Entuity for BMC TrueSight Operations Management v21.0 Patch Notification P03

January 15, 2024

Technical Bulletin January 15, 2024

Version 2024.01.15

We are pleased to confirm the availability of **patch P03** for **Entuity v21.0**, which has now been certified for customer use; further details of the benefits to be gained from this patch are set out in the table below.

Latest Patch Details

New in v21.0 P03

Please refer to the [Knowledge Base](#) on the Entuity Help Center for help and information on functionality added in this patch.

Functional Area	Platform(s)	Description
Configuration Management and Monitoring	All	Replacement of support for 'SCP' transfer method in configuration retrieval with 'SCP Push', and addition of 'SCP Pull' transfer method support for Juniper and F5 devices.
Event Management System (EMS)	All	Improvement to root cause analysis of network outages, with addition of the following to incident and event details: • IP address of root cause device • devices are impacted by outage. Addition to entuity.cfg of a parameter enabling a user to view corresponding 'Network Outage' incidents and events from the Incidents dashboard of impacted devices, as well as the device on which the incident/event originated.

Server OS Monitoring and OS Service Management	All	Addition of View-based profiles for OS Services, enabling users to restrict, by means of profiles, monitoring of OS Services to just the server devices in a given View or Views.
User Defined REST Polling	All	Improvements and fixes to the process of creating a user defined REST poller: • Addition of option to create user defined device types for which REST pollers can be specifically created, and based on which custom devices can be added via Asset Management. • Addition of option to specify the media response of a REST poller step, either XML, JSON or auto-detect, and fixed an issue with XML support. • Addition of options to define a status attribute that drives the object status for a new user defined device type, and to add user-editable attributes to the new device type. • Addition of support for rate limiting to REST poller steps to better handle server 429 codes for 'too many requests'. • Addition of support for conditional processing of REST poller steps. • Improvement to warn the user when selecting incompatible attribute data types and display formats during the

		process of creating a REST poller.
		• Fixed an issue that could cause errors when adding attributes to a REST poller.
		• Improvement to handling of URL parameters with no value.
		• Improvement to handling poller steps that collect data but do not have any attributes.
		• Fixed an issue whereby a user could be incorrectly presented with a ${src::} variable placeholder option after having specified a step with no data collection.
		• Improvement to error handling.

Improvements and Fixes in P03

Functional Area	Platform(s)	Description
Asset Management	All	Fixed an issue affecting addition of local credentials to custom devices.
Configuration Management and Monitoring	All	Improvement to error handling when incorrect StormWorks filter is input.
Credential Management	All	Improvement to the process of modifying a shared credential set, so that a warning dialog appears if the credential set is in use by one or more devices. Addition of audit log entries for modifications to shared credential sets.

Custom Webhooks	All	Fixed an issue whereby processing of custom webhooks was unable to handle JSON attributes containing the '-' character.
Dashlets	All	Fixed an issue that caused incidents to filter incorrectly on the Incidents List dashlet. Improvement to the Pie Chart dashlet so that longer value names in the legend do not remain abbreviated when the dashlet size is widened within its dashboard. Fixed an issue affecting custom Table dashlets that use an 'Include Objects of Type' selection from the extended list, whereby saving the table and re-editing it could incorrectly change the name of the selected type.
Database	All	Changed a database upgrade component to prevent it being falsely identified as a threat by Windows Defender.
Device Support	All	Improvement to support for Dell ML3 and Quantum Tape storage devices. Improved collection of LLDP connectivity data for Cisco Nexus devices. Improvement to port VLAN and IP information for Aruba 6000 devices. Improvements to port connected-host and VLAN information for newly discovered Cisco devices. Improvements to Juniper port discovery for certain devices. Updates and improvements to device support, including server and storage devices.
Event Management System (EMS)	All	Fixed an issue whereby Cisco Viptela vManage Alarms could be raised in

		an incorrect order. As a result of this fix, alarms are now processed by entry time before being forwarded to the Entuity EMS. Improvements to incident handling of 'Module Disappeared', 'VPN Tunnel Disappeared', and MPLS events. Fixed an issue whereby 'Open For' time details for incidents and events could be incorrect if the timezone of an Entuity server differed to that of the user's web client.
General Performance Improvements	All	Performance improvements when managing Cisco Viptela devices.
General UI/UX Improvements	All	Improvement to the process of assigning and editing user group access to Views and dashboards, enabling a user to filter through available user groups. A filter has also been added to the forms used for assigning Report Permissions and Task Permissions to user groups via the Account Management page. Addition of a filter to simplify the selection of zones from dropdown fields, enabling a user to filter through available zones where this is required in the UI, e.g. when adding an asset to management. Improvement also made to the sort order of zones in such dropdown fields. Fixed a daylight savings issue affecting the date picker calendar widget. Fixed an issue affecting the Search form, whereby 'My Network' was incorrectly no longer the default View for the search parameter.
IP Address Management (IPAM)	All	Fixed an issue that prevented hostnames from being visible on a

		network, by improving the ping and DNS scans used for IPAM networks.
Licensing	All	Fixed an occasional timing problem with adding a remote server to a central license server and allocating license credits to it.
Maintenance Mode	All	Fixed an issue that incorrectly prevented a user from adding a ping-only device to a maintenance schedule via the context menu.
Maps – Topological Maps	All	Fixed an issue whereby customized hover-over tooltips for devices on Topological Maps could incorrectly appear whilst the right-click context menu was displayed (and subsequently cause the context menu to disappear).
Multi-Server Configuration	All	Improvement to performance of synchronization tasks across large numbers of Views. Improvement to depiction of sync progress for large numbers of synchronization tasks, and improved error handling during synchronization. Improvement to restrict the access of users authenticated by a consolidation server to data on their assigned remote servers. Improvement to error handling when adding a new server configuration set with the same name as one already existing, and fixed an issue whereby modifying an existing config set to have the same name as another could cause the deletion of that other set. Fixed an issue whereby external authentication via LDAP would incorrectly fail to create users on remote servers in instances where config sets were enabled.

| Multi-Server Topology | All | Fixed a UI issue when changing tabs on the Topology Group Management page.

Fixed an issue whereby topology group discovery would fail if a device was configured with a CDP IP address that was not IPv4.

Fixed an issue that caused an error when protocol data (e.g. LLDP) contained invalid XML characters.

Fixed an issue whereby non-admin users with the Topology Group Administration permission were incorrectly prevented from managing topology groups. |
|---|---|---|
| RESTful API | All | Fixed an issue whereby addition and modification of devices with local credentials to asset management via RESTful API would fail, and credentials would not be saved. |
| Security Updates | All | Updated Entuity Maverick SSH library default configuration to avoid certain cipher suites, and therefore avoiding the recent Terrapin SSH vulnerability. Note, this change reduces the available options to make an SSH connection, so if an SSH server only supports CBC and/or ChaChaPoly, it is no longer possible to connect.

Improvement to report security.

Tomcat upgraded to version 9.0.83.

General security improvements. |
| Server OS Monitoring and OS Service Management | All | Fixed an issue whereby if two or more different OS Services have the same name, then only one will appear in the View-level OS Services dashlet, incorrectly excluding the other(s).

Improvements to the process of configuring OS Service rules. |

SurePath	All	Fixed an issue whereby red ('path down' status) bars were in some circumstances incorrectly not displayed on the Status History chart dashlet of the SurePath dashboard.
User Account Management	All	Fixed an issue affecting password encryption via the authtool batch file for LDAP users with a space in their username.
User Defined SNMP Polling	All	Increase to the UDComponent index attribute data type field from 64 to 128 characters.
View Management	All	Fixed an issue whereby View content filters using more than one IP range could incorrectly include objects outside those ranges.
Virtualization	All	Fixed an issue whereby OS-level Virtual Disk information was incorrectly not displayed on Summary dashboards for Instrumented VMs of a Microsoft Azure VM platform.
Zones	All	Fixed an issue whereby modifications to certain devices (custom devices and virtualization devices) via the Asset Management UI page could incorrectly reset the devices' zone.

Notes

Following the updates to 'Module Disappeared', 'VPN Tunnel Disappeared' and MPLS events and incidents in P03, users will need to merge a new event project into their live event project as part of this patch installation.

Entuity is supplied with the RSSO client version 20.02.00. Your RSSO client version should not be greater than the RSSO server version. Please contact Entuity support if your RSSO server version is less than 20.x in order to obtain a compatible RSSO client.

Entuity recommends that all servers in a multi-server configuration run the same patch version.

Downloading Patches

Patches for all supported platforms are available from the Entuity FTP site (ftp.entuity.com/), and the Product Downloads section of the BMC Support Central site (https://www.bmc.com/support/support-central.html).

The Entuity FTP site is arranged into separate directories for each version, operating platform, and patch number. Each directory also includes a readme file and any other relevant documents, including checksums, which you are advised to verify before applying each patch. Patches must always be applied via the Patch Installer, which will ensure they are applied in a consistent and reliable manner.

Access to the BMC patches on the Entuity FTP site requires a valid username and password that can be obtained from BMC Support. For added security, the FTP site requires connection via SFTP.