity Configuration Management includes an example policy file for Cisco devices, `cisco-generic-policies.cfg`.

Each pattern is defined within its own section. The section names should be meaningful, as when a pattern is violated Entuity raises a policy violation event that includes the section name.

Include and exclude policy statements are defined in the same file. For illustrative purposes these include and exclude examples are explained separately.

### Policy Include Examples

```
[PolicyMustInclude logging]
IncludePattern=^logging.*

[PolicyMustInclude logging_buffered]
IncludePattern=^logging buffered.*

[PolicyMustInclude snmp_server]
IncludePattern=^snmp-server.*

[PolicyMustInclude no_ip_source-route]
IncludePattern=^no ip source-route.*
```

```
[PolicyMustInclude no_service_pad]
IncludePattern=^no service pad.*

[PolicyMustInclude no_ip_domain_lookup]
IncludePattern=^no ip domain lookup.*

[PolicyMustInclude interface_FastEthernet_no_ip_proxy-arp]
IncludePattern=^interface FastEthernet.*no ip proxy-arp.*

[PolicyMustInclude interface_FastEthernet_no_ip_unreachables]
IncludePattern=^interface FastEthernet.*no ip unreachables.*

[PolicyMustInclude interface_FastEthernet_no ip_redirects]
IncludePattern=^interface FastEthernet.*no ip redirects.*

[PolicyMustInclude interface_FastEthernet_no mop_enabled]
IncludePattern=^interface FastEthernet.*no mop enabled.*
```

where:

- ^logging.*, checks that logging is enabled.
- ^logging buffered.*, a second check for enabled logging, by checking the router has the buffer enabled.
- ^snmp-server.*, checks SNMP server is enabled.
- ^no ip source-route.*, checks that the sender of a packet cannot specify the route the packet should take.
- ^no service pad.*, checks service packet assembler/disassembler (PAD) functionality is disabled.
- ^no ip domain lookup.*, checks routers do not allow DNS lookup.
- ^interface FastEthernet.*no ip proxy-arp.*, checks proxy ARP is disabled on the device. Proxy ARP may have security and performance overhead:
  - Increasing the amount of ARP traffic on your segment.
  - Hosts need larger ARP tables to handle IP-to-MAC address mappings.
  - a machine can claim to be another in order to intercept packets, an act called "spoofing."
- ^interface FastEthernet.*no ip unreachables.*, checks the router configuration prevents sending of ICMP unreachable message, the information within which can be used for DNS ping attacks.
- ^interface FastEthernet.*no ip redirects.*, checks routers do not support IP redirects. IP redirects allow the sender to bypass the router and forward future packets directly to the destination (or a router closer to the destination).
- ^interface FastEthernet.*no mop enabled.*, checks maintenance operation protocol is disabled, reducing network traffic.

### Policy Exclude Examples

```
[PolicyMustExclude no_logging]
ExcludePattern=^no logging.*

[PolicyMustExclude no_snmp-server]
ExcludePattern=^no snmp-server.*

[PolicyMustExclude snmp-server_community_public]
ExcludePattern=^snmp-server community public.*

[PolicyMustExclude snmp-server_community_private]
ExcludePattern=^snmp-server community private.*

[PolicyMustExclude service_tcp-small-servers]
ExcludePattern=^service tcp-small-servers.*

[PolicyMustExclude service_udp-small-servers]
ExcludePattern=^service udp-small-servers.*

[PolicyMustExclude ip_finger]
ExcludePattern=^ip finger.*

[PolicyMustExclude ip_ident]
ExcludePattern=^ip ident.*

[PolicyMustExclude tftp-server]
ExcludePattern=^tftp-server.*

# The following might sometimes be desirable
[PolicyMustExclude ip_http_server]
ExcludePattern=^ip http server.*

[PolicyMustExclude service_config]
ExcludePattern=^service config.*

[PolicyMustExclude boot_network]
ExcludePattern=^boot network.*

[PolicyMustExclude interface_ip_mask_reply]
ExcludePattern=^interface.*ip mask reply.*

[PolicyMustExclude interface_ip_directed-broadcast]
ExcludePattern=^interface.*ip directed-broadcast.*
```

where:

- ^no logging.*, checks that logging is enabled.
- ^no snmp-server.*, checks SNMP server is enabled.
- ^snmp-server community public.*, checks that well known, and therefore insecure community strings are not used.
- ^snmp-server community private.*, checks that well known, and therefore insecure community strings are not used.
- ^service tcp-small-servers.*, checks whether TCP small server is enabled in the router. These services should not be activated unless it is absolutely necessary, as they exploited indirectly to gain information about the target system.
- ^service udp-small-servers.*, checks whether UDP small server is enabled in the router. These services should not be activated unless it is absolutely necessary, as they exploited indirectly to gain information about the target system or directly as is the case with the fraggle attack which uses UDP echo.
- ^ip finger.*, checks whether the finger command is enabled. It can be used to see what users are logged on to the network device.
- ^ip ident.*, checks whether querying a TCP port for identification is permitted.
- ^tftp-server.*, checks whether the Trivial File Transfer Protocol (TFTP) server is enabled. When enabled it provides basic file transfer functionality, with no user authentication.
- ^ip http server.*, check for the running of the HTTP service. Unless implementing authentication proxy, the HTTP service should not run on the router.
- ^service config.*, checks whether service configuration is enabled.
- ^boot network.*, checks whether boot for network software configuration file is allowed.
- ^interface.*ip mask reply.*, checks whether the Cisco IOS software responds to Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages.
- ^interface.*ip directed-broadcast.*, checks that the IP-directed broadcast service is not enabled. It is a service that is commonly used in Smurf attacks. Smurf attacks send ICMP echo requests from a spoofed source address to a directed broadcast that cause all hosts to respond to the ping echo request, creating a lot of traffic on the network.

# Appendix H  Scripting Configuration Management

Entuity Configuration Management includes an Expect API and a Groovy implementation through which you can manage device and port configuration. Entuity also includes a set of example scripts that you can use as a starting point when developing your own configuration scripts.

The scripts are a starting point from which you can extend and enhance the management of your network. This section explains the mechanics of the example scripts and the Groovy and Expect techniques used. It is not an introduction to, or tutorial on, developing Groovy scripts.

## Configuration Management Script Examples

As configuration scripts may be defined on a central server but run on a remote server it is important central and remote servers are running the same version of Entuity.

Entuity Configuration Management delivers a powerful tool set for managing ports and devices on your network. You are strongly advised to control user access to the Configuration Management module and fully test your scripts before applying them to your live network. The scripts provided here are only intended to illustrate the functionality and scripting techniques available with this module. Entuity accepts no liability in the event of the instructions in the documentation not being followed when using the module.

Entuity example tasks and steps are categorized as System tasks and steps. Login Script

This example login script checks for the device vendor, identifies the authentication setup of the device and responds appropriately. It is intended as the first step in tasks that require logging into devices, as such it:

- Sets parameters, for example `vendor`, `configPrompt`, `configIfPrompt` that are used by other steps subsequently called during the task.
- Sets diagnostic logging to **on** for all subsequent steps, unless one of the subsequent steps changes it.
- Sets tests that are performed before each expect interaction is processed (`expectBefore`).

```
expect.with
{
 setDiagnosticLogging( true )
 vendor = device.sysOid.split("\\.")[7]
 if( vendor.equals("9") )
 {
   println "Starting Cisco login"
   // look for first stage login, e.g. password, username, login
   // should then receive first stage login prompt, i.e. # or >
10.   expect( ~/(?i)(name:|login:|logon:|user:|username:)/ ,
11.    { sendln param.username; CONTINUE },
12.    ~/(?i)password:/ ,
13.    { sendPassword();
14.     sendln "; CONTINUE } ,
15.    ~/([a-zA-Z0-9\-_]+[#>]+)/, { } )
16.    // extract prompt
17.    prompt = getMatcher().group(0)
18.    // check to see if the prompt ends with '>' if so, issue the enable command
19.    String lastPromptCharacter = prompt.substring(prompt.length()-1)
20.    if( lastPromptCharacter.equals( ">" ) )
21.     {
22.      sendln "enable"
23.      expect( ~/(?i)password:/ ,
24.      { sendPassword2() ; sendln ""; CONTINUE } ,
25.       ~/([a-zA-Z0-9\-_]+[#>]+)/, { } )
26.       prompt = getMatcher().group(0)
27.     }
28.     // verify logged in and prompt ends in '#'
29.     lastPromptCharacter = prompt.substring(prompt.length()-1)
30.     if( ! lastPromptCharacter.equals( "#" ) )
31.      {
32.       println "FAILED TO LOGIN"
33.       throw new Exception("Failed to successfully login")
34.      }
35.     // create additional prompts for use in subsequent steps
36.     configPrompt = prompt.replaceAll( "#", "(config)#" );
37.     configIfPrompt = prompt.replaceAll( "#", "(config-if)#" );
38.     // add error detection
39.     expectBefore( ~/% Invalid / ,
40.     { throw new Exception("Device returned an error") },
41.     ~/Cannot find community / ,
42.     { throw new Exception("Missing community string") } )
43.    println "login complete"
44.    }
45.     else
46.      {
47.       println "NO VALID LOGIN"
48.       throw new Exception("no valid login method for this device")
49.      }
50. }
```

An overview of the login script structure:

- Line 4. finds the seventh character of the sysOID to identify the device vendor.
- Line 5. performs a check for the device vendor.

This script concentrates on Cisco but you could extended it to use with devices from other vendors.

- Lines 10. to 15. identify the login prompt, e.g. login, logon, and then sends the login value. They also identify the password prompt and send the password value.

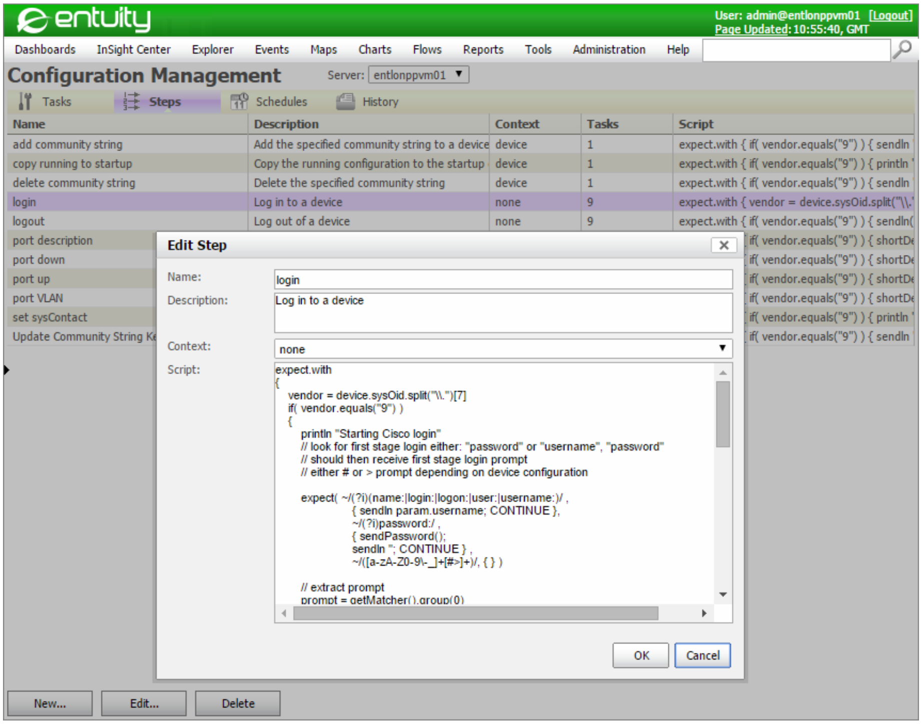
  The script disregards login banners that the device may display when first accessed.

`~/(?i)` indicates the subsequent check is case insensitive.

- Lines 16. to 19. extracts the prompt character returned after entering the user name and password. This is used to identify the current security mode of the device.
- Lines 20. to 27. checks for the prompt. If it equals > the script:
  - Sends the enable command.
  - Checks for the password prompt and sends the second password.
  - Extracts the device hostname and prompt character returned after entering the user name and password.
- Lines 28. to 34. check the prompt equals #, which would indicate a successful logon. If the login was unsuccessful the script raises an error message.

`throw new Exception` includes `new` as it ensures the device name is included in the raised error messages and therefore in the history log. If you do not include `new` the error would still be raised but would not include the device name.

- Lines 35. to 44. set up values that can be used in subsequent scripts called by the task:
  - Two variables to hold the device and interface configuration prompts.
  - `expectBefore` checks for patterns before any other pattern checking, in this case failure to login due to the device including invalid in its response or reporting a missing community string.
- Lines 45. indicates the device vendor was not Cisco. The script raises an error message. If you extend the script to include devices from other vendors it is here that you include the next if test.



Configuration Management

Server: entlonppvm01

| Name | Description | Context | Tasks | Script |
|---|---|---|---|---|
| add community string | Add the specified community string to a device | device | 1 | expect.with { if( vendor.equals("9") ) { sendln |
| copy running to startup | Copy the running configuration to the startup | device | 1 | expect.with { if( vendor.equals("9") ) { println ' |
| delete community string | Delete the specified community string | device | 1 | expect.with { if( vendor.equals("9") ) { sendln |
| login | Log in to a device | none | 9 | expect.with { vendor = device.sysOid.split("\\.' |
| logout | Log out of a device | none | 9 | expect.with { if( vendor.equals("9") ) { sendln( |
| port description | | | | if( vendor.equals("9") ) { shortDe |
| port down | | | | if( vendor.equals("9") ) { shortDe |
| port up | | | | if( vendor.equals("9") ) { shortDe |
| port VLAN | | | | if( vendor.equals("9") ) { shortDe |
| set sysContact | | | | if( vendor.equals("9") ) { println ' |
| Update Community String Ke | | | | if( vendor.equals("9") ) { sendln |

Edit Step

Name: login

Description: Log in to a device

Context: none

Script:

```
expect.with
{
   vendor = device.sysOid.split("\\.")[7]
   if( vendor.equals("9") )
   {
      println "Starting Cisco login"
      // look for first stage login either: "password" or "username", "password"
      // should then receive first stage login prompt
      // either # or > prompt depending on device configuration

      expect( ~/(?i)(name:|login:|logon:|user:|username:)/ ,
                  { sendln param.username; CONTINUE },
                  ~/(?i)password:/ ,
                  { sendPassword();
                  sendln ''; CONTINUE } ,
                  ~/([a-zA-Z0-9\-_]+[#>]+)/, { } )

      // extract prompt
      prompt = getMatcher().group(0)
```

Figure 440 Login Script

## Log Out Script

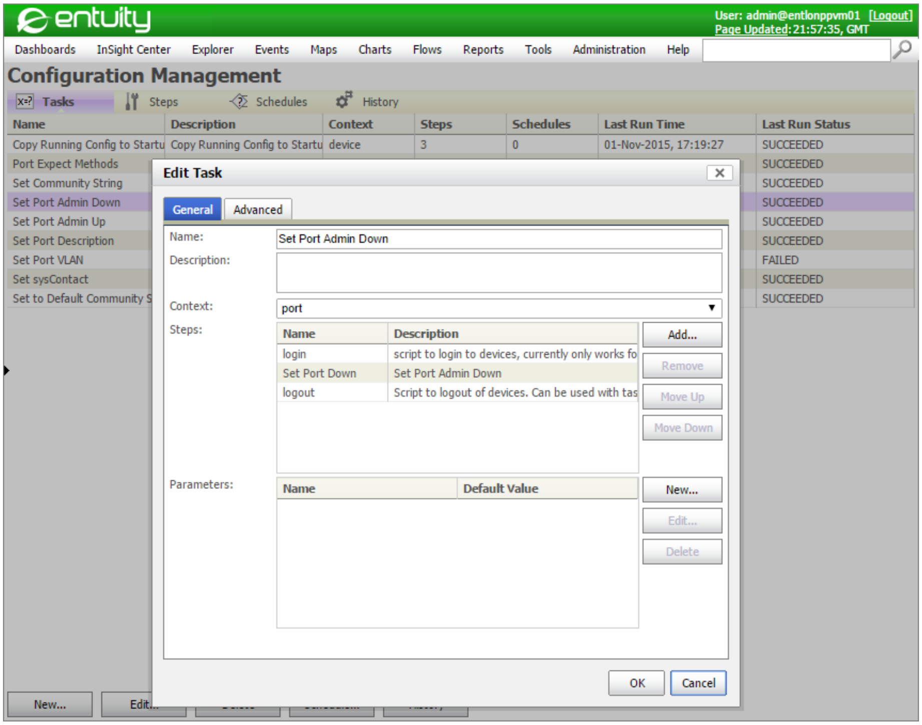
This example log out script only applies to Cisco devices. It sends four exit commands. Depending upon the login depth on the device not all of these exit commands are required, those that are not necessary are simply ignored.

The log out script is intended as the last step in tasks that required logging into devices.

```
expect.with
{
 if( vendor.equals("9") )
 {
  sendln( "exit" )
  sendln( "exit" )
  sendln( "exit" )
  sendln( "exit" )
 }
 else
 {
  println "NO VALID METHOD FOR THIS DEVICE"
  throw new Exception("no valid method for this device")
14.    }
15.  }
```

An overview of the log out script structure:

- Line 3. finds the seventh character of the sysOID to identify the device vendor.
- Line 4. to Line 9. send exit commands to the device.
- Line 10. to Line 14. return an error message when the device is not a Cisco device.



| Name | Description | Context | Steps | Schedules | Last Run Time | Last Run Status |
|---|---|---|---|---|---|---|
| Copy Running Config to Startu | Copy Running Config to Startu | device | 3 | 0 | 01-Nov-2015, 17:19:27 | SUCCEEDED |
| Port Expect Methods | | | | | | SUCCEEDED |
| Set Community String | | | | | | SUCCEEDED |
| Set Port Admin Down | | | | | | SUCCEEDED |
| Set Port Admin Up | | | | | | SUCCEEDED |
| Set Port Description | | | | | | SUCCEEDED |
| Set Port VLAN | | | | | | FAILED |
| Set sysContact | | | | | | SUCCEEDED |
| Set to Default Community S | | | | | | SUCCEEDED |

Name: Set Port Admin Down

Description:

Context: port

Steps:

| Name | Description |
|---|---|
| login | script to login to devices, currently only works fo |
| Set Port Down | Set Port Admin Down |
| logout | Script to logout of devices. Can be used with tas |

Parameters:

| Name | Default Value |
|---|---|

Figure 441 Task Using the Login and Logout Steps

## Set System Contact

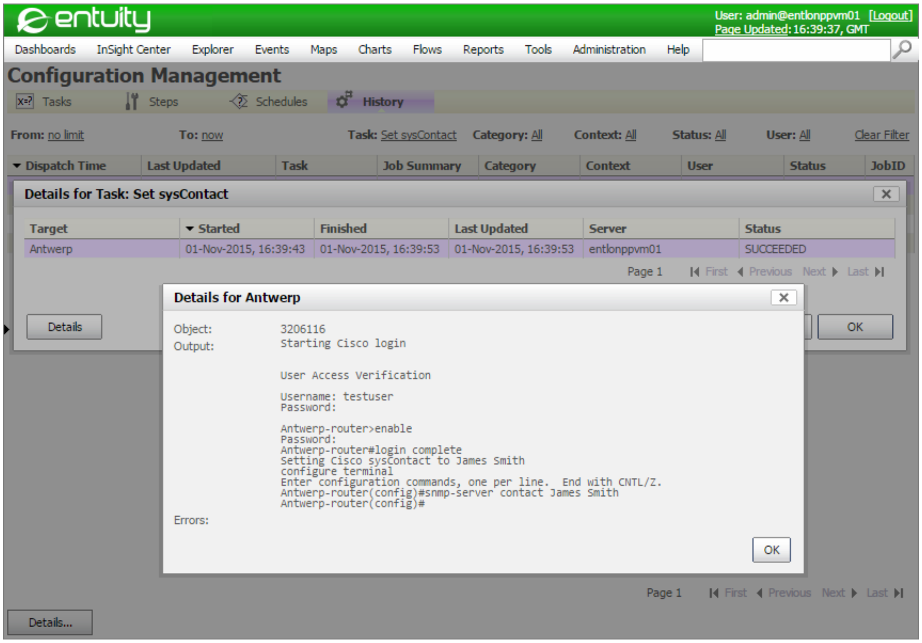
This example script sets the system contact for the selected Cisco device. It relies on the task that is calling the script having a `systemContact` parameter set to the contact name.

In Entuity system contact is an inventory attribute held against the device chassis. Inventory attributes are polled every 24 hours, this reflects their relatively unchanging nature when compared to performance and availability attributes. It may therefore be up to 24 hours before a change in the system contact is reflected in Entuity.

```
1.   expect.with
2.   {
3.    if( vendor.equals("9") )
4.   {
5.    println "Setting Cisco sysContact to " + param.systemContact
6.    sendln "configure terminal"
7.    expect( configPrompt, {} )
8.    sendln "snmp-server contact " + param.systemContact
9.    expect( configPrompt, {} )
10.  }
11.  else
12.  {
13.   println "NO VALID METHOD FOR THIS DEVICE"
14.   throw new Exception("no valid method for this device")
15.  }
16. }
```

An overview of the set system contact script structure:

- Line 3. finds the seventh character of the sysOID to identify the device vendor.
- Line 5. prints the name of the system contact, held in the task's `systemContact` parameter.
- Line 6. sets the terminal to configure.
- Line 7. checks the prompt is the expected terminal prompt. `configPrompt` is defined in the login script. If the prompt is not as expected the job would eventually return a timeout error.
- Line 8. sets the snmp-server contact to the value of the task's `systemContact` parameter.
- Line 11. to Line 15. return an error message when the device is not a Cisco device.



From: no limit To: now Task: Set sysContact Category: All Context: All Status: All User: All

Details for Task: Set sysContact

| Target | Started | Finished | Last Updated | Server | Status |
|---|---|---|---|---|---|
| Antwerp | 01-Nov-2015, 16:39:43 | 01-Nov-2015, 16:39:53 | 01-Nov-2015, 16:39:53 | entlonppvm01 | SUCCEEDED |

Details for Antwerp

Object: 3206116

Output:

```
Starting Cisco login


User Access Verification

Username: testuser
Password:

Antwerp-router>enable
Password:
Antwerp-router#login complete
Setting Cisco sysContact to James Smith
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Antwerp-router(config)#snmp-server contact James Smith
Antwerp-router(config)#
```

Errors:

Figure 442 Set System Contact

# Add Community String

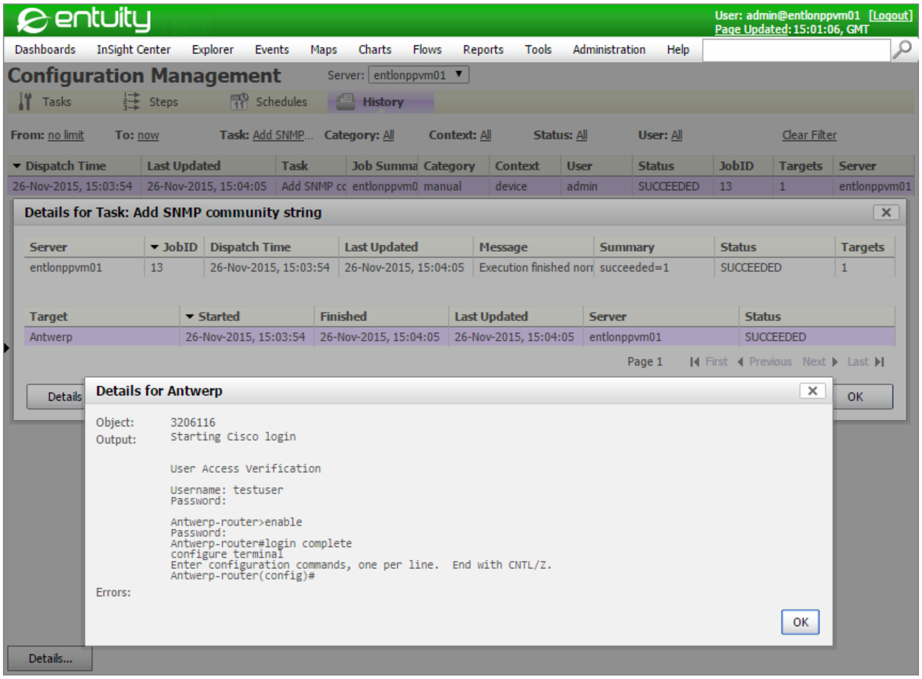
This example script adds a read only community string to the selected Cisco device. It relies on the task that is calling the script having a `newCommunity` parameter. Different tasks can use the same add community string step but have different values for their `newCommunity` parameter.

```
expect.with
{
 if( vendor.equals("9") )
 {
  sendln "configure terminal"
  expect( configPrompt, {} )
  setDiagnosticLogging false
  setLogUser false
  sendln "snmp-server community " + param.newCommunity + " ro"
  expect( configPrompt, {} )
  setLogUser true
  setDiagnosticLogging true
  }
 else
 {
  println "NO VALID METHOD FOR THIS DEVICE"
17.    throw new Exception("no valid method for this device")
18.   }
19.  }
```

An overview of the add read only community string script structure:

- Line 3. finds the seventh character of the sysOID to identify the device vendor.
- Line 5. sets the terminal to configure.
- Lines 7. and 8. turn off the terminal logging. This hides the community string from the display.
- Line 9. sets the snmp-server community to the value of the task's `newCommunity` parameter.
- Line 10. checks for the return of the prompt. This instruction is sent before turning on logging as it clears from the expect buffer the community string. The next two lines turn on logging and will clear the buffer displaying the prompt.
- Lines 11. and 12. turn on the terminal logging.
- Line 14. to Line 18. return an error message when the device is not a Cisco device.

  This script concentrates on Cisco but you could extended it to use with devices from other vendors.



Server: entlonppvm01

From: no limit To: now Task: Add SNMP... Category: All Context: All Status: All User: All Clear Filter

| Dispatch Time | Last Updated | Task | Job Summa | Category | Context | User | Status | JobID | Targets | Server |
|---|---|---|---|---|---|---|---|---|---|---|
| 26-Nov-2015, 15:03:54 | 26-Nov-2015, 15:04:05 | Add SNMP cc | entlonppvm0 | manual | device | admin | SUCCEEDED | 13 | 1 | entlonppvm01 |

Details for Task: Add SNMP community string

| Server | JobID | Dispatch Time | Last Updated | Message | Summary | Status | Targets |
|---|---|---|---|---|---|---|---|
| entlonppvm01 | 13 | 26-Nov-2015, 15:03:54 | 26-Nov-2015, 15:04:05 | Execution finished norı | succeeded=1 | SUCCEEDED | 1 |

| Target | Started | Finished | Last Updated | Server | Status |
|---|---|---|---|---|---|
| Antwerp | 26-Nov-2015, 15:03:54 | 26-Nov-2015, 15:04:05 | 26-Nov-2015, 15:04:05 | entlonppvm01 | SUCCEEDED |

Details for Antwerp

Object: 3206116

Output:

```
Starting Cisco login


User Access Verification

Username: testuser
Password:

Antwerp-router>enable
Password:
Antwerp-router#login complete
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Antwerp-router(config)#
```

Errors:

Figure 443 Add Community String

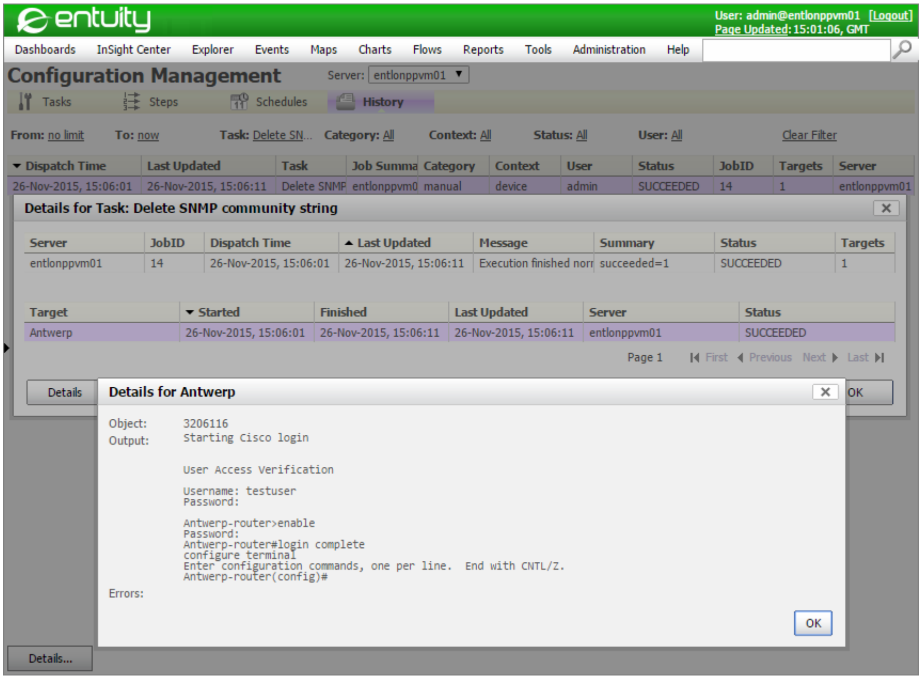
## Remove Community String

This example script deletes a read only community string from the selected Cisco device. It relies on the task that is calling the script having an `oldCommunity` parameter. Different tasks can use the same remove community string step but have different values for their `oldCommunity` parameter.

```
1.   expect.with
2.   {
3.    if( vendor.equals("9") )
4.    {
5.     sendln "configure terminal"
6.     expect( configPrompt, {} )
7.     setDiagnosticLogging false
8.     setLogUser false
9.     sendln "no snmp-server community " + param.oldCommunity + " ro"
10.    expect( configPrompt, {} )
11.    setLogUser true
12.    setDiagnosticLogging true
13.    }
14.   else
15.   {
16.    println "NO VALID METHOD FOR THIS DEVICE"
17.    throw new Exception("no valid method for this device")
18.   }
19.  }
```

An overview of the remove read only community string script structure:

- Line 3. finds the seventh character of the sysOID to identify the device vendor.
- Line 5. sets the terminal to configure.
- Lines 7. and 8. turn off the terminal logging. This hides the community string from the display.
- Line 9. removes the snmp-server community string that matches the value of the task’s `oldCommunity` parameter.
- Line 10. checks for the return of the prompt. This instruction is sent before turning on logging as it clears from the expect buffer the community string. The next two lines turn on logging and will clear the buffer and in doing so display the prompt.
- Lines 11. and 12. turn on the terminal logging.
- Line 14. to Line 18. return an error message when the device is not a Cisco device.



Configuration Management

Server: entlonppvm01

From: no limit To: now Task: Delete SN... Category: All Context: All Status: All User: All

| Dispatch Time | Last Updated | Task | Job Summa | Category | Context | User | Status | JobID | Targets | Server |
|---|---|---|---|---|---|---|---|---|---|---|
| 26-Nov-2015, 15:06:01 | 26-Nov-2015, 15:06:11 | Delete SNMP | entlonppvm0 | manual | device | admin | SUCCEEDED | 14 | 1 | entlonppvm01 |

Details for Task: Delete SNMP community string

| Server | JobID | Dispatch Time | Last Updated | Message | Summary | Status | Targets |
|---|---|---|---|---|---|---|---|
| entlonppvm01 | 14 | 26-Nov-2015, 15:06:01 | 26-Nov-2015, 15:06:11 | Execution finished norr | succeeded=1 | SUCCEEDED | 1 |

| Target | Started | Finished | Last Updated | Server | Status |
|---|---|---|---|---|---|
| Antwerp | 26-Nov-2015, 15:06:01 | 26-Nov-2015, 15:06:11 | 26-Nov-2015, 15:06:11 | entlonppvm01 | SUCCEEDED |

Details for Antwerp

Object: 3206116

Output:

```
Starting Cisco login

User Access Verification

Username: testuser
Password:

Antwerp-router>enable
Password:
Antwerp-router#login complete
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Antwerp-router(config)#
```

Errors:

Figure 444 Set Community String

# Compare Running and Startup Configurations

This script compares the Cisco device’s running and startup configurations. It is not included with the example scripts.

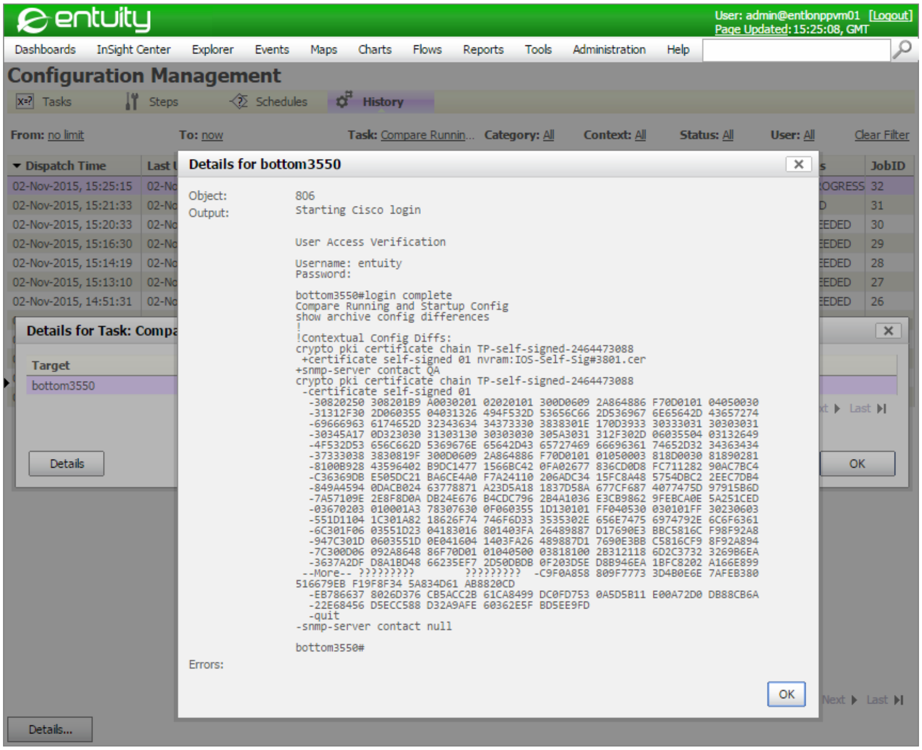
```
expect.with
{
 if( vendor.equals("9") )
 {
  println "Compare Running and Startup Config"
  sendln "show archive config differences"
  expect( prompt, {},"--More--", { send " "; CONTINUE})
 }
 else
 {
  println "NO VALID METHOD FOR THIS DEVICE"
  throw new Exception("no valid method for this device")
 }
}
```

An overview of the compare running configuration to the startup configuration script structure:

- Line 3. finds the seventh character of the sysOID to identify the device vendor.
- Line 5. prints the purpose of the script. This is available through the job history details.
- Line 6. sends the command to show the differences between the running configuration and startup configurations.
- Line 7. tests the response to the command. This has two purposes:
  - Building the running configuration takes time and without this line the script would complete before it had received a response from the device. `expect( prompt, {}` causes the script to wait until the prompt returns on the terminal and therefore it can receive the result of the configuration comparison.
  - The configuration comparison may return more than one page of data. The terminal command line would display `--More--` and wait for you to press the space bar to view the next page. `"--More--", { send " "; CONTINUE}` checks if there is another page to display and if so sends a space.

When you press the space bar in response to `--More--` the device deletes `--More--` from its cache before presenting the next page. When accessed from the command line this is invisible to the user, when accessed through Entuity Configuration Management it is captured as two blocks of question marks, i.e. **?????????     ?????????**.

- Line 9. to Line 13. return an error message when the device is not a Cisco device.


entuity
User: admin@entlonppvm01 [Logout]
Page Updated: 15:25:08, GMT
Dashboards InSight Center Explorer Events Maps Charts Flows Reports Tools Administration Help
Configuration Management
Tasks Steps Schedules History
From: no limit To: now Task: Compare Runnin... Category: All Context: All Status: All User: All Clear Filter
Dispatch Time Last U JobID
02-Nov-2015, 15:25:15 OGRESS 32
02-Nov-2015, 15:21:33 31
02-Nov-2015, 15:20:33 EEDED 30
02-Nov-2015, 15:16:30 EEDED 29
02-Nov-2015, 15:14:19 EEDED 28
02-Nov-2015, 15:13:10 EEDED 27
02-Nov-2015, 14:51:31 EEDED 26
Details for Task: Compa
Target
bottom3550
Details
OK
Next Last
Details...

**Details for bottom3550**

Object: 806

Output:

```
Starting Cisco login


User Access Verification

Username: entuity
Password:

bottom3550#login complete
Compare Running and Startup Config
show archive config differences
!
!Contextual Config Diffs:
crypto pki certificate chain TP-self-signed-2464473088
 +certificate self-signed 01 nvram:IOS-Self-Sig#3801.cer
+snmp-server contact QA
crypto pki certificate chain TP-self-signed-2464473088
 -certificate self-signed 01
  -30820250 308201B9 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  -31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  -69666963 6174652D 32343634 34373330 3838301E 170D3933 30333031 30303031
  -30345A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  -4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34363434
  -37333038 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  -8100B928 43596402 B9DC1477 1566BC42 0FA02677 836CD0D8 FC711282 90AC7BC4
  -C36369DB E505DC21 BA6CE4A0 F7A24110 206ADC34 15FC8A48 5754DBC2 2EEC7DB4
  -849A4594 0DACB024 63778871 A23D5A18 1837D58A 677CF687 4077475D 97915B6D
  -7A57109E 2E8F8D0A DB24E676 B4CDC796 2B4A1036 E3CB9862 9FEBCA0E 5A251CED
  -03670203 010001A3 78307630 0F060355 1D130101 FF040530 030101FF 30230603
  -551D1104 1C301A82 18626F74 746F6D33 3535302E 656E7475 6974792E 6C6F6361
  -6C301F06 03551D23 04183016 801403FA 26489887 D17690E3 BBC5816C F98F92A8
  -947C301D 0603551D 0E041604 1403FA26 489887D1 7690E3BB C5816CF9 8F92A894
  -7C300D06 092A8648 86F70D01 01040500 03818100 2B312118 6D2C3732 3269B6EA
  -3637A2DF D8A1BD48 66235EF7 2D50DBDB 0F203D5E D8B946EA 1BFC8202 A166E899
 --More-- ?????????        ?????????  -C9F0A858 809F7773 3D4B0E6E 7AFEB380
516679EB F19F8F34 5A834D61 AB8820CD
  -EB786637 8026D376 CB5ACC2B 61CA8499 DC0FD753 0A5D5B11 E00A72D0 DB88CB6A
  -22E68456 D5ECC588 D32A9AFE 60362E5F BD5EE9FD
  -quit
-snmp-server contact null

bottom3550#
```

Errors:

OK

Figure 445 Compare Running and Startup Configurations

## Copy Running Configuration to Startup Configuration

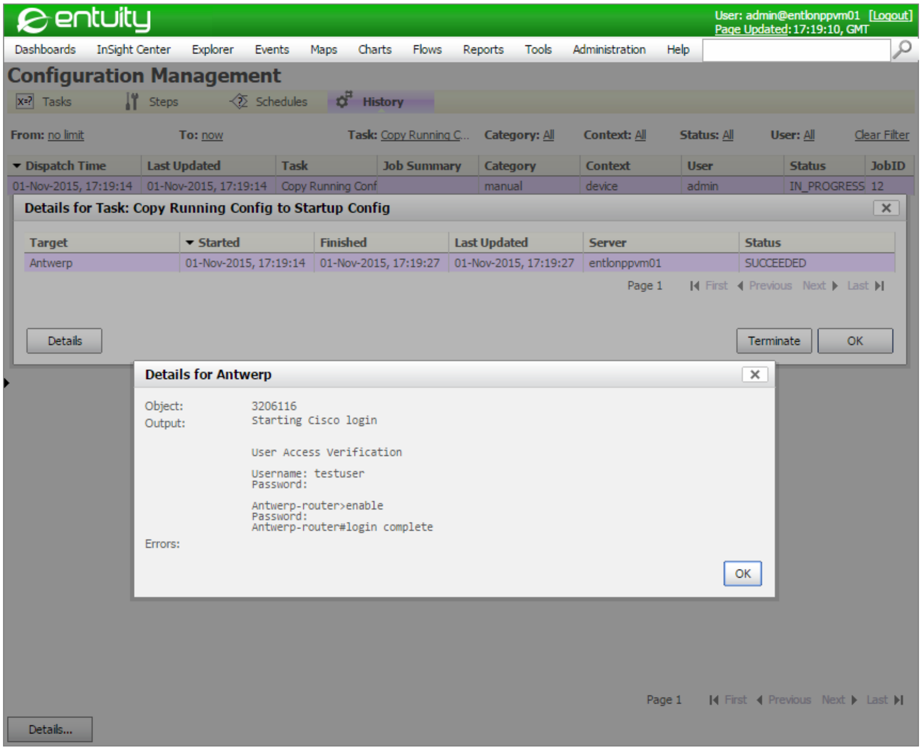
This example script copies the Cisco device’s running configuration over its startup configuration.

```
expect.with
{
 if( vendor.equals("9") )
 {
  println "copying running config to startup config"
  sendln "copy running-config startup-config"
  expect( prompt, {},
  "Destination filename [startup-config]?", { sendln '' ; CONTINUE } )
 }
 else
 {
  println "NO VALID METHOD FOR THIS DEVICE"
  throw new Exception("no valid method for this device")
 }
15.  }
```

An overview of the copy running configuration to the startup configuration script structure:

- Line 3. finds the seventh character of the sysOID to identify the device vendor.
- Line 5. prints the purpose of the script. This is available through the job history details.
- Line 6. sends the copy running configuration to startup configuration command.
- Line 8. sets the destination filename to the startup configuration.
- Line 11. to Line 15. return an error message when the device is not a Cisco device.

  This script concentrates on Cisco but you could extended it to use with devices from other vendors.



| Dispatch Time | Last Updated | Task | Job Summary | Category | Context | User | Status | JobID |
|---|---|---|---|---|---|---|---|---|
| 01-Nov-2015, 17:19:14 | 01-Nov-2015, 17:19:14 | Copy Running Conf |  | manual | device | admin | IN_PROGRESS | 12 |

Details for Task: Copy Running Config to Startup Config

| Target | Started | Finished | Last Updated | Server | Status |
|---|---|---|---|---|---|
| Antwerp | 01-Nov-2015, 17:19:14 | 01-Nov-2015, 17:19:27 | 01-Nov-2015, 17:19:27 | entlonppvm01 | SUCCEEDED |

Details for Antwerp

Object: 3206116

Output:

```
Starting Cisco login

User Access Verification

Username: testuser
Password:

Antwerp-router>enable
Password:
Antwerp-router#login complete
```

Errors:

Figure 446  Task Using the Login and Logout Steps

# Set Port Down

This example script sets the selected Cisco port to administration down.

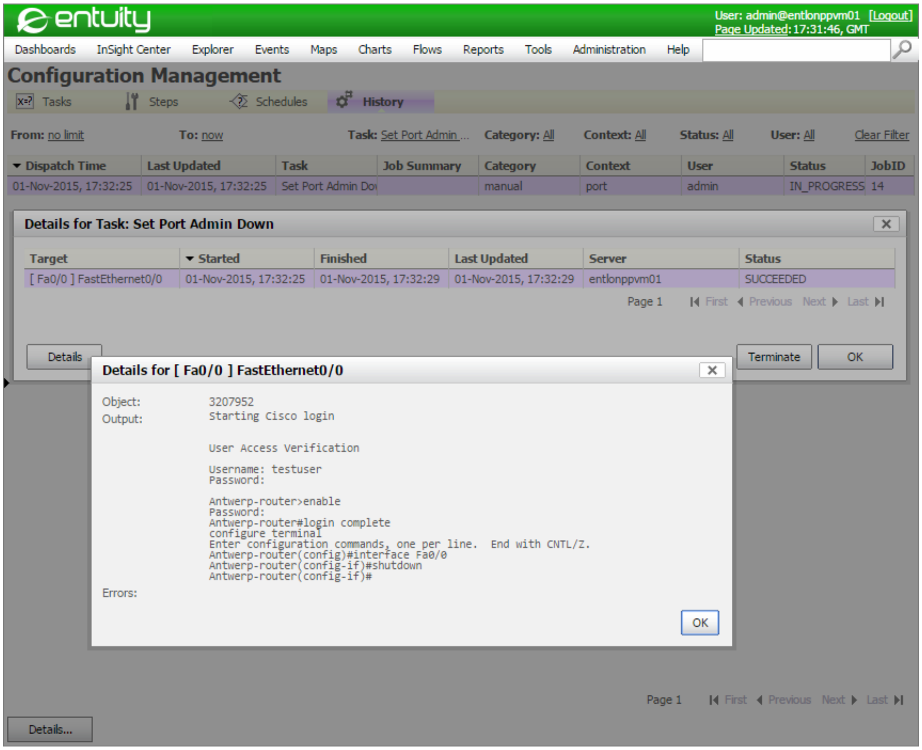
```
1.   expect.with
2.   {
3.    if( vendor.equals("9") )
4.    {
5.     shortDesc = target.portShortDescr
6.     portIdentifier = shortDesc.substring(2,shortDesc.length()-2)
7.     sendln "configure terminal"
8.     expect( configPrompt, {} )
9.     sendln "interface " + portIdentifier
10.    expect( configIfPrompt, {} )
11.    sendln "shutdown"
12.    expect( configIfPrompt, {} )
13.   }
14.   else
15.   {
16.    println "NO VALID METHOD FOR THIS DEVICE"
17.    throw new Exception("no valid method for this device")
18.   }
19.  }
```

An overview of the set port to administration down script structure:

- Line 3. finds the seventh character of the sysOID to identify the device vendor.
- Line 5. sets `shortDescr` to the short description of the selected interface.
- Line 6. extracts from `shortDescr` the port identifier by removing the square brackets and spaces that enclose the port identifier (this is the default format of interface names in Entuity).
- Line 7. sets the terminal to configure mode.
- Line 9. sets context to the selected interface (changing the prompt to the interface prompt).
- Line 11. sends the `shutdown` command to the port.

  Entuity will report the port Admin Status as down within five minutes of you taking it down.
- Line 14. to Line 18. return an error message when the device is not a Cisco device.

  This script concentrates on Cisco but you could extended it to use with devices from other vendors.



Configuration Management

From: no limit To: now Task: Set Port Admin ... Category: All Context: All Status: All User: All Clear Filter

| Dispatch Time | Last Updated | Task | Job Summary | Category | Context | User | Status | JobID |
|---|---|---|---|---|---|---|---|---|
| 01-Nov-2015, 17:32:25 | 01-Nov-2015, 17:32:25 | Set Port Admin Do |  | manual | port | admin | IN_PROGRESS | 14 |

Details for Task: Set Port Admin Down

| Target | Started | Finished | Last Updated | Server | Status |
|---|---|---|---|---|---|
| [ Fa0/0 ] FastEthernet0/0 | 01-Nov-2015, 17:32:25 | 01-Nov-2015, 17:32:29 | 01-Nov-2015, 17:32:29 | entlonppvm01 | SUCCEEDED |

Page 1 First Previous Next Last

Details for [ Fa0/0 ] FastEthernet0/0

Object: 3207952

Output:

```
Starting Cisco login


User Access Verification

Username: testuser
Password:

Antwerp-router>enable
Password:
Antwerp-router#login complete
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Antwerp-router(config)#interface Fa0/0
Antwerp-router(config-if)#shutdown
Antwerp-router(config-if)#
```

Errors:

Page 1 First Previous Next Last

Figure 447 Set Port Admin Down

## Set Port Up

This example script sets the selected Cisco port to administration up.

```
expect.with
{
 if( vendor.equals("9") )
 {
  shortDesc = target.portShortDescr
  portIdentifier = shortDesc.substring(2,shortDesc.length()-2)
  sendln "configure terminal"
  expect( configPrompt, {} )
  sendln "interface " + portIdentifier
  expect( configIfPrompt, {} )
  sendln "no shutdown"
  expect( configIfPrompt, {} )
 }
 else
 {
```

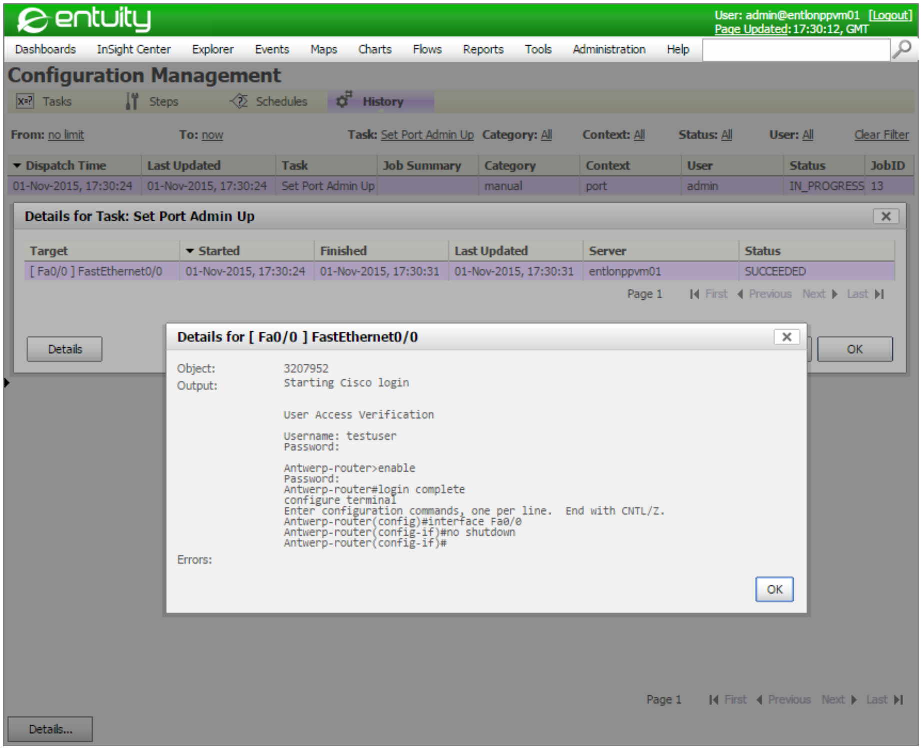
```
16.    println "NO VALID METHOD FOR THIS DEVICE"
17.    throw new Exception("no valid method for this device")
18.   }
19.  }
```

An overview of the set port to administration up script structure:

- Line 3. finds the seventh character of the sysOID to identify the device vendor.
- Line 5. sets `shortDescr` to the short description of the selected interface.
- Line 6. extracts from `shortDescr` the port identifier by removing the square brackets and spaces that enclose the port identifier (this is the default format of interface names in Entuity).
- Line 7. sets the terminal to configure mode.
- Line 9. sets context to the selected interface (changing the prompt to the interface prompt).
- Line 11. sends the `no shutdown` command to the port.

  Entuity will report the port Admin Status as up within five minutes of the script successfully completing.
- Line 14. to Line 18. return an error message when the device is not a Cisco device.

  This script concentrates on Cisco but you could extended it to use with devices from other vendors.



From: no limit To: now Task: Set Port Admin Up Category: All Context: All Status: All User: All

| Dispatch Time | Last Updated | Task | Job Summary | Category | Context | User | Status | JobID |
|---|---|---|---|---|---|---|---|---|
| 01-Nov-2015, 17:30:24 | 01-Nov-2015, 17:30:24 | Set Port Admin Up | | manual | port | admin | IN_PROGRESS | 13 |

Details for Task: Set Port Admin Up

| Target | Started | Finished | Last Updated | Server | Status |
|---|---|---|---|---|---|
| [ Fa0/0 ] FastEthernet0/0 | 01-Nov-2015, 17:30:24 | 01-Nov-2015, 17:30:31 | 01-Nov-2015, 17:30:31 | entlonppvm01 | SUCCEEDED |

Page 1 First Previous Next Last

Details for [ Fa0/0 ] FastEthernet0/0

Object: 3207952

Output:

```
Starting Cisco login


User Access Verification

Username: testuser
Password:

Antwerp-router>enable
Password:
Antwerp-router#login complete
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Antwerp-router(config)#interface Fa0/0
Antwerp-router(config-if)#no shutdown
Antwerp-router(config-if)#
```

Errors:

Page 1 First Previous Next Last

Figure 448 Set Port Admin Up

## Sends Port Description

This example script sets the selected Cisco port description.

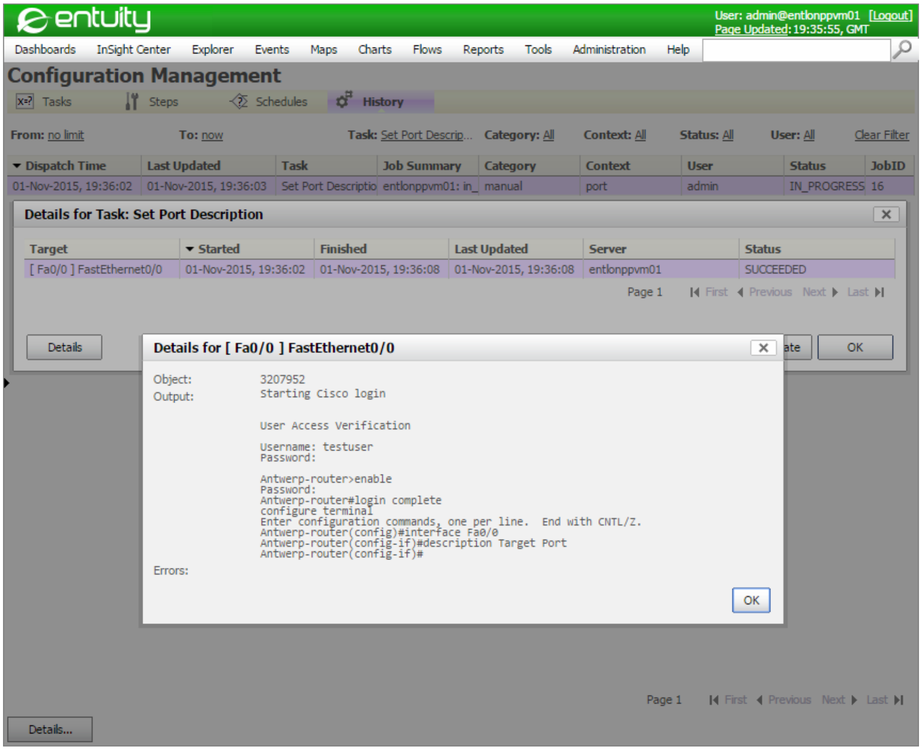
```
expect.with
{
 if( vendor.equals("9") )
 {
  shortDesc = target.portShortDescr
  portIdentifier = shortDesc.substring(2,shortDesc.length()-2)
  sendln "configure terminal"
  expect( configPrompt, {} )
  sendln "interface " + portIdentifier
  expect( configIfPrompt, {} )
  sendln "description " + param.portDescription
  expect( configIfPrompt, {} )
 }
 else
 {
```

```
16.    println "NO VALID METHOD FOR THIS DEVICE"
17.    throw new Exception("no valid method for this device")
18.   }
19.  }
```

An overview of the set port description script structure:

- Line 3. finds the seventh character of the sysOID to identify the device vendor.
- Line 5. sets `shortDescr` to the short description of the selected interface.
- Line 6. extracts from `shortDescr` the port identifier by removing the square brackets and spaces that enclose the port identifier (this is the default format of interface names in Entuity).
- Line 7. sets the terminal to configure mode.
- Line 9. sets context to the selected interface (changing the prompt to the interface prompt).
- Line 11. sends the new port description. `portDescription` is a parameter defined in the task from which the set port description step is called.
- Line 14. to Line 18. return an error message when the device is not a Cisco device.

  This script concentrates on Cisco but you could extended it to use with devices from other vendors.



| Dispatch Time | Last Updated | Task | Job Summary | Category | Context | User | Status | JobID |
|---|---|---|---|---|---|---|---|---|
| 01-Nov-2015, 19:36:02 | 01-Nov-2015, 19:36:03 | Set Port Descriptio | entlonppvm01: in_ | manual | port | admin | IN_PROGRESS | 16 |

Details for Task: Set Port Description

| Target | Started | Finished | Last Updated | Server | Status |
|---|---|---|---|---|---|
| [ Fa0/0 ] FastEthernet0/0 | 01-Nov-2015, 19:36:02 | 01-Nov-2015, 19:36:08 | 01-Nov-2015, 19:36:08 | entlonppvm01 | SUCCEEDED |

Details for [ Fa0/0 ] FastEthernet0/0

Object: 3207952

Output:

```
Starting Cisco login


User Access Verification

Username: testuser
Password:

Antwerp-router>enable
Password:
Antwerp-router#login complete
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Antwerp-router(config)#interface Fa0/0
Antwerp-router(config-if)#description Target Port
Antwerp-router(config-if)#
```

Errors:

Figure 449 Set Port Description

## Sends VLAN Number

This example script sets a VLAN to the selected port of the Cisco switch.

```
expect.with
{
 if( vendor.equals("9") )
 {
  shortDesc = target.portShortDescr
  portIdentifier = shortDesc.substring(2,shortDesc.length()-2)
  sendln "configure terminal"
  expect( configPrompt, {} )
  sendln "interface " + portIdentifier
  expect( configIfPrompt, {} )
  sendln "switchport access vlan " + param.VLANNumber
  expect( configIfPrompt, {} )
 }
 else
 {
```

```
16.    println "NO VALID METHOD FOR THIS DEVICE"
17.    throw new Exception("no valid method for this device")
18.   }
19.  }
```

An overview of the set port description script structure:

- Line 3. finds the seventh character of the sysOID to identify the device vendor.
- Line 5. sets `shortDescr` to the short description of the selected interface.
- Line 6. extracts from `shortDescr` the port identifier by removing the square brackets and spaces that enclose the port identifier (this is the default format of interface names in Entuity).
- Line 7. sets the terminal to configure mode.
- Line 9. sets context to the selected interface (changing the prompt to the interface prompt).
- Line 11. sends the new port description. `portDescription` is a parameter defined in the task from which the set port description step is called.
- Line 14. to Line 18. return an error message when the device is not a Cisco device.

  This script concentrates on Cisco but you could extended it to use with devices from other vendors.

## Expect Methods

| Method | Description |
|---|---|
| `equals` | Used to test that the value of a variable matches the comparison value, for example this tests that the value of vendor is 9:<br>`if( vendor.equals("9") )` |
| `expect` | Command are used when automating any interactive processes wait for the specific string from the process. For example, this command instructs to wait for the **Username** prompt to display before sending the username:<br>`expect.expect('Username', {sendln param.username; CONTINUE;}` |
| `expectAfter` | Performs the included actions at the end of each expect block. It has the format:<br>`public void expectAfter(Object ... args)` |
| `expectBefore` | Performs the included actions at the start of each expect block. It has the format:<br>`public void expectBefore(Object ... args)` |
| `getClass` | Determining Type of object at runtime. |
| `getMatched` | It returns the part of the buffer consumed up until the match. It has the format:<br>`public StringBuffer getMatched()` |

Table 139 Expect Methods

| Method | Description |
|---|---|
| `getMatcher` | Returns matcher to allow access to groups.. It has the format:<br>`public Matcher getMatcher()` |
| `getTimeout` | Returns the timeout value. It has the format:<br>`public int getTimeout()` |
| `hashCode` | Returns a hashcode for the object. |
| `log` | Writes to the Expect log but only if `DiagnosticLogging` is enabled. It has the format:<br>`public void log(String log)` |
| `notify` | Allows waking of one waiting thread, which can be used when you require a particular waiting thread to take action. |
| `notifyAll` | Allows waking of all waiting threads, which can be used when all waiting threads have been waiting for the current thread to complete. |
| `send` | Sends the command to the host without appending a newline. It has the format:<br>`public void send(String s)` |
| `sendPassword` | Sends the password without logging it. It has the format:<br>`public void sendPassword2()` |
| `sendPassword2` | Sends password2 without logging it. It has the format:<br>`public void sendPassword2()` |
| `sendln` | Sends the command to the host with an appended new line instruction. |
| `setDiagnosticLogging` | Sets the level of diagnostic logging. It has the format:<br>`public void setDiagnosticLogging(boolean diagnosticLogging)` |
| `setLogUser` | Controls terminal logging, which is on by default. To turn it off enter:<br>`expect.setLogUser false` |
| `setPassword` | Sets the password without logging it. |
| `setPassword2` | Sets password2 without logging it. |
| `setTimeout` | Sets the timeout. It has the format:<br>`public void setTimeout(int seconds)` |
| `toString` | Converts the data type to a string. |
| `wait` | Pauses the script until an expected character string is received from the host. |

Table 139 Expect Methods

## Manage Magic Values

A magic value is a literal value used within a script. It is recommended you set up named constants for each magic value and use that constant within your script. For example these declarations represent timeout, end of file and continue values respectively:

```
public final static Integer TIMEOUT = -1;
public final static Integer EOF = -2;
```

```
   public final static Integer CONTINUE = -3;
```

Setting these constants makes it easier to identify the purpose of the value and if you have to ever update it you only have to amend it once where you have declared it.

## Print Expect Methods and Bindings

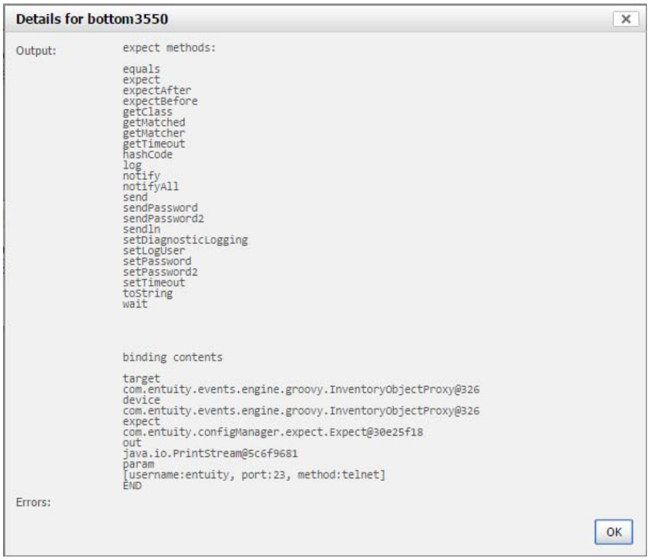
This script returns the available Expect methods and bindings. It must be run against a device for Entuity to then return the available Expect methods and bindings. The script is only intended for use when developing your first Expect scripts. The results are available through the job history details.

```
1.   println "expect methods:\n"
2.   expect.metaClass.methods*.name.sort().unique().each{
3.     println it
4.   }
5.   println "\n\n\n"
6.   println "binding contents\n"
7.   binding.variables.each{
8.     println it.key
9.     println it.value
10.  }
11.
12.  expect.with {
13.    setLogUser true
14.    println("END")
15.  }
```

An overview of the Expect Methods and Bindings script structure:

- Line 1. queries the groovy class for available methods. The statement orders the methods automatically and for clarity only returns one instance of each method.
- Line 3. outputs the returned methods. `it` does not require defining as the closure has only one parameter.
- Line 5. adds three line breaks to the output to improve its layout.
- Lines 7. to 10. iterate over the Groovy bindings. The script outputs the name of the variable and its value. For example target identifies the object against which the script is run.
- Lines 12. to 15. sets user level logging on and prints END when the script finishes.

To run the script against a device you must have credentials to access the device.



Output:

```
expect methods:

equals
expect
expectAfter
expectBefore
getClass
getMatched
getMatcher
getTimeout
hashCode
log
notify
notifyAll
send
sendPassword
sendPassword2
sendln
setDiagnosticLogging
setLogUser
setPassword
setPassword2
setTimeout
toString
wait



binding contents

target
com.entuity.events.engine.groovy.InventoryObjectProxy@326
device
com.entuity.events.engine.groovy.InventoryObjectProxy@326
expect
com.entuity.configManager.expect.Expect@30e25f18
out
java.io.PrintStream@5c6f9681
param
[username:entuity, port:23, method:telnet]
END
```

Errors:

Figure 450  Expect Method Results

# Appendix I BMC TrueSight Operations Management

You configure Entuity Event Management System to forward incidents and events to defined BMC TrueSight Infrastructure Management Servers and cells.

Incident and event forwarding is set up through:

- A set of configuration files to control the mapping of Entuity incidents and events to TrueSight Operations Management events.
- `configure` to set up the default TrueSight Infrastructure Management Server and cell to be used with incident and event forwarding. These details must are stored in `bem.cfg`.
- Event Management System and the Send to BMC Event Manager action.

| File Location | Filename |
|---|---|
| Generated by `configure` and saved to *entuity_home*/`install/template/etc` and *entuity_home*/`etc` | `bem.cfg` |
| *entuity_home*/`integ/BEM/etc` | `BEMEventTypes.properties`<br>`BEMSeverityMapping.properties` |
| *entuity_home*/`integ/BEM/server/etc/CELL/kb/` | `classes/eye_event.baroc`<br>`collectors/eye_collector.mrl`<br>`rules/eye_integration.mrl` |
| *entuity_home*/`integ/BEM/console/etc/event_op/` | `eye_actions.xml`<br>`eye_cross_launch`<br>`eye_cross_launch.cmd`<br>`LocalActions.xml` |
| *entuity_home*/`integ/BEM/lib/` | `BMCEventManager.jar`<br>`iiws-client-stub.jar`<br>`sendEvents.jar` |
| *entuity_home*/`log` | `BemEventEngine.log`<br>`BemEventEngineFailedSent.log`<br>`BemEventEngineSent.log` |
| *entuity_home*/`etc` | `bem.cfg`<br>`bem-connections-example.cfg`<br>`bem-connections.cfg` (user defined configuration file) |

Table 140 TrueSight Infrastructure Management Server Files

## TrueSight Infrastructure Management Server Forwarding Configuration Files

Entuity forwarding events and incidents to TrueSight Infrastructure Management Server uses configuration files:

- During `configure` you set the connection between Entuity and the TrueSight Infrastructure Management Server server (`bem.cfg`).
- Map the different event severity levels of the two sets of software (`BEMSeverityMapping.properties`).
- Map Entuity event fields to TrueSight Infrastructure Management Server slots, using existing slots or ones created for Entuity (`sw_bem_menu_def.cfg`).
- Define the Entuity event class (`eye_event.baroc`).
- To configure additional TrueSight Infrastructure Management Servers and cells to forward incidents and events (`bem-connections.cfg`).

## bem.cfg

`bem.cfg` is automatically generated by `configure`. It defines the connection between Entuity and the TrueSight Infrastructure Management Server cell.

```
[connection]

cellname=entuity

webServerHostName=decade

webServerPortNumber=9080

webServiceName=ImpactManager

refreshCache=3600
```

where:

- *Cellname*, the TrueSight Infrastructure Management Server instance to which Entuity forwards events.
- *webServerHostName*, hostname of the server where the BMC II Web Services Server is located.
- *webServerPortNumber*, the port number used by the BMC II Web Services Server, by default **9080**.
- *webServiceName*, the name of the web service, by default **ImpactManager**.
- *refreshCache* is the time in seconds that the integration slots are maintained in memory by Entuity, after which Entuity automatically initiates a refresh of the list. The default value is **3600**.

## bem-connections.cfg

When you want to forward events and incidents to more than one TrueSight Infrastructure Management Server you define the additional connections in *entuity_home*\etc\`bem-connections.cfg`. Entuity includes an example connections file *entuity_home*\etc\`bem-connections-example.cfg` which you can rename to `bem-connections.cfg` and then amend its connection details.

The default connection remains the connection defined through `configure` and stored in `bem.cfg`, to use the additional connections you must specify them by name.

It defines the connection between Entuity and the TrueSight Infrastructure Management Server cell.

```
[connection C1]
cellname=entuity
webServerHostName=decade
webServerPortNumber=9080
webServiceName=ImpactManager
```

where:

- *connection* is the connection name referred to when specifying where the BMC Event Manager action forwards events and incidents.
- *Cellname*, the TrueSight Infrastructure Management Server instance to which Entuity forwards events.
- *webServerHostName*, hostname of the server where the BMC II Web Services Server is located.
- *webServerPortNumber*, the port number used by the BMC II Web Services Server, by default **9080**.
- *webServiceName*, the name of the web service, by default **ImpactManager**.
- *refreshCache* is the time in seconds that the integration slots are maintained in memory by Entuity, after which Entuity automatically initiates a refresh of the list. The default value is **3600**.

## BEMSeverityMapping.properties

BEMSeverityMapping.properties maps Entuity event severity levels to TrueSight Operations Management event severity levels:

```
EYE_SEVERITY_CRITICAL=BEM_SEVERITY_CRITICAL
EYE_SEVERITY_SEVERE=BEM_SEVERITY_MAJOR
EYE_SEVERITY_MAJOR=BEM_SEVERITY_MINOR
EYE_SEVERITY_MINOR=BEM_SEVERITY_WARNING
EYE_SEVERITY_INFO=BEM_SEVERITY_OK
```

## TrueSight Operations Management Entuity Event Class

`eye_event.baroc` defines the Entuity event class for use in the TrueSight Infrastructure Management Server. Each element within the definition is a slot. This example creates the additional fields required to manage Entuity event information in the sample integration:

```
MC_EV_CLASS :
            EYE_EVENT ISA EVENT
            DEFINES
            {
                   mc_object: dup_detect=yes;
                   mc_tool_id: dup_detect=yes;
                   eye_userId: STRING;
```

```
                                eye_impact_descr: STRING;
                                eye_stormworks_id: STRING;
                                eye_comp_id: STRING;
                                eye_event_group: STRING, dup_detect=yes;
                                eye_event_id: STRING, dup_detect=yes;
                        };
            END
```

# Glossary

## 802.1p

An IEEE standard for providing quality of service (QoS) in 802-based networks. 802.1p uses three bits (defined in 802.1q) to allow switches to reorder packets based on priority level. It also defines the Generic Attributes Registration Protocol (GARP) and the GARP VLAN Registration Protocol (GVRP). GARP lets client stations request membership in a multicast domain, and GVRP lets them register into a VLAN.

## AAL (ATM Adaptation Layer)

AAL enhances the service provided by the ATM layer to a level required by the next higher layer. It performs the functions for the user, control and management planes and supports the mapping between the ATM layer and the next higher layer.

## Advanced Actions

Advanced Actions, also known as user menus and user actions, are defined through configuration files. Actions may be automatically triggered through Entuity raising an appropriate event, or interactively through advanced action menus, available both from the menu bar and context menus.

## Agent

Intelligent management software embedded in a network device. In network management systems, agents reside in all managed devices and report the values of specified variables to management stations.

## Antenna / Radio

Each Wireless Access Point has one or more Antennas. Each Antenna is attached to an 802.11 radio within the Access Point. Wireless Hosts communicate with the network via a wireless association with an Antenna/Radio. Each Antenna/Radio can have multiple hosts simultaneously attached. Each Antenna/ Radio operates in a chosen 802.11 compatibility mode such as 802.11a, 802.11b or 802.11g. Additionally, each Antenna/Radio has a single SSID assigned. Each Antenna/Radio operates on a chosen radio channel and with a specified transmit power setting, which is measured in mW. Many controller based installations use dynamic optimization algorithms to pick a suitable channel and power setting. Frequent auto-adjustment of these setting indicates that there are problems being encountered with the quality of the wireless communications.

## AP (Access Point) / WAP (Wireless Access Point)

A device that has one or more 802.11 radios and Wireless Antennas. For example, laptops, PDAs, connect to a wired LAN through an AP, which is a hardware device or software that acts as a communication hub.

It bridges traffic from wireless attached hosts to/from an Ethernet interface that connects to an access layer switch port. APs provide heightened wireless security and extend the physical range of a wireless

LAN. The access layer switch will see the MAC addresses of the individual wireless attached hosts (the MAC address of the wireless NICs) plus the MAC of the Access Point Ethernet interface.

### AR System

BMC Remedy Action Request System (AR System) is a framework within which applications are built by AR System administrators. Applications consist of a set of AR System forms that are linked using workflow rules designed for the application. These forms contain fields which Entuity can be configured to populate.

### ARs

Entuity integrates with AR System to generate Action Requests (ARs). The sample integration with the Remedy Help Desk includes ARs of the type incident.

### ARP

ARP (Address Resolution Protocol) is the layer 2 standard for TCP/IP. It is used to obtain a node’s physical address when only its logical IP address is known.

### ATM

ATM (Asynchronous Transfer Mode) is a packet-switching technology, that delivers high-speed performance together with a scalable architecture. Its use of small packets (fixed length cells of 53 bytes), provide for low latency so sound and vision arrive together. It can also handle bursty, non time-sensitive data, translating variable length packets to fixed size packets.

### Attribute

In Entuity an attribute is a property of an object that is defined through StormWorks. Attribute data can be charted using the Attribute Grapher and is available to Report Builder.

### Autonomous Wireless Access Point (AWAP)

A Wireless Access Point (WAP) that embodies all of its necessary control functionality in a self-contained manner. AWAPs are usually connected to switched access layer ports and can coexist with ordinary wired connections to end user hosts and servers on the same switch. AWAPs do not require wireless controllers and do not interact with them if they exist.

### Backbone

The part of a network that acts as the primary path for traffic that is most often sourced from, and destined for, other networks.

### BECN (Backward Explicit Congestion Notification)

BECN is a bit in the header of a frame-relay frame that is set when frames are sent on the data path backwards from destination to source. It indicates congestion to the source node.

Frame relay functionality combines BECN and FECN values to determine congestion on a data path.

## Bandwidth

The upper limit of the rate at which data can be transferred.

## BMC Atrium CMDB

The BMC Atrium Configuration Management Database (BMC Atrium CMDB) is a data repository that provides a working model of your enterprise IT infrastructure.

## BMC Cell

BMC Impact Manager instance. A cell receives events from Entuity and displays them in the BMC IX.

## BMC II Web Services Server

BMC Impact Integration Web Services Server. You can connect to the BMC II Web Services at the end point as defined by the URL format,  http://*webServerHostName*: *webServerPortNumber*/ *webServiceName*, e.g. http://decade:6080/impactManager.

## BMC IX

BMC IX (BMC Impact Explorer) displays events received from Entuity.

## BMC ProactiveNet Performance Management

BMC ProactiveNet Performance Management which receives events from Entuity.

## Blackout

Blackout is complete loss of the network, as opposed to a brownout, which is degradation in the performance of the network.

## BPDU

Bridge Data Protocol Units are special frames that contain spanning tree information. There are two types of BPDU, Topology Change Notification (TCN) BPDU contains topology change information, Configuration BDU contain configuration information.

## Bridge

A device that interconnects local or remote networks. Bridges form a single logical network, centralizing network administration. They operate at the physical and link layers of the OSI Reference Model.

## Brownout

Brownouts, also known as soft faults, are typically caused by cabling faults, faulty transceivers, faulty NIC cards and configuration errors such as duplex/half-duplex mismatches. These problems cause a percentage of the packets traversing that particular area of the network to be corrupted. The total number of packets discarded as a percentage of packets is directly related to the severity of the brownout.

## Burst

Burst is the access rate of the physical connection to the Frame Relay carrier network.

## Central Server

A central server is an Entuity server trusted by remote Entuity server(s). A user logged into the central Entuity server is able to view information collected by the remote Entuity server(s), according to their user account access rights. A remote Entuity server responds to requests from a trusted central Entuity server, and freely shares information with it.

An Entuity server can be configured to perform both roles, be both a remote and central Entuity Server. This allows administrators to create both hub-n-spoke and fully meshed deployments.

A central Entuity server can also act as a central license server. From it you can allocate, and de-allocate, license credits to its remote servers.

Configuration of central and remote servers is through the Multi-Server Administration area of the Entuity web UI.

## CDP (Cisco Discovery Protocol)

CDP is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media- and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Entuity uses CDP as a method when maintaining links on maps and identifying trunk ports.

## CI

Within BMC Atrium CMDB a Configuration Item (CI) is a collection of objects related to the specific functionality of a larger system.

## CIR

Committed Information Rate is the rate (in bps) that the network agrees to transfer information over a permanent virtual circuit (PVC) in Frame Relay. The CIR applies to the rate of data entering the network.

## Cisco IOS IP SLA Operations

Cisco IOS IP SLA Operations are created on devices by Entuity (via SNMP). Entuity currently fully supports DHCP, DNS, HTTP, HTTP Raw, ICMP Echo, ICMP Path Echo, TCP, UDP Echo, UDP Jitter and UDP Jitter VoIP operations. Entuity can also monitor operations other than these ten, for example FTP.

The completeness of the returned data depends upon how close the operation’s data structure corresponds to Entuity’s default representation of the IP SLA operation data structure.

These are the ten fully supported operations:

- DHCP, Verify availability of dynamic IP addresses.
- DNS, DNS server functionality check.
- HTTP, Web page availability.
- HTTP Raw, Web page availability.
- ICMP Echo, Simple connectivity tests.
- ICMP Path Echo, Simple connectivity tests.
- TCP, Connect Application availability.
- UDP Echo, Simple connectivity tests.
- UDP Jitter, Detailed latency measurements (requires IP SLA on both devices).
- UDP Jitter VoIP, Detailed latency measurements (requires IP SLA on both devices).

## Collisions

Collisions occur when two transmitters attempt to send data at the same time. The greater the number of collisions the poorer network performance appears.

## Context Menus

Context menus are available from the Entuity web UI and Component Viewer. The contents of the menu are dependent on the position of the mouse when you clicked the right button.

## Core Ports

Entuity considers core ports, as WAN ports, administratively up ports which have a configured IP addresses (i.e. layer 3 ports) on devices which are routers or have router capability, or trunks and uplinks that are administratively up.

By default the port status event, Port Operationally Down, is only enabled for core ports.

## Current Configuration

The device configuration (either startup- or running) currently being processed.

## DLCI (Data Link Connection Identifier)

A unique logical identifier assigned to a PVC end point in a frame relay network. It identifies a particular PVC endpoint within a user’s access channel therefore allowing multiple connections to many destinations over a single, physical channel.

## Data Management Kernel (DMK)

The DMK supports Entuity's intelligent discovery function. It includes out of the box data models for a wide range of managed devices including hundreds of Ethernet switches and routers. These customizable data models define the attributes of each managed element, its possible dependencies in relation to other elements of the network, and the specific details to retrieve for each element. The DMK manages these data models and automatically applies updates and changes to the Entuity database schema.

## Data Path

A data direction on each PVC is a data path. For example, a PVC that connects points A and B has two data paths, from A to B and from B to A. Frame relay functionality analyzes the data paths separately.

## Data Rollup

Data Rollup is a method of taking polled data and bundling it into larger more manageable units, e.g. rolling 24 hourly datapoints into one daily sample. If Entuity generated monthly reports from live polled data then this would cause a significant increase on the processing overhead, i.e. instead of one datapoint for each day there would be hundreds.

## DE (Discard Eligibility)

DE is a bit in the header of a frame-relay frame that indicate the frame may be discarded in preference to other frames if congestion occurs. It is usually set by a network node if the user is offering data (frames) at a higher rate than has been negotiated. This maintains the committed quality of service within the network. Frames with the DE bit set are considered to be excess data.

## Derived Events

IA derived event is an event derived from an existing event definition. It retains the event identifier of the original definition, unlike a custom event which has its own unique identifier. Derived events are defined as part of an action. They useful for adding additional information to an incoming event, and can also be called from an incident.

## Devices

In Entuity devices refers to network devices, for example switches and routers.

## Device Support Datasets

Device support datasets define the attributes of each managed element, its device type, its possible dependencies in relation to other elements of the network, and the specific details to retrieve for each element. This comprehensive library streamlines modeling and ultimately shows exactly what you own, where it is deployed and how it is connected.

Datasets are available through these types of vendor files, all have a .vendor extension. These vendor files are, listed in ascending order of priority:

- `newbin.vendor`, which is created in *entuity_home*\etc when Entuity discovers devices with sysoids for which there is not a device support dataset. These generic device support datasets should be considered temporary definitions, and only used until Entuity supply an appropriate vendor file.

Device support datasets in `newbin.vendor` have the lowest priority when Entuity is determining which vendor device definition to use to manage a device type.

- `bin.vendor` has the second lowest priority when Entuity is determining the source of device information.Device support datasets in bin.vendor have the second lowest priority when Entuity is determining which of those available to use to manage a device type.
- exotica vendor files are installed to *entuity_home*`\etc\exotica`. Exotica files are only used by Entuity when they are copied to *entuity_home*`\etc`, either manually or during Entuity configuration, e.g. when selecting a module.

  Device support datasets in exotica vendor files have the highest priority when Entuity is determining which vendor device definition to use to manage a device type.These files use a simple naming convention, using the vanilla filename, with a plus sign in the filename and identifying name, e.g. `SOLSERV+managed Host.vendor`.

  During Entuity upgrades configure identifies and removes exotica files from the installation that are now part of the updated bin.vendor.

`vendinfo` identifies the vendor device support datasets available to Entuity and the decisions made when more than one vendor file is available for a particular sysoid; which device support dataset Entuity uses to manage that device type (as identified through its sysoid).

## Device Types

In Entuity every device has a type, which you can view through the web interface and Component Viewer. The device type is derived from its vendor file information, and helps to determine how Entuity manages a device. Device types include hubs, switches and routers. There are also two Unclassified device types, Basic Management and Ping Only, and also Full Management.

Unclassified device types have two distinct roles:

- Basic Management and Ping-only, is used for those devices Entuity has taken under management at the Basic Management and Ping-only level.
- Full Management, is used for those devices Entuity has taken under management at the Full level but for which there is no vendor file information but Entuity can generate a suitable generic device type. These are uncertified devices.

## Domains

Domains and domain filters are terms used within Component Viewer, in fact supplied domains are now only used within Component Viewer to group objects in its Explorer tree, e.g. the routers domain. In the web UI, where you manage views In Entuity, domain filters are referred to by the more apt term view content filters as they determine the type of object that can potentially appear in a view.

## DHCP Operation

The IP SLA DHCP operation measures the round trip time (RTT) taken to discover a DHCP Server and obtaining a lease from it. After obtaining an IP Address, Cisco IOS IP SLA releases the IP address that was leased by the server.

The Dynamic Host Configuration Protocol (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router.

## Drop Box

Drop box acts as a temporary repository for objects, for example gauges, charts, links, device metrics, that you want to include to new reports, dashboards.

## Duplex

A full-duplex link with one telegrapher at each end, transmitting alternately in each direction.

## Dynamic Thresholds

Dynamic thresholds enable Entuity to alert the user to deviations from what Entuity's previous polling has established as normal behavior for that hour on that day. Entuity establishes normal behavior for a given attribute on a given port by maintaining the last four weeks worth of polled data, and applying an averaging algorithm.

## EIR

The Excess Information Rate (EIR) is the sustainable rate of information in excess of CIR, that the network will deliver if there is available bandwidth. The total information rate is CIR + EIR.

Frame Relay allows data rates in excess of the CIR to be successfully used on occasions. It is also possible that the amount of data that can be transferred per measurement interval (Tc) may be limited to less than the burst (or access rate) of the physical connection to the carrier network.

EIR defines how many bits per second beyond the CIR the data rate may be exceeded. This is may be policed by the carrier ingress switch per Tc on a pro-rata basis. This means that although data can be transmitted for periods of time at the burst rate of the physical port it would not be possible to continue transferring data at this rate successfully on a continuous basis if the CIR+EIR were to be less than the burst rate.

## Entuity

Entuity is both the name of the network management software and the company producing it. Entuity software is designed for networks of any size and complexity, from the smallest, simplest corporate infrastructure to the largest multinational. Every customer can access the full functionality of our cornerstone solution, incorporating fault, performance and inventory management.

## entuity_home

*entuity_home* is used within the Entuity documentation to indicate the Entuity server's root folder. The root folder is set by Entuity `install`, in Windows environments the default is `C:\Entuity`. You can view its current setting through *destination* in *entuity_home*`\etc\entuity.cfg`. Within Entuity configuration files it is represented by the variable *ENTUITY_HOME.*

## Ethernet

IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. Forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

## Events

Events are alerts and alarms that are generated through Entuity monitoring the network. Event Viewer displays events and they can also be reported on.

## Expect

Expect is a Unix automation and testing tool, written by Don Libes as an extension to the Tcl scripting language, for interactive applications such as telnet, ftp, passwd, fsck, rlogin, tip, ssh, and others. It uses Unix pseudo terminals to wrap up subprocesses transparently, allowing the automation of arbitrary applications that are accessed over a terminal. With Tk, interactive applications can be wrapped in X11 GUIs.

## Eye of the Storm® (EYE)

Until Entuity 12.5 the software was known as Eye of the Storm (EYE).

## Entuity Remedy AR System Integration

The Entuity Remedy AR System integration allows forwarding of event and managed object information from Entuity to one or more AR System servers.

Entuity allows two types of forwarding:

- automatic generation of Action Requests (ARs), derived from Entuity events, to particular application forms on target AR System servers
- interactive generation of Action Requests (ARs), initiated from Entuity. The specified application forms on target AR System servers are opened for editing, with default data populated from the current Entuity managed object(s) or event(s).

Entuity can also pass to AR System a URL identifying the managed object that is the source of the AR. From AR System you can open Entuity’s Component Viewer with the focus on the managed object.

## Factory Default

The shipped values of event thresholds are the factory defaults. You can amend a factory default, which if done at the root level effectively changes the default value for all objects against which that threshold can be set. For example, if you amend a threshold setting for a device event at the Entuity (system) level, all devices on that server will have a new default value.

## FEC

Forwarding Equivalence Class (FEC) is central concept to MPLS. An FEC is a set of packets that a single router forwards to the same next hop, using the same interface and with the same handling (e.g. queuing). The FEC is determined only once, at the ingress to an LSP, rather than at every router hop along the path.

## FECN (Forward Explicit Congestion Notification)

FECN is a bit in the header of a frame relay frame that is set to indicate to the destination node that congestion is occurring on the network. Frame relay functionality combines BECN and FECN values to determine congestion on a data path.

## Filters

Filters in Entuity act by filtering in those objects specified in the filter. There are three types of filters, view, event and Flex Report.

Entuity uses these types of filter:

- View content filters are applied to the views, restricting the components available from a view to those that meet the criteria.
- Event Filters restrict the events available through a view.
- Flex Report filters restrict the data included to the report.

## Flow Collector

The Flow Collector is the set of processes within an Entuity Integrated Flow Analyzer responsible for the receiving, processing and storage of flow records.

Administrators can enable/disable an Entuity server's Flow Collector through `configure`, a decision which should be made according to the role the administrator wants the server to perform in the management of the network.

## Frame Relay

A fast packet protocol that relies on physical component and higher level software reliability. The network discards any frame with bit errors. Frame relay services include PVCs (Permanent Virtual Circuit) and SVCs (Switched Virtual Circuit).

## Full Duplex

A full-duplex link with one telegrapher at each end, transmitting alternately in each direction.

## Generic Device Type

Entuity uses the concept of an underlying generic object against which are mapped the characteristics of different device types, e.g. routers, switch, firewalls, BladeCenters. This allows complete management of devices that have characteristics of one or more of the traditional types of devices, e.g. a router with switching capabilities.

## Half-Duplex

A type of communication channel using a single circuit which can carry data in either direction but not both directions at once.

## Host Identifier

Your Entuity representative requires the host identifier of the Entuity server machine before they can generate your license. The host identifier associates the Entuity license with the physical footprint of the machine. Entuity install and configure programs both display the host identifier, alternatively you can run the command line program `hostIdent` (which is included with the software but is also available from the Support website).

## Hot Standby Router Protocol (HSRP)

Hot Standby Router Protocol (HSRP) establishes a framework between network routers to achieve default gateway failover if the primary gateway becomes unavailable in close association with a rapid-converging routing protocol like EIGRP or OSPF. By multicasting packets, HSRP sends its hello messages to the multicast address 224.0.0.2 (all routers) using UDP port 1985, to other HSRP-enabled routers, defining priority between the routers. The primary router with the highest configured priority will act as a virtual router with its own IP and MAC address, which the hosts on the local segment will be configured to use as a gateway to the destination in question. If the primary router should fail, or the link to the destination drop, the router with the next-highest priority would take over communications through alternative routes within seconds, without major interruption to network connectivity.

HSRP and VRRP on some routers have the ability to trigger a failover if one or more interfaces on the router go down. This can be useful for dual branch routers each with a single serial link back to the head end. If the serial link of the primary router goes down, you would want the backup router to take over the primary functionality and thus retain connectivity to the head end.

## Hypervisor

A hypervisor, also called virtual machine monitor (VMM), allows multiple operating systems to run concurrently on a host computer. The hypervisor presents to the guest operating systems a virtual operating platform and monitors the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources. Hypervisors are installed on server hardware whose only task is to run guest operating systems.

## Infrastructure Ports

Entuity considers infrastructure ports, as:

Entuity considers infrastructure ports, as router ports, as uplinks which are ports connecting routers with switches and as trunk ports which are ports connecting switches together.

- Router ports.
- Uplinks, ports connecting routers with switches.
- Trunk ports, ports connecting switches together.

## Interface

This is the entity on a node which is polled, such as a physical port. Nodes are likely to have more than one interface.

## IP

In TCP/IP, the standard for sending the basic unit of data, an IP datagram, through the Internet.

## IP Link

IP links may be autoDiscovered or created manually. They represents a link of some form at layer 3 or above e.g. a pair of IP addresses, an IP address and a URL.

## IP Peering

IP Peering provides visibility into your WAN links, i.e. leased line, Frame Relay DLCIs, ATM VCCs, using subnet masking. It also reflects any manual IP pairings you may have made in Entuity.

## ISO

International body that is responsible for establishing standards for communications and information exchange; developed the OSI reference model. ISO is not an acronym, but the Greek word for "equal."

## Key Metrics Gauge

From Entuity's Explorer you can access the Device and Port Summary pages, both of which display Key Metric graphs. Key metrics vary according to the managed object, e.g. Device CPU utilization, Port Inbound Utilization%.

These graphs are of two forms a:

- green only gauge is used with metrics that do not have thresholds.
- green and red gauge is used with metrics that have thresholds. When the indicator is pointing to the red area then the threshold has been crossed. The relative size of the red and green areas of the gauge is fixed, i.e. the red area does not take a larger or smaller proportion of the total area of the gauge on changes to the threshold level.

  You can view the current threshold value by passing the cursor over the data value below the graph.

You can click on each key metric gauge to view a larger graph.

## LAP (Lightweight Wireless Access Point)

A low cost Wireless Access Point (WAP) that delegates much of the control functionality usually embodied within an Autonomous WAP to a WC. LAPs are usually connected to switched access layer ports and can coexist with ordinary wired connections to end user hosts and servers on the same switch. The associations between the LAPs and WCs are negotiated dynamically and can change under fault conditions.

A LAP is an AP that is designed to be connected to a wireless LAN (WLAN) controller (WLC). The LAP provides dual band support for IEEE 802.11a, 802.11b, and 802.11g and simultaneous air monitoring for dynamic, real-time radio frequency (RF) management. In addition, Cisco Aironet 1000 Series LAPs handle time-sensitive functions, such as Layer 2 encryption, that enable Cisco WLANs to securely support voice, video, and data applications.

Entuity Wireless currently supports Cisco LAP, part of the Cisco Unified Wireless Network architecture.

## Leased Line

A leased line is a dedicated point-to-point connection over a WAN via a router at the subscriber’s premises to the telecommunications provider.

Entuity identifies a leased line, by default, when both of these conditions are true:

- The interface type is either IANAifType 22 (propPointToPointSerial) or 23 (PPP).
- The WAN port is not:
- A Frame Relay port.
- An ATM port.
- An ISDN port. These are identified as having an associated lower layer protocol port (found from the ifStack table) of ifType 81 (ds0). This indicates the port is a layer on top of either basic rate or primary rate ISDN.

## Link Layer Discovery Protocol (LLDP)

The IEEE 802.1AB Link Layer Discovery Protocol (LLDP), provides a solution for the configuration issues caused by expanding LANs. It runs over the data link layer and specifically defines a standard method for Ethernet network devices to advertise information about themselves to other nodes on the network and store the information they discover. LLDP is available as a technology link type on the Entuity maps.

## Load Balancers

Load balancers are devices that control and optimize traffic flow over your network. For example directing traffic away from over utilized servers to those less utilized, improving mission critical service delivery, providing fall over protection.

Entuity delivers a similar level of fault, performance and inventory management for load balancers as provided for other standard Entuity device types, e.g. routers, switches, hubs. For example device reports include load balancers, you can build your own reports using Flex Reports, device and port events apply and full load balancer details are viewable through Component Viewer.

Entuity currently manages F5 Labs Big IP 6400 Load Balancer. Entuity delivers additional polling of the device ports using F5 lab’s propriety MIB, returning additional port identification, port status, port traffic and port utilization data. The full integration of this additional data within Entuity allows administrators to set up utilization and traffic events against this data.

## Log Files

Entuity process messages are written to their individual log files, in *entuity_home*/`log`. For example, `applicationMonitor` writes to `applicationMonitor.log`. When the log file becomes full, it automatically wraps to another file with up to four versions, e.g. `applicationMonitor.log.1`, `applicationMonitor.log.2`, `applicationMonitor.log.3`.

## Management Level

Every device under Entuity management is managed according to its management level, which is set when the device is added to Entuity but can be subsequently amended. Each managed device costs one license object.

These are the management levels:

- Full Management (all interfaces), Entuity manages all interfaces on the device.
- Full Management (management interfaces only), Entuity only manages the management interface.
- Full Management (no interfaces)
- Basic Management Entuity collects only basic system information and the full IP address table via SNMP. This management level is used when Entuity does not have the appropriate device support dataset (vendor file), cannot generate an appropriate dataset or you only want the device placed under basic management. Entuity does not manage any ports or modules on the device.
- Ping Only, devices only under ping management, SNMP data is not collected for these devices.

## Managing Agent

Handles requests for information or action from the management station on a node. A protocol links the management station and the Managing Agent; for Entuity users this must be SNMP.

## MIB (Management Information Base)

Entuity supports SNMP MIBs only. MIBs are present within nodes on a network, and comprise a logical collection of managed objects arranged in a tree structure. Managing agents on an element use MIBs to store information regarding the element, e.g. the speed at which packets of information are transferred.

All managed objects within a MIB share a common root.

## Mobility Controller

An SNMP manageable hardware device, manufactured by Aruba, that controls and coordinates the operation of a group of Aruba Wireless Access Points. In an Aruba wireless network deployment all wireless equipment discovery and real-time monitoring is performed via the Mobility Controllers rather than via SNMP/ping monitoring of the individual Access Points.

## Multicast

Network communication between a single sender and multiple receivers.

## My Network

Supplied view that contains the entire set of managed object’s the user is permitted to view. Different users may have different devices in their My Network view, reflecting their different access permissions.

## Node

An SNMP managed device attached to a network, from which data can be retrieved. For example, node devices such as hubs, routers, bridges, or network printers.

## OID

An Object Identifier is a sequence of integers that represent the position of an object in the hierarchical structure of objects in a MIB.

## OMF (Open Modeling Framework)

Flexible Entuity framework that allows the fast integration and management of new types of managed objects, e.g. new device types. For example, the BladeCenter device type is implemented through the OMF.

## OSI Model

A model for networks developed by International Standards Organization (ISO). The network is divided into seven layers, each layer building on the services provided below it.

## Packet

Any logical block of data sent over a network; it contains a header consisting of control information such as sender, receiver, and error-control data, as well as the message itself. May be fixed or variable length.

## PCR (Peak Cell Rate)

PCR is the maximum short term data throughput supported by an ATM port; the limit to which traffic can burst.

## Percentile Utilization

Percentile Utilization indicates that for a defined percent of the time, e.g. 95, port utilization is below this value. It is useful for monitoring the sustained utilization of the port.

The 95th percentile is derived by ordering the utilization data by value, from highest to lowest. Application of a least square fit method removes spikes that would distort the analysis. The top 5% values are discarded, leaving the 95th percentile. This value is calculated for both inbound and outbound utilization.

## Policy Group

Entuity licensing is enabled by grouping related types of managed objects into groups. These Policy Groups are then assigned a license credit quota. Before Entuity manages an object it first checks whether the license allows its management and then whether a credit is required. When a license credit is required, Entuity checks that the policy group to which the object's type is associated has available credits. For example, before Entuity manages a device it checks the device licensing policy group for available credits.

## Polling

Devices on the network are accessed by the system at regular, pre-defined, intervals in order to retrieve required data. This is referred to as polling the devices.

## Polling Engine

The Polling Engine (or Core Management Engine) is the set of processes within an Entuity server responsible for all general network management tasks excluding flow collection (e.g. network discovery, inventory, monitoring, event management).

Administrators can enable/disable an Entuity server's Polling Engine through `configure`, a decision which should be made according to the role the administrator wants the server to perform in the management of the network.

## Port

Entuity considers ports as interfaces on network devices, e.g. routers, and as endpoints in communications systems. In IP an upper-layer process that receives information from lower layers. Ports are numbered, and each numbered port is associated with a specific process. For example, SMTP is associated with port 25.

TCP and UDP transport layer protocols used on Ethernet use port numbers to distinguish between (demultiplex) different logical channels on the same network interface on the same computer.

## Protocol

A set of formal rules detailing how to transmit data across a network. Example protocols include TCP, UDP and IP.

## PVC (Permanent Virtual Circuit)

PVC is a Frame Relay virtual connection providing the user with the equivalent of a physical connection to a destination address, using shared facilities. Virtual circuits can be permanent (PVC) or switched (SVC).

## Reachability

Availability Monitor sends an ICMP ping to the management IP address of managed devices, by default every two minutes. Devices that respond are considered reachable, those that do not respond, after the set number of retries, are considered unreachable. When Availability Monitor (`applicationMonitor`) is not running, then the reachability of the device is Unknown for that period, although Entuity maintains the last known state of the device.

## Reboot

Entuity uses the device sysuptime to calculate when the device was last rebooted, or more accurately when the device last came up after being rebooted.

## Reconciliation Rules

Within BMC Atrium reconciliation rules are applied by the reconciliation engine to improve accuracy and efficiency of maintaining IT environment data in the CMDB. Reconciliation is used to identify and merge CI information and relationship form imported dataset with production dataset.

## Remedy Help Desk / Service Desk

Entuity Remedy AR System Integration for Remedy AR System 7.0 includes a sample configuration which integrates with the Remedy Service Desk application.

## Remote Server

A remote server is an Entuity server configured to trust another central Entuity server. A user logged into the central Entuity server is able to view information collected by the remote Entuity server(s), according to their user account access rights. A remote Entuity server responds to requests from a trusted central Entuity server, and freely shares information with it.

An Entuity server can be configured to perform both roles, be both a remote and central Entuity Server, allowing administrators to create both hub-n-spoke and fully meshed deployments.

Configuration of central and remote servers is through the Multi-Server Administration area of the Entuity web UI.

## Router

A device that routes data between networks. Routers connect multiple LAN segments to each other or to a WAN.

Routers may be equipped to provide frame relay support to the LAN devices they serve. These routers can:

- encapsulate LAN frames in frame relay frames and send those frames to a frame relay switch for transmission across the WAN.
- receive frame relay frames from the WAN, strip the frame relay frame off each frame producing the original LAN frame, and forward it to the end device.

## Running-config

The configuration controlling the current operation of a piece of Cisco hardware. This may be different to the start-up config if changes have been made since start-up and the changes have not been saved. The running-config can be saved as the startup-config replacing any previous start-up config. The running config is held in DRAM. If the machine is restarted without the running-config being saved, all changes are lost.

## Sample Interval

In Entuity the period between two data samples. This may be between two pollings of a port, or between two rolled up data samples.

## SCR (Sustainable Cell Rate)

SCR is the long term data throughput of an ATM port. Traffic can burst above this limit up to the PCR.

## Server

Any computer whose function in a network is to provide user access to files, printing, communications, and other services. Servers usually have more memory, more disk storage, and a more advanced processor than a single-user desktop PC.

Where Entuity manages an application, Entuity can manage the application server as a device.

## Services

Services is a method of grouping together collections of ports that provide a service and associating with them other ports which use that service. For example, a service maybe e-mail, with one port designated as the provider of the service and all others in the group defined as consumers.

## SLA

A Service Level Agreement (SLA) is a set of rules and metrics which can be used to measure the efficiency and performance of an object. That object may be a department, a server, a network or any other functional component of an organization. If an object adheres to its associated set of rules and metrics, then it can be said to be conforming to its SLA. Similarly, if the object breaches the set of rules and metrics, then this means that it is no longer conforming to its SLA.

## SNMP

Standardized method of managing and monitoring network devices on TCP/IP based internets. SNMP defines the formats of a set of network management messages, and the rules by which those messages are exchanged. The network management messages are used to make requests for performing network management functions and to report on events that occur in the network. Also, SNMP defines the allowable data types for MIBs, they way in which MIBs can be structured, and a set of standard objects that can be used in implementing a MIB.

## Spanning Tree

Spanning tree provides a vendor neutral technology for visibility into your network. When correctly implemented Entuity discovers bridge links, switch to switch relationships, through polling the Bridge MIB. Complete spanning tree connectivity relies on a contiguous set of Entuity managed devices.

## Spare Ports

By default Entuity spare port calculations include ports that have been unused for forty days or more, include ports that have system uptime of less than forty days and are currently unused and exclude ports that have been unused for less than forty days but have a system uptime of forty days or more.

By default Entuity spare port calculations:

- Include ports that have been unused for forty days or more.

- Include ports that have system uptime of less than forty days and are currently unused.
- Exclude ports that have been unused for less than forty days but have a system uptime of forty days or more.

The forty day threshold is configurable through the reporting section of entuity.cfg. Entuity distinguishes between physical and virtual ports using interface type. If required System Administrators can amend the virtual port identifier.

## SNMP Agent

Management code that resides in the device, controls the operation of the device, and responds to SNMP requests.

## SSL

An SSL Certificate consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it. When a browser points to a secured domain, an SSL handshake authenticates the server and the client and establishes an encryption method and a unique session key. They can begin a secure session that guarantees message privacy and message integrity.

## Startup-config

The initial configuration when a piece of Cisco hardware starts-up. If there have been no changes to the configuration since start-up, this will be the same as the running-config. The startup-config is also referred to as the saved config. The startup-config is held in NVRAM.

## Static Thresholds

Static threshold settings allow you to configure the trigger points which when crossed cause Entuity to raise events. You can set thresholds against an individual event, a managed object, view or all objects on an Entuity server.

## StormWorks

StormWorks is the internal Entuity engine, also known as the Data Management Kernel (DMK). It runs as the ***DsKernelStatic*** process.StormWorks enables the delivery of functionality through a highly configurable set of core services. The configuration files, found in *entuity_home*\etc, prefixed with ***sw_*** define and configure StormWorks services.

Entuity assigns all of the objects it manages their own StormWorks identifier. StormWorks identifiers are sequentially assigned, do not consider the object type and are unique within each Entuity server. *StormWorks ID* is visible from the object's web UI Advanced tab, and is used in creating dashboards to the user, for example during Data Export, Map Export, running of Flex Reports.

## Stream Attributes

Information Entuity collects from your network is stored within Entuity as an attribute of the managed object, for example a port's name, a port's utilization are stored as attributes. Stream attributes are to maintain a history of a metric, for example Entuity maintains a history of port utilization.

## SVG

Scalable Vector Graphics (SVG) is a graphics file format and Web development language based on XML. SVG is used by Entuity's reports to dynamically generate, high-quality graphics from real-time data.

## Switch

A switch is a network device that selects a path or circuit for sending a unit of data to its next destination. It is usually simpler and faster than a router, which requires knowledge about the network to determine the route.

A switch may also include the function of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to.

## SynOptics Network Management Protocol (SONMP)

SONMP is also known as the Nortel Discovery Protocol (NDP), a Data Link Layer network protocol for discovery of Nortel (Avaya and Ciena) devices. It is available as a technology link type for the Entuity maps.

## System Capabilities

Entuity determines the switching capability of a device by checking the group dot1dtp, specifically the mandatory scalar value dot1dTpLearnedEntryDiscards.  dot1dtp is only present when the device supports transparent bridging, which implies it has Ethernet switching capability.

Entuity determines the routing capability of a device by checking for the ip-forwarding variable from the ip group in the MIB of the device. When ip-forwarding has a value of 1, this implies the device is acting as a gateway and so has routing capability.

Entuity determines whether the device type is hub by comparing its type to device types detailed in the vendor files.

## TCP

Connection-oriented protocol that provides a reliable byte stream over IP. A reliable connection means that each end of the session is guaranteed to receive all of the data transmitted by the other end of the connection, in the same order that it was originally transmitted without receiving duplicates.

## TCP/IP

Combination of TCP and IP protocols common to many different computer systems and so often used for communication between them.

## TFTP

Trivial File Transfer Protocol (TFTP) is a very simple file transfer protocol, with the functionality of a very basic form of FTP. It uses UDP as its transport protocol and has no authentication or encryption mechanisms.

## Ticker

Ticker allows you to view real time output at the device and port level, viewing data changes as they occur. You can select to view data activity for one or more client devices or ports.

For monitored:

- Ports you can select from a list of MIB variables the particular variable(s) you want to use to monitor the port. Entuity is supplied with a default number of MIB variables for use with ports and you can also add your own MIB variables to this list.
- Devices you can create your own list of MIB variables on which to monitor the device.

## traceroute

Entuity includes two types of traceroute functionality, identified in the Entuity client as TraceRoute from Client and TraceRoute from Server.

TraceRoute from Entuity Client, calls the traceroute utility installed on the Entuity client machine and performs a live traceroute from the Entuity client to the target IP address.

TraceRoute from Entuity Server, uses data collected by `applicationMonitor`. This traceroute information is updated every two minutes, so calling TraceRoute from Server does not initiate a live traceroute but instead interrogates the data returned from the last `applicationMonitor` traceroute.

`applicationMonitor` uses Entuity’s own implementation of traceroute functionality. This implementation performs ICMP pings in a similar way to a standard traceroute but with this key difference. When performing a traceroute `applicationMonitor` increments TTL values by one, until the pings reach the edge of an invisible cloud. At this point `applicationMonitor` increase the TTL value to 32. When this results in the ping reaching its target, the response from the target includes the actual number of hops required to reach target.

## Traps

Traps can be used by network components to signal abnormal conditions. Entuity can both receive and forward SNMP traps.

Entuity can be configured to:

- Generate events in Event Viewer then traps are received.
- Forward traps to up to six concurrent recipients.

Entuity also supply a more advanced SNMP trap forwarding integration module. Contact your Entuity sales representative for details.

## Trivial Change

A difference between a current-configuration file and a previously archived one that is not considered important by the system because it matches a set of rules codified as patterns in an “ignore file”. Trivial changes may include comments such as timestamps in a configuration file.

## Root Cause Analysis (RCA)

RCA isolates IT related problems using vector differencing. This involves the building of a dependency chain of objects and monitoring the object states in that chain. In the event of state changes (where each object state change is a vector), differencing the dependency chain state vectors enables Entuity to determine the true cause of the event. Entuity can then raise the appropriate event.

For example, if an application becomes unavailable because a switch has failed then Entuity raises an event relating to the switch failure in Event Viewer. Entuity does not raise events for the application being unavailable as changes in state in the dependency chain are attributed to the switch failure.

## Trunk Ports

Trunk ports, i.e. ports connecting switches together.

Entuity identifies a trunk port by:

- reading the MIB.
- ***macman*** identifying the switch port as having more than ten MAC addresses and also having associated VLANs.
- using CDP Trunk Port Discovery, a CISCO proprietary method.

When one or more of these methods identifies a trunk port, Entuity also considers it as a trunk port.

## Unclassified Devices

Entuity managed devices for which Entuity does not have a device support dataset, provided through individual vendor, bin.vendor or newbin.vendor files, are included to Entuity as Unclassified devices under Full Management, or Unclassified devices under Ping-only and Basic Management.

Unclassified generically managed devices use an Uncertified device type, created by Entuity and held in newbin.vendor. These are Entuity managed devices and do incur a license charge. System Administrators should contact their Entuity support representative for a vendor file which would ensure Entuity fully manages these devices.

## Unicast

Unicast is network communication between a single sender and a single receiver.

## Uplink Detection

Entuity considers an uplink as trunking on a connection to a router or layer 3 switch, which is visible through spanning tree. This technology attempts to link layer 3 with layer 2.

Where links between switches and routers are not done using VLAN trunking and spanning tree then the spanning tree technology will not detect them. This is typically at smaller satellite offices, which do not need the greater port density and much greater speed available from router on a stick and even greater speed available from layer 3 switching.

## Uplinks

Ports connecting routers with switches.

## Uptime

By default Entuity polls devices every five minutes, retrieving device *sysuptime*. Entuity checks as to whether the device has been continually up since the last poll, and modifies the device's uptime value accordingly.

When *sysuptime* indicates the device has been down during the polling interval but is now up, from *sysuptime* alone Entuity cannot identify for how long the device was down. Entuity takes this unknown time, and adds fifty percent of it to the known uptime value, with the remaining fifty percent considered UNKNOWN. For example where *sysuptime* has a value of two minutes. Entuity cannot determine the state of the device over the first three minutes of the polling interval. Entuity adds ninety seconds to the *sysuptime* value, giving an uptime value of two hundred and ten seconds and records the device state as UNKNOWN for ninety seconds.

Device uptime is visible through Component Viewer, and is used in many reports, e.g. Routing Summary, Switching Summary.

## Utilization

In Entuity port utilization is expressed as a percentage of actual traffic volume against the maximum volume that can be handled by the port.

## UUID (Universally Unique ID)

A 16 byte value written to a system's planar at manufacturing time to uniquely identify a system across time and space.

## Variable Binding

A variable binding, or VarBind, refers to the pairing of the name of a MIB variable to the variable's value. A VarBindList is a simple list of variable names and corresponding values. Some PDUs are concerned only with the name of a variable and not its value (e.g., the GetRequest-PDU). In this case, the value portion of the binding is ignored by the protocol entity. However, the value portion must still have valid ASN.1 syntax and encoding. It is recommended that the ASN.1 value NULL be used for the value portion of such bindings.

## VCC (Virtual Channel Connection)

A VCC is an association established at the ATM Layer between two or more endpoints for the purpose of user-user, user-network, or network-network information transfer. The points at which the ATM cell payload is passed to the AAL for processing signify the endpoints of a VCC. Virtual Circuit is a more generic, non-ATM specific term.

## VCI (Virtual Channel Identifier)

VPI and VCI together identify a virtual channel link on an ATM interface.

## Vendor Files

Entuity identifies the device type of discovered devices by matching their sysoid to that held against the device support datasets. Device support dataset definitions are held in, listed here in order of precedence, individual vendor files, bin.vendor file, newbin.vendor file, and then uncertified file.

***vendinfo*** identifies the vendor information available to Entuity and the decisions made when more than one vendor file is available for a particular sysoid; which vendor device definition Entuity uses to manage that device type.

| File Type | Description |
|---|---|
| individual vendor files | When Entuity does not currently manage a device that you require it to, you can request your Entuity support representative for an appropriate vendor file. Those non-standard definitions are listed in entuity_home/etc/exotica. Only when a vendor file is moved to entuity_home/etc does Entuity use that definition. |
| bin.vendor file | File includes the default vendor file definition |
| newbin.vendor file | File includes device type definitions generated by earlier versions of Entuity. |
| uncertified file | File includes device type definitions created by Entuity, using proliferate with the -g parameter. Devices of this type are considered as Unclassified Devices. |

## View

All network objects within Entuity are displayed through views. View filters allow you to restrict the displayed objects in the view to the ones you are interested in. You can also use user profiles to control access to different views.

## Virtual Channel Links (VCLs)

A VCC consists of the concatenated VCLs. A VCL is a means of unidirectional transport of ATM cells between the points where a VCI value is assigned and the point where the value is translated or removed. The VPI and VCI within the ATM cell header associates each cell with a particular VCL over a given physical link.

## Virtual Circuit

A Virtual Circuit is a generic term for an association established between two or more endpoints for the purpose of user-user, user-network, or network-network information transfer. An example would be ATM's VCC.

## Virtual Port

Entuity distinguishes between physical and virtual ports using interface type. If required System Administrators can amend the virtual port identifier.

## VLAN

A logical association that allows users to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of the network.

## VM Platforms

Entuity currently manages Oracle and VMware VMs through its VM Platform device type. Entuity communicates with VMs and their hypervisors through the VM's SDK. This requires specification of different connection attributes when compared to devices of other types. It also requires that all VMs are added to Entuity with a **Ping Only** management level, as this allows the selection of the VM Platform type and its connection configuration. When adding VMs using autoDiscovery care must be taken to ensure candidate device VMs are always added as **Ping Only**.

## VPD (Vital Product Data)

VPD is information about a device that is stored on a computer's hard disk (or the device itself) that allows the device to be administered at a system or network level. Typical VPD information includes a product model number, a unique serial number, product release level, maintenance level, and other information specific to the device type. Vital product data can also include user-defined information, such as the building and department location of the device. The collection and use of vital product data allows the status of a network or computer system to be understood and service provided more quickly.

## VPI (Virtual Path Identifier)

VPI identifies a virtual path leg on an ATM interface.

## VRF (Virtual Routing and Forwarding)

VRF allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.

## VTP (VLAN Trunk Protocol) Domain

A VTP domain consists of one or more connected switches that share the same VTP domain name. A switch can be configured to be in one and only one VTP domain. The vtpDomainTool generates a view that groups devices and VLANS by this VTP domain name.

## Wireless Controller (WC)

A network attached device that coordinates traffic to and from Lightweight Wireless Access Points (LAPs). It provides centralized control over the configuration and dynamic behavior of potentially many LAPs.

# Index