




Entuity[®] 16.5

Entuity Events Reference Manual



Entuity was founded to develop intelligent network management solutions. Entuity delivers the best value in infrastructure and network management by integrating into a single solution Performance Management, Availability Management and Resource Management.

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

Entuity

The Entuity product and its related documentation are protected by copyright and distributed under licenses restricting use, copying, distribution and decompilation. Unless you have negotiated with Entuity specific terms and conditions for using its product and associated documentation, such use shall be governed by Entuity's standard licence terms, a copy of which is distributed with the product.

Entuity may make improvements and/or changes to the product(s) and/or program(s) described in this publication at any time. These changes will be incorporated into new editions of the relevant publication.

Entuity®, **SurePath®**, **Eye of the Storm®**, **InSight Center®**, **Green IT Perspective™**, **Network Delivery Perspective™** and **Service Delivery Perspective™** are registered trademarks of Entuity. All other trademarks are the property of their respective owners.

License terms and conditions of use for Entuity and included third party software can be found on the Entuity server at [entuity_home/licenseTerms/](#). A listing of these third party trademarks, references and software included with Entuity is available through its web UI.



Contents

1 System Event Types Listing	
AP Antenna Host Count High	25
AP Antenna Host Count High Cleared	25
AP Antenna Host Count Low	25
AP Antenna Host Count Low Cleared	26
AP Antenna Channel Change Frequency High	26
AP Antenna Channel Change Frequency High Cleared	26
AP Antenna Offline	27
AP Antenna Online	27
AP Antenna Power Change Frequency High	27
AP Antenna Power Change Frequency High Cleared	28
AP Associated With Controller	28
AP Host Count High	28
AP Host Count High Cleared	28
AP Host Count Low	29
AP Host Count Low Cleared	29
AP Not Associated With Controller	29
ATM VCC High Inbound Utilization	30
ATM VCC High Inbound Utilization Cleared	30
ATM VCC High Outbound Utilization	30
ATM VCC High Outbound Utilization Cleared	31
ATM VCC Link Down	31
ATM VCC Link Up	31
ATM VCC Low Inbound Utilization	31
ATM VCC Low Inbound Utilization Cleared	32
ATM VCC Low Outbound Utilization	32
ATM VCC Low Outbound Utilization Cleared	33
AvailMonitor Application Available	33
AvailMonitor Application Unavailable	33
AvailMonitor Falling Average Latency	33
AvailMonitor High Latency	34
AvailMonitor High Latency Reaching Application	34
AvailMonitor High Latency Reaching Application Cleared	34
AvailMonitor Low View Device Reachability	35

AvailMonitor Normal Latency	35
AvailMonitor Normal View Device Reachability	35
AvailMonitor Rising Average Latency	36
AvailMonitor Rising Trend in Average Latency	36
AWAP Host Count High	36
AWAP Host Count High Cleared	37
AWAP Host Count Low	37
AWAP Host Count Low Cleared	37
Background Reachability Check Succeeded	38
Background Reachability Check Failed	38
Backplane Bus A High Utilization	38
Backplane Bus A High Utilization Cleared	39
Backplane Bus B High Utilization	39
Backplane Bus B High Utilization Cleared	39
Backplane Bus C High Utilization	40
Backplane Bus C High Utilization Cleared	40
Backplane System Bus High Utilization	40
Backplane System Bus High Utilization Cleared	41
BGP Peer Briefly Established	41
BGP Peer Briefly Not Established	41
BGP Peer Disappeared	42
BGP Peer Established	42
BGP Peer Newly Discovered	42
BGP Peer Not Established	42
BladeCenter Blade +1.25V Rail High Voltage	43
BladeCenter Blade +1.25V Rail High Voltage Cleared	43
BladeCenter Blade +1.25V Rail Low Voltage	43
BladeCenter Blade +1.25V Rail Low Voltage Cleared	44
BladeCenter Blade +1.5V Rail High Voltage	44
BladeCenter Blade +1.5V Rail High Voltage Cleared	45
BladeCenter Blade +1.5V Rail Low Voltage	45
BladeCenter Blade +1.5V Rail Low Voltage Cleared	45
BladeCenter Blade +12V Rail High Voltage	46
BladeCenter Blade +12V Rail High Voltage Cleared	46
BladeCenter Blade +12V Rail Low Voltage	46
BladeCenter Blade +12V Rail Low Voltage Cleared	47
BladeCenter Blade +2.5V Rail High Voltage	47

BladeCenter Blade +2.5V Rail High Voltage Cleared	47
BladeCenter Blade +2.5V Rail Low Voltage	48
BladeCenter Blade +2.5V Rail Low Voltage Cleared	48
BladeCenter Blade +3.3V Rail High Voltage	48
BladeCenter Blade +3.3V Rail High Voltage Cleared	49
BladeCenter Blade +3.3V Rail Low Voltage	49
BladeCenter Blade +3.3V Rail Low Voltage Cleared	50
BladeCenter Blade +5V Rail High Voltage	50
BladeCenter Blade +5V Rail High Voltage Cleared	50
BladeCenter Blade +5V Rail Low Voltage	51
BladeCenter Blade +5V Rail Low Voltage Cleared	51
BladeCenter Blade Powered Off	51
BladeCenter Blade Powered On	52
BladeCenter Blower Failed	52
BladeCenter Blower Ok	52
BladeCenter Blower Slow	53
BladeCenter Chassis +1.8V Rail High Voltage	53
BladeCenter Chassis +1.8V Rail High Voltage Cleared	53
BladeCenter Chassis +1.8V Rail Low Voltage	54
BladeCenter Chassis +1.8V Rail Low Voltage Cleared	54
BladeCenter Chassis +12V Rail High Voltage	54
BladeCenter Chassis +12V Rail High Voltage Cleared	55
BladeCenter Chassis +12V Rail Low Voltage	55
BladeCenter Chassis +12V Rail Low Voltage Cleared	55
BladeCenter Chassis +2.5V Rail High Voltage	56
BladeCenter Chassis +2.5V Rail High Voltage Cleared	56
BladeCenter Chassis +2.5V Rail Low Voltage	56
BladeCenter Chassis +2.5V Rail Low Voltage Cleared	57
BladeCenter Chassis +3.3V Rail High Voltage	57
BladeCenter Chassis +3.3V Rail High Voltage Cleared	58
BladeCenter Chassis +3.3V Rail Low Voltage	58
BladeCenter Chassis +3.3V Rail Low Voltage Cleared	58
BladeCenter Chassis +5V Rail High Voltage	59
BladeCenter Chassis +5V Rail High Voltage Cleared	59
BladeCenter Chassis +5V Rail Low Voltage	59
BladeCenter Chassis +5V Rail Low Voltage Cleared	60
BladeCenter Chassis -5V Rail High Voltage	60

BladeCenter Chassis -5V Rail High Voltage Cleared	61
BladeCenter Chassis -5V Rail Low Voltage	61
BladeCenter Chassis -5V Rail Low Voltage Cleared	61
BladeCenter CPU1 High Temperature	62
BladeCenter CPU1 High Temperature Cleared	62
BladeCenter CPU2 High Temperature	62
BladeCenter CPU2 High Temperature Cleared	63
BladeCenter DASD1 High Temperature	63
BladeCenter DASD1 High Temperature Cleared	63
BladeCenter Front Panel High Temperature	64
BladeCenter Front Panel High Temperature Cleared	64
BladeCenter Management Module High Temperature	64
BladeCenter Management Module High Temperature Cleared	65
Chassis Fan Major Fault	65
Chassis Fan Minor Fault	65
Chassis Fan OK	65
Chassis Fan Status Unknown	66
Chassis Major Alarm	66
Chassis Major Alarm Cleared	66
Chassis Minor Alarm	67
Chassis Minor Alarm Cleared	67
Chassis Temperature Alarm	67
Chassis Temperature Alarm Cleared	67
Chassis Temperature Critical Alarm	68
CM Configuration Includes Policy Exclusion	68
CM Configuration Missing Policy Mandated Statement	68
CM Firmware Version Changed	69
CM Previously Unsaved Configuration Saved	69
CM Running Configuration Changed	69
CM Running Configuration Retrieval Failed	70
CM Startup Configuration Changed	71
CM Startup Configuration Retrieval Failed	71
CM Unsaved Configuration	72
Config Mgmt Job Failed	72
Config Mgmt Job Succeeded	73
CUCM CPU High Utilization	73
CUCM CPU High Utilization Cleared	73

CUCM CTI Device Not Registered	73
CUCM CTI Device Registered	74
CUCM Gatekeeper Not Registered	74
CUCM Gatekeeper Registered	75
CUCM Gateway Not Registered	75
CUCM Gateway Registered	75
CUCM H.323 Device Not Registered	76
CUCM H.323 Device Registered	76
CUCM Media Device Not Registered	76
CUCM Media Device Registered	77
CUCM Phone Not Registered	77
CUCM Phone Registered	78
CUCM Process Memory High Utilization	78
CUCM Process Memory High Utilization Cleared	78
CUCM Voicemail Device Not Registered	79
CUCM Voicemail Device Registered	79
Device Average CPU Utilization Critical	80
Device Average CPU Utilization High	80
Device Average CPU Utilization Cleared	80
Device Average Memory Usage Critical	80
Device Average Memory Usage High	81
Device Average Memory Usage Cleared	81
Device Clock Inconsistency	81
Device Cold Reboot	82
Device Fan Failure	82
Device Fan Failure Cleared	82
Device High Active Sessions	82
Device High Active Sessions Cleared	83
Device High Authenticated Response Time	83
Device High Authenticated Response Time Cleared	83
Device High External URL Response Time	84
Device High External URL Response Time Cleared	84
Device High Messages Received	84
Device High Messages Received Cleared	84
Device Low Disk Space	85
Device Low Disk Space Cleared	85
Device Name Resolution Failure	85

Entuity

Device Name Resolution Failure Cleared	85
Device Port(s) Utilization Accuracy Lost	86
Device Port(s) Utilization Accuracy at Risk	86
Device Port(s) Utilization Missed Due to Slow Response	86
Device Reboot Detected	87
Device Sensor Non-Operational	87
Device Sensor Non-Operational Cleared	87
Device Sensor Warning Value	88
Device Sensor Value Cleared	88
Device Reachability Degraded	88
Device Unreachable	89
Device Unreachable Cleared	89
Device Warm Reboot	89
EGP Neighbor Loss	90
EIGRP Peer Briefly Not Established	90
EIGRP Peer Disappeared	90
EIGRP Peer Newly Discovered	90
Entuity License Expired and This Entuity Server is No Longer Operational	91
Entuity License Not Updated by License Server and Will Expire	91
Entuity License on Remote Server Could Not be Updated	91
Entuity License on Remote Server Expired	92
Entuity License on Remote Server Successfully Updated	92
Entuity License Successfully Updated by License Server	92
Entuity Server Automated Shutdown	93
Entuity Server Component Restarting After Failure	93
Entuity Server Critical Component Restarting After Failure	93
Entuity Server Database Backup Failure	94
Entuity Server Disk Space Alert	94
Entuity Server Explicit Shutdown Initiated	95
Entuity Server Internal Event	95
Entuity Server License Alert	95
Entuity Server Permanent Component Failure	95
Entuity Server Shutdown Forced By Critical Failure To Restart	96
Entuity Server Started	96
Firewall Access Control Violations High	96
Firewall Access Control Violations High Cleared	97
Firewall High Avail User Set Oper State Compliant	97

Firewall High Avail User Set Oper State Non Compliant	98
Firewall High Current Connections	98
Firewall High Current Connections Cleared	98
Firewall Overflow and Intrusion Violations High	99
Firewall Overflow and Intrusion Violations High Cleared	99
Firewall URL Alerts High	100
Firewall URL Alerts High Cleared	100
FR DLCI High BECN	100
FR DLCI High BECN Cleared	101
FR DLCI High DE	101
FR DLCI High DE Cleared	101
FR DLCI High FECN	102
FR DLCI High FECN Cleared	102
FR DLCI High Inbound Utilization	102
FR DLCI High Inbound Utilization Cleared	102
FR DLCI High Outbound Utilization	103
FR DLCI High Outbound Utilization Cleared	103
FR DLCI Link Down	103
FR DLCI Link UP	103
HSRP Port Group Activated	104
HSRP Port Group Deactivated	104
IP SLA Creation Failure	104
IP SLA Creation Failure Cleared	105
IP SLA High ICPIF	105
IP SLA High ICPIF Cleared	105
IP SLA Low MOS	105
IP SLA Low MOS Cleared	106
IP SLA Test Failed	106
IP SLA Test High Latency	106
IP SLA Test High Latency Cleared	107
IP SLA Test Succeeded	107
IS-IS Peer Disappeared	107
IS-IS Peer Established	108
IS-IS Peer Newly Discovered	108
IS-IS Peer Not Established	108
LAP Antenna Host Count High	108
LAP Antenna Host Count High Cleared	109

LAP Antenna Host Count Low	109
LAP Antenna Host Count Low Cleared	109
Load Balancer High Connection Limit Pkt Drop Rate	110
Load Balancer High Connection Limit Pkt Drop Rate Cleared	110
Load Balancer High Current Sessions	110
Load Balancer High Current Sessions Cleared	111
Load Balancer High Error Count	111
Load Balancer High Error Count Cleared	111
Load Balancer High Inbound Error Rate	111
Load Balancer High Inbound Error Rate Cleared	112
Load Balancer High License Denied Pkt Rate	112
Load Balancer High License Denied Pkt Rate Cleared	112
Load Balancer High Maximum Sessions	112
Load Balancer High Maximum Sessions Cleared	113
Load Balancer High Memory Error Pkt Rate	113
Load Balancer High Memory Error Pkt Rate Cleared	113
Load Balancer High No Handler Denied Pkt Rate	114
Load Balancer High No Handler Denied Pkt Rate Cleared	114
Load Balancer High Non Syn Denied Pkt Rate	114
Load Balancer High Non Syn Denied Pkt Rate Cleared	115
Load Balancer High Outbound Error Rate	115
Load Balancer High Outbound Error Rate Cleared	115
Load Balancer High Packet Drop Rate	115
Load Balancer High Packet Drop Rate Cleared	116
Load Balancer High SLB SP Current Sessions	116
Load Balancer High SLB SP Current Sessions Cleared	116
Load Balancer Pool Critical Member Availability	117
Load Balancer Pool Critical Member Availability Cleared	117
Load Balancer Pool Critical Services Availability	117
Load Balancer Pool Critical Services Availability Cleared	117
Load Balancer Pool Low Member Availability	118
Load Balancer Pool Low Member Availability Cleared	118
Load Balancer Pool Low Services Availability	118
Load Balancer Pool Low Services Availability Cleared	119
MAC Address High Port Count	119
MAC Address High Port Count Cleared	119
MAC Address New	120

MAC Address Port Change	121
Memory Low	121
Memory Low Cleared	122
Missing Events	122
Module Disappeared	122
Module Discovered	123
Module Down	123
Module Major Fault	123
Module Minor Fault	123
Module Status OK	124
Module Status Unknown	124
MPLS LDP Entity Errors	124
MPLS LDP Entity Errors Cleared	125
MPLS LDP Entity Non-operational	125
MPLS LDP Entity Operational	125
MPLS LDP Entity Rejected Sessions	126
MPLS LDP Entity Rejected Sessions Cleared	126
MPLS LDP Entity Shutdown Notifications Received	126
MPLS LDP Entity Shutdown Notifications Received Cleared	126
MPLS LDP Entity Shutdown Notifications Sent	127
MPLS LDP Entity Shutdown Notifications Sent Cleared	127
MPLS LDP Peer Disappeared	127
MPLS LDP Peer Newly Discovered	128
MPLS LDP Peer Non-operational	128
MPLS LDP Peer Operational	128
MPLS LDP Peer TLV Errors	129
MPLS LDP Peer TLV Errors Cleared	129
MPLS LDP Peer Unknown Message Types	129
MPLS LDP Peer Unknown Message Types Cleared	129
MPLS LSR Interface High Discard Rate (Lookup Failure)	130
MPLS LSR Interface High Discard Rate (Lookup Failure) Cleared	130
MPLS LSR Interface High Error Free Discard Rate (RX)	130
MPLS LSR Interface High Error Free Discard Rate (RX) Cleared	131
MPLS LSR Interface High Error Free Discard Rate (TX)	131
MPLS LSR Interface High Error Free Discard Rate (TX) Cleared	131
MPLS LSR Interface High Fragmentation Rate	131
MPLS LSR Interface High Fragmentation Rate Cleared	132

MPLS LSR Interface Low Bandwidth	132
MPLS LSR Interface Low Bandwidth Cleared	132
MPLS LSR Interface Low Buffer Space	133
MPLS LSR Interface Low Buffer Space Cleared	133
MPLS LSR Platform High Discard Rate (Lookup Failure)	133
MPLS LSR Platform High Discard Rate (Lookup Failure) Cleared	133
MPLS LSR Platform High Error Free Discard Rate (RX)	134
MPLS LSR Platform High Error Free Discard Rate (RX) Cleared	134
MPLS LSR Platform High Error Free Discard Rate (TX)	134
MPLS LSR Platform High Error Free Discard Rate (TX) Cleared	134
MPLS LSR Platform High Fragmentation Rate	135
MPLS LSR Platform High Fragmentation Rate Cleared	135
MPLS VRF High Illegal Label Rate	135
MPLS VRF High Illegal Label Rate Cleared	136
MPLS VRF Interface BGP Neighbor Disappeared	136
MPLS VRF Interface BGP Neighbor Newly Discovered	136
MPLS VRF Non-operational	136
MPLS VRF Operational	137
Network Outage	137
Network Outage Cleared	139
OSPF Peer Briefly Not Established	139
OSPF Peer Disappeared	140
OSPF Peer Established	140
OSPF Peer Newly Discovered	140
OSPF Peer Not Established	140
Port Duplex Change	141
Port Error Disable Alarm	141
Port High Inbound Discards (Dynamic)	142
Port High Inbound Discards (Dynamic) Cleared	142
Port High Inbound Fault (Dynamic)	142
Port High Inbound Fault (Dynamic) Cleared	143
Port High Inbound Utilization (Dynamic)	143
Port High Inbound Utilization (Dynamic) Cleared	144
Port High Outbound Discards (Dynamic)	144
Port High Outbound Discards (Dynamic) Cleared	145
Port High Outbound Fault (Dynamic)	145
Port High Outbound Fault (Dynamic) Cleared	146

Port High Outbound Utilization (Dynamic)	146
Port High Outbound Utilization (Dynamic) Cleared	146
Port Inbound Discards High (Device Congestion)	146
Port Inbound Discards High Cleared (No Device Congestion)	147
Port Inbound Fault High (Packet Corruption)	147
Port Inbound Fault High (No Packet Corruption) Cleared	148
Port Link Down	148
Port Link Up	149
Port Low Inbound Utilization (Dynamic)	149
Port Low Inbound Utilization (Dynamic) Cleared	149
Port Low Outbound Utilization (Dynamic)	149
Port Low Outbound Utilization (Dynamic) Cleared	150
Port Operationally Down	150
Port Operationally Down Cleared	151
Port Outbound Discards High (Port Congestion)	151
Port Outbound Discards High (No Port Congestion) Cleared	151
Port Outbound Fault High (Transmit Errors)	152
Port Outbound Fault High Cleared (No Transmit Errors)	152
Port Speed Change	153
Port Utilization High	153
Port Utilization High Cleared	153
Port Utilization Low	153
Port Utilization Low Cleared	154
Power Supply Major Fault	154
Power Supply Minor Fault	154
Power Supply OK	154
Power Supply Unknown State	155
Processor Utilization High	155
Processor Utilization High Cleared	155
Routing Broadcast Traffic High	156
Routing Broadcast Traffic High Cleared	157
Routing High No Routes to IP Destination	157
Routing High No Routes to IP Destination Cleared	157
Routing ICMP High Redirects	157
Routing ICMP High Redirects Cleared	158
Routing ICMP High TTL Exceeds	158
Routing ICMP High TTL Exceeds Cleared	158

Service Down	158
Service State Degraded	159
Service State Off	159
Service State Unknown	159
Service Up	159
SNMP Agent Not Responding	160
SNMP Agent Responding	160
SNMP Agent Restart Detected	160
SNMP Authentication Failure	161
SNMP Response Time High	161
SNMP Response Time High Cleared	161
SNMP v3 Duplicate Engine ID	162
SSL Certificate Expired	162
SSL Certificate Expiring	162
SSL Proxy Service Administrative Available to SNMP Poll	162
SSL Proxy Service Administrative Unavailable to SNMP Poll	163
SSL Proxy Service Operational Available to SNMP Poll	163
SSL Proxy Service Operational Unavailable to SNMP Poll	163
STP New Root Device	163
STP VLAN Topology Change	164
Syslog Alert Event	164
Syslog Critical Events	165
Syslog Debug Events	165
Syslog Emergency Event	166
Syslog Error Events	166
Syslog Information Events	167
Syslog Notice Events	167
Syslog Warning Events	168
UCS Blade Down	168
UCS Blade Major Fault	169
UCS Blade Minor Fault	169
UCS Blade OK	169
UCS Blade Status Unknown	170
UCS Chassis Down	170
UCS Chassis Major Fault	170
UCS Chassis Minor Fault	171
UCS Chassis Status OK	171

UCS Chassis Status Unknown	171
UCS Fabric Extender Down	172
UCS Fabric Extender Major Fault	172
UCS Fabric Extender Minor Fault	172
UCS Fabric Extender Status OK	173
UCS Fabric Extender Status Unknown	173
UCS Fan Down	173
UCS Fan Major Fault	174
UCS Fan Minor Fault	174
UCS Fan Module Down	175
UCS Fan Module Major Fault	175
UCS Fan Module Minor Fault	175
UCS Fan Module Status OK	176
UCS Fan Module Status Unknown	176
UCS Fan Status OK	176
UCS Fan Status Unknown	176
UCS Local Disk Down	177
UCS Local Disk Major Fault	177
UCS Local Disk Minor Fault	178
UCS Local Disk Unknown	178
UCS Local Disk OK	178
UCS PSU Down	179
UCS PSU Major Fault	179
UCS PSU Minor Fault	179
UCS PSU Unknown	180
UCS PSU OK	180
UCS Switch Card Down	180
UCS Switch Card Major Fault	181
UCS Switch Card Minor Fault	181
UCS Switch Card Status OK	181
UCS Switch Card Status Unknown	182
Unknown Trap	182
User Defined Attribute State Disabled	182
User Defined Attribute State Down	183
User Defined Attribute State Other	183
User Defined Attribute State Up	183
User Defined Attribute Value Abnormality Cleared	183

User Defined Attribute Value Critical	184
User Defined Attribute Value High	184
User Defined Attribute Value Low	184
User Defined Attribute Value Warning	185
Virtual Machine Moved	185
Virtual Machine Powered Off	185
Virtual Machine Powered On	185
Virtualization Connection Failed	186
Virtualization Connection Success	186
VM Guest Memory High	186
VM Guest Memory High Cleared	186
VPN High Active Tunnels	187
VPN High Active Tunnels Cleared	187
VPN Load Average High	187
VPN Load Average High Cleared	187
VPN Network Port Utilization High	188
VPN Network Port Utilization High Cleared	188
VPN Tunnel Usage High	188
VPN Tunnel Usage High Cleared	188
WAN Port High Inbound Discards	189
WAN Port High Inbound Discards Cleared	189
WAN Port High Inbound Errors	189
WAN Port High Inbound Errors Cleared	190
WAN Port High Inbound Utilization	190
WAN Port High Inbound Utilization Cleared	190
WAN Port High Outbound Discards	191
WAN Port High Outbound Discards Cleared	191
WAN Port High Outbound Errors	191
WAN Port High Outbound Errors Cleared	192
WAN Port High Outbound Utilization	192
WAN Port High Outbound Utilization Cleared	192
WAN Port Low Inbound Utilization	193
WAN Port Low Inbound Utilization Cleared	193
WAN Port Low Outbound Utilization	193
WAN Port Low Outbound Utilization Cleared	194
Wireless Controller High Number of Connected APs	194
Wireless Controller High Number of Connected APs Cleared	194

2 Incidents Listing

AP Antenna Channel Change Frequency High Incident	195
AP Antenna Host Count Abnormality Incident	195
AP Antenna Offline Incident	196
AP Antenna Power Change Frequency High Incident	196
AP Host Count Abnormality Incident	196
AP Not Associated With Controller Incident	197
ATM VCC Inbound Utilization Abnormality Incident	197
ATM VCC Link Down Incident	197
ATM VCC Outbound Utilization Abnormality Incident	198
AvailMonitor Application Problem Incident	198
AvailMonitor High Latency Incident	198
AvailMonitor Low View Device Reachability Incident	199
Awap Host Count Abnormality Incident	199
Background Reachability Check Failure Incident	199
Backplane Bus A High Utilization Incident	200
Backplane Bus B High Utilization Incident	200
Backplane Bus C High Utilization Incident	200
Backplane System Bus High Utilization Incident	201
BGP Peer Briefly Established Incident	201
BGP Peer Briefly Not Established Incident	201
BGP Peer Disappeared Incident	201
BGP Peer Newly Discovered Incident	201
BGP Peer Not Established Incident	202
BladeCenter Blade +1.25V Rail Voltage Problem Incident	202
BladeCenter Blade +1.5V Rail Voltage Problem Incident	202
BladeCenter Blade +12V Rail Voltage Problem Incident	203
BladeCenter Blade +2.5V Rail Voltage Problem Incident	203
BladeCenter Blade +3.3V Rail Voltage Problem Incident	204
BladeCenter Blade +5V Rail Voltage Problem Incident	204
BladeCenter Blade Powered Off Incident	204
BladeCenter Blower Problem Incident	205
BladeCenter CPU1 High Temperature Incident	205
BladeCenter CPU2 High Temperature Incident	205
BladeCenter Chassis +1.8V Rail Voltage Problem Incident	206
BladeCenter Chassis +12V Rail Voltage Problem Incident	206
BladeCenter Chassis +2.5V Rail Voltage Problem Incident	207

BladeCenter Chassis +3.3V Rail Voltage Problem Incident	207
BladeCenter Chassis +5V Rail Voltage Problem Incident	207
BladeCenter Chassis -5V Rail Voltage Problem Incident	208
BladeCenter DASD1 High Temperature Incident	208
BladeCenter Front Panel High Temperature Incident	208
BladeCenter Management Module High Temperature Incident	209
CM Configuration Includes Policy Exclusion Incident	209
CM Configuration Missing Policy Mandated Statement Incident	209
CM Firmware Version Changed Incident	210
CM Running Configuration Changed Incident	210
CM Running Configuration Retrieval Failed Incident	210
CM Startup Configuration Changed Incident	210
CM Startup Configuration Retrieval Failed Incident	210
CM Unsaved Configuration Incident	211
CM Job Succeeded Incident	211
CM Job Failed Incident	211
CUCM CPU High Utilization Incident	211
CUCM CTI Device Not Registered Incident	212
CUCM Gatekeeper Not Registered Incident	212
CUCM Gateway Not Registered Incident	212
CUCM H323 Device Not Registered Incident	213
CUCM Media Device Not Registered Incident	213
CUCM Phone Not Registered Incident	213
CUCM Process Memory High Utilization Incident	213
CUCM Voicemail Device Not Registered Incident	214
Chassis Alarm Incident	214
Chassis Fan Status Problem Incident	214
Chassis Temperature Alarm Incident	215
Device Clock Inconsistency Incident	215
Device Average CPU Utilization High Incident	215
Device Average Memory Usage High Incident	216
Device Fan Failure Incident	216
Device High Active Sessions Incident	216
Device High Authenticated Response Time Incident	217
Device High External URL Response Time Incident	217
Device High Messages Received Incident	217
Device Low Disk Space Incident	217

Device Name Resolution Failure Incident	218
Device Not Responding to SNMP Incident	218
Device Port(s) Utilization Accuracy Problem	219
Device Reachability Problems Incident	219
Device Reboot Incident	219
Device Sensor Non-Operational Incident	219
Device Sensor Warning Value Incident	220
EGP Neighbor Loss Incident	220
EIGRP Peer Briefly Not Established Incident	220
EIGRP Peer Disappeared Incident	220
EIGRP Peer Newly Discovered Incident	221
Entuity License on Remote Server Problem Incident	221
Entuity License Problem Incident	221
Entuity Server Automated Shutdown Incident	222
Entuity Server Component Problem Incident	222
Entuity Server Database Backup Incident	222
Entuity Server Disk Space Alert Incident	222
Entuity Server Explicit Shutdown Initiated Incident	223
Entuity Server Internal Event Incident	223
Entuity Server License Alert Incident	223
Entuity Server Shutdown Forced by Critical Failure to Restart Incident	223
FR DLCI High BECN Incident	224
FR DLCI High DE Incident	224
FR DLCI High FECN Incident	224
FR DLCI High Inbound Utilization Incident	224
FR DLCI High Outbound Utilization Incident	225
FR DLCI Link Down Incident	225
Firewall Access Control Violations High Incident	225
Firewall High Avail User Set Oper State Non Compliant Incident	226
Firewall High Current Connections Incident	226
Firewall Overflow and Intrusion Violations High Incident	226
Firewall URL Alerts High Incident	227
HSRP Port Group Activated Incident	227
HSRP Port Group Deactivated Incident	227
IP SLA Creation Failure Incident	227
IP SLA Low MOS Incident	228
IP SLA Problem Incident	228

IP SLA Test Failed Incident	228
IP SLA Test High Latency Incident	229
IS-IS Peer Not Established Incident	229
IS-IS Peer Disappeared Incident	229
IS-IS Peer Newly Discovered Incident	229
LAP Antenna Host Count Abnormality Incident	230
Load Balancer High Connection Limit Pkt Drop Rate Incident	230
Load Balancer High Inbound Error Rate Incident	230
Load Balancer High License Denied Pkt Rate Incident	231
Load Balancer High Memory Error Pkt Rate Incident	231
Load Balancer High No Handler Denied Pkt Rate Incident	231
Load Balancer High Non Syn Denied Pkt Rate Incident	232
Load Balancer High Outbound Error Rate Incident	232
Load Balancer High Packet Drop Rate Incident	232
Load Balancer High SLB SP Current Sessions Incident	233
Load Balancer High Current Sessions Incident	233
Load Balancer High Maximum Sessions Incident	233
Load Balancer High Total Errors Incident	234
Load Balancer Pool Member Availability Problem Incident	234
Load Balancer Pool Services Availability Problem Incident	234
MAC Address High Port Count Incident	235
MAC Address New Incident	235
MAC Address Port Change Incident	235
MPLS LDP Entity Errors Incident	235
MPLS LDP Entity Non-operational Incident	236
MPLS LDP Entity Rejected Sessions Incident	236
MPLS LDP Entity Shutdown Notifications Received Incident	236
MPLS LDP Entity Shutdown Notifications Sent Incident	237
MPLS LDP Peer Non-operational Incident	237
MPLS LDP Peer TLV Errors Incident	237
MPLS LDP Peer Unknown Message Types Incident	238
MPLS LSR Interface High Discard Rate (Lookup Failure) Incident	238
MPLS LSR Interface High Error Free Discard Rate (RX) Incident	238
MPLS LSR Interface High Error Free Discard Rate (TX) Incident	239
MPLS LSR Interface High Fragmentation Rate Incident	239
MPLS LSR Interface Low Bandwidth Incident	239
MPLS LSR Interface Low Buffer Space Incident	239

MPLS LSR Platform High Discard Rate (Lookup Failure) Incident	240
MPLS LSR Platform High Error Free Discard Rate (RX) Incident	240
MPLS LSR Platform High Error Free Discard Rate (TX) Incident	240
MPLS LSR Platform High Fragmentation Rate Incident	241
MPLS VRF High Illegal Label Rate Incident	241
MPLS VRF Non-operational Incident	241
Memory Low Incident	242
Module Disappeared Incident	242
Module Discovered Incident	242
Module Status Problem Incident	242
Network Outage Incident	243
OSPF Peer Briefly Not Established Incident	243
OSPF Peer Disappeared Incident	243
OSPF Peer Newly Discovered Incident	244
OSPF Peer Not Established Incident	244
Port Error Disable Alarm Incident	244
Port High Inbound Discards (Dynamic) Incident	244
Port High Inbound Fault (Dynamic) Incident	245
Port High Outbound Discards (Dynamic) Incident	245
Port High Outbound Fault (Dynamic) Incident	245
Port Inbound Discards High (Device Congestion) Incident	246
Port Inbound Fault High (Packet Corruption) Incident	246
Port Inbound Utilization (Dynamic) Abnormality Incident	246
Port Link Down Incident	247
Port Operationally Down Incident	247
Port Outbound Discards High (Port Congestion) Incident	247
Port Outbound Fault High (Transmit Errors) Incident	247
Port Outbound Utilization (Dynamic) Abnormality Incident	248
Port Status Problem	248
Power Supply Problem Incident	249
Port Utilization Abnormality Incident	249
Processor Utilization High Incident	250
QoS Bandwidth Problem Incident	250
QoS Class Bit Rate High Incident	250
QoS Class Drop Bit Rate High Incident	250
QoS Class Drop Packet Rate (Buffer Shortage) High Incident	251
QoS Queue Drop Bit Rate High Incident	251

Routing Broadcast Traffic High Incident	251
Routing High No Routes To IP Destination Incident	252
Routing ICMP High Redirects Incident	252
Routing ICMP High TTL Exceeds Incident	252
Service State Problem Incident	253
SNMP Agent Restart Detected Incident	253
SNMP Authentication Failure Incident	253
SNMP Response Time High Incident	253
SNMP v3 Duplicate Engine ID Incident	254
SSL Certificate Problem Incident	254
SSL Proxy Service Administrative Unavailable to SNMP Poll Incident	254
SSL Proxy Service Operational Unavailable to SNMP Poll Incident	254
STP Topology Change Incident	255
Syslog Alert	255
Syslog Critical	255
Syslog Debug	255
Syslog Emergency	256
Syslog Error	256
Syslog Information	256
Syslog Notice	256
Syslog Warning	256
UCS Blade Status Incident	257
UCS Chassis Status Incident	257
UCS Fabric Extender Status Incident	257
UCS Fan Module Status Incident	258
UCS Fan Status Incident	258
UCS Local Disk Status Incident	259
UCS Power Supply Status Problem Incident	259
UCS Switch Card Status Incident	259
Unknown Trap Incident	260
User Defined Attribute Status Incident	260
User Defined Attribute Value Abnormality Incident	260
Virtualization Connection Failed Incident	261
VM Guest Memory High Incident	261
VM Moved Incident	261
VM Power Status Changed Incident	262
VPN High Active Tunnels Incident	262

Entuity

VPN Load Average High Incident	262
VPN Network Port Utilization High Incident	262
VPN Tunnel Usage High Incident	263
WAN Port High Inbound Discards Incident	263
WAN Port High Inbound Errors Incident	263
WAN Port High Outbound Discards Incident	264
WAN Port High Outbound Errors Incident	264
WAN Port Inbound Utilization Abnormality Incident	264
WAN Port Outbound Utilization Abnormality Incident	265
Wireless Controller High Number of Connected APs Incident	265
3 Event Groups, IDs and Severity	
Event Groups	266
Event and Incident Severity Levels	266
Event Type Identifiers	267
Index	284

Tables

Table 1	Event Groups.....	266
Table 2	Event Severity	267
Table 3	Event Identifiers	267

1 System Event Types Listing

Entuity includes an extensive set of events, categorized as system events. Through the Event Management System you can create new event types, these are categorized as custom events. This section contains system event descriptions, causes and possible actions to take for each event type.

Context sensitive help is available for all system events:

- 1) From the event viewer highlight an event and then from the context menu click **Help**.

The event help topic is integrated within the help system, you can use the Previous Topic and Next Topic links to step through the event help.

AP Antenna Host Count High

For each AWAP antenna you can set the number of hosts that when attached to an antenna would impact performance. You can set the threshold hierarchy at the global, AWAP and antenna levels.

Default severity level: **minor**, color code: yellow.

Typical Causes

Changes in wireless usage have occurred since the network was designed.

Actions

Through the AWAP Advanced tab you can review the hourly and daily mean and maximum attached host values. When the historic record indicates a rising usage trend you may want to extend the capabilities of your wireless network.

AP Antenna Host Count High Cleared

Raised when the number of hosts attached to the AWAP antenna has returned to an acceptable level.

Default severity level: **information**, color code: green.

Typical Causes

The managed object's performance is now within the set thresholds.

Actions

No action required.

AP Antenna Host Count Low

The number of hosts attached to the antenna has fallen below the set threshold. You can set this at the global, AWAP and antenna level. By default the threshold is set to 0, and disabled.

Default severity level: **minor**, color code: yellow.

Typical Causes

Changes in wireless usage have occurred since the network was designed.

Actions

You can check the Interface Advanced tab and review the hourly and daily mean and maximum attached host values. When the historic record indicates a falling usage trend you may want to adjust the capabilities of your wireless network.

AP Antenna Host Count Low Cleared

The number of hosts attached to the AWAP antenna has returned to an acceptable level.

Default severity level: **information**, color code: green.

Typical Causes

The managed object's performance is now within the set thresholds.

Actions

No action required.

AP Antenna Channel Change Frequency High

Automatic configuration change volatility indicates a trouble spot location.

Default severity level: **minor**, color code: yellow.

Typical Causes

A high frequency of channel change indicates a transmission problem. A change in the antenna's local environment impacts its effectiveness on the current channel, causing it to switch to another channel. Practically any appliance that operates on the same frequency level (2.4 GHz) as 802.11b or 802.11g can cause interference with your wireless network.

Actions

There are a number of factors that can cause the signal of your access point to deteriorate and the performance of your network to fall under par. Be sure to keep cordless phones, other electrical equipment at least one meter away from the access point.

You can check the WAP Advanced for example reviewing the antenna's current physical channel number and its history.

AP Antenna Channel Change Frequency High Cleared

The clearing correlation event for WAP's AP Antenna Channel Change Frequency High event.

Default severity level: **information**, color code: green.

Typical Causes

Automatic configuration change volatility that indicated a trouble spot location has been resolved.

Actions

No action required.

AP Antenna Offline

A WAP that was administratively up and operationally up Entuity has observed to transition into the administratively up and operationally down state.

Default severity level: **minor**, color code: yellow.

Typical Causes

A problem has occurred on the antenna.

Actions

Investigate the history of the antenna's performance.

AP Antenna Online

The clearing correlation event for WAP's AP Antenna Offline event.

Default severity level: **information**, color code: green.

Typical Causes

A WAP that was administratively up and operationally down Entuity has observed to transition into the administratively up and operationally up state.

Actions

No action required.

AP Antenna Power Change Frequency High

WAP antenna power changes more frequently than the set threshold during the polling interval. By default the frequency is set to three and enabled.

Default severity level: **minor**, color code: yellow.

Typical Causes

Automatic configuration is set to too an interval.

Actions

Review the WAP antenna power change history, frequent changes may indicate an unstable local environment.

AP Antenna Power Change Frequency High Cleared

The clearing correlation event for WAP Antenna Power Change Frequency High event.

Default severity level: **information**, color code: green.

Typical Causes

The number of hosts attached to the antenna has returned to an acceptable level.

Actions

No action required.

AP Associated With Controller

Indicates the WAP has transitioned to another wireless controller.

Default severity level: **minor**, color code: yellow.

Typical Causes

The wireless controller has gone down and been automatically, the WAP has been manually reassigned.

Actions

Investigate the status of the wireless controller.

AP Host Count High

The combined count of hosts that are wirelessly associated with all the antennas on a WAP has dropped below a selectable threshold. The threshold hierarchy will cover the global, wireless controller and WAP levels and will be disabled but set to 0 by default.

Default severity level: **minor**, color code: yellow.

Typical Causes

Changes in wireless usage have occurred since the network was designed.

Actions

You can check the WAP Advanced tab and review the hourly and daily mean and maximum attached host values. When the historic record indicates a rising usage trend you may want to extend the capabilities of your wireless network.

AP Host Count High Cleared

The clearing correlation event for WAP Host Count High event.

Default severity level: **information**, color code: green.

Typical Causes

The sum number of hosts attached to the WAP's antennas has returned to an acceptable level.

Actions

No action required.

AP Host Count Low

The sum number of hosts attached to the WAP's antennas has fallen below the set threshold.

Default severity level: **minor**, color code: yellow.

Typical Causes

Changes in wireless usage have occurred since the network was designed.

Actions

You can check the Interface Advanced tab and review the hourly and daily mean and maximum attached host values. When the historic record indicates a falling usage trend you may want to adjust the capabilities of your wireless network.

AP Host Count Low Cleared

The clearing correlation event for WAP Host Count Low event.

Default severity level: **information**, color code: green.

Typical Causes

The sum number of hosts attached to the WAP's antennas has returned to an acceptable level.

Actions

No action required.

AP Not Associated With Controller

Indicates the WAP has transitioned to another wireless controller.

Default severity level: **minor**, color code: yellow.

Typical Causes

The wireless controller has gone down and been automatically, the WAP has been manually reassigned.

Actions

Investigate the status of the wireless controller.

ATM VCC High Inbound Utilization

Indicates the Virtual Channel's inbound utilization has crossed its high threshold level.

Default severity level: **major**, color code: amber.

- *Source* identifies the router, port (ifDescr) and AAL5 VPI/VCI.
- *Impacted* identifies the impacted peer router, port and AAL5 VPI/VCI. When the impacted routers are not identified then Entuity displays **peer not known**.
- *Details* displays the channel's both actual, and threshold, utilization values.

Typical Causes

Virtual Channel's utilization is higher than the high utilization threshold for the port due to increased traffic.

Actions

Generate ATM utilization reports to monitor the situation.

ATM VCC High Inbound Utilization Cleared

Indicates a previous High ATM Inbound Utilization event for the Virtual Channel has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Reduced usage.

Actions

None.

ATM VCC High Outbound Utilization

Indicates the Virtual Channel's outbound utilization has crossed its high threshold level, where:

- *Source* identifies the router, port (ifDescr) and AAL5 VPI/VCI.
- *Impacted* identifies the impacted peer router, port and AAL5 VPI/VCI. When the impacted routers are not identified then Entuity displays **peer not known**.
- *Details* displays the channel's both actual, and threshold, utilization values.

Default severity level: **major**, color code: amber.

Typical Causes

Virtual Channel's utilization is higher than the high utilization threshold for the port due to increased traffic.

Actions

Generate ATM utilization reports to monitor the situation.

ATM VCC High Outbound Utilization Cleared

Indicates a previous High ATM Outbound Utilization event for the Virtual Channel has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Reduced usage.

Actions

None.

ATM VCC Link Down

Indicates that an ATM virtual channel has transitioned to the down state.

Default severity level: **severe**, color code: orange.

Typical Causes

The virtual channel is not functional because either the PVC is disabled or a port (on this switch) used by the PVC is down.

Actions

Check the ATM connection first by pinging the port. If the port responds contact your ATM service provider.

ATM VCC Link Up

Indicates that an ATM VCC has transitioned to the up state.

Default severity level: **information**, color code: green.

Typical Causes

Connecting a PC or server to a switch port, re-booting the PC or server attached to a switch port, WAN link CSU/DSU equipment re-establishing carrier detection.

Actions

None.

ATM VCC Low Inbound Utilization

Indicates the Virtual Channel's inbound utilization has crossed its low threshold level, where:

- *Source* identifies the router, port (ifDescr) and AAL5 VPI/VCI.

- *Impacted* identifies the impacted peer router, port and AAL5 VPI/VCI. When the impacted routers are not identified then Entuity displays **peer not known**.
- *Details* displays the channel's both actual, and threshold, utilization values.

Default severity level: **major**, color code: amber.

Typical Causes

Route changes, outages upstream of the link, server problems.

Actions

This problem may be symptomatic of an issue elsewhere in the network. Check through other events that have recently been reported if excessively low levels of utilization persist. Generate ATM utilization reports to monitor the situation.

ATM VCC Low Inbound Utilization Cleared

Indicates a previous ATM VCC Low Inbound Utilization alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Indicates previously low inbound utilization for the ATM VCC is now within the set thresholds.

Actions

None.

ATM VCC Low Outbound Utilization

Indicates the Virtual Channel's outbound utilization has crossed its low threshold level.

Default severity level: **major**, color code: amber.

- *Source* identifies the router, port (ifDescr) and AAL5 VPI/VCI.
- *Impacted* identifies the impacted peer router, port and AAL5 VPI/VCI. When the impacted routers are not identified then Entuity displays **peer not known**.
- *Details* displays the channel's both actual, and low threshold, outbound utilization values.

Typical Causes

Route changes, outages upstream of the link, server problems.

Actions

This problem may be symptomatic of an issue elsewhere in the network. Check through other events that have recently been reported if excessively low levels of utilization persist. Generate ATM utilization reports to monitor the situation.

ATM VCC Low Outbound Utilization Cleared

Indicates a previous ATM VCC Low Outbound Utilization alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Indicates previously low outbound utilization for the ATM VCC is now within the set thresholds.

Actions

None.

AvailMonitor Application Available

Entuity checks the availability of a monitored application by every two minutes attempting a TCP connect. If an application responds after previously failing to respond Entuity changes its availability state to Up.

Indicates a previous alarm has been cleared, e.g. Application Unavailable.

Default severity level: **information**, color code: green.

Typical Causes

Application is now available.

Actions

None.

AvailMonitor Application Unavailable

Entuity checks the availability of a monitored application by every two minutes attempting a TCP connect. If an application fails to respond Entuity considers the application as Down.

Default severity level: **severe**, color code: orange.

Typical Causes

Problem with server resources causing the application to crash, application bug or shutdown.

Actions

Check the server for the application.

AvailMonitor Falling Average Latency

Indicates the average real-time latency value for the hour falls short of the previous hourly value by the Falling Latency threshold set for the device. If the threshold has been changed during the preceding hour, then the most recent setting is used in the comparison. This threshold is in milliseconds.

Default severity level: **minor**, color code: yellow.

Typical Causes

Decrease in network traffic.

Actions

Investigate network resources.

AvailMonitor High Latency

Indicates the average real-time latency value for the hour exceeds the ICMP High Latency threshold set for the device. If the threshold has been changed during the preceding hour, then the most recent setting is used in the comparison. This threshold is in milliseconds.

Default severity level: **severe**, color code: orange.

Typical Causes

Increase in network traffic.

Actions

Investigate network resources.

AvailMonitor High Latency Reaching Application

Entuity checks the availability of a monitored application by every two minutes attempting a TCP connect, it also records the time taken to respond. For each application you can set a latency threshold, by default 3000ms, if the application response is slower than the set threshold then Entuity raises an event.

Default severity level: **severe**, color code: orange.

Typical Causes

Insufficient application resource or network congestion.

Actions

Use the Ticker tool to check the current application port utilization. If this is high, and a historical graph of port utilization reveals that, in general, the link is highly utilized, then more bandwidth may be needed.

AvailMonitor High Latency Reaching Application Cleared

Entuity checks the availability of a monitored application by every two minutes attempting a TCP connect, it also records the time taken to respond. For each application you can set a latency threshold, by default 3000ms. This event indicates that an application that was responding slowly is now responding within the Latency threshold.

Default severity level: **information**, color code: green.

Typical Causes

Reduced traffic.

Actions

None.

AvailMonitor Low View Device Reachability

Entuity measures device reachability by pinging a monitored device's IP management address every two minutes. Entuity raises this event when the combined number of devices responding to the ICMP ping and therefore reachable, set to Admin Down or in an Uninitialized state is, expressed as a percentage, below the Device Reachability threshold for the view.

Default severity level: **severe**, color code: orange.

Typical Causes

High utilization of the area of the network where the devices within the view are located.

Actions

Investigate the devices within the view. If the device reporting the event is a router, then Telnet to the router to ascertain possible causes for the outage.

AvailMonitor Normal Latency

Indicates the average real-time latency value for the hour is below the High Latency threshold. If the threshold has been changed during the preceding hour, then the most recent setting is used in the comparison. This threshold is in milliseconds.

Default severity level: **information**, color code: green.

Typical Causes

Correlated event to AvailMonitor High Latency, network latency has returned to within set boundaries.

Actions

None.

AvailMonitor Normal View Device Reachability

Entuity measures device reachability by pinging a monitored device's IP management address every two minutes. Entuity raises this event when the number of devices responding to the ICMP ping and therefore reachable is, expressed as a percentage, now above the Device Reachability threshold for the view.

Indicates device reachability within the view has returned to acceptable levels.

Default severity level: **information**, color code: green.

Typical Causes

Device reachability within the view has transitioned to be within the set threshold

Actions

None.

AvailMonitor Rising Average Latency

Indicates the average real-time latency value for the hour is above the Rising Latency threshold. If the threshold has been changed during the preceding hour, then the most recent setting is used in the comparison. This threshold is in milliseconds.

Default severity level: **severe**, color code: orange.

Typical Causes

Increase in network traffic.

Actions

Investigate network resources.

AvailMonitor Rising Trend in Average Latency

Indicates the average real-time latency value for the previous hour exceeds the trend for the same hour of the week by a value greater than the Rising Trend Latency threshold. If the threshold has been changed during the preceding hour, then the most recent setting is used in the comparison. This threshold is in milliseconds.

Default severity level: **severe**, color code: orange.

Typical Causes

Increase in network traffic.

Actions

Investigate network resources.

AWAP Host Count High

For each AWAP you can set the number of hosts that when attached to the AWAP would impact performance (this equates to the sum of the hosts each antenna can handle). You can set the threshold hierarchy at the global and antenna levels, By default the threshold is enabled and set to 512.

Default severity level: **minor**, color code: yellow.

Typical Causes

Changes in wireless usage have occurred since the network was designed.

Actions

You can check the AWAP Advanced tab and review the hourly and daily mean and maximum attached host values. When the historic record indicates a rising usage trend you may want to extend the capabilities of your wireless network.

AWAP Host Count High Cleared

The number of hosts attached to the AWAP has returned to an acceptable level.

Default severity level: **information**, color code: green.

Typical Causes

The managed object's performance is now within the set thresholds.

Actions

No action required.

AWAP Host Count Low

The combined count of hosts that are wirelessly associated with the AWAP has fallen below the set threshold. For all AWAPs the default threshold is set to 0, and disabled.

Default severity level: **minor**, color code: yellow.

Typical Causes

Changes in wireless usage have occurred since the network was designed.

Actions

You can check the AWAP Advanced tab and review the hourly and daily mean and maximum attached host values. When the historic record indicates a falling usage trend you may want to adjust the capabilities of your wireless network.

AWAP Host Count Low Cleared

The number of hosts attached to the AWAP has returned to an acceptable level.

Default severity level: **information**, color code: green.

Typical Causes

The managed object's performance is now within the set thresholds.

Actions

No action required.

Background Reachability Check Succeeded

Indicates a remote server that was not responding to the central server has started responding.

Default severity level: **information**, color code: green.

Typical Causes

A remote Entuity server that was not responding to the central server's reachability check has now responded.

Actions

No action required.

Background Reachability Check Failed

Indicates the Entuity central server check of the reachability of its remote server(s) has failed. One or more remote servers has failed to respond within the defined period.

By default the central server polls its remote servers every 15000 milliseconds and allows 10000 milliseconds to receive a response. These settings are configurable through *reachabilityAuditorPollingInterval* and *reachabilityAuditorFutureResultsTimeout* in *entuity.cfg*.

Default severity level: **severe**, color code: orange.

Typical Causes

Network outage, network congestion, Entuity server overload either of the remote or central server, or the restart of the remote Entuity, e.g. it was taken down for maintenance.

Actions

Check the status of the remote Entuity server, for example has it been taken down for scheduled maintenance? Review other raised events, do they indicate a general networking issue.

Backplane Bus A High Utilization

With some devices this indicates a major issue when the port speed and density is higher than the available backplane capabilities. When backplane utilization is over 50% it may also indicate port queuing or dropped traffic, which then leads to re-transmission and so more traffic.

There are separate backplane utilization events for Bus A, Bus B, Bus C and System Bus against each can be set a threshold value.

Default severity level: **minor**, color code: yellow.

Typical Causes

Insufficient backplane resources.

Actions

Consider reassigning links to under utilized backplanes, possible backplane upgrade.

Backplane Bus A High Utilization Cleared

Indicates that backplane utilization is now responding normally.

Default severity level: **information**, color code: green.

Typical Causes

Reduced utilization.

Actions

None.

Backplane Bus B High Utilization

With some devices this indicate a major issue when the port speed and density is higher than the available backplane capabilities. When backplane utilization is over 50% it may also indicate port queuing or dropped traffic, which then leads to re-transmission and so more traffic.

There are separate backplane utilization events for Bus A, Bus B, Bus C and System Bus against each can be set a threshold value.

Default severity level: **minor**, color code: yellow.

Typical Causes

Insufficient backplane resources.

Actions

Consider reassigning links to under utilized backplanes, possible backplane upgrade.

Backplane Bus B High Utilization Cleared

Indicates that backplane utilization is now responding normally.

Default severity level: **information**, color code: green.

Typical Causes

Reduced utilization.

Actions

None.

Backplane Bus C High Utilization

With some devices this indicate a major issue when the port speed and density is higher than the available backplane capabilities. When backplane utilization is over 50% it may also indicate port queuing or dropped traffic, which then leads to re-transmission and so more traffic.

There are separate backplane utilization events for Bus A, Bus B, Bus C and System Bus against each can be set a threshold value.

Default severity level: **minor**, color code: yellow.

Typical Causes

Insufficient backplane resources.

Actions

Consider reassigning links to under utilized backplanes, possible backplane upgrade.

Backplane Bus C High Utilization Cleared

Indicates that backplane utilization is now responding normally.

Default severity level: **information**, color code: green.

Typical Causes

Reduced utilization.

Actions

None.

Backplane System Bus High Utilization

With some devices this indicate a major issue when the port speed and density is higher than the available backplane capabilities. When backplane utilization is over 50% it may also indicate port queuing or dropped traffic, which then leads to re-transmission and so more traffic.

There are separate backplane utilization events for Bus A, Bus B, Bus C and System Bus against each can be set a threshold value.

Default severity level: **minor**, color code: yellow.

Typical Causes

Insufficient backplane resources.

Actions

Consider reassigning links to under utilized backplanes, possible backplane upgrade.

Backplane System Bus High Utilization Cleared

Indicates that backplane utilization is now responding normally.

Default severity level: **information**, color code: green.

Typical Causes

Reduced utilization.

Actions

None.

BGP Peer Briefly Established

Indicates to administrators that virtual links between BGP speakers are not established but bounced recently. Entuity identifies a recent bounce as the peer transition count is greater than zero.

Default severity level: **critical**, color code: red.

Typical Causes

BGP keep-alives may be lost, so the local router terminates the connection and then successfully attempt to reestablish it. Other causes maybe an unstable remote router, traffic shaping limitations.

Actions

Check logs are activated on the device. Use the logs to investigate error messages.

BGP Peer Briefly Not Established

Indicates to administrators that virtual links between BGP speakers are now established but bounced recently. Entuity identifies a recent bounce as the up time is lower than in the previous poll.

Default severity level: **critical**, color code: red.

Typical Causes

BGP keep-alives may be lost, so the local router terminates the connection and then successfully attempt to reestablish it. Other causes maybe an unstable remote router, traffic shaping limitations.

Actions

Check logs are activated on the device. Use the logs to investigate error messages.

BGP Peer Disappeared

Indicates a former adjacent peer has been removed from router's configuration. Administrator's should be aware of this change to be able to detect rogue configuration updates.

Default severity level: **critical**, color code: red.

Typical Causes

Update of router configuration.

Actions

Investigate the cause of router disappearance.

BGP Peer Established

Indicates to administrators that virtual links between BGP peer have just become well established.

Default severity level: **minor**, color code: yellow.

Typical Causes

BGP peer established.

Actions

None.

BGP Peer Newly Discovered

Indicates Entuity's discovery of a new BGP peer.

Default severity level: **minor**, color code: yellow.

Typical Causes

Configuration of a new BGP peer.

Actions

None.

BGP Peer Not Established

Indicates to administrators that a former adjacent peer is no longer in reach.

Default severity level: **critical**, color code: red.

Typical Causes

Problems with IP reachability or incorrect BGP configuration.

Actions

At the router's command line interface use the ping and show route commands to verify network connectivity to the BGP peer. You can use the **show log messages** command to look for errors relating to the peer.

BladeCenter Blade +1.25V Rail High Voltage

Indicates that the voltage reading for the +1.25v rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade +1.25V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade +1.25V Rail Low Voltage

Indicates that the voltage reading for the +1.25v rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade + 1.25V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade + 1.5V Rail High Voltage

Indicates that the voltage reading for the rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade + 1.5V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade + 1.5V Rail Low Voltage

Indicates that the voltage reading for the rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade + 1.5V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade + 12V Rail High Voltage

Indicates that the voltage reading for the rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade + 12V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade + 12V Rail Low Voltage

Indicates that the voltage reading for the rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade + 12V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade +2.5V Rail High Voltage

Indicates that the voltage reading for the rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade +2.5V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade +2.5V Rail Low Voltage

Indicates that the voltage reading for the rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade +2.5V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade +3.3V Rail High Voltage

Indicates that the voltage reading for the rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold

voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade +3.3V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade +3.3V Rail Low Voltage

Indicates that the voltage reading for the rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade +3.3V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade +5V Rail High Voltage

Indicates that the voltage reading for the rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade +5V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade +5V Rail Low Voltage

Indicates that the voltage reading for the rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Blade +5V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Blade Powered Off

Indicates that a blade has been switched off. This is identified through monitoring the voltage on the blade.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Blade switched off.

Actions

None.

BladeCenter Blade Powered On

Indicates that a blade has been switched on. This is identified through monitoring the voltage on the blade.

Default severity level: **information**, color code: green.

Event only available with the BladeCenter module.

Typical Causes

Blade switched on.

Actions

None.

BladeCenter Blower Failed

Indicates that a blower has failed. This is identified through monitoring the voltage on the blade. BladeCenter's built-in redundancy allows the remaining blower to successfully cool the BladeCenter.

Default severity level: **major**, color code: amber.

Event only available with the BladeCenter module.

Typical Causes

Blower failure.

Actions

Replace the blower. The failed blower module must be replaced within two minutes during service.

BladeCenter Blower Ok

Indicates that a BladeCenter blower has transitioned from a failed, or blower slow, state.

Default severity level: **information**, color code: green.

Event only available with the BladeCenter module.

Typical Causes

Previous problem with the blower, either slow performance or failure, has cleared.

Actions

None.

BladeCenter Blower Slow

Indicates that a blower is running at less than twenty percent (default threshold) of its maximum rotational speed. BladeCenter blowers usually operate at thirty percent or above of their maximum rotational speed, the exact speed depending upon the ambient temperature.

Default severity level: **minor**, Default color code: yellow.

Event only available with the BladeCenter module.

Typical Causes

Blower engine failure.

Actions

Replace the blower.

BladeCenter Chassis +1.8V Rail High Voltage

Indicates that the voltage reading for the +1.8v rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis +1.8V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the +1.8v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis + 1.8V Rail Low Voltage

Indicates that the voltage reading for the +1.8v rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis + 1.8V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the +1.8v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis + 12V Rail High Voltage

Indicates that the voltage reading for the +12v rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis + 12V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the +12v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis + 12V Rail Low Voltage

Indicates that the voltage reading for the +12v rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis + 12V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the +12v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis +2.5V Rail High Voltage

Indicates that the voltage reading for the +2.5v rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis +2.5V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the +2.5v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis +2.5V Rail Low Voltage

Indicates that the voltage reading for the +2.5v rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the

threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis +2.5V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the +2.5v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis +3.3V Rail High Voltage

Indicates that the voltage reading for the +3.3v rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis +3.3V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the +3.3v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis +3.3V Rail Low Voltage

Indicates that the voltage reading for the +3.3v rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis +3.3V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the +3.3v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis +5V Rail High Voltage

Indicates that the voltage reading for the +5v rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis +5V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the +5v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis +5V Rail Low Voltage

Indicates that the voltage reading for the +5v rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis +5V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the +5v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis -5V Rail High Voltage

Indicates that the voltage reading for the -5v rail has crossed the maximum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

Surge in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis -5V Rail High Voltage Cleared

Indicates a previous high voltage alarm raised against the -5v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter Chassis -5V Rail Low Voltage

Indicates that the voltage reading for the -5v rail has crossed the minimum voltage threshold for that rail. *Details* identifies the rail's correct voltage, the actual voltage and the threshold voltage (by default a 5% variance from the correct voltage). Voltage readings are given in millivolts.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A drop in BladeCenter power supply, poorly seated or malfunctioning blade.

Actions

- 1) Check BladeCenter power.
- 2) Reseat blade server.
- 3) Replace blade server.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Chassis -5V Rail Low Voltage Cleared

Indicates a previous low voltage alarm raised against the -5v rail has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the rail voltage has cleared.

Actions

None.

BladeCenter CPU1 High Temperature

Indicates that the temperature reading for the CPU has crossed the maximum threshold for that CPU. *Details* identifies the actual temperature and the temperature threshold. Temperature readings are given in degrees Celsius.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A rise in the ambient temperature, blower failure or missing components, e.g. a blade, that impact the cooling of the BladeCenter.

Actions

Ensure the BladeCenter is properly cooled; checking blower performance, ambient temperature and missing components.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter CPU1 High Temperature Cleared

Indicates a previous high temperature alarm raised against the CPU has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the CPU temperature has cleared.

Actions

None.

BladeCenter CPU2 High Temperature

Indicates that the temperature reading for the CPU has crossed the maximum threshold for that CPU. *Details* identifies the actual temperature and the temperature threshold. Temperature readings are given in degrees Celsius.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A rise in the ambient temperature, blower failure or missing components, e.g. a blade, that impact the cooling of the BladeCenter.

Actions

Ensure the BladeCenter is properly cooled; checking blower performance, ambient temperature and missing components.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter CPU2 High Temperature Cleared

Indicates a previous high temperature alarm raised against the CPU has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the CPU temperature has cleared.

Actions

None.

BladeCenter DASD1 High Temperature

Indicates that the temperature reading for the CPU has crossed the maximum threshold for that CPU. *Details* identifies the actual temperature and the temperature threshold. Temperature readings are given in degrees Celsius.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A rise in the ambient temperature, blower failure or missing components, e.g. a blade, that impact the cooling of the BladeCenter.

Actions

Ensure the BladeCenter is properly cooled; checking blower performance, ambient temperature and missing components.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter DASD1 High Temperature Cleared

Indicates a previous high temperature alarm raised against the DASD1 has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the CPU temperature has cleared.

Actions

None.

BladeCenter Front Panel High Temperature

Indicates that the temperature reading for the CPU has crossed the maximum threshold for that CPU. *Details* identifies the actual temperature and the temperature threshold. Temperature readings are given in degrees Celsius.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A rise in the ambient temperature, blower failure or missing components, e.g. a blade, that impact the cooling of the BladeCenter.

Actions

Ensure the BladeCenter is properly cooled; checking blower performance, ambient temperature and missing components.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Front Panel High Temperature Cleared

Indicates a previous high temperature alarm raised against the Front Panel has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the CPU temperature has cleared.

Actions

None.

BladeCenter Management Module High Temperature

Indicates that the temperature reading for the CPU has crossed the maximum threshold for that CPU. *Details* identifies the actual temperature and the temperature threshold. Temperature readings are given in degrees Celsius.

Default severity level: **severe**, color code: orange.

Event only available with the BladeCenter module.

Typical Causes

A rise in the ambient temperature, blower failure or missing components, e.g. a blade, that impact the cooling of the BladeCenter.

Actions

Ensure the BladeCenter is properly cooled; checking blower performance, ambient temperature and missing components.



Entuity recommend always consulting the BladeCenter documentation.

BladeCenter Management Module High Temperature Cleared

Indicates a previous high temperature alarm raised against the management module has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the CPU temperature has cleared.

Actions

None.

Chassis Fan Major Fault

Indicates that a device has a major fan hardware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty fan hardware, faulty environmental card, faulty supervisor card.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

Chassis Fan Minor Fault

Indicates that a device has a minor fan hardware problem.

Default severity level: **major**, color code: amber.

Typical Causes

Faulty fan hardware, faulty environmental card, faulty supervisor card.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

Chassis Fan OK

Indicates that a previous fan fault for a device has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Faulty firmware has been swapped out.

Actions

None.

Chassis Fan Status Unknown

Indicates the status of the fan is not reportable or is unknown.

Default severity level: **minor**, color code: yellow.

Typical Causes

The status of the fan is not reportable. Or, the fan status is unknown.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

Chassis Major Alarm

Indicates that a device is reporting a major hardware or firmware problem which is causing or may cause the device to fail.

Default severity level: **critical**, color code: red.

Typical Causes

Power supply problems, fan failures, temperature alarms, module faults.

Actions

Telnet to the device and check the current system settings. A hardware swap out may need to be scheduled depending on the type of problem.

Chassis Major Alarm Cleared

Indicates a previous alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

The original cause of the alarm, e.g. power supply problems, fan failures, temperature alarms, module faults has been corrected.

Actions

No action required.

Chassis Minor Alarm

Indicates that a device is reporting a minor hardware or firmware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Power supply problems, fan failures, temperature alarms, module faults.

Actions

Telnet to the device and check the current system settings. A hardware swap out may need to be scheduled depending on the type of problem.

Chassis Minor Alarm Cleared

Indicates a previous alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

The original cause of the alarm, e.g. power supply problems, fan failures, temperature alarms, module faults has been corrected.

Actions

No action required.

Chassis Temperature Alarm

Indicates that a device has measured a significant increase in ambient temperature.

Default severity level: **major**, color code: amber.

Typical Causes

Faulty fan hardware, faulty environmental card, comms room problems.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

Chassis Temperature Alarm Cleared

Indicates that a device temperature problem is resolved.

Default severity level: **information**, color code: green.

Typical Causes

Hardware swap out to resolve a previous problem.

Actions

None.

Chassis Temperature Critical Alarm

Indicates that a device has measured a potentially fatal increase in ambient temperature.

Default severity level: **critical**, color code: red.

Typical Causes

Faulty fan hardware, faulty environmental card, communications room problems.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

CM Configuration Includes Policy Exclusion

Indicates Entuity Configuration Monitor has identified a device configuration which includes a setting that violates good practice.

Default severity level: **minor**, color code: yellow.

Typical Causes

Poorly, or wrongly defined device configuration.

Actions

Entuity raises an event for each policy violation. In the Open view mode of Event Viewer these events are collapsed into one row, with # identifying the number of events. View the events in History mode to view in the event's *Details* the specific policy violation.

Correct the configuration on the device or amended your policy mandated statements file.

CM Configuration Missing Policy Mandated Statement

Indicates Entuity Configuration Monitor has identified that the device configuration does not include a setting required for the device to be configured according to good practice.

Default severity level: **minor**, color code: yellow.

Typical Causes

Poorly, or wrongly defined device configuration.

Actions

Entuity raises an event for each policy violation. In the Open view mode of Event Viewer these events are collapsed into one row, with # identifying the number of events. View the events in History mode to view in the event's *Details* the specific policy violation.

Correct the configuration on the device or amended your policy mandated statements file.

CM Firmware Version Changed

Indicates Entuity has identified a change in the device firmware. configuration. Entuity raises this event and also retrieves the device configuration.

Default severity level: **minor**, color code: yellow.

Typical Causes

This would usually be an authorized change in the device firmware, however an unauthorized change may indicate a security issue.

Actions

Entuity Configuration Monitor initiates a retrieval of device configuration, which you can view in the archive directory.

CM Previously Unsaved Configuration Saved

Indicates the current running and startup device configuration files are now the same.

Default severity level: **information**, color code: green.

Typical Causes

A device configuration previously identified as not being saved, has now been saved.

Actions

None required.

CM Running Configuration Changed

Indicates Entuity Configuration Monitor has retrieved a device running configuration that is significantly different from the previous running configuration retrieved from that device. This new configuration is stored making it the new last-seen running-configuration. This event expires in 24 hours.

Default severity level: **severe**, color code: orange.

Typical Causes

A known configuration change to the device.

Actions

From the event's context menu you can compare the most recent running configurations. You can also compare configurations through the device's web UI Entuity Configuration Monitor page.

CM Running Configuration Retrieval Failed

Indicates Entuity Configuration Monitor attempted, but failed, to retrieve device running configuration. *Details* describes the failure to retrieve the configuration and identifies the device, either by resolved name or IP address. This event ages out after 24 hours.

Default severity level: **minor**, color code: yellow.

Typical Causes

When this event is raised against:

- All devices with configuration retrieval enabled it suggests a system wide problem, for example that the transport server is not running, that the transfer and archive folders do not exist or permission to write to them is denied.
- Many devices with configuration retrieval enabled it suggests a localized issue, for example maybe those devices share the same credential set the definition of which is no longer valid.
- 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.

Actions

- 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 TFTP, TFTP, SCP and RCP servers it does not check that a required 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 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.

- 3) To assist your investigation you may want to activate debug mode and then re-run configuration retrieval. The additional information assists in identifying where the failure in configuration retrieval occurs.

CM Startup Configuration Changed

Indicates Entuity Configuration Monitor has retrieved a device startup configuration that is significantly different from the previous startup configuration retrieved from that device. This new configuration is stored making it the new last-seen startup-configuration. This event ages out in twenty-four hours.

Default severity level: **severe**, color code: orange.

Typical Causes

A known configuration change to the device.

Actions

From Event Viewer open the current and previous configurations and compare the difference.

CM Startup Configuration Retrieval Failed

Indicates Entuity Configuration Monitor attempted, but failed, to retrieve device running configuration. *Details* describes the failure to retrieve the configuration and identifies the device, either by resolved name or IP address. This event ages out after 24 hours.

Default severity level: **minor**, color code: yellow.

Typical Causes

When this event is raised against:

- All devices with configuration retrieval enabled it suggests a system wide problem, for example that the transport server is not running, that the transfer and archive folders do not exist or permission to write to them is denied.
- Many devices with configuration retrieval enabled it suggests a localized issue, for example maybe those devices share the same credential set the definition of which is no longer valid.
- 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.

Actions

- 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 transport servers. Although Entuity Configuration Monitor is configured to work with the specified FTP, TFTP, SCP and RCP 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 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.

- 3) To assist your investigation you may want to activate debug mode and then re-run configuration retrieval. The additional information assists in identifying where the failure in configuration retrieval occurs.

CM Unsaved Configuration

Indicates Entuity Configuration Monitor has retrieved, and compared, the current running and startup device configuration files. Entuity Configuration Monitor has found a significant difference between the two, which indicates an unsaved configuration change.

Default severity level: **minor**, color code: yellow.

Typical Causes

A configuration change to the device.

Actions

From Event Viewer open the current and previous configurations and compare the differences.

Config Mgmt Job Failed

Indicates one or more of the sub-jobs associated with the identified job failed.

This event can be disabled for all jobs derived from the task through the task's administration Advanced page and the *Raise Event on Completion* check box.

Default severity level: **severe**, color code: orange.

Typical Causes

The event details includes information on the cause of the job failure, for example:

- Validation failure
- User credential failure
- Timeout of a sub-job.

Actions

Investigate the task history.

Config Mgmt Job Succeeded

Indicates the identified job successfully completed and therefore all of its sub-jobs successfully completed.

This event can be disabled for all jobs derived from the task through the task's administration Advanced page and the *Raise Event on Completion* check box.

Default severity level: **information**, color code: green.

Typical Causes

N/A.

Actions

None.

CUCM CPU High Utilization

Indicates a process on the Cisco Unified Communications Manager server has high CPU utilization.

Default severity level: **severe**, color code: orange.

Typical Causes

High Cisco Unified Communications Manager CPU utilization due to interrupts, or a particular process using a lot of CPU resources. Each device type registered with the Cisco Unified Communications Manager has a weight, this weight should match the Cisco Unified Communications Manager server specification. Problems may occur when this is not the case.

Actions

Use Flex Reports to create a Cisco Unified Communications Manager CPU Report, for example one that runs every hour to monitor CPU utilization.

CUCM CPU High Utilization Cleared

Indicates a previous alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with the CPU utilization has cleared.

Actions

None.

CUCM CTI Device Not Registered

Indicates the CTI device has not registered to the Cisco Unified Communications Manager.

Default severity level: **critical**, color code: red.

Typical Causes

Cisco Unified Communications Manager or the CTI Manager may have failed. Alternatively, the Cisco Unified Communications Manager may have insufficient resources to handle additional devices.

Actions

- 1) Check the event *Details*. This indicates the particular cause of the event.
- 2) Incomplete registration may indicate a device is re-homing in the middle of registration.
- 3) The alarm could also indicate a device misconfiguration, database error, or an illegal/unknown device trying to attempt a connection.
- 4) For a Cisco Unified Communications Manager or CTI Manager failure the device attempts to re-register with the back up Cisco Unified Communications Manager or CTI Manager. Entuity raises a successful device registration event. Check the Cisco Unified Communications Manager and CTI Manager for failures.
- 5) If multiple device types are failing to register with the Cisco Unified Communications Manager check the Cisco Unified Communications Manager server has sufficient available CPU and memory resources to support additional devices.

Entuity monitors Cisco Unified Communications Manager CPU and Memory performance, raising events when high utilization thresholds are crossed. Also run a Flex Report on these metrics.

Consult the Cisco Unified Communications Manager documentation for details on device weighting.

CUCM CTI Device Registered

Indicates the CTI device has successfully registered to the Cisco Unified Communications Manager.

Default severity level: **information**, color code: green.

Typical Causes

Successful CTI device registration.

Actions

None.

CUCM Gatekeeper Not Registered

Cisco Unified Communications Manager cannot register with the gatekeeper.

Default severity level: **critical**, color code: red.

Typical Causes

Gatekeeper configuration problems. Entuity details the specific error code.

Actions

- 1) Check IP visibility from Cisco Unified Communications Manager to the gatekeeper.
- 2) Check gatekeeper status and verify that the gatekeeper state is up.
- 3) When there is a zone subnet defined on the gatekeeper, verify that the subnet of the gateway is in the allowed subnets.

CUCM Gatekeeper Registered

Indicates the gatekeeper has successfully registered to the Cisco Unified Communications Manager.

Default severity level: **information**, color code: green.

Typical Causes

Successful gatekeeper registration.

Actions

None.

CUCM Gateway Not Registered

Gateway registration may fail for a number of reasons.

Default severity level: **critical**, color code: red.

Typical Causes

Gateway registration may fail for a number of reasons, e.g. gateway software failure.

Actions

Check that the gateway is up and running. All gateways have a heartbeat LED that blinks one second on and one second off when the gateway software is running normally. After a registration failure the gateway attempts to recover, which alters the LED blink pattern. If the gateway fails to recover consult the gateway documentation.

CUCM Gateway Registered

Indicates the gateway has successfully registered to the Cisco Unified Communications Manager.

Default severity level: **information**, color code: green.

Typical Causes

Successful gateway registration.

Actions

None.

CUCM H.323 Device Not Registered

H.323 Gateway device registration may fail for a number of reasons.

Default severity level: **critical**, color code: red.

Typical Causes

H.323 registration may fail for a number of reasons, e.g. gateway software failure.

Actions

Check that the gateway is up and running. All gateways have a heartbeat LED that blinks one second on and one second off when the gateway software is running normally. After a registration failure the gateway attempts to recover, which alters the LED blink pattern. If the gateway fails to recover consult the gateway documentation.

CUCM H.323 Device Registered

Indicates the H323 device has successfully registered to the CUCM.

Default severity level: **information**, color code: green.

Typical Causes

Successful H232 device registration.

Actions

None.

CUCM Media Device Not Registered

Indicates the media device has not registered to the Cisco Unified Communications Manager.

Default severity level: **critical**, color code: red.

Typical Causes

Cisco Unified Communications Manager may have failed or not recognized the device type. Alternatively, the Cisco Unified Communications Manager may have insufficient resources to handle additional devices.

Actions

- 1) Check the event *Details*. This indicates the particular cause of the event.
- 2) Incomplete registration may indicate a device is re-homing in the middle of registration.
- 3) The alarm could also indicate a device misconfiguration, database error, or an illegal/

unknown device trying to attempt a connection.

- 4) For a Cisco Unified Communications Manager failure the device attempts to re-register with the back up Cisco Unified Communications Manager. Entuity raises a successful device registration event. Check the Cisco Unified Communications Manager for failures.
- 5) If multiple device types are failing to register with the Cisco Unified Communications Manager check the Cisco Unified Communications Manager machine has sufficient available CPU and memory resources to support additional devices.

Entuity monitors Cisco Unified Communications Manager CPU and Memory performance, raising events when high utilization thresholds are crossed. Also run a Flex Report on these metrics.

Consult the Cisco Unified Communications Manager documentation for details on device weighting.

CUCM Media Device Registered

Indicates the media device has successfully registered to the Cisco Unified Communications Manager.

Default severity level: **information**, color code: green.

Typical Causes

Successful media device registration.

Actions

None.

CUCM Phone Not Registered

Indicates the phone has not registered to the Cisco Unified Communications Manager.

Default severity level: **critical**, color code: red.

Typical Causes

Cisco Unified Communications Manager may have failed. Automatic phone registration may be turned off (default state). The Cisco Unified Communications Manager may have insufficient resources to handle additional devices.

Actions

- 1) Check the event *Details*. This indicates the particular cause of the event.
- 2) Incomplete registration may indicate a device is re-homing in the middle of registration.
- 3) The alarm could also indicate a device misconfiguration, database error, or an illegal/unknown device trying to attempt a connection.
- 4) For a Cisco Unified Communications Manager failure the device attempts to re-register with the back up Cisco Unified Communications Manager. Entuity raises a successful device registration event. Check the Cisco Unified Communications Manager for failure.

- 5) If multiple device types are failing to register with the Cisco Unified Communications Manager check the Cisco Unified Communications Manager machine has sufficient available CPU and memory resources to support additional devices.

Entuity monitors Cisco Unified Communications Manager CPU and Memory performance, raising events when high utilization thresholds are crossed. Also run a Flex Report on these metrics.

Consult the Cisco Unified Communications Manager documentation for details on device weighting.

CUCM Phone Registered

Indicates the phone has successfully registered to the Cisco Unified Communications Manager.

Default severity level: **information**, color code: green.

Typical Causes

Successful phone registration.

Actions

None.

CUCM Process Memory High Utilization

Indicates the Cisco Unified Communications Manager has high process memory utilization.

Default severity level: **severe**, color code: orange.

Typical Causes

High CUCM process memory utilization due to interrupts, or a particular process using a lot of memory resources. Each device type registered with the Cisco Unified Communications Manager has a weight, this weight should match the Cisco Unified Communications Manager server specification. Problems may occur when this is not the case.

Actions

Use Flex Reports to create a Cisco Unified Communications Manager memory report, for example one that runs every hour to monitor Cisco Unified Communications Manager memory utilization.

CUCM Process Memory High Utilization Cleared

Indicates a previous alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Previous problem with high memory utilization has cleared.

Actions

None.

CUCM Voicemail Device Not Registered

Indicates the voicemail device has not registered to the CUCM.

Default severity level: **critical**, color code: red.

Typical Causes

Cisco Unified Communications Manager may have failed or not recognized the device type. Alternatively, the Cisco Unified Communications Manager may have insufficient resources to handle additional devices.

Actions

- 1) Check the event *Details*. This indicates the particular cause of the event.
- 2) Incomplete registration may indicate a device is re-homing in the middle of registration.
- 3) The alarm could also indicate a device misconfiguration, database error, or an illegal/unknown device trying to attempt a connection.
- 4) For a Cisco Unified Communications Manager failure the device attempts to re-register with the back up Cisco Unified Communications Manager. Entuity raises a successful device registration event. Check the Cisco Unified Communications Manager for failure.
- 5) If multiple device types are failing to register with the Cisco Unified Communications Manager check the Cisco Unified Communications Manager machine has sufficient available CPU and memory resources to support additional devices.

Entuity monitors Cisco Unified Communications Manager CPU and Memory performance, raising events when high utilization thresholds are crossed. Also run a Flex Report on these metrics.

Consult the Cisco Unified Communications Manager documentation for details on device weighting.

CUCM Voicemail Device Registered

Indicates the voicemail device has successfully registered to the Cisco Unified Communications Manager.

Default severity level: **information**, color code: green.

Typical Causes

Successful voicemail device registration.

Actions

None.

Device Average CPU Utilization Critical

Indicates high device CPU utilization, as an average of the utilization of all of its processors.

Default severity level: **severe**, color code: orange.

Typical Causes

High CPU utilization due to interrupts, a particular process using a lot of CPU resources.

Actions

Use the managed host function to view current and historic levels of process usage. Also create reports, for example a Routing Summary Report that runs every hour to monitor router CPU utilization.

Device Average CPU Utilization High

Indicates high device CPU utilization, as an average of the utilization of all of its processors.

Default severity level: **severe**, color code: orange.

Typical Causes

High CPU utilization due to interrupts, a particular process using a lot of CPU resources.

Actions

Use the managed host function to view current and historic levels of process usage. Also create reports, for example a Routing Summary Report that runs every hour to monitor router CPU utilization.

Device Average CPU Utilization Cleared

Indicates that processor utilization on the device, as an average of all the device's processor utilization, is no longer higher than the set threshold.

Default severity level: **information only**, color code: green.

Typical Causes

Reduced usage.

Actions

None.

Device Average Memory Usage Critical

Indicates the device has a high level of usage resulting in a critically low level of available memory. Entuity combines all memory resources on the device, calculates the assigned resource and then raises the event when that resource is greater than the set threshold, by default 90%.

Default severity level: **severe**, color code: orange.

Typical Causes

Low memory may be caused through a combination of factors; as a memory leak that has consumed a large amount of memory, a network instability pushes the free memory to zero and the device does not have enough memory to begin with but the problem is discovered only during a rare network event.

Actions

Use the managed host function to view current and historic levels of memory

Device Average Memory Usage High

Indicates the device has low memory. Entuity combines all memory resources on the device, calculates the assigned resource and then raises the event when that resource is greater than the set threshold, by default 80%.

Default severity level: **severe**, color code: orange.

Typical Causes

Low memory may be caused through a combination of factors; as a memory leak that has consumed a large amount of memory, a network instability pushes the free memory to zero and the device does not have enough memory to begin with but the problem is discovered only during a rare network event.

Actions

Use the managed host function to view current and historic levels of memory

Device Average Memory Usage Cleared

Indicates the device is no longer suffering from low memory.

Default severity level: **information**, color code: green.

Typical Causes

Reduced usage.

Actions

None.

Device Clock Inconsistency

Poll samples for the device have been discarded because of a too great discrepancy between the sample interval according to device sysUpTime and the sample interval according to Entuity's clock.

Default severity level: **minor**, color code: yellow.

Typical Causes

Slow running network. misconfigured device clock.

Actions

This event does not necessarily indicate a network problem. Tolerance values for this event may be adjusted via settings in `entuity.cfg`.

Device Cold Reboot

Indicates that a device has just been rebooted or reset. This event is detected by the generation of an SNMP trap on the device.

Default severity level: **severe**, color code: orange.

Typical Causes

Device configuration changes, hardware/software/firmware faults, lack of memory on the device, power failures.

Actions

Telnet to the device and check the system logs for an indication of what caused the device to reboot.

Device Fan Failure

Indicates the failure of a fan on the device.

Default severity level: **critical**, color code: red.

Typical Causes

Fan failure on the device.

Actions

The event includes the identifier of the failed fan, which you can use when investigating the failure and to locate it if you have to replace the fan.

Device Fan Failure Cleared

Indicates a fan that had failed on the device is once again working.

Default severity level: **information**, color code: green.

Typical Causes

The fan may have restarted, or it may have been replaced with a new fan.

Actions

None required.

Device High Active Sessions

Indicates the number of active sessions is greater than the set threshold, by default 1000.

Default severity level: **warning**, color code: amber.

Typical Causes

Highest number of active sessions is greater than the set threshold when the device is polled.

Actions

Investigate the session history of the device.

Device High Active Sessions Cleared

Indicates the number of active sessions was greater than the set threshold, by default 1000, but has now transitioned below the set boundary.

Default severity level: **information**, color code: green.

Typical Causes

The number of sessions is below the set threshold.

Actions

None.

Device High Authenticated Response Time

Data for this event is retrieved through custom scripts. Contact Entuity Professional Services for details.

Default severity level: **warning**, color code: amber.

Typical Causes

Authentication response time is greater than the set threshold.

Actions

Investigate the authentication history of the device.

Device High Authenticated Response Time Cleared

Data for this event is retrieved through custom scripts. Contact Entuity Professional Services for details.

Default severity level: **information**, color code: green.

Typical Causes

Authentication response time was greater than the set threshold, but has now transitioned below the set boundary.

Actions

None.

Device High External URL Response Time

Data for this event is retrieved through custom scripts. Contact Entuity Professional Services for details.

Default severity level: **warning**, color code: amber.

Typical Causes

External URL response time is greater than the set threshold.

Actions

Investigate the history of the device.

Device High External URL Response Time Cleared

Data for this event is retrieved through custom scripts. Contact Entuity Professional Services for details.

Default severity level: **information**, color code: green.

Typical Causes

External URL response time was greater than the set threshold, but has now transitioned below the set boundary.

Actions

None.

Device High Messages Received

Indicates the number of message received is greater than the set threshold, by default 1000.

Default severity level: **warning**, color code: amber.

Typical Causes

A large number of messages have been sent to this device.

Actions

Investigate the history of the device.

Device High Messages Received Cleared

Indicates the number of message received was greater than the set threshold, by default 1000, but has now transitioned below the set boundary..

Default severity level: **information**, color code: green.

Typical Causes

A reduction in the number of messages.

Actions

None.

Device Low Disk Space

Indicates the device has low disk space.

Default severity level: **severe**, color code: orange.

Typical Causes

The cause of low disk space depends on the device, for example firewalls can generate large log files.

Actions

Use the managed host function to view current and historic levels of disk space.

Device Low Disk Space Cleared

Indicates the device is no longer suffering from low disk space.

Default severity level: **information**, color code: green.

Typical Causes

Reduced usage.

Actions

None.

Device Name Resolution Failure

Indicates Entuity (eyepoller) could reach the device using its IP address but not resolve its device host name.

Default severity level: **minor**, color code: yellow.

Typical Causes

A corruption or incorrect entry in the hosts file. An incorrect configuration of the Domain Name System server.

Actions

Investigate domain name resolution, the exact steps depend upon your operating system and domain name system configuration.

Device Name Resolution Failure Cleared

Indicates Entuity can resolve the device hostname.

Default severity level: **information**, color code: green.

Typical Causes

Correction of previous DNS problem.

Actions

None.

Device Port(s) Utilization Accuracy Lost

eyepoller counter wrap margin allows Entuity to identify devices for which it may miss counter wraps. This event indicates that the traffic rate is being polled from 32 bit counters and that the combination of the poll rate and linespeed make the resulting measurement susceptible to inaccuracy and the polled data is therefore discarded.

Default severity level: **major**, color code: amber.

Typical Causes

This event may be triggered if poll operations take longer, for example as a result of SNMP timeouts. Otherwise this event may suggest that the polling load is beyond Entuity's capacity, in which case the problem is with Entuity, not with the network.

Actions

Check the device for polling problems, check the Entuity server load.

Device Port(s) Utilization Accuracy at Risk

eyepoller counter wrap margin allows Entuity to identify devices for which it may miss counter wraps. This event indicates that a device was in danger of missing a counter wrap for, is being safely polled.

Default severity level: **minor**, color code: yellow.

Typical Causes

This event may be triggered if poll operations take longer, for example as a result of SNMP timeouts. Otherwise this event may suggest that the polling load is beyond Entuity's capacity, in which case the problem is with Entuity, not with the network.

Actions

Check the device for polling problems, check the Entuity server load.

Device Port(s) Utilization Missed Due to Slow Response

This event indicates that a device has responded too slowly to Entuity polling and data has been lost.

Default severity level: **major**, color code: amber.

Typical Causes

A configuration change to Entuity may mean the device is polled more frequently. If the polling frequency has not changed and there has been no significant change to the device configuration or loading then SNMP traffic may be being lost either in the device or between the Entuity server and the device. This may be because the weakest link is now overloaded for some reason.

Actions

Monitor the polling of the device.

Device Reboot Detected

Indicates that a device has recently been rebooted or reset. Entuity monitors device system uptime by polling the device every ten minutes, gathering SysUpTime.

Default severity level: **severe**, color code: orange.

Typical Causes

Device configuration changes, hardware/software/firmware faults, lack of memory on the device, power failures.

Actions

Telnet to the device and check the system logs for an indication of what caused the device to reboot. Through Flex Reports you can generate device system uptime reports.

Device Sensor Non-Operational

Indicates a high temperature on the device, with the event details including the device's reported temperature.

Default severity level: **minor**, color code: yellow.

Typical Causes

Overworked device, fan failure, air conditioner failure in the room, air blockage to cooling vents.

Actions

Consult your device documentation on investigating the device cooling system.

Device Sensor Non-Operational Cleared

Indicates a device that was reporting a high temperature is now returning a value within accepted boundaries.

Default severity level: **information**, color code: green.

Typical Causes

Resolution of original problem.

Actions

None required.

Device Sensor Warning Value

Indicates a high temperature on the device, with the event details including the device's reported temperature.

Default severity level: **major**, color code: amber.

Typical Causes

Overworked device, fan failure, air conditioner failure in the room, air blockage to cooling vents.

Actions

Consult your device documentation on investigating the device cooling system.

Device Sensor Value Cleared

Indicates a device that was reporting a high temperature is now returning a value within accepted boundaries.

Default severity level: **information**, color code: green.

Typical Causes

Resolution of original problem.

Actions

None required.

Device Reachability Degraded

This event is not enabled by default. It is enabled from the ICMP Monitor Settings page (click **Administration > Inventory / Topology > ICMP Monitor**) by selecting the Enable Device Unreachable Events and Raise Device Reachability Degraded events checkboxes.

Default severity level: **severe**, color code: orange.

Typical Causes

Entuity identifies reachability of the device as degraded but Entuity does not consider it as the root cause of the degradation. Potentially reachability to the device is only degraded because of the behavior of the identified root cause, i.e. this may be a symptomatic event.

Actions

Through the device Advanced page you can check the history of the Device Status.

Device Unreachable

This event is not enabled by default. It is enabled from the ICMP Monitor Settings page (click **Administration > Inventory / Topology > ICMP Monitor**) by selecting the Enable Device Unreachable Events checkbox.

Default severity level: **critical**, color code: red.

Typical Causes

Entuity identifies the device as unavailable and also if it is the root cause of the outage. Potentially reachability to the device is only degraded because of the behavior of the identified root cause, i.e. this may be a symptomatic event.



The Network Outage event is only raised against devices that are the root cause of the outage, the Device Unreachable event is raised against any device Entuity identifies as unreachable.

Actions

Through the device Advanced page you can check history of the Device Status.

Device Unreachable Cleared

Entuity identifies the device as available and clears the original Device Unreachable or Device Reachability Degraded event.

Default severity level: **information**, color code: green.

Typical Causes

Resolution of the original problem.

Actions

None required.

Device Warm Reboot

Indicates that a device has just been rebooted or reset. This event is detected by the generation of an SNMP trap on the device.

Default severity level: **severe**, color code: orange.

Typical Causes

Device configuration changes, hardware/software/firmware faults, lack of memory on the device, power failures.

Actions

Telnet to the device and check the system logs for an indication of what caused the device to reboot.

EGP Neighbor Loss

Indicates that the device's peer relationship with an EGP (Extended Gateway Protocol) neighbor no longer exists. The SNMP trap includes the identity IP address of the peered router, which Entuity attempts to resolve to the host name.

Default severity level: **critical**, color code: red.

Typical Causes

Peer router has gone down.

Actions

Investigate the peer router.

EIGRP Peer Briefly Not Established

Indicates to administrators that virtual links between EIGRP speakers are now well established but bounced recently. Entuity identifies a recent bounce as the up time is lower than in the previous poll.

Default severity level: **critical**, color code: red.

Typical Causes

EIGRP keep-alives may be lost, so the local router terminates the connection and then successfully attempt to reestablish it. Other causes maybe an unstable remote router, traffic shaping limitations.

Actions

Check logs are activated on the device. Use the logs to investigate error messages.

EIGRP Peer Disappeared

Indicates a former adjacent peer has been removed from router's configuration. Administrator's should be aware of this change to be able to detect rogue configuration updates.

Default severity level: **critical**, color code: red.

Typical Causes

Removal of an adjacent router.

Actions

Investigate the cause of router disappearance.

EIGRP Peer Newly Discovered

Indicates Entuity's discovery of a new EIGRP peer.

Default severity level: **minor**, color code: yellow.

Typical Causes

Configuration of a new EIGRP peer.

Actions

None.

Entuity License Expired and This Entuity Server is No Longer Operational

Indicates the license on the central license server has expired. The central license server provides the credits for the remote Entuity license client to manage its network, this remote Entuity server also requires a locally installed valid license. The local license determines the modules and integrations enabled on that Entuity install.

Default severity level: **critical**, color code: red.

Typical Causes

The license installed on the central Entuity license server has expired.

Actions

Contact your Entuity representative for a new license.

Entuity License Not Updated by License Server and Will Expire

Indicates the Entuity license server cannot contact the remote Entuity server. The license server regularly contacts its remote clients to maintain and verify their license details. A remote server can only run for a limited time, by default seven days, without contact from its license server. This event is raised after a set period of non-contact, by default two days. These settings are configurable through `entuity.cfg`.

Default severity level: **minor**, color code: yellow.

Typical Causes

The Entuity central license server is down, a general network problem is preventing communication between the Entuity servers.

Actions

Check the status of the license server, for example has it been taken down for scheduled maintenance. Review other raised events, do they indicate a general networking issue.

Entuity License on Remote Server Could Not be Updated

Indicates the central license server cannot contact one of its remote Entuity servers. This event is raised after a set period of non-contact, by default two days. These settings are configurable through `entuity.cfg`.

Default severity level: **minor**, color code: yellow.

Typical Causes

The remote Entuity server is down, a general network problem is preventing communication between the Entuity servers.

Actions

Check the status of the remote Entuity server, for example has it been taken down for scheduled maintenance? Review other raised events, do they indicate a general networking issue.

Entuity License on Remote Server Expired

Indicates the license for a remote client is no longer verified. An Entuity server using a client license can only run for a limited time, by default seven days, without contact from its license server. This setting is configurable through `entuity.cfg`.

When running multiple Entuity servers and using centralized licensing the local license determines the modules and integrations enabled on that Entuity install. The license server provides the credits for the client server to manage its network.

Default severity level: **critical**, color code: red.

Typical Causes

The license server has not contacted its client for a minimum of seven days.

Actions

Check the status of the remote Entuity server, for example has it been taken down for scheduled maintenance? Review other raised events, do they indicate a general networking issue.

Entuity License on Remote Server Successfully Updated

Indicates the Entuity license server has restored contact to the remote client Entuity server. The license server regularly contacts its remote clients to maintain and verify their license details. A remote server can only run for a limited time, by default seven days, without contact from its license server. This setting is configurable through `entuity.cfg`.

Default severity level: **information**, color code: green.

Typical Causes

The central Entuity license server was down, for example for maintenance, but is now online.

Actions

No action required.

Entuity License Successfully Updated by License Server

Indicates the Entuity license server has reestablished contact with this Entuity server.

Default severity level: **minor**, color code: yellow.

Typical Causes

The remote Entuity license server was down, for example for maintenance, but is now online.

Actions

No action required.

Entuity Server Automated Shutdown

Event generated by Entuity warning it is shutting down. This is raised by `diskMonitor` and indicates Entuity is closing down to protect the database from possible corruption. This is a system wide event, appearing in all views.

Default severity level: **critical**, color code: red.

Typical Causes

Low disk space.

Actions

Check server for disk space, if the space appears sufficient you can amend the `diskMonitor` threshold settings to values more appropriate to your system.



`diskMonitor` is intended to protect the Entuity database from corrupting when the server runs out of disk space, configuring it inappropriately removes this safeguard.

Entuity Server Component Restarting After Failure

Indicates a non-critical Entuity component has failed. This is a system wide event, appearing in all views.

Default severity level: **severe**, color code: orange.

Typical Causes

A component of the Entuity server has failed, for example in Windows an Entuity service.

Actions

Use the *Impacted* and *Details* fields to identify the failed Entuity component. Entuity will attempt to restart the component, raising an Entuity Server Permanent Failure of Component event if it fails to restart the component. You can view more details through `systemcontrol.log` in `entuity_home\log`.

Entuity Server Critical Component Restarting After Failure

Indicates a critical Entuity component has failed and that Entuity is attempting to restart that component. This is a system wide event, appearing in all views. It persists in the logger pane for twenty-four hours or until the Entuity server is restarted, whichever is the earlier.

Default severity level: **severe**, color code: orange.

Typical Causes

A component key to Entuity server performance has failed.

Actions

Use the *Impacted* and *Details* fields to identify the failed Entuity component. Entuity will attempt to restart the component, raising an Entuity Server Permanent Failure of Component event if it fails to restart the component. You can view more details through `systemcontrol.log` in `entuity_home` log.

Entuity Server Database Backup Failure

Indicates the Entuity backup failed.

Default severity level: **critical**, color code: red.

Typical Causes

A component key to Entuity server performance has failed.

Actions

Use the *Impacted* and *Details* fields to identify the failed Entuity component. Entuity will attempt to restart the component, raising an Entuity Server Permanent Failure of Component event if it fails to restart the component. You can view more details through `systemcontrol.log` in `entuity_home` log.

Entuity Server Disk Space Alert

Indicates the Entuity server is running low on disk space, and details the remaining disk space in megabytes. It is generated by `diskMonitor`. This is a system wide event, appearing in all views.

Default severity level: **critical**, color code: red.

Typical Causes

Low disk space.

Actions

Check server for disk space, if the space appears sufficient you can amend the `diskMonitor` threshold settings to values more appropriate to your system.



`diskMonitor` is intended to protect the Entuity database from corrupting when the server runs out of disk space, configuring it inappropriately will remove this safeguard.

Entuity Server Explicit Shutdown Initiated

Indicates Entuity server has been instructed to shutdown, for example from the command line using `stopeye` or as a result of critical shortage of disc space. This is a system wide event, appearing in all views when the Entuity server restarts.

Default severity level: **severe**, color code: orange.

Typical Causes

Administrator has taken down the server.

Actions

When the Entuity server has shut itself down investigate available disk space on the server.

Entuity Server Internal Event

Event generated by Entuity, reporting on the status of an Entuity service.

Default severity level: **minor**, color code: yellow.

Typical Causes

License expiry, Entuity process failure.

Actions

Determined by event type.

Entuity Server License Alert

Indicates one or more of Entuity's licensable components is approaching or has reached either its limit of managed objects or expiry date. The event description details the licensable component(s) and the number of free credits. This is a system wide event, appearing in all views.

Default severity level: **critical**, color code: red.

Typical Causes

Addition of managed objects or approaching expiry date.

Actions

Either unmanage objects to free up license credits or contact your Entuity representative and purchase additional credits.

Entuity Server Permanent Component Failure

Indicates the Entuity server has attempted to restart the failed component, but has been unable to do so. The component remains down until manually restarted, if possible, or the Entuity server is restarted. This is a system wide event, appearing in all views.

Default severity level: **critical**, color code: red.

Typical Causes

Failure to restart a failed Entuity component.

Actions

Use the *Impacted* and *Details* fields to identify the failed Entuity component. You can view more details through `systemcontrol.log` in `entuity_home\log`.

Entuity Server Shutdown Forced By Critical Failure To Restart

Indicates a critical Entuity component has failed repeatedly preventing the Entuity server from performing normally. The Entuity server has then automatically shutdown. This is a system wide event, appearing in all views when the Entuity server restarts.

Default severity level: **critical**, color code: red.

Typical Causes

Indicates a critical Entuity component has failed repeatedly preventing the Entuity server from performing normally.

Actions

Investigate the Entuity log files, available from `entuity_home\log`, e.g. `systemcontrol.log`, `DsKernelStatic.log`.

Entuity Server Started

Indicates the Entuity server has successfully started. This is a system wide event, appearing in all views.

Default severity level: **information**, color code: green.

Typical Causes

Indicates the Entuity server has successfully started.

Actions

None.

Firewall Access Control Violations High

Indicates the NetContinuum firewall is identifying a high number of access control violations by a managed application. This may indicate an attack, or an inappropriate firewall configuration for a particular application. NetContinuum firewalls identify a series of access control type violations:

- Denied HTTP Requests
- Blocked DAP
- Blacklisted
- Blocked Methods

- Robots Denied
- Robots Allowed.

Entuity sums the total number of violations that occurred during the last polling period, by default Entuity polls NetContinuum firewalls every five minutes. When the total number of access control violations exceeds the set threshold, configurable but by default set to ten, Entuity raises this event.

Default severity level: **severe**, color code: orange.

Typical Causes

An application is being inappropriately used, this may be because users are either consciously or inadvertently attempting to use an application beyond the configured constraints.

Actions

Entuity includes to the event the source application and the breakdown of access control violations by type, from which you can identify the particular types, or types of violation, causing concern. After investigation you may determine an attack has occurred, or that, for example, the URL Access Control Lists (ACLs) require adjustment.

Firewall Access Control Violations High Cleared

Indicates that the high number of access control violations rate has returned to within acceptable boundaries.

Default severity level: **information**, color code: green.

Typical Causes

Reduced number of control violations.

Actions

None.

Firewall High Avail User Set Oper State Compliant

The High Availability module status on the device and the *User Set Oper State* set in Entuity were different but are now the same.

Default severity level: **information**, color code: green.

Typical Causes

User Set Oper State may have been amended to match the state on the device, or the device state may have transitioned to be the same as *User Set Oper State*.

Actions

None.

Firewall High Avail User Set Oper State Non Compliant

The High Availability module status on the device and the *User Set Oper State* set in Entuity are different.

Default severity level: **severe**, color code: orange.

Typical Causes

User Set Oper State may have been amended to a state different to that on the device. More significantly, the device state may have transitioned to a different state to that of *User Set Oper State*.

Actions

In Event Viewer the event Details column displays both the *User Set Oper State* and the polled device state. The type of disparity determines your action where the change in High Availability module was:

- Expected and permanent, amend the module's *User Set Oper State*.
- Unexpected, investigate the cause of the change in module state. It may indicate a serious problem that could impact the performance of the firewall cluster.

Firewall High Current Connections

Indicates the number of current connections is greater than the set threshold, by default 1000.

Default severity level: **severe**, color code: orange.

Typical Causes

Highest number of current connections is greater than the set threshold when the firewall is polled.

Actions

Investigate the connection history of the device.

Firewall High Current Connections Cleared

Indicates the number of current connections was greater than the set threshold, by default 1000, but is now below that boundary.

Default severity level: **information**, color code: green.

Typical Causes

A reduction in the number of current connections.

Actions

None.

Firewall Overflow and Intrusion Violations High

Indicates the NetContinuum firewall is identifying a high number of overflow and intrusion violations. This may indicate an attack, or an inappropriate firewall configuration for a particular application. NetContinuum firewalls identify a series of overflow and intrusion type violations:

- Keyword Intrusions
- Query Length Intrusions
- Cookie Overflow Intrusions
- Header Count Intrusions
- Content Overflow Intrusions
- Parameter Length Overflows
- Empty Valued.

Entuity sums the total number of violations that occurred during the last polling period, by default Entuity polls NetContinuum firewalls every five minutes. When the total number of overflow and intrusion violations exceeds the set threshold, configurable but by default set to ten, Entuity raises this event.

Default severity level: **severe**, color code: orange.

Typical Causes

Forms tampering can modify the information sent from a particular field on a form, for example adding extra, malicious instructions through a buffer overflow.

Actions

Entuity includes to the event the source application and the breakdown of overflow and intrusion violations by type, from which you can identify the particular types, or types of violation, causing concern.

Firewall Overflow and Intrusion Violations High Cleared

Indicates that the high number of overflow and intrusion violations has returned to within acceptable boundaries.

Default severity level: **information**, color code: green.

Typical Causes

Reduced number of overflow and intrusion violations.

Actions

None.

Firewall URL Alerts High

Indicates the NetContinuum firewall is identifying a high number of URL alerts against a particular application. NetContinuum firewalls identify these types of violations:

- URL Encoding Errors
- Slash Dot URLs Blocked
- Tilde in URL Blocked
- Character Set Encoding Errors
- Bad Certificates.

Entuity sums the total number of alerts against the application that occurred during the last polling period, by default Entuity polls NetContinuum firewalls every five minutes. When the total number of URL alerts exceeds the set threshold, configurable but by default set to five hundred, Entuity raises this event.

Default severity level: **severe**, color code: orange.

Typical Causes

An attack can use different ploys based around how URLs are handled. For example, hiding an attack within a different character set. The NetContinuum Controller can identify character set encoding schemes and identify attacks hidden within them.

Actions

Entuity includes to the event the source application and the breakdown of URL alerts by type, from which you can identify the particular types, or types of URL violation, causing concern.

Firewall URL Alerts High Cleared

Indicates that the number of URL alerts has returned to within acceptable boundaries.

Default severity level: **information**, color code: green.

Typical Causes

Reduced number of URL alerts against the application.

Actions

None.

FR DLCI High BECN

Indicates the frame relay is encountering congestion, specifically the available bandwidth at the time of transmission is not as great as can be supported by the sending terminal.

Default severity level: **major**, color code: amber.

Typical Causes

Inadequate network infrastructure, heavy network traffic, high levels of line noise, or portions of the system going down.

Actions

Identifying and resolving these issues can improve overall network performance, especially when the system is called upon to carry a large volume of traffic.

FR DLCI High BECN Cleared

Indicates that the frame relay encountering congestion has returned to within acceptable boundaries.

Default severity level: **information**, color code: green.

Typical Causes

Reduced usage.

Actions

None.

FR DLCI High DE

Indicates that the Committed Information Rate (CIR) has been exceeded on inbound traffic on this PVC.

Default severity level: **major**, color code: amber.

Typical Causes

When the CIR is exceeded, traffic gets marked DE by the frame relay switch, if congestion is then detected these packets are dropped.

Actions

Use the PVC Utilization report to investigate further.

FR DLCI High DE Cleared

Indicates that the Committed Information Rate (CIR) has returned to within acceptable boundaries on inbound traffic on this PVC.

Default severity level: **information**, color code: green.

Typical Causes

Reduced usage.

Actions

None.

FR DLCI High FECN

Indicates the WAN is encountering congestion forward of the packet, i.e. the available bandwidth at the time of transmission is not as great as can be supported by the receiving terminal.

Default severity level: **major**, color code: amber.

Typical Causes

Inadequate network infrastructure, heavy network traffic, high levels of line noise, or portions of the system going down.

Actions

Identify and resolve these issues can improve overall network performance, especially when the system is called upon to carry a large volume of traffic.

FR DLCI High FECN Cleared

Indicates that the Committed Information Rate (CIR) has returned to within acceptable boundaries on outbound traffic on this PVC.

Default severity level: **information**, color code: green.

Typical Causes

Reduced usage.

Actions

None.

FR DLCI High Inbound Utilization

Indicates inbound utilization of the port is high and could impact performance.

Default severity level: **major**, color code: amber.

Typical Causes

PVC utilization is higher than PVC utilization threshold for the port due to increased traffic.

Actions

Generate PVC utilization reports to monitor situation.

FR DLCI High Inbound Utilization Cleared

Indicates PVC utilization is now below the high threshold value.

Default severity level: **information**, color code: green.

Typical Causes

Reduced transmission.

Actions

None.

FR DLCI High Outbound Utilization

Indicates outbound utilization of the port is high and could impact performance.

Default severity level: **major**, color code: amber.

Typical Causes

PVC utilization higher than PVC utilization threshold for the port due to increased traffic.

Actions

Generate PVC utilization reports to monitor situation.

FR DLCI High Outbound Utilization Cleared

Indicates PVC utilization is now below the high threshold value.

Default severity level: **information**, color code: green.

Typical Causes

Reduced transmission.

Actions

None.

FR DLCI Link Down

Indicates PVC is unavailable.

Default severity level: **severe**, color code: orange.

Typical Causes

Problems with connection to router-CSU/DSU devices, PVC congestion indicated by CIR exceeded.

Actions

Investigate whether the problem occurs on the public or private section of the network, run PVC reports.

FR DLCI Link UP

Indicates PVC is available.

Default severity level: **information**, color code: green.

Typical Causes

A PVC that was unavailable is now available.

Actions

None.

HSRP Port Group Activated

Indicates the HSRP port is active.

Default severity level: **major**, color code: amber.

Typical Causes

When preemption is enabled the newly activated router has a higher priority than the previously active router. The previously active router has become unavailable, this router was the standby router and has now activated.

Actions

None.

HSRP Port Group Deactivated

Indicates the HSRP port group has transitioned from an active to a deactivated state.

Default severity level: **major**, color code: amber.

Typical Causes

Indicates the HSRP port group has transitioned from an active state to one of n/a, Initial, Learn, Listen, Speak, or Standby. You can view the current state through the event details column.

Actions

Investigate the cause of the transition of the HSRP port group to deactivated when preemption is not enabled. When Entuity monitors the router it raises events indicating the cause of failure.

IP SLA Creation Failure

Indicates the creation of an IP SLA operation has failed on the source device.

Default severity level: **critical**, color code: red.

Typical Causes

The create command does not include the correct SNMP write community string. Alternatively, there may be access restrictions to the device.

Actions

- 1) Check the correct SNMP write community string is set on the device.

- 2) Check access is not restricted to the device, including any firewall allows through the appropriate commands (i.e. snmpSet permission).

IP SLA Creation Failure Cleared

Indicates the operation was successfully created, but does not indicate that it is collecting data.

Default severity level: **information**, color code: green.

Typical Causes

Raised the first time the operation is successfully created on the device.

Actions

None.

IP SLA High ICPIF

ICPIF attempts to quantify the key impairments to voice quality that are encountered in the network. A high ICPIF value indicates high impairment.

Default severity level: **critical**, color code red.

Typical Causes

Packet loss due to equipment impairment and latency due to increased traffic.

Actions

Run a Flex Report to investigate further.

IP SLA High ICPIF Cleared

Indicates a previous High ICPIF alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

VoIP quality of service, as measured by ICPIF, has returned to acceptable levels.

Actions

No action required.

IP SLA Low MOS

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.

Default severity level: **critical**, color code red.

Typical Causes

Packet loss due to equipment impairment and latency due to increased traffic.

Actions

Run a Flex Report to investigate further.

IP SLA Low MOS Cleared

Indicates a previous Low MOS alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

VoIP quality of service, as measured by MOS, has returned to acceptable levels.

Actions

No action required.

IP SLA Test Failed

Indicates the operation was successfully created but it failed to connect to the target device.

Default severity level: **major**, color code: amber.

Typical Causes

There may be access restrictions to the device or a failure on the network.

Actions

- 1) Check the target device is available.
- 2) When communicating through a firewall check the IP SLA source port is set correctly.
- 3) Check the target device's destination port is IP SLA responsive. This is achieved either by having the IP SLA responder enabled or having a process listening on that port. When using IP SLA responder's control packets must also be used (and also allowed through the firewall).

IP SLA Test High Latency

Indicates the operation is reporting latency between the source and target device above the threshold settings for the operation.

Default severity level: **critical**, color code red.

Typical Causes

Packet loss due to equipment impairment and latency due to increased traffic.

Actions

- 1) Check the performance of the target device.
- 2) Review latency over an extended period, e.g. run the IP SLA Details report.

IP SLA Test High Latency Cleared

Indicates that the operation is reporting latency between the source and target device that has returned to below its threshold settings, having previously been above.

Default severity level: **information**, color code: green.

Typical Causes

The cause of high latency on the network has been resolved, for example a high latency may only be reported at peak times.

Actions

None.

IP SLA Test Succeeded

Indicates the operation is successfully collecting data.

Default severity level: **information**, color code: green.

Typical Causes

Raised the first time the operation collects data from a device, or after a failure in operation collection has been resolved and data is being collected again.

Actions

None.

IS-IS Peer Disappeared

Indicates a former adjacent peer has been removed from router's configuration. Administrator's should be aware of this change to be able to detect rogue configuration updates.

Default severity level: **critical**, color code: red.

Typical Causes

Removal of an adjacent router.

Actions

Investigate the cause of router disappearance.

IS-IS Peer Established

Indicates to administrators that virtual links between IS-IS peers are well established. the state has just transitioned to **Full**.

Default severity level: **minor**, color code: yellow.

Typical Causes

OSPF peering established.

Actions

None.

IS-IS Peer Newly Discovered

Indicates Entuity's discovery of a new IS-IS peer.

Default severity level: **minor**, color code: yellow.

Typical Causes

Configuration of a new IS-IS peer.

Actions

None.

IS-IS Peer Not Established

Indicates to administrators that a former adjacent peer is no longer in reach. The state has just transitioned out of the **Full** state.

Default severity level: **critical**, color code: red.

Typical Causes

Problems with IP reachability or incorrect IS-IS configuration.

Actions

Use the ping and show route commands to verify network connectivity to the IS-IS peer. You can use the **show log messages** command to look for errors relating to the peer.

LAP Antenna Host Count High

For each WAP antenna you can set a maximum number of hosts that they can handle, a number higher than the antenna can efficiently handle.

Default severity level: **minor**, color code: yellow.

Typical Causes

Changes in wireless usage have occurred since the network was designed.

Actions

You can check the Interface Advanced tab and review the hourly and daily mean and maximum attached host values. When the historic record indicates a rising usage trend you may want to extend the capabilities of your wireless network.

LAP Antenna Host Count High Cleared

Raised when the number of hosts attached to the WAP antenna has returned to an acceptable level.

Default severity level: **information**, color code: green.

Typical Causes

The number of hosts attached to the antenna has returned to an acceptable level.

Actions

No action required.

LAP Antenna Host Count Low

The combined count of hosts that are wirelessly associated with all of the antennas on a WAP has fallen below the set threshold.

Default severity level: **minor**, color code: yellow.

Typical Causes

Changes in wireless usage have occurred since the network was designed.

Actions

You can check the Antenna Advanced tab and review the hourly and daily mean and maximum attached host values. When the historic record indicates a falling usage trend you may want to adjust the capabilities of your wireless network.

LAP Antenna Host Count Low Cleared

The clearing correlation event for WAP Antenna Host Count Low event.

Default severity level: **information**, color code: green.

Typical Causes

The number of hosts attached to the antenna has returned to an acceptable level.

Actions

No action required.

Load Balancer High Connection Limit Pkt Drop Rate

The connection requests rejected because they exceeded the connection drop rate for a virtual server (IP address:Port).

Default severity level: **critical**, color code: red.

Typical Causes

Availability of load balancer servers is insufficient to meet demand, inefficient assignment of clients to servers.

Actions

Investigate the client connection history.

Load Balancer High Connection Limit Pkt Drop Rate Cleared

The connection requests rejected because they exceeded the connection limit for a virtual server (IP address:Port) is now within the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

Reduced demand on the load balancer hardware accelerator.

Actions

No action required.

Load Balancer High Current Sessions

Indicates the number of current sessions is equal to, or greater than the set current sessions threshold, which is by default 10000000.

Typical Causes

- 1) A change in the usage of the network placing an unexpected demand on your load balancer setup.
- 2) Persistent sessions not releasing resources.
- 3) A misconfiguration of your load balancer setup, or a failure.
- 4) Entuity settings inappropriate to load balancer pool services.

Actions

Investigate the history of session assignment, a persistent problem may indicate a requirement to reconfigure your load balancer setup.

Load Balancer High Current Sessions Cleared

Indicates the number of current sessions is less than the set current sessions threshold, which is by default 10000000.

Default severity level: **information**, color code: green.

Typical Causes

A return to the expected network load.

Actions

No action required.

Load Balancer High Error Count

The total session errors are greater than the set threshold, by default 10000000.

Default severity level: **critical**, color code: red.

Typical Causes

Availability of load balancer servers is insufficient to meet demand, inefficient assignment of clients to servers.

Actions

Investigate load balancer resourcing and configuration.

Load Balancer High Error Count Cleared

The total inbound and outbound packet errors for the system is within the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

Availability of load balancer servers is insufficient to meet demand, inefficient assignment of clients to servers.

Actions

Investigate load balancer resourcing and configuration.

Load Balancer High Inbound Error Rate

The error rate for incoming packets for the load balancer is higher than the set threshold, by default 6250000 packets per second.

Default severity level: **critical**, color code: red.

Typical Causes

Availability of load balancer servers is insufficient to meet demand, inefficient assignment of clients to servers.

Actions

Investigate load balancer resourcing and configuration.

Load Balancer High Inbound Error Rate Cleared

The error rate for incoming packets for the load balancer is within than the set threshold, by default 6250000 packets per second.

Default severity level: **information**, color code: green.

Typical Causes

Reduced demand on the load balancer hardware accelerator.

Actions

No action required.

Load Balancer High License Denied Pkt Rate

Packets were dropped due to exceeding licensing limitations, by default 500 packets per second.

Default severity level: **critical**, color code: red.

Typical Causes

Availability of load balancer servers is insufficient to meet demand, inefficient assignment of clients to servers.

Actions

Investigate load balancer resourcing and configuration.

Load Balancer High License Denied Pkt Rate Cleared

Rate of dropped packets due to exceeding licensing limitations no longer exceeds the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

Reduced traffic, availability of greater load balancer resource.

Actions

No action required.

Load Balancer High Maximum Sessions

Indicates the number of maximum sessions is equal to, or greater than the set maximum sessions threshold, which is by default 10000000.

Typical Causes

- 1) A change in the usage of the network placing an unexpected demand on your load balancer setup.
- 2) Persistent sessions not releasing resources.
- 3) A misconfiguration of your load balancer setup, or a failure.
- 4) Entuity settings inappropriate to load balancer pool services.

Actions

Investigate the history of session assignment, a persistent problem may indicate a requirement to reconfigure your load balancer setup.

Load Balancer High Maximum Sessions Cleared

Indicates the number of maximum sessions is less than the set maximum sessions threshold, which is by default 10000000.

Default severity level: **information**, color code: green.

Typical Causes

A return to the expected network load.

Actions

No action required.

Load Balancer High Memory Error Pkt Rate

Indicates connection errors were the result of insufficient available memory.

Default severity level: **critical**, color code: red.

Typical Causes

Availability of load balancer servers is insufficient to meet demand, inefficient assignment of clients to servers.

Actions

Investigate load balancer resourcing and configuration.

Load Balancer High Memory Error Pkt Rate Cleared

Indicates connection errors that were the result of insufficient available memory are resolved.

Default severity level: **information**, color code: green.

Typical Causes

Reduced traffic, availability of greater load balancer resource.

Actions

No action required.

Load Balancer High No Handler Denied Pkt Rate

Indicates that the incoming packets that could not be processed by a virtual server, NAT or SNAT is at a rate greater than the set threshold.

Default severity level: **critical**, color code: red.

Typical Causes

Availability of load balancer servers is insufficient to meet demand, inefficient assignment of clients to servers.

Actions

No action required.

Load Balancer High No Handler Denied Pkt Rate Cleared

Indicates that the incoming packets that could not be processed by a virtual server, NAT or SNAT is now at a rate within the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

Reduced traffic, availability of greater load balancer resource.

Actions

No action required.

Load Balancer High Non Syn Denied Pkt Rate

Indicates that the packets that are not connection requests and are destined for a virtual server that has no connection for the client address are at a rate greater than the set threshold.

Default severity level: **critical**, color code: red.

Typical Causes

The packets that are not connection requests and are destined for a virtual server that has no connection for the client address.

Actions

Investigate client's server address list.

Load Balancer High Non Syn Denied Pkt Rate Cleared

Indicates that the packets that are not connection requests and are destined for a virtual server that has no connection for the client address are now at a rate within than the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

Client now has access to the virtual server.

Actions

No action required.

Load Balancer High Outbound Error Rate

The total outgoing packet errors for the system is greater than the set threshold.

Default severity level: **critical**, color code: red.

Typical Causes

Availability of load balancer servers is insufficient to meet demand, inefficient assignment of clients to servers.

Actions

Investigate load balancer resourcing and configuration.

Load Balancer High Outbound Error Rate Cleared

The total outgoing packet errors for the system is now within the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

Reduced traffic, availability of greater load balancer resource.

Actions

No action required.

Load Balancer High Packet Drop Rate

The total number of dropped packets is higher than the set threshold.

Default severity level: **critical**, color code: red.

Typical Causes

Availability of load balancer servers is insufficient to meet demand, inefficient assignment of clients to servers.

Actions

Investigate load balancer resourcing and configuration.

Load Balancer High Packet Drop Rate Cleared

The total number of dropped packets is within the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

Reduced traffic, availability of greater load balancer resource.

Actions

No action required.

Load Balancer High SLB SP Current Sessions

The number of sessions the Server Load Balancing (SLB) service processor is currently handling is higher than the set threshold, by default 75% of the maximum allowed.

Typical Causes

- 1) A change in the usage of the network placing an unexpected demand on your load balancer setup.
- 2) Persistent sessions not releasing resources.
- 3) A misconfiguration of your load balancer setup, or a failure.
- 4) Entuity settings inappropriate to the SLB setup, for example too low a threshold.

Actions

Investigate history of service processor utilization.

Load Balancer High SLB SP Current Sessions Cleared

The number of sessions the Server Load Balancing (SLB) service processor is currently handling is within the set threshold, by default 75% of the maximum allowed.

Default severity level: **information**, color code: green.

Typical Causes

A reduction in the load on the load balancer.

Actions

No action required.

Load Balancer Pool Critical Member Availability

The number of members available to the pool is reduced to a critical level.

Default severity level: **critical**, color code: red.

Typical Causes

Number of available members is less than the set threshold when the device is polled.

Actions

Investigate the history of member usage for the pool.

Load Balancer Pool Critical Member Availability Cleared

The number of members available to the pool has transitioned to a value within the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

A reduction in the resources used for the load balancer pool.

Actions

None.

Load Balancer Pool Critical Services Availability

Indicates the number of available services is below the set critical services thresholds, which is by default 0.

Default severity level: **critical**, color code: red.

Typical Causes

- 1) A change in the usage of the network placing an unexpected demand on your load balancer setup.
- 2) A misconfiguration of your load balancer setup, or a failure.
- 3) Entuity settings inappropriate to load balancer pool services.

Actions

Investigate the history of service availability a persistent problem may indicate a requirement to reconfigure your load balancer setup.

Load Balancer Pool Critical Services Availability Cleared

Indicates the number of available services has transitioned above the set critical services thresholds, which is by default 0.

Default severity level: **information**, color code: green.

Typical Causes

A reduction in the services used for the load balancer pool.

Actions

No action required.

Load Balancer Pool Low Member Availability

The number of members available to the pool is reduced to a low level.

Default severity level: **major**, color code: amber.

Typical Causes

Number of available members is less than the set threshold when the device is polled.

Actions

None.

Load Balancer Pool Low Member Availability Cleared

The number of members available to the pool has transitioned to a value within the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

A reduction in the resources used for the load balancer pool.

Actions

None.

Load Balancer Pool Low Services Availability

Indicates the number of available services is equal to or below the set services thresholds, which is by default 2.

Default severity level: **severe**, color code: orange.

Typical Causes

- 1) A change in the usage of the network placing an unexpected demand on your load balancer setup.
- 2) A misconfiguration of your load balancer setup, or a failure.
- 3) Entuity settings inappropriate to load balancer pool services.

Actions

Investigate the history of service availability a persistent problem may indicate a requirement to reconfigure your load balancer setup.

Load Balancer Pool Low Services Availability Cleared

Indicates the number of available services has transitioned above the set services thresholds, which is by default 2.

Default severity level: **information**, color code: green.

Typical Causes

A reduction in the services used for the load balancer pool.

Actions

No action required.

MAC Address High Port Count

This is a threshold-based event and is disabled by default. It can be enabled through Threshold Settings by setting the number of MAC addresses you consider is a high MAC address count.

Entuity does not raise this event against trunking ports.

Typical Causes

`macman` compares the number of MAC addresses discovered on a port against the Entuity threshold set for that port, by default set to three.

Actions

Investigate why the device is handling so many MAC addresses, and monitor the impact on its performance.

If you judge the:

- Threshold setting is too low you can amend it for the individual port, for all of the ports on the current port's device or as a global change for all of the port's managed by the server.
- Event is not appropriate for the port you can disable it for the individual port, for all of the ports on the current port's device or as a global change for all of the port's managed by the server.

MAC Address High Port Count Cleared

Indicates a previous MAC Address High Port Count alarm associated with this port has been cleared.

Typical Causes

Number of MAC addresses associated with the port is now within the set thresholds.

Actions

None.

MAC Address New

Entuity discovers one or more new mac addresses on a port, raising one event for all of the new MAC addresses on the port. Entuity considers a new MAC address as one not listed in the retained history of MAC addresses for the current port. By default Entuity retains the last fifty MAC addresses discovered on a port, although this is configurable through *machistorylimit* in *entuity.cfg*.

Entuity does not raise events for:

- Newly discovered ports within a defined inhibit time, which prevents Entuity from raising a torrent of events caused by Entuity discovering new devices. By default this inhibit time is twenty-four hours, but it is configurable through the MAC Addresses threshold tab.



A twenty-four hour inhibit period allows `provost` scheduled `macman` to run and discover MAC addresses, providing a base against which new and change events can be recognized. When `macman` is run through `macScheduler` then that baseline can be discovered earlier and Entuity can ignore the inhibit time.

- The very first mac address(es) seen on a port, to avoid a blizzard of events when Entuity manages new devices
- Any mac addresses that recur on a port.

Entuity checks for changes in port state every hour, and events are raised within that context.



When the conditions of the new MAC address match the criteria of the MAC Address Port Change event, Entuity raises both events against this port.

This is a threshold-based event and is disabled by default.

Default severity level: **major**, color code: amber.

Typical Causes

Entuity discovers a new MAC address on a managed port. For example when a host, such as a PC, is plugged into an access layer switch that Entuity manages, Entuity raises a MAC Address New event.

Actions

When this event is not accompanied by a MAC Port Address Port Change event it is a warning to you that a new host has connected to your network. Although the introduction of a new host might be a benign event it requires further investigation as it may:

- Indicate a personally owned device has connected to the network, which may be compromised, e.g. insufficient anti-virus protection which could allow access to malicious worms, adware, viruses and other infectious material.
- Be the signature of the introduction of an unauthorized Wireless Access Point which might not have its security configuration enabled (they are unsecured by default) and would therefore invite intrusion to an otherwise secure network.

MAC Address Port Change

When Entuity discovers a MAC address that is new to the current port, but which it has a record of occurring on one or more other ports, it raises a MAC Address Port Change event.

Entuity considers a change MAC address as one not listed in the retained history of ports for that MAC address, but other ports are listed in this retained history. By default Entuity retains the last fifty ports associated with a MAC address, although this is configurable through *machistorylimit* in *entuity.cfg*.

Entuity raises the event against the first new port (in terms of lexicographic listing), specifying the mac address, together with the ports it was last seen on and the ports it is now seen on. Entuity checks for changes in port state every hour, and events are raised within that context.



When the conditions of the port change MAC address match the criteria of the MAC Address New event Entuity also raises a MAC Address New event against this port.

This is a threshold-based event and is disabled by default.

Typical Causes

A MAC address `macman` previously discovered on one port, or ports, it now discovers on an additional port. For example when a host, such as a PC, is unplugged from one access layer switch that Entuity manages and plugged into another, Entuity raises a MAC Address Port Change event.

Actions

May indicate a security concern that requires further investigation.

Memory Low

Indicates the managed memory object is running low on available memory.

Default severity level: **severe**, color code: orange.

Typical Causes

Low memory may be caused through a combination of factors; as a memory leak that has consumed a large amount of memory, a network instability pushes the free memory to zero and the device does not have enough memory to begin with but the problem is discovered only during a rare network event.

Actions

Use the managed host function to view current and historic levels of memory.

Memory Low Cleared

Indicates the managed object is no longer suffering from low memory.

Default severity level: **information**, color code: green.

Typical Causes

Reduced usage.

Actions

None.

Missing Events

These are generated when Entuity detects an event has occurred but cannot display it.

Default severity level: n/a Color code: white.

Typical Causes

This indicates Entuity has raised an event for which it does not have record for that type in its database. This may happen, for example, when creating an event through the Open Trap Receiver and the event being raised before Event Viewer has updated its tables to recognize the event. After the next refresh the event would be properly recognized, i.e. the event has not been received by the client.

Actions

None, this should be a temporary issue resolved when Entuity's tables and event caches are synchronized.

Module Disappeared

Indicates a module (card) is no longer on a device.

Default severity level: **critical**, color code: red.

Typical Causes

Removal of a module by an administrator. Critical failure of a module on the device.

Actions

When the module has failed the system administrator should investigate. You can Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

Module Discovered

Indicates discovery of a module (card) for a device Entuity already manages.

Default severity level: **minor**, color code: yellow.

Typical Causes

Addition of a module on the device. It may also be raised when a device is added to Entuity.

Actions

None.

Module Down

Indicates a module (card) fault for a device.

Default severity level: **critical**, color code: red.

Typical Causes

Faulty module card hardware or firmware.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

Module Major Fault

Indicates that a device has a major module (line card) hardware or firmware problem

Default severity level: **critical**, color code: red.

Typical Causes

Faulty card hardware or firmware.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

Module Minor Fault

Indicates that a device has a minor module (line card) hardware or firmware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty card hardware or firmware.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

Module Status OK

Indicates that a module (card) fault for a device has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Faulty module (card) has been swapped out.

Actions

None.

Module Status Unknown

Indicates that Entuity cannot determine the status of the device.

Default severity level: **major**, color code: amber.

Typical Causes

Faulty card hardware or firmware.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

MPLS LDP Entity Errors

The LDP entity represents a label space that is targeted for distribution to an LDP peer.

Default severity level: **critical**, color code: red.

Typical Causes

Entity errors may be:

- Bad LDP Identifier Errors
- Bad PDU Length Errors
- Bad Message Length Errors
- Bad Message Length Errors
- Bad TLV Length Errors
- Malformed TLV Value Errors
- Keep Alive Timer Expiry Errors.

Actions

Investigate the entity configuration. The event includes the LDP entity device and associated LDP peer.

MPLS LDP Entity Errors Cleared

The LDP entity no longer has associated errors.

Default severity level: **information**, color code: green.

Typical Causes

A corrected configuration, improvement in network performance.

Actions

None.

MPLS LDP Entity Non-operational

Indicates the LDP session state has transitioned from operational to a non-operational state.

Default severity level: **critical**, color code: red.

Typical Causes

Indicates the LDP session state has transitioned from operational.

Actions

The event includes the LDP entity device and associated LDP peer. Investigate the entity configuration; the event includes the new state of the session:

- Unknown
- Non existent
- Initialized
- Open Receive
- Open Sent.

MPLS LDP Entity Operational

Indicates the LDP session state has transitioned from a non-operational to an operational state.

Default severity level: **information**, color code: green.

Typical Causes

The session is operational as the LSR has received acceptable initialization and keep alive messages.

Actions

None.

MPLS LDP Entity Rejected Sessions

LSR has received a session initialization message but has rejected the session.

Default severity level: **critical**, color code: red.

Typical Causes

One or more of the session parameters, for example LDP protocol version, label distribution method, timer values are not acceptable. The LSR responds by sending a Session Rejected/Parameters Error Notification message and closing the TCP connection.

Actions

Investigate the configuration of the LSR.

MPLS LDP Entity Rejected Sessions Cleared

The LDP entity has now accepted the session.

Default severity level: **information**, color code: green.

Typical Causes

The LDP entity has now accepted the session.

Actions

None.

MPLS LDP Entity Shutdown Notifications Received

The LSR has received a shutdown notification message from the peered LSR.

Default severity level: **critical**, color code: red.

Typical Causes

When the last Hello adjacency for a LDP session is deleted, the connected LSR terminates the LDP session. The peer may close the session when it concludes that the transport connection is bad or that the peer has failed, and it terminates the LDP session by closing the transport connection.

Actions

Investigate the network connection, the status of the LSR.

MPLS LDP Entity Shutdown Notifications Received Cleared

The integrity of the LDP session has been reestablished.

Default severity level: **information**, color code: green.

Typical Causes

The peered LSR prematurely sent a session terminated notification message, which was subsequently followed by a Want To Reestablish session message.

Actions

None.

MPLS LDP Entity Shutdown Notifications Sent

When the last Hello adjacency for a LDP session is deleted, the LSR terminates the LDP session.

Default severity level: **critical**, color code: red.

Typical Causes

The LSR may close the session when it concludes that the transport connection is bad or that the peer has failed, and it terminates the LDP session by closing the transport connection.

Actions

Investigate the network connection, the status of the LSR.

MPLS LDP Entity Shutdown Notifications Sent Cleared

The integrity of the LDP session has been reestablished.

Default severity level: **information**, color code: green.

Typical Causes

The LSR prematurely sent a session terminated notification message, which was subsequently followed by a Want To Reestablish session message.

Actions

None.

MPLS LDP Peer Disappeared

The LSR peer has disappeared, an Entity Shutdown Notification message may already have been raised.

Default severity level: **critical**, color code: red.

Typical Causes

The session has been shutdown and so the peer has disappeared. The administrator may have reconfigured\removed the LSR. Alternatively the LSR may have encountered problems.

Actions

When the disappearance is unexpected Entuity may have raised additional events that indicate the cause of the disappearance.

MPLS LDP Peer Newly Discovered

A newly discovered LDP peer indicates the establishment of a new LDP session.

Default severity level: **information**, color code: green.

Typical Causes

Administrator has added a new LSR to your network.

Actions

Check that the newly discovered peer is an expected LSR, an unexpected LSR may indicate a security failure.

MPLS LDP Peer Non-operational

Indicates the LDP session state has transitioned from an operational to a non-operational state.

Default severity level: **critical**, color code: red.

Typical Causes

The event associated LDP peer has a state other than operational:

- Unknown
- Non existent
- Initialized
- Open Receive
- Open Sent.

Actions

The event includes the non-operational peer's device name and advertised IP address that you can use to investigate the state of the peer.

MPLS LDP Peer Operational

Indicates the LDP peer state has transitioned from a non-operational to an operational state.

Default severity level: **information**, color code: green.

Typical Causes

Peer has returned to an operational state, for example after the device has been rebooted.

Actions

None.

MPLS LDP Peer TLV Errors

The peer has received a packet of the correct type but of unknown content.

Default severity level: **critical**, color code: red.

Typical Causes

The content may have been corrupted during transmission across the network.

Actions

Check the sending LSR configuration.

MPLS LDP Peer TLV Errors Cleared

A previous message from the peered LSR had corrupt content, the subsequent message was correctly formed.

Default severity level: **information**, color code: green.

Typical Causes

The state that caused corrupt content, for example transport problems, has been resolved.

Actions

None.

MPLS LDP Peer Unknown Message Types

The LDP peer received a message of an unknown type.

Default severity level: **critical**, color code: red.

Typical Causes

LSR's support a defined set of message types, a packet that includes a message type not configured to the LSR cannot be processed.

Actions

Check the supports message types on the LSRs.

MPLS LDP Peer Unknown Message Types Cleared

A previous message from the peered LSR was of a type this LSR did not recognize.

Default severity level: **information**, color code: green.

Typical Causes

The most recent packet from the peer is of a supported message type.

Actions

None.

MPLS LSR Interface High Discard Rate (Lookup Failure)

Indicates the number of labeled packets that have been received on this interface and were discarded because there were no matching entries found for them in mplsInSegmentTable.

Default severity level: **severe**, color code: orange.

Typical Causes

There were no forwarding rules for these received packets.

Actions

Check the configuration of your forwarding tables.

MPLS LSR Interface High Discard Rate (Lookup Failure) Cleared

Indicates the interface's discard rate caused by lookup failure has transitioned to below the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

The interface is receiving packets for which it has appropriate lookup table entries.

Actions

None.

MPLS LSR Interface High Error Free Discard Rate (RX)

The rate per second of inbound labeled packets, for which no error was detected, that the LSR discarded is above the set threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

The LSR may be short of buffer space.

Actions

Check the LSR configuration, there may also be low buffer events raised for the device.

MPLS LSR Interface High Error Free Discard Rate (RX) Cleared

Indicates the interface's discard rate of error free packets has transitioned to below the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

The initial reason for discarding packets, e.g. low buffer space, has been resolved, or traffic to the LSR may have dropped.

Actions

None.

MPLS LSR Interface High Error Free Discard Rate (TX)

The rate per second of outbound labeled packets, for which no error was detected, that the LSR discarded is above the set threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

The LSR may be short of buffer space.

Actions

Check the LSR configuration, there may also be low buffer events raised for the device.

MPLS LSR Interface High Error Free Discard Rate (TX) Cleared

Indicates the interface's discard rate of error free packets has transitioned to below the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

The initial reason for discarding packets, e.g. low buffer space, has been resolved, or traffic to the LSR may have dropped.

Actions

None.

MPLS LSR Interface High Fragmentation Rate

This event indicates the number of outgoing MPLS packets that required fragmentation before transmission on this interface is above the set threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

An interface capacity mismatch causes incoming packets to be fragmented before they can be transmitted. Fragmentation is a resource intensive process and can adversely affect LSR performance.

Actions

Configure the LSR to send and receive compatible sized packets.

MPLS LSR Interface High Fragmentation Rate Cleared

Indicates the interface's fragmentation rate of has transitioned to below the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

A reconfiguration of the involved interfaces, a drop in traffic on the interface.

Actions

None.

MPLS LSR Interface Low Bandwidth

Indicates the total amount of available bandwidth available on this interface is below the set threshold. Available bandwidth is calculated as the difference between the amount of bandwidth currently in use and total bandwidth.

Default severity level: **severe**, color code: orange.

Typical Causes

Overused interface.

Actions

For an interface showing consistently low bandwidth consider adjusting its load.

MPLS LSR Interface Low Bandwidth Cleared

Indicates the amount of free bandwidth on the interface has transitioned to below the low bandwidth threshold.

Default severity level: **information**, color code: green.

Typical Causes

Reduced load on the interface.

Actions

None.

MPLS LSR Interface Low Buffer Space

Indicates the total amount of available buffer space available on this interface is below the set threshold. Available buffer space is calculated as the difference between the amount of buffer space currently in use and total buffer space.

Default severity level: **severe**, color code: orange.

Typical Causes

Overused interface.

Actions

For an interface showing consistently low buffer space consider adjusting its load.

MPLS LSR Interface Low Buffer Space Cleared

Indicates the amount of free buffer space on the interface has transitioned to above the low buffer space threshold.

Default severity level: **information**, color code: green.

Typical Causes

Reduced load on the interface.

Actions

None.

MPLS LSR Platform High Discard Rate (Lookup Failure)

Indicates the number of labeled packets that have been received on this platform and were discarded because there were no matching entries found for them in mplsInSegmentTable.

Default severity level: **severe**, color code: orange.

Typical Causes

There were no forwarding rules for these received packets.

Actions

Check the configuration of your forwarding tables.

MPLS LSR Platform High Discard Rate (Lookup Failure) Cleared

Indicates the platform's discard rate caused by lookup failures has transitioned to below the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

The platform is receiving packets for which it has appropriate lookup table entries.

Actions

None.

MPLS LSR Platform High Error Free Discard Rate (RX)

The rate per second of inbound labeled packets, for which no error was detected, that the LSR discarded is above the set threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

The LSR may be short of buffer space.

Actions

Check the LSR configuration, there may also be low buffer events raised for the device.

MPLS LSR Platform High Error Free Discard Rate (RX) Cleared

Indicates the platform's discard rate of error free packets has transitioned to below the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

The initial reason for discarding packets, e.g. low buffer space, has been resolved, or traffic to the LSR may have dropped.

Actions

None.

MPLS LSR Platform High Error Free Discard Rate (TX)

The rate per second of outbound labeled packets, for which no error was detected, that the LSR discarded is above the set threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

The LSR may be short of buffer space.

Actions

Check the LSR configuration, there may also be low buffer events raised for the device.

MPLS LSR Platform High Error Free Discard Rate (TX) Cleared

Indicates the platform's discard rate of error free packets has transitioned to below the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

The initial reason for discarding packets, e.g. low buffer space, has been resolved, or traffic to the LSR may have dropped.

Actions

None.

MPLS LSR Platform High Fragmentation Rate

This event indicates the number of outgoing MPLS packets that required fragmentation before transmission on this platform is above the set threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

An interface capacity mismatch causes incoming packets to be fragmented before they can be transmitted. Fragmentation is a resource intensive process and can adversely affect LSR performance.

Actions

Configure the LSR to send and receive compatible sized packets.

MPLS LSR Platform High Fragmentation Rate Cleared

Indicates the platform's fragmentation rate has transitioned to below the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

A reconfiguration of the involved interfaces, a drop in traffic on the platform.

Actions

None.

MPLS VRF High Illegal Label Rate

The VRF is receiving packets with labels for which it is not configured at a rate above the set threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

The VRF is receiving packets from an area of the network for which it is not configured. This may indicate a misconfiguration or security problem.

Actions

Investigate the source of the illegal labels.

MPLS VRF High Illegal Label Rate Cleared

The VRF is receiving packets with labels for which it is not configured at a rate below the set threshold.

Default severity level: **information**, color code: green.

Typical Causes

A misconfiguration has been corrected.

Actions

None.

MPLS VRF Interface BGP Neighbor Disappeared

The interface has not received the BGP keep alive message within the set time.

Default severity level: **critical**, color code: red.

Typical Causes

This may be, for example, because the router has gone, or the route to the router is down.

Actions

When the involved devices are managed by Entuity you view router status.

MPLS VRF Interface BGP Neighbor Newly Discovered

A new BGP neighbor has been added to the network.

Default severity level: **minor**, color code: yellow.

Typical Causes

The administrator has added a new BGP neighbor to the network.

Actions

Where you have concerns over security check the new neighbor is expected.

MPLS VRF Non-operational

When the number of active interfaces associated with a VRF is zero, then the VRF is not operational.

Default severity level: **critical**, color code: red.

Typical Causes

The interfaces associated with the VRF are down, or a change in configuration has removed all of the interfaces associated with the VRF.

Actions

Check the number of interfaces, and check the configuration.

None.

MPLS VRF Operational

Indicates the VRF has transitioned from a non-operational to an operational state.

Default severity level: **information**, color code: green.

Typical Causes

VRF has returned to an operational state, for example after the device has been rebooted.

Actions

None.

Network Outage

Network Outage events are raised on information Entuity collects using traceroute and ICMP ping. It indicates an outage on your network, caused for example by node failure, unreachability of a managed port.

The *Details* column of the event indicates the particular category of the outage, how Entuity identifies the outage category is a product of how it handles traceroute data. Entuity discovers all IP addresses configured on a device and then determines which ports, if any, these IP addresses belong to. The success of this association is dependent on the structure of the SNMP MIB. Also if a port is unmanaged within Entuity then an IP address cannot be associated with the port.

Default severity level: **critical**, color code: red.

Typical Causes

The *Details* column in Event Viewer indicates the particular cause of the outage:

- **Managed IP On Device Unreachable:** Indicates that an IP address is not responding to ping:
 - The port for the IP address is not managed by Entuity but the device is managed by Entuity. This may be caused by a routing problem, interface shutdown.
 - Entuity cannot determine the port associated with the IP address because the IP address is not fixed to a port.
- **Port Unreachable:** Indicates that an IP address that is associated with a port is not responding to ping.

When Entuity is managing the device through a network cloud, Entuity raises this event when some of the device's IP addresses are down. Event details lists the unreachable IP addresses in the cloud.

- **Node Unreachable:** Indicates that all of the IP addresses of a network node are not responding to ping. The node (typically a router or a switch) has transitioned to the down state.

When Entuity is managing the device through a network cloud, Entuity raises this event when all of the device's IP addresses are down. Event details lists the unreachable IP addresses in the cloud.

- **Entuity Server disconnected from network:** Indicates that all discovered IP addresses are not responding to ping, suggesting the disconnection of the Entuity server from the network.



The Network Outage event is only raised against devices that are the root cause of the outage, the Device Unreachable event, when enabled, is raised against any device Entuity identifies as unreachable.

Actions

In the *Impacted* column of Event Viewer Entuity displays a count of the nodes, servers and applications impacted by the port down or node failure. You can view the list of impacted objects - or at least those components for which you have permission to view - by from the context sensitive menu clicking **Show Details**.

When Entuity raises a network outage event the action you take depends upon the event type raised, on your network administrator role and whether you have physical access to the device. When event *Details* identifies the cause of the outage as:

- **Managed IP On Device Unreachable or Port Unreachable**

For these two categories check that the relevant network is routable from Entuity. If the network is not routable and this is:

- Intentional then to prevent the raising of this event consider excluding the network from Entuity management through Entuity's configuration settings.
- A Port Unreachable network outage check the operation status of the port. If this is down it may indicate a damaged or pulled out cable or that the device at the other end of the link has failed.

- **Node Unreachable**

If all of a device's IP addresses are not responding to ping and the device is also not responding to SNMP polling it is probable that the node has failed. You can review the incident history for the device, for example for fan failure and temperature incidents. If the device does not restart the only recourse is a physical inspection.

- **Entuity Server disconnected from network**

From the Entuity server machine use the ping utility installed as part of its operating system to ping network devices. If ping fails to elicit a response check for Access Control Lists and firewalls that may be blocking ICMP ping. If ping succeeds check that the

server's firewall permits `applicationMonitor` access, you may have to add a rule for the Entuity process.

Network Outage Cleared

Indicates an outage on your network, caused for example by node failure, unreachability of a managed port is now resolved.

Default severity level: **information**, color code: green.

Typical Causes

The Details column in Event Viewer indicates the particular network outage clearance:

- **Managed IP Address Reachable**

Indicates that the IP address is now responding to ping. The port for the IP address is not managed by Entuity, but the device is managed by Entuity.

- **Port Reachable**

Indicates that a port is once again responding to ping. For router ports a filter ensures only ports with an associated IP address are included.

- **Node Reachable**

Indicates that a node (typically a router or a switch) has transitioned to the up state. All of the IP addresses of a network node do not respond to ping.

- **Entuity Server connected to the network**

Indicates a restored connection of the Entuity server to the network.

Actions

None.

OSPF Peer Briefly Not Established

Indicates to administrators that virtual links between OSPF speakers are now well established but bounced recently. Entuity identifies a recent bounce as the up time is lower than in the previous poll.

Default severity level: **critical**, color code: red.

Typical Causes

OSPF keep-alives may be lost, so the local router terminates the connection and then successfully attempt to reestablish it. Other causes maybe an unstable remote router, traffic shaping limitations.

Actions

Check logs are activated on the device. Use the logs to investigate error messages.

OSPF Peer Disappeared

Indicates a former adjacent peer has been removed from router's configuration. Administrator's should be aware of this change to be able to detect rogue configuration updates.

Default severity level: **critical**, color code: red.

Typical Causes

Removal of an adjacent router.

Actions

Investigate the cause of router disappearance.

OSPF Peer Established

Indicates to administrators that virtual links between OSPF peers are well established. the state has just transitioned to **Full**.

Default severity level: **minor**, color code: yellow.

Typical Causes

OSPF peering established.

Actions

None.

OSPF Peer Newly Discovered

Indicates Entuity's discovery of a new OSPF peer.

Default severity level: **minor**, color code: yellow.

Typical Causes

Configuration of a new OSPF peer.

Actions

None.

OSPF Peer Not Established

Indicates to administrators that a former adjacent peer is no longer in reach. The state has just transitioned out of the **Full** state.

Default severity level: **critical**, color code: red.

Typical Causes

Problems with IP reachability or incorrect OSPF configuration.

Actions

Use the ping and show route commands to verify network connectivity to the OSPF peer. You can use the **show log messages** command to look for errors relating to the peer.

Port Duplex Change

Indicates that an Ethernet port has changed from half to full duplex or vice versa.

Default severity level: **information**, color code: green.

Typical Causes

Configuration change, auto- detection mechanism has detected a duplex change on the attached PC or server NIC card.

Actions

None.

Port Error Disable Alarm

On Cisco Stack devices Entuity identifies the additional port status, error disabled port.



This event is only enabled through additions to Entuity's configuration. Contact your Entuity Support representative for details.

Default severity level: **critical**, color code: red.

Typical Causes

The port error disable state indicates that the port has been brought down by the device (even though its admin status is up) because of detected errors persisting for a configured errdisable timeout period. This only happens if sysErrDisableTimeoutEnable is set for the device.

Actions

A port in this state will not come up again unless manually re-enabled by the network administrator.



This event is only enabled through additions to Entuity's configuration. Contact your Entuity Support representative for details.

Default severity level: **information**, color code: green.

Typical Causes

Transition of port status to normal.

Actions

None.

Port High Inbound Discards (Dynamic)

Indicates that a port is dropping some packets in its receive buffers. Packet loss and transmission delays cause end to end application performance degradation, as applications timeout and re-transmit data intermittently.

The discard rate is higher than the active dynamic threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

Lack of bandwidth on the port, transmit buffer sizes too small.

Actions

Use the Ticker tool to check the current outbound port utilization. If this is high, and a historical graph of port utilization reveals that, in general, the link is highly utilized, then more bandwidth may be needed.

Although the percentage level of discards the port reports may be high if it has a low packet throughput then you may want to amend the behavior of the event. You can activate a low traffic filter to eliminate nuisance events. Port Minimum Packet Rate for Discards allows you to set a packets per second threshold; only when this threshold is crossed could Entuity potentially raise this event. When activated the threshold is included to the event details string, for example:

```
InDiscards=0.32% (threshold=1%) of 7.66Mppts/300s. Packet-  
rate=25.54kppts/s (threshold=0.001ppts/s)
```

Port High Inbound Discards (Dynamic) Cleared

Indicates that a port that was dropping enough packets in its receive buffers to cross the set dynamic threshold is no longer doing so.

Default severity level: **information**, color code: green.

Typical Causes

Inbound discards has returned to levels within the dynamic threshold.

Actions

No action required.

Port High Inbound Fault (Dynamic)

Indicates that a port is receiving corrupted packets from the network (a brownout). These packets will be thrown away by the switch or router that is reporting this problem, causing application layer timeouts and re-transmissions. Network users may be complaining about

slow application response times. Types of corrupted packets include CRC errors, alignment errors, giants, and runt packets.

Default severity level: **severe**, color code: orange.

Typical Causes

Duplex/Half Duplex configuration mismatches on switch and router ports, faulty cabling between PCs/servers and switch ports, faulty NIC cards on PCs and servers, faulty transceivers, noise on WAN circuits. Giant packets may be caused by faulty firmware on switch devices or encapsulation mis-configuration on trunk ports.

Actions

Check the duplex settings on switch ports reporting this problem, and the PC or server which is attached to the switch port. If this isn't the cause of the problem, move the PC or server to a different port and see if the corruption continues. If so, swap out the NIC card on the PC or server.

Although the percentage level of faults the port reports may be high if it has a low packet throughput then you may want to amend the behavior of the event. You can activate a low traffic filter to eliminate nuisance events. The Port Minimum Packet Rate for Faults allows you to set a packets per second threshold; only when this threshold is crossed could Entuity potentially raise this event. When activated the threshold is included to the event details string, for example:

```
InFault=0.28% (threshold=1.00%) of 24.05Mppts/300s --> align=9%,  
crc=4%, abort=16%. Packet-rate=80.16kppts/s (threshold=1.00ppts/s)
```

Port High Inbound Fault (Dynamic) Cleared

Indicates that a port that was receiving corrupted packets from the network (a brownout) is no longer receiving those packets.

Default severity level: **information**, color code: green.

Typical Causes

Reduction in traffic.

Actions

None.

Port High Inbound Utilization (Dynamic)

Indicates that a port (link) is experiencing high levels of utilization (bandwidth usage). This may cause users who are communicating over this area of the network to experience slow application response times.

Default severity level: **severe**, color code: orange.

Typical Causes

Excessive application traffic, configuration changes.

Actions

If high port level utilization persists, then the link speed may need to be increased to accommodate the extra traffic levels.

Port High Inbound Utilization (Dynamic) Cleared

Indicates that a port (link) that was experiencing high levels of utilization (bandwidth usage) is now operating within dynamic thresholds.

Default severity level: **information**, color code: green.

Typical Causes

Utilization for the port has during the past hour is within the expected threshold.

Actions

None.

Port High Outbound Discards (Dynamic)

Indicates that a port is dropping some packets in its transmit buffers, and/or experiencing difficulties transmitting packets out onto the network. Packet loss and transmission delays cause end to end application performance degradation, as applications timeout and re-transmit data intermittently.

The discard rate is higher than the active dynamic threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

Lack of bandwidth on the port, transmit buffer sizes too small.

Actions

Use the Ticker tool to check the current outbound port utilization. If this is high, and a historical graph of port utilization reveals that, in general, the link is highly utilized, then more bandwidth may be needed.

Although the percentage level of discards the port reports may be high if it has a low packet throughput then you may want to amend the behavior of the event. You can activate a low traffic filter to eliminate nuisance events. Port Minimum Packet Rate for Discards allows you to set a packets per second threshold; only when this threshold is crossed could Entuity potentially raise this event. When activated the threshold is included to the event details string, for example:

```
OutDiscards=0.32% (threshold=1%) of 7.66Mppts/300s. Packet-  
rate=25.54kppts/s (threshold=0.001ppts/s)
```


Port High Outbound Discards (Dynamic) Cleared

Indicates that a port that was dropping large numbers of packets in its transmit buffers, and or experiencing severe difficulties transmitting packets out onto the network is now performing normally.

Default severity level: **information**, color code: green.

Typical Causes

Reduced traffic.

Actions

None.

Port High Outbound Fault (Dynamic)

Indicates that a port is failing to transmit some packets onto the network (a brownout). These packets will be thrown away by the switch or router that is reporting this problem, causing application layer timeouts and re-transmissions. Network users may be complaining about slow application response times. Types of transmit errors include late collisions, carrier loss, and SQE test errors.

The outbound fault rate is higher than the active dynamic threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

Duplex/Half Duplex configuration mismatches on switch and router ports, faulty cabling between PCs/servers and switch ports, faulty NIC cards on PCs and servers, faulty transceivers.

Actions

Check the duplex settings on switch ports reporting this problem, and the PC or server which is attached to the switch port. If this is not the cause of the problem, move the PC or server to a different port and see if the corruption continues. If so, swap out the NIC card on the PC or server.

Although the percentage level of faults the port reports may be high if it has a low packet throughput then you may want to amend the behavior of the event. You can activate a low traffic filter to eliminate nuisance events. The Port Minimum Packet Rate for Faults allows you to set a packets per second threshold; only when this threshold is crossed could Entuity potentially raise this event. When activated the threshold is included to the event details string, for example:

```
OutFault=7.40% (threshold=1.00%) of 2.21Mppts/300s --> SQE=1%, late
col=7%, ex col=11%, abort=7%, car loss=75%. Packet-rate=7.37kppts/s
(threshold=1.00ppts/s)
```

Port High Outbound Fault (Dynamic) Cleared

Indicates that a port that was failing to transmit some packets onto the network (a brownout), is now transmitting successfully.

Default severity level: **information**, color code: green.

Typical Causes

Resolution of Duplex/Half Duplex configuration mismatches on switch and router ports, faulty cabling between PCs/servers and switch ports, faulty NIC cards on PCs and servers, faulty transceivers.

Actions

None

Port High Outbound Utilization (Dynamic)

Indicates that a port (link) is experiencing high levels of utilization (bandwidth usage). This may cause users who are communicating over this area of the network to experience slow application response times.

Default severity level: **severe**, color code: orange.

Typical Causes

Excessive application traffic, configuration changes.

Actions

If high port level utilization persists, then the link speed may need to be increased to accommodate the extra traffic levels.

Port High Outbound Utilization (Dynamic) Cleared

Indicates that a port (link) that was experiencing high levels of utilization (bandwidth usage) is now operating within dynamic thresholds.

Default severity level: **information**, color code: green.

Typical Causes

Utilization for the port has during the past hour is within the expected threshold.

Actions

None.

Port Inbound Discards High (Device Congestion)

Indicates that a port is dropping some packets in its receive buffers. Packet loss and transmission delays cause end to end application performance degradation, as applications timeout and re-transmit data intermittently.

Default severity level: **severe**, color code: orange.

Typical Causes

Lack of bandwidth on the port, transmit buffer sizes too small.

Actions

Use the Ticker tool to check the current outbound port utilization. If this is high, and a historical graph of port utilization reveals that, in general, the link is highly utilized, then more bandwidth may be needed.

Although the percentage level of discards the port reports may be high if it has a low packet throughput then you may want to amend the behavior of the event. You can activate a low traffic filter to eliminate nuisance events. Port Minimum Packet Rate for Discards allows you to set a packets per second threshold; only when this threshold is crossed could Entuity potentially raise this event. When activated the threshold is included to the event details string, for example:

```
InDiscards=0.32% (threshold=1%) of 7.66Mpkts/300s. Packet-  
rate=25.54kppts/s (threshold=0.001ppts/s)
```

Port Inbound Discards High Cleared (No Device Congestion)

Indicates that a port that was dropping enough packets in its receive buffers to cross the set dynamic threshold is no longer doing so.

Default severity level: **information**, color code: green.

Typical Causes

Inbound discards has returned to levels within the dynamic threshold.

Actions

No action required.

Port Inbound Fault High (Packet Corruption)

Indicates that a port is receiving corrupted packets from the network (a brownout). These packets will be thrown away by the switch or router that is reporting this problem, causing application layer timeouts and re-transmissions. Network users may be complaining about slow application response times. Types of corrupted packets include CRC errors, alignment errors, giants, and runt packets.

Default severity level: **major**, color code: amber.

Typical Causes

Duplex/Half Duplex configuration mismatches on switch and router ports, faulty cabling between PCs/servers and switch ports, faulty NIC cards on PCs and servers, faulty transceivers, noise on WAN circuits. Giant packets may be caused by faulty firmware on switch devices or encapsulation mis-configuration on trunk ports.

Actions

Check the duplex settings on switch ports reporting this problem, and the PC or server which is attached to the switch port. If this isn't the cause of the problem, move the PC or server to a different port and see if the corruption continues. If so, swap out the NIC card on the PC or server.

Although the percentage level of faults the port reports may be high if it has a low packet throughput then you may want to amend the behavior of the event. You can activate a low traffic filter to eliminate nuisance events. The Port Minimum Packet Rate for Faults allows you to set a packets per second threshold; only when this threshold is crossed could Entuity potentially raise this event. When activated the threshold is included to the event details string, for example:

```
InFault=0.28% (threshold=1.00%) of 24.05Mppts/300s --> align=9%,  
crc=4%, abort=16%. Packet-rate=80.16kpkts/s (threshold=1.00pkts/s)
```

Port Inbound Fault High (No Packet Corruption) Cleared

Indicates that a port that was receiving corrupted packets from the network (a brownout) is no longer receiving those packets.

Default severity level: **information**, color code: green.

Typical Causes

Reduction in traffic.

Actions

None.

Port Link Down

Indicates that a port has transitioned to the down state.

Default severity level: **critical**, color code: red.

Typical Causes

Disconnecting a PC or server from a switch port, re-booting the PC or server attached to a switch port, faulty cabling, faulty NIC card on the PC or server attached to a switch port, device configuration changes, WAN link CSU/DSU has reported a carrier loss, a sub-interface on a managed device not responding.

Actions

If the device reporting the event is a switch then check what is attached to the port. If it is a trunk or a server port, then this event indicates that there may be a network problem. If the device reporting the event is a router, then Telnet to the router to ascertain possible causes for the outage.

Port Link Up

Indicates that a port has transitioned to the up state.

Default severity level: **information**, color code: green.

Typical Causes

Connecting a PC or server to a switch port, re-booting the PC or server attached to a switch port, WAN link CSU/DSU equipment re-establishing carrier detection.

Actions

None.

Port Low Inbound Utilization (Dynamic)

Indicates that a port (link) is experiencing low levels of inbound utilization (bandwidth usage).

The low inbound utilization is lower than the active dynamic threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

Route changes, outages upstream of the link, server problems.

Actions

This problem may be symptomatic of an issue elsewhere in the network. Check through other events that have recently been reported if excessively low levels of utilization persist.

Port Low Inbound Utilization (Dynamic) Cleared

Indicates that a port (link) that was experiencing low levels of utilization (bandwidth usage) is now operating within dynamic thresholds.

Default severity level: **information**, color code: green.

Typical Causes

Utilization for the port has during the past hour is within the expected threshold.

Actions

None.

Port Low Outbound Utilization (Dynamic)

Indicates that a port (link) is experiencing low levels of inbound utilization (bandwidth usage).

The low inbound utilization is lower than the active dynamic threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

Route changes, outages upstream of the link, server problems.

Actions

This problem may be symptomatic of an issue elsewhere in the network. Check through other events that have recently been reported if excessively low levels of utilization persist.

Port Low Outbound Utilization (Dynamic) Cleared

Indicates that a port (link) that was experiencing low levels of utilization (bandwidth usage) is now operating within dynamic thresholds.

Default severity level: **information**, color code: green.

Typical Causes

Utilization for the port has during the past hour is within the expected threshold.

Actions

None.

Port Operationally Down

Indicates that the port is not responding, its administrative state is up but the operational status is down. By default this event is only enabled for core ports, specifically:

- WAN ports.
- Administrative up ports which have a configured IP addresses (i.e. layer 3 ports) on devices which are routers or have router capability
- Trunks and uplinks that are administrative up.

From Entuity Explorer you can highlight a port and from the context menu click **Polling > Status Events > Enable** to activate this event on a non-core port. From the same menu you also have the option to deactivate this event on a port.

Default severity level: **critical**, color code: red.

Typical Causes

Routing problem, interface shutdown.

Actions

Attempt to ping the device. If the device reporting the event is a switch then check what is attached to the port. If it is a trunk or a server port, then this event indicates that there may be a network problem.

Port Operationally Down Cleared

Indicates that a port that was not responding, is now either responding or its administrative state has been set to down.

Default severity level: **information**, color code: green.

Typical Causes

Routing problem corrected, interface restarted.

Actions

None.

Port Outbound Discards High (Port Congestion)

Indicates that a port is dropping some packets in its transmit buffers, and/or experiencing difficulties transmitting packets out onto the network. Packet loss and transmission delays cause end to end application performance degradation, as applications timeout and re-transmit data intermittently.

Default severity level: **major**, color code: amber.

Typical Causes

Lack of bandwidth on the port, transmit buffer sizes too small.

Actions

Use the Ticker tool to check the current outbound port utilization. If this is high, and a historical graph of port utilization reveals that, in general, the link is highly utilized, then more bandwidth may be needed.

Although the percentage level of discards the port reports may be high if it has a low packet throughput then you may want to amend the behavior of the event. You can activate a low traffic filter to eliminate nuisance events. Port Minimum Packet Rate for Discards allows you to set a packets per second threshold; only when this threshold is crossed could Entuity potentially raise this event. When activated the threshold is included to the event details string, for example:

```
OutDiscards=0.32% (threshold=1%) of 7.66Mppts/300s. Packet-  
rate=25.54kppts/s (threshold=0.001ppts/s)
```

Port Outbound Discards High (No Port Congestion) Cleared

Indicates that a port that was dropping large numbers of packets in its transmit buffers, and or experiencing severe difficulties transmitting packets out onto the network is now performing normally.

Default severity level: **information**, color code: green.

Typical Causes

Reduction in traffic.

Actions

None.

Port Outbound Fault High (Transmit Errors)

Indicates that a port is failing to transmit some packets onto the network (a brownout). These packets will be thrown away by the switch or router that is reporting this problem, causing application layer timeouts and re-transmissions. Network users may be complaining about slow application response times. Types of transmit errors include late collisions, carrier loss, and SQE test errors.

Default severity level: **major**, color code: amber.

Typical Causes

Duplex/Half Duplex configuration mismatches on switch and router ports, faulty cabling between PCs/servers and switch ports, faulty NIC cards on PCs and servers, faulty transceivers.

Actions

Check the duplex settings on switch ports reporting this problem, and the PC or server which is attached to the switch port. If this is not the cause of the problem, move the PC or server to a different port and see if the corruption continues. If so, swap out the NIC card on the PC or server.

Although the percentage level of faults the port reports may be high if it has a low packet throughput then you may want to amend the behavior of the event. You can activate a low traffic filter to eliminate nuisance events. The Port Minimum Packet Rate for Faults allows you to set a packets per second threshold; only when this threshold is crossed could Entuity potentially raise this event. When activated the threshold is included to the event details string, for example:

```
OutFault=7.40% (threshold=1.00%) of 2.21Mppts/300s --> SQE=1%, late
col=7%, ex col=11%, abort=7%, car loss=75%. Packet-rate=7.37kppts/s
(threshold=1.00ppts/s)
```

Port Outbound Fault High Cleared (No Transmit Errors)

Indicates that a port that was failing to transmit some packets onto the network (a brownout), is now transmitting successfully.

Default severity level: **information**, color code: green.

Typical Causes

Resolution of Duplex/Half Duplex configuration mismatches on switch and router ports, faulty cabling between PCs/servers and switch ports, faulty NIC cards on PCs and servers, faulty transceivers.

Actions

None

Port Speed Change

Indicates that a port has changed its interface speed.

Default severity level: **information**, color code: green.

Typical Causes

Configuration change, auto-detection mechanism has detected a speed change on the attached PC or server NIC card.

Actions

None.

Port Utilization High

Indicates that a port (link) is experiencing high levels of utilization (bandwidth usage). This may cause users who are communicating over this area of the network to experience slow application response times.

Default severity level: **severe**, color code: orange.

Typical Causes

Excessive application traffic, configuration changes.

Actions

If high port level utilization persists, then the link speed may need to be increased to accommodate the extra traffic levels.

Port Utilization High Cleared

Indicates that a port (link) that was experiencing high levels of utilization is now transmitting lower traffic volumes.

Default severity level: **information**, color code: green.

Typical Causes

Reduced application traffic

Actions

None.

Port Utilization Low

Indicates that a port (link) is experiencing low levels of utilization (bandwidth usage).

Default severity level: **severe**, color code: orange.

Typical Causes

Route changes, outages upstream of the link, server problems.

Actions

This problem may be symptomatic of an issue elsewhere in the network. Check through other events that have recently been reported if excessively low levels of utilization persist.

Port Utilization Low Cleared

Indicates that a port (link) that was experiencing low levels of utilization is now transmitting higher traffic volumes.

Default severity level: **information**, color code: green.

Typical Causes

Increased application traffic.

Actions

None.

Power Supply Major Fault

Indicates that a device has a major power supply hardware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty power supply hardware.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

Power Supply Minor Fault

Indicates that a device has a minor power supply hardware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty power supply hardware.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

Power Supply OK

Indicates that the power supply fault for a device has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Faulty power supply has been swapped out.

Actions

None.

Power Supply Unknown State

Indicates that the state of the device's power supply hardware is unknown.

Default severity level: **severe**, color code: orange.

Typical Causes

The power supply type is unknown. The ID EEPROM of the power supply has not been programmed or has been corrupted, or the power supply is not supported by the router.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem. Refer to the device documentation for details on power supply unknown.

Processor Utilization High

Indicates the identified processor on the device has high CPU utilization. When the processor cannot be identified Entuity raises the event against single processor 1.

Default severity level: **minor**, color code: yellow.

Typical Causes

High CPU utilization due to interrupts, a particular process using a lot of CPU resources.

Actions

Use the managed host function to view current and historic levels of process usage. Also create reports, for example a Router Summary Report that runs every hour to monitor router CPU utilization.

Processor Utilization High Cleared

Indicates the processor on the device no longer has high processor utilization.

Default severity level: **information only**, color code: green.

Typical Causes

Reduced usage.

Actions

None.



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 monitors bit rate. Bit rate thresholds can be set at the individual interface class level.

For each class Entuity monitors bit rate, and bit rate thresholds can be set at the individual class level.

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 monitors drop bit rate, and drop bit rate thresholds can be set at the individual class level. For each class Entuity monitors drop bit rate, and the high drop bit rate thresholds can be set at the individual class level.

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 monitors drop packet rate, and drop packet rate thresholds can be set at the individual class level.

For each queue Entuity monitors drop bit rate. Drop bit rate thresholds can be set at the individual queue level. Queue management is an important congestion tool,

For each queue Entuity monitors drop bit rate. Drop bit rate thresholds can be set at the individual queue



Routing Broadcast Traffic High

Indicates an incorrect packet broadcast on a network that causes most hosts to respond all at once, typically with wrong answers that start the process over again.

Default severity level: **major**, color code: amber.

Typical Causes

Within a TCP/IP network is the use of ARP (Address Resolution Protocol) requests for address resolution, where the number of devices in a segment is too large.

Defective network adapter card or cable run may cause electrical noise to be sent along the cable causing broadcast packets to be unanswered. This may cause more broadcast traffic, generating a broadcast storm

Actions

Check broadcast traffic domains, configure the network to block illegal broadcast messages, where electrical noise is a problem power down the failing device and disconnect from the cable.

Routing Broadcast Traffic High Cleared

Sent by the router to the sender of a packet indicating that the route is now available.

Default severity level: **information**, color code: green.

Typical Causes

Resolution of high broadcast problem.

Actions

None.

Routing High No Routes to IP Destination

Sent by the router to the sender of a packet indicating that there is no route available to deliver the packet to the intended receiver.

Default severity level: **minor**, color code: yellow.

Typical Causes

A network link is disconnected, the destination address does not exist.

Actions

Investigate destination address, network connections.

Routing High No Routes to IP Destination Cleared

Sent by the router to the sender of a packet indicating that the route is now available.

Default severity level: **information**, color code: green.

Typical Causes

A network link is re-connected.

Actions

None.

Routing ICMP High Redirects

Indicates routers handling packets with incorrect addresses.

Default severity level: **minor**, color code: yellow.

Typical Causes

Device configured with incorrect routing entries.

Actions

Locate the incorrectly configured device and correct. Alternatively, where you feel it's appropriate you can disable ICMP redirects.

Routing ICMP High Redirects Cleared

Indicates a reduction in incorrectly addressed packets.

Default severity level: **information**, color code: green.

Typical Causes

Device reconfiguration.

Actions

None.

Routing ICMP High TTL Exceeds

Indicates TTL (Time To Live) value in the IP Packet is decremented to zero. The Router discards the IP Packet and an ICMP 'TTL Expired in transit' message is sent back to the sending IP Address.

Default severity level: **minor**, color code: yellow.

Typical Causes

Unreachable device, a routing loop.

Actions

Locate the incorrectly configured sending device and correct.

Routing ICMP High TTL Exceeds Cleared

Indicates transmission to the device is now within TTL (Time To Live) value in the IP Packet.

Default severity level: **information**, color code: green.

Typical Causes

Device now online.

Actions

None.

Service Down

Indicates the named service is down.

Typical Causes

The number of components failing in the service is sufficient to cause the service to fail.

Actions

Click **Dashboards > Service Summary**. You can view the current status of all services and then select the required service to drill down and view the status of its components.

Service State Degraded

Indicates the state of the named service is degraded.

Default severity level: **severe**, color code: orange.

Typical Causes

The combined state of components in the service crosses the set threshold at which Entuity determines performance of the service is compromised but the second threshold at which the service would have failed has not been crossed.

Actions

Click **Dashboards > Service Summary**. You can view the current status of all services and then select the required service to drill down and view the status of its components.

Service State Off

Indicates the named service is now set to not generate a state. The event details indicate Status is set to None.

Typical Causes

User has amended the service configuration setting *Type* to **None**.

Actions

None

Service State Unknown

Indicates the state of the named service is unknown.

Default severity level: **severe**, color code: orange.

Typical Causes

The state of one or more of the components in the service is unknown.

Actions

Click **Dashboards > Service Summary**. You can view the current status of all services and then select the required service to drill down and view the status of its components.

Service Up

Indicates the named service is up, its state having previously been **Down** or **Unknown**.

Typical Causes

The state of enough components in the service is up, so the service is now available.

Actions

None

SNMP Agent Not Responding

Indicates the device, or more specifically its SNMP agent, is not responding to SNMP requests, but was available when Entuity last attempted to Ping it as part of its availability monitoring of the device. It is the response to the ping that determines whether Entuity considers a device is up or down, SNMP Agent Not Responding events are not raised when a device is down.

Entuity availability monitoring operates in one of two modes:

- By ICMP ping to the management IP address only.
- By ICMP ping to all IP addresses on the device (default). The device is considered up when Entuity receives one or more responses.

Default severity level: **critical**, color code: red.

Typical Causes

Device configuration changes, e.g. to SNMP read community string or SNMP access lists, or device resource issues.

Actions

Check that the SNMP community string of the device in Entuity is still configured correctly.

SNMP Agent Responding

Indicates the device is now responding to SNMP requests, but was unavailable when Entuity last attempted to Ping it. Entuity pings the IP addresses of managed objects every two minutes.

Default severity level: **information**, color code: green.

Typical Causes

Device configuration changes, e.g. to SNMP read community string or SNMP access lists, or device resource issues.

Actions

None.

SNMP Agent Restart Detected

Indicates the SNMP service has restarted on the managed host, since Entuity last attempted to poll it. It also indicates the SNMP counters polled by Entuity for the managed host have been reset, which may explain any unexpected data spikes.

Default severity level: **major**, color code: amber.

Typical Causes

The device restarted, a manual restart of the SNMP agent.

Actions

None.

SNMP Authentication Failure

Indicates that a request did not get proper authentication, usually the result of a bad community string.

Default severity level: **severe**, color code: orange.

Typical Causes

An invalid community was received in a message.

Actions

Ping the device to ensure that it is still contactable. If ping is successful then check that the IP address and SNMP community string of the device in Entuity are still configured correctly (although it may not be the Entuity server that is issuing the SNMP requests that are failing).

SNMP Response Time High

Indicates that a device's response to an SNMP request was greater than the set threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

Latency may be caused by the traffic load on the network or by load on the device or intermediate devices.

Actions

Entuity displays latency metrics through gauges and charts on the device Summary page. You can then drill down to view latency charts. To view this device's latency performance within the context of other devices you can run the Administrative report, Device SNMP Response Time.

SNMP Response Time High Cleared

Indicates that a device's response to an SNMP request has now returned to within the set threshold.

Default severity level: **severe**, color code: orange.

Typical Causes

Latency has returned to within the set threshold.

Actions

None.

SNMP v3 Duplicate Engine ID

Indicates that two or more devices under management now have the same SNMPv3 engine identifier. Under SNMPv3 devices use the engine identifier when determining the source of a trap and decoding its message.

Default severity level: **severe**, color code: orange.

Typical Causes

A device under Entuity management has been reconfigured with a engine identifier used by another device also under management.

Actions

The event details includes information on the two devices with the same engine identifier. You should reconfigure one of the devices with a unique engine identifier.

SSL Certificate Expired

Indicates the SSL certificate has expired. Entuity continues to raise this event, every twenty-four hours, until the certificate is renewed or removed.

Default severity level: **critical**, color code: red.

Typical Causes

SSL certificate has passed its expiry date.

Actions

Install a new SSL certificate.

SSL Certificate Expiring

Indicates the SSL certificate expiry date is within the set expiry notification period. You can amend the notification period against the device. Entuity continues to raise this event, every 24 hours, until the certificate is renewed, removed or expires.

Default severity level: **severe**, color code: orange.

Typical Causes

SSL certificate expiry date is within the set notification period.

Actions

Obtain a new SSL certificate. Self signed certificates you can create yourself, otherwise obtain one from a recognized SSL certificate issuing authority.

SSL Proxy Service Administrative Available to SNMP Poll

Indicates that the device is responding, as its administrative state is up.

Default severity level: **information**, color code: green.

Typical Causes

Administrator has configured the administrative state to up.

Actions

None.

SSL Proxy Service Administrative Unavailable to SNMP Poll

Indicates that the device is not responding, as its administrative state is down.

Default severity level: **critical**, color code: red.

Typical Causes

Administrator has taken the module down.

Actions

None.

SSL Proxy Service Operational Available to SNMP Poll

Indicates that the device is responding to SNMP polling, as its operational state is up.

Default severity level: **information**, color code: green.

Typical Causes

The SSL Proxy service has been down but is now available.

Actions

None.

SSL Proxy Service Operational Unavailable to SNMP Poll

Indicates that the device is not responding to SNMP polling, as its operational state is down.

Default severity level: **critical**, color code: red.

Typical Causes

SSL certificate has passed its expiry date.

Actions

Contact your SSL authority for a valid certificate.

STP New Root Device

Indicates that a device reported a new root switch for a spanning tree in which it participates. This event is detected by the generation of an SNMP trap on the device.

Default severity level: **critical**, color code: red.

Typical Causes

Device configuration changes, device or link failures.

Actions

Telnet to the device and check the system logs for an indication of what caused a new device to become the root switch.

STP VLAN Topology Change

Indicates that a device reported a topology change for a spanning tree in which it participates. This event is detected by the generation of an SNMP trap on the device.

Default severity level: **major**, color code: amber.

Typical Causes

Device configuration changes, device or link failures.

Actions

Telnet to the device and check the system logs for an indication of what caused the topology change.

Syslog Alert Event

Syslog can generate system messages for each of the defined facilities, those defined by default and those defined locally. All of the system message can be prioritized. 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.

Default severity level: **severe**, color code: orange.

Typical Causes

The Entuity System Administrator determines which system messages from which facilities and at what priority level, generate events displayed through Event Viewer. (see the *Entuity User and System Administrator Guide*.)

Actions

Dependent on the syslog event raised.

Syslog Critical Events

Syslog can generate system messages for each of the defined facilities, those defined by default and those defined locally. All of the system message can be prioritized. 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.

Default severity level: **severe**, color code: orange.

Typical Causes

The Entuity System Administrator determines which system messages from which facilities and at what priority level, generate events displayed through Event Viewer. (see the *Entuity User and System Administrator Guide*.)

Actions

Dependent on the syslog event raised.

Syslog Debug Events

Syslog can generate system messages for each of the defined facilities, those defined by default and those defined locally. All of the system message can be prioritized. 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.

Default severity level: **information**, color code: green.

Typical Causes

The Entuity System Administrator determines which system messages from which facilities and at what priority level, generate events displayed through Event Viewer.

Actions

None required.

Syslog Emergency Event

Syslog can generate system messages for each of the defined facilities, those defined by default and those defined locally. All of the system message can be prioritized.

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.

Default severity level: **critical**, color code: red.

Typical Causes

The Entuity System Administrator determines which system messages from which facilities and at what priority level, generate events displayed through Event Viewer. (see the *Entuity User and System Administrator Guide*.)

Actions

Dependent on the syslog event raised.

Syslog Error Events

Syslog can generate system messages for each of the defined facilities, those defined by default and those defined locally. All of the system message can be prioritized. 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.

Default severity level: **major**, color code: amber.

Typical Causes

The Entuity System Administrator determines which system messages from which facilities and at what priority level, generate events displayed through Event Viewer. (see the *Entuity User and System Administrator Guide*.)

Actions

Dependent on the syslog event raised.

Syslog Information Events

Syslog can generate system messages for each of the defined facilities, those defined by default and those defined locally. All of the system message can be prioritized. 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.

Default severity level: **information**, color code: green.

Typical Causes

The Entuity System Administrator determines which system messages from which facilities and at what priority level, generate events displayed through Event Viewer. (See the *Entuity User and System Administrator Guide*.)

Actions

None required.

Syslog Notice Events

Syslog can generate system messages for each of the defined facilities, those defined by default and those defined locally. All of the system message can be prioritized. 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.

Default severity level: **minor**, color code: yellow.

Typical Causes

The Entuity System Administrator determines which system messages from which facilities and at what priority level, generate events displayed through Event Viewer. (See the *Entuity User and System Administrator Guide*.)

Actions

None required.

Syslog Warning Events

Syslog can generate system messages for each of the defined facilities, those defined by default and those defined locally. All of the system message can be prioritized. 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.

Default severity level: **minor**, color code: yellow.

Typical Causes

The Entuity System Administrator determines which system messages from which facilities and at what priority level, generate events displayed through Event Viewer. (See the *Entuity User and System Administrator Guide*.)

Actions

Dependent on the syslog event raised.

UCS Blade Down

Indicates a blade fault for a device.

Default severity level: **critical**, color code: red.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Blade Major Fault

Indicates a major blade hardware or firmware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Blade Minor Fault

Indicates that a blade has a minor hardware or firmware problem.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Blade OK

Indicates that a blade fault for a device has been cleared.

Default severity level: **ok**, color code: green.

Typical Causes

Faulty blade has been swapped out.

Actions

None.

UCS Blade Status Unknown

Indicates that Entuity cannot determine the status of the blade.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Chassis Down

Indicates a fault for a device.

Default severity level: **critical**, color code: red.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Chassis Major Fault

Indicates a major chassis hardware or firmware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty hardware or firmware.

Actions

Telnet to the device and check the system settings for an indication of what the problem is. A hardware swap out may need to be scheduled depending on the type of problem.

UCS Chassis Minor Fault

Indicates that a chassis has a minor hardware or firmware problem.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Chassis Status OK

Indicates that a chassis fault for a device has been cleared.

Default severity level: **ok**, color code: green.

Typical Causes

Faulty chassis has been swapped out.

Actions

None.

UCS Chassis Status Unknown

Indicates that Entuity cannot determine the status of the chassis.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fabric Extender Down

Indicates a fabric extender fault for a device.

Default severity level: **critical**, color code: red.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fabric Extender Major Fault

Indicates a major fabric extender hardware or firmware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fabric Extender Minor Fault

Indicates that a fabric extender has a minor hardware or firmware problem.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fabric Extender Status OK

Indicates that a fabric extender fault for a device has been cleared.

Default severity level: **ok**, color code: green.

Typical Causes

Faulty fabric extender has been swapped out.

Actions

None.

UCS Fabric Extender Status Unknown

Indicates that Entuity cannot determine the status of the fabric extender.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fan Down

Indicates a fault on a fan on the device chassis.

Default severity level: **critical**, color code: red.

Typical Causes

Faulty fan hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fan Major Fault

Indicates a fan on the device chassis has a major fault.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty fan hardware, faulty environmental card, faulty supervisor card.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fan Minor Fault

Indicates a fan on the device chassis is reporting a minor fault.

Default severity level: **major**, color code: amber.

Typical Causes

Faulty fan hardware, faulty environmental card, faulty supervisor card.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fan Module Down

Indicates a fault for a device.

Default severity level: **critical**, color code: red.

Typical Causes

Faulty fan module hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fan Module Major Fault

Indicates that a module has a major fan hardware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty fan hardware, faulty environmental card, faulty supervisor card.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fan Module Minor Fault

Indicates that a module has a minor fan hardware problem.

Default severity level: **major**, color code: amber.

Typical Causes

Faulty fan hardware, faulty environmental card, faulty supervisor card.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot

resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fan Module Status OK

Indicates that a fan module fault for a device has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Faulty fan module has been swapped out.

Actions

None.

UCS Fan Module Status Unknown

Indicates the status of the fan module is not reportable or is unknown.

Default severity level: **minor**, color code: yellow.

Typical Causes

The status of the fan module is not reportable. Or, the fan module status is unknown.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Fan Status OK

Indicates that a fan fault for a device has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Faulty fan has been swapped out.

Actions

None.

UCS Fan Status Unknown

Indicates the status of the fan is not reportable or is unknown.

Default severity level: **minor**, color code: yellow.

Typical Causes

The status of the fan is not reportable. Or, the fan status is unknown.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Local Disk Down

Indicates a local disk fault for a device.

Default severity level: **critical**, color code: red.

Typical Causes

Faulty local disk hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Local Disk Major Fault

Indicates that a device has a major local disk hardware or firmware problem

Default severity level: **major**, color code: amber.

Typical Causes

Faulty local disk hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Local Disk Minor Fault

Indicates that a device has a minor module (line card) hardware or firmware problem.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty local disk hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Local Disk Unknown

Indicates that the local disk is unknown.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Local Disk OK

Indicates that a module (card) fault for a device has been cleared.

Default severity level: **ok**, color code: green.

Typical Causes

Faulty local disk has been swapped out.

Actions

None.

UCS PSU Down

Indicates a PSU fault for a device.

Default severity level: **critical**, color code: red.

Typical Causes

Faulty PSU hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS PSU Major Fault

Indicates that a device has a major PSU hardware or firmware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty PSU hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS PSU Minor Fault

Indicates that a device has a minor PSU hardware or firmware problem.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty PSU hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot

resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS PSU Unknown

Indicates that the PSU is unknown.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS PSU OK

Indicates that a PSU fault for a device has been cleared.

Default severity level: **ok**, color code: green.

Typical Causes

Faulty PSU has been swapped out.

Actions

None.

UCS Switch Card Down

Indicates a switch card fault for a device.

Default severity level: **major**, color code: amber.

Typical Causes

Faulty switch card hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Switch Card Major Fault

Indicates that a device has a major switch card hardware or firmware problem.

Default severity level: **severe**, color code: orange.

Typical Causes

Faulty switch card hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Switch Card Minor Fault

Indicates that a device has a minor switch card hardware or firmware problem.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty switch card hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

UCS Switch Card Status OK

Indicates that a switch card fault for a device has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Faulty switch card has been swapped out.

Actions

None.

UCS Switch Card Status Unknown

Indicates that Entuity cannot determine the status of the device.

Default severity level: **minor**, color code: yellow.

Typical Causes

Faulty switch card hardware or firmware.

Actions

Copy the message from the event description, or you can access the Cisco UCS Manager and copy it from the console or the system log. Research and attempt to resolve the issue using the tools and utilities provided at <http://www.cisco.com/tac>. Also refer to the *Release Notes for Cisco UCS Manager* and the *Cisco UCS Troubleshooting Guide*. If you cannot resolve the issue, execute the show tech-support command and contact Cisco Technical Support.

Unknown Trap

Indicates Entuity received an enterprise trap for which it does not have a loaded MIB, rules or custom event. Trap details include its OID and argument values.

Default severity level: **major**, color code: amber.

Typical Causes

Entuity received an enterprise trap for which a mapping has been included to the Entuity database.

Actions

Through the Event Management System you can import and load MIBs, creating rules and custom events for trap definitions. Alternatively you can prevent Entuity raising Unknown Trap events by activating the Discard Unknown Trap rule.

User Defined Attribute State Disabled

Through User Defined Polling you can create attributes for Entuity to poll and set up Entuity to raise events depending upon the values returned.

Default severity level: **major**, color code: amber.

Typical Causes

This event is a state event and is raised when the attribute reports its state as disabled.

Actions

View the event details. This contains the configuration setup for the disabled state.

User Defined Attribute State Down

Through User Defined Polling you can create attributes for Entuity to poll and set up Entuity to raise events depending upon the values returned.

Default severity level: **severe**, color code: orange.

Typical Causes

This event is a state event and is raised when the attribute reports its state as down.

Actions

View the event details. This contains the configuration setup for the disabled state.

User Defined Attribute State Other

Through User Defined Polling you can create attributes for Entuity to poll and set up Entuity to raise events depending upon the values returned.

Default severity level: **major**, color code: amber.

Typical Causes

This event is a state event and is raised when the attribute reports its state as other.

Actions

View the event details. This contains the configuration setup for the other state.

User Defined Attribute State Up

Through User Defined Polling you can create attributes for Entuity to poll and set up Entuity to raise events depending upon the values returned.

Default severity level: **ok**, color code: green.

Typical Causes

This event is a state event and is raised when the attribute reports its state as up.

Actions

View the event details. This contains the configuration setup for the Up state.

User Defined Attribute Value Abnormality Cleared

Through User Defined Polling you can create attributes for Entuity to poll. You can also set up Entuity to raise events depending upon the values returned.

Default severity level: **ok**, color code: green.

Typical Causes

This event is a threshold event and is raised when the polled attribute value has transitioned to a normal state.

Actions

View the event details. This contains the configuration setup for the normal state.

User Defined Attribute Value Critical

Through User Defined Polling you can create attributes for Entuity to poll. You can also set up Entuity to raise events depending upon the values returned.

Default severity level: **critical**, color code: red.

Typical Causes

This event is a threshold event and is raised when the polled attribute value is greater than the set threshold.

Actions

View the event details. This contains the configuration setup for the critical threshold state.

User Defined Attribute Value High

Through User Defined Polling you can create attributes for Entuity to poll. You can also set up Entuity to raise events depending upon the values returned.

Default severity level: **severe**, color code: orange.

Typical Causes

This event is a threshold event and is raised when the polled attribute value is within the set High threshold boundary.

Actions

View the event details. This contains the configuration setup for the high threshold state.

User Defined Attribute Value Low

Through User Defined Polling you can create attributes for Entuity to poll. You can also set up Entuity to raise events depending upon the values returned.

Default severity level: **major**, color code: amber.

Typical Causes

This event is a threshold event and is raised when the polled attribute value is within the set low threshold boundary.

Actions

View the event details. This contains the configuration setup for the low threshold state.

User Defined Attribute Value Warning

Through User Defined Polling you can create attributes for Entuity to poll. You can also set up Entuity to raise events depending upon the values returned.

Default severity level: **major**, color code: amber.

Typical Causes

This event is a threshold event and is raised when the polled attribute value is within the set low threshold boundary.

Actions

View the event details. This contains the configuration setup for the low threshold state.

Virtual Machine Moved

Entuity has monitored the moving of a VM between hypervisors.

Default severity level: **minor**, color code yellow.

Typical Causes

Corrected connection details.

Actions

No action required.

Virtual Machine Powered Off

Entuity has monitored the powering off of a VM.

Default severity level: **information**, color code green.

Typical Causes

Corrected connection details.

Actions

No action required.

Virtual Machine Powered On

Entuity has monitored the powering on of a VM.

Default severity level: **information**, color code green.

Typical Causes

Corrected connection details.

Actions

No action required.

Virtualization Connection Failed

Indicates Entuity has failed to connect to the identified VM platform.

Default severity level: **severe**, color code orange.

Typical Causes

Incorrect connection details, e.g. an aged out connection password, an incorrect connection URL. An unavailable VM platform.

Actions

Confirm the connection details, connection to a VM platform is through its SDK. From the **Administration > Inventory /Topology > Inventory Administration** page you can view and modify connection details.

Virtualization Connection Success

Entuity has successfully connected to the VM platform after a previous failure.

Default severity level: **information**, color code green.

Typical Causes

Corrected connection details.

Actions

No action required.

VM Guest Memory High

Indicates high memory utilization on the VM. VM High Guest Memory Threshold can be set against the VM Platform and against individual VMs.

Default severity level: **minor**, color code yellow.

Typical Causes

Excessive application holding of resources.

Actions

Run a Flex Report to identify long term utilization of tunnels on the VPN.

VM Guest Memory High Cleared

Indicates a previous VM Guest Memory High alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

VM memory utilization has returned to acceptable levels.

Actions

No action required.

VPN High Active Tunnels

Indicates high VPN tunnel usage.

Default severity level: **minor**, color code yellow.

Typical Causes

Excessive application traffic, configuration changes.

Actions

Run a Flex Report to identify long term utilization of tunnels on the VPN.

VPN High Active Tunnels Cleared

Indicates a previous VPN Load Average High alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

VPN tunnel usage has returned to acceptable levels.

Actions

No action required.

VPN Load Average High

Load average is the average number of processes in the runqueue during the polling interval.

Default severity level: **minor**, color code yellow.

Typical Causes

Excessive application traffic, configuration changes.

Actions

Run a Flex Report to identify long term utilization of tunnels on the VPN.

VPN Load Average High Cleared

Indicates a previous VPN Load Average High alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

Average loading for the runqueue has returned to acceptable levels.

Actions

No action required.

VPN Network Port Utilization High

Indicates that a VPN ethernet port (link) is experiencing high levels of utilization (bandwidth usage). This may cause users who are communicating over this area of the network to experience slow application response times.

Default severity level: **minor**, color code yellow.

Typical Causes

Excessive application traffic, configuration changes.

Actions

If high port level utilization persists, then the link speed may need to be increased to accommodate the extra traffic levels.

VPN Network Port Utilization High Cleared

Indicates a previous VPN Load Average High alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

VPN port utilization has returned to acceptable levels.

Actions

No action required.

VPN Tunnel Usage High

Indicates high VPN tunnel usage.

Default severity level: **minor**, color code yellow.

Typical Causes

Excessive application traffic, configuration changes.

Actions

Run a Flex Report to identify long term utilization of tunnels on the VPN.

VPN Tunnel Usage High Cleared

Indicates a previous VPN Load Average High alarm has been cleared.

Default severity level: **information**, color code: green.

Typical Causes

VPN tunnel usage has returned to acceptable levels.

Actions

No action required.

WAN Port High Inbound Discards

Indicates that a WAN port (link) is discarding packets. This packet loss causes end to end application performance degradation, as applications timeout and re-transmit data intermittently.

Default severity level: **major**, color code: amber.

Typical Causes

When congestion occurs downstream in the network, and the device needs to free buffer space frames are discarded. For Frame Relay the switch dropping frames will select from its buffer the frames with the DE bit set first. If this is not sufficient to relieve the congestion, frames with DE bit clear will be dropped next.

Actions

Use the Ticker tool to check inbound broadcast traffic on the port reporting discards. If broadcast traffic is light, telnet to the device and check system resources. Increasing the size of the receive buffers, and/or upgrading the device hardware (CPU and memory) may be necessary.

WAN Port High Inbound Discards Cleared

Indicates a High WAN Port Inbound Discards alarm has been cleared as the port discard rate is now below the high threshold value.

Default severity level: **information**, color code: green.

Typical Causes

Reduced transmission.

Actions

None.

WAN Port High Inbound Errors

Indicates that a port is receiving corrupted packets from the network (a brownout). These packets are thrown away by the port's device, causing application layer timeouts and re-transmissions. Network users may complain about slow application response times. Types of corrupted packets include CRC errors, alignment errors, giants, and runt packets.

Default severity level: **major**, color code: amber.

Typical Causes

Duplex/Half Duplex configuration mismatches on switch and router ports, faulty cabling between PCs/servers and switch ports, faulty NIC cards on PCs and servers, faulty transceivers, noise on WAN circuits. Giant packets may be caused by faulty firmware on switch devices or encapsulation mis-configuration on trunk ports.

Actions

Check the duplex settings on switch ports reporting this problem, and the PC or server which is attached to the switch port. If this isn't the cause of the problem, move the PC or server to a different port and see if the corruption continues. If so, swap out the NIC card on the PC or server.

WAN Port High Inbound Errors Cleared

An event correlated with WAN Port High Inbound Errors event.

Default severity level: **information**, color code: green.

Typical Causes

Indicates a High WAN Port Inbound Errors alarm has been cleared as the port error rate is now below the high threshold value.

Actions

None.

WAN Port High Inbound Utilization

Indicates that a WAN port (link) is experiencing high levels of utilization (bandwidth usage). This may cause users who are communicating over this area of the network to experience slow application response times.

Default severity level: **major**, color code: amber.

Typical Causes

Excessive application traffic, configuration changes.

Actions

If high port level utilization persists, then the link speed may need to be increased to accommodate the extra traffic levels.

WAN Port High Inbound Utilization Cleared

The correlated clearing event for the WAN Port High Inbound Utilization event.

Default severity level: **information**, color code: green.

Typical Causes

Indicates a WAN Port High Inbound Utilization alarm has been cleared as the port error rate is now below the high threshold value.

Actions

None.

WAN Port High Outbound Discards

Indicates that a port is dropping some packets in its transmit buffers even though no errors had been detected to prevent their being transmitted. Packet loss and transmission delays cause end to end application performance degradation, as applications timeout and re-transmit data intermittently.

Default severity level: **major**, color code: amber.

Typical Causes

Lack of bandwidth on the port, transmit buffer sizes too small.

Actions

Use the Ticker tool to check the current outbound port utilization. If this is high, and a historical graph of port utilization reveals that, in general, the link is highly utilized, then more bandwidth may be needed.

WAN Port High Outbound Discards Cleared

The correlated clearing event for the WAN Port High Outbound Discards event.

Default severity level: **information**, color code: green.

Typical Causes

Indicates a WAN Port High Outbound Discards alarm has been cleared as the port discard rate is now below the high threshold value.

Actions

None.

WAN Port High Outbound Errors

Indicates that the WAN port is dropping large numbers of packets in its transmit buffers, and or experiencing severe difficulties transmitting packets out onto the network. Packet loss and transmission delays cause end to end application performance degradation, as applications timeout and re-transmit data intermittently.

Default severity level: **major**, color code: amber.

Typical Causes

Lack of bandwidth on the port, transmit buffer sizes too small, network congestion causing excessive/late collisions and carrier sense errors.

Actions

Use the Ticker tool to check the current outbound port utilization. If this is high, and a historical graph of port utilization reveals that, in general, the link is highly utilized, then more bandwidth may be needed.

WAN Port High Outbound Errors Cleared

The correlated clearing event for the WAN Port High Outbound Errors event.

Default severity level: **information**, color code: green.

Typical Causes

Indicates a WAN Port High Outbound Errors alarm has been cleared as the port error rate is now below the high threshold value.

Actions

None.

WAN Port High Outbound Utilization

Indicates that a WAN port (link) is experiencing high levels of outbound utilization (bandwidth usage). This may cause users who are communicating over this area of the network to experience slow application response times.

Default severity level: **major**, color code: amber.

Typical Causes

Excessive application traffic, configuration changes.

Actions

If high port level utilization persists, then the link speed may need to be increased to accommodate the extra traffic levels.

WAN Port High Outbound Utilization Cleared

The correlated clearing event for the WAN Port High Outbound Utilization event.

Default severity level: **information**, color code: green.

Typical Causes

Indicates a High WAN Port Outbound Utilization alarm has been cleared as the port utilization is now below the high threshold value.

Actions

None.

WAN Port Low Inbound Utilization

Indicates that a WAN port (link) is experiencing low levels of inbound utilization (bandwidth usage).

Default severity level: **major**, color code: amber.

Typical Causes

Route changes, outages upstream of the link, server problems.

Actions

This problem may be symptomatic of an issue elsewhere in the network. Check through other events that have recently been reported if excessively low levels of utilization persist.

WAN Port Low Inbound Utilization Cleared

Indicates that a WAN port (link) that was experiencing low levels of utilization is now receiving higher traffic volumes.

Default severity level: **information**, color code: green.

Typical Causes

Increased application traffic.

Actions

None.

WAN Port Low Outbound Utilization

Indicates that a WAN port (link) is experiencing low levels of outbound utilization (bandwidth usage).

Default severity level: **major**, color code: amber.

Typical Causes

Route changes, outages upstream of the link, server problems.

Actions

This problem may be symptomatic of an issue elsewhere in the network. Check through other events that have recently been reported if excessively low levels of utilization persist.

WAN Port Low Outbound Utilization Cleared

Indicates that a WAN port (link) that was experiencing low levels of utilization is now transmitting higher traffic volumes.

Default severity level: **information**, color code: green.

Typical Causes

Increased application traffic.

Actions

None.

Wireless Controller High Number of Connected APs

Indicates the number of connected access points is greater than the set threshold, by default 1000.

Default severity level: **major**, color code: amber.

Typical Causes

Changes in wireless usage have occurred since the network was designed.

Actions

Investigate the attached AP history of the device.

Wireless Controller High Number of Connected APs Cleared

Indicates the number of connected access points was greater than the set threshold, by default 1000, but is now below that boundary.

Default severity level: **information**, color code: green.

Typical Causes

The number of APs attached to the Wireless Controller has returned to an acceptable level.

Actions

None.

2 Incidents Listing

Entuity is shipped with an extensive set of system events together with their associated incidents. Incidents are raised, updated and closed by events. Incidents are part of the event system event project and are therefore completely configurable to anyone with the appropriate access rights.

Each incident and event is listed with its unique type identifier. Although often incident and event types share the same number, within Entuity the different contexts ensure they are unique. Type identifiers are useful when building rules.

Context sensitive help is available for all incidents shipped with Entuity:

- 1) From the event viewer highlight an incident and then from the context menu click **Help**.

Each event name is a hyperlink to the help on that event.

AP Antenna Channel Change Frequency High Incident

Incident ID: 842

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
AP Antenna Channel Change Frequency High	842	1

Event Name	Closing Event Type	Number Required
AP Antenna Channel Change Frequency High Cleared	843	1

AP Antenna Host Count Abnormality Incident

Incident ID: 804

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
AP Antenna Host Count High	804	1
AP Antenna Host Count Low	806	1

Event Name	Closing Event Type	Number Required
AP Antenna Host Count High Cleared	805	1
AP Antenna Host Count Low Cleared	807	1

AP Antenna Offline Incident

Incident ID: 846

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
AP Antenna Offline	846	1

Event Name	Closing Event Type	Number Required
AP Antenna Online	847	1

AP Antenna Power Change Frequency High Incident

Incident ID: 840

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
AP Antenna Power Change Frequency High	840	1

Event Name	Closing Event Type	Number Required
AP Antenna Power Change Frequency High Cleared	841	1

AP Host Count Abnormality Incident

Incident ID: 832

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
AP Host Count High	832	1
AP Host Count Low	834	1

Event Name	Closing Event Type	Number Required
AP Host Count High Cleared	833	1
AP Host Count Low Cleared	835	1

AP Not Associated With Controller Incident

Incident ID: 844

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
AP Not Associated With Controller	844	1

Event Name	Closing Event Type	Number Required
AP Associated With Controller	845	1

ATM VCC Inbound Utilization Abnormality Incident

Incident ID: 46

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
ATM VCC Low Inbound Utilization	48	1
ATM VCC High Inbound Utilization	46	1

Event Name	Closing Event Type	Number Required
ATM VCC Low Inbound Utilization Cleared	49	1
ATM VCC High Inbound Utilization Cleared	47	1

ATM VCC Link Down Incident

Incident ID: 54

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
ATM VCC Link Down	54	1

Event Name	Closing Event Type	Number Required
ATM VCC Link Up	55	1

ATM VCC Outbound Utilization Abnormality Incident

Incident ID: 50

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
ATM VCC Low Outbound Utilization	52	1
ATM VCC High Outbound Utilization	50	1

Event Name	Closing Event Type	Number Required
ATM VCC Low Outbound Utilization Cleared	53	1
ATM VCC High Outbound Utilization Cleared	51	1

AvailMonitor Application Problem Incident

Incident ID: 917505

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
AvailMonitor Application Unavailable	917506	1
AvailMonitor High Latency Reaching Application	917507	1

Event Name	Closing Event Type	Number Required
AvailMonitor Application Available	917505	1
AvailMonitor High Latency Reaching Application Cleared	917508	1

AvailMonitor High Latency Incident

Incident ID: 750

Incident Ageout: 300 Time unit: seconds

Event Name	Raising Event Type	Number Required
AvailMonitor High Latency	750	1

Event Name	Closing Event Type	Number Required
AvailMonitor Normal Latency	751	1

AvailMonitor Low View Device Reachability Incident

Incident ID: 80

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
AvailMonitor Low View Device Reachability	80	1

Event Name	Closing Event Type	Number Required
AvailMonitor Normal View Device Reachability	81	1

Awap Host Count Abnormality Incident

Incident ID: 800

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
AWAP Host Count Low	802	1
AWAP Host Count High	800	1

Event Name	Closing Event Type	Number Required
AWAP Host Count Low Cleared	803	1
AWAP Host Count High Cleared	801	1

Background Reachability Check Failure Incident

Incident ID: 786454

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Background Reachability Check Failed	786454	1

Event Name	Closing Event Type	Number Required
Background Reachability Check Succeeded	786455	1

Backplane Bus A High Utilization Incident

Incident ID: 655438

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Backplane Bus A High Utilization	655438	1

Event Name	Closing Event Type	Number Required
Backplane Bus A High Utilization Cleared	655439	1

Backplane Bus B High Utilization Incident

Incident ID: 655440

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Backplane Bus B High Utilization	655440	1

Event Name	Closing Event Type	Number Required
Backplane Bus B High Utilization Cleared	655441	1

Backplane Bus C High Utilization Incident

Incident ID: 655442

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Backplane Bus C High Utilization	655442	1

Event Name	Closing Event Type	Number Required
Backplane Bus C High Utilization Cleared	655443	1

Backplane System Bus High Utilization Incident

Incident ID: 655436

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Backplane System Bus High Utilization	655436	1

Event Name	Closing Event Type	Number Required
Backplane System Bus High Utilization Cleared	655437	1

BGP Peer Briefly Established Incident

Incident ID: 133

Incident Ageout: 300 Time unit: seconds

Event Name	Raising Event Type	Number Required
BGP Peer Briefly Established	133	1

BGP Peer Briefly Not Established Incident

Incident ID: 132

Incident Ageout: 300 Time unit: seconds

Event Name	Raising Event Type	Number Required
BGP Peer Briefly Not Established	132	1

BGP Peer Disappeared Incident

Incident ID: 130

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
BGP Peer Disappeared	130	1

BGP Peer Newly Discovered Incident

Incident ID: 131

Incident Ageout: 60 Time unit: seconds

Event Name	Raising Event Type	Number Required
BGP Peer Newly Discovered	131	1

BGP Peer Not Established Incident

Incident ID: 128

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
BGP Peer Not Established	128	1

Event Name	Closing Event Type	Number Required
BGP Peer Established	129	1

BladeCenter Blade + 1.25V Rail Voltage Problem Incident

Incident ID: 547

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Blade + 1.25V Rail Low Voltage	549	1
BladeCenter Blade + 1.25V Rail High Voltage	547	1

Event Name	Closing Event Type	Number Required
BladeCenter Blade + 1.25V Rail Low Voltage Cleared	550	1
BladeCenter Blade + 1.25V Rail High Voltage Cleared	548	1

BladeCenter Blade + 1.5V Rail Voltage Problem Incident

Incident ID: 543

Incident Ageout: Time unit:

Event Name	Raising Event Type	Number Required
BladeCenter Blade +1.5V Rail Low Voltage	545	1
BladeCenter Blade +1.5V Rail High Voltage	543	1

Event Name	Closing Event Type	Number Required
BladeCenter Blade +1.5V Rail Low Voltage Cleared	546	1
BladeCenter Blade +1.5V Rail High Voltage Cleared	544	1

BladeCenter Blade +12V Rail Voltage Problem Incident

Incident ID: 535

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Blade +12V Rail High Voltage	535	1
BladeCenter Blade +12V Rail Low Voltage	537	1

Event Name	Closing Event Type	Number Required
BladeCenter Blade +12V Rail High Voltage Cleared	536	1
BladeCenter Blade +12V Rail Low Voltage Cleared	538	1

BladeCenter Blade +2.5V Rail Voltage Problem Incident

Incident ID: 539

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Blade +2.5V Rail High Voltage	539	1
BladeCenter Blade +2.5V Rail Low Voltage	541	1

Event Name	Closing Event Type	Number Required
BladeCenter Blade +2.5V Rail High Voltage Cleared	540	1
BladeCenter Blade +2.5V Rail Low Voltage Cleared	542	1

BladeCenter Blade +3.3V Rail Voltage Problem Incident

Incident ID: 531

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Blade +3.3V Rail Low Voltage	533	1
BladeCenter Blade +3.3V Rail High Voltage	531	1

Event Name	Closing Event Type	Number Required
BladeCenter Blade +3.3V Rail Low Voltage Cleared	534	1
BladeCenter Blade +3.3V Rail High Voltage Cleared	532	1

BladeCenter Blade +5V Rail Voltage Problem Incident

Incident ID: 527

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Blade +5V Rail High Voltage	527	1
BladeCenter Blade +5V Rail Low Voltage	529	1

Event Name	Closing Event Type	Number Required
BladeCenter Blade +5V Rail High Voltage Cleared	528	1
BladeCenter Blade +5V Rail Low Voltage Cleared	530	1

BladeCenter Blade Powered Off Incident

Incident ID: 519

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Blade Powered Off	519	1

Event Name	Closing Event Type	Number Required
BladeCenter Blade Powered On	520	1

BladeCenter Blower Problem Incident

Incident ID: 512

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Blower Failed	514	1
BladeCenter Blower Slow	512	1

Event Name	Closing Event Type	Number Required
BladeCenter Blower Ok	513	1

BladeCenter CPU1 High Temperature Incident

Incident ID: 521

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter CPU1 High Temperature	521	1

Event Name	Closing Event Type	Number Required
BladeCenter CPU1 High Temperature Cleared	522	1

BladeCenter CPU2 High Temperature Incident

Incident ID: 523

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter CPU2 High Temperature	523	1

Event Name	Closing Event Type	Number Required
BladeCenter CPU2 High Temperature Cleared	524	1

BladeCenter Chassis + 1.8V Rail Voltage Problem Incident

Incident ID: 567

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Chassis +1.8V Rail Low Voltage	569	1
BladeCenter Chassis +1.8V Rail High Voltage	567	1

Event Name	Closing Event Type	Number Required
BladeCenter Chassis +1.8V Rail Low Voltage Cleared	570	1
BladeCenter Chassis +1.8V Rail High Voltage Cleared	568	1

BladeCenter Chassis +12V Rail Voltage Problem Incident

Incident ID: 559

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Chassis +12V Rail Low Voltage	561	1
BladeCenter Chassis +12V Rail High Voltage	559	1

Event Name	Closing Event Type	Number Required
BladeCenter Chassis +12V Rail Low Voltage Cleared	562	1
BladeCenter Chassis +12V Rail High Voltage Cleared	560	1

BladeCenter Chassis +2.5V Rail Voltage Problem Incident

Incident ID: 563

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Chassis +2.5V Rail High Voltage	563	1
BladeCenter Chassis +2.5V Rail Low Voltage	565	1

Event Name	Closing Event Type	Number Required
BladeCenter Chassis +2.5V Rail High Voltage Cleared	564	1
BladeCenter Chassis +2.5V Rail Low Voltage Cleared	566	1

BladeCenter Chassis +3.3V Rail Voltage Problem Incident

Incident ID: 555

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Chassis +3.3V Rail High Voltage	555	1
BladeCenter Chassis +3.3V Rail Low Voltage	557	1

Event Name	Closing Event Type	Number Required
BladeCenter Chassis +3.3V Rail High Voltage Cleared	556	1
BladeCenter Chassis +3.3V Rail Low Voltage Cleared	558	1

BladeCenter Chassis +5V Rail Voltage Problem Incident

Incident ID: 551

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Chassis +5V Rail Low Voltage	553	1
BladeCenter Chassis +5V Rail High Voltage	551	1

Event Name	Closing Event Type	Number Required
BladeCenter Chassis +5V Rail Low Voltage Cleared	554	1
BladeCenter Chassis +5V Rail High Voltage Cleared	552	1

BladeCenter Chassis -5V Rail Voltage Problem Incident

Incident ID: 571

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Chassis -5V Rail High Voltage	571	1
BladeCenter Chassis -5V Rail Low Voltage	573	1

Event Name	Closing Event Type	Number Required
BladeCenter Chassis -5V Rail High Voltage Cleared	572	1
BladeCenter Chassis -5V Rail Low Voltage Cleared	574	1

BladeCenter DASD1 High Temperature Incident

Incident ID: 525

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter DASD1 High Temperature	525	1

Event Name	Closing Event Type	Number Required
BladeCenter DASD1 High Temperature Cleared	526	1

BladeCenter Front Panel High Temperature Incident

Incident ID: 517

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Front Panel High Temperature	517	1

Event Name	Closing Event Type	Number Required
BladeCenter Front Panel High Temperature Cleared	518	1

BladeCenter Management Module High Temperature Incident

Incident ID: 515

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
BladeCenter Management Module High Temperature	515	1

Event Name	Closing Event Type	Number Required
BladeCenter Management Module High Temperature Cleared	516	1

CM Configuration Includes Policy Exclusion Incident

Incident ID: 346

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
CM Configuration Includes Policy Exclusion	346	1

CM Configuration Missing Policy Mandated Statement Incident

Incident ID: 345

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
CM Configuration Missing Policy Mandated Statement	345	1

CM Firmware Version Changed Incident

Incident ID: 350

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
CM Firmware Version Changed	350	1

CM Running Configuration Changed Incident

Incident ID: 342

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
CM Running Configuration Changed	342	1

CM Running Configuration Retrieval Failed Incident

Incident ID: 348

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
CM Running Configuration Retrieval Failed	348	1

CM Startup Configuration Changed Incident

Incident ID: 341

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
CM Startup Configuration Changed	341	1

CM Startup Configuration Retrieval Failed Incident

Incident ID: 349

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
CM Startup Configuration Retrieval Failed	349	1

CM Unsaved Configuration Incident

Incident ID: 343

Incident Ageout: 129600 Time unit: seconds

Event Name	Raising Event Type	Number Required
CM Unsaved Configuration	343	1

Event Name	Closing Event Type	Number Required
CM Previously Unsaved Configuration Saved	344	1

CM Job Succeeded Incident

Incident ID: 352

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Config Mgmt Job Succeeded	352	1

CM Job Failed Incident

Incident ID: 351

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Config Mgmt Job Failed	351	1

CUCM CPU High Utilization Incident

Incident ID: 416

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
CUCM CPU High Utilization	416	1

Event Name	Closing Event Type	Number Required
CUCM CPU High Utilization Cleared	417	1

CUCM CTI Device Not Registered Incident

Incident ID: 402

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
CUCM CTI Device Not Registered	402	1

Event Name	Raising Event Type	Number Required
CUCM CTI Device Registered	403	1

CUCM Gatekeeper Not Registered Incident

Incident ID: 404

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
CUCM Gatekeeper Not Registered	404	1

Event Name	Closing Event Type	Number Required
CUCM Gatekeeper Registered	405	1

CUCM Gateway Not Registered Incident

Incident ID: 410

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
CUCM Gateway Not Registered	410	1

Event Name	Closing Event Type	Number Required
CUCM Gateway Registered	411	1

CUCM H323 Device Not Registered Incident

Incident ID: 406

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
CUCM H.323 Device Not Registered	406	1

Event Name	Closing Event Type	Number Required
CUCM H.323 Device Registered	407	1

CUCM Media Device Not Registered Incident

Incident ID: 408

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
CUCM Media Device Not Registered	408	1

Event Name	Closing Event Type	Number Required
CUCM Media Device Registered	409	1

CUCM Phone Not Registered Incident

Incident ID: 400

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
CUCM Phone Not Registered	400	1

Event Name	Closing Event Type	Number Required
CUCM Phone Registered	401	1

CUCM Process Memory High Utilization Incident

Incident ID: 418

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
CUCM Process Memory High Utilization	418	1

Event Name	Closing Event Type	Number Required
CUCM Process Memory High Utilization Cleared	419	1

CUCM Voicemail Device Not Registered Incident

Incident ID: 412

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
CUCM Voicemail Device Not Registered	412	1

Event Name	Closing Event Type	Number Required
CUCM Voicemail Device Registered	413	1

Chassis Alarm Incident

Incident ID: 655395

Incident Ageout: 5400 Time unit: seconds

Event Name	Raising Event Type	Number Required
Chassis Major Alarm	655397	1
Chassis Minor Alarm	655395	1

Event Name	Closing Event Type	Number Required
Chassis Minor Alarm Cleared	655396	1
Chassis Major Alarm Cleared	655398	1

Chassis Fan Status Problem Incident

Incident ID: 655390

Incident Ageout: 5400 Time unit: seconds

Event Name	Raising Event Type	Number Required
Chassis Fan Status Unknown	655391	1
Chassis Fan Minor Fault	655392	1
Chassis Fan Major Fault	655393	1

Event Name	Closing Event Type	Number Required
Chassis Fan OK	655390	1

Chassis Temperature Alarm Incident

Incident ID: 655410

Incident Ageout: 5400 Time unit: seconds

Event Name	Raising Event Type	Number Required
Chassis Temperature Critical Alarm	655412	1
Chassis Temperature Alarm	655410	1

Event Name	Closing Event Type	Number Required
Chassis Temperature Alarm Cleared	655411	1

Device Clock Inconsistency Incident

Incident ID: 655444

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device Clock Inconsistency	655444	1

Device Average CPU Utilization High Incident

Incident ID: 655414

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device Average CPU Utilization Critical	655460	1
Device Average CPU Utilization High	655415	1

Event Name	Closing Event Type	Number Required
Device Average CPU Utilization Cleared	655414	1

Device Average Memory Usage High Incident

Incident ID: 655416

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device Average Memory Usage Critical	655461	1
Device Average Memory Usage High	655417	1

Event Name	Closing Event Type	Number Required
Device Average Memory Usage Cleared	655416	1

Device Fan Failure Incident

Incident ID: 937

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device Fan Failure	938	1

Event Name	Closing Event Type	Number Required
Device Fan Failure Cleared	937	1

Device High Active Sessions Incident

Incident ID: 620

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device High Active Sessions	621	1

Event Name	Closing Event Type	Number Required
Device High Active Sessions Cleared	620	1

Device High Authenticated Response Time Incident

Incident ID: 622

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device High Authenticated Response Time	623	1

Event Name	Closing Event Type	Number Required
Device High Authenticated Response Time Cleared	622	1

Device High External URL Response Time Incident

Incident ID: 624

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device High External URL Response Time	625	1

Event Name	Closing Event Type	Number Required
Device High External URL Response Time Cleared	624	1

Device High Messages Received Incident

Incident ID: 626

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device High Messages Received	627	1

Event Name	Closing Event Type	Number Required
Device High Messages Received Cleared	626	1

Device Low Disk Space Incident

Incident ID: 314

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device Low Disk Space	314	1

Event Name	Closing Event Type	Number Required
Device Low Disk Space Cleared	315	1

Device Name Resolution Failure Incident

Incident ID: 655448

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device Name Resolution Failure	655448	1

Event Name	Closing Event Type	Number Required
Device Name Resolution Failure Cleared	655449	1

Device Not Responding to SNMP Incident

Incident ID: 655361

Incident Ageout: None

Event Name	Raising Event Type	Number Required
SNMP Agent Not Responding	655363	1

Event Name	Updating Event Type	Number Required
Device Cold Reboot	655361	1
Device Warm Reboot	655362	1
Device Reboot Detected	655365	1

Event Name	Closing Event Type	Number Required
SNMP Agent Responding	655364	1

Device Port(s) Utilization Accuracy Problem

Incident ID: 655445

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device Port(s) Utilization Accuracy at Risk	655445	1
Device Port(s) Utilization Accuracy Lost	655446	1
Device Port(s) Utilization Missed Due to Slow Response	655447	1

Device Reachability Problems Incident

Incident ID: 655380

Incident Ageout: None

Event Name	Raising Event Type	Number Required
Device Unreachable	655381	1
Device Reachability Degraded	655382	

Event Name	Closing Event Type	Number Required
Device Unreachable Cleared	655380	1

Device Reboot Incident

Incident ID: 655361

Incident Ageout: 300 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device Cold Reboot	655361	1
Device Warm Reboot	655362	1
Device Reboot Detected	655365	1

Device Sensor Non-Operational Incident

Incident ID: 941

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device Sensor Non-Operational	942	1

Event Name	Closing Event Type	Number Required
Device Sensor Non-Operational Cleared	941	1

Device Sensor Warning Value Incident

Incident ID: 939

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Device Sensor Warning Value	940	1

Event Name	Closing Event Type	Number Required
Device Sensor Value Cleared	939	1

EGP Neighbor Loss Incident

Incident ID: 655369

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
EGP Neighbor Loss	655369	1

EIGRP Peer Briefly Not Established Incident

Incident ID: 146

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
EIGRP Peer Briefly Not Established	146	1

EIGRP Peer Disappeared Incident

Incident ID: 144

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
EIGRP Peer Disappeared	144	1

EIGRP Peer Newly Discovered Incident

Incident ID: 145

Incident Ageout: 60 Time unit: seconds

Event Name	Raising Event Type	Number Required
EIGRP Peer Newly Discovered	145	1

Entuity License on Remote Server Problem Incident

Incident ID: 786445

Incident Ageout: 3153600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Entuity License on Remote Server Could Not be Updated	786445	1
Entuity License on Remote Server Expired	786446	1

Event Name	Closing Event Type	Number Required
Entuity License on Remote Server Successfully Updated	786447	1

Entuity License Problem Incident

Incident ID: 786448

Incident Ageout: 3153600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Entuity License Not Updated by License Server and Will Expire	786448	1
Entuity License Expired and This Entuity Server is No Longer Operational	786449	1

Event Name	Closing Event Type	Number Required
Entuity License Successfully Updated by License Server	786450	1

Entuity Server Automated Shutdown Incident

Incident ID: 786436

Incident Ageout: 900 Time unit: seconds

Event Name	Raising Event Type	Number Required
Entuity Server Automated Shutdown	786436	1

Entuity Server Component Problem Incident

Incident ID: 786437

Incident Ageout: None

Event Name	Raising Event Type	Number Required
Entuity Server Critical Component Restarting After Failure	786441	1
Entuity Server Component Restarting After Failure	786442	1
Entuity Server Permanent Component Failure	786440	1

Event Name	Updating Event ID	Number Required
Entuity Server Started	786437	1

Entuity Server Database Backup Incident

Incident ID: 786436

Incident Ageout: 43200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Entuity Server Database Backup Failure	786436	1

Entuity Server Disk Space Alert Incident

Incident ID: 786434

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Entuity Server Disk Space Alert	786434	1

Entuity Server Explicit Shutdown Initiated Incident

Incident ID: 786438

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Entuity Server Explicit Shutdown Initiated	786438	1

Entuity Server Internal Event Incident

Incident ID: 786436

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Entuity Server Internal Event	786436	1

Entuity Server License Alert Incident

Incident ID: 786436

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Entuity Server License Alert	786435	1

Entuity Server Shutdown Forced by Critical Failure to Restart Incident

Incident ID: 786439

Incident Ageout: None

Event Name	Raising Event Type	Number Required
Entuity Server Shutdown Forced By Critical Failure To Restart	786439	1

FR DLCI High BECN Incident

Incident ID: 3

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
FR DLCI High BECN	3	1

Event Name	Closing Event Type	Number Required
FR DLCI High BECN Cleared	4	1

FR DLCI High DE Incident

Incident ID: 5

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
FR DLCI High DE	5	1

Event Name	Closing Event Type	Number Required
FR DLCI High DE Cleared	6	1

FR DLCI High FECN Incident

Incident ID: 1

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
FR DLCI High FECN	1	1

Event Name	Closing Event Type	Number Required
FR DLCI High FECN Cleared	2	1

FR DLCI High Inbound Utilization Incident

Incident ID: 7

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
FR DLCI High Inbound Utilization	7	1

Event Name	Closing Event Type	Number Required
FR DLCI High Inbound Utilization Cleared	8	1

FR DLCI High Outbound Utilization Incident

Incident ID: 9

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
FR DLCI High Outbound Utilization	9	1

Event Name	Closing Event Type	Number Required
FR DLCI High Outbound Utilization Cleared	10	1

FR DLCI Link Down Incident

Incident ID: 11

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
FR DLCI Link Down	11	1

Event Name	Closing Event Type	Number Required
FR DLCI Link UP	12	1

Firewall Access Control Violations High Incident

Incident ID: 900

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Firewall Access Control Violations High	900	1

Event Name	Closing Event Type	Number Required
Firewall Access Control Violations High Cleared	901	1

Firewall High Avail User Set Oper State Non Compliant Incident

Incident ID: 1017

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Firewall High Avail User Set Oper State Non Compliant	1018	1

Event Name	Closing Event Type	Number Required
Firewall High Avail User Set Oper State Compliant	1017	1

Firewall High Current Connections Incident

Incident ID: 906

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Firewall High Current Connections	907	1

Event Name	Closing Event Type	Number Required
Firewall High Current Connections Cleared	906	1

Firewall Overflow and Intrusion Violations High Incident

Incident ID: 902

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Firewall Overflow and Intrusion Violations High	902	1

Event Name	Closing Event Type	Number Required
Firewall Overflow and Intrusion Violations High Cleared	903	1

Firewall URL Alerts High Incident

Incident ID: 904

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Firewall URL Alerts High	904	1

Event Name	Closing Event Type	Number Required
Firewall URL Alerts High Cleared	905	1

HSRP Port Group Activated Incident

Incident ID: 175

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
HSRP Port Group Activated	175	1

HSRP Port Group Deactivated Incident

Incident ID: 176

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
HSRP Port Group Deactivated	176	1

IP SLA Creation Failure Incident

Incident ID: 234

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
IP SLA Creation Failure	234	1

Event Name	Closing Event Type	Number Required
IP SLA Creation Failure Cleared	235	1

IP SLA Low MOS Incident

Incident ID: 238

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
IP SLA Low MOS	238	1

Event Name	Closing Event Type	Number Required
IP SLA Low MOS Cleared	239	1

IP SLA Problem Incident

Incident ID: 230

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
IP SLA High ICPIF	236	1
IP SLA Test Failed	230	1

Event Name	Closing Event Type	Number Required
IP SLA High ICPIF Cleared	237	1

IP SLA Test Failed Incident

Incident ID: 230

Incident Ageout: 450 Time unit: seconds

Event Name	Raising Event Type	Number Required
IP SLA Test Failed	230	1

Event Name	Closing Event Type	Number Required
IP SLA Test Succeeded	231	1

IP SLA Test High Latency Incident

Incident ID: 232

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
IP SLA Test High Latency	232	1

Event Name	Closing Event Type	Number Required
IP SLA Test High Latency Cleared	233	1

IS-IS Peer Not Established Incident

Incident ID: 116

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
IS-IS Peer Not Established	116	1

Event Name	Closing Event Type	Number Required
IS-IS Peer Established	117	1

IS-IS Peer Disappeared Incident

Incident ID: 118

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
IS-IS Peer Disappeared	118	1

IS-IS Peer Newly Discovered Incident

Incident ID: 119

Incident Ageout: 60 Time unit: seconds

Event Name	Raising Event Type	Number Required
IS-IS Peer Newly Discovered	119	1

LAP Antenna Host Count Abnormality Incident

Incident ID: 836

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
LAP Antenna Host Count High	836	1
LAP Antenna Host Count Low	838	1

Event Name	Closing Event Type	Number Required
LAP Antenna Host Count High Cleared	837	1
LAP Antenna Host Count Low Cleared	839	1

Load Balancer High Connection Limit Pkt Drop Rate Incident

Incident ID: 972

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High Connection Limit Pkt Drop Rate	972	1

Event Name	Closing Event Type	Number Required
Load Balancer High Connection Limit Pkt Drop Rate Cleared	973	1

Load Balancer High Inbound Error Rate Incident

Incident ID: 976

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High Inbound Error Rate	976	1

Event Name	Closing Event Type	Number Required
Load Balancer High Inbound Error Rate Cleared	977	1

Load Balancer High License Denied Pkt Rate Incident

Incident ID: 968

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High License Denied Pkt Rate	968	1

Event Name	Raising Event Type	Number Required
Load Balancer High License Denied Pkt Rate Cleared	969	1

Load Balancer High Memory Error Pkt Rate Incident

Incident ID: 970

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High Memory Error Pkt Rate	970	1

Event Name	Closing Event Type	Number Required
Load Balancer High Memory Error Pkt Rate Cleared	971	1

Load Balancer High No Handler Denied Pkt Rate Incident

Incident ID: 966

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High No Handler Denied Pkt Rate	966	1

Event Name	Closing Event Type	Number Required
Load Balancer High No Handler Denied Pkt Rate Cleared	967	1

Load Balancer High Non Syn Denied Pkt Rate Incident

Incident ID: 964

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High Non Syn Denied Pkt Rate	964	1

Event Name	Closing Event Type	Number Required
Load Balancer High Non Syn Denied Pkt Rate Cleared	965	1

Load Balancer High Outbound Error Rate Incident

Incident ID: 978

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High Outbound Error Rate	978	1

Event Name	Closing Event Type	Number Required
Load Balancer High Outbound Error Rate Cleared	979	1

Load Balancer High Packet Drop Rate Incident

Incident ID: 974

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High Packet Drop Rate	974	1

Event Name	Closing Event Type	Number Required
Load Balancer High Packet Drop Rate Cleared	975	1

Load Balancer High SLB SP Current Sessions Incident

Incident ID: 1004

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High SLB SP Current Sessions	1005	1

Event Name	Closing Event Type	Number Required
Load Balancer High SLB SP Current Sessions Cleared	1004	1

Load Balancer High Current Sessions Incident

Incident ID: 660

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High Current Sessions	660	1

Event Name	Closing Event Type	Number Required
Load Balancer High Current Sessions Cleared	661	1

Load Balancer High Maximum Sessions Incident

Incident ID: 662

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High Maximum Sessions	662	1

Event Name	Closing Event Type	Number Required
Load Balancer High Maximum Sessions Cleared	663	1

Load Balancer High Total Errors Incident

Incident ID: 664

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer High Error Count	664	1

Event Name	Closing Event Type	Number Required
Load Balancer High Error Count Cleared	665	1

Load Balancer Pool Member Availability Problem Incident

Incident ID: 1013

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer Pool Critical Member Availability	1015	1
Load Balancer Pool Low Member Availability	1016	1

Event Name	Closing Event Type	Number Required
Load Balancer Pool Critical Services Availability Cleared	1013	1
Load Balancer Pool Low Member Availability Cleared	1014	1

Load Balancer Pool Services Availability Problem Incident

Incident ID: 666

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Load Balancer Pool Critical Services Availability	666	1
Load Balancer Pool Low Services Availability	668	1

Event Name	Closing Event Type	Number Required
Load Balancer Pool Critical Services Availability Cleared	667	1
Load Balancer Pool Low Services Availability Cleared	669	1

MAC Address High Port Count Incident

Incident ID: 524336

Incident Ageout: 300 Time unit: seconds

Event Name	Raising Event Type	Number Required
MAC Address High Port Count	524336	1

Event Name	Closing Event Type	Number Required
MAC Address High Port Count Cleared	524337	1

MAC Address New Incident

Incident ID: 524334

Incident Ageout: 300 Time unit: seconds

Event Name	Raising Event Type	Number Required
MAC Address New	524334	1

MAC Address Port Change Incident

Incident ID: 524332

Incident Ageout: 300 Time unit: seconds

Event Name	Raising Event Type	Number Required
MAC Address Port Change	524332	1

MPLS LDP Entity Errors Incident

Incident ID: 192

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LDP Entity Errors	192	1

Event Name	Closing Event Type	Number Required
MPLS LDP Entity Errors Cleared	193	1

MPLS LDP Entity Non-operational Incident

Incident ID: 182

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LDP Entity Non-operational	182	1

Event Name	Closing Event Type	Number Required
MPLS LDP Entity Operational	183	1

MPLS LDP Entity Rejected Sessions Incident

Incident ID: 190

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LDP Entity Rejected Sessions	190	1

Event Name	Closing Event Type	Number Required
MPLS LDP Entity Rejected Sessions Cleared	191	1

MPLS LDP Entity Shutdown Notifications Received Incident

Incident ID: 194

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LDP Entity Shutdown Notifications Received	194	1

Event Name	Closing Event Type	Number Required
MPLS LDP Entity Shutdown Notifications Received Cleared	195	1

MPLS LDP Entity Shutdown Notifications Sent Incident

Incident ID: 196

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LDP Entity Shutdown Notifications Sent	196	1

Event Name	Closing Event Type	Number Required
MPLS LDP Entity Shutdown Notifications Sent Cleared	197	1

MPLS LDP Peer Non-operational Incident

Incident ID: 180

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LDP Peer Non-operational	180	1

Event Name	Closing Event Type	Number Required
MPLS LDP Peer Operational	181	1

MPLS LDP Peer TLV Errors Incident

Incident ID: 188

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LDP Peer TLV Errors	188	1

Event Name	Closing Event Type	Number Required
MPLS LDP Peer TLV Errors Cleared	189	1

MPLS LDP Peer Unknown Message Types Incident

Incident ID: 186

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LDP Peer Unknown Message Types	186	1

Event Name	Closing Event Type	Number Required
MPLS LDP Peer Unknown Message Types Cleared	187	1

MPLS LSR Interface High Discard Rate (Lookup Failure) Incident

Incident ID: 206

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LSR Interface High Discard Rate (Lookup Failure)	206	1

Event Name	Closing Event Type	Number Required
MPLS LSR Interface High Discard Rate (Lookup Failure) Cleared	207	1

MPLS LSR Interface High Error Free Discard Rate (RX) Incident

Incident ID: 202

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LSR Interface High Error Free Discard Rate (RX)	202	1

Event Name	Closing Event Type	Number Required
MPLS LSR Interface High Error Free Discard Rate (RX) Cleared	203	1

MPLS LSR Interface High Error Free Discard Rate (TX) Incident

Incident ID: 204

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LSR Interface High Error Free Discard Rate (TX)	204	1

Event Name	Closing Event Type	Number Required
MPLS LSR Interface High Error Free Discard Rate (TX) Cleared	205	1

MPLS LSR Interface High Fragmentation Rate Incident

Incident ID: 208

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LSR Interface High Fragmentation Rate	208	1

Event Name	Closing Event Type	Number Required
MPLS LSR Interface High Fragmentation Rate Cleared	209	1

MPLS LSR Interface Low Bandwidth Incident

Incident ID: 198

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LSR Interface Low Bandwidth	198	1

Event Name	Closing Event Type	Number Required
MPLS LSR Interface Low Bandwidth Cleared	199	1

MPLS LSR Interface Low Buffer Space Incident

Incident ID: 200

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LSR Interface Low Buffer Space	200	1

Event Name	Closing Event Type	Number Required
MPLS LSR Interface Low Buffer Space Cleared	201	1

MPLS LSR Platform High Discard Rate (Lookup Failure) Incident

Incident ID: 218

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LSR Platform High Discard Rate (Lookup Failure)	218	1

Event Name	Closing Event Type	Number Required
MPLS LSR Platform High Discard Rate (Lookup Failure) Cleared	219	1

MPLS LSR Platform High Error Free Discard Rate (RX) Incident

Incident ID: 214

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LSR Platform High Error Free Discard Rate (RX)	214	1

Event Name	Closing Event Type	Number Required
MPLS LSR Platform High Error Free Discard Rate (RX) Cleared	215	1

MPLS LSR Platform High Error Free Discard Rate (TX) Incident

Incident ID: 216

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LSR Platform High Error Free Discard Rate (TX)	216	1

Event Name	Closing Event Type	Number Required
MPLS LSR Platform High Error Free Discard Rate (TX) Cleared	217	1

MPLS LSR Platform High Fragmentation Rate Incident

Incident ID: 220

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS LSR Platform High Fragmentation Rate	220	1

Event Name	Closing Event Type	Number Required
MPLS LSR Platform High Fragmentation Rate Cleared	221	1

MPLS VRF High Illegal Label Rate Incident

Incident ID: 224

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS VRF High Illegal Label Rate	224	1

Event Name	Closing Event Type	Number Required
MPLS VRF High Illegal Label Rate Cleared	225	1

MPLS VRF Non-operational Incident

Incident ID: 222

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
MPLS VRF Non-operational	223	1

Event Name	Closing Event Type	Number Required
MPLS VRF Operational	222	1

Memory Low Incident

Incident ID: 655418

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Memory Low	655419	1

Event Name	Closing Event Type	Number Required
Memory Low Cleared	655418	1

Module Disappeared Incident

Incident ID: 912

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Module Disappeared	912	1

Module Discovered Incident

Incident ID: 912

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Module Discovered	912	1

Module Status Problem Incident

Incident ID: 589844

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Module Down	589848	1
Module Major Fault	589847	1
Module Minor Fault	589846	1
Module Status Unknown	589845	1

Event Name	Closing Event Type	Number Required
Module Status OK	589844	1

Network Outage Incident

Incident ID: 983047

Incident Ageout: 0 Time unit: seconds

Event Name	Raising Event Type	Number Required
Network Outage	983047	1

Event Name	Closing Event Type	Number Required
Network Outage Cleared	983048	1

OSPF Peer Briefly Not Established Incident

Incident ID: 164

Incident Ageout: 300 Time unit: seconds

Event Name	Raising Event Type	Number Required
OSPF Peer Briefly Not Established	164	1

OSPF Peer Disappeared Incident

Incident ID: 162

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
OSPF Peer Disappeared	162	1

OSPF Peer Newly Discovered Incident

Incident ID: 163

Incident Ageout: 60 Time unit: seconds

Event Name	Raising Event Type	Number Required
OSPF Peer Newly Discovered	163	1

OSPF Peer Not Established Incident

Incident ID: 160

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
OSPF Peer Not Established	160	1

Event Name	Closing Event Type	Number Required
OSPF Peer Established	161	1

Port Error Disable Alarm Incident

Incident ID: 524328

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port Error Disable Alarm	524328	1

Event Name	Raising Event Type	Number Required
Port Error Disable Alarm Cleared	524329	1

Port High Inbound Discards (Dynamic) Incident

Incident ID: 384

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port High Inbound Discards (Dynamic)	385	1

Event Name	Raising Event Type	Number Required
Port High Inbound Discards (Dynamic) Cleared	384	1

Port High Inbound Fault (Dynamic) Incident

Incident ID: 388

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port High Inbound Fault (Dynamic)	389	1

Event Name	Closing Event Type	Number Required
Port High Inbound Fault (Dynamic) Cleared	388	1

Port High Outbound Discards (Dynamic) Incident

Incident ID: 382

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port High Outbound Discards (Dynamic)	383	1

Event Name	Closing Event Type	Number Required
Port High Outbound Discards (Dynamic) Cleared	382	1

Port High Outbound Fault (Dynamic) Incident

Incident ID: 386

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port High Outbound Fault (Dynamic)	387	1

Event Name	Closing Event Type	Number Required
Port High Outbound Fault (Dynamic) Cleared	386	1

Port Inbound Discards High (Device Congestion) Incident

Incident ID: 524302

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port Inbound Discards High (Device Congestion)	524302	1

Event Name	Closing Event Type	Number Required
Port Inbound Discards High Cleared (No Device Congestion)	524303	1

Port Inbound Fault High (Packet Corruption) Incident

Incident ID: 524298

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port Inbound Fault High (Packet Corruption)	524298	1

Event Name	Raising Event Type	Number Required
Port Inbound Fault High (No Packet Corruption) Cleared	524299	1

Port Inbound Utilization (Dynamic) Abnormality Incident

Incident ID: 394

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port High Inbound Utilization (Dynamic)	397	1
Port Low Inbound Utilization (Dynamic)	395	1

Event Name	Closing Event Type	Number Required
Port High Inbound Utilization (Dynamic) Cleared	396	1
Port Low Inbound Utilization (Dynamic) Cleared	394	1

Port Link Down Incident

Incident ID: 524290

Incident Ageout: 1800 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port Link Down	524290	1

Event Name	Closing Event Type	Number Required
Port Link Up	524291	1

Port Operationally Down Incident

Incident ID: 36

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port Operationally Down	36	1

Event Name	Closing Event Type	Number Required
Port Operationally Down Cleared	37	1

Port Outbound Discards High (Port Congestion) Incident

Incident ID: 524304

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port Outbound Discards High (Port Congestion)	524304	1

Event Name	Closing Event Type	Number Required
Port Outbound Discards High (No Port Congestion) Cleared	524305	1

Port Outbound Fault High (Transmit Errors) Incident

Incident ID: 524300

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port Outbound Fault High (Transmit Errors)	524300	1

Event Name	Closing Event Type	Number Required
Port Outbound Fault High Cleared (No Transmit Errors)	524301	1

Port Outbound Utilization (Dynamic) Abnormality Incident

Incident ID: 390

Incident Ageout: 7200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port High Outbound Utilization (Dynamic)	393	1
Port Low Outbound Utilization (Dynamic)	391	1

Event Name	Closing Event Type	Number Required
Port High Outbound Utilization (Dynamic) Cleared	392	1
Port Low Outbound Utilization (Dynamic) Cleared	390	1

Port Status Problem

Port Status Problem is raised through the application of rules to incoming events. 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.

Incident ID: 524293

Incident Ageout: 172800 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port Flapping	524293	1
Port Down	524290, 1024_36	1

Event Name	Closing Event Type	Number Required
Port Up	524291, 1024_37	1

Power Supply Problem Incident

Incident ID: 655480

Incident Ageout: 5400 Time unit: seconds

Event Name	Raising Event Type	Number Required
Power Supply Minor Fault	655482	1
Power Supply Unknown State	655486	1
Power Supply Major Fault	655484	1

Event Name	Closing Event Type	Number Required
Power Supply OK	655480	1

Port Utilization Abnormality Incident

Incident ID: 524310

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
Port Utilization High	524310	1
Port Utilization Low	524312	1

Event Name	Closing Event Type	Number Required
Port Utilization High Cleared	524311	1
Port Utilization Low Cleared	524313	1

Processor Utilization High Incident

Incident ID: 655420

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Processor Utilization High	655420	1

Event Name	Closing Event Type	Number Required
Processor Utilization High Cleared	655421	1

QoS Bandwidth Problem Incident

Incident ID: 56

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
QoS At Bandwidth Limit	57	1
QoS Above Bandwidth Limit	56	1

Event Name	Closing Event Type	Number Required
QoS Under Bandwidth Limit	58	1

QoS Class Bit Rate High Incident

Incident ID: 100

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
QoS Class Bit Rate High	100	1

Event Name	Closing Event Type	Number Required
QoS Class Bit Rate High Cleared	101	1

QoS Class Drop Bit Rate High Incident

Incident ID: 102

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
QoS Class Drop Bit Rate High	102	1

Event Name	Closing Event Type	Number Required
QoS Class Drop Bit Rate High Cleared	103	1

QoS Class Drop Packet Rate (Buffer Shortage) High Incident

Incident ID: 104

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
QoS Class Drop Packet Rate (Buffer Shortage) High	104	1

Event Name	Closing Event Type	Number Required
QoS Class Drop Packet Rate (Buffer Shortage) High Cleared	105	1

QoS Queue Drop Bit Rate High Incident

Incident ID: 106

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
QoS Queue Drop Bit Rate High	106	1

Event Name	Closing Event Type	Number Required
QoS Queue Drop Bit Rate High Cleared	107	1

Routing Broadcast Traffic High Incident

Incident ID: 524322

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Routing Broadcast Traffic High	524322	1

Event Name	Closing Event Type	Number Required
Routing Broadcast Traffic High Cleared	524323	1

Routing High No Routes To IP Destination Incident

Incident ID: 655432

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Routing High No Routes to IP Destination	655432	1

Event Name	Closing Event Type	Number Required
Routing High No Routes to IP Destination Cleared	655433	1

Routing ICMP High Redirects Incident

Incident ID: 655434

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Routing ICMP High Redirects	655434	1

Event Name	Closing Event Type	Number Required
Routing ICMP High Redirects Cleared	655435	1

Routing ICMP High TTL Exceeds Incident

Incident ID: 655430

Incident Ageout: 600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Routing ICMP High TTL Exceeds	655430	1

Event Name	Raising Event Type	Number Required
Routing ICMP High TTL Exceeds Cleared	655431	1

Service State Problem Incident

Incident ID: 919

Incident Ageout: 36000 Time unit: seconds

Event Name	Raising Event Type	Number Required
Service Down	919	1
Service State Degraded	918	1
Service State Unknown	921	1

Event Name	Closing Event Type	Number Required
Service State Off	917	1
Service Up	920	1

SNMP Agent Restart Detected Incident

Incident ID: 254

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
SNMP Agent Restart Detected	254	1

SNMP Authentication Failure Incident

Incident ID: 655368

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
SNMP Authentication Failure	655368	1

SNMP Response Time High Incident

Incident ID: 655377

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
SNMP Response Time High	655377	1

Event Name	Closing Event Type	Number Required
SNMP Response Time High Cleared	655378	1

SNMP v3 Duplicate Engine ID Incident

Incident ID: 655450

Incident Ageout: 5400 Time unit: seconds

Event Name	Raising Event Type	Number Required
SNMP v3 Duplicate Engine ID	655450	1

SSL Certificate Problem Incident

Incident ID: 1023

Incident Ageout: None

Event Name	Raising Event Type	Number Required
SSL Certificate Expiring	1024	1
SSL Certificate Expired	1023	1

SSL Proxy Service Administrative Unavailable to SNMP Poll Incident

Incident ID: 1021

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
SSL Proxy Service Administrative Unavailable to SNMP Poll	1022	1

Event Name	Closing Event Type	Number Required
SSL Proxy Service Administrative Available to SNMP Poll	1021	1

SSL Proxy Service Operational Unavailable to SNMP Poll Incident

Incident ID: 1019

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
SSL Proxy Service Operational Unavailable to SNMP Poll	1020	1

Event Name	Closing Event Type	Number Required
SSL Proxy Service Operational Available to SNMP Poll	1019	1

STP Topology Change Incident

Incident ID: 720897

Incident Ageout: None

Event Name	Raising Event Type	Number Required
STP VLAN Topology Change	720898	1
STP New Root Device	720897	1

Syslog Alert

Incident ID: 1048578

Incident Ageout: 1200 Time unit: seconds

Syslog Name	Raising Syslog Type	Number Required
Syslog Alert Event	1048578	1

Syslog Critical

Incident ID: 1048579

Incident Ageout: 1200 Time unit: seconds

Syslog Name	Raising Syslog Type	Number Required
Syslog Critical Events	1048579	1

Syslog Debug

Incident ID: 1048584

Incident Ageout: 1200 Time unit: seconds

Syslog Name	Raising Syslog Type	Number Required
Syslog Debug Events	1048584	1

Syslog Emergency

Incident ID: 1048577

Incident Ageout: 1200 Time unit: seconds

Syslog Name	Raising Syslog Type	Number Required
Syslog Emergency Event	1048577	1

Syslog Error

Incident ID: 1048580

Incident Ageout: 1200 Time unit: seconds

Syslog Name	Raising Syslog Type	Number Required
Syslog Error Events	1048580	1

Syslog Information

Incident ID: 1048583

Incident Ageout: 1200 Time unit: seconds

Syslog Name	Raising Syslog Type	Number Required
Syslog Information Events	1048583	1

Syslog Notice

Incident ID: 1048582

Incident Ageout: 1200 Time unit: seconds

Syslog Name	Raising Syslog Type	Number Required
Syslog Notice Events	1048582	1

Syslog Warning

Incident ID: 1048581

Incident Ageout: 1200 Time unit: seconds

Syslog Name	Raising Syslog Type	Number Required
Syslog Warning Events	1048581	1

UCS Blade Status Incident

Incident ID: 715

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
UCS Blade Down	719	1
UCS Blade Major Fault	718	1
UCS Blade Minor Fault	717	1
UCS Blade Status Unknown	716	1

Event Name	Closing Event Type	Number Required
UCS Blade OK	715	1

UCS Chassis Status Incident

Incident ID: 680

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
UCS Chassis Down	684	1
UCS Chassis Major Fault	683	1
UCS Chassis Minor Fault	682	1
UCS Chassis Status Unknown	681	1

Event Name	Closing Event Type	Number Required
UCS Chassis Status OK	680	1

UCS Fabric Extender Status Incident

Incident ID: 705

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
UCS Fabric Extender Down	709	1
UCS Fabric Extender Major Fault	708	1
UCS Fabric Extender Minor Fault	707	1
UCS Fabric Extender Status Unknown	706	1

Event Name	Closing Event Type	Number Required
UCS Fabric Extender Status OK	705	1

UCS Fan Module Status Incident

Incident ID: 690

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
UCS Fan Module Down	694	1
UCS Fan Module Major Fault	693	1
UCS Fan Module Minor Fault	692	1
UCS Fan Module Status Unknown	691	1

Event Name	Closing Event Type	Number Required
UCS Fan Module Status OK	690	1

UCS Fan Status Incident

Incident ID: 695

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
UCS Fan Down	699	1
UCS Fan Major Fault	698	1
UCS Fan Minor Fault	697	1
UCS Fan Status Unknown	696	1

Event Name	Closing Event Type	Number Required
UCS Fan Status OK	695	1

UCS Local Disk Status Incident

Incident ID: 710

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
UCS Local Disk Down	714	1
UCS Local Disk Major Fault	713	1
UCS Local Disk Minor Fault	712	1
UCS Local Disk Unknown	711	1

Event Name	Closing Event Type	Number Required
UCS Local Disk OK	710	1

UCS Power Supply Status Problem Incident

Incident ID: 685

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
UCS PSU Down	689	1
UCS PSU Major Fault	688	1
UCS PSU Minor Fault	687	1
UCS PSU Unknown	686	1

Event Name	Closing Event Type	Number Required
UCS PSU OK	685	1

UCS Switch Card Status Incident

Incident ID: 700

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
UCS Switch Card Down	704	1

UCS Switch Card Major Fault	703	1
UCS Switch Card Minor Fault	702	1
UCS Switch Card Status Unknown	701	1

Event Name	Closing Event Type	Number Required
UCS Switch Card Status OK	700	1

Unknown Trap Incident

Incident ID: 655370

Incident Ageout: 2400 Time unit: seconds

Event Name	Raising Event Type	Number Required
Unknown Trap	655370	1

User Defined Attribute Status Incident

Incident ID: 356

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
User Defined Attribute State Down	358	1
User Defined Attribute State Disabled	357	1
User Defined Attribute State Other	356	1

Event Name	Closing Event Type	Number Required
User Defined Attribute State Up	359	1

User Defined Attribute Value Abnormality Incident

Incident ID: 360

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
User Defined Attribute Value Critical	364	1

User Defined Attribute Value High	363	1
User Defined Attribute Value Warning	362	1
User Defined Attribute Value Low	361	1

Event Name	Closing Event Type	Number Required
User Defined Attribute Value Abnormality Cleared	360	1

Virtualization Connection Failed Incident

Incident ID: 64

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
Virtualization Connection Failed	65	1

Event Name	Closing Event Type	Number Required
Virtualization Connection Success	64	1

VM Guest Memory High Incident

Incident ID: 983116

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
VM Guest Memory High	983116	1

Event Name	Closing Event Type	Number Required
VM Guest Memory High Cleared	983115	1

VM Moved Incident

Incident ID: 983103

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
Virtual Machine Moved	983103	1

VM Power Status Changed Incident

Incident ID: 983109

Incident Ageout: 86400 Time unit: seconds

Event Name	Raising Event Type	Number Required
Virtual Machine Powered Off	983110	1

Event Name	Closing Event Type	Number Required
Virtual Machine Powered On	983109	1

VPN High Active Tunnels Incident

Incident ID: 606

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
VM Guest Memory High	607	1

Event Name	Closing Event Type	Number Required
VM Guest Memory High Cleared	606	1

VPN Load Average High Incident

Incident ID: 600

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
VPN Load Average High	600	1

Event Name	Closing Event Type	Number Required
VPN Load Average High Cleared	601	1

VPN Network Port Utilization High Incident

Incident ID: 604

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
VPN Network Port Utilization High	604	1

Event Name	Closing Event Type	Number Required
VPN Network Port Utilization High Cleared	605	1

VPN Tunnel Usage High Incident

Incident ID: 602

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
VPN Tunnel Usage High	602	1

Event Name	Closing Event Type	Number Required
VPN Tunnel Usage High Cleared	603	1

WAN Port High Inbound Discards Incident

Incident ID: 32

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
WAN Port High Inbound Discards	32	1

Event Name	Closing Event Type	Number Required
WAN Port High Inbound Discards Cleared	33	1

WAN Port High Inbound Errors Incident

Incident ID: 28

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
WAN Port High Inbound Errors	28	1

Event Name	Closing Event Type	Number Required
WAN Port High Inbound Errors Cleared	29	1

WAN Port High Outbound Discards Incident

Incident ID: 34

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
WAN Port High Outbound Discards	34	1

Event Name	Closing Event Type	Number Required
WAN Port High Outbound Discards Cleared	35	1

WAN Port High Outbound Errors Incident

Incident ID: 30

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
WAN Port High Outbound Errors	30	1

Event Name	Closing Event Type	Number Required
WAN Port High Outbound Errors Cleared	31	1

WAN Port Inbound Utilization Abnormality Incident

Incident ID: 20

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
WAN Port High Inbound Utilization	20	1
WAN Port Low Inbound Utilization	22	1

Event Name	Closing Event Type	Number Required
WAN Port High Inbound Utilization Cleared	21	1
WAN Port Low Inbound Utilization Cleared	23	1

WAN Port Outbound Utilization Abnormality Incident

Incident ID: 24

Incident Ageout: 1200 Time unit: seconds

Event Name	Raising Event Type	Number Required
WAN Port High Outbound Utilization	24	1
WAN Port Low Outbound Utilization	26	1

Event Name	Closing Event Type	Number Required
WAN Port High Outbound Utilization Cleared	25	1
WAN Port Low Outbound Utilization Cleared	27	1

Wireless Controller High Number of Connected APs Incident

Incident ID: 810

Incident Ageout: 3600 Time unit: seconds

Event Name	Raising Event Type	Number Required
Wireless Controller High Number of Connected APs	811	1

Event Name	Closing Event Type	Number Required
Wireless Controller High Number of Connected APs Cleared	810	1

3 Event Groups, IDs and Severity

In Entuity events are uniquely identified by the combination of their event group, `${event.PAPIEventGroup}`, and their own event identifier within that group, `${event.PAPIEventID}`.

Event Groups

The Event Groups table lists the available event groups. Entuity uses the event type group to populate event source information.

Group ID	Event Type Groups
2	Port
4	Module
8	Device
16	VLAN
32	Entuity Server
64	Syslogger
256	Availability Monitor Application
512	Availability Monitor IP Address
1024	StormWorks
2048	Open Trap Receiver

Table 1 Event Groups

Event and Incident Severity Levels

Severity levels are associated to events. Incidents inherit the highest severity level of the events that raised or updated its status.

The Event Severity table matches the severity level to its description. Entuity has two event severity levels, the display event severity level and an internal severity level. You only require the internal event severity level when forwarding events to third party software and wanting to forward event severity or when adjusting the severity level through the Event System.

Entuity also includes one event that does not have a severity level, Missing Events. This indicates Entuity has raised an event for which it does not have a record for that type in its database. This may happen, for example, when creating an event through the Open Trap Receiver and the event is raised before Event Viewer has updated its tables to recognize the event. After the next refresh the event would be properly recognized.

Display Severity	Internal Severity	Color Code	Description
1	2	Green	Information or Cleared
2	4	Yellow	Minor
3	6	Amber	Major
4	8	Orange	Severe
5	10	Red	Critical

Table 2 Event Severity

Event Type Identifiers

This table lists events by description and then details each event's Group ID, Event ID and internal severity level. Entuity has two methods of representing the event type identifier either it is a combination of the event and group identifiers or a single identifier of the same format as the incident identifier.

Event Name	Group ID	Event ID	Internal Severity
AP Antenna Channel Change Frequency High	1024	842	4
AP Antenna Channel Change Frequency High Cleared	1024	843	2
AP Antenna Host Count High	1024	804	4
AP Antenna Host Count High Cleared	1024	805	2
AP Antenna Host Count Low	1024	806	4
AP Antenna Host Count Low Cleared	1024	807	2
AP Antenna Offline	1024	846	4
AP Antenna Online	1024	847	2
AP Antenna Power Change Frequency High	1024	840	4
AP Antenna Power Change Frequency High Cleared	1024	841	2
AP Associated With Controller	1024	845	4
AP Host Count High	1024	832	4
AP Host Count High Cleared	1024	833	2
AP Host Count Low	1024	834	4
AP Host Count Low Cleared	1024	835	2
AP Not Associated With Controller	1024	844	2
ATM VCC High Inbound Utilization	1024	46	6
ATM VCC High Inbound Utilization Cleared	1024	47	2
ATM VCC High Outbound Utilization	1024	50	6
ATM VCC High Outbound Utilization Cleared	1024	51	2

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
ATM VCC Link Down	1024	54	8
ATM VCC Link Up	1024	55	2
ATM VCC Low Inbound Utilization	1024	48	6
ATM VCC Low Inbound Utilization Cleared	1024	49	2
ATM VCC Low Outbound Utilization	1024	52	6
ATM VCC Low Outbound Utilization Cleared	1024	53	2
AvailMonitor Application Available	256	1	2
AvailMonitor Application Unavailable	256	2	8
AvailMonitor Falling Average Latency	1024	753	4
AvailMonitor High Latency	1024	750	8
AvailMonitor High Latency Reaching Application	256	3	8
AvailMonitor High Latency Reaching Application Cleared	256	4	2
AvailMonitor Low View Device Reachability	1024	80	8
AvailMonitor Normal Latency	1024	751	4
AvailMonitor Normal View Device Reachability	1024	81	4
AvailMonitor Rising Average Latency	1024	752	8
AvailMonitor Rising Trend in Average Latency	1024	754	8
AWAP Host Count High	1024	800	4
AWAP Host Count High Cleared	1024	801	2
AWAP Host Count Low	1024	802	4
AWAP Host Count Low Cleared	1024	803	2
Backplane Bus A High Utilization	8	78	4
Backplane Bus A High Utilization Cleared	8	79	2
Backplane Bus B High Utilization	8	80	4
Backplane Bus B High Utilization Cleared	8	81	2
Backplane Bus C High Utilization	8	82	4
Backplane Bus C High Utilization Cleared	8	83	2
Backplane System Bus High Utilization	8	76	4
Backplane System Bus High Utilization Cleared	8	77	2
BGP Peer Briefly Established	1024	133	10
BGP Peer Briefly Not Established	1024	132	10
BGP Peer Disappeared	1024	130	10
BGP Peer Established	1024	129	4
BGP Peer Newly Discovered	1024	131	4

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
BGP Peer Not Established	1024	128	10
BladeCenter Blade +1.25V Rail High Voltage	1024	547	8
BladeCenter Blade +1.25V Rail High Voltage Cleared	1024	548	2
BladeCenter Blade +1.25V Rail Low Voltage	1024	549	8
BladeCenter Blade +1.25V Rail Low Voltage Cleared	1024	550	2
BladeCenter Blade +1.5V Rail High Voltage	1024	543	8
BladeCenter Blade +1.5V Rail High Voltage Cleared	1024	544	2
BladeCenter Blade +1.5V Rail Low Voltage	1024	545	8
BladeCenter Blade +1.5V Rail Low Voltage Cleared	1024	546	2
BladeCenter Blade +12V Rail High Voltage	1024	535	8
BladeCenter Blade +12V Rail High Voltage Cleared	1024	536	2
BladeCenter Blade +12V Rail Low Voltage	1024	537	8
BladeCenter Blade +12V Rail Low Voltage Cleared	1024	538	2
BladeCenter Blade +2.5V Rail High Voltage	1024	539	8
BladeCenter Blade +2.5V Rail High Voltage Cleared	1024	540	2
BladeCenter Blade +2.5V Rail Low Voltage	1024	541	8
BladeCenter Blade +2.5V Rail Low Voltage Cleared	1024	542	2
BladeCenter Blade +3.3V Rail High Voltage	1024	531	8
BladeCenter Blade +3.3V Rail High Voltage Cleared	1024	532	2
BladeCenter Blade +3.3V Rail Low Voltage	1024	533	8
BladeCenter Blade +3.3V Rail Low Voltage Cleared	1024	534	2
BladeCenter Blade +5V Rail High Voltage	1024	527	8
BladeCenter Blade +5V Rail High Voltage Cleared	1024	528	2
BladeCenter Blade +5V Rail Low Voltage	1024	529	8
BladeCenter Blade +5V Rail Low Voltage Cleared	1024	530	2
BladeCenter Blade Powered Off	1024	519	8
BladeCenter Blade Powered On	1024	520	2
BladeCenter Blower Failed	1024	514	6
BladeCenter Blower OK	1024	513	2
BladeCenter Blower Slow	1024	512	4
BladeCenter Chassis -5V Rail High Voltage	1024	571	8
BladeCenter Chassis -5V Rail High Voltage Cleared	1024	572	2
BladeCenter Chassis -5V Rail Low Voltage	1024	573	8
BladeCenter Chassis -5V Rail Low Voltage Cleared	1024	574	2

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
BladeCenter Chassis +1.8V Rail High Voltage	1024	567	8
BladeCenter Chassis +1.8V Rail High Voltage Cleared	1024	568	2
BladeCenter Chassis +1.8V Rail Low Voltage	1024	569	8
BladeCenter Chassis +1.8V Rail Low Voltage Cleared	1024	570	2
BladeCenter Chassis +12V Rail High Voltage	1024	559	8
BladeCenter Chassis +12V Rail High Voltage Cleared	1024	560	2
BladeCenter Chassis +12V Rail Low Voltage	1024	561	8
BladeCenter Chassis +12V Rail Low Voltage Cleared	1024	562	2
BladeCenter Chassis +2.5V Rail High Voltage	1024	563	8
BladeCenter Chassis +2.5V Rail High Voltage Cleared	1024	564	2
BladeCenter Chassis +2.5V Rail Low Voltage	1024	565	8
BladeCenter Chassis +2.5V Rail Low Voltage Cleared	1024	566	2
BladeCenter Chassis +3.3V Rail High Voltage	1024	555	8
BladeCenter Chassis +3.3V Rail High Voltage Cleared	1024	556	2
BladeCenter Chassis +3.3V Rail Low Voltage	1024	557	8
BladeCenter Chassis +3.3V Rail Low Voltage Cleared	1024	558	2
BladeCenter Chassis +5V Rail High Voltage	1024	551	8
BladeCenter Chassis +5V Rail High Voltage Cleared	1024	552	2
BladeCenter Chassis +5V Rail Low Voltage	1024	553	8
BladeCenter Chassis +5V Rail Low Voltage Cleared	1024	554	2
BladeCenter CPU1 High Temperature	1024	521	8
BladeCenter CPU1 High Temperature Cleared	1024	522	2
BladeCenter CPU2 High Temperature	1024	523	8
BladeCenter CPU2 High Temperature Cleared	1024	524	2
BladeCenter DASD1 High Temperature	1024	525	8
BladeCenter DASD1 High Temperature Cleared	1024	526	2
BladeCenter Front Panel High Temperature	1024	517	8
BladeCenter Front Panel High Temperature Cleared	1024	518	2
BladeCenter Management Module High Temperature	1024	515	8
BladeCenter Management Module High Temperature Cleared	1024	516	2
Chassis Fan Major Fault	8	33	8
Chassis Fan Minor Fault	8	32	6
Chassis Fan OK	8	30	2
Chassis Fan Status Unknown	8	31	4

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
Chassis Major Alarm	8	37	10
Chassis Major Alarm Cleared	8	38	2
Chassis Minor Alarm	8	35	8
Chassis Minor Alarm Cleared	8	36	2
Chassis Temperature Alarm	8	50	6
Chassis Temperature Alarm Cleared	8	51	2
Chassis Temperature Critical Alarm	8	52	10
CM Configuration Includes Policy Exclusion	1024	346	4
CM Configuration Missing Policy Mandated Statement	1024	345	4
CM Firmware Version Changed	1024	350	2
CM Previously Unsaved Configuration Saved	1024	344	2
CM Running Configuration Changed	1024	342	4
CM Running Configuration Retrieval Failed	1024	348	4
CM Startup Configuration Changed	1024	341	2
CM Startup Configuration Retrieval Failed	1024	349	4
CM Unsaved Configuration	1024	343	4
Config Mgmt Job Failed	1024	351	8
Config Mgmt Job Succeeded	1024	352	2
CUCM CPU High Utilization	1024	416	8
CUCM CPU High Utilization Cleared	1024	417	2
CUCM CTI Device Not Registered	1024	402	10
CUCM CTI Device Registered	1024	403	2
CUCM Gatekeeper Not Registered	1024	404	10
CUCM Gatekeeper Registered	1024	405	2
CUCM Gateway Not Registered	1024	410	10
CUCM Gateway Registered	1024	411	2
CUCM H323 Device Not Registered	1024	406	10
CUCM H323 Device Registered	1024	407	2
CUCM Media Device Not Registered	1024	408	10
CUCM Media Device Registered	1024	409	2
CUCM Phone Not Registered	1024	400	10
CUCM Phone Registered	1024	401	2
CUCM Process Memory High Utilization	1024	418	8
CUCM Process Memory High Utilization Cleared	1024	419	2

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
CUCM Voicemail Device Not Registered	1024	412	10
CUCM Voicemail Device Registered	1024	413	2
Device Average CPU Utilization Critical	8	101	8
Device Average CPU Utilization High	8	55	8
Device Average CPU Utilization High Cleared	8	54	2
Device Average Memory Usage Cleared	8	56	2
Device Average Memory Usage Critical	8	101	8
Device Average Memory Usage High	8	57	8
Device Clock Inconsistency	8	84	6
Device Cold Reboot	8	1	8
Device Fan Failure	1024	938	10
Device Fan Failure Cleared	1024	937	2
Device High Active Sessions	1024	621	6
Device High Active Sessions Cleared	1024	620	2
Device High Authenticated Response Time	1024	623	6
Device High Authenticated Response Time Cleared	1024	622	2
Device High External URL Response Time	1024	625	6
Device High External URL Response Time Cleared	1024	624	2
Device High Messages Received	1024	627	6
Device High Messages Received Cleared	1024	626	2
Device Low Disk Space	1024	314	8
Device Low Disk Space Cleared	1024	315	2
Device Name Resolution Failure	8	88	4
Device Name Resolution Failure Cleared	8	89	2
Device Port(s) Utilization Accuracy at Risk	8	86	4
Device Port(s) Utilization Accuracy Lost	8	85	6
Device Port(s) Utilization Missed Due to Slow Response	8	87	6
Device Reboot Detected	8	5	8
Device Sensor Warning Value	1024	940	10
Device Sensor Warning Value Cleared	1024	939	2
Device Warm Reboot	8	2	8
EGP Neighbor Loss	8	9	10
EIGRP Peer Briefly Not Established	1024	146	8
EIGRP Peer Disappeared	1024	144	10

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
EIGRP Peer Newly Discovered	1024	145	4
Entuity License Expired and This Entuity Server is No Longer Operational	32	17	10
Entuity License on Remote Server Could Not be Updated	32	13	4
Entuity License on Remote Server Expired and No Longer Operational	32	14	10
Entuity License on Remote Server Successfully Updated	32	15	2
Entuity License Successfully Updated by License Server	32	18	4
Entuity License Was Not Updated by License Server and Will Expire	32	16	4
Entuity Server Automated Shutdown	32	4	10
Entuity Server Component Restarting After Failure	32	10	8
Entuity Server Critical Component Restarting After Failure	32	9	8
Entuity Server Disk Space Alert	32	2	10
Entuity Server Explicit Server Shutdown Initiated	32	6	8
Entuity Server Internal Event	32	1	4
Entuity Server License Alert	32	3	10
Entuity Server Permanent Component Failure	32	8	10
Entuity Server Shutdown Forced by Critical Failure to Restart	32	7	10
Entuity Server Started	32	5	2
Firewall Access Control Violations High	1024	900	8
Firewall Access Control Violations High Cleared	1024	901	2
Firewall High Avail User Set Oper State Compliant	1024	1017	2
Firewall High Avail User Set Oper State Non Compliant	1024	1018	8
Firewall High Current Connections	1024	907	6
Firewall High Current Connections Cleared	1024	906	2
Firewall Overflow and Intrusion Violations High	1024	902	8
Firewall Overflow and Intrusion Violations High Cleared	1024	903	2
Firewall URL Alerts High	1024	904	4
Firewall URL Alerts High Cleared	1024	905	4
FR DLCI High BECN	1024	3	6
FR DLCI High BECN Cleared	1024	4	2
FR DLCI High DE	1024	5	6
FR DLCI High DE Cleared	1024	6	2
FR DLCI High FECN	1024	1	6

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
FR DLCI High FECN Cleared	1024	2	2
FR DLCI High Inbound Utilization	1024	7	6
FR DLCI High Inbound Utilization Cleared	1024	8	2
FR DLCI High Outbound Utilization	1024	9	6
FR DLCI High Outbound Utilization Cleared	1024	10	2
FR DLCI Link Down	1024	11	8
FR DLCI Link Up	1024	12	2
HSRP Port Group Activated	1024	175	6
HSRP Port Group Deactivated	1024	176	6
IP SLA Creation Failure	1024	234	10
IP SLA Creation Failure Cleared	1024	235	2
IP SLA High ICPIF	1024	236	10
IP SLA High ICPIF Cleared	1024	237	2
IP SLA Low MOS	1024	238	10
IP SLA Low MOS Cleared	1024	239	2
IP SLA Test Failed	1024	230	10
IP SLA Test High Latency	1024	232	10
IP SLA Test High Latency Cleared	1024	233	2
IP SLA Test Succeeded	1024	231	2
LAP Antenna Host Count High	1024	836	4
LAP Antenna Host Count High Cleared	1024	837	2
LAP Antenna Host Count Low	1024	838	4
LAP Antenna Host Count Low Cleared	1024	839	2
Load Balancer High Client Connection Limit Pkt Drop Rate	1024	972	10
Load Balancer High Client Connection Limit Pkt Drop Rate Cleared	1024	973	2
Load Balancer High Client Connections	1024	956	10
Load Balancer High Client Connections Cleared	1024	957	2
Load Balancer High Client Hw Accel Connections	1024	958	10
Load Balancer High Client Hw Accel Connections Cleared	1024	959	2
Load Balancer High Inbound Error Rate	1024	976	10
Load Balancer High Inbound Error Rate Cleared	1024	977	2
Load Balancer High License Denied Pkt Rate	1024	968	10
Load Balancer High License Denied Pkt Rate Cleared	1024	969	2

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
Load Balancer High Memory Error Pkt Rate	1024	970	10
Load Balancer High Memory Error Pkt Rate Cleared	1024	971	2
Load Balancer High No Handler Denied Pkt Rate	1024	966	10
Load Balancer High No Handler Denied Pkt Rate Cleared	1024	967	2
Load Balancer High Non Syn Denied Pkt Rate	1024	964	10
Load Balancer High Non Syn Denied Pkt Rate Cleared	1024	965	2
Load Balancer High Outbound Error Rate	1024	978	10
Load Balancer High Outbound Error Rate Cleared	1024	979	2
Load Balancer High Packet Drop Rate	1024	974	10
Load Balancer High Packet Drop Rate Cleared	1024	975	2
Load Balancer High Server Connections	1024	960	10
Load Balancer High Server Connections Cleared	1024	961	2
Load Balancer High Server Hw Accel Connections	1024	962	10
Load Balancer High Server Hw Accel Connections Cleared	1024	963	2
Load Balancer Nortel High MP CPU 1sec Utilization	1024	989	10
Load Balancer Nortel High MP CPU 1sec Utilization Cleared	1024	988	2
Load Balancer Nortel High MP CPU 4sec Utilization	1024	991	10
Load Balancer Nortel High MP CPU 4sec Utilization Cleared	1024	990	2
Load Balancer Nortel High MP CPU 64sec Utilization	1024	993	8
Load Balancer Nortel High MP CPU 64sec Utilization Cleared	1024	992	2
Load Balancer Nortel High Real Server Current Sessions	1024	1001	10
Load Balancer Nortel High Real Server Current Sessions Cleared	1024	1000	2
Load Balancer Nortel High Real Server Max Sessions	1024	1003	10
Load Balancer Nortel High Real Server Max Sessions Cleared	1024	1002	2
Load Balancer Nortel High SLB SP Current Sessions	1024	1005	10
Load Balancer Nortel High SLB SP Current Sessions Cleared	1024	1004	2
Load Balancer Pool Critical Member Availability	1024	1015	10
Load Balancer Pool Critical Member Availability Cleared	1024	1013	2
Load Balancer Pool Low Member Availability	1024	1016	8
Load Balancer Pool Low Member Availability Cleared	1024	1014	2
Load Balancer Virtual Server High Average Connection Duration	1024	982	10
Load Balancer Virtual Server High Average Connection Duration Cleared	1024	983	2
Load Balancer Virtual Server High Connection Request Rate	1024	980	10

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
Load Balancer Virtual Server High Connection Request Rate Cleared	1024	981	2
Load Balancer Virtual Server High Ephemeral Connections	1024	984	10
Load Balancer Virtual Server High Ephemeral Connections Cleared	1024	985	2
Load Balancer Virtual Server High Hw Accel Connections	1024	986	10
Load Balancer Virtual Server High Hw Accel Connections Cleared	1024	987	2
MAC Address High Port Count	2	48	6
MAC Address High Port Count Cleared	2	49	2
MAC Address New	2	26	6
MAC Address Port Changed	2	44	6
Memory Low	8	59	8
Memory Low Cleared	8	58	2
Module Disappeared	1024	913	10
Module Discovered	1024	912	4
Module Down	4	24	10
Module Major Fault	4	23	10
Module Minor Fault	4	22	8
Module Status OK	4	20	2
Module Status Unknown	4	21	6
MPLS LDP Entity Errors	1024	192	8
MPLS LDP Entity Errors Cleared	1024	193	2
MPLS LDP Entity Non-operational	1024	182	10
MPLS LDP Entity Operational	1024	183	2
MPLS LDP Entity Rejected Sessions	1024	190	10
MPLS LDP Entity Rejected Sessions Cleared	1024	191	2
MPLS LDP Entity Shutdown Notifications Received	1024	194	10
MPLS LDP Entity Shutdown Notifications Received Cleared	1024	195	2
MPLS LDP Entity Shutdown Notifications Sent	1024	196	10
MPLS LDP Entity Shutdown Notifications Sent Cleared	1024	197	2
MPLS LDP Peer Disappeared	1024	184	10
MPLS LDP Peer Newly Discovered	1024	185	2
MPLS LDP Peer Non-operational	1024	180	10
MPLS LDP Peer Operational	1024	181	2
MPLS LDP Peer TLV Errors	1024	188	10

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
MPLS LDP Peer TLV Errors Cleared	1024	189	2
MPLS LDP Peer Unknown Message Types	1024	186	10
MPLS LDP Peer Unknown Message Types Cleared	1024	187	2
MPLS LSR Interface High Discard Rate (Lookup Failure)	1024	206	6
MPLS LSR Interface High Discard Rate (Lookup Failure) Cleared	1024	207	2
MPLS LSR Interface High Error Free Discard Rate (RX)	1024	202	6
MPLS LSR Interface High Error Free Discard Rate (RX) Cleared	1024	203	2
MPLS LSR Interface High Error Free Discard Rate (TX)	1024	204	6
MPLS LSR Interface High Error Free Discard Rate (TX) Cleared	1024	205	2
MPLS LSR Interface High Fragmentation Rate	1024	208	6
MPLS LSR Interface High Fragmentation Rate Cleared	1024	209	2
MPLS LSR Interface Low Bandwidth	1024	198	6
MPLS LSR Interface Low Bandwidth Cleared	1024	199	2
MPLS LSR Interface Low Buffer Space	1024	200	6
MPLS LSR Interface Low Buffer Space Cleared	1024	201	2
MPLS LSR Platform High Discard Rate (Lookup Failure)	1024	218	6
MPLS LSR Platform High Discard Rate (Lookup Failure) Cleared	1024	219	2
MPLS LSR Platform High Error Free Discard Rate (RX)	1024	214	6
MPLS LSR Platform High Error Free Discard Rate (RX) Cleared	1024	215	2
MPLS LSR Platform High Error Free Discard Rate (TX)	1024	216	6
MPLS LSR Platform High Error Free Discard Rate (TX) Cleared	1024	217	2
MPLS LSR Platform High Fragmentation Rate	1024	220	6
MPLS LSR Platform High Fragmentation Rate Cleared	1024	221	2
MPLS LSR Platform Low Bandwidth	1024	210	6
MPLS LSR Platform Low Bandwidth Cleared	1024	211	2
MPLS LSR Platform Low Buffer Space	1024	212	6
MPLS LSR Platform Low Buffer Space Cleared	1024	213	2
MPLS VRF High Illegal Label Rate	1024	224	6
MPLS VRF High Illegal Label Rate Cleared	1024	225	2
MPLS VRF Interface BGP Neighbor Disappeared	1024	228	10
MPLS VRF Interface BGP Neighbor Newly Discovered	1024	227	4
MPLS VRF Non-operational	1024	223	10
MPLS VRF Operational	1024	222	2
Network Outage	512	7	10

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
Network Outage Cleared	512	8	2
OSPF Peer Briefly Disappeared	1024	162	10
OSPF Peer Briefly Not Established	1024	164	10
OSPF Peer Established	1024	161	4
OSPF Peer Newly Discovered	1024	163	4
OSPF Peer Not Established	1024	160	10
Port Duplex Change	2	20	2
Port Error Disable Alarm	2	40	8
Port Error Disable Alarm Cleared	2	41	2
Port High Inbound Discards (Dynamic)	1024	385	6
Port High Inbound Discards (Dynamic) Cleared	1024	384	2
Port High Inbound Fault (Dynamic)	1024	389	6
Port High Inbound Fault (Dynamic) Cleared	1024	388	2
Port High Inbound Utilization (Dynamic)	1024	397	6
Port High Inbound Utilization (Dynamic) Cleared	1024	396	2
Port High Outbound Discards (Dynamic)	1024	383	6
Port High Outbound Discards (Dynamic) Cleared	1024	382	2
Port High Outbound Fault (Dynamic)	1024	387	6
Port High Outbound Fault (Dynamic) Cleared	1024	386	2
Port High Outbound Utilization (Dynamic)	1024	393	6
Port High Outbound Utilization (Dynamic) Cleared	1024	392	2
Port Link Down	2	2	10
Port Link Up	2	3	2
Port Low Inbound Utilization (Dynamic)	1024	395	6
Port Low Inbound Utilization (Dynamic) Cleared	1024	394	2
Port Low Outbound Utilization (Dynamic)	1024	391	6
Port Low Outbound Utilization (Dynamic) Cleared	1024	390	2
Port Operationally Down	1024	36	10
Port Operationally Down Cleared	1024	37	2
Port Outbound Discards High (Port Congestion)	2	16	6
Port Outbound Discards High Cleared (No Port Congestion)	2	17	8
Port Outbound Fault High (Transmit Errors)	2	12	6
Port Outbound Fault High Cleared (No Transmit Errors)	2	13	8
Port Speed Change	2	21	2

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
Port Utilization High	2	22	8
Port Utilization High Cleared	2	23	2
Port Utilization Low	2	24	8
Port Utilization Low Cleared	2	25	2
Power Supply Major Fault	8	124	8
Power Supply Minor Fault	8	122	8
Power Supply OK	8	120	2
Power Supply Unknown Status	8	126	8
Processor High Utilization	8	60	4
Processor High Utilization Cleared	8	61	2
QoS Above Bandwidth Limit	1024	56	8
QoS At Bandwidth Limit	1024	57	4
QoS Class Bit Rate High	1024	100	4
QoS Class Bit Rate High Cleared	1024	101	2
QoS Class Drop Bit Rate High	1024	102	4
QoS Class Drop Bit Rate High Cleared	1024	103	2
QoS Class Drop Packet Rate (Buffer Shortage) High	1024	104	8
QoS Class Drop Packet Rate (Buffer Shortage) High Cleared	1024	105	2
QoS Queue Drop Bit Rate High	1024	106	4
QoS Queue Drop Bit Rate High Cleared	1024	107	2
QoS Under Bandwidth Limit	1024	58	2
Routing Broadcast Traffic High	2	34	6
Routing Broadcast Traffic High Cleared	2	35	2
Routing High No Routes To IP Destination	8	72	4
Routing High No Routes To IP Destination Cleared	8	73	2
Routing ICMP High Redirects	8	74	4
Routing ICMP High Redirects Cleared	8	75	2
Routing ICMP High TTL Exceeds	8	70	4
Routing ICMP High TTL Exceeds Cleared	8	71	2
Routing Low I/O Contiguous Memory	8	68	4
Routing Low I/O Contiguous Memory Cleared	8	69	2
Routing Low I/O Total Memory	8	66	4
Routing Low I/O Total Memory Cleared	8	67	2
Routing Low Processor Contiguous Memory	8	64	4

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
Routing Low Processor Contiguous Memory Cleared	8	65	2
Routing Low Processor Total Memory	8	62	4
Routing Low Processor Total Memory Cleared	8	63	2
Service Down	1024	919	10
Service State Degraded	1024	918	6
Service State Off	1024	917	6
Service State Unknown	1024	921	2
Service Up	1024	920	2
SLB SP 1 Second CPU Utilization Cleared	1024	994	2
SLB SP 1 Second CPU Utilization High	1024	995	10
SLB SP 4 Second CPU Utilization Cleared	1024	996	2
SLB SP 4 Second CPU Utilization High	1024	997	10
SLB SP 64 Second CPU Utilization Cleared	1024	998	2
SLB SP 64 Second CPU Utilization High	1024	999	10
SNMP Agent Not Responding	8	3	10
SNMP Agent Responding	8	4	2
SNMP Agent Restart Detected	1024	254	8
SNMP Authentication Failure	8	8	6
SNMP v3 Duplicate Engine ID	8	90	8
SSL Certificate Expired	1024	1023	10
SSL Certificate Expiring	1024	1024	8
SSL Proxy Service Administrative Available to SNMP Poll	1024	1021	2
SSL Proxy Service Administrative Unavailable to SNMP Poll	1024	1022	10
SSL Proxy Service Operational Available to SNMP Poll	1024	1019	2
SSL Proxy Service Operational Unavailable to SNMP Poll	1024	1020	10
STP New Root Device	16	1	10
STP VLAN Topology Change	16	2	6
Syslog Alert	64	2	8
Syslog Critical	64	3	8
Syslog Debug	64	8	2
Syslog Emergency	64	1	10
Syslog Error	64	4	6
Syslog Information	64	7	2
Syslog Notice	64	6	4

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
Syslog Warning	64	5	4
UCS Blade Down	1024	719	10
UCS Blade Major Fault	1024	718	8
UCS Blade Minor Fault	1024	717	4
UCS Blade OK	1024	715	2
UCS Blade Status Unknown	1024	716	4
UCS Chassis Down	1024	684	10
UCS Chassis Major Fault	1024	683	8
UCS Chassis Minor Fault	1024	682	4
UCS Chassis Status OK	1024	680	2
UCS Chassis Status Unknown	1024	681	4
UCS Fabric Extender Down	1024	709	10
UCS Fabric Extender Major Fault	1024	708	8
UCS Fabric Extender Minor Fault	1024	707	4
UCS Fabric Extender Status OK	1024	705	2
UCS Fabric Extender Status Unknown	1024	706	4
UCS Fan Down	1024	699	10
UCS Fan Major Fault	1024	698	8
UCS Fan Minor Fault	1024	697	4
UCS Fan Module Down	1024	694	10
UCS Fan Module Major Fault	1024	693	8
UCS Fan Module Minor Fault	1024	692	4
UCS Fan Module Status OK	1024	690	2
UCS Fan Module Status Unknown	1024	691	4
UCS Fan Status OK	1024	695	2
UCS Fan Status Unknown	1024	696	4
UCS Local Disk Down	1024	714	10
UCS Local Disk Major Fault	1024	713	8
UCS Local Disk Minor Fault	1024	712	4
UCS Local Disk OK	1024	710	2
UCS Local Disk Unknown	1024	711	4
UCS PSU Down	1024	689	10
UCS PSU Major Fault	1024	688	8
UCS PSU Minor Fault	1024	687	4

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
UCS PSU OK	1024	685	2
UCS PSU Unknown	1024	686	4
UCS Switch Card Down	1024	704	10
UCS Switch Card Major Fault	1024	703	8
UCS Switch Card Minor Fault	1024	702	4
UCS Switch Card Status OK	1024	700	2
UCS Switch Card Status Unknown	1024	701	4
Unknown Trap	8	10	6
User Defined Attribute State Disabled	1024	357	6
User Defined Attribute State Down	1024	358	10
User Defined Attribute State Other	1024	356	6
User Defined Attribute State Up	1024	359	2
User Defined Attribute Value Abnormality Cleared	1024	360	2
User Defined Attribute Value Critical	1024	364	10
User Defined Attribute Value High	1024	363	8
User Defined Attribute Value Low	1024	361	6
User Defined Attribute Value Warning	1024	362	6
Virtualization Connection Failed	1024	65	8
Virtualization Connection Success	1024	64	2
VPN High Active Tunnels	1024	607	6
VPN High Active Tunnels Cleared	1024	606	2
VPN Load Average High	1024	600	4
VPN Load Average High Cleared	1024	601	2
VPN Network Port Utilization High	1024	604	4
VPN Network Port Utilization High Cleared	1024	605	2
VPN Tunnel Usage High	1024	602	4
VPN Tunnel Usage High Cleared	1024	603	2
WAN Port High Inbound Discards	1024	32	6
WAN Port High Inbound Discards Cleared	1024	33	2
WAN Port High Inbound Errors	1024	28	6
WAN Port High Inbound Errors Cleared	1024	29	2
WAN Port High Inbound Utilization	1024	20	6
WAN Port High Inbound Utilization Cleared	1024	21	2
WAN Port High Outbound Discards	1024	34	6

Table 3 Event Identifiers

Event Name	Group ID	Event ID	Internal Severity
WAN Port High Outbound Discards Cleared	1024	35	2
WAN Port High Outbound Errors	1024	30	6
WAN Port High Outbound Errors Cleared	1024	31	2
WAN Port High Outbound Utilization	1024	24	6
WAN Port High Outbound Utilization Cleared	1024	25	2
WAN Port Low Inbound Utilization	1024	22	6
WAN Port Low Inbound Utilization Cleared	1024	23	2
WAN Port Low Outbound Utilization	1024	26	6
WAN Port Low Outbound Utilization Cleared	1024	27	2
Wireless Controller High Number of Connected APs	1024	811	6
Wireless Controller High Number of Connected APs Cleared	1024	810	2

Table 3 Event Identifiers

Index

A

- Application
 - unavailable [33](#)
- Availability Monitoring
 - application high latency [34](#)
 - application unavailable [33](#)
- AvailMonitor High Latency Reaching Application [34](#)

B

- Backplane
 - utilization high [38](#), [39](#), [40](#)
- BGP
 - Peer Briefly Disappeared [42](#)
 - Peer Briefly Established [41](#)
 - Peer Established [42](#)
 - Peer Newly Discovered [42](#)
 - Peer Not Established [42](#)
- BladeCenter Blade
 - powered off [51](#)
 - rail high voltage [43](#), [44](#), [46](#), [47](#), [48](#), [50](#)
 - rail low voltage [43](#), [45](#), [46](#), [48](#), [49](#), [51](#)
- BladeCenter Blower
 - failed [52](#)
 - slow [53](#)
- BladeCenter Chassis
 - rail high voltage [53](#), [54](#), [56](#), [57](#), [59](#), [60](#)
 - rail low voltage [54](#), [55](#), [56](#), [58](#), [59](#), [61](#)
- BladeCenter CPU
 - temperature high [62](#)
- BladeCenter DASD1
 - temperature high [63](#)
- BladeCenter Front Panel
 - temperature high [64](#)
- BladeCenter Management Module
 - temperature high [64](#)

C

- Chassis

- fan major fault [65](#)
- fan minor fault [65](#), [175](#)
- fan status unknown [66](#), [176](#)
- major alarm [66](#)
- minor alarm [67](#)
- temperature alarm [67](#), [68](#)

Cisco Unified Computing System (UCS) events

- UCS Blade Down [168](#)
- UCS Blade Major Fault [169](#)
- UCS Blade Minor Fault [169](#)
- UCS Blade OK [169](#)
- UCS Blade Status Unknown [170](#)
- UCS Chassis Major Fault [170](#)
- UCS Chassis Minor Fault [171](#)
- UCS Chassis Status OK [171](#)
- UCS Chassis Status Unknown [171](#)
- UCS Fabric Extender Down [172](#)
- UCS Fabric Extender Major Fault [172](#)
- UCS Fabric Extender Minor Fault [172](#)
- UCS Fabric Extender Status OK [173](#)
- UCS Fabric Extender Status Unknown [173](#)
- UCS Fan Down [173](#)
- UCS Fan Major Fault [174](#)
- UCS Fan Minor Fault [174](#)
- UCS Fan Module Down [175](#)
- UCS Fan Module Major Fault [175](#)
- UCS Fan Module Minor Fault [175](#)
- UCS Fan Module Status OK [176](#)
- UCS Fan Module Status Unknown [176](#)
- UCS Fan Status OK [176](#)
- UCS Fan Status Unknown [176](#)
- UCS Local Disk Down [177](#)
- UCS Local Disk Major Fault [177](#)
- UCS Local Disk Minor Fault [178](#)
- UCS Local Disk OK [178](#)
- UCS Local Disk Unknown [178](#)
- UCS PSU Down [179](#)
- UCS PSU Major Fault [179](#)
- UCS PSU Minor Fault [179](#)
- UCS PSU OK [180](#)
- UCS PSU Unknown [180](#)
- UCS Switch Card Down [180](#)
- UCS Switch Card Major Fault [181](#)
- UCS Switch Card Minor Fault [181](#)

- incidents

- UCS Blade Status [257](#)
- UCS Chassis Status [257](#)
- UCS Fabric Extender Status [257](#)
- UCS Fan Module Status [258](#)
- UCS Fan Status [258](#)
- UCS Local Disk Status [259](#)
- UCS Power Supply Status Problem [259](#)
- UCS Switch Card Status [259](#)
- Community String
 - authentication failure [161](#)
- Configuration Retrieval
 - debug mode [72](#)
 - failure
 - running configuration [70](#)
 - startup configuration [71](#)
- Congestion
 - port events [144](#), [145](#), [151](#), [191](#)
- CPU
 - critical device utilization [80](#)
 - CUCM utilization high [73](#)
 - high device utilization [80](#), [155](#)
- CUCM CPU Utilization High [73](#)
- CUCM CPU Utilization High Cleared [73](#)
- CUCM CTI Device Not Registered [73](#)
- CUCM CTI Device Registered [74](#)
- CUCM Gatekeeper Not Registered [74](#)
- CUCM Gatekeeper Registered [75](#)
- CUCM Gateway Not Registered [75](#)
- CUCM Gateway Registered [75](#)
- CUCM H.323 Device Not Registered [76](#)
- CUCM H.323 Device Registered [76](#)
- CUCM Media Device Not Registered [76](#)
- CUCM Media Device Registered [77](#)
- CUCM Phone Not Registered [77](#)
- CUCM Phone Registered [78](#)
- CUCM Process Memory High Utilization [78](#)
- CUCM Process Memory High Utilization Cleared [78](#)
- CUCM Voicemail Device Not Registered [79](#)
- CUCM Voicemail Device Registered [79](#)

D

- Device CPU High Utilization
 - n of m setting [155](#)
- Device Low Disk Space Cleared event [85](#)
- Device Low Disk Space event [85](#)
- Device Low Total Memory Cleared event [81](#), [122](#)
- Device Low Total Memory event [81](#), [122](#)
- Device SNMP Response Time report [161](#)
- Device Status [88](#), [89](#)
- Device Unreachable
 - Network Outage [89](#), [138](#)
- Devices
 - backplane high utilization [38](#), [39](#), [40](#)
 - cold reboot [82](#)
 - CPU critical utilization [80](#)
 - CPU high utilization [80](#), [155](#)
 - EGP Neighbor Loss [90](#)
 - low memory [80](#), [81](#), [121](#)
 - name resolution failure [85](#)
 - power supply fault [154](#)
 - power supply state [155](#)
 - rebooted [87](#)
 - STP new root [163](#)
 - warm reboot [89](#)
- Discards
 - events [189](#)
- Disk Space
 - Entuity server [93](#), [94](#), [95](#), [96](#)
- diskMonitor
 - Entuity server disk space [93](#), [94](#), [95](#), [96](#)
- Dynamic Thresholds
 - high inbound faults [143](#)
 - port high inbound discards [142](#), [146](#), [147](#)

E

- EGP Neighbor Loss [90](#)
- EIGRP
 - Peer Briefly Disappeared [90](#)
 - Peer Briefly Established [90](#)
 - Peer Newly Discovered [90](#)
- Enterprise Trap [182](#)
- Entuity Server

Entuity

- disk space [93](#), [94](#), [95](#), [96](#)
- internal event [95](#)
- shutdown [93](#)

Event Groups [266](#)

Events

- group [266](#)
- identifier [266](#)
- missing [122](#)
- supported in Entuity [25](#)

F

Fan

- chassis major fault [65](#)
- chassis minor fault [65](#), [175](#)
- chassis status unknown [66](#), [176](#)

Firewall

- High Availability events [97](#), [98](#)

Firewall Access Control Violations High [96](#), [99](#), [100](#)

Firewall Access Control Violations High Cleared [97](#), [99](#), [100](#)

Frame Relay

- BECNs high [100](#)
- DE high [101](#)
- DLCI link down [103](#)
- DLCI link up [103](#)
- FECN high [102](#)
- inbound utilization high [102](#)
- outbound utilization high [103](#)

I

ICMP High Redirects [157](#)

ICPIF

- high [105](#)

Inbound Discards

- port high [142](#), [146](#), [147](#)

Inbound Faults

- dynamic threshold events [143](#)

Internal Event

- Entuity server [95](#)

IP Addresses

- high broadcast traffic [157](#)

IP SLA Creation Failure [104](#)

IP SLA Creation Failure Cleared [105](#)

IP SLA High ICPIF [105](#)

IP SLA High ICPIF Cleared [105](#)

IP SLA Low MOS [105](#)

IP SLA Low MOS Cleared [106](#)

IP SLA Operations

- creation failure event [104](#)

IP SLA Test Failed [106](#)

IP SLA Test High Latency [106](#)

IP SLA Test High Latency Cleared [107](#)

IP SLA Test Succeeded [107](#)

IS-IS

- Peer Disappeared [107](#)

- Peer Established [108](#)

- Peer Newly Discovered [108](#)

- Peer Not Established [108](#)

L

License Server

- contacted remote server [92](#)

- license expired [91](#)

- remote server license invalid [92](#)

- remote server uncontactable [91](#)

Licensing

- server alert [95](#)

Link Down

- DLCI [103](#)

- ports [148](#)

Link Up

- DLCI [103](#)

- ports [149](#)

M

MAC Addresses

- high port count [119](#)

- machistorylimit [120](#), [121](#)

- new [120](#)

- port change [120](#)

macman

- machistorylimit [120](#), [121](#)

Managed Hosts

- device low disk space cleared event [85](#)

Entuity

- device low disk space event 85
- device low total memory cleared event 81, 122
- device low total memory event 81, 122

Managed Object
down 138, 139

Memory
device running low 80, 81, 121

Missing Events 266

Module
major fault 123, 169, 170, 172, 177, 179, 181
minor fault 123, 169, 171, 172, 178, 179, 181
status unknown 124, 170, 171, 173, 178, 180, 182

MOS
low 105

N

Network Outage
Device Unreachable 89, 138

Node down 138, 139

O

Operations
connection failed event 106
creation succeeded event 105

OSPF
Peer Briefly Disappeared 140
Peer Briefly Established 139
Peer Established 140
Peer Newly Discovered 140
Peer Not Established 140

P

Packet Corruption
events 142, 147, 148, 189

Ping
ports unavailable 137, 139

Policy Violations
events
bad practice violation 68
good practice violation 68, 69

Port Flapping
Port Status Problem 248

Port Link Down
Port Status Problem 248

Port Operationally Down Cleared
Port Status Problem 248

Port Status Problem 248

Ports
change MAC addresses 121
congestion 144, 145, 151, 191
duplex change 141
error disable alarm 141
link down 148
link up 149
MAC addresses
change 121
high port count 119
new 120
speed change 153
transmit errors 145, 146, 152
unavailable to ping 137, 139
utilization high 143, 144, 146, 149, 150, 153
utilization low 149, 153
VPN utilization high 188
WAN inbound discards 189
WAN inbound utilization 190
WAN outbound discards 191

Power Supply
major fault 154
minor fault 154
unknown state 155

R

Routing
broadcast traffic high 156
ICMP high redirects 157
ICMP high TTL exceeded 158
no routes to IP destination 157

Running Configuration
change events 69

S

Security
MAC address change 120

Entuity

ser [183](#)

Server

Shutdown [93](#)

Service State Problem
incident [253](#)

Service Summary [158](#)

Services

events [158](#), [159](#)

SNMP

Authentication Failure [161](#)
not responding [160](#)
response time high [161](#)

snmpSet

firewall restrictions [105](#)

SNMPv3

engine id duplication [162](#)

SSL Proxy Service Administrative Available to
SNMP Poll [162](#)

SSL Proxy Service Administrative Unavailable to
SNMP Poll [163](#)

SSL Proxy Service Operational Available to SNMP
Poll [163](#)

SSL Proxy Service Operational Unavailable to
SNMP Poll [163](#)

Startup Configuration
change events [71](#)

STP New Root Device [163](#)

STP VLAN Topology Change [164](#)

sw_n_of_m_cpu.cfg
Device CPU High Utilization [155](#)

Syslog events [164](#), [165](#), [166](#), [167](#), [168](#)

T

Transmit Errors

ports [145](#), [146](#), [152](#)

U

User Defined Polling

events

User Defined Attribute State Disabled
[182](#)

User Defined Attribute State Down [183](#)

User Defined Attribute State Other [183](#)

User Defined Attribute State Up [183](#)

User Defined Attribute Value Abnormali-
ty Cleared [183](#)

User Defined Attribute Value Critical [184](#)

User Defined Attribute Value High [184](#)

User Defined Attribute Value Low [184](#)

User Defined Attribute Value Warning
[185](#)

incidents

User Defined Attribute Status [260](#)

User Defined Attribute Value Abnormali-
ty [260](#)

Utilization

events [153](#), [154](#)

port, high [143](#), [144](#), [146](#), [149](#), [150](#), [153](#)

port, low [149](#), [153](#)

VCC high outbound [30](#)

VCC low inbound [31](#)

VCC low outbound [32](#)

VPN network ports [188](#)

WAN ports inbound [190](#)

WAN ports inbound utilization [193](#)

WAN ports outbound [192](#)

WAN ports outbound utilization [193](#)

Utilization CUCM process memory [78](#)

V

VCC

link down [31](#)

link up [31](#)

VLANs

STP topology change [164](#)

VM

memory high usage [186](#)

VoIP

ICPIF high [105](#)

ICPIF high cleared [105](#)

MOS low [105](#)

MOS low cleared [106](#)

VPN

excessive application traffic [187](#)

VPN Load Average [187](#)

VPN Load Average Cleared [187](#)

Entuity

VPN Network Port Utilization High [188](#)

VPN Network Port Utilization High Cleared [188](#)

VPN Tunnel Usage High [187](#), [188](#)

VPN Tunnel Usage High Cleared [187](#), [188](#)

W

WAN Ports

high inbound discards [189](#)

high inbound discards cleared [189](#)

high inbound errors [189](#)

high inbound errors cleared [190](#)

high inbound utilization [190](#)

high inbound utilization cleared [190](#)

high outbound discards [191](#)

high outbound discards cleared [191](#)

inbound utilization low [193](#)

inbound utilization low cleared [193](#)

outbound errors cleared [192](#)

outbound errors high [191](#)

outbound utilization high [192](#)

outbound utilization high cleared [192](#)

outbound utilization low [193](#)

outbound utilization low cleared [194](#)