Avaya Visualization Performance and Fault Manager - Quick Start

3.0
NN48014-302
01.01
March 2012

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 generally makes available to users of its products. 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 Web sites 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 its Hardware and Software (“Product(s)”). 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 Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation 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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation 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 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: Purpose of this document

This document provides the information and procedures necessary to quickly install Avaya Visualization Performance and Fault Manager (VPFM), and outlines the initial procedures to configure the system.

Chapter 2: New in this release

This is the first release of *Avaya Visualization Performance and Fault Manager Quick Start* (NN48014–302).

Chapter 3: Installation

You can install Avaya Visualization Performance and Fault Manager (VPFM) on Windows or Linux operating systems.

For more information about installing VPFM, see *Avaya Visualization Performance and Fault Manager Installation* (NN48014–300).

Installing VPFM on Windows

Use the following procedure to install VPFM for the first time on a Windows platform.

Before you begin

- Ensure that you have logged on to the server platform as an Administrator or as a user with Administrative privileges to install VPFM on a Windows platform.
- The server must have a hard disk labelled C: or the install will fail.
- Before you can proceed with a successful first installation, the results of the preinstall check must return with no errors. If there are errors, you must correct all errors reported by the script before you initiate installation. If there are any warnings, they should also be corrected. These warnings will not stop the installation process but may cause performance issues later. Because the preinstall script is part of the installer, the preinstall script runs for an update or a new install.

Procedure

1. Double-click the VPFM executable file to launch the VPFM installer.

   The VPFM installer prepares for installation and then the License Agreement screen appears.
2. Review the terms of the license agreement and if you agree, select **I accept the terms of the License Agreement** option.
3. Click **Next**.

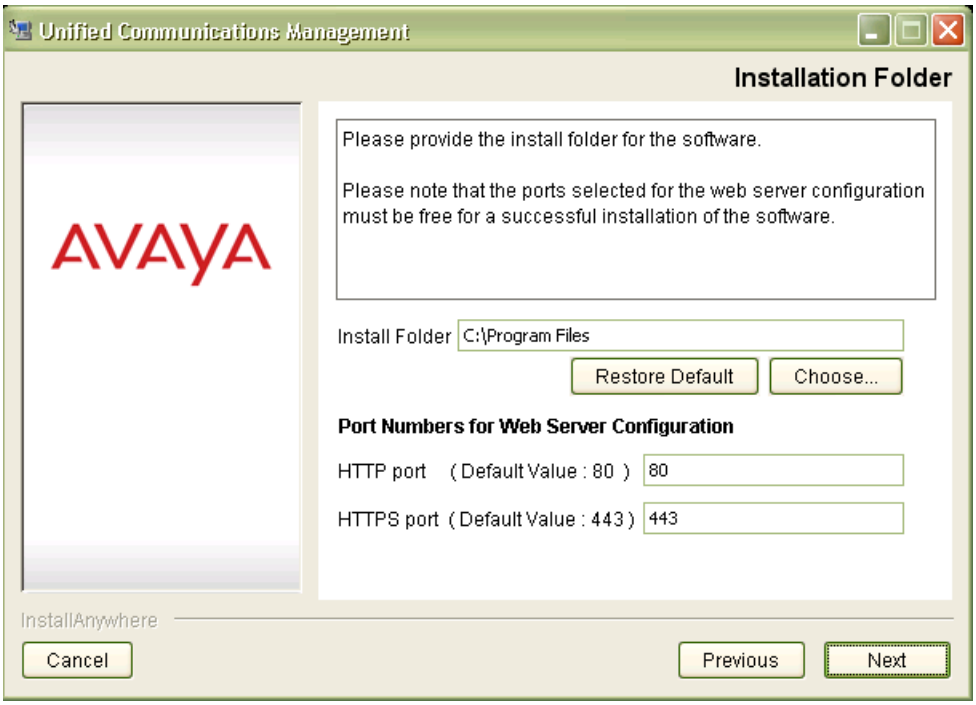
   The License file and port choice screen appears.
4. Choose the License file from appropriate file location and enter the HTTP and HTTPs Port numbers for the VPFM HTTPS Server or you can use the default values.
5. Click **Next**.

If invalid file type is chosen as the license file you will get an error message. For example, an invalid license warning appears.

Therefore, make sure you select the valid license file to avoid any error related to the invalid license.

6. Select **Reenter License**.
7. Click **Next**.

   The **Installation Folder** screen appears.



8. Click **Choose** to browse the destination folder path for installation.

   The default path is available in the location `C:\Program Files`.
9. Enter the HTTP port and HTTPS port numbers for Web Server Configuration.
10. Click **Next**.

The Security Server Mode screen appears.

11. Under Primary Security Server:
    a. Enter the **UCM password (Primary)**.
    b. Re-enter the same password in **Confirm password (Primary)**.

    Note:

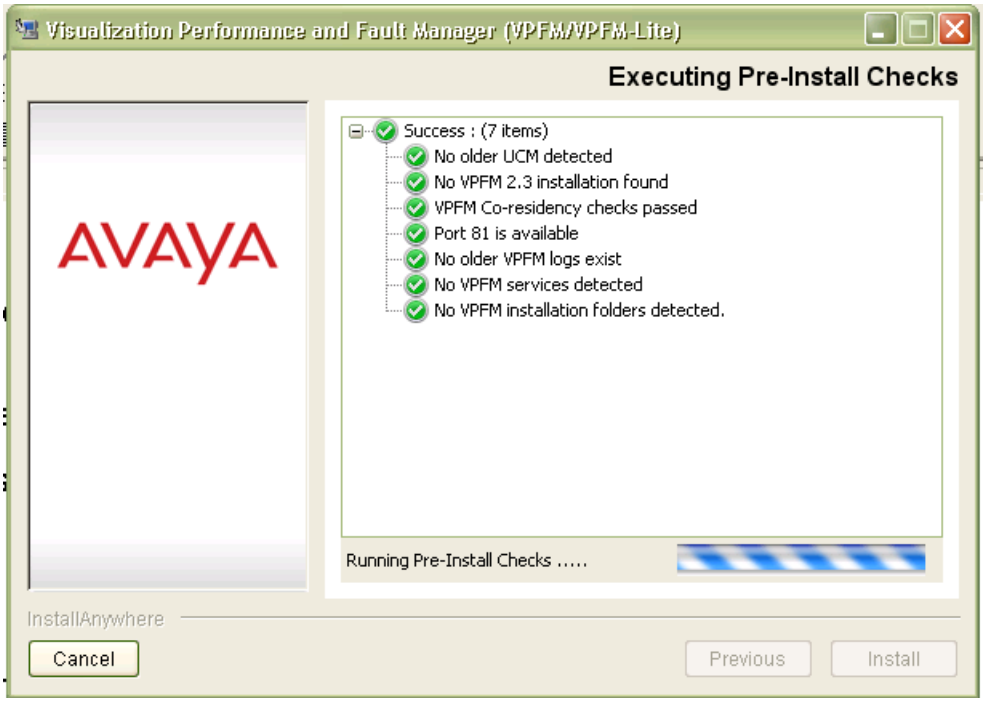
    The password must contain minimum of 8 characters with atleast 1 uppercase, 1 lowercase, 1 special character and 1 numeric character.

    Example: UCM4Avaya@

12. Click **Next**.

    The Executing Pre-install Checks screen appears.

    Running Pre-Install Checks . . . progress bar is displayed and once the system verifies the pre-install checks, **Success** message appears. If you encounter errors, during pre-install check, you will need to address these errors and re-run the installation checks. Some of the examples of the errors are insufficient disk space and unsupported operating system.



13. Click **Install**.
    The Install Complete window appears.
14. Click **Done**.

Installing VPFM on Linux

Use the following procedure to install VPFM on a Linux platform.

Before you begin

- Ensure that you have logged on to the server platform as root to install VPFM on Linux platform.
- Ensure that SELinux administration is disabled.

Procedure

1. Run the VPFM installer .BIN file from the command line.
   An Introduction screen appears.
2. From the Introduction screen, click **Next**.
   An End User License Agreement screen appears.

3. From the License Agreement screen, select **I Accept The Terms Of The License Agreement** option.
4. Click **Next**.

   The License file and port choice screen appears.
5. Specify the destination folder path for the License File and port number.
6. Click **Next**.

   The Installation folder screen appears.
7. From the Choose Install Folder screen, specify the destination folder path for installation.
8. Select the desired shortcut option.
9. Click **Next**
10. Enter the HTTPS port for VPFM server web requests.
11. Click **Next**.

    The Security Server Mode screen appears. screen appears.
12. Under Primary Security Server:
    - Enter the UCM password (Primary)
    - Re-enter the same password in Confirm password (Primary)

    Note:

    The password must contain minimum of 8 characters with atleast 1 uppercase, 1 lowercase, 1 special character and 1 numeric character.
13. Click **Next**.

    The Executing Pre-install Checks screen appears.

    Running Pre-Install Checks . . . . progress bar is displayed and once the system verifies the pre-install checks, **Success** message appears.
14. Click **Install** to start the installation process.

    The Installing Visualization Performance and Fault Manager screen appears displaying the installation process as it progresses.
15. After the completion of the installation process, the Install Complete screen appears.
16. Click **Done** to complete the installation process.

Chapter 4: Unified Communications Management

The following section outlines the procedures for entering credentials in the Avaya Unified Communications Management (Avaya UCM).

For more information about Avaya UCM, see *Avaya Visualization Performance and Fault Manager Common Services Fundamentals Unified Communications Management* (NN48014–100).

Device and Server Credentials Editor configuration

This section provides information about configuring device credentials using the Device and Server Credentials Editor.

Avaya Unified Communications Management (UCM) applications use SNMP v1/v2/v3, Telnet, CIM, SSH, FTP, RLogin, or SSH protocols for communication with network infrastructure devices such as routers. The protocol required depends on the type of device. It uses the WMI protocol to communicate to a windows server. Each set of credential information is referred to as a credential set. These credential sets allow UCM applications to retrieve information from the network elements and devices. The Device and Server Credentials Editor service maintains a list of credential sets for the devices that make up a network. You can enter credentials for every device (IP address) or for a range of IP addresses. See the documentation for your network devices to determine which protocols they use for authentication.

When using Network Discovery in VPFM, the application uses these credentials to discover network devices and servers. For more information about network discovery, see *Avaya Visualization Performance and Fault Manager—Configuration* (NN48014-500).

The following table lists the categories of credential information that can be managed in the Device and Server Credentials Editor.

Table 1: Device and Server Credentials Editor fields

Credential information	Attributes
Set Name	Credential set name
IP Address or Range	Device/Server IP Address or Address Range
SNMPv1/v2	Read Community Write Community

Credential information	Attributes
SNMPv3	SNMPv3 User Authorization Protocol (MD5, SHA1, None) Authorization Key Privacy Protocol (AES128, DES, 3DES, None) Privacy Key
Telnet	Telnet User name Telnet Password Telnet Port
CIM	CIM User name CIM Password
SSH	SSH User name SSH Password SSH Port
NetConf	**Need description**
FTP	FTP User name FTP Password FTP Port
RLogin	RLogin User name RLogin Password
Windows Server	Windows User name Windows Password Windows Domain

Adding a credential set

Before you begin

- You must have installed the UCM. The Unified Communications Management is installed when you install a UCM application (VPFM, VPFM Lite, COM, or IPFM). For more information, see the installation guide for UCM application.
- Ensure that you are logged on to UCM as administrator.

About this task

Perform this procedure to add a new credential set to Unified Communications Management (UCM). You must add a credential set for each device you want to manage.

The set name accepts printable ASCII characters, but not special characters (%(/!\)). You can enter the space ( ), dash (-), and underscore (_) characters.

The set name must be unique. If you add a new entry or rename an existing one with a set name already used in another entry, a warning message appears.

Procedure

1. In the navigation pane, under **Tools**, click **Device and Server Credentials**.
   The Device and Server Credentials Editor page appears.
2. Click **Add Credential Set**.
   The Add Credential Set dialog box appears.

3. In the **Set Name** field, enter the **Set Name**.
4. In the **IP Address/Range** field, specify the IP address information for the credential.

   For a list of valid IP addresses and ranges, see IP addresses and ranges reference on page 67.
5. Add device credential information on the appropriate tab. For more information about the available tabs, see Device and Server Credentials Editor configuration on page 15.

   Each tab corresponds to an authentication protocol. The information you enter depends on the type of authentication your device uses.
6. Click **Save**.

   The credential set appears in the panel.

Importing a credential set

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to import the credential set to the UCM.

Procedure

1. In the navigation pane, under **Tools**, click **Device and Server Credentials**.

   The Device and Server Credentials Editor page appears.
2. Click **Import Credentials** button.

   The Import Credential Set(s) window appears.
3. Click **Browse**, and then choose the credentials XML file to import.
4. (Optional.) To overwrite the existing entries of credential set, select the **Overwrite existing entries** check box.
5. Click **Import**.

Exporting a credential set

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to export credential set from the UCM to a local XML file.

Procedure

1. In the navigation pane, under **Tools**, click **Device and Server Credentials**.
   The Device and Server Credentials Editor page appears.
2. Click **Export Credentials**.
   The Export Credential Set(s) window appears.
3. Click **Export**.
   The Credential Sets exports to a local XML file. The name of the XML file is autogenerated.
   The File Download window appears.
4. Click **Save**.

Chapter 5: Discovery best practices

Prior to performing a discovery, you must perform the following steps:

- Plan the discovery.
  - Do you want to use a router seed or a subnet seed?
  - Picture the network you expect to discover, including approximate number of nodes.
  - Do you need to discover multiple campuses?
  - Do you need to have more than one domain for discovery?
- Check your device credentials.
- Discover your network.
- Open the Discovery Problem Report for the discovered domain by clicking on the tool bar icon on the VPFM Network Discovery page and checking logs for major errors.
- Verify that the devices discovered meet your plan.

The following sections provide best practice information for performing a discovery.

For more information about Avaya Visualization Performance and Fault Manager (VPFM) discovery best practices, see *Avaya Visualization Performance and Fault Manager Discovery Best Practices* (NN48014–105).

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

Plan your discovery

To achieve the best results from Avaya Visualization Performance and Fault Manager (Avaya VPFM), it is important to plan your discovery before starting a discovery with Avaya VPFM.

The following is a list of points to consider when planning a discovery.

- Decide on the parts of the network you want to discover.
- Choose a seed router, any layer-3 device, from which all parts of your network are reachable either directly or indirectly.
- If a subnet does not have any layer-3 device, provide the subnet itself as a seed.
- Avaya VPFM can perform WAN crawls across the supported devices; for example, Contivity devices and Avaya Secure Routers. But, if the connectivity is across a service

provider network, then you must provide a seed device from the remote networks, in addition to the seed you have already specified.

- Specify how far you want the discovery to reach out to by providing subnet limits.
- If there are any device types or specific devices you want to exclude from discovery, specify these in the exclusions criteria.
- Make sure that autotopology, such as SynOptics Network Management Protocol (SONMP) and Cisco Discovery Protocol (CDP), is enabled on all the devices that support these protocols.
- If you have an out-of-band network setup for management, ensure that the devices Address Resolution Protocol (ARP) cache reflects the out-of-band addresses. Otherwise, VPFM tries to access the devices using the in-band addresses, if these are present in the ARP cache.

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.
- 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.

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.

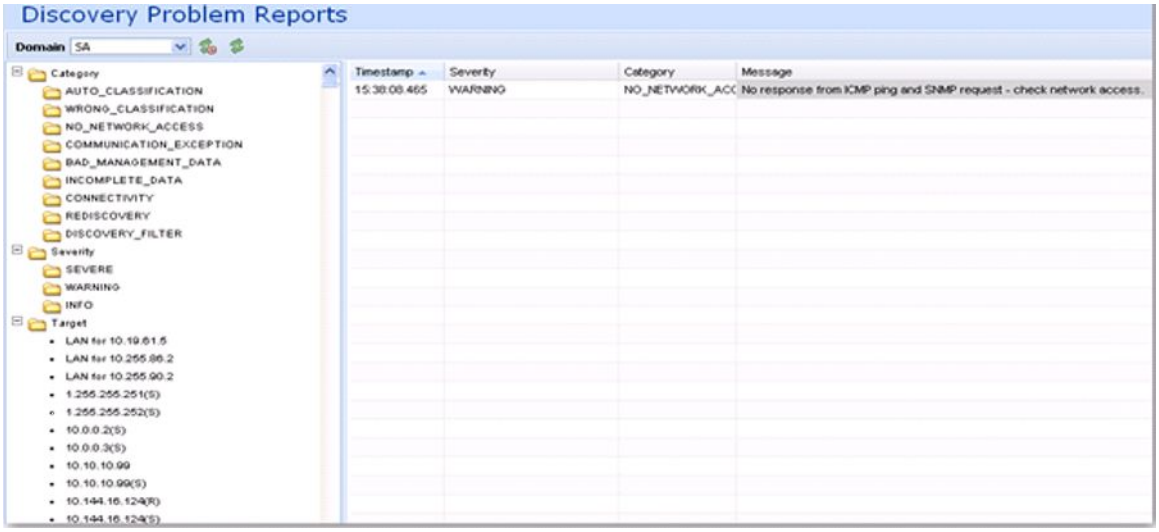
For more information about configuring device credentials from the UCM Device and Server Credentials Editor, see *Avaya Unified Communications Management Common Services Fundamentals* (NN48014–100).

Analyzing Avaya VPFM logs

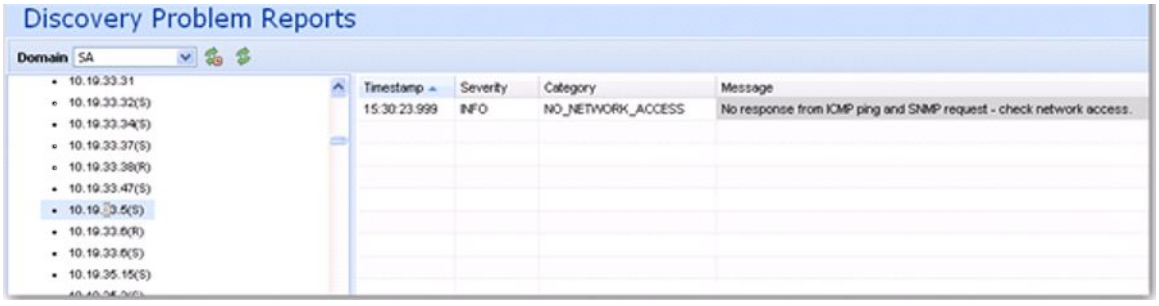
About this task

To view logs related to a discovery, on the toolbar of the Network Discovery page, click on the  button. A Discovery Problem Reports page appears.

The following is an example of a Discover Problem Reports page.



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



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

One common reason for not discovering a device is the lack of response from the device from ping or SNMP requests sent from Avaya VPFM. In this case, check the UCM device credentials to make sure they are correct.

If the credentials are correct, then check for SNMP access using the SNMP MIB browser.

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

- Device did not respond to SNMP or ICMP

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

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

- Potential managed device was excluded from discovery

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

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

- There is no log entry for an undiscovered device

  - Make sure that UCM credentials exist for that IP and that they are correct
  - Make sure that the device's IP address in present in the ARP tables of one or more discovered layer-3 devices in your network.

Viewing discovery results in the Tree Browser

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

Procedure

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

   The Network Browser page appears.
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. Left-click twice on a node to display it on the central panel, in its network context. Scopes and SPBMs are displayed in tabular form.
6. Click the Refresh icon to update the information displayed in the Details panel.
7. Right-click on a device, and select the type of information you want to view .

Locating devices from a discovery

About this task

Perform the following procedure to find devices that you discovered.

Procedure

1. From the VPFM menu bar, select **Topology** > **Network Browser**.
2. From the navigation tree, in the Perspective field, select a perspective and view the menu items that appear for the perspective.
   - Or, select a menu from the navigation tree, and from the topology, navigate to view the device. You can navigate up, down, back, or forward.
3. Select a device, interface, or address.

Map background controls

After you enter the edit mode, you can import a background image by clicking the following button.

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

Device icons color coding

You can see if there are faults on sub items in the tree view without expanding it. Tree view color propagation is available in the Layer 2, Layer 3 and VLAN perspectives only. A partial color spot on one edge of the folder or icon in the collapsed state indicates that there is a fault on some element inside that is partially impairing functionality. The color of the spot indicates the severity of the impairment. A full color spot outside of the icon indicates that there is a full impairment inside one of the items in the icon. The color of the spot indicates the highest severity.

Chapter 6: Dashboard configuration

Visualization Performance and Fault Manager (VPFM) 3.0 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; and 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 preconfigured dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last preconfigured 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 **Site 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 29.

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

Variable	Definition
	an event browser tab with the filter automatically applied for that classification, on the Event Summary dashlet, click on an entry .
Availability Report	Displays the average availability for a class of elements as percentages over intervals of hour, day, month, or year. To view a transient dashlet for the element, on the Availability Report dashlet, click on the element name.
Element Status Summary	Displays the KHI status of the element, including %CPU, %Memory, and number of alerts on the element. To open a transient dashboard for the element, on the Element Status Summary dashlet, click on the element name.
Top-N Report	Top-N Reports are based on Scope and Time, and show histograms of devices and interface statistics. Top-N Reports are available for a current time or for a past time period, and can be exported to PDF, CSV or XML.
Dial Gauge	Provides a set of one or more dial gauges, each displaying the value of a domain element variable on an analog dial. All of the dial gauges in one set must display variables from the same domain element.
Trend Chart	Provides performance trend improvements and trending of device resource usage, and key health indicators. Reporting is made easy by selecting trends and exporting information to PDF.
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
- 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 dashlet, 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**.

   The Select element dialog box appears.
   -
5. Check single elements, or scope name to include all elements within a scope.
6. Click **Next**.
7. From the Dashlet items configurator dialog box, in the Graph column field, click the down arrow and select a time frame for the report.
8. 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.

9. 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. Check single elements, or scope name to include all elements within a scope.
6. Click **Next**.
7. If the dashlet items are correct, click **Finish**.
   - 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 **unacknowledged alerts**.
10. To add the acknowledged alerts status icon to the dashlet, select **acknowledged alerts**.
11. To view variables, in the Show variables section, click **Add**, and select a variable.
12. Click **Next**.
13. Click **Finish**.

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, enter a variable.
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. Click the **Choose a variable field**, and select a variable.

   You can use the Search variable field to locate a variable.
7. To view all variables, click the **Show variables without value** check box. If there is no data available, the dial gauge does not display any value.
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.
12. Click **Next**.
13. Click **Finish**.
14. From the Select an element dialog box, 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.
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, uncheck **Use Current time**, 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.
12. Check the box for **Show all variables** to view all variables, including variables with no data collected.
13. Select a variable.
14. In the Left axis variable (optional) field, select a variable if required.
15. To change the y-axis scale for the graph to show the trend plotting over a larger y-axis, check **Autorange**.
16. To view averages of the trend over an x-axis, check **Averaging Mode**.
17. In the Number of averaging intervals field, enter a value.

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

Result

VPFM adds the Trend Chart dashlet to the dashboard. To edit the Trend 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

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 43.

About this task

Perform the following procedure to configure the Schematic dashlet.

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 preconfigured dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last preconfigured 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 righ-hand side of the screen.
2. Click **Delete dashboard**.
3. 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 preconfigured dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last preconfigured 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 preconfigured dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last preconfigured 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 preconfigured dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last preconfigured 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 preconfigured dashboard page is the landing page. If you click on the home icon in the tool bar, you land on the last preconfigured 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 7: View customization

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.

For more information about custom views, see *Avaya Visualization Performance and Fault Manager Configuration* (NN48014–500).

Saving custom views

There are three procedures to 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**.
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**.

   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**.
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**.
13. Click **OK**.

Chapter 8: Viewing Events

When traps are received by Avaya Visualization Performance and Fault Manager (VPFM) from network devices, they may be turned into events. The Events Browser allows you to monitor, acknowledge, and filter network events. Use the following procedures to customize the information displayed in the Events Browser.

Adding a message board

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

Add multiple message boards, by performing this procedure.

Before you begin

- Log on to VPFM

Procedure

1. From the VPFM menu bar, select **Monitoring** > **Event Browser**.
   The Event Browser page appears.
2. Click **Add a new message board**.
3. Enter a name for the new message board in the **Enter a name for the new board** field.
4. Click **OK**. The new message board appears as a new tab in the Event Browser.

Deleting a message board

About this task

Perform the following procedure to delete a message board.

Procedure

1. From the VPFM menu bar, select **Monitoring** > **Event Browser**.
2. Select a message board.
3. Click **Delete selected message board**.
4. In the Confirm dialog box, click **OK**.

Renaming a message board

About this task

Perform the following procedure to rename a message board.

Procedure

1. From the VPFM menu bar, select **Montoring** > **Event Browser**.
2. Select a message board.
3. Click **Rename selected message board**.
4. In the Prompt dialog box, a new name for the selected message board.
5. Click **OK**.

Sorting messages

Sort messages on the message board by performing this procedure.

Before you begin

- Log on to VPFM

Procedure

1. From the VPFM menu bar, select **Monitoring** > **Event Browser**.
   The Event Browser page appears.
2. On the message board, click the arrow on of the column headings.
   A menu appears.
3. A list appears showing the Sort Ascending, Sort Descending, and Columns options.
4. Select **Ascending** or **Descending** to sort the messages in ascending or descending order.

Filtering messages

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

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

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

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

- Filtering by message priority
- Filtering by acknowledgement status

- Filtering by scope or event type
- Filtering by time event gets updated

Related topics:

Filtering messages by priority on page 50
Filtering messages by scope or event type on page 51
Filtering messages by acknowledged status on page 52

Filtering messages by priority

Use the following procedure to filter messages by priority.

Before you begin

- Log on to VPFM

Procedure

1. From the VPFM menu bar, select **Monitoring** > **Event Browser**.
   The Event Browser page appears.
2. Click the **Configure filter for selected message board** icon located at the top of the message board.
   The Msgs Board Filters window appears.
3. Select or clear the Priorities check box to display or filter the messages.
4. Click **OK**.

Variable definitions

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

Filtering messages by scope or event type

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

Before you begin

- Log on to VPFM

Procedure

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

   The Event Browser page appears.
2. Click the **Configure filter for selected message board** button located at the top of the Event Browser window.

   The Msgs Board Filters window appears.
3. Click the **Scopes** box and expand the scopes tree to locate the scopes you want to include in display.
4. Select the nodes you want to include in message display.
5. Expand the Event Types tree to locate the event types you want to include in display. Toggle the selection to include the event type or exclude the event type from display.
6. Click **OK**.

Result

The Event Selection Tree is a tree that consists of items that can be expanded or closed. Each item also has a box next to it which can display one of three control states and can display one of many informational states. To cycle through the three control states, left-click three times on box or label. The control states are explicit inclusion, explicit exclusion, or inherit from parent. The control state is visually indicated by the border of the box: thick green for explicit inclusion; thick red for explicit exclusion; thin of varying color for inherit from parent.

Filtering messages by acknowledged status

Use the following procedure to filter messages by acknowledged status.

Before you begin

- Log on to VPFM

Procedure

1. From the VPFM menu bar, select **Monitoring** > **Event Browser** .
   The Event Browser page appears.
2. Click the **Configure filter for selected message board** icon located at the top of the Message Board.
   The Msgs Board Filters window appears.
3. Select the **Hide Acknowledged** box to hide acknowledged events.

Viewing OTM error codes

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

Before you begin

Log on to VPFM.

About this task

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

Procedure

1. From the VPFM menu bar, select **Tools** > **Traps & Syslog Browser**.
2. In the **Error code** column, click on the required error code.
   A window appears with the details of the error code.

Exporting a message board

You can export a message board and save the contents.

Before you begin

- Log on to VPFM

Procedure

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

Chapter 10: Diagnostic tools

You can use the Network Browser in Avaya Visualization Performance and Fault Manager (VPFM) to access the following diagnostic tools:

- MIB Query...
- MIB Browse...
- ICMP Ping
- Trace Route
- SNMP Get
- Remote Ping
- Remote Traceroute...

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

Using diagnostic tools

Before you begin

From the Network Browser, select a topology view.

About this task

Perform the following procedure to access the diagnostic tools.

Procedure

1. From the topology, right-click on a device, and select **Diagnose**.
2. From the Diagnose menu, select a tool.

Chapter 11: SNMP MIB Browser

To access the SNMP MIB Browser, from the VPFM menu bar, select **Tools** > **SNMP MIB Browser**. You can view information about SNMP MIBs in two ways: You can expand the tree structure on the left side of the SNMP MIB browser window and select a MI, or, in the OID field, you can enter the OID of a MIB. The MIB information appears in the right panel of the window.

Note:

You can use the SNMP MIB Browser to debug discovery issues. For example, if you see a SNMP no response log in the discovery problem report, use SNMP MIB browser to assess if you can get a response from the device.

For more information about SNMP MIB Browser procedures, see *Avaya Visualization Performance and Fault Manager Fault and Performance Management* (NN480140700).

Modifying SNMP version authentication

You can customize SNMP authentication for MIBs.

Before you begin

- Log on to VPFM.

Procedure

1. From the VPFM menu bar, select **Tools** > **SNMP MIB Browser**.
2. From the list of MIBs in the left pane, select the MIB for which you want to view the information.
3. Click the SNMP version button next to the Target field.

   The Authentication... window opens.
4. Modify the appropriate fields based on the SNMP version.
5. Click **OK**.

Viewing SNMP MIB data

You can do an SNMP MIB query on the MIBs in your system using the SNMP MIB browser.

Before you begin

- Log on to VPFM.

Procedure

1. From the VPFM menu bar, select **Tools** > **SNMP MIB browser**.
2. In the **Target** field, type the IP address for the MIB you want view.
3. From the list of MIBs in left pane, select the MIB for which you want to view the information.

   OR

   In the **OID** field, type the object identifier for the MIB you want to view.
4. Select SNMP version v1, v2c, or v3. If you choose v3, enter the authentication variables as shown in the preceding variable definitions table.
5. Click the **Get** button to retrieve the output for the MIB.

   The information appears in the right panel.
6. If you want to see the next MIB in the list, click the **Get next** button.
7. If you want to save the MIB information, click the **Save last query results** button.

Chapter 12: 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.
- If you use VPFM API, you can generage mobile Apps.

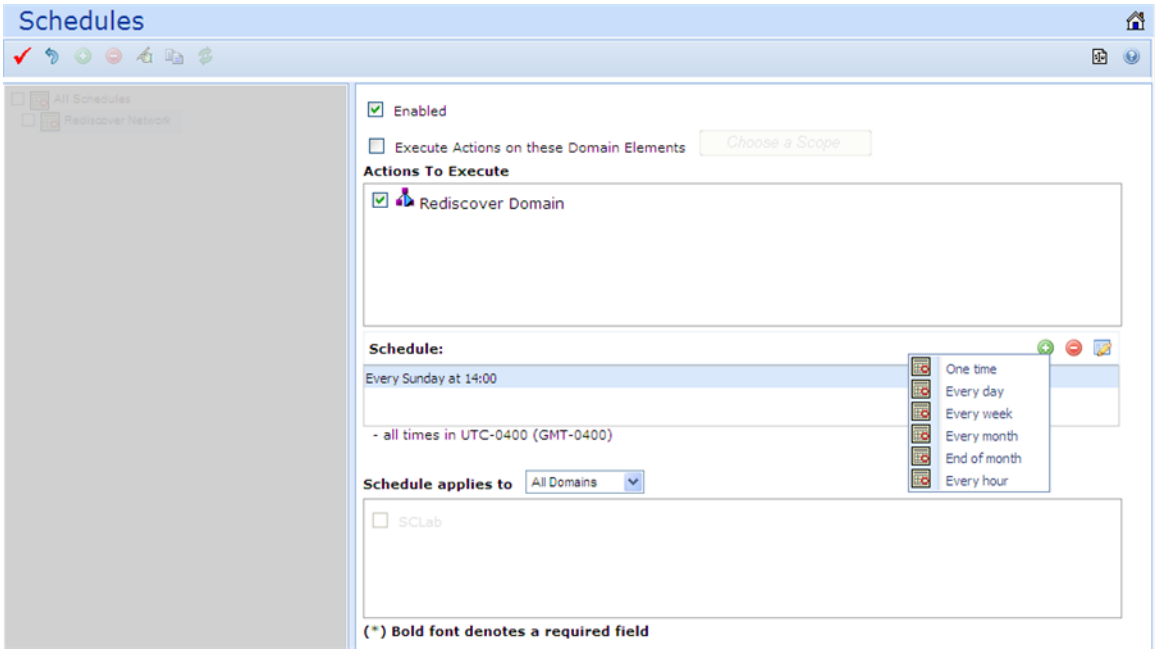
For more information about VPFM actions, see *Avaya Visualization Performance and Fault Manager Configuration* (NN48014–500).

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:



- 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)

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 59.

Before you begin

- Log on to VPFM.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Schedule**.
2. Click **Add a new action schedule**.

   A Prompt dialog box appears.
3. 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.

Before you begin

- Log on to VPFM.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Schedule**.
   The Schedules page appears.
2. Select the schedule you want to rename.
3. Click **Rename selected action schedule**.
   A Prompt dialog box appears.
4. Enter the new name.
5. Click **OK**.

Cloning an action schedule

After you create an action schedule you can clone it.

Before you begin

- Log on to VPFM.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Schedule**.
   The Schedules page appears.
2. Select the schedule you want to clone.
3. Click **Clone selected action schedule**.

A Prompt dialog box appears.

4. 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.

Before you begin

- Log on to VPFM.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Schedule**.
   The Schedules page appears.
2. Select the schedule you want to delete.
3. Click **Delete selected action schedule**.
   The Confirm dialog box appears.
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.

Before you begin

- Log on to VPFM.

Procedure

1. From the VPFM menu bar, select **Actions** > **By Schedule**.
   The Schedules page appears.
2. On the Schedules page, click **Add a new action schedule**.
   A Prompt dialog box appears.

3. Type the name of the new action schedule in the box.
4. Click **Ok**.
   The action schedule definition options appear.
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**.

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.

Chapter 13: IP addresses and ranges reference

This section provides details about the valid IP addresses and IP ranges used by the Device and Server Credentials Editor.

Valid IP addresses and ranges

The following section describes the valid IP addresses and ranges used for device credentials.

Valid IP addresses

IPv4 addresses must conform to the following format: [1-255].[0-255].[0-255].[0.255].

IPv6 addresses must conform to IPv6 rules:

- IPv6 addresses must contain eight groups of four hexadecimal digits.
- Each group must be separated by a colon (:).
- If one or more four-digit group or groups appears as 0000, the zeros may be omitted and replaced with two colons (::). For example, the following are valid IPv6 addresses:
  - 2001:0db8:85a3:08d3:1319:8a2e:0370:7334
  - 2001:0db8::1428:57ab

Valid IP address ranges

When specifying IP address ranges, only consecutive wild cards starting from the last octet of an address are supported. This guarantees one continuous range. For example, only the following combinations are valid:

- IPv4:
  - 17.0.9.* (same as 17.0.9.0-17.0.9.255)
  - 17.0.*.* (same as 17.0.0.0-17.0.255.255)
  - 17.*.*.* (same as 17.0.0.0-17.255.255.255)
  - *.*.*.* (same as 0.0.0.0-255.255.255.255)
  - 17.*.9.9 is invalid
  - 0.0.0.0 and 255.255.255.255 are considered to be valid IPs only if they are given within a range. For example, 0.0.0.0 as single IP is invalid, but 0.0.0.0-2.3.4.5 is a valid range.
- IPv6:
  - 2001:0db8:85a3:08d3:1319:8a2e:0370:* (same as 2001:0db8:85a3:08d3:1319:8a2e:0370:0000-2001:0db8:85a3:08d3:1319:8a2e:0370:ffff)
  - 2001:0db8:85a3:08d3:1319:8a2e:*:*
  - 2001::8a2e:0370:*
- IPs contained in a range cannot have wild cards. For example, 192.168.4.*-192.168.5.245 is an invalid range.

IP address format limitations

The following formats are not supported by Device and Server Credentials Editor:

- An address/subnet mask pair (for example, 10.127.100.0/255.255.255.0)
- Network prefix (CIDR) notation (for example, 10.127.100.0/24)