Configuring the Avaya Visualization Performance and Fault Manager

Release 3.0.3
NN48014-500
Issue 07.02
February 2015

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya 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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya 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 Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's 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

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya 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. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

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

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA 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 AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 Avaya or an Avaya 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 Designated Processor that hosts 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.

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya 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 Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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 Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya 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 Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

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 Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya Aura® is a registered trademark of Avaya Inc.

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya 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 Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Related Links

Purpose on page 7

Related resources on page 7

Purpose

This document provides information on configuring and managing your Avaya Visualization Performance and Fault Manager (VPFM) system.

This document is intended for providing administrators with a management tool that offers solutions within a highly dynamic virtualized data center environment. VPFM reduces troubleshooting issues because of a more complete view of the network. With VPFM, 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.

Related Links

Introduction on page 7

Related resources

Related Links

Introduction on page 7

Documentation on page 7

Training on page 8

Viewing Avaya Mentor videos on page 9

Support on page 9

Documentation

See the following related documents:

Title	Purpose	Link
Avaya Visualization Performance and Fault Manager — Common Services Fundamentals Unified Communications Management (NN48014–100)	Fundamentals	http://support.avaya.com
Avaya Visualization Performance and Fault Manager VPFM SCOM Connector Fundamentals (NN48014–101)	Fundamentals	http://support.avaya.com
Avaya VPFM Traps and Trends (NN48014–103)	Reference	http://support.avaya.com
Avaya VPFM Supported Devices, Device MIBs, and Legacy Devices (NN48014–104)	Reference	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Discovery Best Practices (NN48014–105)	Best Practices	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Installation (NN48014–300)	Installation	http://support.avaya.com
Avaya Visualization Performance and Fault Manager VPFM SCOM Connector Installation (NN48014–301)	Installation	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Quick Start (NN48014–302)	Quick Start	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Using Unified Communications Management to Manage the Converged Voice and Data Network (NN48014–501)	Deployment	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Fault and Performance Management (NN48014–700)	Administration	http://support.avaya.com

Related Links

Related resources on page 7

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Related Links

Related resources on page 7

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Related Links

Related resources on page 7

Support

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.

Related Links

Related resources on page 7

Chapter 2: New in this release

Features

See the following sections for information about feature changes.

New and updated device support

The following Avaya data devices are added:

- ERS 3500 v5.1.1
- VSP 4000 series v3.0.1.0
- Avaya SRA firewall Sw:1.0.1

The following Avaya data devices are updated:

- VSP 7000 series v10.2.1

The following Avaya Voice Devices (Aura VE) are added:

- Avaya Aura Messaging (AAM) release v6.3
- Avaya Aura Contact Center Control Manager (ACCCM) release 7.0
- Avaya Navigator (A-NAV) release 4.1
- Avaya Contact Recorder (ACR) release 12.0
- Contact Center (CC) Elite Multi Channel (EMC) release 6.3
- Avaya Call Management System (CMS) release 17.0
- Avaya Session Border Controller (Sipera SBC) release 6.2
- Avaya G860 Media Gateway (M3K) release 6.2
- Avaya Meeting Exchange (MX) release 6.2
- Avaya Aura Experience Portal (AAEP) release 6.0.2

The following Avaya Aura Virtual Environment (Aura VE) devices are updated:

- Presence Service (PS) release 6.2.2

- Agile Communication Environment (ACE/AIE) release 6.3
- Avaya Application Enablement Services (AES) release 6.3.1
- Avaya CM duplex or simplex release 6.3.2
- Session Manager release 6.3.4
- System Manager release 6.3.4
- Utility Services (US) release 6.3

The following third party devices are updated:

- VMware ESXi v5.1
- VMware VSphere v5.1
- VMware VCenter v5.1

The following third party devices are added:

- Acme Packet Net-Net 4000 (SBC) release 6.3
- Sentry Smart CDU power supply firmware 7.0j

Upgrades

You can upgrade directly from VPFM release 3.0.1 to release 3.0.3, or from release 3.0.2 to release 3.0.3. If you want to upgrade from a release older than 3.0.1, you must first upgrade to release 3.0.1, then upgrade to release 3.0.3.

Upgrade on a VM environment

When you upgrade VPFM from a release older than VPFM 3.0.2 to release 3.0.3 on a VM environment, Unified Communication Management (UCM) removes the license associated with the application from the license file. Therefore, make a copy of the license file before you perform the upgrade; you can use the copy of the license file to return to the older release, if required.

VPFM hardware requirements

Avaya Visualization Performance and Fault Manager (VPFM) 3.0.3 supports a 64-bit Linux system using a 64-bit VPFM application.

Client browsers

Avaya Visualization Performance and Fault Manager (VPFM) 3.0.3 supports the following browsers:

- Internet Explorer (IE), versions 9 and 10.
- Mozilla Firefox (FF), versions 24 and 25.

Dashboard enhancements

Enhancements to the Avaya Visualization Performance and Fault Manager (VPFM) dashboard include the following:

- addition of a Power Savings dashboard that displays dashlets containing information about total network power savings and top switch watt reduction.

Reporting enhancements

Enhancements to Avaya Visualization Performance and Fault Manager (VPFM) reporting include the following:

- introduction of Pod specific Inventory Reports
- addition of three new Event browser columns to display Pod specific information:
    - Host
    - VM Host
    - Pod
- introduction of Power Savings reporting
- ability to aggregate statistics per stack and per domain

Discovery features

Avaya Visualization Performance and Fault Manager (VPFM) 3.0.3 introduces the following discoveries:

- discovery of Unified Communications as a Service (UCaaS) Collaboration Pod — discovering and visualizing the UCaaS Collaboration Pod as a single logical unit
- discovery of Contact Center as a Service (CCaaS) Collaboration Pod — discovering and visualizing the CCaaS Collaboration Pod as a single logical unit
- discovery of UCaaS and CCaaS Collaboration Pod components
    - VSP 4000 series
    - Avaya Aura Messaging (AAM)
    - Avaya SRA firewall Sw : 1.0.1
    -
- discovery of UCaaS and CCaaS Collaboration Pod applications
    - Call Management System (CMS) VE and correlated traps
    - Avaya Aura Experience Portal (AEP) and correlated traps

  - Elite Multi Channel (EMC) and correlated traps
  - Work Force Optimization (WFO)
  - A-NAV
  - Avaya Contact Center Control Manager (ACCCM)
  - Meeting Exchange (MX)
  - Avaya Contact Recorder (ACR)
- discovery of third party devices
  - Avaya Media Gateway G860: software version: AudioCodes MEDIANT5000; sw version 5.8.103
  - Acme Packet Net-Net Session Border Controller (SBC)
  - Sipera Session Border Controller (SBC)
  - Sentry smart PDU power supply
- discovery of additional phone properties (for managed phones that support SNMP)
  - serial numbers of phones
  - OEM model name

Avaya VPFM 3.0.3 introduces the following Advanced Discovery Options:

- Abort hung queries after (minutes)
- SNMP timeout (seconds)
- Max SNMP retries
- Estimated max request time (2-126)

Fault and diagnostics enhancements

Enhancements to fault and diagnostics include the following:

- VoIP Fault performance management now displays trunk utilization on CM, SBC, and gateways.

Supporting operating systems

Avaya Visualization Performance and Fault Manager (VPFM) release 3.0.3 supports the following operating systems:

- Windows Server 2003 Standard or Enterprise Service Pack 2, 32-bit or 64-bit version. VPFM supports Windows 2003 through upgrade only.
- Windows Server 2008 Enterprise and Datacenter editions R2 Service Pack 2, 32-bit or 64-bit versions.

- Red Hat Enterprise Linux 5.6, 32–bit or 64-bit. VPFM supports RHEL only.

Topology and GUI enhancements

Avaya Visualization Performance and Fault Manager (VPFM) release 3.0.3 displays an extension pod shown in the topology as an aggregate icon.

Avaya VPFM introduces the following enhancements to the central browser panel:

- ability to launch VMware vCenter by right clicking on a virtual machine (VM) host

  Note:

  Beginning with Release 3.0.3, you must manually set the IP address of vCenter into action after the VPFM installation. You must manually edit the sample action named "VMware vCenter" replacing the host name in the URL with the name or IP address of a real vCenter server. You can configure one vCenter server to manage all VMs on all VHs, i.e., the same vCenter server can be the destination for all VM hosts.

- ability to launch EMC Unisphere by right clicking on a storage device

Avaya VPFM release 3.0.3 adds the following enhancements to the SNMP MIB Query page menu bar:

- **Switch to columns** menu item
- **Clear** menu item
- history to SNMP MIB query is maintained with multiple tab support

Other information

See the following sections for information about changes that are not feature-related.

UCaaS Pod OVA and CCaaS Pod OVA

This release introduces the Unified Communications as a Service (UCaaS) Collaboration Pod OVA version of VPFM 3.0.3 and the Contact Center as a Service (CCaaS) Collaboration Pod OVA version of VPFM 3.0.3.

Chapter 3: Fundamentals

The following information is an overview of the Avaya Visualization Performance and Fault Manager (VPFM) system.

Managed objects

A managed object (MO) is a device that VPFM actively processes information about to reflect the current status and condition of the object in real-time. The data that VPFM 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, VPFM 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 VPFM 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 counte towards the MO license count of VPFM.

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 500 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 500.
- 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

You can configure many components for VPFM application. You must configure Network Discovery to run network auto-discoveries. A discovery is a snapshot taken of part or all of a network.

After you log on to VPFM for the first time, and before you can browse your network, you must complete the following steps:

- Configure device credentials using the Device and Server credentials editor in common services in Avaya Unified Communications Management (UCM). For more information see, *Avaya Unified Communications Management Common Services Fundamentals* (NN48014-100).
- Add a new discovery domain.
- Configure the discovery options for the discovery domain.
- Discover the domain.

❗ **Important:**

The only configuration required to manage a device is for it to respond to SNMP and to have the SNMP credentials for this device added to the Device and Server Credentials Editor in UCM. If a device is changed from Unmanaged to Managed by either adding credentials for it or by enabling SNMP on it after the discovery is completed, you must run rediscovery on the domain or create a new domain and discover it.

On the network discovery page, you can work with discovery domains, configure discovery options, perform discoveries, and view discovery status. To access the Network Discovery page, log on to VPFM, and on the VPFM menu bar, click Topology, and select Network Discovery.

The following general controls are available on the Network Discovery page:

- Apply—Saves the edits to the server. All edits you make to domain configuration are client-side only, clicking the Apply button saves the edits to the server.
- Revert—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 the Revert button.
- 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 and names may include numbers, letters with spaces, underscores (_) or hyphens (-) but not special characters.
- Delete selected domain—Deletes the selected discovery domain. You are prompted 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.
- Clone selected domain—Clones the selected discovery domain. When you clone an existing discovery domain, you create a new domain using the existing domain's discovery configuration. No other information is cloned. After you clone a domain, a discovery must be performed before the new domain can be browsed or monitored. The same rules for domain names apply for cloned domains as for those created using the create operation.
- Discover—Initiates the discovery for the domain.
- Manual Discovery—Initiates the manual discovery for 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—Saves the domain. Larger domains require longer save times.

  ❗ **Important:**

  If you specify a custom name for a device, you must go to the Network Discovery page and click **Save** to save the domain. If you do not save the domain, the custom name is not saved after a VPFM restore or restart.

- Auto refresh—Turns on or off page refresh or changes the refresh interval. The default is auto refresh every 15 seconds.
- Refresh—Refreshes the page once. The refresh is performed immediately.

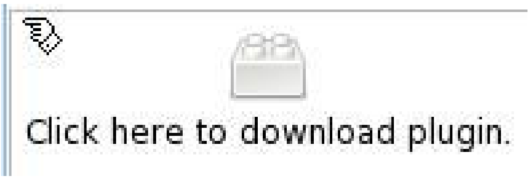
- Start/Stop Monitoring—Starts or stops monitoring of the discovery domain. By default when the domain is discovered only Start Monitoring is available.

Moving icons in the topology view

The topology browser permits you to move icons, save the new layout, and share it for other users to see. Before you can move an icon, in the Network Browser 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 make the view visible to other users by checking Share with all 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.

Before you can use the Network Browser in VPFM, you must install the Adobe™ Flash browser plug-in. If you do not have the Adobe Flash browser plug-in installed, the Network Browser displays a plug-in icon instead of the network map.

The following figure is the icon you click to download a plugin.



Note:

If a security warning appears asking you if you want to view only the webpage content that was delivered securely, click **No**. The Install Flash Player prompt appears.

If you select Yes, then the Install Flash Player prompt does not appear and the Network Browser page appears without the Flash Player.

Default discovery policy

By default, the discovery has the following policy:

- Wide Area Network (WAN) Crawl (not selected) - VPFM discovers devices on the far side of every router interface, regardless of the interface type. If the WAN Crawl option is not selected then VPFM Discovery does not go beyond any interface which is considered to be WAN interface.
- VPN Crawl (not selected) - VPFM 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.
- DNS Lookup (not selected) - VPFM performs DNS lookup on all devices.
- Service By PortScan — VPFM discovery scans for well known service ports on servers. The option is to look for services running on a server at the time of discovery.

- For all Devices — You can perform a service by PortScan for all devices.
- Avaya Only Discovery (selected) - Ignores any devices that are not on the approved Avaya list.
- Storage Discovery — VPFM discovers file systems based on Linux log-in and scan of file systems on a server.

Domain, pods, campus, and seeds

Domains, pods, campuses, and seeds are part of the discovery.

With Avaya VPFM, 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 it. It can be a device or an application. VPFM supports multiple discovery domains. You can manage and browse each discovery domain independently of the others.

After VPFM 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.

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 which could be discovered and monitored.

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 it appears because you can apply a different action to each instance of the MO in each VPFM discovery domain.

A pod contains Avaya networking components such as applications, servers, and disk units in a single enclosure. You can view details of these components such as corresponding status, and serial numbers.

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. VPFM 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

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 VPFM identifies from a large set of possible addresses that have been detected by VPFM 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 IP v4 and v6 standard syntax is supported for seeds.

Important:

For v6, VPFM 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 router’s ARP cache, 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 addresses without corresponding devices are probed until timeout. Use subnets as discovery seeds if your network has no router or if important devices are missed when a router is used as the discovery seed.

For example, if you want to discover a network with two subnets and nothing beyond it: Add the IP Address of Router/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 VPFM 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 should be 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 filter’s conditions.

- Options - You can specify the manner in which the discovery crawls your network (Wide Area Crawl, VPN Crawl, DNS Lookup, Service By PortScan, For All Devices, Avaya Only Discovery, and 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 VPFM automatically discovers the following Avaya applications as part of its discovery process:

- Avaya Multimedia Conferencing Release 6.0
- Avaya NES Interactive Communications Portal (Avaya NES ICP) Release 1.0

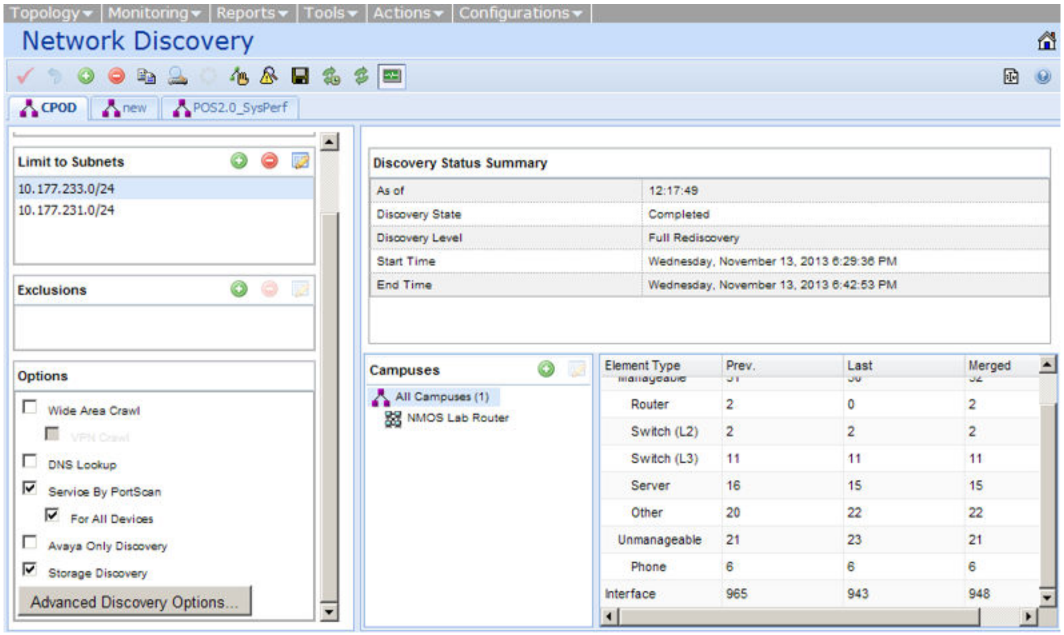
To have VPFM automatically discover these applications, you must include the media application server in the discovery recipe. You must also configure the device credentials for the media application server in the Device Credentials panel. The applications discovered are displayed in the Network Browser; select the Applications perspective to view them.

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

Manual device discovery

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



Limit to Subnets

10.177.233.0/24
10.177.231.0/24

Exclusions

Options

☐ Wide Area Crawl
☐ VPN Crawl
☐ DNS Lookup
☑ Service By PortScan
☑ For All Devices
☐ Avaya Only Discovery
☑ Storage Discovery

Discovery Status Summary

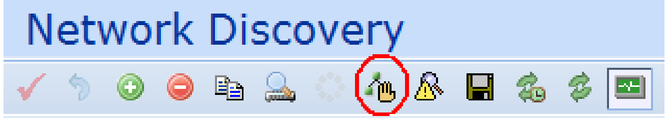
As of	12:17:49
Discovery State	Completed
Discovery Level	Full Rediscovery
Start Time	Wednesday, November 13, 2013 6:29:36 PM
End Time	Wednesday, November 13, 2013 6:42:53 PM

Campuses

All Campuses (1)
NMOS Lab Router

Element Type	Prev.	Last	Merged
Manageable	31	30	32
Router	2	0	2
Switch (L2)	2	2	2
Switch (L3)	11	11	11
Server	16	15	15
Other	20	22	22
Unmanageable	21	23	21
Phone	6	6	6
Interface	965	943	948

The manual device discovery control bar button is enabled 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 can use manual discovery when you want to add one or more devices to the discovery, without performing a complete rediscovery. 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 VPFM
- network previously not configured to allow auto discovery of new device(s) by VPFM
- 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

Scopes

A scope (device classification) defines a set of discovery domain elements and or events based on several criteria. Scopes are used 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.

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.
- Revert - 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.
- Remove (Delete) - Remove a scope. You cannot delete built-in scopes. A prompt appears to confirm deletion of the scope.
- Rename - Change the name of a selected scope.
- Clone - Create a duplicate of an existing scope to facilitate the creation of a new, similar scope.
- Hierarchical/Alphabetical toggle - You can toggle the way in which scopes are listed. The Hierarchical view lists scopes in a tree, organized hierarchically according to the domain elements that each scope encompasses. The Alphabetical view shows a flat list of scopes, sorted alphabetically by name.
- Disable/Enable text view mode - You can 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 - You 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.

Scopes can be configured 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 allow you to create and edit scopes.

Types of scopes

There are three types of scopes:

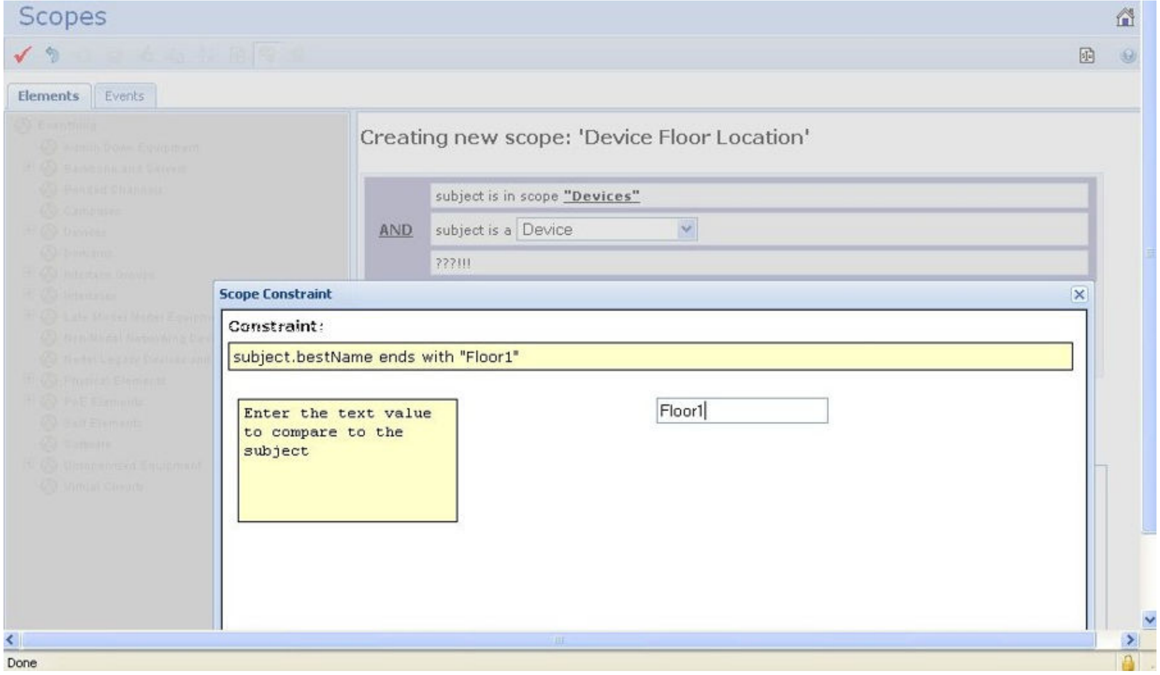
- Constraint-based scopes are defined by a set of elements that meet specified criteria. Both domain element scopes and event scopes may be of the constraint-based scope type.
- Union-based scopes are the union of at least two existing scopes. Both domain element scopes and event scopes may be of the 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.

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, which might not share any common attributes apart form the domain. Create a union-based when you want a new scope which is based on a combination of two or more existing scopes.

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.

The following image is an example of a constraint based scope.



Creating new scope: 'Device Floor Location'

subject is in scope "Devices"

subject is a Device

???!!!

Constraint:

subject.bestName ends with "Floor1"

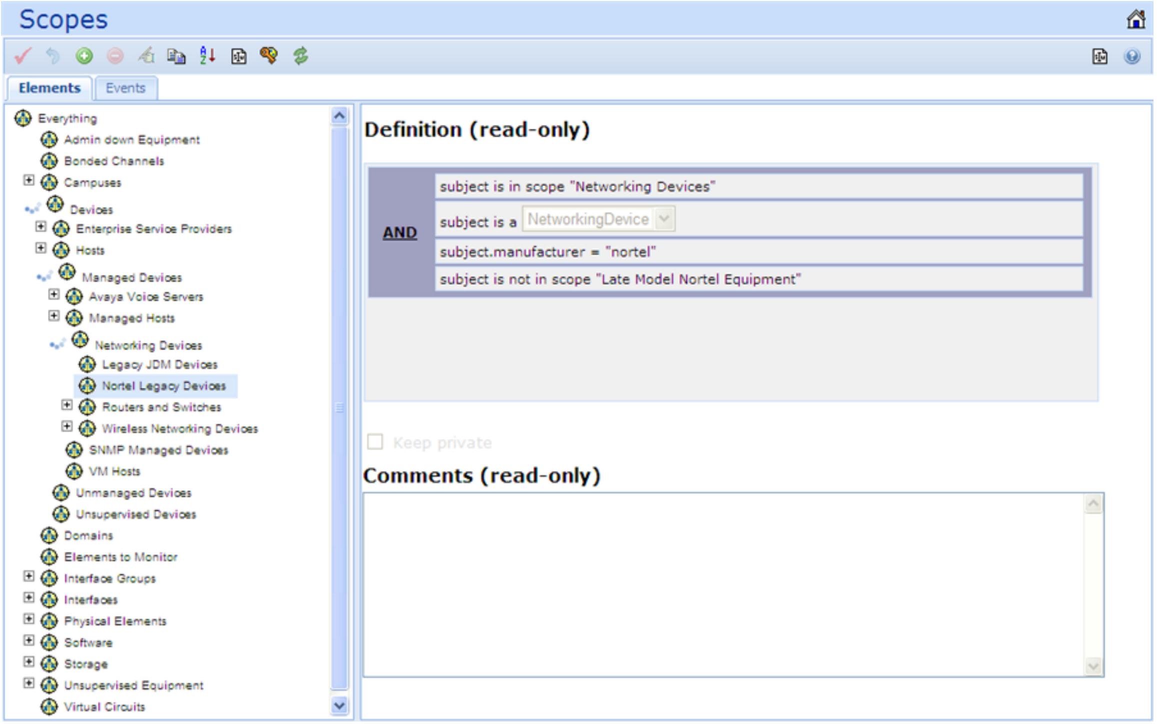
Enter the text value to compare to the subject

Floor1

Legacy devices monitoring scopes

Monitoring support is accomplished in part by the addition of at least one new monitoring configuration and at least one new scope for legacy devices. Additional availability reports for legacy devices are available in the Nortel legacy device scope.

The following is an example of a legacy device scope.



Definition (read-only)

AND
subject is in scope "Networking Devices"
subject is a NetworkingDevice
subject.manufacturer = "nortel"
subject is not in scope "Late Model Nortel Equipment"

☐ Keep private

Comments (read-only)

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.

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

- Apply - All edits to overrides are client-side only. Pressing the Apply button saves the edits to the server.
- Revert - Unapplied edits to an override can be undone by pressing the Revert button. No confirmation will be offered and unapplied edits are immediately lost.
- Add - Add a new override.
- Remove - Deletes an existing override.
- Rename - Allows you to rename an existing override.
- Clone - 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.

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.

Important:

When you define an event processing override (either global or scoped), the override does not take effect for a domain element if there are existing events of the same type posted against that domain element. You should 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).
- 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.
- Parameter overrides - Provides a list of the existing parameter overrides. Includes links that enable users to edit existing override values.

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. Avaya Visualization Performance and Fault Manager (VPFM) supports a number of different action types.

VPFM 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 / JDM tools.
- Run Remote Monitoring Script as plug in on KHI threshold.

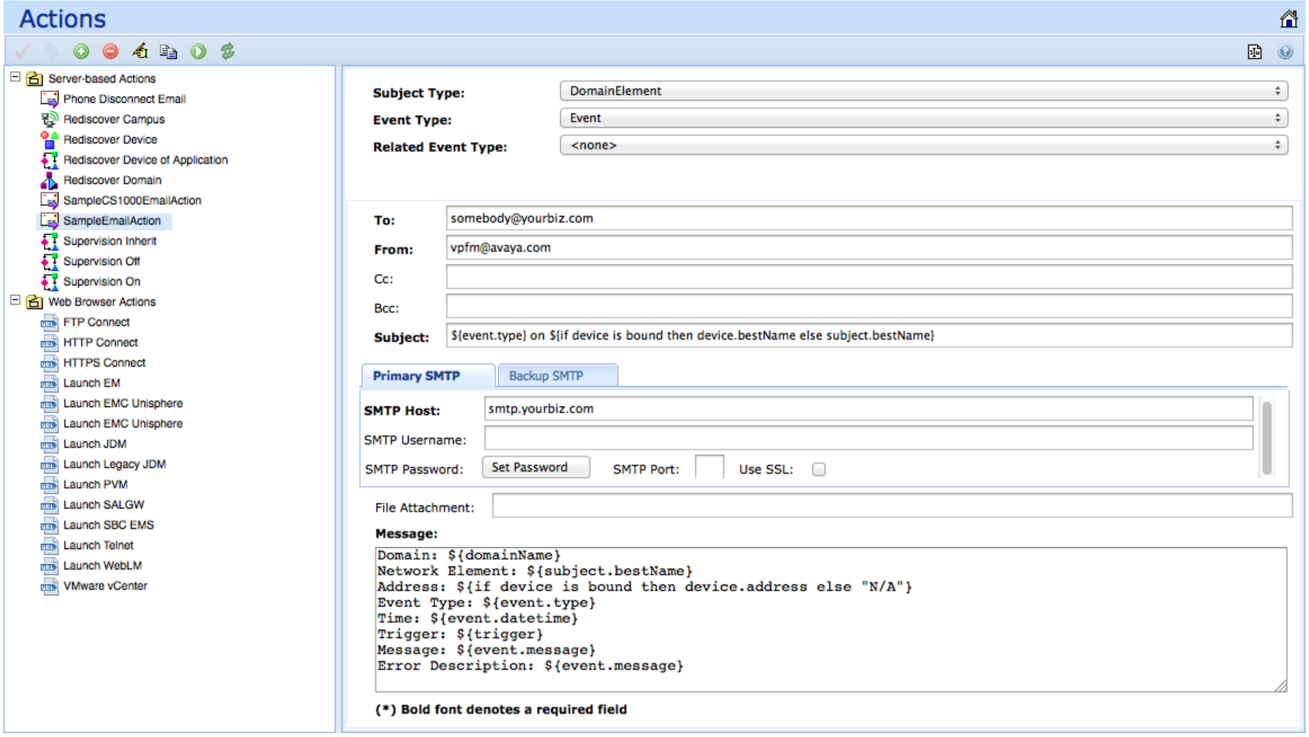
VPFM provides the following templates for scripting and mail:

- RMS scripts that are wizard driven for ease of use.
- Email templates with variable building blocks.

If you use VPFM API, you can generage mobile Apps.

For more information about writing custom scripts for VPFM actions, or obtaining a development kit for VPFM API, contact Avaya Global Services at http://www.avaya.com.

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



Subject Type: DomainElement

Event Type: Event

Related Event Type: <none>

To: somebody@yourbiz.com

From: vpfm@avaya.com

Cc:

Bcc:

Subject: ${event.type} on ${if device is bound then device.bestName else subject.bestName}

SMTP Host: smtp.yourbiz.com

SMTP Username:

SMTP Password: Set Password SMTP Port: Use SSL: □

File Attachment:

Message:

```
Domain: ${domainName}
Network Element: ${subject.bestName}
Address: ${if device is bound then device.address else "N/A"}
Event Type: ${event.type}
Time: ${event.datetime}
Trigger: ${trigger}
Message: ${event.message}
Error Description: ${event.message}
```

(*) Bold font denotes a required field

- Apply - All edits to actions are client-side only. Pressing the Apply button saves the edits to the server.

- Revert - Unapplied edits to an action can be undone by pressing the Revert button. No confirmation will be offered and unapplied edits are immediately lost.
- Add—Create a new action. The available actions will depend on the selected group.
- Delete—Deletes an existing action.
- Rename—Allows you to rename an existing action.
- Clone—Duplicates an existing action.
- Execute—Executes the action.
- Refresh—Refreshes the actions list.

Action types

The following actions are available in VPFM:

- 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.
- SNMPv1 Trap initiates an SNMPv1 trap.
- SNMPv2 Notification initiates an SNMPv2 notification.
- Custom Action permits advanced customizing of action.
- 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.

There are two types of actions: Server-based Actions and Web Browser Actions.

Server-based actions are actions that are executed from the VPFM 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 browser.

Command Action

A command action executes command scripts using scripting languages such as sh or DOS batch files.

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.
- 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 new tab is added 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.
- Raise Script in Selection Order - Enables you to move the current script to a higher position in the selection order.
- Lower Script in Selection Order - Enables you to move the current script to a lower position in the selection order.
- Delete Script - Deletes the selected script definition.

Email Action

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 the 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 recipient's inbox 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.
- Primary SMTP - enables you to specify the primary SMTP Host (required, the name of the mail server, running SMTP), SMTP Username (the username associated with the SMTP user

account that sends the message), SMTP Password (the password for the SMTP user account that sends the message), SMTP Port (the default port—can be changed for secure SMTP), and SSL for selecting secure SMTP.

- Backup SMTP - enables you to specify the backup SMTP Host (required, the name of the mail server, running SMTP), Backup SMTP Username (the username associated with the SMTP user account that sends the message), Backup SMTP Password (the password for the SMTP user account that sends the message), Backup SMTP Port (the default port—can be changed for secure SMTP), and Backup SSL for selecting secure SMTP.
- File Attachment - The file name and path of an optional attachment that is to be sent with the email.
- Message - (Required) The message.

SNMPv1 Trap

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.
- 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.
- Trap Type - Valid values include 0-Cold Start (the device that originates the trap has rebooted), 1- Warm Start (the device that originates the trap has been reset), 2-Link Down (the affected interface is not in service), 3-Link Up (the affected interface is in service), 4-Authentication Failure (the device has received a message that lacks the correct authentication), 5-EGP Neighbor Loss (the exterior gateway protocol neighbor to which a PDU was sent is no longer a neighbor), and 6-Enterprise Specific (an event has taken place that is specific to an enterprise MIB).
- Specific Type - If the Trap Type is Enterprise Specific, this value is an integer corresponding to the specific enterprise trap being sent.
- Enterprise OID - (Required) The trap's text-based object ID.
- Equipment Address - The name SNMP uses for the device.
- 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 SNMPv1 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 SNMPv1 trap action definition.

Custom actions

If you have advanced knowledge of VPFM, you can customize actions. If you require assistance, contact Avaya Global Services.

The following options apply to create custom actions:

- Subject Type—(Required) Displays a subject type from a pull down menu. For example, if the subject of this action is a network device, choose Device.
- Event Type—(Required) Displays an event type from the drop down menu.
- Action Class Name—(Required) Action classes are defined in the VPFM knowledge base. There are many actions listed in the VPFM knowledge base; an example of an action class is, DiscoveryLogMaintenance (scans the discovery log folder of a domain and keeps a certain number of logs).
- Reload Action class—(Optional) If checked, the action class is reloaded every time the action is executed. Bindings is used to input name value bindings for the action; for example, in DiscoveryLogMaintenance action class, the name is maxLogsToRetain and the value is an integer greater than 0.

Rediscovery Action

If a rediscovery action is selected (or being edited), the following fields display (or can be edited) in the right panel of the Actions Configuration Editor:

- Rediscovery Policy - Drop-down selection list of available rediscovery policies to use when the rediscovery action is executed. Rediscovery actions can be used in action schedules to rediscover a domain according to a user-specified schedule.

Config Control Action

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), and Override Configuration (displays Enable/Disable window where you can enable or disable individual override configurations).
- Changes to Make — Delete - Delete selected configuration control actions.

Campus Rediscovery Action

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.

Server-Based Actions

Server-based actions will always be dispatched for execution to the server process. The following built-in server-based actions are included:

- Rediscover Campus—Automates the rediscovery of a campus.
- Rediscover Device—Automates the rediscovery of a device.
- Rediscover Domain—Automates the rediscovery of a domain.
- SampleEmailAction—Provides a sample email 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.
- 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 back on the supervision of network elements after a planned shutdown.
- Supervision Restore—Reverts to monitoring in the original state.
- Supervision Inherit—Inherits supervision settings from an higher level of the domain element class hierarchy.
- SampleCS1000EmailAction—Provides a sample email action for Avaya CS 1000. This is similar to SampleEmailAction, but customized for Avaya CS 1000 and required for the OTM replacement feature.

Web Browser Actions

Web browser actions are actions that are executed from the client browser, and are therefore affected by the browser settings.

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 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 JDM — Downloads and launches Avaya JDM from the VPFM server.
- Launch Legacy JDM — Downloads and launches Legacy JDM from the VPFM server.
- Launch Telnet — Opens a telnet connection.

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 a user's inbox as:

A FanWarning has been acknowledged on 172.16.67.23

You can sometimes just use an identifier directly when it 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}.

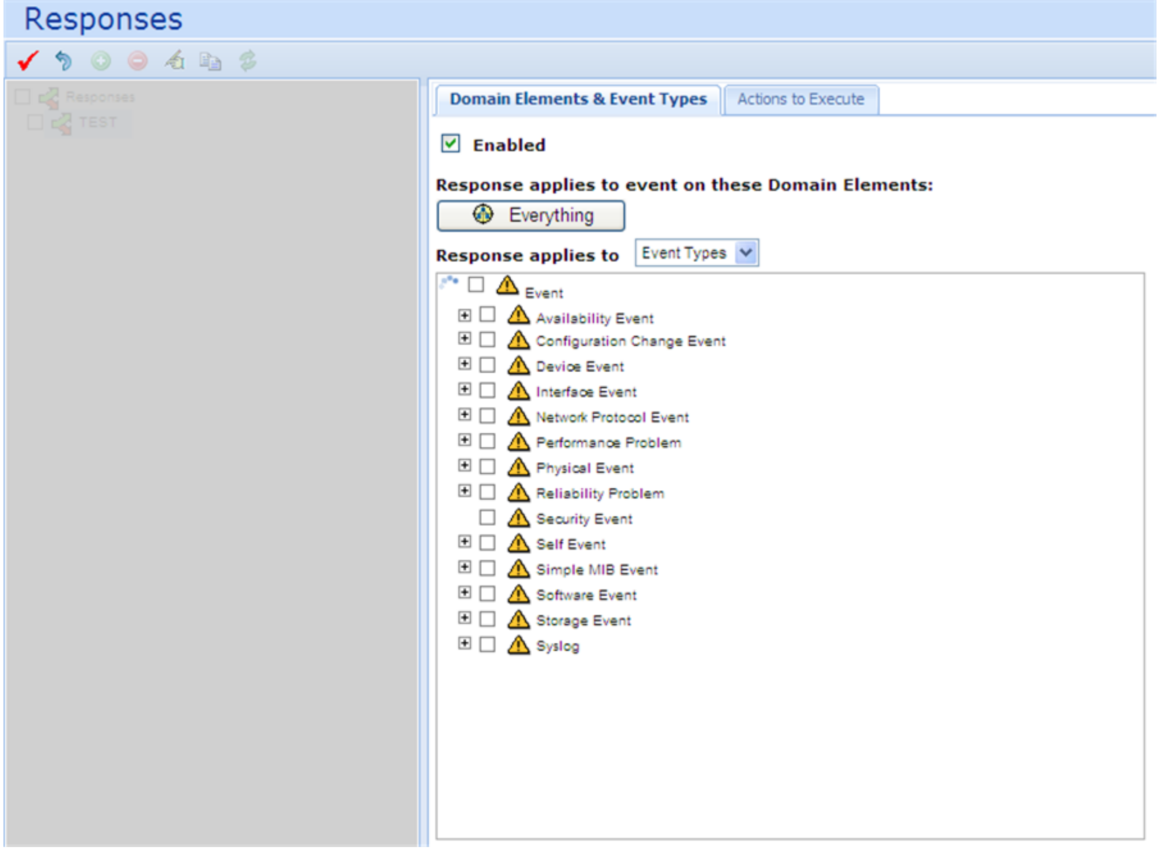
The properties defined for an identifier (if any) vary depending on the type of the identifier.

For ease of adding contextual variable information, VPFM prompts the completion of the valid variables in the context. For example, after typing "${device.", VPFM 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.

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



☑ Enabled

Response applies to event on these Domain Elements: Everything

Response applies to: Event Types

- □ Event
  - □ Availability Event
  - □ Configuration Change Event
  - □ Device Event
  - □ Interface Event
  - □ Network Protocol Event
  - □ Performance Problem
  - □ Physical Event
  - □ Reliability Problem
  - □ Security Event
  - □ Self Event
  - □ Simple MIB Event
  - □ Software Event
  - □ Storage Event
  - □ Syslog

- Apply - All edits to responses are client-side only. Pressing the Apply button saves the edits to the server.
- Revert - Unapplied edits to a response can be undone by pressing the Revert button. No confirmation will be offered and unapplied edits are immediately lost.
- Add - Add a new response.
- Remove - Deletes an existing response.
- Rename - Allows you to rename an existing response.
- Clone - Duplicates an existing response.
- Refresh - Refreshes the responses list.

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. 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 Apples 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, enabling 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). The Actions to Execute Tab displays the following options when a response is selected or edited:

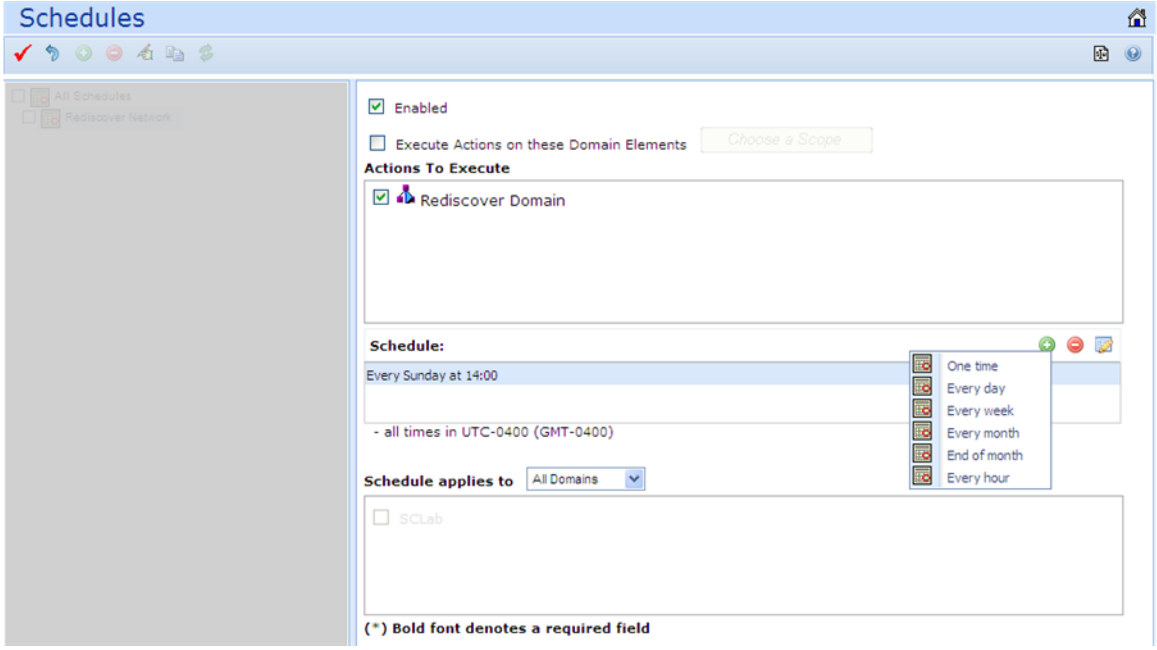
- Response is Triggered When – Displays a list of properties that can be used to trigger responses which include:
- An event is posted (triggers a response when an event has been posted to the message board)
- An event is acknowledged (triggers a response when an event is acknowledged by a user)
- An 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

The Action window enables you to define a schedule that VPFM follows to perform one or more actions at a specified time or interval. To access the Action Scheduler page, from the VPFM menu bar, select **Actions** > **By Schedule**.

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:



☑ Enabled

□ Execute Actions on these Domain Elements

Actions To Execute

☑ Rediscover Domain

Schedule:

Every Sunday at 14:00

- all times in UTC-0400 (GMT-0400)

Schedule applies to All Domains

□ SCLab

(*) Bold font denotes a required field

- Apply - All edits to schedules are client-side only. Pressing the Apply button saves the edits to the server.
- Revert - Unapplied edits to an action schedule can be undone by pressing the Revert button. No confirmation will be offered and unapplied edits are immediately lost.
- Add - Add a new action schedule.
- Remove - Deletes an existing action schedule.
- Rename - Allows you to rename a selected action schedule.
- Clone - Duplicates an existing action schedule.
- Refresh - Refreshes the responses list.

The following fields display on the right-side panel of the Action Scheduler page when editing or viewing an action schedule:

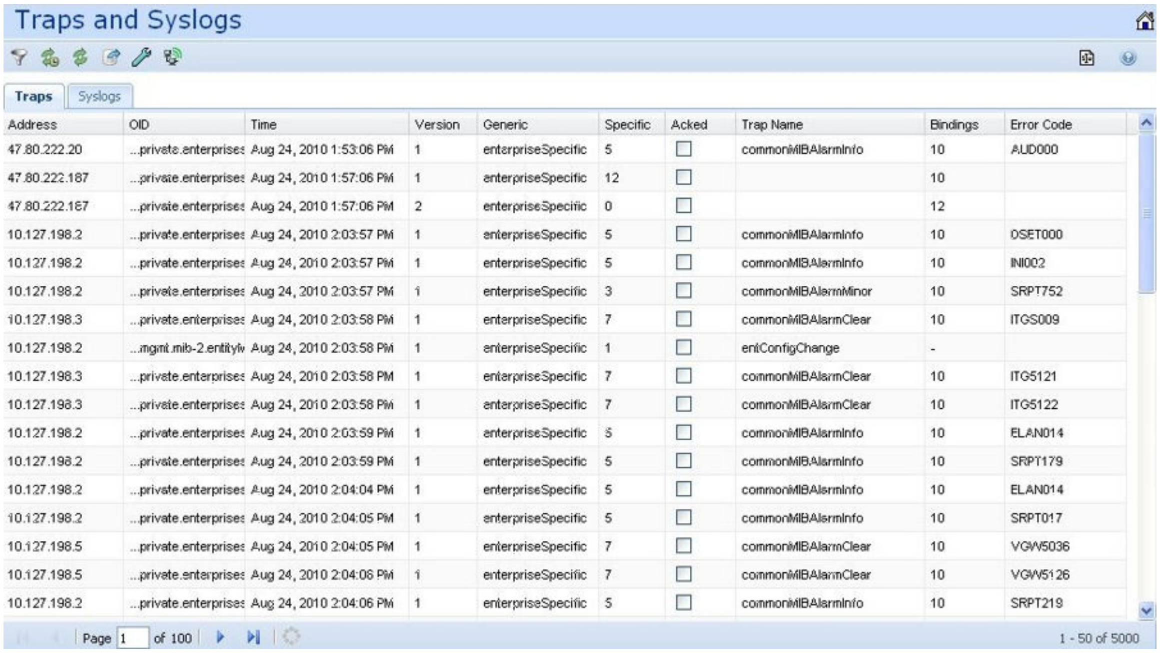
- Enabled - Enables you to toggle the action schedule on or off (default is on).
- Execute Actions on these Domain Elements - Combo-box that enables you to select the domain elements for which the scheduled action is to apply.

- 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 at which the action must be executed. Interval options are:
- One Time (executes the action only once at the date and time specified)
- Everyday (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)

Traps, Syslogs, and Events

On the Traps and Syslogs page you can view information SNMP traps and syslogs reports. You can also configure how you view the traps and syslogs. To access the Traps and Syslogs page, from the VPFM menu bar, select **Tools** > **Trap & Syslog Browser**.

The following general controls are available on the Traps and Syslogs page.



Traps and Syslogs

Address	OID	Time	Version	Generic	Specific	Acked	Trap Name	Bindings	Error Code
47.80.222.20	...private.enterprises	Aug 24, 2010 1:53:06 PM	1	enterpriseSpecific	5	□	commonMIBAlarmInfo	10	AUD000
47.80.222.187	...private.enterprises	Aug 24, 2010 1:57:06 PM	1	enterpriseSpecific	12	□		10	
47.80.222.167	...private.enterprises	Aug 24, 2010 1:57:06 PM	2	enterpriseSpecific	0	□		12	
10.127.198.2	...private.enterprises	Aug 24, 2010 2:03:57 PM	1	enterpriseSpecific	5	□	commonMIBAlarmInfo	10	OSET000
10.127.198.2	...private.enterprises	Aug 24, 2010 2:03:57 PM	1	enterpriseSpecific	5	□	commonMIBAlarmInfo	10	INI002
10.127.198.2	...private.enterprises	Aug 24, 2010 2:03:57 PM	1	enterpriseSpecific	3	□	commonMIBAlarmMinor	10	SRPT752
10.127.198.3	...private.enterprises	Aug 24, 2010 2:03:58 PM	1	enterpriseSpecific	7	□	commonMIBAlarmClear	10	ITGS009
10.127.198.2	...mgmt.mib-2.entityM	Aug 24, 2010 2:03:58 PM	1	enterpriseSpecific	1	□	entConfigChange	-	
10.127.198.3	...private.enterprises	Aug 24, 2010 2:03:58 PM	1	enterpriseSpecific	7	□	commonMIBAlarmClear	10	ITG5121
10.127.198.3	...private.enterprises	Aug 24, 2010 2:03:58 PM	1	enterpriseSpecific	7	□	commonMIBAlarmClear	10	ITG5122
10.127.198.2	...private.enterprises	Aug 24, 2010 2:03:59 PM	1	enterpriseSpecific	5	□	commonMIBAlarmInfo	10	ELAN014
10.127.198.2	...private.enterprises	Aug 24, 2010 2:03:59 PM	1	enterpriseSpecific	5	□	commonMIBAlarmInfo	10	SRPT179
10.127.198.2	...private.enterprises	Aug 24, 2010 2:04:04 PM	1	enterpriseSpecific	5	□	commonMIBAlarmInfo	10	ELAN014
10.127.198.2	...private.enterprises	Aug 24, 2010 2:04:05 PM	1	enterpriseSpecific	5	□	commonMIBAlarmInfo	10	SRPT017
10.127.198.5	...private.enterprises	Aug 24, 2010 2:04:05 PM	1	enterpriseSpecific	7	□	commonMIBAlarmClear	10	VGW5036
10.127.198.5	...private.enterprises	Aug 24, 2010 2:04:06 PM	1	enterpriseSpecific	7	□	commonMIBAlarmClear	10	VGW5126
10.127.198.2	...private.enterprises	Aug 24, 2010 2:04:06 PM	1	enterpriseSpecific	5	□	commonMIBAlarmInfo	10	SRPT219

- Autorefresh - Enables users to specify the time interval at which trap information is refreshed. The Autorefresh button, when clicked, displays a popup window that enables users to select the appropriate refresh interval.
- Refresh - Refreshes the traps table.
- Export records - Enables users to export traps records as an .xml document.
- Settings - Enables users to specify traps configuration that control how trap information is stored in and removed from the VPFM 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, the packets per second, packets received and status.
- Traps - Displays a tabular view of trap data.
- Syslogs - Displays a tabular view of syslog data.

Filter is also available on this page. It enables you to create filters for viewing traps and syslogs based on selected criteria. The following filters are available for traps:

- IP - Filters traps based on the IP address of the device from which it was sent. Wildcards are accepted.
- OID - Filters traps based on the object ID of the trap.
- Interval - Filters the displayed traps based on the time received. (For example, last day or last minute)
- Generic - Filters traps based on predefined, generic trap class (for example, coldStart, warmStart, linkUp, linkDown).
- Specific - Filters displayed traps based on the specific trap.
- SNMP Version - Filters traps based on the SNMP version of the trap.

- Ack - Filters the displayed Traps based on their Acknowledgement Status (Acked or Not Acked).

The following filters are available for syslogs:

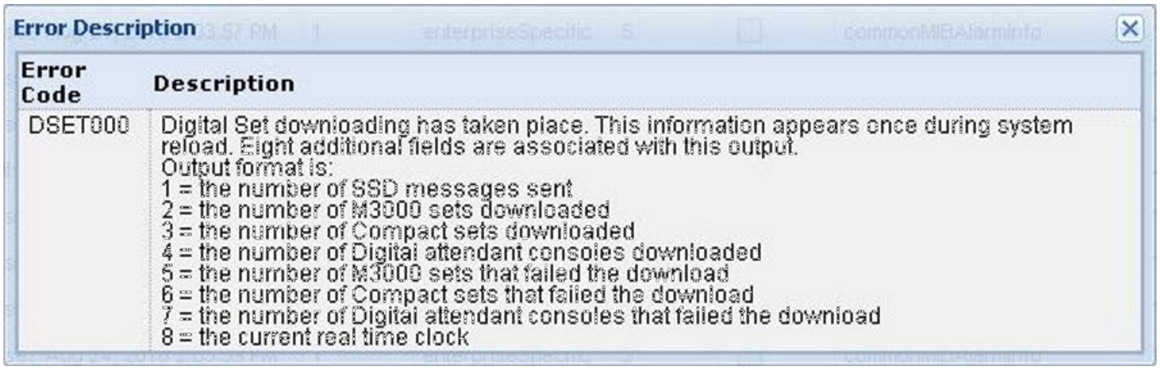
- Subject Address - Filters syslogs based on the IP address of the device from which it was sent.
- Facility - Filters syslogs based on the facility that generated the syslog. For example: kernel, user, mail, uucp, or clock.
- Severity - Filters syslogs based on severity: emergency, alert, critical, error, warning, notice informational, or debug.
- Text - Filters syslogs based on specified text contained within the syslog.
- Interval - Filters syslogs based on the time received.
- Ack - Filters the displayed syslogs based on their Acknowledgement Status (Acked or Not Acked).
- Device Time - Filters out the displayed syslogs based on the Server Time column. For example, Last Day, Last Minute, or Last Hour.

Traps tab

The Trap Viewer table displays a list of traps that have been issued in the network. The following columns display in the trap table:

- Address - The port on which to listen for traps and notifications (default is 162).
- OID - the ID of the SNMP object for which you want to send a notification.
- Time - The date and time the trap was generated.
- Version - The trap version.
- Generic - Indicates a number of generic trap types.
- Specific - Indicates a number of specific trap types.
- Acked - Indicates if the trap is acknowledged.
- Trap name - name of the trap.
- Bindings - The number of object IDs (OID) associated with the trap.
- Error Code - 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.



Error Description

Error Code	Description
DSET000	Digital Set downloading has taken place. This information appears once during system reload. Eight additional fields are associated with this output. Output format is: 1 = the number of SSD messages sent 2 = the number of M3000 sets downloaded 3 = the number of Compact sets downloaded 4 = the number of Digital attendant consoles downloaded 5 = the number of M3000 sets that failed the download 6 = the number of Compact sets that failed the download 7 = the number of Digital attendant consoles that failed the download 8 = the current real time clock

Syslogs tab

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 displays a table of syslogs for your network. The following columns display in the syslogs table:

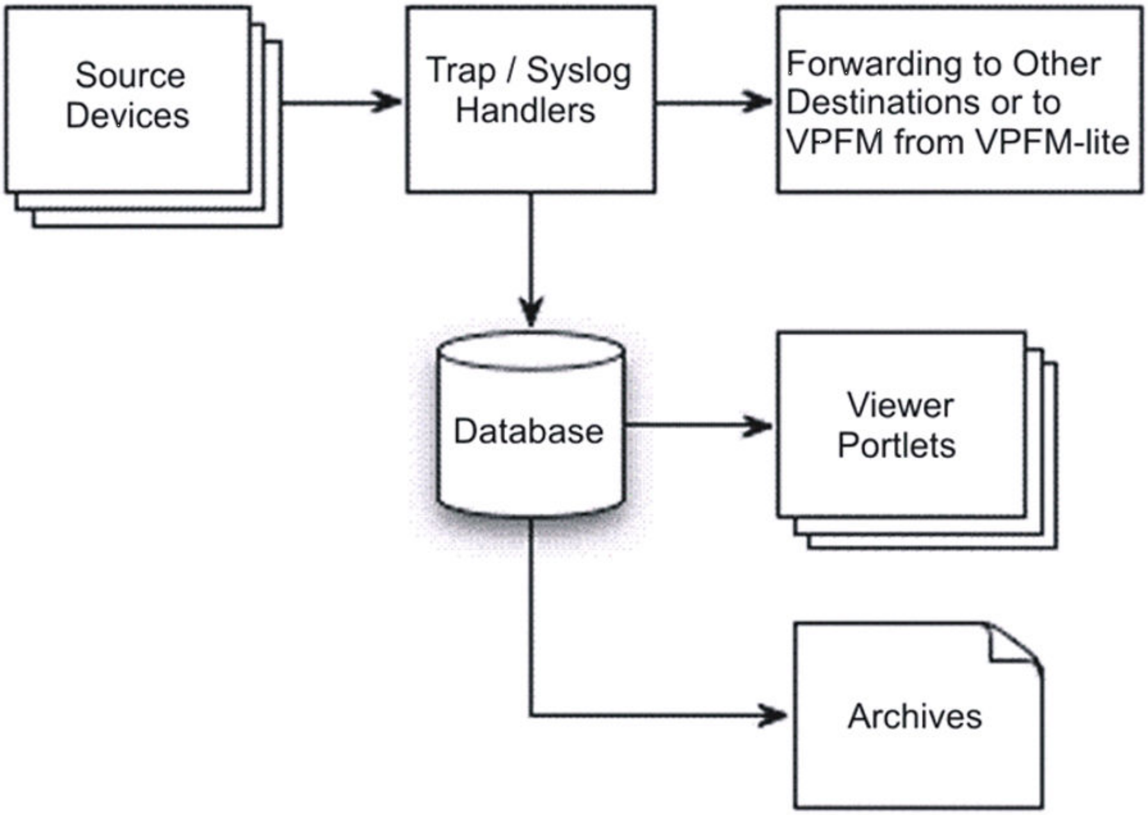
- Server Time - The time the VPFM server received the syslog.
- Device Time - The time on the device when it sent the syslog to VPFM. The device time can be different than the server time if your network devices are in different time zones than your VPFM server.
- Address - The IP address associated with the syslog.
- Facility - The facility associated with the syslog.
- Severity - The severity of the syslog.
- Text - The syslog text.
- Acked - Indicates whether or not the syslog has been acknowledged.

Data flow in Traps and Syslogs

The following figure describes the data flow of traps/syslog information. Traps and syslog information is sent to the host where the VPFM service is running. Once received, they are processed and stored/archived/viewed according to various options.

In VPFM, a VPFM-lite collects the Avaya CS 1000 traps and forwards the Avaya CS 1000 traps to the VPFM master. VPFM-lite is configured to forward Avaya CS 1000 traps. For more information, see Configuring VPFM-lite for forwarding traps to VPFM on page 109.

The general flow of information is as follows:



In terms of Traps/Syslogs Configuration options, the data flow proceeds as follows:

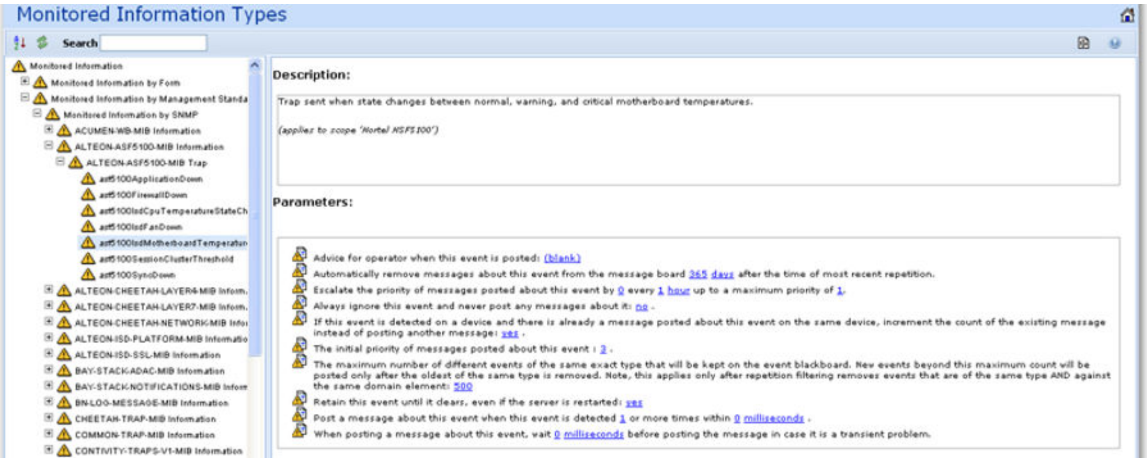
- Listening - You can configure the VPFM or VPFM-lite through the Traps/Syslogs Configuration to listen to non-default ports. If you do this, the VPFM listens on default ports 162/514 if they are available and the VPFM can get them from the operating system.
- Forwarding - You can configure VPFM or VPFM-lite to forward to multiple destinations.
- Storage to VPFM Database - The VPFM can apply three kinds of filters to control the information that gets stored in the VPFM database (and what information is ignored). Traps/ syslogs that are filtered out still get forwarded.
- Viewing - Trap/Syslog view portlets provide many ways of filtering what you see from the VPFM database. You can view by property value (for example, you can show only traps/ syslogs unacknowledged or show only traps/syslogs from a certain IP address range). You can view by age (for example, you can show only those from the last hour). Note: Filters have no effect on what information is stored in the VPFM database.
- Purge and Archive - VPFM services periodically purge the VPFM database and archive the oldest traps/syslogs.

MIT

A Monitored Information Type (MIT) is any data that VPFM 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 VPFM 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.

To configure MIT, from the VPFM menu bar, select **Configurations** > **Monitored Information Types**.

The following general controls are available on the Monitoring Information Types page:


Monitored Information Types
Search
Monitored Information
Monitored Information by Form
Monitored Information by Management Standa
Monitored Information by SNMP
ACUMEN-WB-MIB Information
ALTEON-ASF5100-MIB Information
ALTEON-ASF5100-MIB Trap
asf5100ApplicationDown
asf5100FirewallDown
asf5100IsdCpuTemperatureStateCh
asf5100IsdFanDown
asf5100IsdMotherboardTemperatur
asf5100SessionClusterThreshold
asf5100SyncDown
ALTEON-CHEETAH-LAYER4-MIB Inform.
ALTEON-CHEETAH-LAYER7-MIB Inform.
ALTEON-CHEETAH-NETWORK-MIB Infor
ALTEON-ISD-PLATFORM-MIB Informatio
ALTEON-ISD-SSL-MIB Information
BAY-STACK-ADAC-MIB Information
BAY-STACK-NOTIFICATIONS-MIB Inform
BN-LOG-MESSAGE-MIB Information
CHEETAH-TRAP-MIB Information
COMMON-TRAP-MIB Information
CONTIVITY-TRAPS-V1-MIB Information

Description:

Trap sent when state changes between normal, warning, and critical motherboard temperatures.

(applies to scope 'Nortel NSF5100')

Parameters:

Advice for operator when this event is posted: (blank)

Automatically remove messages about this event from the message board 365 days after the time of most recent repetition.

Escalate the priority of messages posted about this event by 0 every 1 hour up to a maximum priority of 1.

Always ignore this event and never post any messages about it: no .

If this event is detected on a device and there is already a message posted about this event on the same device, increment the count of the existing message instead of posting another message: yes .

The initial priority of messages posted about this event : 3 .

The maximum number of different events of the same exact type that will be kept on the event blackboard. New events beyond this maximum count will be posted only after the oldest of the same type is removed. Note, this applies only after repetition filtering removes events that are of the same type AND against the same domain element: 500

Retain this event until it clears, even if the server is restarted: yes

Post a message about this event when this event is detected 1 or more times within 0 milliseconds .

When posting a message about this event, wait 0 milliseconds before posting the message in case it is a transient problem.

- Hierarchical/Alphabetical – 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 in to VPFM that characterize 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 VPFM MIT hierarchy supports multiple inheritance, so you will 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 Subject - Organizes MITs according to what they affect (such as device). For example, you will find InterfaceUtilizationProblem under both OverUtilizationProblem (which is a sub-event type of PerformanceProblem) and under InterfaceEvent
- 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 will

have further subtypes based on different MIBs and the events are grouped depending on which MIB they are derived.

VPFM provide self events to inform you about changes to the server configuration and other state changes in server processing. Self events are implemented 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. Self Elements can be used for message board filtering to only display self events, for example. You may also configure responses to self events. Actions that are connected to self events must be created as server based actions.

Each monitored information type has a description and a set of configurable parameters associated with it. 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 there is more than one parent with the same parameter).

Often, an MIT will have a predefined override value for a parameter that it 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.

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 which 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

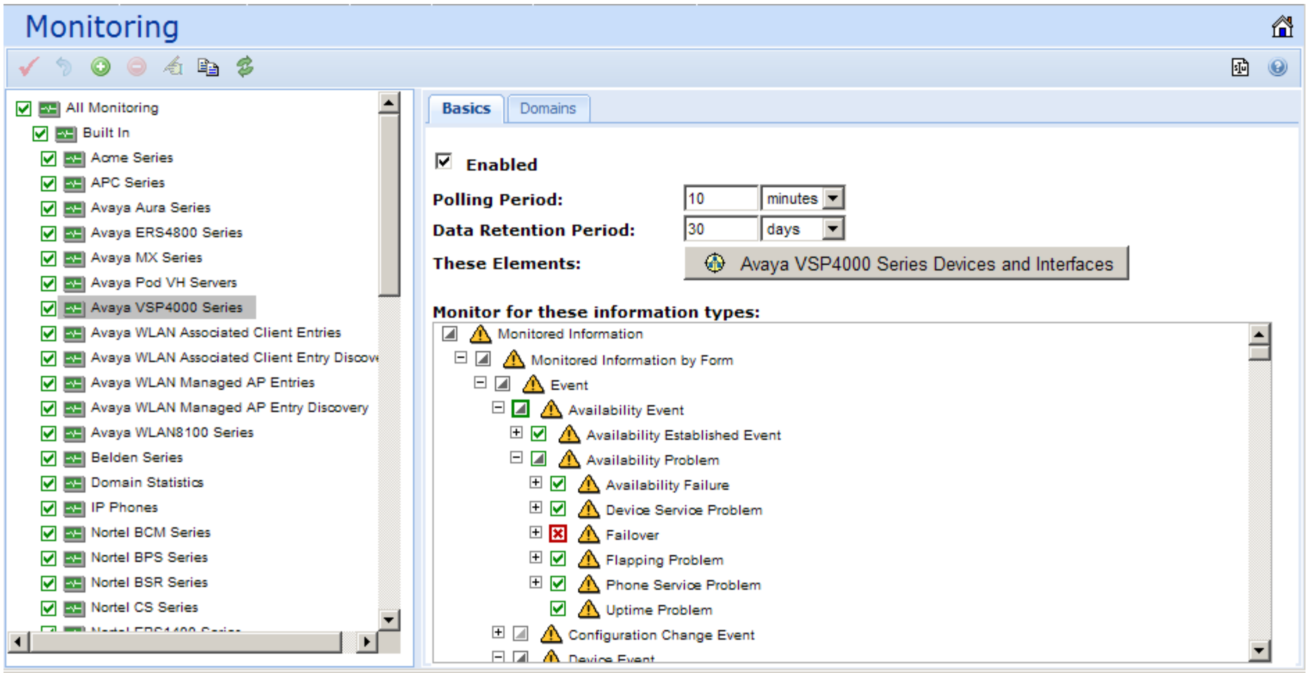
Search 3

Search term: act*fa

Search Results: Action Failure

MIT selection tool

You can use the MIT selection tool when configuring monitoring. To access this tool, navigate to **Configurations > Monitoring** and view it from the **Monitor for these information types** section of the monitoring configuration window, as shown below.



☑ Enabled

Polling Period: 10 minutes

Data Retention Period: 30 days

These Elements: Avaya VSP4000 Series Devices and Interfaces

Monitor for these information types:

The MIT selection tool displays a hierarchy of MITs with a selection box next to each. The box color, thickness, and the icons they contain indicate the selected or deselected state of the MIT and its children.

Rules

The entries are arranged in an inheritance hierarchy with multiple inheritance rules, which are as follows:

- Selecting a parent causes its children to be selected and also the reverse (unless overridden).
- A child can inherit from multiple parents. Changes in one part of the tree can affect other parts of the tree.
- The thickness of the box indicates whether it is explicit (thick) or implicit (thin).
- The selection state indicates whether the MIT is ON, OFF, or Unspecified.
- The enablement state indicates whether or not an MIT will be monitored, as follows:
    - Selection ON = Enabled

  - Selection OFF = Disabled
  - Selection Unspecified = Disabled
- The box color indicates a selection state of self or ancestor, as follows:
  - Red, if the MIT selection state is OFF or if it inherits an OFF selection state from its ancestors.
  - Green, if the MIT selection state is ON or if it inherits an ON selection state from its ancestors.
  - Gray, if the MIT selection state is unspecified or if it does not inherit any selection state from its ancestors.
- The box contains a green check if MIT and all if its descendants have a selection state ON, without exception .
- The box contains a red x if MIT and all if its descendants have a selection state OFF, without exception.
- The box contains a triangle if the selection state of MIT and its descendants is heterogeneous, as follows:
  - Green triangle, if no descendants have a selection state OFF and at least one descendant has a selection state ON.
  - Red triangle, if no descendants have a selection state ON and at least one descendant has a selection state OFF.
  - Gray triangle, if descendants have a heterogeneous selection state including at least one ON and one OFF (the unspecified state cannot be the cause of a gray triangle).
- The box content is empty if the MIT is unspecified and all its descendants are unspecified.
- The triangle hue is dark if at least one descendant is explicitly selected or deselected. A dark hue is accompanied by tail.
- The hue can apply to gray, green, and red.

Key to boxes and icons

Icon	Description
☑	The MIT is explicitly selected (green, thick box) and all of its descendents have a selection state ON, without exception (green check mark).
☑	The MIT is implicitly selected (green, thin box) and all of its descendents have a selection state ON, without exception (green check mark).
☒	The MIT is explicitly deselected (red, thick box) and all of its descendents have a selection state OFF, without exception (red x mark).
☒	The MIT is implicitly deselected (red, thick box) and all of its descendents have a selection state OFF, without exception (red x mark).
◪	The MIT is implicitly selected (green, thin box) and no descendants have a selection state OFF and at least one descendant has a selection state ON (green triangle).
◪	The MIT is implicitly deselected (red, thin box) and no descendants have a selection state OFF and at least one descendant has a selection state ON (red triangle).

Table continues…

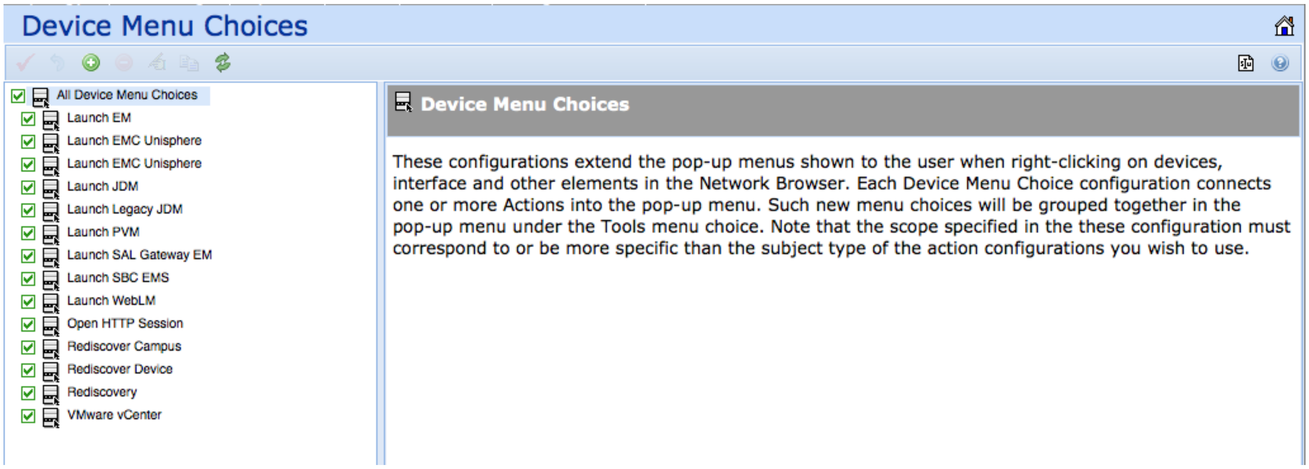
Icon	Description
◪	The MIT is of an unspecified state or does not inherit any selection state from its ancestors (gray, thin box) and descendants have a heterogeneous selection state including at least one ON and one OFF (gray triangle).
◪	The MIT is of an unspecified state or does not inherit any selection state from its ancestors (gray, thin box) and no descendants have a selection state OFF and at least one descendant has a selection state ON (green triangle).
◪	The MIT is of an unspecified state or does not inherit any selection state from its ancestors (gray, thin box) and no descendants have a selection state OFF and at least one descendant has a selection state ON (red triangle).
◪	The MIT is of an unspecified state or does not inherit any selection state from its ancestors (gray, thin box) and descendants have a heterogeneous selection state including at least one ON and one OFF (gray triangle).
□	The MIT is of an unspecified state or does not inherit any selection state from its ancestors (gray, thin box).
◪	The MIT is implicitly selected (green, thin box) and descendants have a heterogeneous selection state including at least one ON and one OFF (gray triangle).
◪	The MIT is explicitly selected (green, thick box) and descendants have a heterogeneous selection state including at least one ON and one OFF (gray triangle).
◪	The MIT is explicitly deselected (red, thick box) and descendants have a heterogeneous selection state including at least one ON and one OFF (gray triangle).
◪	The MIT is implicitly deselected (red, thin box) and descendants have a heterogeneous selection state including at least one ON and one OFF (gray triangle).

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 its manufacturer's proprietary management application, making it easier to modify the device configuration. 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, from the VPFM menu bar, select **Actions** > **By Device Menu Choice**. The following general controls are available on the Device Menu Choices page:



Device Menu Choices

☑ All Device Menu Choices
- ☑ Launch EM
- ☑ Launch EMC Unisphere
- ☑ Launch EMC Unisphere
- ☑ Launch JDM
- ☑ Launch Legacy JDM
- ☑ Launch PVM
- ☑ Launch SAL Gateway EM
- ☑ Launch SBC EMS
- ☑ Launch WebLM
- ☑ Open HTTP Session
- ☑ Rediscover Campus
- ☑ Rediscover Device
- ☑ Rediscovery
- ☑ VMware vCenter

Device Menu Choices

These configurations extend the pop-up menus shown to the user when right-clicking on devices, interface and other elements in the Network Browser. Each Device Menu Choice configuration connects one or more Actions into the pop-up menu. Such new menu choices will be grouped together in the pop-up menu under the Tools menu choice. Note that the scope specified in the these configuration must correspond to or be more specific than the subject type of the action configurations you wish to use.

- Apply - All edits to device menu choices are client-side only. Clicking the Apply button saves the edits to the server.
- Revert - 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—Add a new device menu choice.
- Remove—Remove a selected device menu choice.
- Rename—Rename a selected device menu choice.
- Clone—Clone a selected device menu choice.
- Refresh—Refresh 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 - Toggle the device menu choice on or off. You must select this check box to make the device menu choice active.
- Obtain user confirmation before executing - You can require user confirmation prior to performing the device menu choice.
- Attach actions to these 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 will not appear until you select the appropriate scope.
- Comments - Descriptive text associated with the device menu choice.

Monitoring configuration

Monitoring configurations define what events are received for which domain elements and with what alternative event processing options.

You can define multiple separate monitoring configurations so that each monitoring configuration has the following:

- its own interval
- its own set of events to monitor
- its own set of domain elements to monitor by scope (defined by selecting elements explicitly or by specifying one or more constraints for the set)
- its own specific event parameter overrides which can be different for each scope and explicit selection

For example, to monitor all servers for availability:

- the scope would be Servers
- the event would be Availability Problem

There are two types of monitoring configurations. The first type is the Built In configurations. The Built In configurations are the monitoring configurations that are predefined by VPFM. You can view the information for the Built In configurations, but you cannot edit them. If you want to change a predefined configuration, you must clone the configuration.

In the Built In Configurations, in the left panel, you can select the devices that you want to monitor.

The second type of monitoring configuration is User defined. You can add monitoring configurations and modify them for your system requirements.

To define a monitoring configuration, you specify a set of event types and a set of elements (a scope), and optionally one or more parameter overrides that modify the event processing behavior. To specify the set of elements covered by the monitoring configuration, you select a scope from the list of all scopes for your system. To specify the set of event types, you check off those event types or groups of event types to include or exclude using a tree structure selection tool.

In the case where two monitoring configurations overlap and only one specifies overrides, the overrides will apply to the common events and elements. In overlap cases with conflicting parameter overrides, behavior is non-deterministic, and a configuration error will be reported.

To configure monitoring, from the VPFM menu bar, select **Configurations** > **Monitoring**.

The following general controls are available on the Monitoring page:

- Apply - All edits to monitoring configuration are client-side only. Clicking the Apply button saves the edits to the server.
- Revert - Unapplied edits to a monitoring configuration are undone by clicking the Revert button. There is no confirmation and unapplied edits are immediately lost.
- Add - Adds a new monitoring configuration.
- Remove - Deletes an existing monitoring configuration.
- Rename - Enables the alteration of the name of an existing monitoring configuration.
- Clone - Duplicates an existing monitoring configuration.
- Refresh - Refreshes the monitoring configuration list.

The monitoring configuration form displays the following options:

- Enabled – Indicates whether or not polling (the process that VPFM uses to identify and monitor domain elements) is enabled. Default is on.
- Polling period - The interval at which polling occurs (if enabled).
- Data retention period - The length of time for which data is retained.
- These elements – Displays a list of scopes. If you select a scope from the list, the information types list is modified to display monitored information appropriate for the selected scope.
- Monitor for these information types - Displays a tree structure of monitored information types for the selected scope (the scope defined using the These Elements list) from which you can select individual events or categories of events for use with the monitoring configuration.

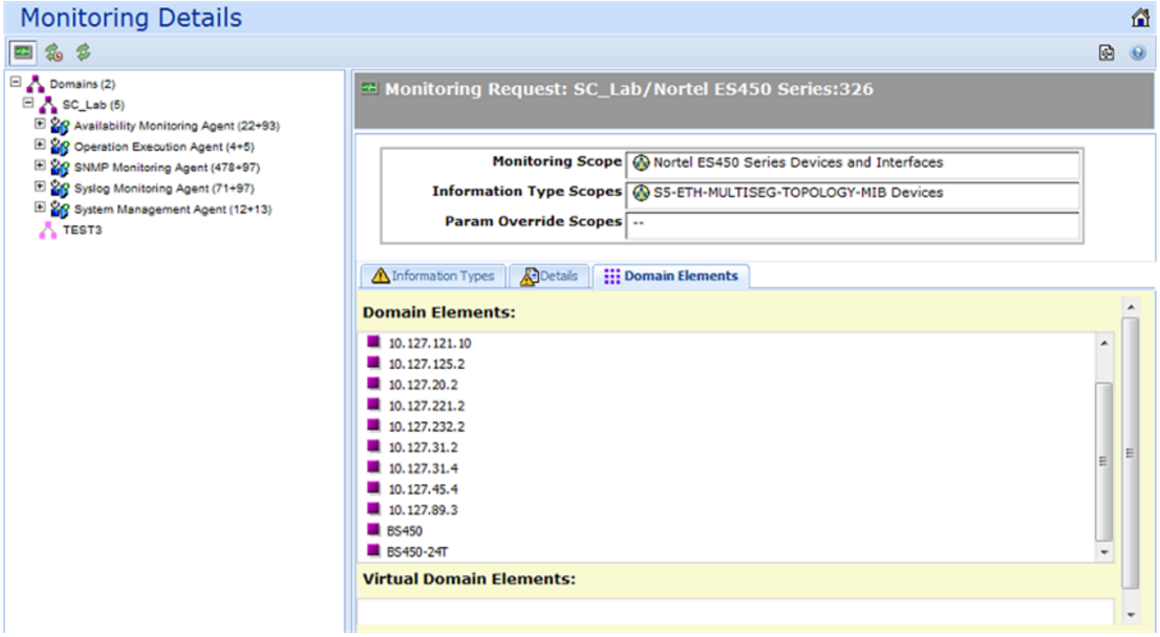
Monitoring details browser

You can use the Monitoring details browser to start and stop availability monitoring agents and SNMP monitoring agents for your VPFM system.

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

The monitoring details browser displays 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 monitoring details browser window 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 monitoring details browser window:



Monitoring Details

Domains (2)
SC_Lab (5)
Availability Monitoring Agent (22+93)
Operation Execution Agent (4+5)
SNMP Monitoring Agent (478+97)
Syslog Monitoring Agent (71+97)
System Management Agent (12+13)
TEST3

Monitoring Request: SC_Lab/Nortel ES450 Series:326

Monitoring Scope	Nortel ES450 Series Devices and Interfaces
Information Type Scopes	S5-ETH-MULTISEG-TOPOLOGY-MIB Devices
Param Override Scopes	--

Domain Elements:

10.127.121.10
10.127.125.2
10.127.20.2
10.127.221.2
10.127.232.2
10.127.31.2
10.127.31.4
10.127.45.4
10.127.89.3
BS450
BS450-24T

Virtual Domain Elements:

- Monitoring scope - (read-only) the set of domain elements at which the monitoring request is targeted explicitly.
- Information type scopes - (read-only) the set of domain elements encompassed by the information types specified.
- Parameter override scopes - lists the parameter overrides specified in the definition of the current monitoring operation.
- Information types tab - 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 element 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 monitoring details browser window.

UCM Device Credentials

From the Avaya Visualization Performance and Fault Manager (VPFM) top of the page menu bar, you can connect directly to the UCM Device and Server Credentials Editor by selecting **Configurations** > **UCM Device Credentials**.

From the UCM Device and Server Credentials Editor, you can configure device credentials.

For more information about configuring device credentials from the UCM Device and Server Credentials Editor, see *Avaya Unified Communications Management Common Services Fundamentals* (NN48014–100).

Chapter 4: Dashboard configuration

Visualization Performance and Fault Manager (VPFM) offers multiple levels of dashboards to monitor Avaya Aura 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 VPFM, and you can modify a dashboard to make it a default dashboard for a device.

There are three types of dashboards:

- Preconfigured — Includes the Network Overview which displays information about network health; the Power Savings dashboard which displays dashlets containing information about total network power savings and top switch watt reduction; and the 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 server.
- Customized — You can configure the dashboard by adding, deleting, or cloning a dashlet to delve deeper into the network health.

For more information about dashboards, see *Avaya Visualization Performance and Fault Manager Fault and Performance Management* (NN48014–700).

Adding a dashboard

Before you begin

You must be on the VPFM home page. After you click on the VPFM link from the UCM, the VPFM landing page appears. The VPFM landing page can vary. If you have not performed a discovery for any VPFM domain, then the discovery page is the landing page. If you previously performed a discovery, then the last visited dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last dashboard page.

About this task

Perform the following procedure to add a dashboard.

Procedure

1. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the dashboard.
2. Click **Add new dashboard**.

3. In the Prompt dialog box, enter the new dashboard name.
4. To permit other users to view your changes, click **Public dashboard**.
5. Click **OK**.
6. 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.
7. Enter information in the configuration dialog box.
8. 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**.
9. After you complete the edits to the dashlet, click **Finish**.
10. To add another dashlet, repeat step 6 to step 9.
11. Click **Save dashboard**.

    For more information about configuring dashlets, see Dashboard wizards on page 55.

Variable definitions

The following table lists the dashboard configuration buttons.

Variable	Definition
Dashboard dashlet configuration button	Provides a series of steps to configure the dashlet. The steps are wizard-like and present you with choices that you can select to customize a dashlet.
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 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

Table continues…

Variable	Definition
	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. Drag and drop the **Event Listing** icon onto the canvas outlined on the Dashboard work area.

   The Configure dialog box appears.
2. In the Dashlet title field, enter a name.
3. In the Domain field, click the down arrow to select a domain.
4. Click **Choose a Scope**.

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

   Note:

   You can use the Search field to search for a scope.
6. From the Configure dialog box, in the Rows / page field, enter the number of rows to appear in the dashlet.
7. The Columns sections displays the columns headers to appear in the dashlet.
   - To add a new column, click **Add**, and 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.
8. Click **OK**.

Result

VPFM adds the Event Listing dashlet to the dashboard. To edit the Event Listing dashlet, click the dashlet tool icon.

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. Drag and drop the **Event Summary** icon onto the canvas outlined on the Dashboard work area.

   The Configure dialog box appears.
2. In the Dashlet title field, enter a name.
3. 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.
4. In the Dashlet items section, click **Add**.
5. In the Domains section, select a domain.
6. Click **Next**.
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 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 **Previous**.

12. To add another dashlet item, repeat step 4 to step 11.
    - Or, click **Finish**.

Result

VPFM adds the Event Summary dashlet to the dashboard. To edit the Event Summary dashlet, click the dashlet tool icon.

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. Drag and drop the **Availability Report** icon onto the canvas outlined on the Dashboard work area.

   The Dashlet items configurator dialog box appears.
2. In the Dashlet title field, enter a name.
3. In the Domain field, click the down arrow to select a Domain.
4. In the Dashlet Items section, click **Add**.
5. In the Select element dialog box, select an element.
6. Check single elements, or scope name to include all elements within a scope.
7. Click **Next**.
8. From the Dashlet items configurator dialog box, in the Graph column field, click the down arrow and select a time frame for the report.
9. 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.
10. To continue configuring the dashlet, click **Next**.
    - Or, if the configurations are complete, click **Finish**.

Result

VPFM adds the Availability Report dashlet to the dashboard. To edit the Availability Report dashlet, click the dashlet tool icon.

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. Drag and drop the **Element Status Summary** icon onto the canvas outlined on the Dashboard work area.

   The Configure dialog box appears.
2. In the Dashlet title field, enter a name.
3. In the Domain field, click the down arrow to select a domain.
4. In the Dashlet items section, click **Add**.
5. 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.
6. Click **Next**.
7. If the dashlet items are correct, click **Finish**.
   - To add another dashlet item, click **Add**.
   - To delete a dashlet item, click **Delete**.
   - To edit a dashlet item, click **Edit**.

   ✱ **Note:**

   Use the up or down arrows to move up or down the list of available column headers.
8. To add the show reachability status icon to the dashlet, select **Show reachability**.
9. To add the unacknowledged status icon to the dashlet, select **Show unacknowledged alerts**.
10. To add the acknowledged alerts status icon to the dashlet, select **Show acknowledged alerts**.
11. To view variables, in the Show variables section, click **Add**, and select a variable.
    - To include variables with no value, check **Include variables with no value**.
12. Click **Next**.
13. If the dashlet items are correct, click **Finish**.
    - To add another dashlet item, click **Add**.

- To delete a dashlet item, click **Delete**.
- To edit a dashlet item, click **Edit**.

Note:

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

Result

VPFM adds the Element Status Summary dashlet to the dashboard. To edit the Element Summary dashlet, click the dashlet tool icon.

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. Drag and drop the **Top-N Report** icon onto the canvas outlined on the Dashboard work area.

   The Dashlet items configurator dialog box appears.
2. In the Dashlet title field, enter a name.
3. In the Domain field, click the down arrow to select a Domain.
4. Click **Choose a Scope**.

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

   Note:

   You can use the Search field to search for a scope.
6. From the Dashlet items configurator dialog box Variable field, select a variable.
   - To include variables with no value, check **Include variables with no value**.
7. In the Sort Order field, click the down arrow and select **Top** or **Bottom**.
8. In the Top-N Number field, enter the number of items to appear in the Top-N Report dashlet.
9. In the Secondary 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.

10. Click **OK**.

Result

VPFM adds the Top-N Report dashlet to the dashboard. To edit the Top-N Report dashlet, click the dashlet tool icon.

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. Drag and drop the **Dial Gauge** icon onto the canvas outlined on the Dashboard work area.

   The Select an element dialog box appears.
2. In the Domain field, click the down arrow to select a domain.
3. In the Perspective field, click the down arrow and select a perspective from the available list.
4. From the folders or icons that appear in the box, navigate to the element you require.
5. To input item parameters, click **Next**.
6. To add a dashlet item, click **Add**.
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 variables with no value**. If there is no data available, the dial gauge does not display any value.
   - To show thresholds, select **Show thresholds**.
8. Enter 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 12.
14. Click **Finish**.

Result

VPFM adds the Dial Gauge dashlet to the dashboard. To edit the Dial Gauge dashlet, click the dashlet tool icon.

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. Drag and drop the **Trend Chart** icon onto the canvas outlined on the Dashboard work area.

   The Select an element dialog box appears.

2. In the Domain field, click the down arrow to select a domain.

3. In the Perspective field, click the down arrow to select a perspective.
4. 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.
5. Click **Next**.
6. In the Choose elements dialog box, select an element from the list.
    - To add an element, click **Add**.
    - To delete an element, highlight an element, and click **Delete**.
7. Click **Next**.
8. From the Choose time interval dialog box, click the down arrow and select a time interval from the list.
9. 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.
10. Click **Next**.
11. 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.
    - Check the box for **Include variables with no value** to view all variables, including variables with no data collected.
    - To show thresholds, select **Show thresholds**.
12. Select a variable.
13. In the Left axis variable (optional) field, select a variable if required.
14. To change the y-axis scale for the graph to show the trend plotting over a larger y-axis, check **Autorange**.
15. To view averages of the trend over an x-axis, check **Averaging Mode**.
16. 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.
17. In the Dashlet Title field, enter the name of the dashlet.
18. Click **Next**, or **Finish**.

Result

VPFM adds the Trend Chart dashlet to the dashboard. To edit the Trend Chart dashlet, click the dashlet tool icon.

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. Drag and drop the Pie Chart icon onto the canvas outlined on the Dashboard work area.

   The Configure dialog box appears.

2. In the Dashlet title field, enter a name.
3. In the Domain field, click the down arrow to select a domain.
4. In the Dashlet items section, click **Add**.
5. Select a perspective.
6. 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.

7. Click **Next**.
8. To add another dashlet item, repeat steps 4 to 6.
   - To delete a dashlet item, highlight the item, and click **Delete**.
   - To edit a dashlet item, highlight the item, and click **Edit**.
   - To move up the list of dashlet items, click the up arrow.
   - To move down the list of dashlet items, click the down arrow.
9. In the Pie variables section, click **Add**.
10. Select variables that are supported by dashlet items.
    - You can use the Search variable field to search for a specific variable.
    - To include variables with no value, check **Include variables with no value**.

    After you select a variable, the system displays the variable name in the Variable or remainder title field.

11. (Optional) To view free, used, and total properties for variables, select **Calculate remainder from total**.
12. (Optional) In the Variable title field, rename the title of the variable.
13. To leave any slice in the pie chart colorless, select **Leave slice transparent**.
14. Click **Next**.

15. To add another pie variable, repeat steps 9 to 14.

    Note:

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

    - 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.

16. Click **Finish**.

Result

VPFM adds the Pie Chart dashlet to the dashboard. To edit the Pie Chart dashlet, click the dashlet tool icon.

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. Drag and drop the **Element Property Table** icon onto the canvas outlined on the Dashboard work area.

   The Select an domain dialog box appears.

2. In the Domain field, click the down arrow to select a domain.
3. Click **Next**.
4. From the Select an element dialog box, select a Perspective from the drop-down menu.
5. From the folders that appear in the box, navigate to the element you require.
6. Click **Finish**.

Result

VPFM adds the Element Property Table dashlet to the dashboard. To edit the Element Property Table dashlet, click the dashlet tool icon.

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 Browser. For information about creating custom views, see Saving custom views on page 82.

Procedure

1. Drag and drop the **Schematic** icon onto the canvas outlined on the Dashboard work area.

   The Select a schematic dialog box appears.
2. In the Domain field, click the down arrow to select a domain.
3. In the Perspective field, click the down arrow to select a perspective.
4. From the folders that appear in the box, navigate to the element you require.
5. Click **OK**.
6. Click **Save dashboard**.

Result

VPFM adds the Schematic dashlet to the dashboard. To edit the Schematic dashlet, click the dashlet tool icon.

Viewing the dashboard for a device

About this task

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

Procedure

1. From the VPFM menu bar, select **Topology** > **Network Browser**.
2. From the Network Browser center pane, right click on a device.
3. From the application menu, select **Show dashboard...**.

Deleting a dashboard

Before you begin

You must be on the VPFM home page. After you click on the VPFM link from the UCM, the VPFM landing page appears. The VPFM landing page can vary. If you have not performed a discovery for any VPFM domain, then the discovery page is the landing page. If you previously performed a discovery, then the last visited dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last dashboard page.

About this task

Perform the following procedure to delete a dashboard.

Procedure

1. From the VPFM home page, select a dashboard from the drop-down list located on the top right-hand side of the screen.
2. To view the menu bar, click the dashboard down button.
3. From the menu bar, click **Delete dashboard**.
4. In the Confirm dialog box, click **OK**.

Editing a dashlet

Before you begin

You must be on the VPFM home page. After you click on the VPFM link from the UCM, the VPFM landing page appears. The VPFM landing page can vary. If you have not performed a discovery for any VPFM domain, then the discovery page is the landing page. If you previously performed a discovery, then the last visited dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last dashboard page.

About this task

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

Procedure

1. From the VPFM main page, select a dashboard from the drop-down menu.
2. Select a dashlet to edit, and click on the tools icon.

   A configuration dialog box specific to the dashlet you selected appears. This is the beginning of the dashlet wizard.
3. Enter information in the configuration dialog box.
4. 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**.
5. After you complete the edits to the dashlet, click **Finish**.

Renaming a dashboard

Before you begin

You must be on the VPFM home page. After you click on the VPFM link from the UCM, the VPFM landing page appears. The VPFM landing page can vary. If you have not performed a discovery for any VPFM domain, then the discovery page is the landing page. If you previously performed a discovery, then the last visited dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last dashboard page.

About this task

Perform the following procedure to rename a dashboard.

Procedure

1. To view the dashboard configuration buttons and menu icons, click the down arrow located at the top of the dashboard.
2. Click **Rename dashboard**.
3. In the Prompt dialog box, enter a new dashboard name.
4. Click **OK**.

Updating a dashlet

Before you begin

You must be on the VPFM home page. After you click on the VPFM link from the UCM, the VPFM landing page appears. The VPFM landing page can vary. If you have not performed a discovery for any VPFM domain, then the discovery page is the landing page. If you previously performed a discovery, then the last visited dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last dashboard page.

About this task

Perform the following procedure to immediately update a dashlet.

Procedure

1. Select a dashlet.
2. On the selected dashlet, click **Update**.

Configuring auto refresh for a dashlet

Before you begin

You must be on the VPFM home page. After you click on the VPFM link from the UCM, the VPFM landing page appears. The VPFM landing page can vary. If you have not performed a discovery for any VPFM domain, then the discovery page is the landing page. If you previously performed a discovery, then the last visited dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last dashboard page.

About this task

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

The time intervals are:

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

Procedure

1. Select a dashlet.
2. Click **Update interval**.

   A list of update time intervals appears.
3. Click on a time interval.
   - Or, to turn the update interval off, click **Off**.

Chapter 5: Network Discovery configuration

Perform the following procedures to configure network discoveries on your Avaya Visualization Performance and Fault Manager (VPFM). For information about how to perform a discovery, see *Avaya Visualization Performance and Fault Manager Fault and Performance Management* (NN48014-700), and *Avaya Visualization Performance and Fault Manager Discovery Best Practices* (NN48014–105).

Perform the following procedures to configure network discoveries.

For more information about network discovery, see Network Discovery on page 16.

For information about performing a network discovery, see the *Avaya Visualization Performance and Fault Manager Fault and Performance Management* (NN48014-700).

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 Avaya VPFM. A discovery domain is a virtual representation of part or all of a network.

Procedure

1. From the VPFM menu bar, select **Topology** > **Network Discovery**.

   The Network Discovery page appears.
2. From the Network Discovery menu bar, click the **Add a new domain** button.
3. Type a domain name for the domain you are creating.

   Each domain must have a unique name and names may 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.

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. From the VPFM menu bar, select **Topology** > **Network Discovery**.

   The Network Discovery page appears.
2. Select the domain you want to clone.
3. From the Network Discovery menu bar, click the **Clone selected domain** button.

   A dialog box appears to enter a new name.
4. Enter the new domain name.
5. Click **OK**.

   The tab of the cloned domain appears.

Deleting discovery domains

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

Procedure

1. From the VPFM menu bar, select **Topology** > **Network Discovery**.

   The Network Discovery page appears.

2. Select the domain you want to delete.
3. From the Network Discovery menu bar, click **Delete selected domain**.

   A dialog box appears to confirm deletion.

4. Click **OK**.

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.

Use the following procedure to add a seed to your discovery recipe.

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. For more information, see Adding discovery domains on page 71.

Procedure

1. From the Network Discovery page, select the domain tab to which you want to add a seed.
2. In the **Seeds** box, click the **Add** button.
3. Select **Seed**.
4. Select either **Router** or **IP Subnet** to indicate the type of seed you want to add.
5. 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 IP v4 and v6 standard syntax is supported.

6. Select the **Enabled** check box.
7. If you want VPFM to partition the selected subnet to find router-based seeds, select the **Partition** checkbox.
8. Click **OK**.

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

Adding a seed group

Before you begin

- Add a network discovery domain. For more information, see Adding discovery domains on page 71.

About this task

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

Procedure

1. From the Network Discovery page, select the domain tab to which you want to add a seed.
2. In the **Seeds** box, click the **Add** button.
3. Select **Seed Group**.
4. In the Add a new seed group dialog box, enter the name of the seed group.
5. Next to Seeds, click **Add**.
6. Select either **Router** or **IP Subnet** to indicate the type of seed you want to add.
7. 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 IP v4 and v6 standard syntax is supported.
8. Select the **Enabled** check box.
9. If you want VPFM to partition the selected subnet to find router-based seeds, select the **Partition** check box.
10. Click **OK**.

    The system adds a list of router-based seeds to the seed list.
11. To add another seed to the seed group, repeat step 4 to step 10.
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 71.

Procedure

1. On the Network Discovery page, click the domain tab corresponding to the domain for which you want to edit a seed.
2. From the **Seeds** box, select the seed you want to edit.
3. In the **Seeds** box, click **Edit**.
4. Modify the seed as needed.
5. Click **OK**.
6. To save the changes, click **Apply your changes**.

Reordering seeds

Seeds are discovered in the order in which they are listed in the Seeds box. The reordering of seeds may be necessary, for example, if a router does not populate the arp cache and you need to ensure that a discovery extends beyond a firewall. You must place a subnet seed (behind the firewall) as the first seed, and the core router seed as the second seed.

Before you begin

- Add a network discovery domain and a seed. For more information about adding a discovery domain, see Adding discovery domains on page 71. For more information about adding a seed, see Adding seeds on page 72.

Procedure

1. On the Network Discovery page, click the domain tab corresponding to the domain for which you want to reorder seeds.
2. In the **Seeds** box, select the seed you want to reorder.
3. Click the **Up** button to ascend the position of the seed in the list.

   Or
4. Click the **Down** button to descend the position of the seed in the list.
5. Repeat steps 2 and 3 for any additional seeds you would like to reorder.
6. Click **OK**.

Deleting seeds

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

Before you begin

- From the VPFM menu bar, select **Topology** > **Network Discovery**.
- Add a network discovery domain and a seed. For more information about adding a discovery domain, see Adding discovery domains on page 71. For more information about adding a seed, see Adding seeds on page 72.

Procedure

1. On the Network Discovery page, click the domain tab corresponding to the domain for which you want to delete a seed.
2. In the **Seeds** box, select the seed to be deleted from the list of seeds.
3. Click **Delete**, located at the top of the Seeds box.

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

Adding limits to subnets

You can limit the extent of a discovery by specifying subnets to which the discovery should be restricted. 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. From the VPFM menu bar, select **Topology** > **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. Type 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 subnet box.

6. To save the change, **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, is faster, and provides 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. From the VPFM menu bar, select **Topology** > **Network Discovery**.
2. From the Limit to subnet box select the limit that you want to edit.
3. In the **Limit to Subnets** box, 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. From the VPFM menu bar, select **Topology** > **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 subnet** 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 parts of your network that match the filter conditions.

Procedure

1. From the VPFM menu bar, select **Topology** > **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. Select a **Filter Type** from the list.
5. For the Filter type selected, choose a **Value**.

   The values that are valid for the exclude filter definition depend on which Filter Type you select in step 4.

   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	
Device Type	Exclude all devices of a certain type.
IP Address	Exclude all devices with addresses within the range specified. You can specify subnet syntax or use wildcards. For example, 172.16.67.0/24 or 172.16.67.*.
IP Subnet	Exclude all devices with addresses within the range specified. You can specify subnet syntax or use wildcards. For example, 172.16.67.0/24 or 172.16.67.*.

Table continues…

Variable	Value
IP Range	Excludes all devices with addresses within the range specified.
Domain Name	Excludes all devices whose domain name matches the range specified.
MAC Address	Exclude 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	Exclude 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 beginning of string is required).
Value	
Access Router	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	Digital Subscriber Line Access Multiplexer (enables telephone lines to make faster connections to the Internet).
DSU/CSU	Digital (or Data) Service Unit - Channel Service Unit.
Firewall	Device that is configured to permit, deny, or proxy data through a computer network which has different levels of trust.
Host	Personal computer, Macintosh, other non-server workstation, or any device that supports SNMP but has not been classified by the discovery as one of the other specific types.
Hub	Device for connecting multiple twisted pair or fiber optic Ethernet devices together, making them act as a single segment.
IP Phone	VoIP phone
PLC	Programmable Logic Controller
Printer	A printer
Printer Server	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.
Router	Networking device that interconnects separate logical subnets
SAN Bridge	Storage Area Network bridge
SAN Switch	Storage Area Network switch

Table continues…

Variable	Value
Server	Network-connected computer hardware that provides specific services onto the network.
Layer 2 Switch	Networking device which performs pure switching.
Switch/Router	Layer-3 switch
Terminal Server	Computer that aggregates multiple communication channels into one.
Unmanageable	Any device that can be pinged but does not respond to any known management protocol
WAP	Wireless Access Point
Uninterruptible Power Supplies	Devices and equipments that provide emergency power when the input power source fails. VPFM supports the APC UPS devices.
VM Hosts	A physical server which hosts the virtual machines.

Editing exclusions

Edit an exclusion to modify the discovery of your network.

Procedure

1. From the VPFM menu bar, select **Topology** > **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 Type** list, select a value.
6. Click **OK**.

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

Variable definitions

For information about variables for Editing exclusions, see the variable definitions table for Adding exclusions on page 77.

Deleting exclusions

You can delete an exclusion if it is not required.

Procedure

1. From the VPFM menu bar, select **Topology** > **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.

Setting the network discovery options

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

Procedure

1. From the VPFM menu bar, select **Topology** > **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).
4. To set advanced discovery options, click the **Advanced Discovery Options** button.
5. In the **Options** box, enter values for the advanced discovery options you want to use.

   Note:

   You can click the **Revert to default settings** link to restore the values to the default settings.
6. Click **OK**.
7. To save the changes, click **Apply your changes**.

Variable definitions

Variable	Value
Wide Area Crawl	VPFM discovers devices on the far side of every router interface, regardless of the interface type. Supported WAN interfaces:

Table continues…

Variable	Value
	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 VPFM Discovery does not go beyond any interface which is considered to be WAN interface.
VPN Crawl	Usually not needed to discover VPN client campuses. This option causes VPFM to augment discovery with information from vendor-specific VPN tables. Initiates VPFM to detect for remote sites through VPN connections.
DNS Lookup	VPFM performs DNS lookup on all devices.
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.
Avaya Only Discovery	Ignores any devices that are not on the approved Avaya list. Includes devices with IDs that begin with one of the following: 15 (Xylogics), 18 (Wellflee), 45 (Synoptics), 335 (Micom), 562 (Avaya), 569 (Armon), 930 (Centillion), 1424 (Performance Technology), 1872 (Alteon), 2272 (Rapid City), 2505 (New Oak), 2865 (Opteron)
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.
Advanced Discovery Options	
Abort hung queries after (minutes)	Specifies when to abort hung queries. The default is 20 minutes.
SNMP timeout (seconds)*	Specifies the SNMP timeout period in seconds. The default is 1.8 seconds
Max SNMP retries	Specifies the maximum number of SNMP retries. The default is 3 retries.

Table continues…

Variable	Value
Estimated max request time (2–126)	Read-only. Indicates the estimated maximum request time.

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. From the VPFM menu bar, select **Topology** > **Network Discovery**.
2. On the Network Discovery page, highlight the campus you would like to rename, and then click **Rename Campus**.
3. Type 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.

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. From the VPFM menu bar, select **Topology** > **Network Browser**.
2. 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**.
4. Make changes to the schematic.
5. Click **save schematic**.

   The Save schematic dialog box appears.
6. Enter a name for the schematic.
7. Select the public folder or private folder.
8. To permit other users to edit the custom view, in the editable by field, click the down arrow and select **authorized users** or **all**.

   Note:

   The Share with all users option is only available if you select the Public folder.
9. Click **OK**.

   The custom view is saved, and is located in the folder you selected in the Custom Views perspective.

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. From the VPFM menu bar, select **Topology** > **Network Browser**.
2. From the tree browser, select the **Custom Views** perspective.
3. From the Custom Views perspective, 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. To allow other users to edit the custom view, in the editable by field, click the down arrow and select, **authorized users** or **all**.
7. Click **From Scratch...**.

8. From the topology menu bar, click **add elements**.

   The Domain Element Chooser screen appears.
9. Select a perspective.
10. 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.
11. To select links automatically, check the **Auto-link new elements** check box.

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

    VPFM creates a custom schematic with links drawn in.

    Note:

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

    The Save schematic dialog box appears.
14. Enter the name for the schematic.
15. Select a folder; public or private.
16. To allow other users to edit the custom view, in the editable by field, click the down arrow and select, **authorized users** or **all**.

    Note:

    The Share with all users option is only available if you select the Public folder.
17. 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. From the VPFM menu bar, select **Topology** > **Network Browser**.
2. From the tree browser, select the **Custom Views** perspective.
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. To allow other users to edit the custom view, in the editable by field, click the down arrow and select, **authorized users** or **all**.
7. 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, VPFM removes the non-device icons from the custom view.

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

   The Save schematic dialog box appears.
10. Enter the name for the schematic.
11. Select a folder; public or private.
12. To allow other users to edit the custom view, in the editable by field, click the down arrow and select, **authorized users** or **all**.

    Note:

    The Share with all users option is only available if you select the Public folder.
13. Click **OK**.

Chapter 6: Manual device discovery

Perform the following procedures to start a manual device discovery.

Adding a device to an existing discovery

Perform the following procedure to add a device to an existing discovered domain.

Before you begin

- You must configure the device to respond to SNMP queries from Avaya Visualization Performance and Fault Manager (VPFM).
- VPFM 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. From the VPFM menu bar, select **Topology** > **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 VPFM.

About this task

Procedure

1. From the VPFM menu bar, select **Topology** > **Network Discovery**.
2. On the Network Discovery page, click **Manual Discovery**.
3. In the **Previous Requests** panel, select the device to be modified.
4. In the **Previous Requests** panel, click **Edit**.
5. Modify the value as required.
6. Click **OK** to save the changes.

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 VPFM.

Procedure

1. From the VPFM menu bar, select **Topology** > **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. The manual discovery starts 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 VPFM.

Procedure

1. From the VPFM menu bar, select **Topology** > **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

Click the **Progress** icon to cancel a discovery that is in progress.

Viewing a manual discovery report file

For information on how to view a discovery report, see Network Discovery on page 16.

Viewing manual discovery results

Perform the following procedure to view the results of a manual discovery.

Procedure

1. From the VPFM menu bar, select **Topology** > **Network Browser**.
2. 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. Double click on a node to display it on the central panel, in its network context. Scopes 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 from the menu options.

Chapter 7: 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 could specify the set of elements for which a particular response is used.

Perform the following procedures to create scopes on your Avaya Visualization Performance and Fault Manager (VPFM) system.

- Adding constraint based scopes on page 90
- Adding enumerated member scopes on page 93
- Adding union based scopes on page 94
- Editing scopes on page 95
- Renaming scopes on page 95
- Cloning scopes on page 96
- Deleting scopes on page 96
- Creating templates for scopes on page 97

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. From the VPFM menu bar, select **Configurations** > **Scopes**.
2. From the Scopes window, 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**.

A Prompt dialog box appears.

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**.

Variable definitions

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.

Table continues…

Variable	Value
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.
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 enumerated member scopes

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

Procedure

1. From the VPFM menu bar, select **Configurations** > **Scopes**.
2. From the Scopes window, 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**.

   A Prompt dialog box appears.
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**.

Variable definitions

Variable	Value
Scope Members	Specify the domain elements to include in the scope.

Table continues…

Variable	Value
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)

Adding union based scopes

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

Procedure

1. From the VPFM menu bar, select **Configurations** > **Scopes**.
2. From the Scopes window, 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**.

   A Prompt dialog box appears.
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.
Comments	Specify a description of the scope. Comment text is not part of the scope definition. (Optional)

Editing scopes

You can edit a scope after you create it.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Scopes**.
2. From the Scopes window, 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 it.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Scopes**.
2. From the Scopes window, 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.

   A Prompt dialog box appears.
5. Enter the new name.
6. Click **OK**.

Cloning scopes

You can clone an existing scope.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Scopes**.
2. From the Scopes window, click the **Elements** tab to select the Elements domain.

   Or

   Click the **Events** tab.
3. Select the scope you want to clone.
4. Click **Clone selected scope**.

   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. From the VPFM menu bar, select **Configurations** > **Scopes**.
2. From the Scopes window, 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**.

   A Confirmation dialog box appears.

5. Click **OK** to confirm the deletion.

Creating templates for scopes

About this task

Perform the following procedure to create templates for scopes.

Procedure

1. From the VPFM menu bar, select **Topology** > **Network Browser**.
2. From the left pane, select a perspective, and then select a topology.
3. From the Network Browser center pane, right click on a device.
4. From the application menu, select **Show dashboard…**.

   A dashboard template appears with all related elements such as Device, Interface, and server specific dashlets.

5. To edit the dashboard, see Dashboard wizards on page 55.

Chapter 8: Monitoring configuration

Perform the following procedures to set up monitoring for your Avaya Visualization Performance and Fault Manager (VPFM) system.

- Adding a monitoring configuration on page 98
- Editing a monitoring configuration on page 99
- Renaming a monitoring configuration on page 100
- Deleting a monitoring configuration on page 101
- Starting and stopping monitoring on page 101
- Viewing active monitoring configurations on page 102
- Defining a parameter override on page 102
- Configuring overrides for a device from the Network Browser on page 104
- Viewing overrides on page 105
- Editing an override on page 105
- Renaming an override on page 106
- Cloning an override on page 106
- Deleting an override on page 107

Adding a monitoring configuration

Monitoring configurations define what events are received for which domain elements and with what alternative event processing options. Add a new monitoring configuration to specify a new set of constraints to monitor your network.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Monitoring**.
2. From the Monitoring window, click **Add a new monitoring configuration**.
3. In the Prompt dialog box, enter the name of the new configuration.
4. Click **OK**.
5. There are two tabs, Basics and Domains. Select the **Basics** tab.

6. In the Basics tab, select the **Enabled** option to enable polling for the configuration.
7. From the **Polling Period** list, specify the interval at which the polling must occur.
8. From the **Data Retention Period** list, specify the duration for which the data can be retained.
9. From the **These Elements** list, select a scope.

   The information type list shows the modified monitoring information.
10. From the **Monitor for these information types** section, select the appropriate events or categories of events.
11. Select the **Domains** tab.
12. Select **All Domains** if you want to configure this monitoring configuration for all the domains created. Or select **These Domains** and then select one or more of the created domains.

    The monitoring configuration is associated with only the selected domains.
13. To save the changes, click **Apply your changes** .

Variable definitions

Variable	Value
Enabled	Indicates whether polling is enabled.
Polling period	Indicates the interval at which polling for the selected MITs occurs. (If Enabled is selected.)
Data retention period	Specifies the duration for which the data is retained.
These Elements	Provides a list of scopes. Selecting a scope from the list causes the information types list to be modified to display monitored information appropriate for the selected scope.
Monitored for these information types	Displays a tree structure of monitored information types for the selected scope (the scope defined using the These Elements list) from which individual events or categories of events can be selected for use with the monitoring configuration.

Editing a monitoring configuration

After you add a monitoring configuration you can edit the parameters. You cannot edit the parameters of the default configurations.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Monitoring**.

2. From the Monitoring window, select the configuration you want to edit.

   The configuration settings for the selected monitoring configuration display on the right panel of the Monitoring page.
3. Edit the settings as needed.
4. To save the change, click **Apply your changes**.

Variable definitions

Variable	Value
Enabled	Indicates whether polling is enabled.
Polling period	Indicates the interval at which polling for the selected MITs occurs. (If Enabled is selected.)
Data retention period	Specifies the duration for which the data is retained.
These Elements	Provides a list of scopes. Selecting a scope from the list causes the information types list to be modified to display monitored information appropriate for the selected scope.
Monitored for these information types	Displays a tree structure of monitored information types for the selected scope (the scope defined using the These Elements list) from which individual events or categories of events can be selected for use with the monitoring configuration.

Renaming a monitoring configuration

You can change the name of a monitoring configuration after you create it.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Monitoring**.
2. From the Monitoring window, select the configuration you want to rename.
3. Click **Rename selected monitoring configuration**.
4. In the Prompt dialog box, enter the new name.
5. Click **OK**.
6. To save the change, click **Apply your changes**.

Deleting a monitoring configuration

Delete a monitoring configuration to end the monitoring process related to the configuration.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Monitoring**.
2. From the Monitoring window, select the configuration you wish to delete.
3. Click **Delete selected monitoring configuration**.

   A Prompt dialog box appears to confirm the deletion.
4. Click **OK**.

Starting and stopping monitoring

You can start and stop availability monitoring agents and SNMP monitoring agents for your VPFM system using the monitoring details browser.

For more information about the monitoring details browser, see Monitoring details browser on page 50, and Viewing active monitoring configurations on page 102.

Procedure

1. From the VPFM menu bar, select **Monitoring** > **Monitoring Details Browser**.

   The Monitoring Details Browser page appears.
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**.

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

Variable definitions

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.
SNMP monitoring agent	Displays the monitoring requests and domain elements defined for the SNMP monitoring agent.

Viewing active monitoring configurations

You can view the active monitoring configurations using the Monitoring Details Browser.

Procedure

1. From the VPFM menu bar, select **Monitoring** > **Monitoring Details Browser**.
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.

Variable definitions

Variable	Value
Name	The name of the monitoring agent.
Location	The location of the monitoring agent.
Domain	The domain to which the monitoring agent applies.
Status	The status of the monitoring agent.

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 VPFM that, for the domain elements encompassed by the indicated scope(s), you want to monitor for this value specified in the override, not the value that is set in the MIT definition.

For more information about overrides, see Monitoring overrides on page 26.

Procedure

1. From the VPFM menu bar, select **Configurations** > **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**.

   The Parameter Override window appears.
9. Select the MIT for which you want to define a 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

Variable	Value
Enabled	Indicates whether or not the event processing override is active (enabled).
Add domain element scope	Click the Add domain element scope link to select the domain element scopes to which you want the override to apply.

Table continues…

Variable	Value
Override Applies to	The Override Applies to menu appears twice for the event processing overrides and once for the monitoring overrides. 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. 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).
Parameter Overrides	Provides a list of the existing parameter overrides. Includes links that enable users to edit existing override values.

Configuring overrides for a device from the Network Browser

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

Procedure

1. From VPFM menu bar, select **Topology** > **Network Browser**.
2. Select a Perspective, and select an element.

   ✱ **Note:**

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

   The Overrides window for the device appears.
4. To add an override configuration, click **Add**.
   - To edit an override configuration, select the configuration, click **Edit**, and enter the required information.
   - To delete an override configuration, select the configuration, and click **Delete**.
5. In the Specify Scope 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 to applies to one device only, check **Apply new override only to the <device name>**.
7. Click **Next**.
8. In the Parameter Override dialog box, select a parameter override.
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 or create a configuration in which to save the new overrides table in, and enter the override name.
13. Click **OK**.

    The override configuration window appears with overrides for the device.
14. Click **Close**.

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. VPFM crosses out overrides if another override takes precedence.

Procedure

1. From the VPFM menu bar, select **Topology** > **Network Browser**.
2. From the Network Browser center pane, right click on a device.
3. From the menu, select **Configure** > **Overrides...**.

Editing an override

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

Procedure

1. From the VPFM menu bar, select **Configurations** > **Monitoring Overrides**.

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

   The settings for the selected override display on the right panel.
3. 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. From the VPFM menu bar, select **Configurations** > **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. From the VPFM menu bar, select **Configurations** > **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 it.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Monitoring Overrides**.
2. Select the override you want to delete.
3. Click **Delete**.
4. In the Confirm dialog box, click **OK**.

Chapter 9: Trap and syslog configuration

The Traps and Syslogs page enables you to view information SNMP traps and syslogs reports.

To configure the traps viewer and syslog viewer, perform the following procedures.

- Configuring Traps Viewer settings on page 108
- Configuring VPFM-lite for forwarding traps to VPFM on page 109
- Configuring Syslog Viewer settings on page 110

For more information about traps and syslog, see Traps, Syslogs, and Events on page 38.

Configuring Traps Viewer settings

Traps viewer window enables a user to configure how trap information is organized and displayed. Use the following procedure to configure the Traps viewer.

Procedure

1. From the VPFM menu bar, select **Tools** > **Trap & Syslog Browser**.
2. Select the **Traps** tab.
3. On the Traps and Syslogs page, click **Settings**.
4. Set the **Maximum age**. Entries that are older than the maximum age defined in this field are purged from the VPFM database.
5. Enter the **Maximum number**. After the maximum number of entries are in the VPFM database, the oldest entries are deleted as new entries are added.
6. Set the **Limit to disc. devices** to true or false. This determines whether the trap data is limited to discovered devices.
7. Set the **Limit to auth. devices** to true or false. This determines whether the trap data is limited to authenticated devices.
8. Enter the **Listener port** (default is 162).
9. Enter the **Archive depth**. Older files beyond this number are deleted.
10. In the **Archive directory** field, enter the file path for the directory where you want archive files to be stored.
11. In the **Forwarding** field, click **Add** to enter the destination IP address for trap information.

12. Click **OK** to save the changes.

Configuring VPFM-lite for forwarding traps to VPFM

For configuring the Optivity Telephony Manager (OTM) fault feature, you can configure VPFM-lite as a trap receiver for Avaya CS 1000 and forward the traps to Avaya Performance and Fault Manager (VPFM) for fault correlation.

Use the following procedure to configure VPFM-lite for forwarding traps to VPFM.

Procedure

1. On the VPFM-lite Welcome page, select the **Traps and Syslog** Browser.
2. Select the **Traps** tab.
3. On the Traps and Syslog page, click **Settings**.

   The Traps Configuration Settings window appears.
4. Change, or keep as is, the **Maximum age**, **Maximum number**, **Limit to Disc. Devices**, **Limit to Auth. Devices**, and **Listen port** .
5. Select the **CS 1000 Trap Forwarders add** button.

   The CS1000 Traps Forwarders configuration windows appears.
6. Enter the **Filter** name.
7. Select **Severity** of traps to filter.
8. Select **Device Type**.
9. Enter the required **Error Code** to filter on. You can use the wild card (*) or ranges (for example ERR0012 - ERR0017).
10. After the filter is in effect, select **Day of the Week**.
11. After the filter is in effect, select **Time of the Day** .
12. Select **SNMP** tab.
13. Enter the IP address of the VPFM server where the trap has to be forwarded to.
14. If the VPFM server is configured to listen on a different port, change the port number from 162.
15. Select the **Actions** tab.
16. To send an email every time the filter forwards a trap, select the **Sample CS1000 Email Action**.

    If the traps received is large, selecting email action may generate a lot of emails. You can select other actions that you created using the procedure Creating an action on page 115.
17. On the Trap Forwarding and Trap Configuration windows, click **OK** .

Configuring Syslog Viewer settings

You can configure how syslog information is organized and displayed. Use the following procedure to configure the Syslog viewer.

The communication protocol for traps supports specification of original source address. However, this is not true for syslogs because the subject address cannot be reliably parsed from a syslog message because of the different formats in use.

Procedure

1. From the VPFM menu bar, select **Tools** > **Trap & Syslog Browser**.
2. Select the **Syslogs** tab.
3. On the Traps and Syslogs page, click **Settings**.
4. Set the **Maximum age**. Entries that are older than the maximum age defined in this field are purged from the VPFM database.
5. Enter the **Maximum number**. After the maximum number of entries are in the VPFM database, the oldest entries are deleted as new entries are added.
6. Set the **Limit to disc. devices** to true or false. This determines whether the trap data is limited to discovered devices.
7. Enter the **Listener port** (default is 162).
8. Enter the **Archive depth**. Older files beyond this number are deleted.
9. In the **Archive directory** field, enter the file path for the directory where you want archive files to be stored.
10. In the **Forwarding** section, click **Add** to enter the Host Address, and port number for syslog information.
11. Click **OK** to return to the Syslog Configuration dialog box.
12. Click **OK** to save the changes.

Chapter 10: MIB configuration

If you have a new device that you want to monitor, you can import the required MIBs using the Avaya Visualization Performance and Fault Manager (VPFM) Administrator client. After you add the MIBs, you must add an enumerated member scope to specify the elements in the scope and you must add a monitoring configuration to define which events are received.

Adding a MIB

You can add a MIB using the VPFM Administrator Client.

Procedure

1. On your computer go to **Start** > **Programs** > **Avaya** > **UCM** > **VPFM** > **VPFM Administrator Client**.

   The VPFM Login box appears.

2. Type your VPFM user name and password.
3. Click **Login**.
4. In the left panel, click **MIB definitions**.

   The Import MIB window appears.

5. Find the MIB you want to import. If you want to import multiple MIBs from a folder, select the required folder.
6. In the **Target Repository** folder, select the appropriate folder for the type of MIB you are importing.
7. Click **Import**.

   The MIB appears in the left panel. All the traps available for this MIB appear in the bottom right panel.

8. In the bottom right panel, in the **Notifications** tab, select the traps you want to add by clicking on the red flag.

   After you select the red flag, it changes color to green.

9. Click **Apply**.

VPFM generates a new event type for each SNMP notification and trap defined within the MIB.

Next steps

After you add the MIB, perform the following procedures:

- Adding enumerated member scopes on page 93
- Adding a monitoring configuration on page 98

Chapter 11: MIT configuration

Perform the following procedures for Monitored Information Type (MIT) configuration.

- Configuring Monitored Information Types on page 113
- Viewing Monitored Information Types on page 114

For more information about MIT configuration, see MIT on page 43.

Configuring Monitored Information Types

You can modify the parameters of the Monitored Information Types (MIT).

Procedure

1. From the VPFM menu bar, select **Configurations** > **Monitored Information Types**.
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

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. From the VPFM menu bar, select **Configurations** > **Monitored Information Types**.
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

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 12: Automating configuration tasks

With Avaya Visualization Performance and Fault Manager (VPFM) you can automate actions, responses, and schedules. The procedures in this section show how to configure these tasks.

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.

For more information about actions, see Actions on page 27.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Actions**.

2. On the Actions page, select the action group to which you want to add an action by highlighting the folder in the left panel of the Actions page.
3. Click **Add**.

   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 in the box, and then click **OK**.

   The right panel of the Actions window displays the parameters for defining the new action.
6. Specify values for all mandatory parameters and for any optional parameters you want to use.
7. Click **Apply your changes**.

Variable definitions

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.
SNMPv1 Trap	Initiates an SNMPv1 trap.
SNMPv2 Notification	Initiates an SNMPv2 notification.
Custom Action	Permits advanced customizing of action.
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.

Renaming an action

After you create an action you can change the name.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Actions**.
2. Select the action you want to rename.

3. Click the **Rename** 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 it.

Procedure

1. From the VPFM menu bar, select **Configurations** > **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 it.

Procedure

1. From the VPFM menu bar, select **Configurations** > **Actions**.
2. Select the action you want to delete.
3. Click **Delete selected action**.
4. Click **OK** to confirm the deletion.

Creating a response

Responses define the ways in which Avaya VPFM 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. For more information about responses, see Event responses on page 35.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Event Response**.
2. On the 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**.

Renaming a response

After you create a response you can change the name.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Event Response**.
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 it.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Event Response**.
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 it.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Event Response**.
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 it implements, and the time table by which those actions are performed on those domain elements.

For more information about schedules, see Schedules on page 37.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Schedule**.
2. Click **Add a new 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. If you want to execute actions on specific domains, select the **Execute Actions on these Domain Elements** box and use the combo-box to select the appropriate domain elements.

6. Specify the **Actions to Execute** by checking the boxes corresponding to the desired action(s).
7. 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. It is the time zone of where the VPFM server is located.
8. Enter the interval information, and click **OK**.
9. In the **Schedule applies to** section, specify the applicable domains.
10. Click **Apply your changes**.

Renaming an action schedule

You can rename an action schedule after you create it.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Schedule**.
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 an action schedule

After you create an action schedule you can clone it.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Schedule**.
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 an action schedule

You can delete an action schedule if it is not required.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Schedule**.
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. From the VPFM menu bar, select **Actions** > **By Schedule**.
2. On the Schedules page, click **Add a new 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. Select the **Schedule applies to** check box and select or clear the applicable domains.
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**.

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.

For more information about device menu choices, see Device Menu Choices on page 47.

Procedure

1. From the VPFM menu bar, select **Actions** > **By 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

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. VPFM 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. From the VPFM menu bar, select **Actions** > **By 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. In the right panel, click the **Everything** button.
6. From the list in the dialog box, select **Devices**, and then click **OK**.
7. Select the **Enabled** check box.
8. Select the **Obtain user confirmation before executing** check box.
9. From the **Make these actions available** list, select the actions you want to launch.
10. Click **Apply your changes**.
11. From the VPFM menu bar, select **Topology** > **Network Browser**.
12. Right click on any device for which you want to launch a Telnet/Http/Https/Ftp session.
13. From the list, select **Tools** and click the option you want to launch.

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. VPFM 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. From the VPFM menu bar, select **Configurations** > **Actions**.
2. On the Actions page, select the **Web Browser Actions** folder.
3. Click the **Add** 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.

Chapter 13: Supported devices

The following table lists devices that Avaya Visualization Performance and Fault Manager (VPFM) supports.

For more information about supported devices, see *Avaya VPFM Supported Devices, Device MIBs, and Legacy Devices* (NN48014-104).

Device name	Release
Avaya Data Devices	
Application Switch 2208 / 2216 / 2224 / 2424 / 2424-SSL / 3408	(2216, 2224, 2424, 2424-SSL, 3408) (2216-E, 2224-E, 2424-E, 2424-SSL-E, 3408-E) 23.2
Avaya Advanced Gateway AG2330MCR	10.3
Business Policy Switch	3.2
ES 325-24T and 24G	3.6
ES 425-24T and 48T	3.6
ES 460-24T-PWR, 470-24T, 470-48T, 470-24T-PWR, 470-48T-PWR	3.7
ERS 1612G, 1624G, 1648T	2.1.5
ERS 2500 series (2526T 2526 PWR, 2550T, 2550T-PWR)	4.4
ERS 3500	5.1
ERS 4500 series (4526-FX, 4550T, 4550T-PWR, 4548GT, 4548GT-PWR, 4524GT, 4526GTX, 4526GTX-PWR, 4526T, 4526T-PWR)	5.5, 5.6, 5.6.3
ERS 4600 series	5.2, 5.4, 5.6.3
ERS 4800 series (ERS4826GTS, ERS4826GTS-PWR-PLUS, ERS4850GTS, ERS4850GTS-PWR-PLUS)	v5.6, v5.6.2, 5.6.3
ERS 1424 T	2.1.6
ERS 3510 T	4.0.4
ERS 5510, ERS 5520, ERS 5530, ERS 5530-24TFD	5.1, 6.0, 6.2, 6.3.1
ERS 5600	6.2, 6.3.1
ERS 8300	4.2, 4.2.3.7
ERS 8600	7.1, 7.1.6, 7.3

Table continues…

Device name	Release
ERS 8800	7.1, 7.1.6, 7.3
Business Secure Router 222	2.6
Business Secure Router 252	2.6
Secure Router 1000, 3000	9.4.1
Secure Router 1001 and 1001S	9.3
Secure Router 1002, 1004	9.3
Secure Router 3120	9.3
Secure Router 4000	10.3
Secure Router 4134	10.3
SNAS 4050	1.0
VPN Router 600 / 1750 / 2700 / 2750 / 5000	8.0
VSP 4000 series	3.0
VSP 7000	10.1, 10.2, 10.2.1
VSP 9000	3.1, 3.3
WLAN SS 2350	5.0
WLAN SS 2360/2361	5.0
WLAN SS 2382	5.0
Wireless Bridge 7230	1.51
Wireless Gateway 7240/7250	3.0.1
Wireless LAN AP 7215/7220	3.01
Wireless LAN 8100	1.1
Wireless LAN AP 8120	1.1
Avaya Voice Devices	
Avaya Aura Messaging (AAM)	6.2
CS 1000	7.0 and 7.5
CS1000 E, 1000 S	5.0
Business Communications Manager 200 , 400	4.0
Business Communications Manager 50	3.0
Communication Manager (CM)	5.2.1, 6.0, 6.0.1, 6.2, 6.3.2
IP Phones H.323 or SIP and Avaya Flare 9600	2.6.4
IP Phones H.323 or SIP and Avaya Flare 96x1	6.0.0
IP Phones H.323 or SIP and Avaya Flare 1600	1.6
IP Phones H.323 or SIP and Avaya Flare 4800	2.9
Media Gateway G430 , G450,	1.1
Media Gateway G650	v6.2

Table continues…

Device name	Release
Media Gateway G860	v2.1.1
Media Gateway IG550	1.1
Session Manager (ASM)	6.0, 6.0.1, 6.2, 6.3.2
System Manager (SMGR)	6.0, 6.0.1, 6.2, 6.3.2
Avaya Aura Virtual Environment (Aura VE) devices	
Presence Service (PS)	6.2, 6.2.2
Secure Access Link (SAL) gateway (ASG support only)	2.2
Agile Communication Environment (ACE/AIE)	6.2, 6.3
Application Enablement Service (AES)	6.2, 6.3
Avaya CM duplex or simplex	6.2, 6.3
Session Manager	6.2, 6.3.2
System Manager	6.2, 6.3.2
Web License Manager standalone (WebLM)	6.2
Utility Services (US)	6.2, 6.3
Avaya IDE Ignition Server	8.0
Enterprise Legacy Devices	
ES 450	4.5.5
ES 460-24T-PWR	3.7
Secure Router 1400	1424 (2.1.6)
Wireless Gateway 7240	3.0.1
WLAN 8100	1.0
WLAN SS 2380	5.0
Third party devices	
EMC VNX 5300 series	
Lenovo RD530	
VMware ESXi	5.0, 5.1
VMware VSphere	v5.0, 5.1
VMware VCenter	5.0, 5.1
AudioCodes Mediant 3000 (M3K) Media Gateway	
Acme Packet Net-Net Session Border Controller (SBC)	6.3.0
Sipera Session Border Controller (SBC)	6.2