ExtremeManagement™

Network Monitoring using Extreme Fabric Orchestrator

Release 1.2
NN48100-500
Issue 03.01
December 2017

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks’ agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks’ standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: http://www.extremenetworks.com/support under the link ““Policies” or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

“Hosted Service” means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND EXTREME NETWORKS INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE (“EXTREME NETWORKS”).

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Extreme Networks, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Extreme Networks' prior consent and payment of an upgrade fee.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Extreme Networks' website at:http://www.extremenetworks.com/support/policies/software-licensing or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at https://gtacknowledge.extremenetworks.com/.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: http://documentation.extremenetworks.com, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

See the Extreme Networks Support website:http://www.extremenetworks.com/support for product or Hosted Service notices and articles, or to report a problem with your Extreme Networks product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Extreme Networks Support website:http://www.extremenetworks.com/support/contact/ (or such successor site as designated by Extreme Networks), scroll to the bottom of the page, and select Contact Extreme Networks Support.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For additional information on Extreme Networks trademarks, please see: http://www.extremenetworks.com/company/legal/

Contents

Chapter 1: Preface

Purpose

This document provides information on configuring and managing your Monitoring system.

This document is intended to provide administrators with a management tool that offers solutions within a highly dynamic virtualized data center environment. Monitoring reduces troubleshooting issues because of a more complete view of the network. With Monitoring, efficiency in your IT department is increased by the time you save in regards to deploying new applications as well as adding or modifying applications or services.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help.

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to service notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to http://www.extremenetworks.com/support/service-notification-form/ .
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this document

The following sections detail what is new in *Network Monitoring using Extreme Fabric Orchestrator*, NN48100–500. See *Extreme Fabric Orchestrator Release Notes* for a list of supported features.

Resource monitoring enhancements

The system provides the ability to monitor EFO resources with trending events and alerts covering CPU usage, RAM usage, disk usage, NIC usage, and VM status. You must provide the SSH credentials of the KVM and EFO VMs to enable self resource monitoring. Once configured, you can right click the device and select show dashboard to view the resource usage. Monitoring session limit has been increased to 50 concurrent sessions. Also the system now supports Bridge Protocol Data Unit (BPDU) trap port and slot monitoring.

Launch Wireless Management tool

The system provides the ability to launch a wireless management tool for supported wireless devices. From **Network** > **Topology**, right click a supported wireless device and choose **Tools** > **Launch WOS**

Chapter 3: Dashboard information

Dashboard conceptual information

Use the following information to understand the Dashboard in the system under **Network** > **Overview**.

Managed objects

A managed object (MO) is a device that Monitoring actively processes information about to reflect the current status and condition of the object in real-time. The data that Monitoring gathers about the MO includes status propagation, fault, and performance information.

Every object that is an MO counts towards the license count. The license number decreases each time you add a new MO. When the maximum MO license count is reached, Monitoring no longer discovers new objects until you reduce the number of MOs to match the number of available licenses, or you apply a new license that is greater than the current MO count.

An unmanaged object (UMO) is an object that Monitoring has discovered, and which can appear on the interface as a gray icon, but does not process any information on the device, including status information, faults, and performance management. A UMO does not count towards the MO license count of Monitoring.

Supported devices

For more information about supported devices for Monitoring, see *Deploying Extreme Fabric Orchestrator*, NN48100–101.

Integrated dashboards

Monitoring offers multiple levels of dashboards to monitor system health. You can monitor network health, application and server health, device health, trunk utilization, and power savings.

Network Overview dashboard

The Network Overview dashboard displays dashlets containing information about the network health.

To access Network Overview, select **Network** > **Overview**, and then select **Network Overview**.

The dashlets are:

- Events by Element—Event summary dashlet showing the current event count, based on severity, for Aura servers.
- Events by Concern—Events by Concern dashlet allows you to click on a specific server to open a transient dashboard page for that server.
- Avaya Servers and Gateway Status—Server and gateway status dashlet showing alerts status for Avaya servers and gateways.
- Avaya Server and Gateway Availability—Availability dashlet showing current and historical availability for Avaya servers and gateways.
- IP Phone Availability—Availability dashlet showing current and historical availability for endpoints.
- L3 Switch Status—Element Status Summary dashlet showing alerts status for all discovered Layer-3 switches.
- L3 Switch Availability—Availability dashlet showing current and historical availability for all discovered Layer-3 switches.
- Router Availability—Availability dashlet showing current and historical availability for all discovered Routers.
- Router Status—Element Status Summary dashlet showing alerts status for all discovered Routers.

Device health

You can open a transient dashboard page for a server by clicking on a specific server located on the Network Overview page. Details about the server are visible on various dashlets on the dashboard.

The common dashlets that appear on transient dashboards include the following:

- Properties—Displays the properties of a specific server.
- Node Events—Displays node events of a specific server.
- Availability Report—Displays the Availability Report for a specific server.
- Node Performance—Displays KPI gauges for a specific server. The KPI gauges are: % CPU, % Memory, % TCP Retransmit.
- Interface Status Summary—Displays the interface status summary for a specific device.
- Top Interfaces by Total Usage—Displays the top interfaces by total usage for a specific device.

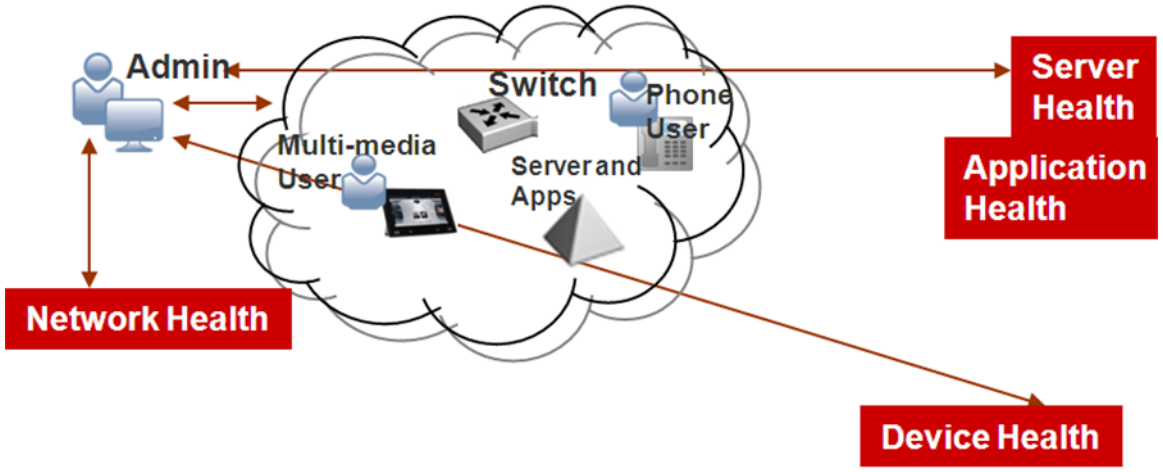
You can delve deeper into the device health from the dashboard by clicking on an interface item in the Availability, or Status. The Monitoring opens a transient dashboard for the specific interface.

Navigation between dashboards

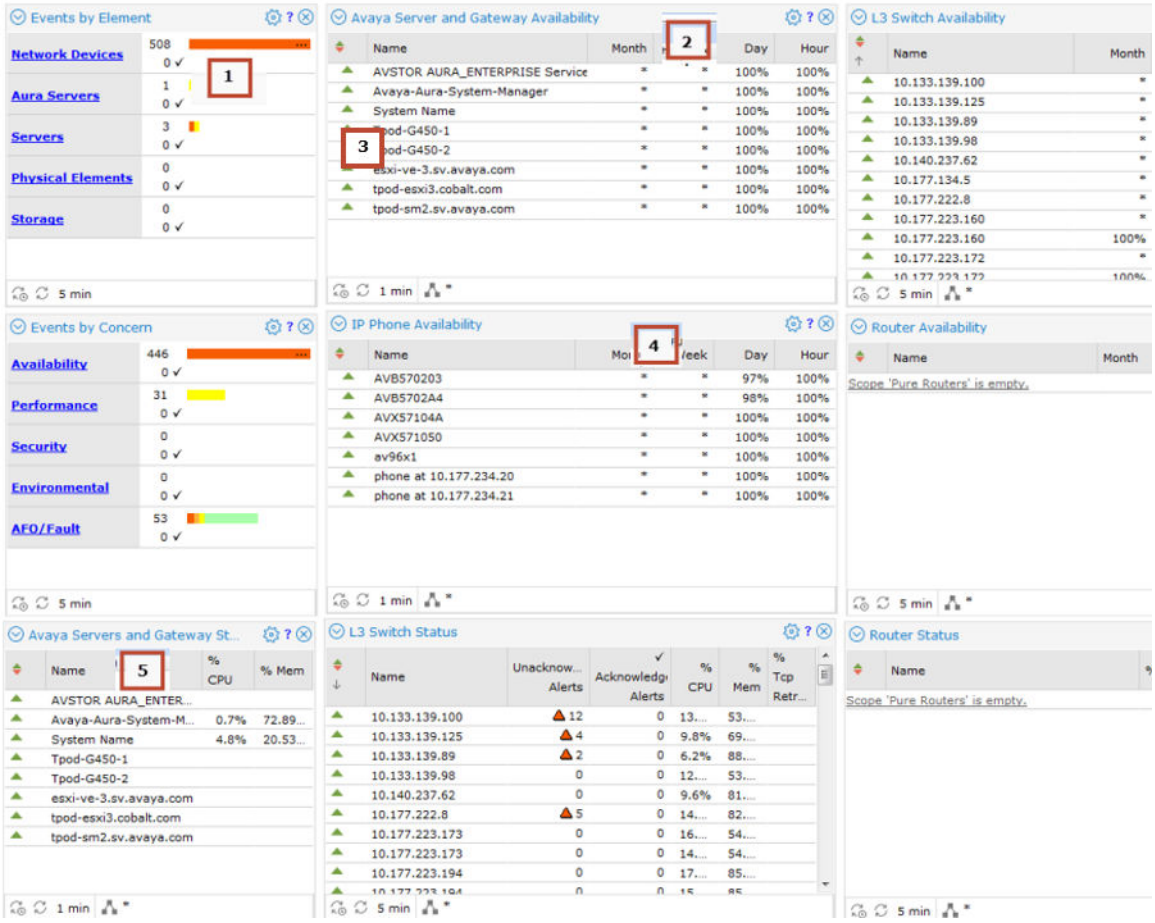
The following figures demonstrate how you can navigate between dashboards to delve deeper into device or system health.

Integrated dashboards for Aura System Health

The following figure demonstrates the multiple levels of dashboards used to monitor Aura System Health.



The following figure demonstrates a general overview of an integrated dashboard for Aura System Health.



1. Event summary dashlet showing current event count (based on severity) for Aura servers
2. Availability dashlet showing current and historical availability for the servers and gateways
3. Click on a specific server or gateway to open a transient dashboard page for that server or gateway
4. Availability dashlet showing current and historical availability for endpoints
5. Servers and gateway status dashlet showing alerts status for servers and gateways

Power Savings dashboard

The Power Savings dashboard displays dashlets containing information about total network power savings and top switch watt reduction. To access the dashboard, select **Network** > **Overview**, and select **Power Savings**.

The Power Savings dashboard includes the following dashlets:

- Average daily energy savings (kWh) vs. Total real-time savings
- Top Switches by Total Watt Reduction
- Top Switches by PoE Watt Reduction
- Top Switches by Slowdown Watt Reduction

Note:

The Power Savings dashboard only displays information for devices that support PoE.

Top-N Reports Dashboard

You can access Top-N availability and Inventory reports. Click **Network** > **Overview** to display the overview, and select **Top-N Dashboards**. The Top-N Dashboard displays the top ten dashlets for CPU and memory utilization, and for interface statistics such as utilization, traffic, errors and discards.

The Top-N Reports include the following:

- Top 10 Devices by CPU Usage
- Top 10 Devices by Processor Memory Used
- Top 10 Interfaces by In Util
- Top 10 Interfaces by Out Util
- Top 10 Interfaces by Traffic In
- Top 10 Interfaces by Traffic Out
- Top 10 Interfaces by Errors In
- Top 10 Interfaces by Errors Out
- Top 10 Interfaces by Discards In
- Top 10 Interfaces by Discards Out

Dashboard configuration

A dashboard displays information about the system health, and consists of different dashlets that delve deeper into the network health. You can add, delete, or clone a dashlet to configure the dashboard.

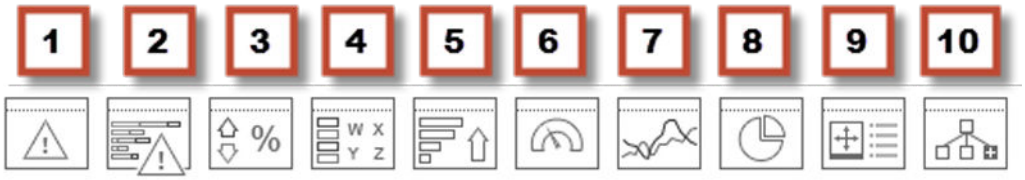
The dashboard configuration buttons refer to the different dashlets that you can add to the dashboard. You can drag and drop a dashlet onto the dashboard canvas, and use the dashlet wizard to configure each dashlet.

You can access the dashboard information by clicking **Network** > **Overview**.

To view the dashboard configuration buttons, click the following icon.

To hide the dashboard configuration button, click the following icon.

The following figure displays the dashboard configuration buttons.



The following list describes the dashboard configuration buttons.

1. Event Listing
2. Event Summary
3. Availability Report
4. Element Status Summary
5. Top-N Report
6. Dial Gauge
7. Trend Chart
8. Pie Chart
9. Element Property Table
10. Schematic

When you add a dashboard, the system asks if you want to save as public or private.

Dashboard configuration

Monitoring offers multiple levels of dashboards to monitor system health. You can configure a dashboard to monitor network health, application and server health, and device health. You can create a different dashboard for every model of equipment on the system, and you can modify a dashboard to make the dashboard a default dashboard for a device.

1. To access dashboards, select **Network** > **Overview**, and the overview appears.
2. If you cannot see the dashboard toolbar, click on the grey drop-down arrow above the content panel.

There are three types of dashboards:

- Preconfigured—Includes the following:
  - Network Overview, which displays information about network health
  - Power Savings Dashboard, which displays dashlets containing information about total network power savings and top switch watt reduction
  - Top-N Dashboard, which displays the top ten dashlets for CPU and memory utilization, and for interface statistics such as utilization, traffic, errors and discards

- Transient—Displays information about a specific network element.
- Customized—You can configure the dashboard by adding, deleting, or cloning a dashlet to delve deeper into the network health.

Adding a dashboard

About this task

Use this procedure to add a new dashboard.

You can also clone an existing or transient dashboard using the **Save dashboard as** option.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Click **New dashboard**, which is the plus sign on the left of the toolbar.
4. In the Prompt dialog box, enter the new dashboard name.
5. To permit other users to view your changes, select **Public**.

   You must have administrator privileges to save a dashboard in the public folder.
6. Click **OK**.
7. Drag and drop a dashboard configuration button onto the square that appears in the work area.

   A configuration dialog box specific to the dashlet you selected appears. This is the beginning of the dashlet wizard.
8. Enter information in the configuration dialog box.
9. If you do not edit dashlet items or other variables, click **Finish**.

   If you edit dashlet items or other variables, select one of the following actions:

   - Add
   - Delete
   - Edit

   Another configuration screen appears. After you complete each configuration screen, click **Next**.
10. After you complete the edits to the dashlet, click **Finish**.
11. To add another dashlet, repeat step 6 to step 10.
12. Click **Save dashboard**.

    For more information about configuring dashlets, see Dashboard wizards on page 21.

Variable definitions

The following table lists the dashboard configuration buttons.

Variable	Definition
Event Listing	Provides you with the events information of devices or interfaces, and can contain a maximum of 100 events. You can select events for a specific domain or all domains. To open another transient dashboard on the Event Listing dashlet, select Ack and click on the subject of the event.
Event Summary	Displays the summary of events by either domain classification or by concern. To open an event browser tab with the filter automatically applied for that classification on the Event Summary dashlet, click on an entry.
Availability Report	Displays the average availability for a class of elements as percentages over intervals of hour, day, month, or year. To view a transient dashlet for the element on the Availability Report dashlet, click on the element name.
Element Status Summary	Displays the KHI status of the element, including %CPU, %Memory, and number of alerts on the element. To open a transient dashboard for the element on the Element Status Summary dashlet, click on the element name.
Top-N Report	Top-N Reports are based on Scope and Time, and show histograms of devices and interface statistics. Top-N Reports are available for a current time or for a past time period, and can be exported to PDF, CSV or XML.
Dial Gauge	Provides a set of one or more dial gauges, each displaying the value of a domain element variable on an analog dial. All of the dial gauges in one set must display variables from the same domain element.
Trend Chart	Provides performance trend improvements and trending of device resource usage and key health indicators. Reporting is made easy by selecting trends and exporting information to PDF.
Pie Chart	Provides a set of one or more percentage pie charts displaying the following information: • Disk Usage—used space and free space • Host Memory—allocated space and available space
Element Property Table	Provides the properties of the device or interface on the dashboard.
Schematic	Displays the custom views on the dashboard.

Dashboard wizards

Each dashlet contains different elements that you must configure. After you drag and drop a dashlet onto the dashboard, a dialog box appears to help you configure the dashlet.

The following list outlines the dashlets that you can add to the dashboard.

- Event Listing
- Event Summary
- Availability Report
- Element Status Summary
- Top-N Report
- Dial Gauge
- Trend Chart
- Pie Chart
- Element Property Table
- Schematic

Configuring the Event Listing dashlet

Before you begin

You must create a dashboard or edit an existing dashboard.

About this task

Perform the following procedure to configure the Event Listing dashlet.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Drag and drop the **Event Listing** icon onto the canvas outlined on the Dashboard work area.
4. In the Name field, enter a name for the event listing.
5. In the Domain field, click the down arrow to select a domain.
6. Click **Choose a Scope**.

   The Choose a Scope page appears.
7. Select one or more scopes from the available list, and click **OK**.

   Note:

   You can use the Search field to search for a scope.
8. In the Events field, click on the Change field and select an event or events.
9. Click **OK**.
10. In the Rows/page field, enter the number of rows to appear in the dashlet.

11. The Columns sections displays the columns headers to appear in the dashlet.
    - To add a new column, click **Add**. From the list, select an item to appear in the dashlet.
    - To delete a column from the dashlet, highlight the item and click **Delete**.

    Note:

    Use the up or down arrows to move up or down the list of available column headers.
12. Click **OK**.

Result

Monitoring adds the Event Listing dashlet to the dashboard. To edit the Event Listing dashlet, click the **Configure** icon on the top right corner of each dashlet.

Configuring the Event Summary dashlet

Before you begin

You must create a dashboard or edit an existing dashboard.

About this task

Perform the following procedure to configure the Event Summary dashlet.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Drag and drop the **Event Summary** icon onto the canvas outlined on the Dashboard work area.
4. In the Name field, enter a name.
5. In the Event bar scale field, enter a number between 1 and 10000.

   Note:

   The Event bar scale is for the histogram bar. For example, if you enter 100 as scale and there are 10 events, then the bar is 1/10 of the available length. If you choose 1000, then the bar shrinks.
6. In the Items section, click **Add**.
7. In the Domains section, select a domain.
8. Click **Next**.
9. Click **Choose a Scope**.

   The Choose a Scope page appears.
10. Select one or more scopes from the available list and click **OK**.

Note:

You can use the Search field to search for a scope.

11. From the Configure dialog box, select one or more Events.
12. In the Item Title field, enter the item title.
13. To accept your changes and go to the next step of the configuration wizard, click **Next**.
    - To discard your changes and return to the previous step of the dashboard wizard, click **Previous**.
14. Click **Finish**.

Result

Monitoring adds the Event Summary dashlet to the dashboard. To edit the Event Summary dashlet, click the dashlet tool icon on the top right corner of each dashlet.

Configuring the Availability Report dashlet

Before you begin

You must create a dashboard or edit an existing dashboard.

About this task

Perform the following procedure to configure the Availability Report dashlet.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Drag and drop the **Availability Report** icon onto the canvas outlined on the Dashboard work area.
4. In the Name field, enter a name.
5. In the Domain field, click the down arrow to select a Domain.
6. In the Items section, click **Add**.
7. In the dialog box, select an element.
8. Check single elements or check a scope name to include all elements within a scope.
9. Click **Next**.
10. Select the Graph column checkbox, and use the drop-down menu to select a time frame for the report.
11. Select Filter by graph value, and use the drop-down menu to select a graph value of greater than, less than, greater or equal to, less than or equal to.
12. The Secondary columns section displays additional columns to appear on the dashlet.
    - To remove a column, click **Delete**.

- To add a column, click **Add**.

Note:

Use the up or down arrows to move up or down the list of available column headers.

13. Click **Finish**.

Result

Monitoring adds the Availability Report dashlet to the dashboard. To edit the Availability Report dashlet, click the dashlet tool icon on the top right corner of each dashlet

Configuring the Element Status Summary dashlet

Before you begin

You must create a dashboard or edit an existing dashboard.

About this task

Perform the following procedure to configure the Element Status Summary dashlet.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Drag and drop the **Element Status Summary** icon onto the canvas outlined on the Dashboard work area.
4. In the Name field, enter a name.
5. In the Domain field, click the down arrow to select a domain.
6. In the Dashlet Items section, click **Add**.
7. In the Perspective field, click the down arrow to select a perspective and then select an element.

   Only the first 100 scopes are shown if you select the perspective Scopes, select an element, and then check individual elements, or scope name to include all scopes.
8. Click **Next**.
9. To add the show reachability status icon to the dashlet, select **Show reachability**.
10. To add the unacknowledged status icon to the dashlet, highlight **Unacknowledged Alerts**.
11. To add the acknowledged alerts status icon to the dashlet, highlight **Acknowledged Alerts**.
12. If the dashlet items are correct, click **Finish**.

Result

Monitoring adds the Element Status Summary dashlet to the dashboard. To edit the Element Summary dashlet, click the dashlet tool icon on the top right corner of each dashlet.

Configuring the Top-N Report dashlet

Before you begin

You must create a dashboard or edit an existing dashboard.

About this task

Perform the following procedure to configure the Top-N Report dashlet.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Drag and drop the **Top-N Report** icon onto the canvas outlined on the Dashboard work area. The Dashlet items configurator dialog box appears.
4. In the **Name** field, enter a name.
5. In the **Domain** field, click the down arrow to select a Domain.
6. Click **Choose a Scope**.
7. Select one or more scopes from the available list and click **OK**.

   Note:

   You can use the Search field to search for a scope.
8. From the **Variable** field, select a variable.
9. To include all variables for this type of element, select the **Include all variables for this type of element** checkbox.
10. Select the filter checkbox, and enter the appropriate values.
11. In the **Top-N number** field, enter the number of items to appear in the Top-N Report dashlet.
12. In the Sort Order field, click **Bottom report** if you want to see the bottom first.
13. Select **Show reachability status** if you want to see this.
14. In the **Identification columns**, click **Add** and select the information you want to add.
15. In the Secondary value columns section, click **Add** and select the optional secondary columns to appear in the Top-N Report dashlet.

    To remove a secondary column, highlight a column header and click **Delete**.

    Note:

    Use the up or down arrows to move up or down the list of available column headers.
16. Click **OK**.

Result

Monitoring adds the Top-N Report dashlet to the dashboard. To edit the Top-N Report dashlet, click the dashlet tool icon on the top right corner of each dashlet.

Configuring the Dial Gauge dashlet

Before you begin

You must create a dashboard or edit an existing dashboard.

About this task

Perform the following procedure to configure the Dial Gauge dashlet.

Note:

Dial gauges support scope-based configuration. Only the first six elements of scope appear on the dial gauge dashlet.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Drag and drop the **Dial Gauge** icon onto the canvas outlined on the Dashboard work area.
4. In the **Domain** field, click the down arrow to select a domain.
5. In the **Perspective** field, click the down arrow and select a perspective from the available list.
6. From the folders or icons that appear in the box, navigate to the element you require. Click the plus signs at the left to expand the folders.
7. To input item parameters, click **Next**.
8. Click the **Choose a variable** field and select a variable.

   You can use the Search variable field to locate a variable.

   - To include all variables for this type of element select, **Include all variables for this type of element**.
   - To show thresholds, select **Show thresholds**.
9. Enter the Variable label.
10. In the Select units field, click on the down arrow to select a units field.
11. In the **Minimum** field, enter a value.

    The minimum value shows the lowest label in the dial gauge scale.
12. In the **Maximum** field, enter a value.

    The maximum value shows the highest label in the dial gauge scale.

Important:

The system displays the values for intermediate labels based on the values you enter for minimum and maximum labels. Intermediate labels are at fifth values between minimum and maximum. Ensure you configure minimum and maximum values to have integer intermediate labels.

13. In the Color zones field, click on the down arrow to select a value.

    The colors green, yellow, and red appear on the dial gauge based on the following configurations.

    - none—Indicates no color zones.
    - 1—Indicates one color zone. You can select a color. The from and to fields are preselected from start to end.
    - 2—Indicates two color zones. You can select a color for zone 1 and zone 2, and select the end location for zone 1 or the start location for zone 2.
    - 3—Indicates three color zones. You can select a color for zone 1, 2 and 3, and then enter a value in an available from or to field.

    Important:

    The zone to value must be more than the minimum range value. The zone from value must be less than the maximum value. If you enter incorrect zone values, the system displays a message indicating the value requirements.

14. Click **Next**.
15. Click **Finish**.

Result

Monitoring adds the Dial Gauge dashlet to the dashboard. To edit the Dial Gauge dashlet, click the dashlet tool icon on the top right corner of each dashlet.

Configuring the Trend Chart dashlet

Before you begin

You must create a dashboard or edit an existing dashboard.

About this task

Perform the following procedure to configure the Trend Chart dashlet.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Drag and drop the **Trend Chart** icon onto the canvas outlined on the Dashboard work area.

4. In the **Domain** field, click the down arrow to select a domain.
5. In the **Perspective** field, click the down arrow to select a perspective.
6. From the folders that appear in the box, navigate to the element you require.
   - If you select the Scope perspective, select an element and then check single elements or select a scope name to include all elements. The system displays the first 100 elements only.
7. Click **Next**.
8. In the dialog box, select an element from the list.
   - To add an element, click **Add**.
   - To delete an element, highlight the element and click **Delete**.
9. Click **Next**.
10. From the Choose time interval dialog box, click the down arrow and select a time interval from the list.
11. Use Current time draws the trend up to the current time. To show trends to another time range, remove the check from the **Use Current time** check box and select a fixed time.
12. Click **Next**.
13. In the Configure variables dialog box, click ***No variable selected*** to view all variables for which sufficient data has been collected to display in the dashlet.
    - To include all variables for this type of element, select the **Include all varialbes of this type of element** checkbox.
    - To show thresholds, select **Show thresholds**.
14. Select a variable.
15. In the Left axis variable (optional) field, select a variable if required.
16. To change the y-axis scale for the graph to show the trend plotting over a larger y-axis, check **Autorange**.
17. To view averages of the trend over an x-axis, check **Averaging Mode**.
18. In the Number of averaging intervals field, enter a value.

    The Number of averaging intervals calculates the averages for the x-axis. The number of the average intervals must be a minimum of 2. For example, if 6 is selected as the number of average intervals and if 10 minutes is the polling period, then the value is averaged over one hour.
19. In the Dashlet Title field, enter the name of the dashlet.
20. Click **Finish**.

Result

Monitoring adds the Trend Chart dashlet to the dashboard. To edit the Trend Chart dashlet, click the dashlet tool icon on the top right corner of each dashlet.

Configuring the Pie Chart dashlet

Before you begin

You must create a dashboard or edit an existing dashboard.

About this task

Perform the following procedure to configure the Pie Chart dashlet.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Drag and drop the Pie Chart icon onto the canvas outlined on the Dashboard work area.
4. In the Dashlet **Name** field, enter a name.
5. In the **Domain** field, click the down arrow to select a domain.
6. In the Dashlet items section, click **Add**.
7. Select a perspective.
8. From perspective list, select an element.

   If you select Scopes, select a scope name from the available list and then check individual elements or check the scope name to include all elements. Scopes that exceed undefined elements are not shown.
9. Click **Next**.
10. To add another dashlet item, repeat steps 6 to 9.
11. To add device name qualifier labels, select the **Add device name qualifier labels** checkbox.
12. To display variables by size, select the **Display variables by size** checkbox.
13. To show percents in legend, select the **Show percents in a legend** checkbox.
14. To show values in the legend, select the **Show values in legend** checkbox.
15. In the Pie variables section, click **Add**.
16. Select variables that are supported by dashlet items.
    - You can use the Search variable field to search for a specific variable.
    - To include all variables, check **Include all variables for this type of element**.

    After you select a variable, the system displays the variable name in the Variable or remainder title field.
17. To add another pie variable, repeat steps 11 to 18.

Note:

To complete the Pie Chart dashlet, you must select a minimum of two variables.

18. Click **Finish**.

Result

Monitoring adds the Pie Chart dashlet to the dashboard. To edit the Pie Chart dashlet, click the dashlet tool icon on the top right corner of each dashlettest.

Configuring the Element Property Table dashlet

Before you begin

You must create a dashboard or edit an existing dashboard.

About this task

Perform the following procedure to configure the Element Property Table dashlet.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Drag and drop the **Element Property Table** icon onto the canvas outlined on the Dashboard work area.
4. In the Domain field, click the down arrow to select a domain.
5. Click **Next**.
6. Select a Perspective from the drop-down menu.
7. From the folders that appear in the box, navigate to the element you require.
8. Click **Finish**.

Result

Monitoring adds the Element Property Table dashlet to the dashboard. To edit the Element Property Table dashlet, click the dashlet tool icon on the top right corner of each dashlet.

Configuring the Schematic dashlet

Perform the following procedure to configure the Schematic dashlet.

Before you begin

- You must create a dashboard or edit an existing dashboard.
- You must create at least one custom view in the Custom Views perspective of the Network Topology. For information about creating custom views, see Saving custom views on page 66.

Procedure

1. Select **Network** > **Overview**.

2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. Drag and drop the **Schematic** icon onto the canvas outlined on the Dashboard work area.
4. In the **Domain** field, click the down arrow to select a domain.
5. In the **Perspective** field, click the down arrow to select a perspective.
6. From the folders that appear in the box, navigate to the element you require.
7. Enter a dashlet name in the **Dashlet Name** field.
8. Select the **Display Heat Map** checkbox if you want to display the heat map.
9. Select the **Pie Chart Heat Map** checkbox if you want to pie chart the heat map.
10. Click **Next**.
11. Choose a variable.
12. Enter a minimum value and radius.
13. Enter a maximum value and radius.
14. Select the **Hide Element Icons on Schematic** checkbox if you want to hide element icons.
15. Click **Next**.
16. Select a color.
17. Click **Finish**.

Result

Monitoring adds the Schematic dashlet to the dashboard. To edit the Schematic dashlet, click the dashlet tool icon on the top right corner of each dashlet.

Viewing the dashboard for a device

About this task

Perform the following procedure to view the dashboard for a device.

Procedure

1. Select **Network** > **Topology**.
2. From the Network Topology center pane, right-click on a device.
3. From the application menu, select **Show Dashboard**.

Deleting a dashboard

About this task

Perform the following procedure to delete a dashboard.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.
3. From the Network Overview page, select a dashboard from the left of the screen.
4. From the menu bar, click **Delete dashboard**.

   If you do not see the delete option, click on the grey drop-down arrow in the top middle of the content pane.
5. In the Confirm dialog box, click **OK**.

Renaming a dashlet

About this task

Perform the following procedure to rename a dashlet.

Procedure

1. Select **Network** > **Overview**.
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the dashboard.
3. Click **Configure** on the top right of the dashlet.
4. In the Prompt dialog box, enter a new dashlet name in the Name field.
5. Click **Finish**.

Editing a dashlet

About this task

Perform the following procedure to edit an existing dashlet on the Monitoring dashboard.

Procedure

1. Select **Network** > **Overview**
2. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the content pane.

3. From the Network Overview page, select a dashboard from the left of the screen.
4. Select a dashlet to edit and click on the Configure icon on the top right corner of the dashlet.
5. Enter information in the configuration dialog box.
6. If you do not edit dashlet items or other variables, click **Finish**.

   If you edit dashlet items or other variables, select one of the following actions:

   - Add
   - Delete
   - Edit

   Another configuration screen appears. After you complete each configuration screen, click **Next**.
7. After you complete the edits to the dashlet, click **Finish**.

Updating a dashlet

About this task

Perform the following procedure to immediately update a dashlet.

Procedure

1. Select **Network** > **Overview**.
2. Select a dashboard on the left.
3. Select a dashlet in the content pane on the right.
4. On the selected dashlet, click **Update** on the bottom left of the dashlet.

Configuring auto refresh for a dashlet

About this task

Perform the following procedure to specify the time interval for Monitoring to update the dashlet.

The time intervals are:

- 20 minutes
- 5 minutes
- 1 minute
- 30 seconds
- 15 seconds
- Off

Procedure

1. Select **Network** > **Overview**.
2. Select a dashboard on the left.
3. Select a dashlet on the right.
4. Click **Update interval** on the bottom left of the dashlet.
5. Select a time interval.
   - Or, to turn the update interval off, select **Off**.

Chapter 4: Network Discovery

Network Discovery conceptual information

Use the following information to understand Network Discovery in the system under **Network** > **Discovery**.

Network Discovery

You must configure Network Discovery to run network auto-discoveries. A discovery is a snapshot taken of a part or a complete network. Select **Network** > **Discovery** to access the Network Discovery options.

You must complete the following steps after you log on to the system for the first time, and before you can browse your network.

- Configure device credentials using the Device and Server Credentials Editor available from **Administration** > **Credentials**.
- Select the Default discovery domain, or add a new discovery domain.
- Configure the discovery options for the discovery domain.
- Discover the domain.

Important:

A device must have SNMP credentials and be able to respond to SNMP for the system to add the device to the Device and Service Credentials Editor. If a device changes from Unmanaged to Managed by either adding credentials for the device or by enabling SNMP on the device after the discovery is completed, you must run rediscovery on the domain, or create a new domain to discovery the device.

On the Network Discovery page, you can work with discovery domains, configure discovery options, perform discoveries, and view discovery status.

General controls

Note:

Monitoring supports two types of licenses, Basic and Advanced, in addition to different license tiers: 250-Node, 1500-Node, and 5000-Node. The options and sub-menu may be disabled or hidden depending on the type of license you install.

License tier	Networking nodes	Other nodes (Includes items such as server and phones)	Total nodes
250-Node	250	750	1000
1500-Node	1500	4500	6000
5000-Node	5000	25,000	30,000

The following general controls are available on the Network Discovery page, under **Network** > **Discovery**.

Name	Description
Apply your changes	Saves the edits to the server. All edits you make to the domain configuration are client-side only. Click **Apply** to save the edits to the server.
Discard changes, reverting to the previous values	Discards any unapplied edits you have made to a discovery configuration. You are not asked to confirm a revert action, any unapplied edits are immediately lost after you click **Revert**.
Add a new domain	After you click this button, a dialog box appears for the discovery domain name. Each discovery domain must have a unique name that may include numbers, letters with spaces, underscores (_) or hyphens (-) but not special characters.
Delete selected domain	Deletes the selected discovery domain. The system prompts you to confirm the deletion prior to it taking effect. After you delete a discovery domain you permanently delete the domain configuration, all discoveries and logs made from it, and any persistent history metric, and the persistent form of currently posted events. Delete operations cannot be undone.
Clear out all discovered and monitored data	Deletes the domain data such as custom views, trends, events, traps, event history, and monitoring data while keeping the seed definition and device custom names. After you clear the data for the selected domain, perform a network discovery to start a new discovery.
Clone selected domain	Clones the selected discovery domain. When you clone an existing discovery domain, you create a new domain using the discovery configuration of the existing domain. No other information is cloned. After you clone a domain, you must perform a discovery before you can browse or monitor the new domain. The same rules for domain names apply for cloned domains as for those created using the create operation.
Discover selected domain	Initiates the discovery of the domain.
Manual Discovery	Initiates the manual discovery of the domain.
Discovery Problem Report	Takes you to the Discovery Problem Report screen where you can choose to view the discovery report for one or all domains.
Save Domain	Saves the domain. Larger domains require longer save times.

Table continues…

Name	Description
Auto-refresh	Turns on or off servlet refresh or changes the refresh interval. The default is auto refresh every 15 seconds.
Refresh	Refreshes the servlet once. The refresh is performed immediately.
Start/Stop Monitoring	Starts or stops monitoring of the discovery domain. By default when the domain is discovered only Start Monitoring is available.

Default discovery options

The system ships with a default domain. You cannot remove the domain or tab from Monitoring, but you can delete the content, seeds, and discovery data from this domain, and refine a new seed, and then run discovery. To access the options, go to **Network** > **Discovery**, and go to the options on the bottom left. The **Configuration** tab uses the domain information for network elements.

By default, the discovery has the following options:

- Wide Area Network (WAN) Crawl (not selected)—Monitoring discovers devices on the far side of every router interface, regardless of the interface type. If the WAN Crawl option is not selected then Monitoring Discovery does not go beyond any interface that is considered to be a WAN interface. You need an Advanced license to access the Wide Area Network (WAN) Crawl option.
- VPN Crawl (not selected)—Monitoring discovers VPN clients even if this option is not selected. If this option is checked, then the discovery algorithm augments the discovered data with the information from vendor-specific VPN Tables. You need an Advanced license to access the VPN Crawl option.
- DNS Lookup (not selected)—Monitoring performs DNS lookup on all devices.
- Service by Port Scan (not selected)—Monitoring discovery scans for well known service ports on servers. The option looks for services running on a server at the time of discovery. You need an Advanced license to access the Service by Port Scan option.
- For All Devices (not selected)—Monitoring performs a service by PortScan for all devices. You need an Advanced license to access the For All Devices option.
- Multi-vendor discovery (not selected)—Monitoring discovers devices from multiple third party vendors.
- Host Storage Discovery (not selected)—Monitoring discovers file systems based on Linux log-in and scan of file systems on a server.

The options above exist at the bottom left of the screen for **Network** > **Discovery**.

Domain, campuses, and seeds

After you go to **Network** > **Discovery**, the following are part of the discovery:

- Domains
- Campuses

- Seeds

Domains

With Monitoring, you manage discovery domains. A discovery domain is a virtual container of network objects or applications. A discovery domain can be a part of your network or the entire network, depending on how you want to manage a discovery domain. A discovery domain can be a device or an application. Monitoring supports multiple discovery domains. You can manage and browse each discovery domain independently of the others.

Important:

You can have multiple domains if your enterprise has disjointed networks. For example, if your site has an internal production network and a DMZ. Each would be their own separate domain that you can discover and monitor.

Important:

An object can appear as a managed object (MO) in more than one discovery domain. The object is counted as an MO in each discovery domain in which the object appears because you can apply a different action to each instance of the MO in each Monitoring discovery domain.

Campuses

A campus is a location at which devices reside, such as an office, a building, or a set of buildings. Campuses are defined by devices separated by wide area links (for auto-discovered campuses). Subnet discovery might collapse several campuses together. Monitoring discovery automatically determines what constitutes a campus. The campus name is based on:

- Best router (The best router is usually the seed by which the campus was discovered. This is usually the edge router, unless the seed is explicitly specified.)
- First discovered switch
- First subnet

After Monitoring performs a discovery, you can navigate between network layers to view your network topology. If you selected WAN Crawl, you start with a domain view of all campuses. Selecting a campus gives you a view of all discovered devices within that campus, which you can then select individually to view the device details. If you did not select WAN Crawl, the network browser defaults to the campus view.

Router, subnet, and generated router seeds

A seed is the starting point of a discovery. There are three types of seeds:

- A router seed, which is specified by the IP address or DNS name of the router
- A subnet seed, which is specified by a subnet's IP address and subnet mask
- A generated router seed, which the Monitoring identifies from a large set of possible addresses that have been detected by Monitoring when the subnet partitioning option is selected

For example: a.b.c.d/n IP address 134.68.1.1 DNS name nmos_dns.avaya.us.com 255.255.123.1/134 The same seed can be used for multiple domains. Both IPv4 and IPv6 standard syntax is supported for seeds.

Important:

For IPv6, Monitoring does not support subnet discovery seeds larger than Class B or 16-bit address spaces.

The discovery begins with the seed(s) you provide and follows all leads from them, such as ARP cache entries and contiguous IP addresses, to discover the domain circumscribed by the configuration data you supply. Routers are the preferred type of discovery seed, enabling the simplest discovery. Once the router specified by the seed is discovered, the discovery proceeds with every device listed in the ARP cache of the router, within the bounds defined by the discovery configuration.

Subnets are useful as discovery seeds also, but the resulting discoveries may be slower than those performed using routers. This is because the discovery probes all addresses in the subnet range, even if most are not in use, and the discovery probes addresses without corresponding devices until timeout. Use subnets as discovery seeds if your network has no router, or if the discovery misses important devices when the discovery uses a router as the discovery seed.

For example, if you want to discover a network with two subnets and nothing beyond the network: Add the IP address of the router or routers as a seed, and then add the two subnets within the Limit to Subnets.

If you have a large subnet (larger than Class C), you can use a partitioning subnet seed instead of a regular subnet seed. A partitioning subnet seed partitions large subnets to find reachable devices and determines which ones are routers. For subnets that are between Class C and Class B in size, you can use either:

- A regular subnet seed, in which case every address in the range will be probed during discovery
- A partitioning seed, in which case a subnet will be probed and Monitoring will use a set of routers within the subnet as seeds

You have the following options to configure your discovery:

- Seeds and seed groups—The starting point of a discovery (router or DNS name). You can group router seeds and subnet seeds, and merge results of subnet seeds into one campus.
- Limit to subnets—You can limit the extent of a discovery by specifying subnets to which the discovery is restricted. Restricting the discovery to one or more specific subnets is useful for narrowing the scope of a discovery to a specific portion of your network, and devices that are not members of those subnets are not discovered.
- Exclusions—You can limit the extent of a discovery by specifying filters that exclude parts of your network that match the conditions of the filter.
- Options—You can specify the manner in which the discovery crawls your network (Wide Area Crawl, VPN Crawl, DNS Lookup, Service by Port Scan, For All Devices, Multi-vendor Discovery, and Host Storage Discovery).

Important:

To discover a device properly, the device must respond to SNMP v1 queries.

Media application discovery

If your discovery domain includes a media application server, the Monitoring automatically discovers the following applications as part of its discovery process:

- Multimedia Conferencing
- NES Interactive Communications Portal (NES ICP)

For more information on supported releases, see *Deploying Extreme Fabric Orchestrator*, NN48100–101.

To have Monitoring automatically discover these applications, you must include the media application server in the discovery recipe. You must also configure the device credentials for the media application server in the Device and Server Credentials Editor available from **Administration** > **Credentials.**

The user interface displays discovered applications on the Network Topology page; select the Applications perspective to view them. To select the Applications perspective, go to **Network** > **Topology**, and then use the drop-down menu on the tree to the left. Select **Applications** from the drop-down menu.

Discovery licensing restrictions

There are discovery restrictions because of licensing.

The following discovery restrictions apply:

- The license you purchase determines the number of managed devices you have permission to discover and monitor. If, during discovery, you reach the maximum limit for the number of managed devices that can be discovered as defined by your license, you receive a message indicating that you have met this limit. Although there is a limit to the number of managed devices that can be discovered, there is no limit on the domains. For example, if you have a license for 1000 managed devices, you can create and discover as many domains as you would like, but the sum of all managed devices across the domains you manage cannot exceed 1000.
- The license count does not take into consideration the uniqueness of a managed device being discovered under multiple domains. For example, if the same managed device gets discovered in two different domains the license count will increment twice. Once for being discovered in each domain.
- Your license restricts the managed device count. This restriction is based on managed device count, not on the total count of all devices.
- You can have different functions or actions associated with a managed device if it is discovered in multiple domains.

Network Discovery management

This section provides information and procedures for using the Network Discovery feature.

Shortest Path Bridging

Shortest Path Bridging (IEEE 802.1aq) provides logical Ethernet networks on native Ethernet infrastructure using a link state protocol to advertise both topology and logical network membership.

Packets are encapsulated at the edge either q-in-q IEEE 802.1ad (SPBV) or in MAC-in-MAC IEEE 802.1ah (SPBM) frames and transported only to other members of the logical network.

SPB uses the link state protocol (IS-IS) to discover and advertise the network topology and compute shortest path trees from all bridges in the SPB Region.

SPB supports unicast and multicast, and all routing is on symmetric shortest paths. Many equal cost shortest paths are supported.

Shortest Path Bridging MAC

Shortest Path Bridging MAC (SPBM) is a standard Ethernet control plane that combines the positive attributes of routing with switching for all paths active, and rapid failure restoration and scalability. SPBM enables both campus and data center solutions by enabling sever consolidation and virtualization for data centers, and provides campus benefits such as plug and play deployments and simplification of the internet protocol. SPBM provides IP shortcuts to simplify routing and IP VPFN, and provides resilient access and coexistence with SMLT and MSTP.

Shortest Path Bridging MAC provides the following solutions:

- Scalability such as MAC address explosion
- Loop prevention and suppression
- All links used to prevent blocking and wasting link resources
- Shortest path for unicast and multicast traffic
- Flexible core topologies compared to SMLT
- Ease of provisioning
- Service virtualization (L2, L3 VSNs)
- Simple encapsulation

SPBM workflows

The following sections describe various SPBM workflows.

Note:

For SPBM L2 Diagnostic Tools to operate properly, in the Credentials page, you must provide write credentials for all SPBM enabled devices.

SPBM discovery

The following list outlines the workflow for an SPBM discovery.

- Discover customer VLANs (C-VLAN).
- Discover backbone VLANs (B-VLAN).

- Discover IS-IS interfaces, their admin state, and adjacencies for each SPBM-enabled node.

SPBM Visualization

The following list outlines the workflow for SPBM visualization.

- Create a scope to get a list of SPBM-enabled devices on the network.
- Provide an SPBM perspective that displays the SPBM schematic of the discovered SPBM areas in the campus.

  On the left navigation pane, display the SPBM areas discovered and for each SPBM area, and display the following:

  - Devices
  - B-VLANs
  - C-VLANs
  - L3 VPN (VRF)
- To display the schematic for the SPBM, click on a SPBM area in the navigation pane.
- To display details of the VLAN or VRF in a tabular format, click on a SPBM area in the navigation pane. You can right-click on an element to highlight an element of the VLAN or VRF on the schematic.
- If you click on a device in the left navigation pane, a tabular view of the SPBM configuration on the device appears with the following information:

  - I-SIDs configured
  - B-VLANs configured
  - C-VLANs configured
  - L3 VPNs (VRFs) configured

SPBM monitoring

There are various monitoring aspects for Shortest Path Bridging MAC (SPBM). Any change in the network creates a change in the network topology. Therefore the network participants, or the nodes, must quickly become aware of changes and adjust their shortest path algorithm to each destination as quickly and efficiently as possible through SPBM. Each node maintains a list of adjacencies and creates a list of shortest path computations that you must monitor.

Virtual Routing and Forwarding

In IP-based computer networks, Virtual Routing and Forwarding (VRF) is a technology that allows multiple instances of a routing table to coexist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.

For information on Extreme Networks devices that support VRF, see *Deploying Extreme Fabric Orchestrator*, NN48100–101.

Layer 3 subnet partitioning

The Layer 3 subnet partitioning feature is a discovery phase that you can execute prior to performing a normal network discovery. When you use the Layer 3 partitioning feature, Monitoring

executes a discovery phase that takes as its starting input one or more large subnet seeds. From these seeds, Monitoring analyzes the network and produces generated router IP address seeds that you can use in the place of input subnets for the main discovery.

Device discovery

Monitoring can discover devices that support the following protocols:

- 802.1ab (Link Layer Data Protocol, or LLDP)

  Note:

  ERS 8000 and VSP 9000 devices do not support LLDP.

- Discovery Protocol (NDP), formerly known as Bay Networks Autotopology Discovery Protocol, or SynOptics Network Manager Protocol (SONMP)

One of these protocols must be enabled on the device for Monitoring to discover the device.

For more information on configuring device credentials for network discovery, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

IEEE 802.1ab

Network Discovery supports the discovery of devices using IEEE 802.1ab, Station and Media Access Control Connectivity Protocol, or Link Layer Discovery Protocol (LLDP). Network Discovery uses both 802.1ab and the Discovery Protocol (NDP), formerly Bay Networks Autotopology Discovery Protocol, to discover the devices on the network.

With 802.1ab, stations connected to a LAN can advertise their capabilities to each other, enabling the discovery of physical topology information for network management. The 802.1ab-compatible stations can consist of any interconnection device, including PCs, IP phones, switches, access points, and routers. Each station stores 802.1ab information in a standard Management Information Base (MIB), allowing Monitoring to access the information.

With 802.1ab, Monitoring can discover certain configuration inconsistencies or malfunctions that can result in impaired communications at higher layers, such as duplex mismatches.

Each 802.1ab station:

- Advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN.
- Receives network management information from adjacent stations on the same LAN.

The following devices support 802.1ab:

- Ethernet Routing Switch 55xx Release 5.x and above
- Ethernet Routing Switch 8300 Release 3.x and above
- Ethernet Routing Switch 45xx Release 5.x and above
- Ethernet Routing Switch 25xx Release 4.x and above
- Ethernet Switch 325/425 Release 3.x and above

- Ethernet Switch 470/460 Release 3.x and above
- Avaya IP Phones

With 802.1ab support, Monitoring is not restricted to the discovery of approved vendor devices, and can discover any 802.1ab-enabled devices on the network, including multi-vendor switches, routers, and IP Phones.

Important:

Monitoring can discover third-party 802.1ab-enabled devices on the network but cannot provide management for these devices.

The following figure shows an example of how 802.1ab works in a network.

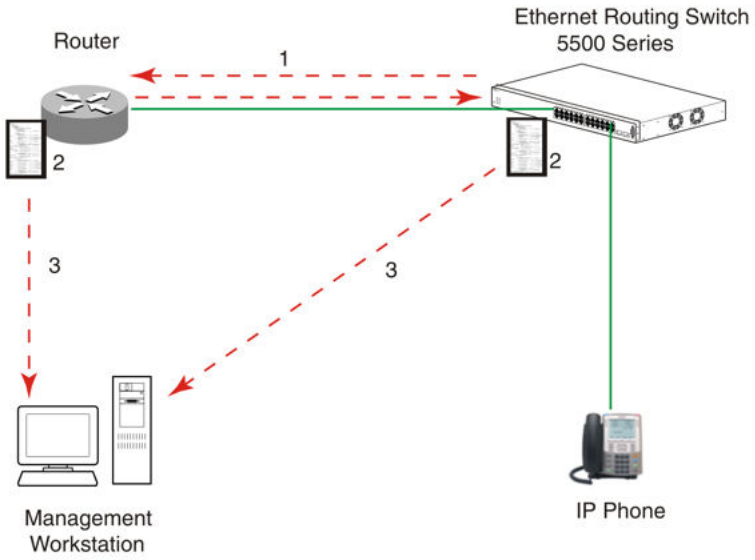


Figure 1: How 802.1ab works

1. The Ethernet Routing Switch and 802.1ab-enabled router advertise chassis/port IDs and system descriptions to each other.
2. The devices store the information about each other in local MIB databases, accessible by using SNMP.
3. A management workstation running Extreme Fabric Orchestrator (EFO) retrieves the data stored by each device and builds a network topology map.

The system displays both approved vendor devices and multi-vendor devices.

IEEE 802.1ab

To enable discovery of a device through 802.1ab, you must enable the following TLVs on the device:

- System Name TLV

- System Capabilities TLV
- Management Address TLV

To enable discovery of MED endpoints, you must also enable the MED TLVs on those endpoints. For more information about configuring 802.1ab on your device, see the documentation for your device.

Network Discovery configuration

Use the following information to configure network discoveries on your Monitoring.

For information about performing a network discovery, see Performing an initial discovery on page 47.

Network Discovery page

To access the Network Discovery, go to **Network** > **Discovery**. On the Network Discovery page, you can perform the following discoveries:

- VMs
- Avaya Aura components, and Layer 7 association of Aura components
- SPBM
- VRF discovery and visualization
- Windows and Linux
- Visualization of slot port module
- RSMLT
- Stackable elements and visualization of stacks
- Additional phone properties

Monitoring key features include the following:

- Router and subnet seed for discovery
- Campus or branch office discovery
- Port scan during discovery detects services on servers
- Storage and file system discovery
- Discovery of both managed and unmanaged devices

Discovery features include the following:

- Discovery of CM, SM, SMGR and Gateways

- Application level discovery
- Port scan during discovery detects services and process
- File system discovery
- Discovery of IP phones – H.323 and SIP
- Discovery of gateways and trunks
- Discovery of Fiber Channel over Ethernet (FCoE) or iSCSI
- Discovery of ToR VSP 7000

Performing an initial discovery

You can perform a discovery for the chosen domain. A discovery is a snapshot taken of part or all of a network. A single domain usually has many discoveries made of the domain over time.

Important:

The default discovery policy only discovers verified vendor devices. To perform a full device discovery, you must edit the options to select a multi-vendor device discovery.

Before you begin

- Configure domain discovery options including Seeds, Limit to Subnets, Exclusions, and Options.

Procedure

1. Select **Network** > **Discovery**.
2. Select the domain you want to discover.
3. Click **Discover selected domain** from the top menu bar.

   A confirmation dialog box appears to confirm the discovery.

   Note:

   Select the appropriate merge policy that applies to your needs only at the end of rediscovery.
4. Click **OK** to start the discovery.

Result

A notification displays the discovery status. The status shown is ACTIVE when discovery is in progress.

Note:

Discovery is queued if a backup is in progress. The status shown is QUIESCENT and discovery begins once the backup is completed.

If discovery results seem incomplete or incorrect, check the following:

- Check to see if the credentials are added for the devices that are not discovered. Go to **Administration** > **Credentials**.

Important:

You must add the credentials for the router seed for the discovery, and the credentials for all the devices in the network.

- Check to see if the SNMP (v1 or v3) is enabled on the undiscovered device or devices.
- On some devices (for example VPN routers), you must configure the IP address of the Monitoring server in order for them to respond back to SNMP queries sent by Monitoring.
- Ensure that a proper seed is used. An improper seed can occur if the device used as seed is not reachable from the Monitoring server. If some devices are separated by a firewall, you should provide a minimum of two seeds, as seeds for the routers from both sides of the firewall.
- Ensure that you use the correct discovery options. Make sure that WAN Crawl, VPN Crawl, DNS Lookup and Discovery are set correctly.
- Ensure that the system has not reached the License Node Count cap. If is reached, discovery stops before the discovery completes and displays a corresponding error message.
- If a switch or AP is not discovered correctly and the switch or access point is hanging off of an undiscovered core switch, troubleshoot undiscovered core switch before the edge.
- Check the discovery logs by clicking the **Discovery problem Report** button on the discovery browser tool bar. You can optionally access the discovery logs by navigating to **Reports** > **Discovery Reports**. Take corrective action indicated by the logs. For example, if you see an SNMP time out, check the device using the MIB browser.

Performing a domain rediscovery

You can perform a rediscovery of the chosen domain. A discovery is a snapshot taken of part or all of a network. A single domain usually has many discoveries made of the domain over time.

Important:

The default discovery policy only discovers verified vendor devices. You must edit this default for full multi-vendor discovery.

Before you begin

- Configure domain discovery options including Seeds, Limit to Subnets, Exclusions, and Options.

Procedure

1. Select **Network** > **Discovery**.
2. Select the domain you want to discover.
3. Click **Discover selected domain** from the top menu bar.

4. From the Confirm dialog box, select the appropriate merge policy that applies to your needs. The following options are available:
   - **Retain missing equipment if possible**—Retains information about equipment found in a past discovery that is not found upon rediscovery. The system retains this information over three rediscoveries. If the equipment is missing three times the equipment is automatically removed.
   - **Rediscover from scratch retaining states** —Retains information about equipment found in past discoveries and also finds all equipment from scratch.
   - **Rediscover from scratch**—Does not retain information about equipment found in past discoveries and instead finds all equipment from scratch.
   - **Retain equipment unless marked to remove** —Retains information about equipment found in a past discovery unless marked to remove.
5. Click **OK**.

Refreshing discovery status

You can configure the discovery status of a domain to refresh or auto-refresh.

Before you begin

- Add a domain.
- Configure domain discovery options including Seeds, Limit to Subnets, Exclusions, and Options.
- Perform an initial discovery.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click the **Refresh** button in the top menu bar.

   The discovery status is refreshed.

Viewing discovery status summary

You can view the statistics about the discoveries you performed in the Discovery Status Summary box.

Procedure

1. Select **Network** > **Discovery**.
2. On the Domains page, click the domain tab corresponding to the domain for which you want to select an option.
3. View the discovery statistics for the selected domain in the Discovery Status Summary pane.

Variable definitions

Variable	Value
As of	The time (of client machine) at which the discovery status was refreshed. This is a read-only value.
Discovery State	The latest status of the discovery process. Valid values are: • In Progress—The discovery process is still in progress. • New Domain—The domain is not discovered. • Completed—The discovery process has finished. This is a read-only value.
Discovery Level	The type of discovery that was performed. Valid values are: • Initial Discovery—The discovery was the first discovery of the network. • Undiscovered—The discovery was not performed. • Full Rediscovery—The discovery was a rediscovery. • Manual Discovery—The discovery is for a particular device or devices. This is a read-only value.
Discovery Type	The discovery type. The possible discovery types are: • Add device discovery—Add device discovery means that Manual Discovery was used to add one ore more devices. • Full discovery—Full discovery means that the system completed a full discovery of the entire network. This is a read-only value.
Start Time	The server time at which the most recent discovery process initiated. This timestamp includes the time zone (GMT offset) of where the server is located. This is a read-only value.
End Time	The server time at which the most recent discovery process completed. This timestamp includes the time zone (GMT offset) of where the server is located. This is a read-only value.
Last Device Discovered	The last device discovered by the system during the discovery process.

Table continues…

Variable	Value
Campuses	A list of the campuses within your network that were included in the discovery. Individual campuses can be selected to display statistics for only that campus or All Campuses can be selected to display combined statistics (sum of all individual campuses) for all campuses within your network. For example, the values displayed in the Prev., Last, and Merged columns reflect values for either a single campus (if you select one campus), or the sum of all campuses if you select All Campuses. A campus is a location at which devices reside, such as an office, a building, or a set of buildings within a reasonably short distance of each other. This is a read-only value.
Element Type	The type of element that was discovered. Element types include: Access Router, Device, DSLAM, DSUCSU, Firewall, Interface, Manageable, Other, Phone, PLC, Printer/Server, Printer, Router, SAN Bridge, SAN Switch, Server, Switch (L2), Switch (L3), Switch/Router, Terminal Server, Unmanageable, VM Image, VPN Server, WAP This is a read-only value.
Prev. (Preview)	The number of each type of element that was discovered in the prior discovery. This is a read-only value.
Last	The number of each type of element that was discovered in the most recent discovery. This is a read-only value.
Merged	The sum of each type of element discovered in all discoveries taking into account the rediscovery policies used. The number of each type of element (the counts in each row) after the merge will differ based on the rediscovery policy used. This is a read-only value.

Viewing a discovery problem report

The left hand navigation pane on the Discovery Reports page organizes log messages based on category, severity, and IP address.

To troubleshoot why a particular IP address is not discovered or is discovered as unmanaged, locate the IP address in the left navigation pane.

One common reason for the system not to discover a device is the lack of response from the device from ping or SNMP requests sent from the system. In this case, ensure the SMGR device credentials are correct and then check for SNMP access using the SNMP MIB browser.

About this task

Use this procedure to view the logs related to a discovery.

Procedure

1. Select **Network** > **Discovery**.
2. Click **Discovery Problem Report** to open the Discovery Reports page and view the logs related to the discovery.
3. Select a node from the navigation pane.

Adding discovery domains

You must add a discovery domain before you can view your network. A discovery domain is the generic term for what you manage with Monitoring. A discovery domain is a virtual representation of part or all of a network.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click **Add a new domain**.
3. Enter a domain name for the domain that you are creating.

   Each domain must have a unique name. Names can include numbers, letters with spaces, underscores (_) or hyphens (-) but not special characters.
4. Click **OK**.

   The system adds a tab to the Network Discovery page for your newly created domain. The name of your domain appears in the tab area.

Deleting discovery domains

Delete the discovery domain configuration to remove the discovery domain from the list of domains.

You cannot delete the default discovery domain.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, select the domain that you want to delete.
3. Click **Delete selected domain**.

4. In the confirmation dialog box, click **OK**.

Deleting the data for a selected domain

About this task

Use the **Erase selected domain** data button to delete domain data such as custom views, trends, events, traps, event history, and monitoring data while keeping the seed definition and device custom names.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, select the domain for which you want to erase the data.
3. Click **Erase selected domain data**.

   A confirmation warning displays that all acquired and generated information including model, data, events, notifications, and logs for this domain will be deleted.
4. Click **OK** to erase the domain data.
5. Click **Discover selected domain** to start a new discovery.

Cloning discovery domains

Clone a domain to create a new domain using the existing discovery of the domain.

Important:

Cloning domains does not copy the discovered data. Cloning domains copies the discovery configuration. For example, the seed, limit to subnet, or exclusions. You cannot clone any other information and a discovery must still be performed before the new domain can be browsed or monitored.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, select the domain that you want to clone.
3. Click **Clone selected domain**.
4. Enter the new domain name.
5. Click **OK**.

   The tab of the cloned domain appears.

Adding seeds

After you add a new network discovery domain, you must configure a discovery recipe, which begins with adding a seed. Seeds are the starting point in a discovery. The discovery begins with the seed(s) you provide and follows all leads from them, such as ARP cache entries and contiguous IP addresses, to discover the domain. Routers are the preferred type of discovery seed, enabling the most straight forward discovery, but you can also use subnets as seeds.

If you have a large subnet (larger than Class C), you can use a partitioning subnet seed instead of a regular subnet seed. A partitioning subnet seed partitions large subnets to find reachable devices and determines which ones are routers.

Before you begin

- Add a network discovery domain; see Adding discovery domains on page 52.

Procedure

1. Select **Network** > **Discovery**.
2. From the Network Discovery page, select the domain tab to which you want to add a seed.
3. In the **Seeds** box, click **Add**.
4. Select **Seed**.
5. In the Add a new seed dialog box, select either **Router** or **IP Subnet** to indicate the type of seed you want to add.
6. Type a discovery seed in the box. If the seed is a subnet, select the subnet mask from the drop-down list.

   Discovery seeds can be a router IP address, a name, or a subnet address. This seed address facilitates the discovery of other elements in the campus. Both IPv4 and IPv6 standard syntax is supported.
7. Select the **Enabled** check box.
8. If you want Monitoring to partition the selected subnet to find router-based seeds, select the **Partition** checkbox.
9. Click **OK**.

   The system adds a list of router-based seeds to the seed list.
10. To save the changes, click **Apply your changes** in the top left toolbar.

Adding a seed group

Before you begin

- Add a network discovery domain. For more information, see Adding discovery domains on page 52.

About this task

Perform the following procedure to add a seed group to your discovery.

Procedure

1. Select **Network** > **Discovery**.
2. From the Network Discovery page, select the domain tab to which you want to add a seed.
3. In the **Seeds** box, click the **Add** button.
4. Select **Seed Group**.
5. In the Add a new seed group dialog box, enter the name of the seed group.
6. In the Seeds field, click **Add**.
7. Select either **Router** or **IP Subnet** to indicate the type of seed you want to add.
8. Type a discovery seed in the box. If the seed is a subnet, select the subnet mask from the drop-down list.

   Discovery seeds can be a router IP address, a name, or a subnet address. This seed address facilitates the discovery of other elements in the campus. Both IPv4 and IPv6 standard syntax is supported.
9. Select the **Enabled** check box.
10. If you want Monitoring to partition the selected subnet to find router-based seeds, select the **Partition** check box.
11. Click **OK**.

    The system adds a list of router-based seeds to the seed list.
12. To save the changes, click **Apply your changes**.

Editing seeds

Edit a seed to modify the value of the seed.

Before you begin

- Add a discovery domain and a seed. For more information, see Adding discovery domains on page 52.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click the domain tab corresponding to the domain for which you want to edit a seed.
3. From the **Seeds** box, select the seed you want to edit.
4. In the **Seeds** box, click **Edit**.

5. In the Edit the selected seed dialog box, modify the seed as needed.
6. Click **OK**.
7. To save the changes, click **Apply your changes** in the top left toolbar.

Deleting seeds

Delete a seed to end the discovery process associated with a seed.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click the domain tab that corresponds to the domain for which you want to delete a seed.
3. In the **Seeds** box, select the seed to be deleted from the list of seeds.
4. In the **Seeds** box, click **Delete**.

   There is no delete confirmation, the seed is deleted immediately.
5. To save the change, click **Apply your changes**.

Adding limits to subnets

You can limit the extent of a discovery by specifying the subnets to which the system restricts the discovery. Restricting the discovery process to one or more specific subnets is useful for narrowing the scope of a discovery to a specific portion of your network. Devices that are not members of the subnets are not discovered.

Before you begin

Important:

All seeds must be in the scope of the subnet constrain to form a valid discovery option.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click the domain tab corresponding to the domain for which you want to add a limit to subnets.
3. In the **Limit to Subnets** box, click the **Add** button.
4. Enter a value. You can enter more than one value.

   Examples of values are: `10.127.240.0/24`, `10.127.231.0/24`, and `10.126.0.0/16`.
5. After you finish entering values, click **OK**.

The new limit appears in the Limit to Subnets box.

6. To save the change, click **Apply your changes**.

Editing limits to subnets

After you limit the extent of the discovery by specifying subnets, you can modify your entry. If you set discovery constraints by specifying certain options like subnets, the domain discovery is limited to fewer devices. As a result, the discovery can be faster, and provide more flexibility to control the view of network devices that you want to manage.

Before you begin

Important:

All seeds must be in the scope of the subnet constrain to form a valid discovery option.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, select the domain tab corresponding to the domain for which you want to edit the limits to subnets.
3. In the **Limit to Subnets** box, select the limit that you want to edit and click **Edit**.
4. Edit the limit as needed.
5. Click **OK**.
6. To save the changes, click **Apply your changes**.

Deleting limits to subnets

After you limit the extent of the discovery by specifying subnets, you can delete your entry.

Before you begin

Important:

All seeds must be in the scope of the subnet constrain to form a valid discovery option.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click the domain tab corresponding to the domain for which you want to delete a limit to subnets.
3. From the **Limit to Subnets** box, select the limit that you want to delete.
4. Click **Delete**.

   There is no delete confirmation, the limit is deleted immediately.

5. To save the changes, click **Apply your changes**.

Adding exclusions

You can limit the extent of a discovery by specifying filters that exclude the parts of your network that match the filter conditions.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click the domain tab corresponding to the domain for which you want to add an exclusion.
3. In the **Exclusion** box, click **Add**.
4. In the Enter an exclude filter definition dialog box, select a Filter type from the drop-down menu.
5. Select a **Value** from the drop-down menu.

   The values that a are valid for the exclude filter definition depend on which Filter Type you select.

   If you select IP Address/Subnet, MAC Address, or SNMP OID as a Filter Type, then specify the appropriate value. Wildcards are accepted.
6. Click **OK**.

   The exclusion is added to the list in the Exclusions box.
7. To save changes, click **Apply your changes**.

Variable definitions

Variable	Value
Filter type	Select a Device Type to exclude all devices of a certain type. Choose from the following: • IP Address—Excludes all devices with addresses within the range specified. You can specify subnet syntax or use wildcards. For example, 192.0.2.0/24 or 192.0.2.*. • IP Subnet—Excludes all devices with addresses within the range specified. You can specify subnet syntax or use wildcards. For example, 192.0.2.0/24 or 192.0.2.*. • IP Range—Excludes all devices with addresses within the range specified. • DNS Name—Excludes all devices whose domain name matches the range specified.

Table continues…

Variable	Value
	• MAC Address—Excludes all devices whose MAC addresses match the range specified using wildcards. Note: Use MAC address syntax and replace any or all octets with asterisks, for example: 00:0D:60:*:*:* • SNMP OID—Excludes all devices whose SNMP OID match the range specified using wildcards. For example, to exclude all Microsoft devices, use the exclusion string: .1.3.6.1.4.1.311.* (Note that the period at the beginning of the string is required.).
Value	Select a value for the exclude filter definition. If you select a filter type of Device Type, choose from one of the following: • Access Router—Specifies a router that sits at the periphery of a network, in contrast with a core router that is in the middle of a network. Also called an edge router. • DSLAM—Specifies the Digital Subscriber Line Access Multiplexer (enables telephone lines to make faster connections to the Internet). • DSU/CSU—Specifies the Digital (or Data) Service Unit - Channel Service Unit. • Firewall—Specifies the device that is configured to permit, deny, or proxy data through a computer network that has different levels of trust. • Hub—Specifies the device for connecting multiple twisted pair or fiber optic Ethernet devices together, making them act as a single segment. • IP Phone—Specifies a VoIP phone. • PLC—Specifies a Programmable Logic Controller. • Printer—Specifies a printer. • Printer Server—Specifies a device to which one or more printers are connected, which can accept print jobs from external client computers connected to the print server over a network. • SAN Bridge—Specifies the Storage Area Network bridge. • SAN Switch—Specifies the Storage Area Network switch.

Table continues…

Variable	Value
	• Server—Specifies the network-connected computer hardware that provides specific services to the network. • Layer 2 Switch—Specifies the networking device that performs pure switching. • Layer 2 Wireless Switch—Specifies the networking device that performs wireless switching. • Terminal Server—Specifies the computer that aggregates multiple communication channels into one. • Unmanageable—Specifies any device that can be pinged but does not respond to any known management protocol. • WAP—Specifies a Wireless Access Point. • Power Supplies—Specifies power supplies. • Uninterruptible Power Supplies—Specifies devices and equipment that provide emergency power when the input power source fails. Monitoring supports the APC UPS devices. • VM Hosts—Specifies a physical server that hosts the virtual machines. If you select a filter type of IP Address, you enter the value field as an IP address, If you select a filter type of IP Subnet, you enter the value field as an IP subnet If you select a filter type of IP Range, you enter the value of an IP range in IPv4 or IPv6. If you select a filter type of DNS Name, you enter the value as a DNS name. If you select a Filter type of MAC Address, you enter the value as a MAC address. If you select a Filter Type of SNMP OID, you enter an SNMP OID starting with .1.3.6.1.4.1

Editing exclusions

Edit an exclusion to modify the discovery of your network.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click the domain tab corresponding to the domain for which you want to edit an exclusion.
3. In the **Exclusions** box, click the **Edit** button.
4. From the **Filter Type** list, select a filter.
5. From the **Value** list, select a value.
6. Click **OK**.

   The exclusion is updated.
7. To save the changes, click **Apply your changes**.

Variable definitions

Variable	Value
Filter type	Select a Device Type to exclude all devices of a certain type. Choose from the following: • IP Address—Excludes all devices with addresses within the range specified. You can specify subnet syntax or use wildcards. For example, 192.0.2.0/24 or 192.0.2.*. • IP Subnet—Excludes all devices with addresses within the range specified. You can specify subnet syntax or use wildcards. For example, 192.0.2.0/24 or 192.0.2.*. • IP Range—Excludes all devices with addresses within the range specified. • DNS Name—Excludes all devices whose domain name matches the range specified. • MAC Address—Excludes all devices whose MAC addresses match the range specified using wildcards. Note: Use MAC address syntax and replace any or all octets with asterisks, for example: 00:0D:60:*:*:* • SNMP OID—Excludes all devices whose SNMP OID match the range specified using wildcards. For example, to exclude all Microsoft devices, use the exclusion string: .1.3.6.1.4.1.311.* (Note that the period at the beginning of the string is required.).
Value	Select a value for the exclude filter definition.

Table continues…

Variable	Value
	If you select a filter type of Device Type, choose from one of the following: • Access Router—Specifies a router that sits at the periphery of a network, in contrast with a core router that is in the middle of a network. Also called an edge router. • DSLAM—Specifies the Digital Subscriber Line Access Multiplexer (enables telephone lines to make faster connections to the Internet). • DSU/CSU—Specifies the Digital (or Data) Service Unit - Channel Service Unit. • Firewall—Specifies the device that is configured to permit, deny, or proxy data through a computer network that has different levels of trust. • Hub—Specifies the device for connecting multiple twisted pair or fiber optic Ethernet devices together, making them act as a single segment. • IP Phone—Specifies a VoIP phone. • PLC—Specifies a Programmable Logic Controller. • Printer—Specifies a printer. • Printer Server—Specifies a device to which one or more printers are connected, which can accept print jobs from external client computers connected to the print server over a network. • SAN Bridge—Specifies the Storage Area Network bridge. • SAN Switch—Specifies the Storage Area Network switch. • Server—Specifies the network-connected computer hardware that provides specific services to the network. • Layer 2 Switch—Specifies the networking device that performs pure switching. • Layer 2 Wireless Switch—Specifies the networking device that performs wireless switching. • Terminal Server—Specifies the computer that aggregates multiple communication channels into one.

Table continues…

Variable	Value
	• Unmanageable—Specifies any device that can be pinged but does not respond to any known management protocol. • WAP—Specifies a Wireless Access Point. • Power Supplies—Specifies power supplies. • Uninterruptible Power Supplies—Specifies devices and equipment that provide emergency power when the input power source fails. Monitoring supports the APC UPS devices. • VM Hosts—Specifies a physical server that hosts the virtual machines. If you select a filter type of IP Address, you enter the value field as an IP address, If you select a filter type of IP Subnet, you enter the value field as an IP subnet If you select a filter type of IP Range, you enter the value of an IP range in IPv4 or IPv6. If you select a filter type of DNS Name, you enter the value as a DNS name. If you select a Filter type of MAC Address, you enter the value as a MAC address. If you select a Filter Type of SNMP OID, you enter an SNMP OID starting with .1.3.6.1.4.1

Deleting exclusions

Use the following procedure to delete an exclusion that you do not require.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click the domain tab corresponding to the domain for which you want to delete an exclusion.
3. From the **Exclusion** box, select the exclusion to be deleted from the list of exclusions.
4. Click **Delete**, located at the top of the Exclusions box.

   There is no delete confirmation, the exclusion is deleted immediately.
5. To save the changes, click **Apply your changes**.

Setting the network discovery options

Set the discovery options to control the extent of your discovery.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click the domain tab corresponding to the domain for which you want to select an option.
3. From the **Options** box, select the discovery option(s).

   Note:

   You can click **Discard changes, reverting to the previous values** to restore the values to the default settings.
4. Click **OK**.
5. To save the changes, click **Apply your changes**.

Variable definitions

Variable	Value
Wide Area Crawl	Monitoring discovers devices on the far side of every router interface, regardless of the interface type. Supported WAN interfaces: PossibleWideAreaInterface, ATMInterface, MultiProtocolEncapOverAAL5Interface, ATMSubinterface, WideAreaInterface, BasicISDNInterface, DS0Interface, FrameRelayInterface, HDLCInterface, IPTunnelInterface, ISDNInterface, MPLSInterface, PacketOverSonetInterface, PPPInterface, PPPMultilinkBundelInterface, ProprietaryPPPInterface, SonetInterface, T1DS1Interface, T3DS3Interface. If the WAN Crawl option is not selected then Monitoring Discovery does not go beyond any interface that is considered to be WAN interface.
VPN Crawl	Usually not needed to discover VPN client campuses. This option causes Monitoring to augment discovery with information from vendor-specific VPN tables. Initiates Monitoring to detect for remote sites through VPN connections.
DNS Lookup	Monitoring performs DNS lookup on all devices.

Table continues…

Variable	Value
Service By PortScan	Determines services running on a server by scanning for well known ports.
For All Devices	The port scan is run on all devices, not just for devices classified as servers.
Multi-vendor Discovery	Discovers devices that are not on the approved vendor list. The Multi-vendor Discovery option is disabled by default.
Host Storage Discovery	Discovers the disks, nodes, files systems, and disk capacity of Windows and Linux servers. For Linux servers, SSH must be enabled and added to the credentials Editor. For Windows, SNMP must be enabled on the server.

Performing a campus rediscovery

Perform a rediscovery of a chosen domain when you wish to have an updated snapshot. There are four different options available to perform a rediscovery.

Important:

The default discovery policy only discovers approved vendor devices. You must edit this default for full multi-vendor device discovery.

Procedure

1. Select **Network** > **Discovery**.
2. Select a campus under the Campuses section.
3. On the Network Discovery page, click **Rediscover selected campus** icon from the toolbar.
4. From the Confirm dialog box, select the appropriate merge policy that applies to your needs. The following options are available:
   - **Retain missing equipment if possible**—Retains information about equipment found in a past discovery that is not found upon rediscovery. The system retains this information over three rediscoveries. If the equipment is missing three times the equipment is automatically removed.
   - **Rediscover from scratch retaining states** —Retains information about equipment found in past discoveries and also finds all equipment from scratch.
   - **Rediscover from scratch**—Does not retain information about equipment found in past discoveries and instead finds all equipment from scratch.
   - **Retain equipment unless marked to remove** —Retains information about equipment found in a past discovery unless marked to remove.

5. Click **OK** to start the rediscovery.

Creating a campus

Use the following procedure to create a campus.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page in the Campuses section, click **Create Campus**.
3. Enter a campus discovery seed and click **OK**.

Renaming a campus

You can customize the name of the campus for the domain.

Before you begin

- Add a discovery domain.
- Configure domain network discovery options including Seeds, Limit to Subnets, Exclusions, and Options.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, select the campus you would like to rename, and then click **Rename Campus**.
3. Enter a new name for the campus.
4. Click **OK**.

Saving custom views

There are three ways you can save a custom view:

- From a default schematic
- From scratch
- From an existing custom view

After you create a custom view, you can edit the view, import a background image, and enable or disable links. Because the layout button is unavailable to change the layout, you must manually move the objects.

You can access custom views by going to **Network** > **Topology**, and selecting Custom Views from the drop-down menu on the top left.

Saving a custom view from a default schematic

About this task

Perform the following procedure to save a custom view from the existing default schematic. Use an existing schematic from the Layer 2 Hierarchy or Layer 3 Hierarchy perspectives.

Procedure

1. Select **Network** > **Topology**.
2. On the Network Typology page, use the drop-down menu on the left, to select one of the following perspectives, Layer 2 Hierarchy, Layer 3 Hierarchy, or Scopes.

   The default schematic appears in the center pane.
3. Click **enter edit mode** above the middle content pane.
4. Make changes to the schematic.
5. Click **save changes**.

   The Save schematic dialog box appears.
6. Enter a name for the schematic.
7. Select the public folder or private folder.
8. Click **OK**.

   The custom view is saved, and is located in the folder you selected in the Custom Views perspective. To access Custom Views, go to **Network** > **Topology**, and select **Custom Views** from the drop-down menu on the top left.

Saving a custom view from scratch

About this task

Perform the following procedure to save a custom view from scratch from the Custom Views perspective.

Procedure

1. Select **Network** > **Topology**.
2. From the tree browser, select the **Custom Views** perspective from the drop-down menu on the left.
3. From the Custom Views perspective, select the public folder or the private folder.
4. Click **Add**.

   The Add new custom view dialog box appears.
5. Enter a name for the schematic.
6. Click **From Scratch**.

   The Domain Element Chooser screen appears.

7. Select a perspective.
8. From the perspective navigation tree, select devices, and click the right-pointing arrow to view the devices in the Elements to Display in New Layout pane.
9. To select links automatically, check the **Auto-link new elements** check box.

   To select links manually, uncheck the **Auto-link new elements** check box.
10. Click **OK**.

    The system creates a custom schematic with links drawn in.

    Note:

    If links do not appear in the schematic, there is no path to the device.
11. Click **save changes**.

    The Save schematic dialog box appears.
12. Enter the name for the schematic.
13. Select a folder: public or private.
14. Click **OK**.

Saving a custom view from an existing schematic

About this task

Perform the following procedure to create a custom view from an existing schematic in the Custom Views perspective.

Procedure

1. Select **Network** > **Topology**.
2. From the tree browser, select the **Custom Views** perspective in the drop-down menu on the left.
3. Select a custom view from the public folder or the private folder.
4. Click **Add**.

   The Add new custom view dialog box appears.
5. Enter a name for the schematic.
6. Click **From Existing**.

   If the schematic view contains non-device icons, a Confirm dialog box appears to warn you that the current view may contain non-device icons that are not supported in custom views. If you proceed, the system removes the non-device icons from the custom view.

   To proceed, click **OK**.
7. Click **enter edit mode** to make changes to the topology.
8. Click **save changes**.

The Save schematic dialog box appears.

9. Enter the name for the schematic.
10. Select a folder: public or private.
11. Click **OK**.

Chapter 5: Manual Discovery Information

Manual device discovery

You can use manual discovery when you want to add one or more devices to the discovery, without performing a complete rediscovery.

You can add a single device or the set of devices (within a subnet) to an existing domain with the Network Discovery. You can add devices by address or subnet range to an existing discovery without doing a complete rediscovery.

Go to **Network** > **Discovery**. The **Manual Discovery** bar button is under the main toolbar on the top left. The system enables the **Manual Discovery** bar button when a completed discovery is currently selected, and no other discovery is currently ongoing for the domain. If a manual discovery is ongoing for the selected domain the manual device discovery button is disabled.

You cannot use manual discovery to add a campus to an existing discovery, or to add a device located in an undiscovered LAN. The manual discovery does not update the element type counters in the summary table of the main discovery page. This device(s) to add was not in the completed discovery because of the following reasons:

- Devices added to network after most recent discovery.
- Devices previously not configured to allow their auto discovery by Monitoring.
- Network previously not configured to allow auto discovery of new device(s) by Monitoring.
- Problematic device(s) or network access cause for simple retry.

The following are the requirements for successful discovery of a device:

- Device must have an existing pre-discovered domain containing a pre-discovered LAN (routed subnet) to which the new device can be added.
- Subnets must not be larger than 256 addresses.

Manual device discovery

Adding a device to an existing discovery

Add a device to an existing discovered domain.

Before you begin

- You must configure the device to respond to SNMP queries from Monitoring.
- Monitoring must have an existing pre-discovered domain containing a pre-discovered LAN, or routed subnet, to which you can add the new device.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click **Manual Discovery**.
3. In the **New Requests** panel, click the **Add** button.
4. Enter the IP address of the device that you want to discover.
5. Click **OK**.
6. Click **Discover** to begin the discovery of the device.

Editing a manual device discovery

Perform the following procedure to edit a manual discovery.

Before you begin

- You must configure the device to respond to SNMP queries from Monitoring.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click **Manual Discovery**.
3. In the Previous Requests panel, select the device to be modified.
4. Select Discover again to move the discovery into the New Requests section.
5. In the New Requests section select the device IP, and click **Edit**.
6. Modify the value as required.
7. Click **OK** to save the changes.
8. Click **Discovery** to run the manual discovery with a new value.

Starting the manual device discovery again

Perform the following procedure to start the manual discovery again.

Before you begin

- You must configure the device to respond to SNMP queries from Monitoring.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click **Manual Discovery**.
3. In the **New Requests** panel, click **Add**.
4. Enter the IP address of the device that you want to discover.
5. Click **OK**.
6. Click **Discover** to begin the discovery of the device.
7. After the manual discovery completes, click on any device.
8. In the **Previous Requests** panel, click the **Discover again** button to add the entry to the New Requests panel.
9. Click **Discover** to run the manual discovery again.

Deleting a manual device discovery

Perform the following procedure to delete a device from the manual discovery panel.

Before you begin

- You must configure the device to respond to SNMP queries from Monitoring.

Procedure

1. Select **Network** > **Discovery**.
2. On the Network Discovery page, click **Manual Discovery**.
3. In the **New Requests** panel, select the device to be deleted.
4. Click **Delete**, located at the top of the **New Requests** panel.

   There is no delete confirmation, the device is deleted immediately.

Cancelling a manual device discovery

Perform the following procedure to cancel a manual device discovery when the discovery is in progress.

Procedure

1. Select **Network** > **Discovery**.
2. If you want to cancel a manual discovery after selecting to do a discovery, click the **Discovery in Progress - Click to cancel** icon from the top menu.

Chapter 6: Discovery Results Information

Topology Viewer discovery results

The Topology Viewer allows you to view the discovery results in graphical format in the middle of the Network Topology page. After the system completes a discovery, the Topology Viewer shows discovered campuses and WAN Links between them.

You can select from different views at the top left of the tree browser, including:

- Layer 2 Hierarchy
- VLAN hierarchy
- SPBM View
- Layer 3 Hierarchy
- Custom Views
- Device Type
- Applications
- Virtualization
- Scopes

You can also learn more by double-clicking in different areas of the topology. The double-click function on an icon in the Topology Viewer or the Tree Browser has a default behavior that depends on the context of the icon. Double-click on an icon or item on the tree browser provides more details about what is inside the domain element. If the icon is an aggregation of other domain elements, then double-clicking the icon displays more details about the domain element.

- Double-click on any campus icon to view its details.
- Double-click on a device within the campus details to show the Layer 2 view for that device.
- Double-click on an interface or an element that does not have further detailed views to display the properties associated with that element in a pop-up window.
- Double-click on a thick line, which is an aggregation of links, to expand the links. If the icon is already expanded to member links, if you double-click the icon collapses.

Note:

If the number of elements in a domain is more than 1000, the schematic cannot be zoomed in or out. Split such large domains into multiple domains to manage and view the discovery results.

Viewing discovery results

This section provides procedures for viewing the results of a network discovery.

Viewing discovery results in the Tree Browser

Use the following procedure to view the results of a network discovery in the Tree Browser.

Procedure

1. Select **Network** > **Topology**.
2. On the Network Topology page, view the network elements in the Tree Browser located on the left side of the page.
3. To view specific device types only, select a filter from the Perspectives drop-down menu.
4. Click the + and - icons to expand and contract the tree folders.
5. Left-click twice on a node to display the node on the central panel, in its network context. Scopes and SPBMs are displayed in tabular form.
6. Click the **Refresh** icon to update the information displayed in the Details panel.
7. Right-click on a device, and select the type of information you want to view.

Variable definitions

The following table describes the options on the drop-down menu in the **Network** > **Topology** toolbar.

Perspective	Description
Layer 2 Hierarchy	Lists domain elements according to their OSI layer 2 functions.
VLAN Hierarchy	Lists the logical nodes that constitute a virtual LAN in each campus.
SPBM View	Lists the supported applications in the SPBM area, including Backbone Core Bridges, Backbone Edge Bridges, Backbone VLANs, Custom VLANs, and VRFs.

Table continues…

Perspective	Description
Layer 3 Hierarchy	Lists domain elements according to their OSI layer 3 organization, which is by their IP addresses.
Custom Views	Lists user-defined public and private views of the network topology.
Device Types	List items as being campuses, devices (managed or unmanaged), or interfaces (including AAL5, ATM, Ethernet, PPP, and a number of others).
Applications	Lists the supported applications that are visible to the Monitoring Server. Applications are listed under the following categories: Operating System, VoIP, and Voice.
Virtualization	Lists all managed VM hosts discovered in the domain.
Scopes	Lists all scopes defined for the domain enabling you to list domain elements according to a scope to which they belong.

Viewing discovery results in the Topology Viewer

The Topology Viewer allows you to view the discovery results in graphical format in the middle of the Network Topology page. After the system completes a discovery, the Topology Viewer shows discovered campuses and WAN Links between them.

Note:

If the number of elements in a domain is more than 1000, the schematic cannot be zoomed in or out. Split such large domains into multiple domains to manage and view the discovery results.

The following navigation controls are available from the Topology Viewer:

- Enter edit mode—freezes the movement of icons.
- Save—Saves unsaved icon moves.
- Discard changes—Discards changes to a layout and reverts to the previous layout.

Procedure

1. Select **Network** > **Topology**.
2. On the Network Topology page, view the network elements in the Topology Viewer located in the middle of the page. Use the arrows to move the view of the topology to the left or right.
3. To view specific device types only, select a filter from the Perspectives drop-down menu.
4. Select a device for which you want to view detailed information.

5. Right-click on the selected device and select an option from the drop-down menu.
6. Double-click on any campus icon to view its details.
7. Double-click on a device within the campus details to show the Layer 2 view for that device.
8. Double-click on an interface or an element that does not have further detailed views to display the properties associated with that element in a pop-up window.

Variable definitions

The following table describes the menu options for a device, or campus in the non-edit mode. The following table displays the options available when you are in **Network** > **Topology**, and you right-click on a router, switch, SPBM area, or other option in the tree browser on the left.

Menu option	Device Group	Description
Tables	Campus	Provides the following details about the campus in a table format: • Devices—Displays a table with information about the devices that are connected to a campus. • Network Devices—Displays a table with information about the network devices connected to a campus. • MLT Details Table—Displays a table with information about the MLT details associated to devices connected to a campus. • campusVoIPDevices—Displays a table with information about VoIP devices associated with a campus.
	Device	Provides the following details about the device in a table format: • Interfaces—Displays a table with information about the interfaces associated with the selected device • Interface Groups—Displays a table with information about the interface groups associated with the selected device. • Physical Elements—Displays a table with information about the physical elements associated with the selected device. • Show Bonded Channels—Displays a table with information about the bonded channels associated with the selected device. • Connected Devices (All)—Displays a table with information about all connected devices associated with the selected device. • Connected Devices (Network)—Displays a table with information about network connected devices associated with the selected device.

Table continues…

Menu option	Device Group	Description
		• Connected Devices (MLT)—Displays a table with information about MLT connected devices associated with the selected device. • Connected Devices (VoIP)—Displays a table with information about VoIP connected devices associated with the selected device. • MLT Details Table—Displays a table with MLT details for the selected device. • Stack Units—Displays a table with the devices connected to the stacked unit. **Note:** After you select a table, you can select another table for the same device from the drop-down list available at the top of the central browser.
	ESXi	Provides the following details about the ESXi device in a table format: • Interfaces—Displays a table with information about the interfaces associated with the selected device **Note:** When viewing scope members for ESXi devices, it is normal for negative values to appear in the Index column. • Processors—Displays a table with information about the processors associated with the selected device. • Physical Elements—Displays a table with information about the physical elements associated with the selected device. • Show File Systems—Displays a table with information about the file systems associated with the selected device. • Show Applications—Displays a table with information about the applications associated with the selected device. • Show Services—Displays a table with information about the services associated with the selected device.
Schematics	Campus	Provides the following schematic information about the campus: • Details • Subnet Details • Physical Datacenter

Table continues…

Menu option	Device Group	Description
	Device	Provides the following schematic information about the device: • Layer 2 Details—Displays the domain element details according to their OSI layer 2 functions. • MLT Schematic—Displays the MLT schematic for the selected device. • Network Neighbors—Provides access to the backbone neighborhood schematic view for a selected domain element. This view, intended for improved viewing of domain elements in very large domains, expands the view to show domain elements that are connected by one hop to the selected domain element. • Show Campus—Shifts view to the campus for the selected device. • Show Paths...—Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.
	ESXi	Provides the following schematic information about the ESXi device: • Layer 2 Details—Displays the domain element details according to their OSI layer 2 functions. • Show Paths...—Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.
	G450	Provides the following schematic information about the G450 device: • Layer 2 Details—Displays the domain element details according to their OSI layer 2 functions. • Network Neighbors—Provides access to the backbone neighborhood schematic view for a selected domain element. This view, intended for improved viewing of domain elements in very large domains, expands the view to show domain elements that are connected by one hop to the selected domain element. • Show Campus—Shifts view to the campus for the selected device. • Show Paths—Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-

Table continues…

Menu option	Device Group	Description
		points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.
Configure	Campus Device ESXi G450	Enables you to perform the following configuration actions: • Mark for Removal—Marks the device for removal from the next discovery. • Supervision Settings—Enables you to define the supervision settings for the selected device. The values include the following: inherit, supervise, unsupervise. • Overrides...—Displays a table with configuration, scope, override, and value of the selected device or campus. You can add, delete or edit an override.
Monitoring	Device	Enables you to perform the following configuration actions: • Add custom monitoring
Diagnose	Device ESXi G450	Enables you to perform the following diagnostic actions for the device: • MIB Query • MIB Browse • ICMP Ping • Trace Route • SNMP Get • Remote Ping • Remote Traceroute
SPBM Diagnose Tools	Device	Provides the following SPBM diagnostic tools: • L2 Ping • L2 Traceroute • Unicast Path • Multicast Path
Tools	Campus	Provides a launch point for commonly used device element management tools. The following tool is available for the campus: • Rediscover Campus
	Device	The following tools are available for the device: • EM-Launch • HTTP-connection • Rediscover Device

Table continues…

Menu option	Device Group	Description
		Note: Rediscover Device detects changes for the selected device only. You must use a campus or domain rediscovery to detect connected devices and topology changes.
	ESXi	The following tools are available for the ESXi device: • HTTP Connect • Rediscover Device • VMware vCenter
	G450	The following tools are available for the G450 device: • EM Launch • Launch Secure EM • Rediscover Device
Trends	Campus Device ESXi G450	Trends are performance graphs for devices or interfaces. The trends menu lists a collection of MITs that are configured and can be trended. For example, device CPU usage is a configured Monitored Information Type (MIT) that you can trend.
Show Events	Campus Device ESXi G450	Opens a tab in the in the bottom pane of the events browser, that displays all events for the selected element. The tab remains open until you manually delete the tab.
Show Dashboard	Campus Device ESXi G450	Opens the dashboard view with details of the selected campus, or device.
Properties	Campus Device ESXi G450	Displays the Properties window for the selected device which shows the device properties and associated values.
Color-Coding of Domain Elements	Campus Device	Domain elements displayed in the schematic diagram are colored based on the messages that relate to them.

The following table describes the menu options for a device, or campus in the edit mode.

Menu option	Description
Hide	Hides the device or campus from view.

Table continues…

Menu option	Description
Show all	Displays all end nodes such as phones, printers, and servers that are connected to the selected devices.
Show VoIP Devices	Displays all VoIP components such as phones, VoIP servers, and media gateways. Properties.
Properties	Displays the Properties window for the selected device which shows the device properties and associated values.

Moving icons in the topology view

The topology browser permits you to move icons, save the new layout, and share the layout for other users to see. Before you can move an icon in the Network Topology work pane, you must click **enter edit mode**. To create a custom view, you can enter the edit mode to save a layout view, or you can delete a layout view. After you save a view, you can save the view in the public or private Custom Views folder.

Viewing discovery results in the Properties Table

Use the following procedure to view discovery results using the Properties Table.

Procedure

1. Select **Network** > **Topology**.
2. On the Network Topology page, select a network element.
3. Right-click on a device.
4. Click **Properties**.

   The Properties Table displays details for the selected network element.

Selecting a layout

Perform the following procedure to select the layout algorithm in the Topology Viewer tool bar.

Procedure

1. Select **Network** > **Topology**.
2. On the Network Topology page, view the network elements in the Topology Viewer, located in the middle of the page.
3. Select any one of the layout algorithms from the Layout box to draw the schematic from the middle toolbar.

The predefined global layout options are: Hierarchical, Symmetric, Circular, Horizontal Grid, and Compact. You can create custom view layouts.

Variable definitions

Variable	Value
Hierarchical	Enables the user to view the schematic or perspective hierarchically when selected.
Symmetric	Enables the user to view the schematic or perspective symmetrically when selected.
Circular	Enables the user to view the schematic or perspective circularly when selected.
Horizontal Grid	Enables the user to view the schematic or perspective in a horizontal line.
Compact	Enables the user to view the schematic or perspective in a compact format.

Moving an icon

Procedure

1. Select **Network** > **Topology**.
2. Select a layout that you can edit.
3. Click **enter edit mode**.
4. Select the icon you want to move.
5. Point over the icon, and then click and hold down the right mouse button.
6. Move the icon.

   The animation of the icon and attached links move.
7. Release the icon on the spot where you want the icon to be moved to.
8. To save the layout, click **save changes**.
9. In the **Enter a name for schematic** field, enter a layout name.
10. Select the private folder or public folder to save the layout in.
11. Click **OK**.

    The layout is saved in the Custom Views perspectives under the public or private folder.

Clearing the background setting

Use the following procedure to clear the background setting.

Procedure

1. Select **Network** > **Topology**.
2. Open a view that has the background setting.
3. Click **enter edit mode**.
4. Click the **Set background** button in the middle toolbar.
5. Click **save changes**.
6. In the Enter a name for schematic field, enter a layout name.
7. Select a folder to save the layout in, private or public.
8. Click **OK**.

Chapter 7: Scope information

Scopes

A scope (device classification) defines a set of discovery domain elements or events based on several criteria. Use scopes in defining monitoring configurations, defining subscriptions, filtering message boards, initiating responses to events, filtering event monitoring, actions, and defining the processes for launching external applications. A scope specifies the elements in a monitoring operation. You must have an Advanced License to use scopes. Go to **Network** > **Scopes**.

Important:

Built-in scopes delivered with the product are read only and cannot be edited or deleted. If you are a UCM or network administrator, you can define your own scopes by using the add or clone control in the Scopes page.

The following general controls are available on the Scopes page:

- Apply your changes—All edits to scopes are client-side only. Clicking the Apply button saves the edits to the server.
- Discard changes, reverting to the previous values—Unapplied edits to a scope can be undone by clicking the Revert button.
- Add—You create a new domain element scope.
  - Select Constraint Based Scope to create a scope defined by a set of domain elements that meet specified criteria.
  - Select Union-Based Scope to create a scope defined by a union of at least two existing scopes.
  - Select Enumerated Member Scope to create a scope defined by an explicit list of individual domain elements.
- Delete selected scope—Remove a scope. You cannot delete built-in scopes. A prompt appears to confirm deletion of the scope.
- Rename selected scope—Change the name of a selected scope.
- Clone selected scope—Create a duplicate of an existing scope to facilitate the creation of a new, similar scope.
- Enable/Disable Alphabetical mode—Toggle the way in which the system lists scopes. The Alphabetical view shows a flat list of scopes sorted alphabetically by name.

- Disable/Enable text view mode—Toggle the way a scope definition displays. Design View displays the scope definition using drop-down menus and links to construct valid scope constraints. Text View displays the scope definition text directly.
- Show/Hide private scopes—Choose if you want to view or hide private scopes. When you create a scope you can select the Keep Private check box and the scope does not appear in the list until you click the Show private scopes button.
- Refresh—Refreshes the scope list.

You can configure scopes for domain elements and events. The Scope Configuration page has two tabs: Elements tab and Events tab. Each tab has two panels that show the following basic groups of information and options:

- The Scopes Management List provides a list of the scopes defined for your system. The tabs allow you to select the type of scopes to appear in the management list (Element scopes or event scopes).
- The Scope Definition and Comments Form provides a set of options and fields that enable you to create and edit scopes.

Types of scopes

There are three types of scopes:

- Constraint-based scopes are defined by a set of elements that meet specified criteria. Both domain element scopes and event scopes may be of the constraint-based scope type.
- Union-based scopes are the union of at least two existing scopes. Both domain element scopes and event scopes may be of the union-based scope type.
- Enumerated member scopes are defined by an explicit list of individual elements. Only domain element scopes can be of the enumerated member scope type. An enumerated member scope is used when you want to define a set of related objects where the relationship is not obvious from the metrics available from the operating system.

To configure scopes, go to **Network** > **Scopes**, and select **Add a new scope**, which is the plus sign on the toolbar at the top left.

You should create a constraint-based scope if you have a set of constraints for which you want to define a scope. Create enumerated scopes when you want to define a scope by selecting some discovered elements that might not share any common attributes apart from the domain. Create a union-based scope when you want a new scope based on a combination of two or more existing scopes.

Example

For example, you want to create a scope for all devices in floor one of your building. If the device name ends with the floor number, then for this example, you can define a constraint based scope; that is, all elements are in scope **“Devices”**, the subject is a Device, and subject.subjectName ends with Floor1.

Scope configuration

You use scopes to define monitoring configurations, define subscriptions, filter message boards, initiate responses to events, filter event monitoring, and define the processes for launching external applications. A scope might specify which elements are included in a monitoring operation. Alternatively a scope can specify the set of elements for which a particular response is used.

Adding constraint based scopes

Create a constraint based scope to have a scope defined by a set of elements that meet a specified criteria.

Procedure

1. Select **Network** > **Scopes**.
2. From the Monitoring Scopes page, click the **Elements** tab to select the Elements domain.

   Or

   Click the **Events** tab.
3. Click **Add a new scope**.
4. Select **Constraint Based Scope**.
5. Enter the name of the scope.

   The name must be unique and may include numbers, letters with spaces, underscores (_) or hyphens (-) but not special characters.
6. Click **OK**.

   The scope definition and the comments appear in the right panel of the Scope window.
7. Edit the default Scope and subject values. Different options are available depending on how you create the scope. See the variable definitions table below for available options.
8. Select the **Keep private** option to create the scope as a private scope. A private scope does not show in the list of public scopes and is not seen in the network browser scope perspective.
9. In the **Comments** box, type a comment to describe the scope.
10. To save changes, click **Apply your changes**, which is the check mark in the top left toolbar.

Variable definitions

The following table describes the options in the Scope content panel window.

Variable	Value
AND Link	Displays a menu of options. Select AND <new> to include a new element in the constraint definition. Select Copy to copy an existing element in the constraint definition. Select And <paste> to paste a copied element in the constraint definition. Select Simplify to remove all hierarchical nesting conventions from the selected block of constraints. The Scope Constraint dialog box displays to guide you through the process of creating each constraint. Constraints you define are added to the scope definition and comments field displayed in the right panel of the Configuration Browser window. The set of properties and relations available to you when writing a constraint depends upon what subjects are defined by earlier constraints. For example, the address property applies (and is available) when the subject is a device but does not apply (and is therefore not available) when the subject is an interface.
Keep Private	Indicates whether or not the scope is to be hidden. A private scope does not show in the list of public scopes and is not seen in the network browser scope perspective.
Comments	Specify a description of the scope. Comment text is not part of the scope definition. (Optional)
Additionally, you can click on a line that is a Boolean operator or constraint within the scope definition. A drop-down menu displays with the some or all of following options enabled:	
Cut	Cut the selected constraint from the scope definition.
Edit	Edit the selected constraint.
Copy	Copy the selected constraint.
Remove	Delete the selected constraint definition from the scope definition.
Not	Changes the BOOLEAN logic for selected constraint to be FALSE (not equal to the constraint string specified).
AND <new>	Create a new constraint that is to be ANDed to the selected constraint. The new constraint is placed at the level of the selected constraint so you can nest constraints in the scope definition.
AND <next>	ANDs the selected constraint with the constraint that follows it.
AND <paste>	Paste a copied constraint as an AND statement related to the selected constraint.
OR <new>	Create a new constraint that is to be ORed to the selected constraint. The new constraint is placed at the level of the selected constraint so you can nest constraints in the scope definition.
OR <next>	ORs the selected constraint with the constraint that follows it.
OR <paste>	Paste a copied constraint as an OR statement related to the selected constraint.

Table continues…

Variable	Value
Raise	Move the selected constraint up one level in its current block.
Lower	Move the selected constraint down one level in its current block.
Promote	Promote to the next highest block level in the scope definition.

Adding union based scopes

Define a union based scope to create a union of at least two existing scopes.

Procedure

1. Select **Network** > **Scopes**.
2. From the Monitoring Scopes page, click the **Elements** tab to select the Elements domain.

   Or

   Click the **Events** tab.
3. Click **Add a new scope**.
4. Select **Union Based Scope**.
5. Enter the name of the new scope. The name must be unique and may include numbers, letters with spaces, underscores (_) or hyphens (-) but not special characters.
6. Click **OK**.

   The Creating New Scope section and the comments appear in the right panel of the Scope window.
7. Select the individual scopes that you want to include in the Union Scope from the tree structure.
8. Select the **Keep private** option to create the scope as a private scope. A private scope does not show in the list of public scopes and is not seen in the network browser scope perspective.
9. In the **Comments** box, type a comment to describe the scope.
10. To save the change, click **Apply your changes**.

Variable definitions

Variable	Value
Scopes tree	Displays a hierarchical list of existing scopes with a check box for each scope that enables you to select at least two scopes on which to base the union scope.
Keep Private	Indicates whether or not the scope is to be hidden. A private scope does not show in the list of public scopes and is not seen in the network browser scope perspective.

Table continues…

Variable	Value
Comments	Specify a description of the scope. Comment text is not part of the scope definition. This is an optional parameter.

Adding enumerated member scopes

Create an Enumerated Member Scope to specify the individual elements that the scope comprises.

Procedure

1. Select **Network** > **Scopes**.
2. From the Monitoring Scopes page, click the **Elements** tab to select the Elements domain.

   Or

   Click the **Events** tab.
3. Click **Add a new scope**.
4. Select **Enumerated Member Scope**.
5. Enter the name of the new scope.

   The name must be unique and may include numbers, letters with spaces, underscores (_) or hyphens (-) but not special characters.
6. Click **OK**.
7. From the Domain menu, choose the domain for which you want the scope to apply.
8. On the right panel, in the Creating New Scope section, click **Add** to specify domain elements to include in the scope.

   The scopes dialog box appears.
9. Select a perspective to view domain elements organized in a way that is useful to you.
10. Select the individual domain elements that you want to include in the scope.
11. Click **OK**.
12. Select the **Keep private** option to create the scope as a private scope. A private scope does not show in the list of public scopes and is not seen in the network browser scope perspective.
13. In the **Comments** box, type a comment to describe the scope.
14. To save the scope definition, click **Apply your changes** in the top left toolbar.

Variable definitions

Variable	Value
Scope Members	Specifies the domain elements to include in the scope.
Keep Private	Indicates whether or not the scope is to be hidden. A private scope does not show in the list of public scopes and is not seen in the network browser scope perspective.
Comments	Specifies a description of the scope. Comment text is not part of the scope definition. This parameter is optional.

Editing scopes

You can edit a scope after you create the scope.

You can edit a custom scope, but not a built-in scope. The apply button is disabled in all built-in scopes.

Procedure

1. Select **Network** > **Scopes**.
2. From the Monitoring Scopes page, click the **Elements** tab to select the Elements domain.

   Or

   Click the **Events** tab.
3. Select the scope you want to edit.

   The settings for the selected scope display on the right panel.
4. Edit the settings as needed.
5. To save the change, click **Apply your changes**.

Renaming scopes

You can change the name of scope after you create the scope.

Procedure

1. Select **Network** > **Scopes**.
2. From the Monitoring Scopes page, click the **Elements** tab to select the Elements domain.

   Or

   Click the **Events** tab.
3. Select the scope you want to rename.
4. Click the **Rename selected scope** button from the top left toolbar.

A Prompt dialog box appears.

5. Enter the new name.
6. Click **OK**.

Cloning scopes

You can clone an existing scope.

Procedure

1. Select **Network** > **Scopes**.
2. From the Monitoring Scopes page, click the **Elements** icon to select the Elements domain.

   Or

   Click the **Events** icon.
3. Select the scope you want to clone.
4. Click **Clone selected scope** from the top left toolbar.

   A Prompt dialog box appears.
5. Enter a new name for the cloned scope.
6. Click **OK**.

Deleting scopes

You can delete an existing scope.

Procedure

1. Select **Network** > **Scopes**.
2. From the Monitoring Scopes page, click the **Elements** tab to select the Elements domain.

   Or

   Click the **Events** tab.
3. Select the scope you want to delete.
4. Click **Delete selected scope** in the top left toolbar.

   A Confirmation dialog box appears.
5. Click **OK** to confirm the deletion.

Chapter 8: Monitoring information

Monitoring conceptual information

Use the following information to understand the monitoring information in the system under **Network** > **Monitoring Details**, and **Network** > **Topology**.

Monitoring Details

You can use the Network Monitoring Details page to start and stop availability of monitoring agents and SNMP monitoring agents for your Monitoring system.

A monitoring agent is a grouping of all network elements being monitored into groups according to the protocol used and functionality supported; for example, SNMP, CIM, SOAP are ways to pull statistics from the devices. You can also group them according to the functions; for instance, the availability monitoring agent checks the availability of all devices with SNMP get and ICMP ping.

To access Network Monitoring Details, go to **Network** > **Monitoring Details**.

After you set up your monitoring configurations, you access the monitoring details to enable the monitoring configurations on specific discovered domains.

The monitoring details display information about which monitoring agents have connected with the server, where monitoring agents are running, the state of monitoring agents, the amount of data monitoring agents are handling, what domain elements are being monitored, and the latest value gathered for each piece of data being polled.

The left panel of the Network Monitoring Details page displays a tree structure of domains, agents, monitoring requests, and domain elements. The right panel displays a list of domains and their monitoring status. You can expand items within the left panel tree to locate specific items of interest. When you select a monitoring request in the list, the following information displays in the right panel of the page:

- Monitoring scope—Specifies a read-only set of domain elements at which the monitoring request is targeted explicitly.
- Information type scopes—Specifies a read-only set of domain elements encompassed by the information types specified.
- Param override scopes—Lists the parameter overrides specified in the definition of the current monitoring operation.
- Information types tab—Specifies an SNMP object for which the monitoring process queries.

- Details tab—Lists the variables (SNMP objects for which the monitoring process queries), notifications (notification actions for which the monitoring operation looks) and parameter overrides (parameter overrides specified in the definition of the current monitoring operation) associated with the monitoring request.
- Domain Elements tab—Lists the specific domain elements affected by the monitoring request. This list comprises the intersection of the monitoring scope with the event type scopes.

When you select a domain element in the list, the variables for that domain element and associated values display in the right panel of the page.

Monitoring overrides

Monitoring overrides enable you to define an exception for a monitored event type for the domain elements in a particular scope. The override definition consists of one or more event type parameter values and one or more scopes. The event type parameters can be from one or more event types.

Note:

The Monitoring Overrides menu is only available with an Advanced Monitoring license.

To access Monitoring overrides, go to **Network** > **Monitoring Overrides**.

The following controls are available at the top of the Overrides window:

- Apply your changes—Applies your changes. All edits to overrides are client-side only. Click Apply to save the edits to the server.
- Discard changes, reverting to the previous values—Discards your changes. Unapplied edits to an override can be undone by clicking the Revert button. No confirmation is offered, and unapplied edits are immediately lost.
- Add a new override—Adds a new override.
- Delete selected override—Deletes an existing override.
- Rename selected override—Allows you to rename an existing override.
- Clone selected override—Duplicates an existing override.
- Refresh—Refreshes an existing override.

Monitoring Overrides tab

The Monitoring Overrides tab provides a list of monitoring parameter overrides. Monitoring overrides take effect before an event occurs. The definition of a monitoring override includes the selection of a domain element scope and the specification of the appropriate parameter override (event types, monitoring parameters, and values) that are to be applied to specified domains.

To access the Monitoring Overrides tab, go to **Network** > **Monitoring Overrides**, and select the **Monitoring Overrides** tab.

The following controls are available on the monitoring overrides tab:

- Enabled—Indicates whether or not the monitoring override parameter is active (default is on).
- Parameter overrides—Provides a list of the existing parameter overrides and allows you to edit existing override values.
- Override applies to—Allows you to select the domain to which the override parameters are to apply. Valid values are All Domains (the override parameters are to apply to all domains) and These Domains (the override parameters are to apply only to the selected domains).

Event Processing Overrides Tab

The Event Processing Overrides tab provides a list of event processing overrides. Event processing overrides take effect after an event has occurred. Event processing overrides define whether the override applies to an event scope or an event type, the parameter override (event processing parameters and values), and the domains to which the override applies.

To access the Event Processing Overrides tab, go to **Network** > **Monitoring Overrides**, and select the **Event Processing Overrides** tab.

Important:

When you define an event processing override (either global or scoped), the override does not take effect for a domain element if events exist that are the same type posted against that domain element. Manually clear all events of a particular type after defining an override for that type.

The following controls are available on the event processing overrides tab:

- Enabled—(Default is on) Indicates whether or not the event processing override is active (enabled).
- Parameter overrides—Provides a list of the existing parameter overrides. Includes links that enable users to edit existing override values.
- Override applies to—Drop-down that enables you to select whether the override applies to an event scope or event type. Once an option is selected, you can then use the tree selection list to specify the appropriate event scope or event type.

Network Topology

The Network Topology enables you to view detailed information about the status of the managed objects in your network. Go to **Network** > **Topology**. The Network Topology provides the following tools for viewing network information:

- Toolbar (top of the screen)
- Tree browser
- Central browser
- Property table (If the table is not visible, click **Show property table**, in the toolbar.)

- Event browser pane

You can also use the Network Topology to access diagnostic tools, such as a ping utility, and to view inventory information. For more information, see Diagnostic tools on page 176.

Network Topology handling of device errors

If an error occurs on a network device nested within a multi-layer design in the Network Topology, the color coding for that error is replicated on all layers above.

General controls

The following general controls are available at the top of the **Network** > **Topology** page.

Tool	Description
Top left Topology toolbar	
Hide tree or Show tree	Hides or shows the navigation panel on the left hand side of the Network Topology page.
Hide property table or Show property table	Toggle to show or hide the Property Table panel. The Property table appears on the right hand side of the Network Topology page.
Hide events or Show events	Closes the Default Message Board and the Events by Concern : Monitoring tabs that appear at the bottom of the Network Topology page.
Auto Refresh	Controls auto-refresh on/off and interval of refresh if on.
Refresh	Refreshes the Network Topology contents.
Save Domain	Saves the domain.
Drop-down menu	
Perspective—located on the toolbar of the navigation tree	The navigation tree changes and provides a different way to navigate the central browser view for each of the following options: • Layer 2 Hierarchy: In the central browser, you can navigate on the Layer 2 view of the network. You can view the details about the applications, servers, storage and network by double-clicking an icon. The tree view lists campus, routers, switches, and border devices. • VLAN Hierarchy: The tree view lists all the VLANs configured for each campus. The right-click menu on the VLAN lists the details of the VLAN in the central browser. • SPBM view: The tree view displays SPBM components listed for an SPBM area. SPBM components include Backbone Core Bridges, Backbone Edge Bridges including backbone VLANs, Custom VLANs, and VRFs. • Layer 3 Hierarchy: Lists all the subnets in the navigation tree. Expand the items on the tree to view members; right-click to view details in the central browser.

Table continues…

Tool	Description
	• Custom Views: Creates a custom view of the topology. The available icons permit you to perform the following actions. - Create new sub-folder - Add custom view - Delete custom view • Device Types: Lists the campus, devices, and interfaces in the navigation tree. Expand the items on the tree view to view details of the devices or interfaces; right-click the leaves of the tree to view details in the central browser. • Applications: This perspective in the tree lists the voice applications and the operating systems in the network. Right-click the leaf item in the tree to view details in the central browser. • Virtualization: The Virtualization view is for browsing the VH and virtual machine infrastructure and associated resource pools. • Scopes: This perspective lists all predefined and user defined scopes. Select a leaf to view a table containing all the members in the scope. This option is very useful when a graphical view is too congested.
Middle content pane middle left toolbar	
Enter edit mode	Permits you to move icons on the topology.
save changes	Saves changes you have made to the topology.
discard changes	Discards changes you have made to the topology.
Add elements	Permits you to add a device to the topology. The Add button is enabled in the custom view.
Hide elements	Permits you to hide a device to the topology. The Add button is enabled in the custom view.
Edit	Permits you to edit the topology.
Set background	Configures a background image onto the topology.
Hide name labels or show name labels	Hides name labels or shows them depending on what you select.
Zoom—percentage value box and slider	Adjusts the level of zoom in the topology viewer so as to fit more or less of the topology in the window. Two different controls are provided—a slider and a percentage value box.
Zoom to fit	Adjusts the level of zoom in the topology viewer to fit the window visible on your screen.
Layout	The global layout policies in the central browser are: hierarchical, symmetric, circular, horizontal grid, and compact.

Tree browser

This section provides an overview of the tree browser or navigation tree, located in the left panel of the **Network** > **Topology** page.

The tree browser enables you to browse the contents of your network as a hierarchical tree with several perspectives to choose from.

The tree browser displays a tree that lists the entities within a domain. Left-clicking on '+' and '-' icons expands and contracts the tree folders. Expansion and selection of entities within the tree browser does not refresh the information displayed in the central browser, therefore the information displayed in the central browser may not reflect the node to which you navigate in the tree browser. To access the tree browser for a domain, the domain must be discovered by the server. If the domain of interest has not yet been discovered, you must discover (load) the domain. The information that displays in the tree browser depends on the perspective you select. The available perspectives are:

- Layer 2 Hierarchy—Lists domain elements according to their OSI layer 2 functions.
- VLAN Hierarchy—Lists the logical nodes that constitute a virtual LAN in each campus.
- SPBM view—Lists the supported components in the SPBm area, including Backbone Core Bridges, Backbone Edge Bridges, Backbone VLANs, Custom VLANs, and VRFs.
- Layer 3 Hierarchy—Lists domain elements according to their OSI layer 3 organization, which is by the IP addresses of the domain elements.
- Custom Views—Creates a custom view of the topology.
- Device Types—Lists items as being campuses, devices (managed or unmanaged), or interfaces (including AAL5, ATM, Ethernet, PPP, and a number of others).
- Applications—Lists the supported applications that are visible to the Monitoring Server. Applications are listed under the following categories: Operating System and Voice.
- Virtualization—The Virtualization view is for browsing the VH and virtual machine infrastructure and associated resource pools.
- Scopes—Lists all scopes defined for the domain enabling you to list domain elements according to a scope to which they belong. Left-clicking on a tree node causes the central browser panel to show the requested node in its network context and shows members of the scope in tabular form.

The tree browser also provides menu options. When you right-click a node in the tree browser, a menu displays enabling you to access information about the selected item. The options that are available for a given node vary based on its context. The possible options are:

- Tables:
  - Interfaces
  - Physical Port Modules
  - Processors
  - Physical Elements
  - Show Bonded Channels
  - Connected Devices (All)
  - Connected Devices (Network)

    - Connected Devices (MLT)
    - Connected Devices (VoIP)
    - MLT Details Table
    - Devices
    - Network devices
- Schematics:
    - Layer 2 Details
    - MLT Schematic
    - Network Neighbors
    - Show Campus
    - Show Paths
    - Details
    - Subnet Details
    - Physical Datacenter
- Configure:
    - Mark for Removal
    - Supervisor Settings
    - Overrides
- Tools:
    - Rediscover Campus
- Monitoring:
    - Add custom monitoring
- Diagnose:
    - MIB Query
    - MIB Browse
    - ICMP Ping
    - Trace Route
    - SNMP Get
    - Remote Ping
    - Remote Trace Route
- Tools:
    - Launch EM

  - Launch Secure EM
  - Rediscover Device
- Trends:
  - Other variables
  - Bridge Num VLANs
  - Bridge VLAN delete count
  - CPU busy
  - CPU busy – rolling average
  - Controlled port count
  - ICMP Response Time
  - ISIS System Authentication Key Failures
  - ISIS System Type Mismatches
  - ISIS System LSP Database Overloads
  - ISIS System LSP Errors
  - ISIS System Manual Address Drops
  - ISIS System Max Sequence Exceeds
  - ISIS System Own LSP Purges
  - ISIS System Partition Changes
  - ISIS System SPF Runs
  - ISIS System Sequence Skips
  - ISIS System
  - MST CIST new root bridge count
  - MST CIST top change count
  - MST region config change count
  - Percent IO Memory Free Low Watermark
  - Percent Processor Memory Free Low Watermark
  - Percent Processor Memory Used
  - Processor Memory Free
  - Processor Memory Used
  - SNMP Response Time
  - STP topology changes count
  - TCP Out Segs

  - TCP Retrans Segs
  - TCP Segment Retransmit Percent
  - Temperature State
  - Temperature value
  - rcKhiPerformanceCurrentOutError
- Show VM Host
- Show Events
- Show Dashboard
- Properties
- VoIP Devices
- Details
- Subnet Details
- Physical Data Center
- Mark for Removal
- Supervisor Settings
- Connections — Displays connections of the selected node.
- VLAN view — Displays the VLAN view of the selected node.
- MLT (Multi-Link Trunking) connections
- MLT interfaces
- MLT view
- Network connections
- VoIP connections
- VoIP devices
- Details (All)
- Physical children
- WAN connections
- Subnet map
- Layer 7 All Dependencies
- Layer 7 Client Dependencies
- Layer 2 All Dependencies
- Layer 2 Client Dependencies
- Layer 2 Server Dependencies

- Layer 7 Server Dependencies
- Applications
- Services

Note:

Applications and services are similar because they refer to software running in a server or any computer platform. Software that serves only one purpose is an application. An application serving other applications is known as a service. For Monitoring, http is a service on the CM; and a phone has a phone application. Another explanation is that services are detected by a port scan, meaning that software listening on a well known port is a service.

Depending on the item you select, the double-click action on a tree browser item has a default behavior. If the item is a folder or any icon with a + in front of the item, then the item or folder is expanded to show sub folders or sub items. If the item or folder is expanded with a - in front of the item, then the item is collapsed. If the icon has no + or - in front of the item, then the double-click action takes the central pane view to that item. If you double-click on an icon, then there is a right-click menu associated with the item.

Faults display in tree view

You can see if faults exist on sub items in the tree view without expanding the item. Tree view color propagation is available in the Layer 2, Layer 3 and VLAN perspectives only.

A partial color spot on one edge of the folder or icon in the collapsed state indicates that a fault exists on some element inside the folder that is partially impairing functionality. The color of the spot indicates the severity of the impairment. A full color spot outside of the icon indicates that a full impairment exists inside one of the items in the icon.

The 10.133.139.125 device displays a partial spot, which means that faults exist on the sub items. You must expand the tree to see the faults. The following image displays a partial spot.

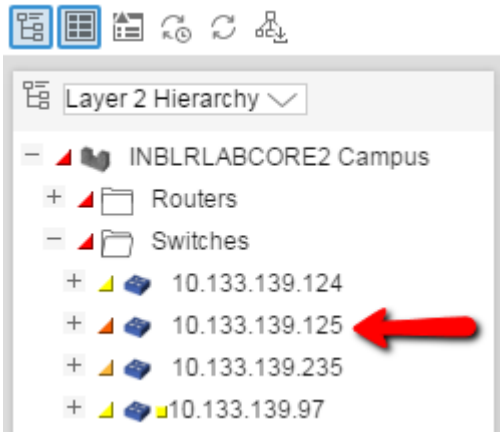


Figure 2: Example of a partial color spot

The following image displays a full spot, which means the fault or problem is with that particular interface. The top level folder or device always displays the highest severity color. In this case, the highest level on the 10.133.139.125 switch in the previous example displays as orange.

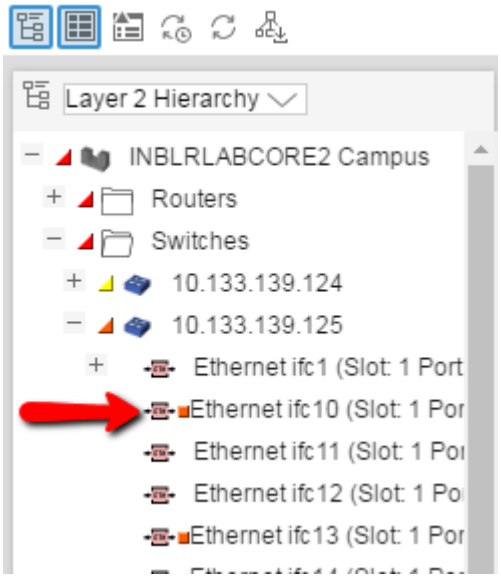


Figure 3: Example of a full color spot

A spot with a color of orange is more severe than a yellow-colored spot. A full spot suggests the problem is with that particular device, or slot and port.

Central browser

This section provides an overview of the central browser, located in the middle panel of the Network Topology page. Select **Network** > **Topology** to access these options. The central browser panel acts as a Topology Viewer or Table Viewer based on the perspective being used.

The central browser provides a graphical display of the network topology, which enables you to visualize a network as a schematic of icons connected by lines.

The central browser permits you to move icons, save the new layout, and share the layout for other users to see. You can enter the edit mode to change a view, save after editing a view, or revert to the previous view. To move icons, click the **enter edit mode** button and then select the icons to move. After you move the icons, you can save the view, and then you can make the view visible to other users by checking Share with other users, or you can keep the view private. You can enable a shared view for other users to edit, or enable the shared view as read only for other users to view.

The table view in the central browser displays groups of network elements in row/column form and provides information that is best shown in tabular format, such as processes running on a server, the databases running on a server, scope members, and listings the interfaces of a device.

VLAN

Select the VLAN Hierarchy in the perspective menu, which is the top left drop-down menu for **Network** > **Topology** to list the VLANs in a campus. Right-click on a VLAN, and select **show Vlan view** to show the VLAN view in the central browser.

Scopes

When viewing scopes, the tree browser shows the scopes, and the central browser shows a table of all members of the scope. To view scopes, in the **Network** > **Topology** section, select scopes from the drop-down menu on the top left above the tree browser.

Note:

When viewing scope members for ESXi devices, it is normal for negative values to appear in the Index column.

The following table describes the menu options when you right-click on an icon in the central browser. Not all options are available for all icons.

Menu option	Device Group	Description
Tables	Campus	Provides the following details about the campus in a table format: • Devices—Displays a table with information about the devices that are connected to a campus. • Network Devices—Displays a table with information about the network devices connected to a campus. • MLT Details Table—Displays a table with information about the MLT details associated to devices connected to a campus. • campusVoIPDevices—Displays a table with information about VoIP devices associated with a campus.
	Device	Provides the following details about the device in a table format: • Interfaces—Displays a table with information about the interfaces associated with the selected device • Interface Groups—Displays a table with information about the interface groups associated with the selected device. • Physical Elements—Displays a table with information about the physical elements associated with the selected device. • Show Bonded Channels—Displays a table with information about the bonded channels associated with the selected device. • Connected Devices (All)—Displays a table with information about all connected devices associated with the selected device. • Connected Devices (Network)—Displays a table with information about network connected devices associated with the selected device. • Connected Devices (MLT)—Displays a table with information about MLT connected devices associated with the selected device.

Table continues…

Menu option	Device Group	Description
		• Connected Devices (VoIP)—Displays a table with information about VoIP connected devices associated with the selected device. • MLT Details Table—Displays a table with MLT details for the selected device. • Stack Units—Displays a table with the devices connected to the stacked unit. **Note:** After you select a table, you can select another table for the same device from the drop-down list available at the top of the central browser.
	ESXi	Provides the following details about the ESXi device in a table format: • Interfaces—Displays a table with information about the interfaces associated with the selected device **Note:** When viewing scope members for ESXi devices, it is normal for negative values to appear in the Index column. • Processors—Displays a table with information about the processors associated with the selected device. • Physical Elements—Displays a table with information about the physical elements associated with the selected device. • Show File Systems—Displays a table with information about the file systems associated with the selected device. • Show Applications—Displays a table with information about the applications associated with the selected device. • Show Services—Displays a table with information about the services associated with the selected device.
Schematics	Campus	Provides the following schematic information about the campus: • Details • Subnet Details • Physical Datacenter
	Device	Provides the following schematic information about the device: • Layer 2 Details—Displays the domain element details according to their OSI layer 2 functions.

Table continues…

Menu option	Device Group	Description
		• MLT Schematic—Displays the MLT schematic for the selected device. • Network Neighbors—Provides access to the backbone neighborhood schematic view for a selected domain element. This view, intended for improved viewing of domain elements in very large domains, expands the view to show domain elements that are connected by one hop to the selected domain element. • Show Campus—Shifts view to the campus for the selected device. • Show Paths...—Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.
	ESXi	Provides the following schematic information about the ESXi device: • Layer 2 Details—Displays the domain element details according to their OSI layer 2 functions. • Show Paths...—Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.
	G450	Provides the following schematic information about the G450 device: • Layer 2 Details—Displays the domain element details according to their OSI layer 2 functions. • Network Neighbors—Provides access to the backbone neighborhood schematic view for a selected domain element. This view, intended for improved viewing of domain elements in very large domains, expands the view to show domain elements that are connected by one hop to the selected domain element. • Show Campus—Shifts view to the campus for the selected device. • Show Paths—Enables you to view the shortest network path between any two points in the network. Show Paths is not a live path trace. Although interfaces may be end-points, intermediate interfaces are not shown along paths. Only intermediate devices are shown.

Table continues…

Menu option	Device Group	Description
Configure	Campus Device ESXi G450	Enables you to perform the following configuration actions: • Mark for Removal—Marks the device for removal from the next discovery. • Supervision Settings—Enables you to define the supervision settings for the selected device. The values include the following: inherit, supervise, unsupervise. • Overrides...—Displays a table with configuration, scope, override, and value of the selected device or campus. You can add, delete or edit an override.
Monitoring	Device	Enables you to perform the following configuration actions: • Add custom monitoring
Diagnose	Device ESXi G450	Enables you to perform the following diagnostic actions for the device: • MIB Query • MIB Browse • ICMP Ping • Trace Route • SNMP Get • Remote Ping • Remote Traceroute
SPBM Diagnose Tools	Device	Provides the following SPBM diagnostic tools: • L2 Ping • L2 Traceroute • Unicast Path • Multicast Path
Tools	Campus	Provides a launch point for commonly used device element management tools. The following tool is available for the campus: • Rediscover Campus
	Device	The following tools are available for the device: • EM-Launch • HTTP-connection • Rediscover Device

Table continues…

Menu option	Device Group	Description
		Note: Rediscover Device detects changes for the selected device only. You must use a campus or domain rediscovery to detect connected devices and topology changes.
	ESXi	The following tools are available for the ESXi device: • HTTP Connect • Rediscover Device • VMware vCenter
	G450	The following tools are available for the G450 device: • EM Launch • Launch Secure EM • Rediscover Device
Trends	Campus Device ESXi G450	Trends are performance graphs for devices or interfaces. The trends menu lists a collection of MITs that are configured and can be trended. For example, device CPU usage is a configured Monitored Information Type (MIT) that you can trend.
Show Events	Campus Device ESXi G450	Opens a tab in the in the bottom pane of the events browser, that displays all events for the selected element. The tab remains open until you manually delete the tab.
Show Dashboard	Campus Device ESXi G450	Opens the dashboard view with details of the selected campus, or device.
Properties	Campus Device ESXi G450	Displays the Properties window for the selected device which shows the device properties and associated values.
Color-Coding of Domain Elements	Campus Device	Domain elements displayed in the schematic diagram are colored based on the messages that relate to them.

The following table lists the symbols used on the Monitoring interface. Symbols in blue denote an approved vendor device, and symbols in grey denote a multi-vendor device.

Device Type		Icon
Generic Router	Xylogics 5399	
	Nautica RAS 4000	
	VPN Branch Access Device	
Host		
Multi-vendor Router		
Multi-vendor L3 switch		
Multi-vendor L2 switch		
Secure Routers	Secure Router 1001/1001S	
	Secure Router 1002/1002E	
	Secure Router 1004/1004E	
	Secure Router 4134	
	Secure Router 3120	
	Business Secure Router 252/222	
	VPN Router 1500	
Ethernet Switches	ES 325 Series	
	ES 425 Series	
	ES 450	
	ES 460 Series	
	ES 470 Series	
	ERS 2500 Series	
	ERS 3500	
	ERS 3510-24T	
	ERS 4500 Series (4526, 4548, 4550)	
	ERS 1424T	
	VSP 4000 series	
	VSP 9000	

Table continues…

Device Type		Icon
Legacy Ethernet Switches	Alteon 180e	
	Alteon 184	
	Alteon AD4	
	Alteon AD3	
	BayStack 28104	
	BayStack 28200	
	BayStack Orion	
	BayStack 350-12T	
	BayStack 3410 100BASE-T	
	BayStack 302T/F Ethernet Workgroup Switch	
	OPTeraMetro ESU 1800 DC	
	OPTeraMetro ESU 8003	
	OPTeraMetro Packet Edge	
	BayStack 100	
	58000	
	BayStack 350	
	BayStack 303	
	BayStack 310	
	BayStack 410	
	Accelar 8132TX	
	BayStack 420	
	OPTeraMetro ESU 1200	
	BayStack 380	
	OPTeraMetro ESU 1450	
	OPTeraMetro ESU 1400	
	Centillion 100	
	Centillion 301	
	Centillion 5000BH	
	Centillion 50 Ethernet	
	Centillion 50 Token Ring	
	Centillion 5005BH	
Legacy Ethernet Switches	Accelar 1100	
	Accelar 1250	
	Accelar 1150	

Table continues…

Device Type		Icon
	Accelar 1200	
	Accelar 1050	
	OPTeraMetro ESU 1800 AC	
	ESU 1850AC	
	ESU 1850DC	
Ethernet Routing Switches	ERS 8300 Series (8306, 8310)	
	ERS 8600 Series (8603, 8606, 8610)	
	ERS 5500 series (5510, 5520, 5530)	
	ERS 1612G/1624F,1648T	
Legacy Switches	Passport 8100	
	OPTeraMetro ESU 8010	
	OPTeraMetro ESU 8010co	
	OPTeraMetro ESU 8003	
	OPTeraMetro ESU 8006	
Server		
Wireless end nodes		
Multi-vendor wireless end nodes		
Wired end nodes		
Communications servers	CS 1000 Signaling Server	
	CS 1000 Call Server	
	Communication Server 2100	
	MCS 5100 System	
Generic Server		

Table continues…

Device Type		Icon
Firewall		
VPN Routers (Contivity)	VPN Router 221	
	VPN Router 251	
	VPN Router 600	
	VPN Router 1010/1050	
	VPN Router 1100	
	VPN Router 1600	
	VPN Router 1700/1740/1750	
	VPN Router 2600	
	VPN Router 2700/2750	
	VPN Router 4600	
	VPN Router 5000	
	VPN Gateway 3050/3070	
Wireless LAN AP 2330/2330A, AP8120		
Wireless switches and gateways	Advanced Gateway AG2330MCR	
	Media Gateway (Gxx0 Gateways)	
	Wireless Security Switch 2350	
	Wireless Security Switch 2380	
	Wireless Security Switch 2360	
	Wireless Security Switch 2361	
	Wireless Gateway 7240/7250	
Switched Firewall (NSF)		
Secure Network Access Switch 4050 Secure Wireless Controller Switch WLAN 8180		
Legacy hubs	MX 200	
	Synoptics Baystack 3000	
	Synoptics Baystack 3030	
	LattisNet 2310 Ethernet	
	LattisNet 2810 Ethernet	
	Synoptics Token Ring 271x	
	Synoptics BayStack 291X FDDI	

Table continues…

Device Type		Icon
	Synoptics BayStack 281X enet	
	Synoptics 5000 / 5050	
	281xSA	
	Synoptics 810M	
	271xSA	
	5DN00x	
	BayStack Ethernet (Hub)	
	BayStack Token Ring (Hub)	
	BayStack 150	
	BayStack 200	
	BayStack 3410 100BASE-T	
	BayStack Ethernet NMM 810M	
	BayStack 100BASE-T Advanced NMM Agent	
Stacks		
Invisible device (can occur in path trace views)		
Alteon Application switch (2208/2216/2216-E/2224/2424/2424-E/ 2424-SSL/2424-SSL-E/3408/3408-E)		
Hub		
IP Deskphone	SIP and H.323 IP Phones	
	1600 Series IP Phones	
	4800 Series IP Phones	
	9600 Series IP Phones	
Printer		
Business Communications Manager (BCM, BCM50, BCM200/400, BCM450) Multiprotocol Router Session Manager (ASM) System Manager (SMGR)		

Table continues…

Device Type	Icon
Belden router	
Belden switch	
Wireless Access Point (7220/7220Duo/7215/7215Duo/8120)	
WLAN Application Gateway 2246 WLAN IP Telephony Manager 2245	
Wireless Bridge 7230/7230 Ext	
Unspecified IP device/Unmanaged device	
Workstation	
PC behind phone	
Ethernet Circuit	
Ethernet Interface	
VLAN	
Subnet/LAN	
Domain	
VMs	

Table continues…

Device Type		Icon
VM hosts		
VM interfaces		
Uninterrupted power supplies (UPS) devices		
Redrack		
Pod Fx		
Third party multitenant application		
management application		
Third party management application		
Storage system		
Building/Campus		
metro_dwdm switch	Optical Metro 5000	
Fault on device: the background color indicates the fault		
Unsupervised device		

Table continues…

Device Type	Icon
Device marked for removal	

Layout options

The layout options enable you to choose a schematic display of the network topology. You access the network topology through **Network** > **Topology**. The following global layout options are available in the central browser toolbar, beside Layout:

- Hierarchical—The hierarchical layout lays out the icons hierarchically.
- Symmetric—The symmetric layout lays out the icons with a tendency towards symmetry.
- Circular—The circular layout lays out the icons in a circle.
- Horizontal Grid—The horizontal grid layout lays out the icons in a horizontal line.
- Compact—The compact layout lays out the icons in an efficiently compressed manner.

Important:

You can move icons in the custom views only, after you click **Enter edit mode**.

For each type of schematic, Monitoring chooses a layout algorithm by default as follows:

Type of schematic	Layout algorithm
WAN view	Symmetric
Campus view	Hierarchical
Subnet view	Symmetric
Backbone Neighborhood	Hierarchical
Layer 2 Details	Hierarchical
Path Trace	Hierarchical
Application Dependency	Hierarchical

When you modify the layout algorithm for a particular schematic, the chosen algorithm becomes the default for that specific view. Other views within the same domain or other domains remain unaffected. The system shares view selections with all users, so that a change by one user applies to all users.

Users share all predefined view selections. You can share custom view layouts only if you share the layout by checking **Share with other users**. After you change and share a layout, other users can view the layout.

After you select a layout option, global or Monitoring defined, the selection you make overrides the settings described in the preceding table.

The predefined layout changes remain in effect until Monitoring restarts. If any two users choose different layouts for the same view at the same time, then the system saves the change made by the last user.

After you enable editing through the central browser toolbar in **Network** > **Topology**, and make changes, you can save the changes.

You can use the following icons to modify the layout of the topology map:

- Zoom to fit—Adjusts the view to fit the contents pane.
- Layout—Lists of available topology layouts. Global layouts are disabled in all custom views.
- Panning—Shifts the view from one area of the contents pane to another area. You can pan in the following two ways:
  - By right-clicking in the central area; the pointer turns to a hand grab gesture that you hold and move.
  - By using the horizontal and vertical scroll bars.
- Magnification—Magnifies an area on the topology. To magnify an area, press and hold down the shift key, right-click and drag the mouse over an area; the pointer turns to a magnification glass and magnifies an area of the topology.
- Schematic zoom level—Adjusts the zoom level in the contents pane. You can use the percentage field or the zoom bar to adjust the schematic zoom level.
- Go to—Shift the current topology view to another view.
- Enter edit mode—Add link, Add icon, Public or private settings.
- Add links—Add a link to the current topology map. Solid lines show actual physical connections. Dotted lines show logical connections or data path between elements.
- Add—Add an icon to the current topology map.
- Save changes—Saves the changes you have made to the system.
- Discard changes—In the custom view, discards all changes and reverts to the previous view.
- Add elements—Adds elements to the topology.
- Set background—Use to set the background.
- Download background image—Downloads a background image.

MLT/SMLT schematic layout

The topology map is enhanced to keep the groups of devices participating in an MLT/SMLT together on the campus detail view so that the SMLT configuration (triangle, square, or mesh) is evident. The possible layouts are grouped at the core for 2, 4, or 6 switches showing the MLT/SMLT and IST links.

The following diagram illustrates the network topologies.

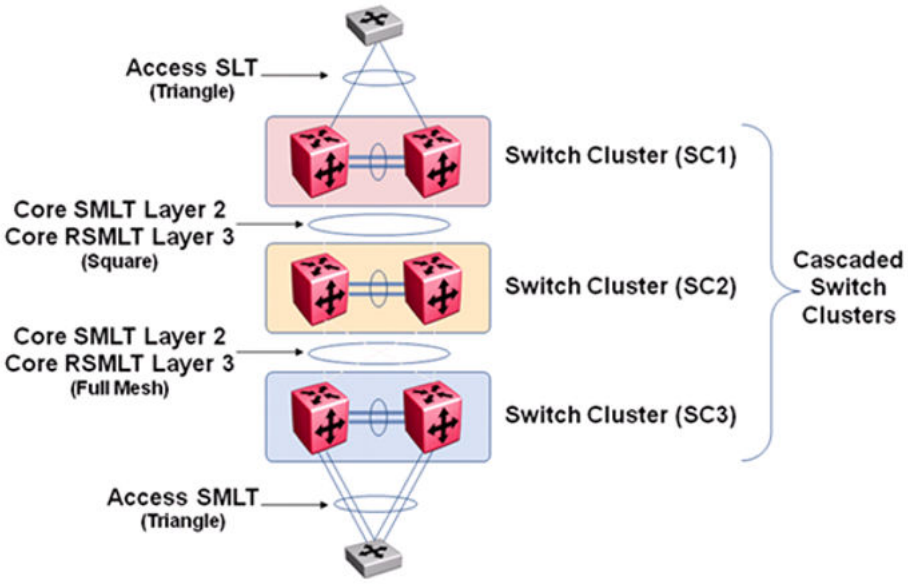


Figure 4: Network topology

A number of edge switches connect to the core switches by simple or SMLT links. The layout does not make an attempt to keep the entire range of edge switches close, because the number of edge switches in a real network can be large and the topology map becomes congested if all edge switches are kept close. However, the user has the move icons feature to make customizations or adjustments to the automatic layout provided by Monitoring.

Map background controls

After you enter the edit mode, in the central browser for **Network** > **Topology**, you can import a background image by clicking the following **Set background** icon.

.

To set a background image, click the download background image button, and browse to the required file. You can set background images with JPEG, GIFF, and PNG files. To save the background image, click **save schematic** in the central browser toolbar, and enter information in the Save schematic dialog box. The schematic is saved in the Custom views perspective under the public or private folder.

Properties table

This section provides an overview of the properties table, located on the right side of the Network Topology page. Access Network Topology by clicking **Network** > **Topology**.

To view the properties table, on the Network Topology menu bar on the top left, click **Show property table**, or in the contents pane, right-click on a device or campus. To remove the properties table from view, click **Hide property table**.

The properties table displays the variables, or properties, and corresponding values for a selected domain element and enables you to edit settings for some of those variables. Properties are grouped in different categories that you can expand or collapse. Each category includes various types of information about the element, and vary based on the class or element. The name or value that appears in a collapsed property is the most common property in that group.

The standard properties that are shared by almost all network elements include:

- Name
- Description
- Network Configuration
- Management State
- Management Config

Variable definitions

The following table describes information in the properties table for the Layer 2 Hierarchy perspective. You can access the table in **Network** > **Topology** by right-clicking on a device, and selecting properties.

Variable	Definition
Name	Displays the following name information about the device. • Name—The name is determined through an algorithm that searches a series of names for a device. The algorithm first looks to any custom name defined by the user (see below) and then continues to search for a DNS name, SNMP management name, WIN name, and IP address and the algorithm selects the first of those names found a result for as the name. • Host Address—The device IP address. Click the drop-down arrow to select another IP address associated to the device. • Custom Name—Enables users to override the name by specifying their own name for the element through this property. Note: When users do a discovery for the first time, no devices have a custom name and therefore the system goes through the basic algorithm to find a name. **Important:** After you create a custom name, you must go to the Network Discovery page and click **Save Domain** to save the domain. If you do not save the domain, the custom name is not saved after an Monitoring restore or restart. • DNS Name—The DNS name of the device. • Management Name—The management name of the device, which may be the same as the name of the device. • Qualified Name—The qualified name of the device, which may be the same as the name of the device.

Table continues…

Variable	Definition
	• ID—The ID number for the device. • WINS Name—The WINS name for the device.
Description	Displays the following information that describes the element. • Description • Device Type • Hardware Version • Location • Manufacturer • OEM Model • SNMP Product ID • CIM Product ID • Serial Number
Network Configuration	Displays the following network information. • Host Address • Interface Info • Layer3 Vlan Interface Info
Management State	Displays the following information about the management of the element. • Alarm State—Indicates if the device has faults. • Subelement Alarm State—Indicates if the subelement has a fault. • Supervised—Like invisibility, only governs whether or not element will be monitored for events. • Marked for Removal—This is referenced during the merge step of rediscoveries. Set this to true if the element is no longer in the network and you want to override the discovery engine's "keep missing equipment" policy. **Note:** If an element is still on the network, discovery does not remove the element from the model. • Invisible—Yes/No/Inherit. Inherit by default except for campus element which have value false. The invisibility property inherits downwards by containment. So, set a campus invisible and all elements within will be invisible. Containment hierarchy is campus - device - interface. • First Discovered • Last Discovered

Table continues…

Variable	Definition
Management Config	Displays the following information about the management config: • SNMP version • Authentication • Management Name • Management Location • Management Contact

Event browser pane

The event browser pane appears at the bottom of the Network Topology page and permits you to view messages for events in the network that you manage.

Controls	Description
Add a new message board	Adds a message board.
Delete selected message board	Deletes the current board (second icon from the left).
Rename selected message board	Renames the current board.
Configure filter for selected message board	Displays message board filter options. Each message board can have its own filter.
Auto refresh	Allows you to specify the time interval at which message board information is refreshed. After you click Auto refresh, a window appears that allows you to select the appropriate refresh interval. If the auto refresh settings are different from the message board settings then they affect the entire Event Browser.
Refresh	Refreshes the message board. Refresh is not only for a single message board, the refresh affects the entire Event Browser.
Export selected message board	Allows you to export the contents of the current message board as an XML file (with the applied filter). Exports the current message board and not the entire Event Browser content.
Message board operation	Allows you to acknowledge, unacknowledge, annotate, or clear all information on the message board.
Dispose transient message boards	Disposes of transient message boards.
Group by:	Specifies how to group events. You can select the following: • None • Ack.

Table continues…

Controls	Description
	• Pri. • Source Address • Target Address • Annotated • Device • Correlation • Event Name • Information Available • Sub. • Domain • Subject • Received • Rep. Count • Summary • Last Updated

Monitoring configuration

Monitoring configurations define what events are received for which domain elements and with what alternative event processing options. The Monitoring application has built-in monitoring configurations. You can also customize monitoring configurations.

Starting and stopping monitoring

Important:

Do not start and stop individual agents. The system allows you to do so, but starting and stopping individual agents can cause issues. Instead only start or stop monitoring on the domain as a whole as suggested below.

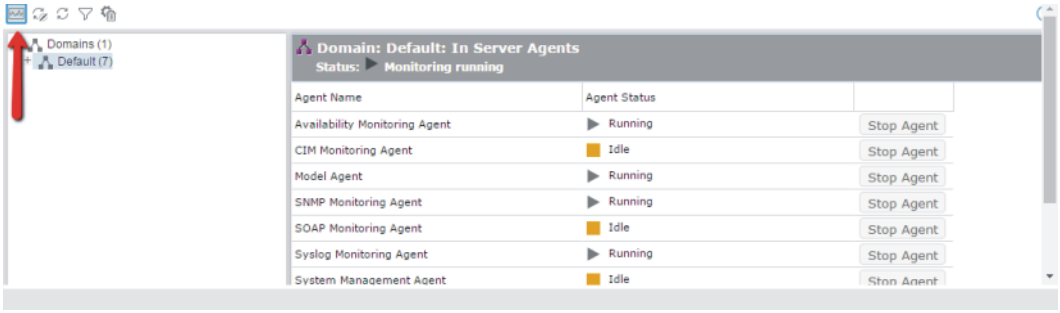
You can start and stop the monitoring action of an entire domain.

Procedure

1. Select **Network** > **Monitoring Details**.
2. Select the domain for which you want to start monitoring from the list of domains and agents in the left panel.

3. Click **Start Monitoring** from the toolbar on the top left to start monitoring.

   Monitoring begins for the selected domain. When monitoring starts for a selected domain, the expandable list of domains and agents is refreshed.



4. Click **Stop Monitoring** from the toolbar on the top left to stop monitoring.

Variable definitions

The following table describes the options in the **Network** > **Monitoring Details** tree on the left.

Variable	Value
Domains	A container element for the list of domains for your system.
Availability Monitoring Agent	Displays the monitoring requests and domain elements defined for the availability monitoring agent.
CIM Monitoring Agent	Displays the monitoring requests and domain elements defined for the CIM monitoring agent.
Model Agent	The primary use of the model agent is to monitor software; for example, application availability. The secondary use of the model agent is to monitor legacy hypercube MITs; for example, power consumption aggregation by stack and campus.
SNMP Monitoring Agent	Displays the monitoring requests and domain elements defined for the SNMP monitoring agent.
SOAP Monitoring Agent	Displays the monitoring requests and domain elements defined for the SOAP monitoring agent.
Syslog Monitoring Agent	Displays the monitoring requests and domain elements defined for the syslog monitoring agent.
System Management Agent	Displays the monitoring requests and domain elements defined for the system management agent.

Viewing active monitoring configurations

Procedure

1. Select **Network** > **Monitoring Details**.

2. Expand the domain for which you want to view the set of active monitoring configurations.

   You must be monitoring the domain to view the active monitoring configurations.

3. Expand the agent you want to view.
4. Select the Monitoring Requests you want to view.

   You may need to expand the Monitoring Requests (if there are multiple Monitoring Requests for the agent). Then select the Monitoring Request of interest to display the details in the right panel of the Monitoring Details.

5. Select the domain element for which you want to view the variables and associated values.

Defining a parameter override

Overrides are parameters that enable you to define an exception for a monitored event type for the domain elements in a particular scope.

The override definition consists of one or more event type parameter values, and one or more scopes. Each override value that you specify is an exception to the usual behavior for which you expect to monitor. By defining an override, you tell Monitoring that you want to monitor for this value specified in the override, not the value that is set in the MIT definition, for the domain elements encompassed by the indicated scope(s)

Procedure

1. Select **Network** > **Monitoring Overrides**.

   You can select either the Monitoring Overrides tab or the Event Processing Override tab. Some of the options are different for each tab.

2. Click **Add a new override**.
3. In the Prompt dialog box, type a name for the parameter override.

   The name must be unique and must start with an alphanumeric, and can contain alphanumerics, spaces, underscores (_) or hyphens (-) but not special characters.

4. Click **OK**.

   The parameter overrides settings display in the right panel of the Parameter Overrides window. For a description of the variables on this screen, see the variable definitions table below.

5. Enable or disable the override by selecting or clearing the **Enabled** box.
6. Click the **Add domain element scope** link. The Choose a scope window appears.
7. Expand the tree structure and select the scope to which you want the monitoring override to apply.
8. Click **OK**.

9. Select the MIT for which you want to define an override. The parameters for the selected MIT appear on the right side of the pane.
10. Select the parameter for which you want to define the override. The parameter description and value appear in the bottom right box.
11. Specify the desired override value for the parameter. Depending on the parameter this might include typing a new value, selecting new units from a drop-down menu, or a combination of actions.
12. After you select the desired override value click **OK**.
    - If you want to add another parameter override, click **Apply**.
13. Click on the drop down menu in front of **Override applies to** and select **All Domains** or **These Domains**. If you choose the option These Domains, then select the domains on which you want this override to apply.
14. To save your changes, click **Apply your changes**.

Variable definitions

The following table describes the **Network** > **Monitoring Overrides**, and select the **Monitoring Overrides** tab.

Variable	Value
Enabled	Indicates whether or not the event processing override is active (enabled).
Parameter Overrides	Provides a list of the existing parameter overrides. Includes links that enable users to edit existing override values. • Add domain element scope—Selects the domain element scopes to which you want the override to apply. • Add domain element—Selects the domain element to which you want the override to apply
Override Applies to	Selects whether the override applies. For the event processing overrides, you select whether the override applies to an event scope or event type. Once an option is selected, you can then use the tree selection list to specify the appropriate event scope or event type. The Override Applies to menu appears twice for the event processing overrides and once for the monitoring overrides. For the monitoring overrides and the event processing overrides you can also select the domain to which the override parameters are to apply. Valid values are All Domains (the override parameters are to apply to all domains) and These Domains (the override parameters are to apply only to the selected domains).

Configuring overrides for a device from the Network Topology

Perform the following procedure to configure overrides for a device from the Network Browser.

Procedure

1. Select **Network** > **Topology**.
2. Select a perspective in the drop-down menu above the left tree browser, and select an element.

   Note:

   You can use any of the network topology views except the scope view. Override navigation is not permitted from scope views.
3. From the Network Topology center pane, right click on a device, and select **Configure** > **Overrides**.
4. To add an override configuration, click **Add**.
5. In the Specify Scope of Override dialog box, select a scope.

   Note:

   You can use the search field to find the scope you require for the device.
6. If the scope applies to one device only, select **Apply new override only to <device name>**.
7. Click **Next**.
8. In the Parameter Override dialog box, select a parameter override, and click **Search Depth**.
9. Configure your value in the parameter value respective field.

   Note:

   Set the appropriate values related to the parameter fields.
10. Click **Next**.

    The Define additional overrides and save to configuration dialog box appears that contains configured overrides and configuration tables.
11. To add another override, click **Add**, select a parameter override and configure your value in the parameter value respective field.
12. Select a configuration in which to save the new overrides table in, or create a configuration by entering a name, and clicking **OK**.
13. Click **Finish**.

Viewing overrides

About this task

Perform the following procedure to view overrides for a device. The most specific overrides appear at the top of the list. Monitoring crosses out overrides if another override takes precedence.

Procedure

1. Select **Network** > **Topology**.
2. Select a perspective from the drop-down menu above the tree browser at the left, and select an element.

   Note:

   You can use any of the network topology views except the scope view. Override navigation is not permitted from scope views.
3. From the Network Topology center pane, right click on a device, and select **Configure** > **Overrides**.

   The Overrides window for the device appears.

Editing an override

You can change the parameters of the override after you create the override.

Procedure

1. Select **Network** > **Monitoring Overrides**.

   The configuration settings for the selected monitoring configuration display on the right panel of the page.
2. Select the override you want to edit.

   The settings for the selected override display on the right panel.
3. Select Edit, and edit the settings as needed.
4. To save the change, click **Apply your changes**.

Renaming an override

After you create an override you can change the name.

Procedure

1. Select **Network** > **Monitoring Overrides**.
2. Select the override you want to rename.
3. Click **Rename selected override**.

   A Prompt dialog box appears.
4. In the Prompt dialog box, enter the new name.
5. Click **OK**.

Cloning an override

You can clone an existing override if you want the same override parameters for different scenarios.

Procedure

1. Select **Network** > **Monitoring Overrides**.
2. Select the override you want to clone.
3. Click **Clone selected override**.
4. In the Prompt dialog box, enter a new name for the cloned override.
5. Click **OK**.

Deleting an override

You can delete an existing override if you do not need the override.

Procedure

1. Select **Network** > **Monitoring Overrides**.
2. Select the override you want to delete.
3. Click **Delete**.
4. In the Confirm dialog box, click **OK**.

Adding custom monitoring for a device from the Network Topology

About this task

Add a custom monitoring configuration to specify a new set of constraints to monitor your network.

Important:

If a device is already being monitored by a built-in monitoring configuration and you add a custom monitoring configuration for the device, the device is excluded from the built-in monitoring configurations.

Procedure

1. Select **Network** > **Topology**.
2. Select a perspective from the drop-down menu in the tree browser on the left, and select an element.

3. From the Network Topology center pane, right click on a device, and select **Monitoring** > **Add custom monitoring**.

   A notice appears if the device is already being monitored warning that if you define custom monitoring for the device, the device will be excluded from the current built-in monitoring configurations. Click **OK**.

4. If you have the Advanced Monitoring license, click **Advanced** to select the advanced options for custom monitoring configuration.
5. Make the appropriate changes to the monitoring configuration.
6. Click **Confirm**.

Variable definitions

Use the following information to configure custom monitoring.

Note:

Not all of the parameters below are available for every device on the system.

Variable	Definition
Networking Device Availability	Monitors any type of event regarding the availability of the device. Typically the option displays the IP availability from the perspective of the management station.
Device Poll Response Statistics	Monitors the response statistics pertaining to availability polls.
KHI Information	Monitors Key Health Indicators (KHI) information.
PoE Information	Monitors any information relating to Power over Ethernet (PoE), and pertaining to PoE hardware.
Interface Information	Monitors any network interface information.
Bridge Statistics	Monitors any statistic related to a network bridge or spanning tree protocol.
ISIS Information	Monitors any information relating to the Intermediate-System-to-Intermediate-System (IS-IS) networking protocol.
Transceiver Information	Monitors the transceiver information in any kind of event or statistic pertaining to a transceiver. Typically this will be an optical transceiver such as an SFP or mini-GBIC conforming to the SFF–8472 industry standard.
Additional SNMP Traps	Monitors the Simple Network Management Protocol (SNMP) traps, which gather information about device activities, alarms, and other information on management stations.

Modifying custom monitoring

Procedure

1. Select **Network** > **Topology**.
2. Select a Perspective, and select an element.
3. From the Network Topology center pane, right click on a device, and select **Monitoring** > **Modify custom monitoring**.
4. A notice appears warning that the device is already being monitored and if you define custom monitoring for the device, the device will be excluded from the current monitoring configurations. Click **OK**.
5. Make the appropriate changes to the monitoring configuration.
6. Click **Confirm**.

Disabling device availability

Use this procedure to disable device availability to stop ICMP polling. SNMP polling continues even with device availability disabled.

Procedure

1. Select **Network** > **Topology**.
2. Select a perspective from the drop-down menu in the tree browser on the left, and select an element.
3. Perform one of the following two steps:
   a. If no custom monitoring exists for the device, from the Network Topology center pane, right click on a device, and select **Monitoring** > **Add custom monitoring**.
   b. If custom monitoring already exists for the device, from the Network Topology center pane, right click on a device, and select **Monitoring** > **Modify custom monitoring**.

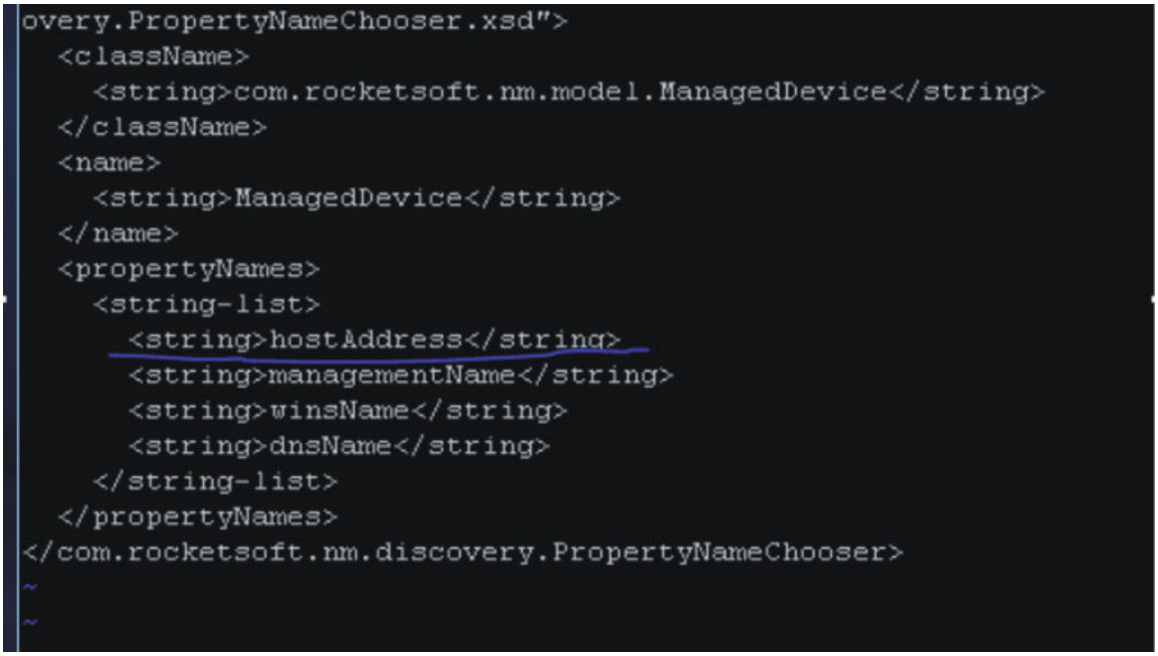
   A notice appears if the device is already monitored warning that if you define custom monitoring for the device, the system will exclude the device from the current built-in monitoring configurations. Click **OK**.
4. Clear the **Networking Device Availability** and **Device Poll Response Statistics** check boxes.
5. Click **Confirm**.

Changing the name of a network device

Use this procedure to change the name of the network device from the management name to the host address.

Procedure

1. Use SSH to access the monitoring virtual machine (VM), and log in as the admin user.
2. Change to the root user.
3. Copy the file from `/opt/avaya/smgr/vpfm/knowledge/product/model/nameChoosers/ManagedDevice.xml` to `/opt/avaya/smgr/vpfm/knowledge/site/nortelvpfm/model/nameChoosers`.
4. Edit the file ManagedDevice.xml and place the name you want, such as the host address, on the top of the list.



5. To restart the kbmd service, elect **Administration** > **Appliance Device Manager**, click on the Monitoring module in the Services portlet, and click **Restart Services**.

   After you make the change the name of the devices will display as the hostAddress, rather than the management or DNS name.

Chapter 9: Monitoring reports

Monitoring reports

Monitoring offers multiple built-in monitoring reports.

If you have an advanced license, the ability to create or customize monitoring reports.

To view the Monitoring Reports, from the menu bar, select **Reports** > **Monitoring Reports**.

The various reports you have configured appear in the content pane at the right.

On the left, of the pane the system displays the following:

- Favorites—Displays the reports you view the most often.
- Most recently viewed—Displays the most recently viewed reports
- Search—Allows you to search the reports for particular information.
- All reports—Displays both the build-in reports, and those you have custom configured.

Hypercube Table reportlet

You can use online analytical processing (OLAP) to analyze information across multiple dimensions. At the center of OLAP is a hypercube. A hypercube is not a cube in the strict mathematical sense. A hypercube is a multi-dimensional generalization of a two or three dimensional spreadsheet.

A hypercube consists in two elements:

- Measures—Specifies the variable you want to measure, such as average CPU, maximum CPU, Memory capacity, or another variable.
- Grouping fields—Specifies how you want to analyze the information, such as by type of device, by time of day, by slot number, by status, by name, or another variable.

You can access the Hypercube Table reportlet under **Reports** > **Monitoring Reports**. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.

For more information about configuring Hypercube, see Configuring the Hypercube Table reportlet on page 145.

Monitoring Reports configuration

Monitoring offers multiple built-in monitoring reports and the ability to create or customize monitoring reports. You cannot edit or delete built-in monitoring reports, but you can use a built-in monitoring report as the basis for a new monitoring report. To view the Monitoring Reports, from the menu bar, select **Reports** > **Monitoring Reports**.

Important:

You must have the Advanced license to create custom reports.

Important:

Users with the operator role can save reports as private only.

Viewing monitoring reports

Use this procedure to view monitoring reports. Monitoring is enabled by default.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. From the left navigation pane, select the report that you want to view from All reports (built-in, public, and private), Most recently viewed, or Favorites.

   The report displays on the right of the page.

Viewing discovery reports

About this task

View the logs related to a discovery.

Procedure

1. Select **Network** > **Discovery**, and click the **Discovery Problem Report** icon, or select **Reports** > **Monitoring Reports**.
2. Select a domain from the drop-down in the left domain field.
3. Select a node from the navigation panel.

   The left hand navigation pane on the Discovery Reports page organizes log messages based on category, severity, and IP address.
4. To troubleshoot why a particular IP address is not discovered or is discovered as unmanaged, locate the IP address in the left navigation pane.

5. One common reason for not discovering a device is the lack of response from the device from ping or SNMP requests sent from Monitoring. In this case, check the UCM device credentials to make sure they are correct.
6. If the credentials are correct, then check for SNMP access using the SNMP MIB browser.

Result

Some of the common messages that you encounter in the logs are as follows:

- Device did not respond to SNMP or ICMP

  If the device does not respond to SNMP or ICMP, then perform the following procedures:

  - Check if the device responds to ping.
  - Check if the device responds to SNMP from the Monitoring MIB browser.
  - Check with Wireshark to determine if the device is sending back a response.
  - If all of the above is occuring, check UCM credentials and rerun the discovery

- Potential managed device was excluded from discovery

  If the potential managed device is excluded from discovery, then perform the following procedures:

  - Check discovery constraints to ensure that the device IP is not excluded by subnet limits or other constraints
  - You may also see this message, or a similar message, if the topology table of one device includes this device, but this device is not found in the ARP table of any of the routers in that subnet. In this case, check the ARP table of the routers and fix any related issues. Monitoring discovers a device only if the device is found in the ARP table.

- There is no log entry for an undiscovered device
  - Make sure that UCM credentials exist for that IP and that they are correct
  - Make sure that the device's IP address in present in the ARP tables of one or more discovered layer-3 devices in your network.

Monitoring Reports wizards

Each Monitoring Report reportlet contains different elements that you must configure. After you drag and drop a reportlet icon onto the monitoring report, a dialog appears to help you configure the reportlet.

To view the Monitoring Reports, from the menu bar, select **Reports** > **Monitoring Reports**. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.

The following lists the reportlets that you can add to a custom monitoring report:

- Text
- Image
- Availability Report

- Top-N Report
- Event Listing
- Pie Chart
- Element Status
- Event Summary
- Dial Gauge
- Trend Chart
- Event History
- Inventory Table
- History Table
- Hypercube Table

Configuring the Text reportlet

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Text** icon onto the canvas outlined in the report work area.
4. In the **Preview** area, enter the text that you want to appear on the report.
5. Select a font and color.
6. In the **Area Adjustment**, select where you want the text to appear on the report.
7. Click **Finish**.

Configuring the Image reportlet

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Image** icon onto the canvas outlined in the report work area.
4. Click the **Select an image to upload** link to search for and select the image.
5. In the **Preview** area, review the image.
6. Scale the image as required.
7. In the **Area Adjustment**, select where you want the image to appear on the report.
8. Click **Finish**.

Configuring the Availability Report reportlet

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Availability Report** icon onto the canvas outlined on the report work area.
4. In the Name field, enter a name.
5. In the Items section, click **Add**.
6. Check single elements, or scope name to include all elements within a scope.
7. Click **Next**.
8. To include a graph, select the **Graph column** check box and click the down arrow to select a time frame for the report.
9. The Secondary columns section displays additional columns to appear on the report.
   - To remove a column, click **Delete**.
   - To add a column, click **Add**.

   Note:

   Use the up or down arrows to move up or down the list of available column headers.
10. To continue configuring, click **Next**.
    - Or, if the configurations are complete, click **Finish**.

Configuring the Top-N Report reportlet

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Top-N Report** icon onto the canvas outlined in the report work area.
4. In the **Name** field, enter a name.
5. Click **Choose a Scope**. The Choose a Scope page appears.
6. Select one or more scopes from the available list, and click **OK**.

Note:

You can use the Search field to search for a scope.

7. Click the **Variable** field, and select a variable.
8. In the **Top-N number** field, enter the number of items to appear in the Top-N Report.
9. Select **Bottom report** if you want to see the bottom first.
10. Select **Show reachability status** if you want to see the reachability status.
11. In the **Identification columns**, click **Add**, and select the information you want to add.
12. In the Secondary value columns section, click **Add**, and select the optional secondary columns to appear in the Top-N Report.
    - To remove a secondary column, highlight a column header and click **Delete**.

    Note:

    Use the up or down arrows to move up or down the list of available column headers.
13. Click **Finish**.

Configuring the Event Listing reportlet

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Event Listing** icon onto the canvas outlined on the report work area.
4. In the Name field, enter a name for the event listing.
5. Click **Choose a Scope**.

   The Choose a Scope page appears.
6. Select one or more scopes from the available list, and click **OK**.

   Note:

   You can use the Search field to search for a scope.
7. The Columns sections displays the columns headers to appear in the report.
   - To add a new column, click **Add**, and from the list, select an item to appear in the report.
   - To delete a column, highlight the item, and click **Delete**.

   Note:

   Use the up or down arrows to move up or down the list of available column headers.

8. Click **Finish**.

Configuring the Pie Chart reportlet

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the Pie Chart icon onto the canvas outlined on the report work area.
4. In the **Name** field, enter a name.
5. In the Items section, click **Add**.
6. Select a perspective.
7. From perspective list, select an element.

   If you select Scopes, from the available list, select a scope name, and then check individual elements or check the scope name to include all elements. Scopes that exceed undefined elements are not shown.
8. Click **Next**.
9. To add another item, repeat steps 4 to 6.
   - To delete an item, highlight the item, and click **Delete**.
   - To edit an item, highlight the item, and click **Edit**.
   - To move up the list of items, click the up arrow.
   - To move down the list of items, click the down arrow.
10. In the Pie variables section, click **Add**.
11. Select variables that are supported by the items.
    - You can use the Search variable field to search for a specific variable.
    - To see all variables, check **Include variables for this type of element**.

    After you select a variable, the system displays the variable name in the Variable title field.
12. To add another pie variable, repeat steps 9 to 15.

    Note:

    To complete the Pie Chart, you must select a minimum of two variables and the variables must be of the same type.

    - To delete a pie variable, highlight the item, and click **Delete**.
    - To edit a pie variable, highlight the item, and click **Edit**.

- To move up the list of pie variables, click the up arrow.
- To move down the list of pie variables, click the down arrow.

13. Click **Finish**.

Configuring the Element Status reportlet

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Element Status** icon onto the canvas outlined on the report work area.
4. In the **Name** field, enter a name.
5. In the Items section, click **Add**.
6. In the Perspective field, click the down arrow to select a perspective, and then select an element.
   - If you select the perspective Scopes, select an element, and then check individual elements, or scope name to include all scopes. Only the first 100 scopes are shown.
7. Click **Next**.
8. To add the show reachability status column to the report, select **Show reachability status column**.
9. The Secondary columns section displays additional columns to appear on the report.
   - To remove a column, click **Delete**.
   - To add a column, click **Add**.

   Note:

   Use the up or down arrows to move up or down the list of available column headers.
10. To view variables, in the Show variables section, click **Add**, and search for a variable.
    - To search all variables for this type of element, check **Include variables for this type of element**.
11. Select a variable. You can edit the name in the Variable title field.
12. Click **Next**.
13. Repeat steps 8 to 10 to add additional variables.
14. If the items are correct, click **Finish**.
    - To add another item, click **Add**.

- To delete an item, click **Delete**.
- To edit an item, click **Edit**.

Configuring the Event Summary reportlet

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Event Summary** icon onto the canvas outlined on the report work area.
4. In the Name field, enter a name.
5. In the Event bar scale field, enter a number between 1 and 10000.

   Note:

   The Event bar scale is for the histogram bar. For example, is you enter 100 as scale and there are 10 events, then the bar is 1/10 of the available length. If you choose 1000 then the bar shrinks.
6. In the Items section, click **Add**.
7. Click **Choose a Scope**

   The Choose a Scope page appears.
8. Select the one or more scopes from the available list, and click **OK**.

   Note:

   You can use the Search field to search for a scope.
9. From the Configure Event Summary dialog box, select one or more Events.
10. In the Item Title field, enter the item title.
11. To accept your changes and go to the next step of the configuration wizard, click **Next** .
    - Or, to discard your changes and return to the previous step of the dashboard wizard, click **Prev**.
12. To add another item, repeat step 4 to step 9.
13. Click **Finish**.

Configuring the Dial Gauge reportlet

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Dial Gauge** icon onto the canvas outlined on the report work area.
4. In the **Perspective** field, click the down arrow and select a perspective from the available list.
5. From the folders or icons that appear in the box, navigate to the element you require. Click the plus signs at the left to expand the folders.
6. Click **Next**.
7. Click the **Choose a variable** field, and select a variable.

   You can use the Search variable field to locate a variable.

   - To view all variables, select **Include all variables for this type of elelment**. If there is no data available, the dial gauge does not display any value.
   - To show thresholds, select **Show thresholds**.
8. Edit the Variable label.
9. In the Select units field, click on the down arrow to select a units field.
10. In the **Minimum** field, enter a value.

    The minimum value shows the lowest label in the dial gauge scale.
11. In the **Maximum** field, enter a value.

    The maximum value shows the highest label in the dial gauge scale.

    Important:

    The system displays the values for intermediate labels based on the values you enter for minimum and maximum labels. Intermediate labels are at fifth values between minimum and maximum. Ensure you configure minimum and maximum values to have integer intermediate labels.
12. In the Color zones field, click on the down arrow to select a value.

    The colors green, yellow, and red appear on the dial gauge based on the following configurations.

    - none — indicates no color zones.
    - 1 — indicates one color zone. You can select a color. The from and to fields are preselected from start to end.
    - 2 — indicates two color zones. You can select a color for zone 1 and zone 2, and select the end location for zone 1 or the start location for zone 2.
    - 3 — indicates three color zones. You can select a color for zone 1, 2 and 3, and then enter a value in an available from or to field.

Important:

The zone to value must be more than the minimum range value. The zone from value must be less than the maximum value. If you enter incorrect zone values, the system displays a message indicating the value requirements.

13. To add another variable, click **Next**, and repeat step 7 to step 11.
14. Click **Finish**.

Configuring the Trend Chart reportlet

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Trend Chart** icon onto the canvas outlined on the report work area.
4. In the **Perspective** field, click the down arrow to select a perspective.
5. From the folders that appear in the box, navigate to the element you require.
   - If you select the Scope perspective, select an element and then check single elements or scope name to include all elements. The system displays the first 100 elements only.
6. Click **Next**.
7. To select an additional perspective, click **Add** and repeat steps 2 to 4.
8. Click **Next**.
9. In the **Time Selection Mode** field, select
   - **Interval** to configure a span of time without restrictions. Select an **End Time** (current or a time in the past) and **Period** (how long the interval should be).
   - **Calendar Unit** to configure a specific unit that always begins and ends at the boundary of the unit. Select a **Period** for the calendar unit.
10. Check the blue text at the bottom of the dialog box to make sure you entered the correct time range.
11. Click **Next**.
12. In the Right axis variable field, click ***No variable selected*** to view all variables for which sufficient data has been collected to display in the report.
    - Check the box for **Include all variables for this type of element** to view all variables, including variables with no data collected.
    - To show thresholds, select **Show thresholds**.
13. Select a variable.

14. In the Left axis variable (optional) field, select a variable if required.
15. To change the y-axis scale for the graph to show the trend plotting over a larger y-axis, check **Autorange**.
16. To view averages of the trend over an x-axis, check **Averaging Mode**.
17. In the Number of averaging intervals field, enter a value.

    The Number of averaging intervals calculates the averages for the x-axis. The number of the average intervals must be a minimum of 2. For example, if 6 is selected as the number of average intervals and if 10 minutes is the polling period, then the values is averaged over one hour.
18. Enter a name for the report.
19. Click **Finish**.

Configuring the Event History reportlet

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Event History** icon onto the canvas outlined in the report work area.
4. Enter a name for the filter.
5. Select:
   - **Last** to specify an interval integer and the units: seconds, minutes, hours, days, or weeks
   - **Between** to filter records between two specific timestamps. Select the timestamps.
6. To filter records by the event name, click **Select value** and select an event name. Click **OK**.
7. To filter records by the subject name, click **Select value** and select a subject name. Click **OK**.
8. To filter records by an event trigger, click **Triggers** and select a trigger. Click **OK**.
9. To filter records by Product ID, enter the product ID.
10. Click **Next**.

    The Columns configuration section appears.
11. The Columns sections displays the columns headers to appear in the report.
    - To add a new column, click **Add**, and from the list, select an item to appear in the report.
    - To delete a column, highlight the item, and click **Delete**.

Note:

Use the up or down arrows to move up or down the list of available column headers.

12. Click **Finish**.

Configuring the Inventory Table reportlet

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the monitoring reports configuration reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Inventory Table** icon onto the canvas outlined on the report work area.
4. In the **Perspective** field, click the down arrow to select a perspective.
5. Select a scope that you want to appear in the report.

   To locate a specific scope, enter the name of the scope in the search field.
6. From the available fields, select column headers to appear in the report.

   To customize a header, enter a name in the **or custom expression** field.
7. Click the arrow to move your selection to the Columns section.
8. In the Columns section, click the down arrow to select a variable to apply to the field name.
9. Click **Next**.
10. Enter the number of rows you want in the report.
11. Enter the number of rows allowed for export.
12. In the Columns section, click on a field name.
13. **(Optional)** In the Details section, perform the following actions:
    a. In the **Display As** field, enter the name that you want the field to appear as.
    b. **(Optional)** Select **Batch by this column**.
    c. Select **Use custom formatting**, and click the down arrow to select a custom format.
14. Click **Finish**.

Configuring the History Table reportlet

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.

2. To view the monitoring reports configuration reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **History Table** icon onto the canvas outlined on the report work area.
4. In the **Perspective** field, click the down arrow to select a perspective from the available list.
5. Select the scopes that you want to appear in the report.

   To locate a specific scope, enter the name of the scope in the search field.
6. Click **Next**.
7. From the Available fields, select the Simple Columns headers to appear in the report.

   To customize a header, enter a name in the **or custom expression** field.
8. Click the arrow to move your selection to the Columns section.
9. Click **Next**.
10. From the Available fields, select the Aggregated Columns to appear in the report.

    To customize a header, enter a name in the custom expression field.
11. Click the arrow to move your selection to the Aggregated columns section.
12. In the Aggregated columns section, click the down arrow to select an aggregation value for each field.
13. Click **Next**.
14. In the **Time Selection Mode** field, select one of the following:
    - **Interval** to configure a span of time without restrictions. Select an **End Time** (current or a time in the past) and **Period** (how long the interval should be).
    - **Calendar Unit** to configure a specific unit that always begins and ends at the boundary of the unit. Select a **Period** for the calendar unit.
15. Use the down arrow to select the history data on variable(s).
    - All from AtmEvent
    - Atm Vcl Admin Status
    - Atm Vcl Oper Status
16. Check the blue text at the bottom of the dialog box to make sure you entered the correct time range.
17. Click **Next**.
18. Select one of the following time groupings:
    - Basic time groups
    - Week-based time groups
19. Click the arrow to move your selection to the Time columns section.

20. Click **Next**.
21. Enter the number of rows you want in the report.
22. Enter the number of rows allowed for export.
23. In the Columns section, click on a field name.
24. In the Details section, perform the following actions:
    a. In the **Display As** field, enter the name that you want the field to appear as.
    b. **(Optional)** Select **Batch by this column**.
    c. **(Optional)** Select **Use custom formatting**, and click the down arrow to select a custom format.
25. For each field in the Columns section, repeat steps 20 to 21.
26. In the Aggregated columns section, click on a field name.
27. In the Details section, perform the following actions:
    a. Click the down arrow to select an aggregation value.
    b. In the **Display As** field, enter a name.
    c. To show a select number of top elements per table, click the check box, and enter a value.
    d. Click **Use custom formatting**, and click the down arrow to select a custom format.
28. For each field in the Aggregated columns section, repeat steps 23 to 24.
29. Click **Finish**.

Configuring the Hypercube Table reportlet

About this task

For assistance on configuring the Hypercube Table reportlet, contact Extreme Networks support at http://www.extremenetworks.com/support.

Before you begin

You must create a new monitoring report or edit an existing customized monitoring report.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the monitoring reports configuration reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Drag and drop the **Hypercube Table** icon onto the canvas outlined on the report work area.
4. In the **Perspective** field, click the down arrow to select a perspective from the available list.
5. Select the scope that you want to appear in the report.

   To locate a specific scope, enter the name of the scope in the search field.

6. Click **Next**.
7. From the Available fields, select the Simple Column headers to appear in the report.

   To customize a header, enter a name in the custom expression field.
8. Click the arrow to move your selection to the Columns section.
9. Click **Next**.
10. From the Available fields, select the Aggregated Columns to appear in the report.

    To customize a header, enter a name in the custom expression field.
11. Click the arrow to move your selection to the Aggregated columns section.
12. In the Aggregated columns section, click the down arrow, and the select an aggregation value for each field.
13. Click **Next**.
14. In the **Time Selection Mode** field, select one of the following time modes:
    - **Current** to configure the time span to the current time.
    - **Interval** to configure a span of time without restrictions. Select an **End Time** (current or a time in the past), and **Period** (how long the interval should be). Use the down arrow to select the history data on variable(s).
    - **Calendar Unit** to configure a specific unit that always begins and ends at the boundary of the unit. Select a **Period** for the calendar unit. Use the down arrow to select the history data on variable(s).
15. Check the blue text at the bottom of the dialog box to make sure you entered the correct time range.
16. Click **Next**.
17. Select one of the following time groupings:
    - Basic time groups
    - Week-based time groups
18. Click the arrow to move your selection to the Time columns section.
19. Click **Next**.
20. Enter the number of rows you want in the report.
21. Enter the number of rows allowed for export.
22. In the Columns section, click on a field name.
23. In the Details section, perform the following actions:
    a. In the **Display As** field, enter the name that you want the field to appear as.
    b. **(Optional)** Select **Batch by this column**.
    c. **(Optional)** Select **Use custom formatting**, and click the down arrow to select a custom format.

24. For each field in the Columns section, repeat steps 22 to 23.
25. In the Aggregated columns section, click on a field name.
26. In the Details section, perform the following actions:
    a. Click the down arrow to select an aggregation value.
    b. In the **Display As** field, enter a name.
    c. To show a select number of top elements per table, click the check box, and enter a value.
    d. **(Optional)** Click **Use custom formatting**, and then click the down arrow to select a custom format.
27. For each field in the Aggregated columns section, repeat steps 25 to 26.
28. Click **Finish**.

Refreshing reports

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. Click **Refresh**.

Adding a report to favorites

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. From the left navigation pane, select the monitoring report that you want to make a favorite.
3. Click **Add to favorites** to add the report to favorites.

Adding a new monitoring report

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. To view the reportlets, click the down arrow located at the top of the Monitoring Reports page.
3. Click **New report**.

   You can also use an existing report as the basis for a new report. Open the existing report and click **Save report as**.

4. In the dialog box, enter the report name.
5. To permit other users to view your changes, select **Public**.
6. Click **OK**.
7. Drag and drop a reportlet onto the work area.

   A configuration dialog box specific to the reportlet you selected appears. This is the beginning of the monitoring report wizard.
8. Enter information in the configuration dialog box.
9. Click **Save report**.

Variable definitions

The following table lists the Monitoring Reports configuration buttons.

Icons	Variable	Definition
	Text	Lets you configure the text to add to a custom monitoring report.
	Image	Lets you add and configure an image for a custom monitoring report.
	Availability Report	Displays the average availability for a class of elements as percentages over intervals of hour, day, month, or year. To view a transient report for the element, on the Availability Report, click on the element name.
	Top-N Report	Top-N Reports are based on Scope and Time, and show histograms of devices and interface statistics. Top-N Reports are available for a current time or for a past time period.
	Event Listing	Provides you with the events information of devices or interfaces, and can contain a maximum of 100 events. You can select the events for any specific domain, or all domains. To open another transient report, on the Event Listing report, select Ack and click on the subject of the event.
	Pie Chart	Provides a set of one or more percentage pie charts. Pie charts need at least two variables and all variables must be of the same type.
	Element Status	Displays the KHI status of the element, including %CPU, %Memory, and number of alerts on the element. To open a transient report for the element, click the element name on the Element Status report.

Table continues…

Icons	Variable	Definition
	Event Summary	Displays the summary of events by either domain classification or by concern.
	Dial Gauge	Provides a set of one or more dial gauges, each displaying the value of a domain element variable on an analog dial. All of the dial gauges in one set must display variables from the same domain element.
	Trend Chart	Provides performance trend improvements and trending of device resource usage, and key health indicators. Reporting is made easy by selecting trends and exporting information to PDF.
	Event History	To create event history reports for specific events.
	Inventory Table	To create reports to show multi-dimensional grouping and presentation of the inventory data.
	History Table	To create reports to show multi-dimensional grouping and presentation of the historical data.
	Hypercube Table	To create complex reports with multi-dimension grouping. Because of the complexity of the Hypercube table, contact customer support for additional information.

Deleting a monitoring report

About this task

You cannot delete built-in monitoring reports.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. From the left navigation pane, select the monitoring report that you want to delete.
3. Click **Delete Report**.
4. In the confirmation dialog box, click **OK**.

Saving a report

Procedure

1. Select **Reports** > **Monitoring Reports**.

2. From the left navigation pane, select the monitoring report that you want to save.
3. Click **Save report**.

Saving a report with a new name

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. From the left navigation pane, select the monitoring report that you want to edit.
3. Click **Save report as**.
4. Update the name in the **Report Name** field.
5. Click **OK**.

Editing a monitoring report

About this task

You cannot edit built-in reports.

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. From the left navigation pane, select the monitoring report that you want to edit.
3. Click **Edit report** to open the Edit report dialog box where you can change the report name, subfolder, and the privacy settings. Click **OK**.
4. To edit the configuration of the report, click the Configuration icon on the top right corner of the reportlet.
5. Edit the settings as required and click **Finish**.
6. Repeat for any other reportlets that you want to edit on the monitoring report.
7. Click **Save report**.

Exporting a monitoring report

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. From the left navigation pane, select the monitoring report that you want to export to PDF.
3. Click **Export to PDF**.
4. Configure the print settings.

5. Click **Export to PDF**.

Searching Monitoring Reports

Procedure

1. Select **Reports** > **Monitoring Reports**.
2. On the left of the Monitoring Reports pane, under the Search banner, enter the information or search term for which you want to search
3. Click **Enter**.

Chapter 10: Events information

Events conceptual information

Use the following information to understand Events information on the system under **Network** > **Events**.

Events tab

You can view messages for events in the network that you manage using the Events tab.

The Events tab interprets the faults across the network and displays the interpretation. The interpretation is refined, diagnosed, analyzed, and researched on the basis of every event.

To access the Events tab, select **Network** > **Events**.

For information about the Events tab procedures, see Viewing Events on page 158.

The Events tab displays message boards, one message board per tab. A tab represents an automatic grouping of an event. Each message board can show messages for events taking place in the domains managed by the product. The Events tab contains a single message board by default, but you can create additional message boards as needed. You can configure individual message boards to provide different views of message activity by changing the filters applied, or by sorting or hiding columns.

By default, a message board displays messages for all domains loaded on the server. However, you can filter message boards to achieve various display results that, for example, correspond to a specific scope, set of event types, or match specific criteria such as priority or event type.

Important:

Taking an action against a message affects the message in all the message boards in which the message appears. For example, clearing a message clears the message from all message boards. Event persistence depends on the event type and associated MITs.

Some events do not persist on a server restart or monitoring restart, primarily Self Event, IP AvailabilityFailure, and SNMPAgentFailure. The engine will re-evaluate and post these events if required.

You can control the messages on the message board by using the controls provided on the menu bar of the Event Browser page.

The following table describes the controls available to manage the messages on the Event Browser page:

Controls	Description
Add a new message board	Adds a message board.
Delete selected message board	Deletes the current board (second icon from the left).
Rename selected message board	Renames the current board.
Configure filter for selected message board	Displays message board filter options. Each message board can have its own filter.
Auto refresh	Allows you to specify the time interval at which message board information is refreshed. After you click Auto refresh, a window appears that allows you to select the appropriate refresh interval. If the auto refresh settings are different from the message board settings then they affect the entire Event Browser.
Refresh	Refreshes the message board. Refresh is not only for a single message board, the refresh affects the entire Event Browser.
Export selected message board	Allows you to export the contents of the current message board as an XML file (with the applied filter). Exports the current message board and not the entire Event Browser content.
Message board operation	Allows you to acknowledge, unacknowledge, annotate, or clear all information on the message board.
Dispose transient message boards	Disposes of transient message boards.
Group by:	Specifies how to group events. You can select the following: • None • Ack. • Pri. • Source Address • Target Address • Annotated • Device • Correlation • Event Name • Information Available • Sub. • Domain

Table continues…

Controls	Description
	• Subject • Received • Rep. Count • Summary • Last Updated

Fault correlation

Monitoring correlates network faults to events in the **Network** > **Evemts** tab and displays a color-coded priority of the faults. If an error occurs on a network device nested within a multi-layer design in the Network Topology, the color coding for that error is replicated on all layers.

Valid color coding includes the following:

- Red (critical)
- Dark Orange (high)
- Orange (medium)
- Yellow (low)
- Turquoise (warning)
- Green (information)

The following diagnostic tools are available on the client browser for troubleshooting:

- Traps, syslogs and the polling of MIBs to monitor faults
- Monitoring with defaults you can use out of the box
- Tools to troubleshoot are available on the client browser
- CLI and special scripts if you have an Advanced License
- Availability events on all devices and applications
- POS diagnostics

Message detail

The Message Detail window shows the complete set of information pertaining to a received message.

First go to **Network** > **Events**. You can view the Message Detail window by performing either one of the following:

- Double-clicking on a message
- Right-clicking on the message row, and then selecting the Message Detail

The following table describes the Message Detail window tabs.

Feature	Description
Messages tab	Displays information about the basic event message, the event type description, and the annotations for any actions or responses that are executed. The Messages tab provides the message text, the date when the message was last updated, the event name, the event ID associated with the message, event description, and advice.
Attributes tab	Displays the sourceAddress and the SubjectAddress. The sourceAddress, specifies the IP address where the trap has originated. The SubjectAddress specifies the device IP that generated the trap.
Annotations tab	Displays annotations that are associated with the message. You can add an annotation by clicking **Add**.
Related Messages tab	Displays a list of downstream events (subsequent messages related to the message of interest) and upstream events (preceding messages related to the message of interest). These lists identify the priority, correlation, event type, and other relevant information about the related messages. There are two mini-message boards that show the associated events.
Monitoring Details tab	Displays the domain name, agent name, and configuration, as well as the poll period of the monitoring.

Message properties

A message board, in the **Network** > **Events** tab, lists messages in rows with the columns representing the properties of the messages.

The following are the various properties for each message as shown in the message board.

Message Properties	Description
Ack (Acknowledged)	A check mark indicates that the message is acknowledged. No check mark indicates the message is not acknowledged.
Pri (Priority)	The integer corresponding to the priority of the event. All priorities are selected by default. The Initial event priority is configured in the monitored information types Configuration Editor. Valid priorities include the following: • Red (critical) • Dark Orange (high) • Orange (medium) • Yellow (low) • Turquoise (warning) and • Green (information)
Annotations (pencil icon)	The presence of an annotation is indicated by a pencil icon in this column. Click the pencil icon and

Table continues…

Message Properties	Description
	the Message Detail box appears. Browse to the annotation tab. Click Annotation to add annotation to the message. The product annotates a message when the product executes an action in response to an event, when a message is acknowledged, or when a message is unacknowledged. You can add notes to the messages by right-clicking a row, and then selecting Annotate. You can also add an annotation from the Annotation tab.
Related messages (I icon)	The I icon indicates if another message is associated with the current one. For example, two messages that are correlated are considered to be related. Related messages are listed in the Message Detail window.
Correlation	The name of correlated messages applied to a message. A plus sign (+) appears in this column when related events for the message exist. When the plus sign (+) sign is clicked the system shows related events, which are also shown in the message detail dialog box. This only appears while a fault is active.
Event Name	The name of the event type.
Sub. (Sub-message count)	An integer count of other events in (correlated under) the line item.
Subject	The subject associated with the event.
Device	The name of the device from which the event originates if you select a device in the topology view and select Show events from the menu. The device is always listed as Monitoring for events about Monitoring.
Summary	A summary of the event.
Received	The date and time of the first repetition of this event (to see the time of most recent repetition, you can view the details of the message).
Rep. (Repetition) Count	The number of times the message is posted. Messages are not received directly from source devices but are inferred by the Knowledge Base Manager engine from a variety of sources and situations.

Message filters

You access the filters panel by clicking the Filters icon in the top right toolbar of the **Network** > **Events** tab.

You can configure each message board in the Events tab to show different message information. By default, a message board displays messages for all domains that are loaded on the server. Using this panel, you can filter each message board so that, among other things, the message board shows only those messages that correspond to a specific scope, set of event types, or by criteria such as priority or network.

The Monitoring retains your changes with other preferences you have set for your user account.

The following table describes the various types of filters you can apply to the messages on the message board.

Message Properties	Description
Priorities	Allows you to turn on or off viewing of each priority by selecting or deselecting the appropriate check boxes. The colors correspond to the following priority levels: • Red (critical) • Dark Orange (high) • Orange (medium) • Yellow (low) • Turquoise (warning) • Green (information)
Updated after	Allows you to only show events updated after a specified time.
Updated before	Allows you to only show events updated before a specified time.
Hide acknowledged	Allows you to show or hide acknowledged events (check box).
Do not apply to subsuming (e.g. causing) events	Allows you to not apply the filter to subsuming events.
IP filter pattern	Allows you to specify a filter pattern based on the IP address.
Scopes	Allows you to show only events whose subject is a member of the selected scope.
Events	Allows you to show only events that are one of the set of checked events.

Viewing Events

When traps are received from network devices, they can be turned into events. The Event Browser allows you to monitor, acknowledge, and filter network events. Use the following procedures to customize the information displayed in the Event Browser.

Adding a message board

By default the Event Browser contains a single message board. You can create multiple message boards.

Use this procedure to add multiple message boards.

Procedure

1. Select **Network** > **Events**.
2. On the Event Browser page, click **Add a new message board** by clicking the plus sign on the top left toolbar.
3. Enter a name in the **Enter a name for the new board** field.
4. Select **Public** or **Private**.
5. Click **OK**. The new message board appears as a new tab in the **Event Browser**.

Deleting a message board

About this task

Perform the following procedure to delete a message board.

Procedure

1. Select **Network** > **Events**.
2. Select a message board.
3. Click **Delete selected message board**.
4. In the Confirm dialog box, click **OK**.

Renaming a message board

Procedure

1. Select **Network** > **Events**.
2. Select a message board.
3. Click **Rename selected message board**.

4. In the Prompt dialog box, enter a new name for the selected message board.
5. Click **OK**.

Sorting messages

Sort messages on the message board by performing this procedure.

Procedure

1. Select **Network** > **Events**.
2. On the Event Browser message board, click the arrow on one of the column headings.
3. The system displays a list showing the Sort Ascending, Sort Descending, and Columns options.
4. Select **Sort Ascending** or **Sort Descending** to sort the messages in ascending or descending order.

Filtering messages

By default, a message board does not use filters. The message board displays all messages (regardless of attributes such as priority, scope, or context) for all domains that are loaded on the server.

Filter allows you to customize the display of the messages for a message board. You can filter individual message boards to show the messages that corresponds to a specific scope, set of event types, priority, network, or other criteria.

Important:

Filtering messages does not delete the messages that are not displayed. Filtering only omits messages not matching filter criteria from the set of messages appearing in the current message board.

The system provides a variety of methods for controlling message board content that allow you to configure powerful filters that allow only events meeting specific criteria. These include:

- Filtering by message priority
- Filtering before or after a specific time
- Filtering by acknowledgement status
- Filtering by scope or event type
- Filtering by IP

Clear the selected message option before filtering.

Filtering messages by priority

Use the following procedure to filter messages by priority.

Procedure

1. Select **Network** > **Events**.
2. Before filtering message, click the **Clear selected message** option, which is the X on the toolbar.
3. On the Event Browser page, click **Configure filter for selected message board**, located at the top of the message board.
4. From the Msgs Board Filters window, select or clear the Priorities check box to display or filter the messages. You can select the color priority you want to display.
5. Click **OK**.

Variable definitions

Variable	Definition
Red	Displays the critical priority messages.
Dark Orange	Displays the high priority messages.
Orange	Displays the medium priority messages.
Yellow	Displays the low priority messages.
Turquoise	Displays the warning messages.
Green	Displays the information messages.

Filtering messages by scope or event type

Use the following procedure to filter messages by scope or event type.

Procedure

1. Select **Network** > **Events**.
2. Before filtering message, click the **Clear selected message** option, which is the X on the toolbar.
3. On the Event Browser page, click **Configure filter for selected message board**, located at the top of the message board.
4. Click the **Scopes** box and expand the scopes tree to locate the scopes you want to include in the display.
5. Select the nodes you want to include in the message display.
6. Expand the Event Types tree to locate the event types you want to include in the display. Toggle the selection to include the event type or exclude the event type from the display.
7. Click **OK**.
8. Click **OK** again.

Result

The Event Selection Tree consists of items that you can expand or close. Each item also has a box that can display one of three control state,s and can display one of many informational states.

To cycle through the three control states, left-click three times on the box or label. The control states are explicit inclusion, explicit exclusion, or inherit from parent. The control state is visually indicated by the border of the box: thick green for explicit inclusion; thick red for explicit exclusion; thin of varying color for inherit from parent.

Filtering messages by acknowledged status

Use the following procedure to filter messages by acknowledged status.

Procedure

1. Select **Network** > **Events**.
2. Before filtering message, click the **Clear selected message** option, which is the X on the toolbar.
3. On the Event Browser page, click **Configure filter for selected message board**, located at the top of the message board.
4. Select the **Hide Acknowledged** box to hide acknowledged events.
5. Click **OK**.

Filtering messages by IP

Procedure

1. Select **Network** > **Events**.
2. Before filtering message, click the **Clear selected message** option, which is the X on the toolbar.
3. On the Event Browser page, click **Configure filter for selected message board**, located at the top of the message board.
4. Select the **IP filter pattern** check box.
5. In the field directly below the **IP filter pattern** box, enter the IP address or range of IP addresses to filter for.
6. Click **OK**.

Suppressing PoE Under-Current warnings

If Monitoring detects a particular value after you poll a MIB value on a device, a PoE Under-Current warning appears on the Event Browser. After the value returns to an acceptable value, Monitoring automatically clears the PoE Under-Current warning.

To prevent the PoE Under-Current warning from appearing on the Event Browser, you can configure the filter on your Event Browser.

About this task

Perform the following procedure to suppress the PoE Under-Current Warning.

Procedure

1. Select **Network** > **Events**.

2. On the Event Browser page, click **Configure filter for selected message board**, located at the top of the message board.
3. From the Msgs Board Filters dialog box, select **Event** > **Physical Event** > **Environmental Event** > **Power Event** > **Power Ethernet Event** > **Power Ethernet Port Event**.
4. Deselect **Power Ethernet Port Under-Current Warning**.
5. Click **OK**.

Note:

The system continues to monitor the device and posts the PoE Under-Current event. However, the PoE Under-Current Warning does not appear on the Event Browser.

Viewing OTM error codes

OTM error codes are error codes from Avaya CS 1000. Error codes are made up of alphabets and numbers (for example, ERR0017) that map to a description of the error.

About this task

You can view error code details and descriptions from the Avaya CS 1000 by performing the following procedure.

Procedure

1. Select **Network** > **Traps**.
2. In the **Error Code** column, click on the required error code.

   A window appears with the details of the error code.

Exporting a message board

You can export a message board and save the contents.

Procedure

1. Select **Network** > **Events**.
2. From the Event Browser page, select the tab corresponding to the message board you want to export.
3. Click the **Export selected message board** button. An xml file opens in your browser with the contents of your exported message board.
4. Save this file to an appropriate location on your hard drive.

Performing a multicolumn sorting

Use the following procedure to perform a multicolumn sorting for a table.

Procedure

1. Press the Shift key while you click the column headers in the table.
2. Hover the mouse over a column header, and click the down arrow.
3. Select **Sort Ascending** or **Sort Descending**.

Undoing a multicolumn sorting

Perform the following procedure to undo a multicolumn sorting.

Procedure

Click on any column header.

Note:

After you click on the column header, you also enable the sorting for that column.

Chapter 11: Event History information

Event History

To access the Event History, select **Network** > **Event History**. On the Event History page, you can view one or more tabs with each tab corresponding to a filter.

The Event History keeps track of every event that occurs, based on the notifications received from the network. Since these events may have been cleared from the Event Browser, you can use the Event History to view cleared events. The Event History displays individual events; therefore, multiple events that the system correlates into a single event on the Event Browser display as individual events on the Event History page.

The following general controls are available on the Event History page:

- New Filter—Creates a new tab with a new filter.
- Create filter from selection—Creates a new tab with a new filter that is preset from current row values.
- Clone Filter—Creates a copy of the currently selected filter.
- Rename Filter—Renames the currently selected filter.
- Edit Filter—Edits the currently selected filter.
- Delete Filter—Deletes the currently selected filter.
- Purge Configuration—Purges the configuration. To save disk space and remove event history records automatically, use the purge configuration settings. You can specify the maximum age in hours, days, or weeks. Alternately, you can specify the maximum number of records to keep. The most recent event history set by these configurations are retained, and the rest are purged.
- Refresh—Refreshes the data on the current or active filter.

Viewing Event History

Viewing the Event History

Procedure

1. Select **Network** > **Event History**.
2. On the Event History page, view the toolbar located on the top of the page.

   The page has seven buttons: New Filter, Create Filter from selection, Clone Filter, Rename Filter, Edit Filter, Delete Filter, and Refresh.
3. Click the **Refresh** icon to refresh the data on the active tab.
4. The table displays the rows matching the filter. The columns correspond to the user-friendly columns in the events table.

Adding a filter in Event History

Procedure

1. Select **Network** > **Event History**.
2. On the Event History page, click the **New Filter** icon.
3. Enter a name for the filter that appears as the label for the tab.
4. Select the Last option to filter by age of the record.

   The interval integer and the units specified can be seconds, hours, days, or weeks.
5. Select the Between option to filter the records between two specific timestamps.
6. Select the Event name to filter by the event name.
7. Select the Subject name (event subject) to filter by the subject name.
8. Select the Domain name to filter by the domain name.
9. Select Triggers to filter by the event trigger.
10. Enter a product ID to filter by product ID.
11. Select **Search only** to specify a number of records to search.
12. Click **OK**.

    The new Filter appears as a new tab in the Event History.

Variable definitions

The following table describes the information in the New filter window for **Network** > **Event History**.

Variable	Value
Filter	Specifies the name of the filter that appears as the label for the tab.
Last	Specifies an interval integer and the units: Seconds, Minutes, Hours, Days, or Weeks.
Between	Filters records between two specific timestamps.
Event Name	Filters records by the event name.
Subject Name	Filters records by the subject name.
Domain name	Filters records by the domain name.
Triggers	Filters records by the event triggers.
Product ID	Filters records by product ID.
Search Only	Enables the user to configure the number of records to search.

Creating a filter from selection in the Event History

Perform the following procedure to create a filter from selection in the Event History Browser.

Procedure

1. Select **Network** > **Event History**.
2. On the Event History page, click on the row which you want to be the selection for the new tab.
3. Click on the **Create Filter from selection** icon from the left toolbar.
4. In the filter field, enter a new name for the cloned filter. If required, you can also edit the other fields in the new filter dialog box.
5. Click **OK**.

Cloning a filter in the Event History

Procedure

1. Select **Network** > **Event History**.
2. On the Event History page, select the filter you want to clone.
3. From the Event History menu bar, click on the **Clone Filter** icon from the top left toolbar.
4. In the Filter field, enter a new name for the cloned filter.
   - If required, you can edit the other fields in the New Filter dialog box.
5. Click **OK**.

Renaming a filter in the Event History

Procedure

1. Select **Network** > **Event History**.
2. On the On the Event History page, select the filter you want to rename.
3. From the Event History menu bar, click on the **Rename Filter** icon from the top left toolbar.

   Prompt dialog box appears.
4. Enter the new name.
5. Click **OK**.

Deleting a filter in the Event History

Procedure

1. Select **Network** > **Event History**.
2. On the Event History page, select the filter you want to delete.
3. From the Event History menu bar, click the **Delete Filter** icon from the top left toolbar.

   A dialog box appears to confirm deletion.
4. Click **OK** to confirm the deletion.

Editing a filter in the Event History

Procedure

1. Select **Network** > **Event History**.
2. On the Event History page, select the filter you want to edit.
3. Click the **Edit Filter** icon from the top left toolbar.

   The Filter Editor dialog box appears.
4. Edit the settings as required.
5. Click **OK** to save the changes.

Configuring purge settings

Configure purge settings for the event history. Monitoring automatically purges the event history according to these settings. For example, the event history can be purged at regular time intervals, by the number of records, or by the age of records.

Procedure

1. Select **Network** > **Event History**.
2. Click the **Purge Configuration** icon from the top left toolbar.
3. Set the values for maximum age and maximum records for the purge to execute.

   Purging occurs at a fixed period by either or both maximum number of records and maximum age of records.
4. To perform an immediate purge, select **Purge Now**.
5. Click **OK**.

   Monitoring executes purge periodically. Purge records are not retrievable by Monitoring.

Refreshing the Event History

Procedure

1. Select **Network** > **Event History**.
2. On the Event History page, click the **Refresh** icon.

   The Event History page is refreshed. Also when the user changes from one tab to another, the filter is refreshed automatically.

Chapter 12: Traps and syslog information

Traps and syslogs

Monitoring supports the use of SNMP traps and syslogs to monitor managed devices in your network. Traps and syslogs are unsolicited, automatic notifications sent by a network object after being triggered by a network event, based on the SNMP MIB-II standard.

To view traps and syslogs, from the menu bar, select **Network** > **Traps** and **Network** > **Syslogs**.

Traps and syslogs can be viewed in the Trap Viewer and Syslog Viewer. Generate traps internally by Monitoring or externally by network objects. If you have defined an MIT for a trap, the information becomes an event displayed in the Events tab. If an event already exists for a given trap, the event count increments by one every time Monitoring receives a trap.

Traps turn into events and display in the Event Browser for debugging and troubleshooting. Monitoring for domain is turned on automatically. For monitoring devices, you must manually turn on some monitoring features, with other monitoring features turned on by default.

Tip:

If you see traps in the traps and syslogs browsers but no corresponding event, go to the Network Monitoring Details and check if monitoring is turned on. If certain traps are not being seen as events, go to Monitored Information Types and check if the event MIT corresponding to the trap exists. For certain toggle kind of traps, one trap clears another. Therefore, for such traps, only one event MIT exists while the other trap is not correlated into an event, but instead, is used to clear another event.

You must configure network objects individually to send traps and syslogs. Do this on the devices themselves. Devices must have SNMP enabled, they must have the IP address of the Monitoring server, and the listening port of the Monitoring configured (the default is 162 for traps, and 512 for syslogs). For information on configuring your network devices to send traps, consult the documentation for your device.

Tip:

If you do not see any traps coming from a device and you know that the device is sending traps, go to the device icon on the Network browser and from the Applications menu select Tools, and launch the HTTP connection. Next, from the HTTP window, check that the Monitoring server IP address is registered as a trap receiver.

Certain events, such as IPAvailability Failure will disappear from the Event Browser if you restart the server or Monitoring. Monitoring automatically evaluates and re-posts these as required.

Certain other events, such as an MLT/SMLT configuration warning, can appear the first time you run the discovery. These are warning messages alerting the operator about possible MLT/SMLT configuration problems. For example, a warning can appear if a port configured as an SMLT port is not connected to anything. Check if this is a real problem, and if it is not, delete the warning from the event browser.

Trap Viewer and Syslog Viewer general controls

On the Trap Viewer and Syslog Viewer pages, you can view information SNMP traps and syslog reports. You can also configure how you view the traps and syslogs.

To access the Trap Viewer, click **Network** > **Traps**. To access the Syslog Viewer, click **Network** > **Syslogs**.

The following general controls are available on the Trap Viewer and Syslog Viewer pages.

- Filter—Filters the traps based on the time traps in the system.
- Autorefresh—Enables you to specify the time interval at which trap information refreshes. Click Autorefresh to display a popup window to select the appropriate refresh interval.
- Refresh—Refreshes the table.
- Export records—Enables you to export traps records as an .xml document.
- Settings—Enables you to specify traps configuration that control how the system stores trap information and removes trap information from the database, as well as what view filters and forwarding destinations are in effect.
- Show/Hide Stats—Displays statistics including the date and time of the last server restart, packets per second, packets received, and status.

You can configure Syslog and Traps settings in the Preferences section. Click on the icon in the upper right corner of the menu bar to select **Preferences**, then select **Monitoring**, and a window displays for Syslog Settings and Traps Settings.

In the Syslog Settings and Traps Settings, you can configure maximum age, maximum number, configure a limit to discovered devices, configure the listener port, archive depth, archive directory and forwarding.

Traps Viewer

The Trap Viewer table under **Network** > **Traps** displays a list of traps that have been issued in the network. The following columns display in the trap table:

- Address—Filters traps based on the IP address of the device from which it was sent. Wildcards are accepted.
- OID—IFilters traps based on the object ID of the trap.
- Time—Filters the displayed traps based on the time received. (For example, last day or last minute).

- Version—Filters traps based on the SNMP version of the trap.
- Generic—Filters traps based on a predefined, generic trap class (for example, coldStart, warmStart, linkUp, linkDown).
- Specific—Filters displayed traps based on the specific trap.
- Acked—Filters the displayed traps based on their Acknowledgement Status (Acked or Not Acked).
- Trap Name-—Filters based on the trap name.
- Bindings—Filters based on bindings. The number of object IDs (OID) associated with the trap.
- Error Code—Filters based on the error code such as the error code for commonMIBAlarm from Avaya CS 1000. The error code is mapped to the error description. To display the error description, click on the error code value. A window appears with a description of the error code.

The following image is an example of an error code description.

Syslogs Viewer

The communication protocol for traps supports specification of original source address. This is not true for Syslogs. The subject address cannot be reliably parsed from a syslog message because of the different formats in use.

The Syslog tab, under **Network** > **Syslogs**, displays a table of syslogs for your network. The following columns display in the syslogs table:

- Server Time—Filters based on server time, which is the time the Monitoring server received the syslog.
- Address—Filters syslogs based on the IP address of the device from which it was sent.
- Facility—Filters syslogs based on the facility that generated the syslog: kernel, user, mail, uucp, or clock.
- Severity—Filters syslogs based on severity: emergency, alert, critical, error, warning, notice informational, or debug.

- Text—Filters syslogs based on specified text contained within the syslog.
- Acked—Filters the displayed syslogs based on their Acknowledgement Status (Acked or Not Acked).

Trap and Syslog configuration

Configuring Traps settings

You can configure how trap information is organized and displayed. Use the following procedure to configure the Trap Viewer.

You can also configure the trap settings through the Settings icon on the Traps page.

Procedure

1. From the quick access toolbar on the top right, select **Preferences**.
2. Click **Monitoring** from the left hand navigation pane.
3. On the Monitoring Preferences page, perform the following tasks in the Trap Settings section:
   - Set the **Maximum age**.
   - Enter the **Maximum number**.
   - Set the **Limit to disc. devices** to true or false.
   - Set the **Limit to auth. devices** to true or false.
   - Enter the **Archive depth**.
   - Enter the **Listener port**.
   - Enter the **Archive directory** field information.
   - Enter the **Forwarding** field information.
4. Click **Apply** to save the changes.

Viewing traps

View traps on the system, and configure the Trap Viewer filters.

Procedure

1. Select **Network** > **Traps** to view trap information.
2. From the Traps page, select **Filter**.

   The Traps Viewer Filters dialog box appears.

3. Configure the filters you want to use to display the trap information.
4. Click **Update**.

Variable definitions

The following table displays the options in the Traps Viewer Filters menu.

Variable	Value
IP	Filters based on IP address.
OID	Filters based on Object Identifier of the trap.
Interval	Filters the displayed traps based on the time received.
Generic	Filters traps based on predefined, generic trap class (for example, coldStart,28 warmStart, linkUp, linkDown)
Specific	Filters based on the specific trap.
SNMP Version	Filters based on the SNMP version of the trap.
Ack	Filters based on the acknowledged status of the trap (acknowledged or not acknowledged).

Configuring Syslog settings

You can configure how syslog information is organized and displayed. Use the following procedure to configure the Syslog Viewer.

You can also configure the syslog settings through the Settings icon on the Syslogs page.

Procedure

1. From the quick access toolbar on the top right, select **Preferences**.
2. Click **Monitoring** from the left hand navigation pane.
3. On the Monitoring Preferences page, perform the following tasks in the Syslog Settings section:
   - Set the **Maximum age**.
   - Enter the **Maximum number**.
   - Set the **Limit to disc. devices** to true or false.
   - Enter the **Listener port**.
   - Enter the **Archive depth**.
   - Enter information in the **Archive directory** field.
   - Enter information in the **Forwarding** section.
4. Click **Apply** to save the changes.

Viewing syslogs

View syslogs on the system, and configure filters.

Procedure

1. Select **Network** > **Syslogs** to view syslogs.
2. From the Syslogs page, select **Filter**.
3. Configure the filters you want to use to display the syslog information.
4. Click **Update**.

Variable Definitions

Use the following information to filter Syslog information.

Variable	Definition
IP	Filters based on the IP address.
Facility	Filters based on the facility. You can choose from the following: • ANY • kernal • user • mail • system_daemons • sec_auth_1 • syslog_internal • line_printer • network_news • uucp • clock • sec_auth_2 • ftp • ntp • log_audit • log_alert • clock_daemon • local_use_0 • local_use_1

Table continues…

Variable	Definition
	• local_use_2 • local_use_3 • local_use_4 • local_use_5 • local_use_6 • local_use_7
Severity	Filters based on the severity of the syslog. You can choose from the following: • ANY • emergency • alert • critical • error • warning • notice • informational • debug
Text	Filters based on text. Enter the text for which you want to filter.
Interval	Filters based on a time interval. You can choose from the following: • Last minute • Last five minutes • Last 10 minutes • Last hour • Last day • Last week • Last month • Last year • Range
Ack	Filters by the following: • ANY • Not Ack’ed—Filters by not acknowledged. • Ack’ed—Filters by acknowledge.

Chapter 13: Diagnostic tools

Diagnostic tools

Use the following diagnostic tools to troubleshoot the system.

Diagnostic tools

You can use the Network Topology to access diagnostic tools such as ping and route trace. To access the diagnostic tools, go to **Network** > **Topology**, right-click on a device in the Topology Viewer and select **Diagnose**.

The diagnostic tools are:

- MIB Query—Opens a new page to query MIBs.
- MIB Browse—Opens the MIB Browser page and displays the MIB Object properties.
- ICMP Ping—After you select a device icon, the IP address appears in the target; if required, you can change the IP address to another IP address. The responses appear in the top area of the window.
- Trace Route—Prompts you for the Destination device, and computes all static routes between Target and Destination.
- SNMP Get—The target IP is queried with the selected SNMP version, community string, Auth Protocol and Privacy Protocol. If required, you can change the information in these fields.
- Remote Ping—Permits you to remote ping between devices.
- Remote Traceroute—Permits you to trace route between two devices.

MIB Query

To access MIB query, select **Tools** > **MIB Query**.

You can view information about MIB queries by expanding the tree structure on the left side of the MIB Query page and selecting a query.

The MIB query information appears in the Results panel.

The following controls are available on the MIB Query page:

- Clear—Clears the query results.
- Execute—Starts the MIB query. Click the checkbox.
- Period—Displays the time period for the MIB query.
- Target—Displays an SNMP MIB based on an IP address.
- SNMP Version—Sets the SNMP authentication.
- Options—Adjusts the timeout value and retries.
- Switch to columns—Displays the results using columns.

From the queries panel, you can perform the following actions:

- Add—Adds a query.
- Delete—Deletes a query.
- Edit—Edits a query.

SNMPv3 authentication

The SNMPv3 authentication permits the user to enter MD5 or SHA as protocols for authentication, and then select the privacy encryption keys of DES, 3DES, or AES128. The user also enters the authentication and privacy passwords. The MIB Query uses these credentials to query the target machine.

1. To access SNMPv3 authentication, go to **Tools** > **MIB Query**.
2. Select the **SNMP version** icon along the toolbar that displays the current SNMP version.
3. Update the parameters you want to change.
4. Click **OK**.

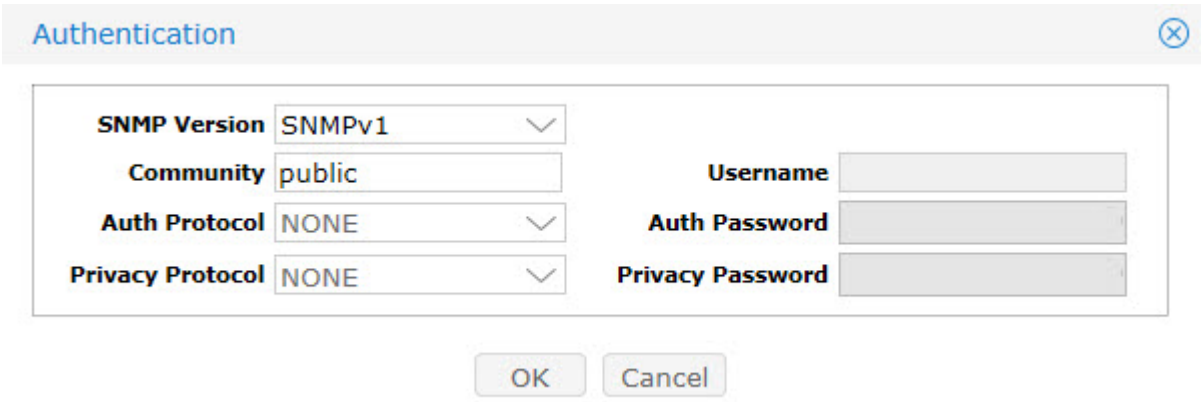


Figure 5: SNMPv3 Authentication screen

MIB Browser

To access the MIB Browser, select **Tools** > **MIB Browser**.

You can view information about MIBs in two ways.

- You can expand the tree structure on the left side of the MIB Browser window and select a MIB.
- In the OID field, you can enter the OID of a MIB.

The SNMP MIB information appears in the right panel of the window.

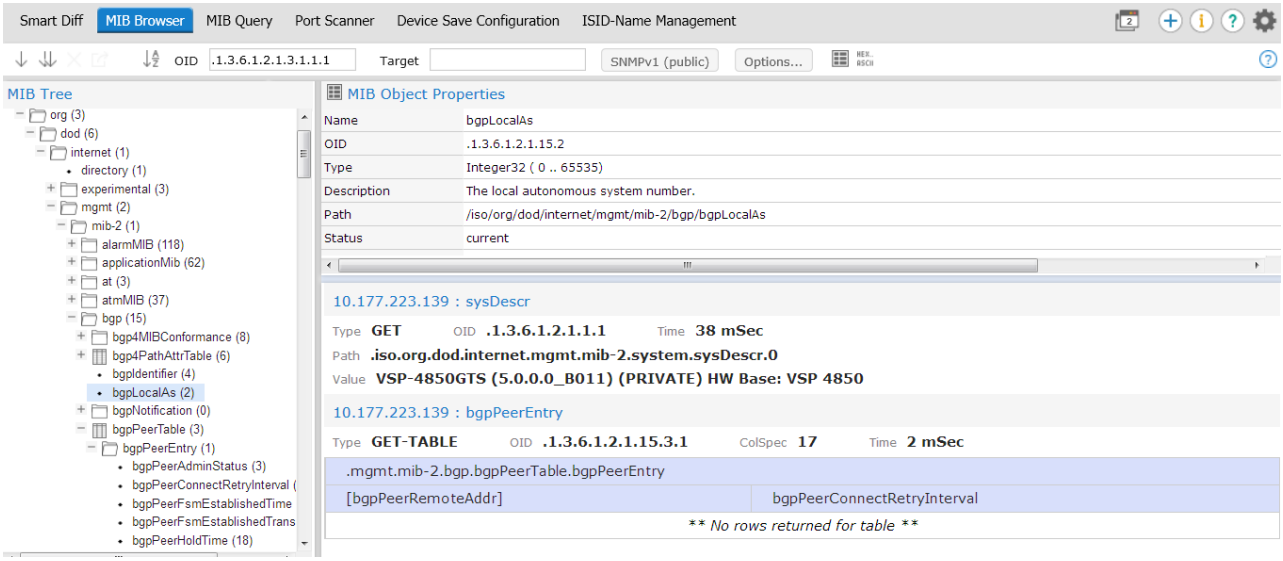


Figure 6: MIB Browser

The following controls are available on the MIB Browser page:

- Get—Retrieves the output for a selected MIB. To select the Get action, from the navigation tree, right-click on a node, and click **Get**.
- Get Next—Retrieves the output for the next MIB.
- Clear results area—Clears the results of any present queries.
- Export—Export the information.
- Refresh—Refresh the information.
- Enable alphabetical mode or Enable ID mode—Expands the navigation tree in alphabetical mode or ID mode.
- OID—Specifies the object text-based identifier for the MIB.
- Target—Displays an SNMP MIB based on an IP address.
- SNMP Version—Sest the SNMP authentication.

- Options—Adjusts the timeout value and retries.
- Show Properties—Displays the properties table for the MIB.
- Trace on—Specifies the trace.

Figure 7: MIB Browser toolbar

Diagnostic tools procedures

Use the following information to understand the diagnostic tools available on the system.

Pinging a device

Use this procedure to test connectivity to a device.

Procedure

1. Select **Network** > **Topology**.

   The Network Topology page displays.

2. In the Topology Viewer in the middle of the panel, select a device. If your network diagram is large, you may wish to filter the devices shown by selecting a perspective from the Perspective drop-down menu.
3. Right-click on the device, and select **Diagnose**.
4. Select **ICMP Ping**.

Tracing a route

Use the following procedure to perform a route trace.

Procedure

1. Select **Network** > **Topology**.

   The Network Topology page displays.

2. In the Topology Viewer in the middle of the panel, select a device. If your network diagram is large, you may wish to filter the devices shown by selecting a perspective from the Perspective drop-down menu.
3. Right-click on the device, and select **Diagnose**.
4. Select **Trace Route**.

SNMP Get

Use the following procedure to access the Diagnostic tools window provides multiple diagnostic functions, including SNMP Get.

Procedure

1. Select **Network** > **Topology**.
2. Right-click on the required device icon from the contents pane.
3. Select **Diagnose** > **SNMP Get**.

Remote pinging between phones

Use the following procedure to remote ping between phones.

This option is available for Avaya CS 1000 phones only.

Procedure

1. Select **Network** > **Topology**.
2. In Perspective field, select **Device Types**, and then expand the tree to locate **Phones**.
3. In the tree, expand the **Phones** list, and then click twice on the required phone to view details of the selected phone in the topology view.
4. In the topology view, right-click on the phone, and then select **Diagnose** > **Remote Ping**.

   A window appears requesting that you select the remote device to ping from the phone.
5. Select the device to ping.

   The system displays the results of the ping in a new window.
6. Click **OK**.

Remote trace route between phones

Remote trace route between phones is an extension of the trace route feature. You can trace route between two phones by selecting, on the phone, Diagnose and Remote trace route. After you make your selection, a window appears prompting you to enter the required information on the device or phone to which you want to trace route.

Remote path tracing between phones

Use the following procedure to perform a remote path trace between phones.

This option is available for Avaya CS 1000 phones only.

Procedure

1. Select **Network** > **Topology**.
2. In Perspective field, select **Device Types**, and expand the tree to locate **Phones**.
3. In the tree, expand the **Phones** list and right click on the required phone to view details of the selected phone.

   The selected phone and connected network devices appear in the topology view.
4. In the topology view, right click on the phone and select **Diagnose** > **Remote Traceroute**.

   A window appears requesting that you select the remote device to ping from the phone.
5. Select the device to ping.

   The results of the ping appear in a new window.
6. Click **OK**.

Managing hardware inventory

You can view and manage the inventory for campus devices, interfaces, and physical elements.

Use the following procedure to manage the hardware assets in your network.

Procedure

1. Select **Network** > **Topology**.

   The Network Topology page displays.
2. In the Topology Viewer in the middle of the panel, select a device. If your network diagram is large, you may wish to filter the devices shown by selecting a perspective from the Perspective drop-down menu.
3. Right-click on a device, and select **Tables** > **Physical Elements** to view information about the physical elements such as fans and chassis associated with the selected device.

Exporting an inventory

Perform the following procedure to export an inventory as a CSV or PDF file.

Before you begin

Select an inventory by performing Managing hardware inventory on page 181.

Procedure

1. Select **Network** > **Topology**.
2. In the content panel in the middle, select **Export** from the toolbar in the middle.
3. In the Export to format section, select **CSV** or **PDF**.

4. In the Scope section, select **Export current page** or **Export all data**.
5. Click **OK**.
6. Save to your chosen location.

Monitoring device level trends

Monitoring provides trending of device resource usage and key health indicators and allows you to view performance trends of network objects. You can view multi-graph trends in a single chart for comparisons, and add a second variable. Charts show auto-ranging on both axis, popup plot values, and average, minimum and maximum bars. You can select time and date ranges, and view a trend in real time from the last hour to up to one year. Monitoring remembers the last time scale and auto ranging changes. Available trends are context sensitive, depending on the selected device.

Important:

- Trends are shown for only those variables for which sufficient data has been collected.
- For the trends menu to be visible, monitoring must be turned on for the domain and device.
- Trends of routers, switches, servers and other managed objects are available based on MIB instrumentation.

Trend charts have the following controls available:

- Interval—The interval (number and unit) displayed on the x-axis of the chart.
- Past/Current Time—If this option is selected, you can select from a drop down of either past or current time.
- Export—Exports the trend data to PDF or XML.
- Refresh—Refreshes the current trend chart.
- Add—Adds a graph in a plot.
- Delete—Deletes a graph in a plot.
- Autorange—Changes the y-axis scale for the graph so that the trend plotting shows over a larger y-axis scale.
- Averaging Mode—Displays averages of the trend over an x-axis.
- Number of averaging intervals—The value used to calculate the averages for the x-axis. The number of average intervals must be a minimum of 2. For example, if you select 6 as the number of average intervals and if 10 minutes is the polling period, then the values are averaged over one hour. You can enter a value only after you enable Averaging mode.

Performance trending

Use the following procedure to view a performance trending chart.

Before you begin

- You must configure a monitoring agent and enable monitoring. For more information, Monitoring configuration on page 121.
- Trending information is only available after MITs are created.

Procedure

1. Select **Network** > **Topology**.

   The Network Topology page appears.
2. In the Topology Viewer in the middle of the panel, select a device. If your network diagram is large, you may wish to filter the devices shown by selecting a perspective from the Perspective drop-down menu.
3. Right-click on the device, and select **Trends**.
4. Select the Trend Chart that you want to view.

Viewing network paths

Perform this procedure to view the network paths between any two points in the network.

Procedure

1. Select **Network** > **Topology**.

   The Network Topology page appears.
2. Locate the device or interface you want to find the path between two points.
3. Right-click the device or interface icon, and select **Schematics** > **Show Paths**.

   The Select path endpoint dialog box appears.
4. From the Select path endpoint dialog box, find and select the other end-point (device or interface).
5. Click **OK**.

   A schematic showing all the paths between the two end-points is displayed.

SPBM diagnose tools

The following SPBM diagnose tools are available:

- L2 Ping

- L2 Traceroute
- Unicast Path
- Multicast Path

Viewing results of a SPBM L2 Ping

Perform the following procedure to view the results of a SPBM L2 Ping.

Before you begin

Before you perform a SPBM diagnostic tool function, you must enter the write community strings at discovery time for the SPB enabled devices.

Procedure

1. Select **Network** > **Topology**.
2. In perspective field, in the top left above the tree browser, select **SPBM View**.
3. From the SPBM View navigation tree, highlight a folder, and then select **Show SPBM Area Schematic**.
   - To hide the Message Board at the bottom of the screen, from the Network Topology tool bar, click **Hide events**.
   - To hide the Property table on the right hand side of the screen, from the Network Topology tool bar, click **Hide property table**.
4. In the Topology Viewer in the middle of the panel, select two devices. To select two devices, click on one device, and then press the shift key and click on another device.
5. Right-click on one device, and select **SPBM Diagnose Tools** > **L2 Ping**.

   Note:

   If a Notice dialog box appears, click **OK**, ensure you select two devices, and then perform step 5.
6. Select a VLAN.
7. Click **Ok**.

   A waiting for results window appears, and then the results appear for the L2 ping for the device.
8. To close the window, click **X**.

Viewing results of a SPBM L2 Traceroute

Perform the following procedure to view results of a SPBM L2 Traceroute.

Before you begin

Before you perform a SPBM diagnostic tool function, you must enter the write community strings at discovery time for the SPB enabled devices.

Procedure

1. Select **Network** > **Topology**.
2. In perspective field, in the toolbar on the top left above the tree browser, select **SPBM View**.
3. From the SPBM View navigation tree, highlight a folder, and then select **Show SPBM Area Schematic**.
   - To hide the Message Board at the bottom of the screen, from the Network Topology tool bar, click **Hide events**.
   - To hide the Property table on the right hand side of the screen, from the Network Topology tool bar, click **Hide property table**.
4. In the Topology Viewer in the middle of the panel, select two devices. To select two devices, click on one device, and then press the shift key and click on another device.
5. Right-click on one device, and select **SPBM Diagnose Tools** > **L2 Traceroute**.

   Note:

   If a Notice dialog box appears, click **OK**, ensure you select two devices, and then perform step 5.
6. Select a VLAN.
7. Click **Ok**.

   A waiting for results window appears, and then the results appear for the L2 Traceroute trace for the device.
8. To close the window, click **X**.

Viewing a SPBM Unicast Path

Perform the following procedure to view a SPBM Unicast Path.

Before you begin

Before you perform a SPBM diagnostic tool function, you must configure the device SSH or Telnet credentials in the Device and Server Credentials Editor available from **Administration** > **Credentials**.

Procedure

1. Select **Network** > **Topology**.
2. In Perspective field, select **SPBM View**.

3. From the SPBM View navigation tree, highlight a folder, and then select **Show SPBM Area Schematic**.
   - To hide the Message Board at the bottom of the screen, from the Network Topology tool bar, click **Hide events**.
   - To hide the Property table on the right hand side of the screen, from theNetwork Topology tool bar, click **Hide property table**.
4. In the Topology Viewer in the middle of the panel, select two devices. To select two devices, click on one device, and then press the shift key and click on another device.
5. Right click on one device, and select **SPBM Diagnose Tools** > **Unicast Path**.

   Note:

   If a Notice dialog box appears, click **OK**, ensure you select two devices, and then perform step 5.
6. Select a VLAN.
7. Click **Ok**.

   Monitoring identifies the unicast path on the topology.

Highlighting a SPBM Multicast Path

Perform the following procedure to highlight a SPBM Multicast Path.

Before you begin

Before you perform a SPBM diagnostic tool function, you must configure the device SSH or Telnet credentials in the Device and Server Credentials Editor available from **Administration** > **Credentials**.

Procedure

1. Select **Network** > **Topology**.
2. In perspective field, in the top left toolbar above the tree browser, select **SPBM View**.
3. From the SPBM View navigation tree, highlight a folder, and then select **Show SPBM Area Schematic**.
   - To hide the Message Board at the bottom of the screen, from the Network Topology tool bar, click **Hide events**.
   - To hide the Property table on the right hand side of the screen, from the Network Topology tool bar, click **Hide property table**.
4. In the Topology Viewer in the middle of the panel, click on one device.
5. Right click on the device, and select **SPBM Diagnose Tools** > **Multicast Path**.
6. Select a VLAN.
7. Select an ISID.

8. Click **Ok**.

   Monitoring highlights the multicast path on the topology.

   - To clear the highlights of the multicast path, click on the background.

MIB query tools

Monitoring offers the following tools to query MIB IOD:

- MIB Browser
- MIB Query

The following sections provide information about the MIB query tools.

MIB Browser

The following sections provide information about using MIB Browser.

Modifying SNMP version authentication

You can customize SNMP authentication for MIBs.

Procedure

1. Select **Tools** > **MIB Browser**.
2. From the list of MIBs in the left pane, select the MIB for which you want to view the information.
3. Click the SNMP version button next to the Target field.
4. In the Authentication dialog box, modify the appropriate fields based on the SNMP version.
5. Click **OK**.

Variable definitions

The following table describes the fields in the Authentication window for SNMP.

Variable	Value
SNMP Version	The SNMP version for the authentication.
Community	The SNMP community for the authentication: SNMPv1, SNMPv2c, or SNMPv3. If SNMPv1 or SNMPv2c, then only the community string needs to be specified. If SNMPv3, then authorization and privacy can be used for additional security.
Auth Protocol	The encryption algorithm to be used: none, MD5, or SHA. (SNPMv3 only)
Privacy Protocol	The encryption algorithm to be used: none, DES 3DES, or AES128. (SNPMv3 only)

Table continues…

Variable	Value
Username	The user name for the authentication. (SNPMv3 only)
Auth Password	An encrypted password for gaining access to the device. (SNPMv3 only)
Privacy Password	A password used to decrypt data sent to and returned from the device. (SNPMv3 only)

Viewing SNMP MIB data

You can do an SNMP MIB query on the MIBs in your system using the MIB Browser.

Procedure

1. Select **Tools** > **MIB Browser**.
2. In the **Target** field, type the IP address for the MIB you want to view.
3. From the list of MIBs in left pane, select the MIB for which you want to view the information.

   OR

   In the **OID** field, type the object identifier for the MIB you want to view.
4. Select SNMP version v1, v2c, or v3. If you choose v3, enter the authentication variables as shown in the preceding variable definitions table.
5. Click the **Get** button to retrieve the output for the MIB.

   The information appears in the right panel.
6. If you want to see the next MIB in the list, click the **Get next** button.
7. If you want to clear the MIB information from the results area, click the **Clear results area** button.
8. If you want to save the MIB information, click the **Save last query results** button.

MIB queries

This section provides information about using the MIB query tools.

Performing an SNMP MIB Query

You can use the MIB Query menu option to query MIB OID.

The MIB Query has predefined queries for commonly used tables such as Arp Cache, Cisco CDP, Interface Entries, Interface Status, and Join of IP Address and Interface. You can add your own commonly used queries by clicking on + or cloning a predefined query and changing the query.

Note:

You can use the Queries tool bar on the left to add a query, delete a query, or edit a query.

- Add—add user defined queries

- Delete—delete a user defined query
- Edit—edit a query

Use the **Options** button, along the top tool bar, to adjust the timeout value and retries.

Procedure

1. Select **Tools** > **MIB Query**.
2. Enter the IP address of the device in the **Target** field.
3. To receive periodic query responses, enter an amount (in seconds) in the **Period** box. To do so, first check the check box before **Period**.
4. Click **SNMPv1(public)**, and select the SNMP version.
5. From the left hand pane, select a predefined or user defined query, and click the **Execute** button (arrow button) to collect data from the target.

   The results of the query appear in tabular form in the right hand pane.

   Use the **Switch to columns/rows** button, along the top tool bar, to change the display of the results to columns or rows.

Adding a query

Perform the following procedure to add a query.

Procedure

1. Select **Tools** > **MIB Query**.
2. From the Queries tool bar on the left, click **Add**.

   The SNMP MIB Query Editor appears.
3. In the Query Name field, enter a name.
4. Click **Apply**.

Deleting a query

Perform the following procedure to delete a query.

Procedure

1. Select **Tools** > **MIB Query**.
2. In the Queries pane, select a query.
3. From the Queries tool bar, click **Delete**.
4. Click **OK**.

Editing a query

Perform the following procedure to edit a query.

Procedure

1. Select **Tools** > **MIB Query**.
2. From the Queries pane, select a query.
3. From the Queries tool bar, click **Edit**.

   The SNMP MIB Query Editor appears.
4. Edit the query.
5. Click **Apply**.

Variable definitions

Variable	Definition
Query Name	Specifies the name assigned to the query.
Binding Source	Specifies the field to use for joining two MIB tables.
Joined to	Joins two MIB tables.
Prefix	Specifies the SNMP OID prefix to a table.
Field	Specifies the individual variables in a MIB table. For example, ipNetToMediaNetAddress or ipNetToMediaPhyAddress in the ipNetToMedia table.

Chapter 14: MIT information

MIT conceptual information

Use the following information to understand MIT information on the system under **Network** > **MIT**.

MIT

A Monitored Information Type (MIT) is any data that Monitoring is capable of monitoring and using to assist in the process of managing your network environment. Most MITs are events, but MITs could also include statistics and raw data. The MITs Configuration Editor is an administrative tool that provides access to the network data that Monitoring is capable of monitoring and using to assist in the process of managing your network. You can configure MITs to control event behavior and message board behavior.

You must have an Advanced License to use MIT.

To configure MIT, select **Network** > **MIT**.

The following general controls are available on the Monitoring Information Types page:

- Enable/Disable alphabetical mode—Toggles between hierarchical and alphabetical views of MITs.
- Refresh—Refreshes the list of MITs.
- Search—Enables you to perform a search of MITs.

The monitored information type (MIT) list is a set of event types built into Monitoring that characterizes most typical events and statistics encountered by administrators and other users. The MIT hierarchy view is organized as a tree. An information type that has sub-types can be expanded by clicking on the "+" to the left of its name to show the sub-types. The Monitoring MIT hierarchy supports multiple inheritance so you often see the same MIT in several places within the tree. Occurrences of MITs are listed in three ways:

- Monitored Information by Form—Organizes the MITs according to what they are (such as data, event, and statistic).
- Monitored Information by Management Standard—Organizes MITs according to a specific management standard such as SNMP. For example, the MITs that are specific to SNMP have further subtypes based on different MIBs, and the system groups the events depending on which MIB they are derived.

- Monitored Information by Subject—Organizes MITs according to what the MITs affect (such as device). For example, you find InterfaceUtilizationProblem under both OverUtilizationProblem, which is a sub-event type of PerformanceProblem, and under InterfaceEvent.
- Monitored Information Deprecated—Organizes MITs according to deprecated events or statistics.

Monitoring provides self events that includes information about changes to the server configuration and other state changes in server processing. You implement self events using a new domain element type, SelfElement, and a new set of monitoring variables, Self Events.

For a complete list of Self Events expand the tree view to a category named Self Event, located under Monitored Information, **By Subject** > **Self Information** > **Self Event**. Expand the items under Self Event to see all of the events that are provided. You can modify parameters for these events and create overrides just like any other monitored information type item. You can use Self Elements for message board filtering to only display self events. You can also configure responses to self events. You must create Actions that are connected to self events as server based actions.

Each monitored information type has a description and a set of configurable parameters associated with the MIT. An MIT sub-type inherits its parameters and the default value for each from its parent event types, taking the value from the first if more than one parent exists with the same parameter.

Often, an MIT has a predefined override value for a parameter that the MIT inherited from a parent information type. For example, Event defines the initialPriority parameter to have a value of 6 (least important) but AvailabilityProblem contains a built-in override for initialPriority to be 4.

MIT search

You can quickly locate MIT definitions using the search functionality. Go to **Network** > **MIT**.

The MIT search box is located in the upper left corner of the MIT panel. To use the search box, type the term you are searching for in the Search box. As you type, the list of MIT definitions is dynamically refreshed to show only those MIT definitions that match the search term you have typed.

Note the following when performing MIT searches:

- Searches are not case sensitive.
- The MIT definitions that are displayed are those that start with the search term you type.
- To find definitions that contain a search term, type the wildcard character (*) before or within the search text.

The following examples illustrate the search behavior:

Search 1

Search term: Act

Search Results: Action Failure and Active Availability Monitoring Change

Search 2

Search term: softw

Search Results: Software Availability Failure, Software Event, Software Information, Software Performance Problem, Software Statistic, and Software Terminated Event

Search 3

Search term: act*fa

Search Results: Action Failure

MIT configuration

Configuring Monitored Information Types

You can modify the parameters of the Monitored Information Types (MIT).

Procedure

1. Select **Network** > **MIT**.
2. To view the information in the navigation tree in alphabetical order, click **Enable alphabetical mode**. To view the information in the navigation tree in the hierarchical mode, click **Disable alphabetical mode**.
3. Expand the monitored information type tree if in hierarchical view or scan the list of entries if in alphabetical view to locate the MIT you want to view.
4. Select the MIT.

   The description and parameters for the MIT display in the right panel.
5. Click the link in the underlined word to change the parameters.

   An Enter value window appears.
6. Change the required parameters.

   You can also use the default values.
7. Click **Apply** to save the values.

   OR

   Click **Revert** to close the window without applying the changes.

Variable definitions

The following table describes the options under **Network** > **MIT**.

Parameters	Description
Description	A brief explanation of the monitored information type.
Parameters	A text-based description of the monitored information type parameter settings. Clicking on a value link displays a window enabling you to configure the parameter.

Viewing Monitored Information Types

You can view the descriptions and parameters associated with Monitored Information Types (MIT).

Procedure

1. Select **Network** > **MIT**.
2. To view the information in the navigation tree in alphabetical order, click **Enable alphabetical mode**. To view the information in the hierarchical mode, click **Disable alphabetical mode**.
3. Expand the monitored information type tree if in hierarchical view or scan the list of entries if in alphabetical view to locate the MIT you want to view.
4. Select the MIT.

   The description and parameters for the MIT display in the right panel of the MITs Configuration window.

Variable definitions

The following table describes the options under **Network** > **MIT**.

Parameters	Description
Description	A brief explanation of the monitored information type.
Parameters	A text-based description of the monitored information type parameter settings. Clicking on a value link displays a window enabling you to configure the parameter.

Chapter 15: Automating configuration tasks

Automation of configuration tasks conceptual information

Use the following information to understand the automation of configuration tasks on the system.

Actions

Actions are commands that you can execute through the user interface interactively by selecting a domain element and initiating the command or automatically using a predefined response or action schedule. Monitoring supports a number of different action types.

The only action available with a Base License is email; all other actions require an Advanced License.

Monitoring provides actions triggered by the following events:

- Generate email to network administrator.
- Generate text / SMS messages using email.
- Run rediscovery based on events.
- Run server side scripts.
- Launch EM.
- Run Remote Monitoring Script as plug in on KHI threshold.

Monitoring provides the following templates for scripting and mail:

- RMS scripts that are wizard driven for ease of use.
- Email templates with variable building blocks.

For more information about writing custom scripts for Monitoring actions, or obtaining a development kit for Monitoring API, contact customer support.

The following controls are available in the top left toolbar under **Network** > **Actions**.

- Apply your changes—Applies changes. All edits to actions are client-side only. Select Apply to save the edits to the server.
- Discard changes, reverting back to the previous values—Discards changes. Unapplied edits to an action can be undone by selecting Revert. No confirmation is offered and unapplied edits are immediately lost.

- Add a new action—Creates a new action. The available actions depend on the selected group.
- Delete selected action—Deletes an existing action.
- Rename selected action—Enables you to rename an existing action.
- Clone selected action—Duplicates an existing action.
- Execute now selected action—Executes the action.
- Refresh—Refreshes the actions list.

Action types

The following actions are available in Monitoring if you have an Advanced License:

- Command Action - executes a command script using languages such as DOS Batch, SH, BASH, CSH or TCSH.
- Email Action sends an email message from a specified user account to one or more recipients.
- SNMPv2 Notification initiates an SNMPv2 notification.
- Rediscovery Action initiates a domain rediscovery.
- Config Control Action generates a configuration control response.
- Campus Rediscovery Action enables you to automate a campus rediscovery. Use this action in Responses to rediscover a campus triggered by a user-specified event.
- Web Browser Action enables you to establish a connection to a specified URL using a web browser.

There are two types of actions: Server-based actions and web browser actions.

Server-based actions are actions that are executed from the Monitoring server. You must configure these actions to be triggered by a response or a schedule.

Web browser actions are actions that are executed from the client browser and are therefore affected by the browser settings. These actions are triggered by a menu that displays when you right-click a device in the Network Topology.

Server-Based Actions

Server-based actions are always dispatched for execution to the server process. The following built-in server-based actions are included:

- EmailAction—Provides a sample email action.
- NewEmailAction—Provides a new email sample action.
- Phone Disconnect Email—Provides a sample email for phone disconnect.
- Rediscover Campus—Automates the rediscovery of a campus. You must have the Advanced License to use this action.

- Rediscover Device—Automates the rediscovery of a device. You must have the Advanced License to use this action.
- Rediscover Device of Application—Automates the rediscovery of a device of the application. You must have the Advanced License to use this action.
- Rediscover Domain—Automates the rediscovery of a domain. You must have the Advanced License to use this action.
- SampleCS1000EmailAction—Provides a sample email action for Avaya CS 1000. SampleCS1000EmailAction is similar to SampleEmailAction but customized for Avaya CS 1000, and required for the OTM replacement feature.
- SampleEmailAction—Provides a sample email action.
- Show containing scopes— You must have the Advanced License to use this action.
- Supervision Inherit—Inherits supervision settings from a higher level in the domain element class hierarchy. You must have the Advanced License to use this action.
- Supervision Off—Initiates an action to turn off monitoring for a domain element, and stops all trend data collection and event correlation. You can schedule the Supervision Off action to turn off supervision of network elements during a planned shutdown. You must have the Advanced License to use this action.
- Supervision On—Initiates an action to turn on monitoring for a domain element, and starts all trend data collection and event correlation. You can schedule the Supervision On action to turn the supervision of network elements back on after a planned shutdown. You must have the Advanced License to use this action.

Web Browser Actions

A Web Browser Actions allows you to establish a connection to a specified URL using a web browser.

If you have an Advanced License, you can use any of the following Web Browser Actions:

- FTP Connect
- HTTP Connect
- HTTPS Connect
- Launch ACCCM
- Launch ACR
- Launch AMS
- Launch ANAV
- Launch CC Elite
- Launch CMS
- Launch EM
- Launch EMC Unisphere

- Launch Hardware Manager
- Launch SALGW
- Launch SBC EMS
- Launch Secure EM
- Launch SLAmon
- Launch Telnet
- Launch WebLM
- SSH Connect
- VMware vCenter

Contextual Information in Action Configurations

By specifying contextual information in your action configurations, you can make your action behavior and content automatically adapt at execution time to the event and or domain element associated with the particular execution of the action.

You can specify this kind of contextual information in your action configurations by inserting expressions as follows:

A ${event.type} has been ${trigger} on ${device.address}

This might appear in the inbox of a user as:

A FanWarning has been acknowledged on 172.16.67.23

You can sometimes just use an identifier directly when the identifier has a simple value such as ${trigger}, and at other times when the identifier is an object, you must specify a property such as ${event.type}. Sometimes the property of an object is another object in which case you must chain your dot notation as in ${device.campus.location}.

The properties defined for an identifier (if any) vary depending on the type of the identifier.

For ease of adding contextual variable information, Monitoring prompts the completion of the valid variables in the context. For example, after typing "${device.", Monitoring displays a menu of available property variables.

Event responses

An event response is an action or set of actions that executes automatically as a result of one or more events occurring. To access event responses, go to: **Network** > **Responses**.

The following controls are available at the top of the Responses window:

- Apply your changes—Applies your changes. All edits to responses are client-side only. Select Apply to save the edits to the server.

- Discard changes, reverting to the previous values—Discards your changes. Unapplied edits to a response can be undone by selecting the Revert button. No confirmation is offered, and unapplied edits are immediately lost.
- Add a new response—Adds a new response.
- Delete selected response—Deletes an existing response.
- Rename selected response—Enables you to rename an existing response.
- Clone selected response—Duplicates an existing response.
- Refresh—Refreshes the responses list.

Note:

Continuous action and response triggers can occur if you select an action failure self event trigger when creating a response. Consider the action and response events to avoid continuous loops.

Domain Elements and Event Types Tab

The Domain Elements and Event Types Tab enables you to specify the event types to which to respond for a particular scope.

1. To access event responses, go to: **Network** > **Responses**.
2. Select One of the options under the Reponses tree.
3. Select **Domain Elements & Event Types**.

The Domain Elements and Event Types Tab displays the following options when a response is selected or edited:

- Enabled—Toggles the response to on or off (default is on).
- Response Applies to Events on These Domain Elements—Combo-box that enables you to select the domain elements for which the response is to apply.
- Response Applies To—Drop-down that enables you to specify whether the response applies to event types or event scopes. After you specify event types or event scopes, a tree structure displays that enables you to select the specific event types (or event scope) for which the response is to be executed.

Actions to Execute Tab

The Actions to Execute Tab enables you to specify the actions that are to be executed for the response being viewed (or edited).

1. To access event responses, go to: **Network** > **Responses**.
2. Select one of the options under the Responses tree.
3. Select **Actions to Execute**.

The Actions to Execute Tab displays the following options when a response is selected or edited:

- Response is Triggered When – Displays a list of properties to trigger responses which include:

- An event is posted (triggers a response when an event is posted to the message board).
- An event is acknowledged (triggers a response when an event is acknowledged by a user).
- An acknowledged event is unacknowledged (triggers a response when an event that was previously acknowledged by a user is unacknowledged).
- An event is cleared (triggers a response when an event is removed from the message board).
- The priority of an event changes (triggers a response when the priority level assisted to an event is altered).
- The repetition count of an event increments (triggers a response when the event has taken place again, and the number of times the event has occurred is incremented).
- The alert status of an element has changed (triggers a response when the alert status of an element is raised or lowered).
- An event is restored (triggers a response when an event is restored to the message board).
- An event is correlated (triggers a response when the event is correlated).
- Execute the Following Actions - Displays a list of existing actions that are valid for the currently specified scope.

Schedules

You can define a schedule that Monitoring follows to perform one or more actions at a specified time or interval. To access the Action Scheduler, select **Network** > **Schedules**.

Only the Campus Rediscovery action is available from the scheduler view, with an Event type of "none".

The following general controls are available on the Schedules page:

- Apply your changes—Applies your changes. All edits to schedules are client-side only. Pressing the Apply button saves the edits to the server.
- Discard changes, reverting to the previous values—Discards your changes. Unapplied edits to an action schedule can be undone by pressing the Revert button. No confirmation is offered, and unapplied edits are immediately lost.
- Add a new action schedule—Adds a new action schedule.
- Delete selected action schedule—Deletes an existing action schedule.
- Rename selected action schedule—Enables you to rename a selected action schedule.
- Clone selected action schedule—Duplicates an existing action schedule.
- Refresh—Refreshes the responses list.
- Test report generation—Tests the schedule you have configured.

The following fields display on the right-side panel of the Action Scheduler page when editing or viewing an action schedule:

- Enabled—Enables you to toggle the action schedule on or off (default is on).
- Execute Actions on these Domain Elements—Combo-box that enables you to select the domain elements for which the scheduled action is to apply.
- Actions to Execute—List that enables you to select one or more previously defined actions to execute.
- Schedule—Enables you to define the timetable that determines when the selected actions are executed.
- Add—Enables you to specify a new interval when the action must be executed. Interval options are:
  - One Time (executes the action only once at the date and time specified)
  - Every day (executes the action at the specified time every 24 hours)
  - Every week (executes the action at the specified time on the same day each week)
  - Every month (executes the action at the specified time on the same day each month)
  - End of month (executes the action at the specified time on the last day of each month).
  - Every hour (executes the action every 60 minutes at the specified number of minutes past the hour)
- Schedule applies to - Enables you to specify the domain that the schedule applies to.

Action Console

The Action Console displays the action schedules as well as the logs for server-based and web client-based actions. Monitoring records and displays the output and error logs from the actions in the bottom pane.

To view the Action Console, select **Network** > **Action Console**.

Click the Action Schedules pane, select a category, and the following fields are available:

- Schedule Name—Schedule name
- Next Occurrence—Next occurrence of the schedule
- Schedule Type—Type of schedule

Click the Active Actions and Action History panes, select a category, and the following fields are available:

- Action—Action name
- Subject—Name of the network element that the action is for
- User —User who performed the action

- Start Time—Action start time
- End Time—Action end time
- Status—Final status of the action: complete, aborted, or started
- Event Type—Event triggering the action
- Event ID—Unique ID of the event triggering the action
- Related Event Type—Related event that is correlated to trigger this action
- Related Event ID—Related event that is correlated to trigger this action

The Agents pane includes the following fields:

- Name
- Location
- Domain
- Execution Groups

You can rearrange the table view on the Action Console by hovering over a column header, clicking on the down arrow and selecting Sort Ascending or Sort Descending, or Columns to select the column headers for the table view.

Device Menu Choices

With the Device Menu Choices configuration, you can associate an action such as launching an external application, sending a trap, launching an embedded web management interface (HTTP), or executing a shell command with the domain elements in a particular scope. The action is associated with the domain elements in the scope so that if you right-click on an associated domain element, you can choose the action from the menu.

For example, you can configure a device menu choice so you can select a device and launch the proprietary management application of the device, which makes modifying device configuration easier. You can configure these menu choices to appear only for a subset of domain elements through a scope, and you can configure the choices to trigger any action. Most actions apply to specific domain element types, such as to data sets, or to logical volumes, so the set of actions that is available for launching typically varies with the scope that is selected.

To configure Device Menu Choices, select **Network** > **Device Menu Choice**. The following general controls are available on the Device Menu Choice page:

- Apply your changes—Applies your changes. All edits to device menu choices are client-side only. Clicking the Apply button saves the edits to the server.
- Discard changes, reverting to the previous values—Discards your changes. Unapplied edits to a device menu choice are undone by clicking the Revert button. No confirmation is offered and unapplied edits are immediately lost.
- Add a new custom launch—Adds a new device menu choice.

- Delete selected custom launch—Removes a selected device menu choice.
- Rename selected custom launch—Renames a selected device menu choice.
- Clone selected custom launch—Clones a selected device menu choice.
- Refresh—Refreshes the list of device menu choices.

You can specify parameters for the device menu choice with the definitions. The device menu choice definition panel displays the following options when you select or edit a device menu choice:

- Enabled—Toggles the device menu choice on or off. You must select this check box to make the device menu choice active.
- Show Output—Displays information regarding the action that is executed. Show Output is for diagnostic purposes.
- Obtain user confirmation before executing—You can require user confirmation prior to performing the device menu choice.
- Attach actions to these domain elements—Attaches actions to specific domain elements. You select the domain elements for which the device menu choice is to apply.
- Make these actions available—Identifies the actions that are to be performed for the device menu choice. You can select multiple actions for a device menu choice. Some actions do not appear until you select the appropriate scope.
- Comments—Specifies descriptive text associated with the device menu choice.

Automating configuration tasks

With Monitoring you can automate actions, responses, and schedules.

Creating an action

An action is an instance of an action type. Automatic execution is initiated as a result of a response configuration or an action schedule. Use the following procedure to create an automatically executed action.

Procedure

1. Select **Network** > **Actions**.
2. On the Monitoring Actions page, select the action group to which you want to add an action by highlighting the folder in the left panel.
3. Click **Add a new action**.

   A drop-down menu displays the available action types.

4. Select the appropriate action type.
5. In the Prompt dialog box, type a name for the action you are creating, and then click **OK**.

   The right panel of the Monitoring Actions page displays the parameters for defining the new action.
6. Specify values for all mandatory parameters and for any optional parameters that you want to use.
7. Click **Apply your changes**.

Variable definitions

The following table describes the options under **Network** > **Actions**, when you select **Add a new action**.

Variable	Definition
Command Action	Executes a command script using languages such as DOS Batch, SH, BASH, CSH, or TCSH.
Email Action	Sends an email message from a specified user account to one or more recipients.
SNMPv2 Notification	Initiates an SNMPv2 notification.
Rediscovery Action	Initiates a domain rediscovery.
Config Control Action	Generates a configuration control response.
Campus Rediscovery Action	Enables you to automate a campus rediscovery. This action can be used in Responses to rediscover a campus triggered by a user-specified event.
Web Browser Action	Enables you to establish a connection to a specified URL using a web browser.

Command Action

A command action executes command scripts using scripting languages such as SH or DOS batch files. You must have an Advanced License to use this action.

1. Go to **Network** > **Actions**.
2. Click **Add a new action** from the top left toolbar.
3. Select **Command Action** from the menu to access the following options.
4. Enter the name of the action.
5. Fill in other information as required.
6. Select **Apply your changes** in the top left toolbar.

You can configure the following options when you create a command action:

- Subject Type—Displays the subject type for the action. When editing an action, this option enables you to select from a drop-down list of the types of domain elements against which the action can be executed.
- Event Type—Displays the event type for the action. When editing an action, this option enables you to select from a drop-down list of the event types for which the action can be executed.
- Related Event Type—Displays a related event type for the action. When editing an action, this option enables you to select from a drop-down list of the related event types for which the you can execute the action.
- Add Script Definition—Displays the script definitions available for the command action. When editing a command action, this option enables you to select from a drop-down list of options that enable you to create a new script definition (DOS Batch, SH, BASH, CSH or TCSH). A system adds a new tab for each script definition. Tabs may be ordered using the raise and lower script in selection order buttons, causing the script to be executed in a specified order with respect to other script definitions.
- Up—Enables you to move the current script to a higher position in the selection order.
- Down—Enables you to move the current script to a lower position in the selection order.
- Delete—Deletes the selected script definition.

Email Action

Email Action sends an email message from a specified user account to one or more recipients.

1. Go to **Network** > **Actions**.
2. Click **Add a new action** from the top left toolbar.
3. Select **Email Action** from the menu to access the following options.
4. Enter the name of the action.
5. Fill in other information as required.
6. Select **Apply your changes** in the top left toolbar.

The following options apply to the creation of email actions:

- Subject Type—Displays the subject type for the action. When editing an action, this option enables you to select from a drop-down list of the types of domain elements against which the action can be executed.
- Event Type—Displays the event type for the action. When editing an action, this option enables you to select from a drop-down list of the event types for which the action can be executed.

- Related Event Type—Displays a related event type for the action. When editing an action, this option enables you to select from a drop-down list of the related event types for which you can execute the action.
- To—(Required) The email address(es) of the user(s) to whom the notification is sent.
- From—(Required) The proper name shown in the inbox of the recipient as the sender of the message.
- Cc—The email address(es) of any recipients who are copied on the message, but to whom the message is not addressed explicitly.
- Bcc—The email address(es) of any recipients who are copied on the message, but whose names are not made visible to other recipients.
- Subject—(Required) The topic that the message covers.
- File Attachment—The file name and path of an optional attachment that is to be sent with the email.
- Message—(Required) The text of the message.

SNMPv2 Notification

SNMPv2 Notification initiates an SNMPv2 notification. You must have an Advanced License to use this action.

1. Go to **Network** > **Actions**.
2. Click **Add a new action** from the top left toolbar.
3. Select **SNMPv2 Notification** from the menu to access the following options.
4. Enter the name of the action.
5. Fill in other information as required.
6. Select **Apply your changes** in the top left toolbar.

The following options apply to the creation of SNMPv1 trap actions:

- Subject Type—Displays the subject type for the action. When editing an action, this option enables you to select from a drop-down list of the types of domain elements against which the action can be executed.
- Event Type—Displays the event type for the action. When editing an action, this option enables you to select from a drop-down list of the event types for which the action can be executed.
- Related Event Type—Displays a related event type for the action. When editing an action, this option enables you to select from a drop-down list of the related event types for which you can execute the action.
- Target Host—(Required) The IP address or DNS name of the host to which the traps are to be sent.

- Target Port—(Required) The UDP port on which the target host listens for traps.
- Enterprise OID—(Required) The trap's text-based object ID.
- Variable Bindings—A list of object IDs (OID, the ID of an SNMP object for which you want to send a notification) and associated values (the value to which the SNMP object is set).
  - Add—Displays the Select Node(s) window that enables you to expand a tree of MIB modules and select a variable binding to which the SNMPv2 trap applies, verify the object ID, Numeric OID, and specify a value for the node.
  - Remove—Enables you to remove a variable binding from the SNMPv2 trap action definition.

Rediscovery Action

A Rediscovery Action initiates a domain rediscovery. You must have an Advanced License to use this action.

1. Go to **Network** > **Actions**.
2. Click **Add a new action** from the top left toolbar.
3. Select **Rediscovery Action** from the menu to access the following options.
4. Enter the name of the action.
5. Fill in other information as required.
6. Select **Apply your changes** in the top left toolbar.

If a rediscovery action is selected, the following field displays in the right panel of the Monitoring Actions page:

- Rediscovery Policy - Drop-down selection list of available rediscovery policies to use when the rediscovery action is executed. You can use rediscovery actions in action schedules to rediscover a domain according to a user-specified schedule.

Config Control Action

A Config Control Action generates a configuration control response. You must have an Advanced License to use this action.

1. Go to **Network** > **Actions**.
2. Click **Add a new action** from the top left toolbar.
3. Select **Config Control Action** from the menu to access the following options.
4. Enter the name of the action.
5. Fill in other information as required.
6. Select **Apply your changes** in the top left toolbar.

The following options apply to the creation of workflow actions:

- Changes to Make—Add - Displays a drop-down selection list of available configuration changes which include:
  - Monitoring Configuration—Displays Enable/Disable window where you can enable or disable individual monitoring configurations.
  - Response—Displays Enable/Disable window where you can enable or disable individual responses.
  - Action Schedule—Displays Enable/Disable window where you can enable or disable individual action schedules.
  - Override Configuration—Displays Enable/Disable window where you can enable or disable individual override configurations.
- Changes to Make:
  - Delete—Deletes selected configuration control actions.

Campus Rediscovery Action

A Campus Rediscovery Action enables you to automate a campus rediscovery. Use this action in responses to rediscover a campus triggered by a user-specified event. You must have an Advanced License to use this action.

1. Go to **Network** > **Actions**.
2. Click **Add a new action** from the top left toolbar.
3. Select **Campus Rediscovery Action** from the menu to access the following options.
4. Enter the name of the action.
5. Fill in other information as required.
6. Select **Apply your changes** in the top left toolbar.

The following options apply to the creation of campus rediscovery actions:

- Subject Type—Displays the subject type for the action. When editing an action, this option enables you to select from a drop-down list of the types of domain elements against which the action can be executed.
- Event Type—Displays the event type for the action. When editing an action, this option enables you to select from a drop-down list of the event types for which the action can be executed.
- Rediscovery Policy—Drop-down selection list of available rediscovery policies to be used when the rediscovery action is executed. Rediscovery actions can be used in action schedules to rediscover a domain according to a user-specified schedule.

Web Browser Action

A Web Browser Action enables you to establish a connection to a specified URL using web browser. Web browser actions are actions that are executed from the client browser and are therefore affected by browser settings. These actions are triggered by a menu that displays when you right-click a device in Network Topology.

1. Go to **Network** > **Actions**.
2. Click **Add a new action** from the top left toolbar.
3. Select **Web Browser Action** from the menu to access the following options.
4. Enter the name of the action.
5. Fill in other information as required.
6. Select **Apply your changes** in the top left toolbar.

You can configure the following options when you create a web browser action:

- Subject Type—Displays the subject type for the action. When editing an action, this option enables you to select from a drop-down list of the types of domain elements against which the action can be executed.
- Event Type—Displays the event type for the action. When editing an action, this option enables you to select from a drop-down list of the event types for which the action can be executed.
- Related Event Type—Displays a related event type for the action. When editing an action, this option enables you to select from a drop-down list of the related event types for which the you can execute the action.
- Protocol—Specifies the connections you can establish using the web browser, with the following protocols: HTTP, HTTPS, Telnet FTP, embedded.
- Location—Specifies the location.
- Timeout—Specifies the timeout value.

Web browser actions are actions that are executed from the client browser, and are therefore affected by the browser settings. The Web Browser is available with the Advanced License.

You can trigger web browser actions from the menu that displays when you right-click on a device in the network browser. There are two ways to configure web browser actions:

- Use the Device Menu Choice link on the navigation panel to establish a connection through a web browser.
- Use the Actions link on the navigation panel to establish a connection to a specified address through a web browser.

Web browser actions can establish connections using the following protocols:

- FTP Connect—Opens an FTP connection.

- HTTP Connect—Opens an HTTP connection.
- HTTPS Connect—Opens an HTTPS connection.
- Launch EM—Opens an HTTP connection to the device which launches the Business Element Manager on the device.
- Launch Telnet—Opens a Telnet connection.

Renaming an action

After you create an action you can change the name.

Procedure

1. Select **Network** > **Actions**.
2. Select the action you want to rename.
3. Click the **Rename selected action** button.
4. In the Prompt dialog box, enter the new name.
5. Click **OK**.

Cloning an action

After you create an action you can clone the action.

Procedure

1. Select **Network** > **Actions**.
2. Select the action you want to clone.
3. Click **Clone selected action**.
4. In the Prompt dialog box, enter a new name for the cloned action.
5. Click **OK**.

Deleting an action

Perform the following procedure to delete an action if you do not need the action.

Procedure

1. Select **Network** > **Actions**.
2. Select the action you want to delete.
3. Click **Delete selected action**.

4. Click **OK** to confirm the deletion.

Performing a selected action

About this task

Perform an action immediately to verify the action settings. An email is sent according to the configuration.

Before you begin

Make sure that the Email SMTP preferences are configured. Click the **Preferences** icon on the quick access toolbar to open the Global Preferences page.

For information on how to configure the preferences, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

Procedure

1. Select **Network** > **Actions**.
2. Select the action you want to perform immediately.
3. Click the **Execute now selected action** button.

Creating a response

Responses define the ways in which Monitoring addresses certain events automatically. The definition of a response requires you to first select a scope and an event that affects that scope, then select an action that addresses that event for that scope.

Only those actions that are guaranteed to apply to every element encompassed by the scope/event combination are shown, even though other actions may have been defined. In addition, you must define how the response handles messages relative to the triggering event.

Note:

Continuous action and response triggers can occur if you select an action failure self event trigger when creating a response. Consider the action and response events to avoid continuous loops.

Procedure

1. Select **Network** > **Responses**.
2. On the Actions By Event Response page, click **Add a new response**.
3. In the Prompt dialog box, enter a name for the response, and then click **OK**.

   The Domain Elements and Event Types and Actions to Execute tabs appear.
4. Select the **Domain Elements & Event Types** tab.
5. Enable or disable the Response by selecting or clearing the **Enabled** check box.

6. Click the combo-box button under the **Response applies to event on these Domain Elements** heading and select the scope for which you want the response to apply, and then click **OK**.
7. From the **Response applies to** menu, select **Event Types** or **Event Scopes**.
8. Use the tree to locate the event type (or event scope) for which you want the response to apply.
9. Click the **Actions to Execute** tab.
10. Select the appropriate options in the **Response is triggered when** field.
11. Select the appropriate options in the **Execute the following actions** section.
12. Click **Apply your changes** from the top left toolbar.

Renaming a response

After you create a response you can change the name.

Procedure

1. Select **Network** > **Responses**.
2. Select the response you want to rename.
3. Click **Rename selected response**.
4. In the Prompt dialog box, enter the new name.
5. Click **OK**.

Cloning a response

After you create a response you can clone the response.

Procedure

1. Select **Network** > **Responses**.
2. Select the response you want to clone.
3. Click **Clone selected response**.
4. In the Prompt dialog box, enter a new name for the cloned response.
5. Click **OK**.

Deleting a response

You can delete a response if you do not need the response.

Procedure

1. Select **Network** > **Responses**.
2. Select the response you want to delete.
3. Click **Delete selected response**.
4. Click **OK** to confirm the deletion.

Creating an action schedule

An action schedule is a tool for initiating one or more actions at a predetermined time or interval. The action schedule consists of a set of domain elements encompassed by a particular scope within one or more domains, the actions that the action schedule implements, and the time table by which those actions are performed on those domain elements.

Procedure

1. Select **Network** > **Schedules**.
2. Click **Add a new schedule** > **Action schedule**.
3. In the Prompt dialog box, type the name of the new action schedule in the field.
4. Click **OK**.

   The action schedule definition options appear.
5. Ensure that you select the Enabled checkbox.
6. If you want to execute actions on specific domains, select the **Execute Actions on these Domain Elements** box and use the combo-box to choose a scope.
7. Specify the **Actions to Execute** by checking the boxes corresponding to the desired action(s).
8. In the **Schedules** section, to select the interval for the schedule to execute the defined actions, click **Add**, and select a time interval.

   The time is shown as the UTC and GMT offset, and specifies the time zone of where the server is located.
9. Enter the interval information, and click **OK**.
10. In the **Schedule applies to** section, specify the applicable domains.
11. Click **Apply your changes** (check mark icon on the left).

Creating a report schedule

Before you begin

Make sure that the Email SMTP preferences are configured. Click the **Preferences** icon on the quick access toolbar to open the Global Preferences page.

For information on how to configure the preferences, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

Procedure

1. Select **Network** > **Schedules**.
2. Click **Add a new schedule** > **Report schedule**.
3. In the Prompt dialog box, type the name of the new report schedule in the field.
4. Click **OK**.

   The report schedule definition options appear.
5. Ensure that you select the Enabled checkbox.
6. In the Reports to Attach section, click **Add**.
7. In the Add new report dialog box, select an available report and click **OK**.
8. Repeat steps 5 and 6 to add additional reports as required.
9. In the **Schedule** section, to select the interval for the schedule to execute the defined actions, click **Add**, and select a time interval.

   The time is shown as the UTC and GMT offset, and specifies the time zone of where the server is located.
10. Enter the interval information, and click **OK**.
11. Enter the required information for the email to be sent to one of more recipients.
12. In the **Schedule applies to** section, specify the applicable domains.
13. Click **Apply your changes** (check mark icon on the left).

Renaming a schedule

You can rename an action schedule after you create the action schedule.

Procedure

1. Select **Network** > **Schedules**.
2. Select the schedule you want to rename.
3. Click **Rename selected action schedule**.

4. In the Prompt dialog box, enter the new name.
5. Click **OK**.

Cloning a schedule

After you create a schedule you can clone the schedule.

Procedure

1. Select **Network** > **Schedules**.
2. Select the schedule you want to clone.
3. Click **Clone selected action schedule**.
4. In the Prompt dialog box, enter a new name for the cloned schedule.
5. Click **OK**.

Deleting a schedule

You can delete a schedule if the schedule is not required.

Procedure

1. Select **Network** > **Schedules**.
2. Select the schedule you want to delete.
3. Click **Delete selected action schedule**.
4. Click **OK** to confirm the deletion.

Creating a domain rediscovery schedule

A domain rediscovery schedule enables you to automate the rediscovery of your domain. Perform the following procedure to create a domain rediscovery schedule.

Procedure

1. Select **Network** > **Schedules**.
2. Click **Add a new schedule** > **Action schedule**.
3. In the Prompt dialog box, type the name of the new action schedule in the box.
4. Click **OK**.

   The system displays the action schedule definition options.
5. Ensure that the Enabled checkbox is selected.

6. Clear the **Execute Actions on these Domain Elements** check box.
7. In the **Actions to Execute** field, select **Rediscover Domain**.
8. In the **Schedule** field, click **Add**.
9. Select the appropriate scheduling option.
10. Specify a time of day for the action to occur.
11. Click **Apply your changes**.

Action Console

The Action Console displays the action schedules as well as the logs for server-based and web client-based actions. Monitoring records and displays the output and error logs from the actions in the bottom pane.

To view the Action Console, select **Network** > **Action Console**.

Click the Action Schedules pane, select a category, and the following fields are available:

- Schedule Name—Schedule name
- Next Occurrence—Next occurrence of the schedule
- Schedule Type—Type of schedule

Click the Active Actions and Action History panes, select a category, and the following fields are available:

- Action—Action name
- Subject—Name of the network element that the action is for
- User —User who performed the action
- Start Time—Action start time
- End Time—Action end time
- Status—Final status of the action: complete, aborted, or started
- Event Type—Event triggering the action
- Event ID—Unique ID of the event triggering the action
- Related Event Type—Related event that is correlated to trigger this action
- Related Event ID—Related event that is correlated to trigger this action

The Agents pane includes the following fields:

- Name
- Location
- Domain

- Execution Groups

You can rearrange the table view on the Action Console by hovering over a column header, clicking on the down arrow and selecting Sort Ascending or Sort Descending, or Columns to select the column headers for the table view.

Viewing action schedules

Procedure

1. Select **Network** > **Action Console**.
2. Select Action Schedules and the interval to view the scheduled actions for that interval.

Viewing active actions

Procedure

1. Select **Network** > **Action Console**.
2. Select **Active Actions** to view currently active actions and related logs.

Viewing the action history

Procedure

1. Select **Network** > **Action Console**.
2. Select **Action History** to view the action history and related logs.
3. Click **Select records to purge** to open the Purge dialog box and configure the records to purge.
4. Select if you want to purge:
   - All history records
   - Current page records
   - Records stated between <a certain timeframe>
5. Click **OK**.

Adding device menu choices

You can associate an action such as launching an external application, sending a trap, or executing a shell command with the discovery domain elements in a particular scope by adding a device menu choice and setting the parameters.

Procedure

1. Select **Network** > **Device Menu Choice**.
2. Click **Add a new custom launch**.
3. In the Prompt dialog box, type a name for the device menu choice in the dialog box.

4. Click **OK**.

   The available options appear in the right panel of the Device Menu Choices window.
5. Select the appropriate options.
6. Click **Apply your changes**.

Variable definitions

The following table describes the options when you select Add a new custom launch, under **Network** > **Device Menu Choice**.

Variable	Value
Enabled	Toggle the device menu choice on or off. You must select this check box to make the device menu choice active.
Show Output	Displays information regarding the action that is executed. Show Output is for diagnostic purposes.
Obtain user confirmation before executing	Select this check box to obtain user confirmation prior to performing the device menu choice.
Attach actions to these Domain Elements	Select the domain elements for which the device menu choice is to apply.
Make these Actions Available	Identifies the actions that are to be performed for the device menu choice. You can select multiple actions for a device menu choice. Some actions will not appear until you select the appropriate scope.
Comments	Descriptive text associated with the device menu choice.

Adding web browser action as a device menu choice

You can add a web browser action as a device menu choice. Monitoring can launch the following connection types:

- FTP connection
- HTTP connection
- HTTPS connection
- telnet connection

When you create an action as a device menu choice, you can launch an FTP, HTTP/S, or telnet session by selecting the option from a right-click menu on a device.

Procedure

1. Select **Network** > **Device Menu Choice**.
2. Click **Add a new custom launch**.

3. In the Prompt dialog box, type a name for the device menu choice in the dialog box.

   For example, `telnet_https`.
4. Click **OK**.
5. Select the **Enabled** check box.
6. Select the **Obtain user confirmation before executing** check box.
7. From the **Make these actions available** list, select the actions you want to launch.
8. Click **Apply your changes** in the top left toolbar.
9. Select **Network** > **Topology**.
10. Select the perspective you want in the drop-down menu above the tree browser.
11. Right-click on any device for which you want to launch a Telnet/Http/Https/Ftp session.
12. From the list, select **Tools** and click the option you want to launch. You can select one of the following:
    - Launch EM
    - Launch Secure EM
    - Rediscover Campus
    - Rediscover Device

Configuring a customized web browser action

Use the following procedure to create a customized web browser action. A customized web browser action establishes a connection to a configured address. Monitoring can launch the following connection types:

- FTP connection
- HTTP connection
- HTTPS connection
- telnet connection

When you create a customized web browser action, you can launch the connection by selecting the option from a right-click menu on a device.

Procedure

1. Select **Network** > **Actions**.
2. On the Monitoring Actions page, select the **Web Browser Actions** folder.
3. Click the **Add a new action** button.

   A drop-down menu displays the available action types.

4. Select **Web Browser Action**.
5. In the Prompt dialog box, type a name for the action you are creating in the box, and then click **OK**.
6. Specify values for all mandatory parameters and for any optional parameters you want to use.
7. Click **Apply your changes**.

Variable definitions

Variable	Value
Subject Type	The scope to which the web browser action will apply.
Event Type	Displays the event type for the action. When editing an action, this option enables you to select from a drop-down list of the event types for which you can execute the action. After you define any customized Web browser action, the event type drop down box is disabled because Web Browser actions are related to Custom Launch on the device.
Related Event Type	Displays a related event type for the action. When editing an action, this option enables you to select from a drop-down list of the related event types for which you can execute the action. After you define any customized Web browser action, the related event type drop down box is disabled because Web Browser actions are related to Custom Launch on the device.
Protocol	Specify the protocol to use when establishing the connection: FTP, HTTP, HTTPS, or Telnet.
Location	The URL to establish the connection with.
Default	Read-only. The device on which the action is invoked.
Timeout	The length of time to wait for the server to respond to the connection request before timing out.