Nortel Visualization Performance and Fault Manager

Configuration

Release: 2.1
Document Revision: 03.01

www.nortel.com

NN48014-500

Nortel Visualization Performance and Fault Manager
Release: 2.1
Publication: NN48014-500
Document release date: March 2010

Printed in Canada

Contents

New in this release

The following sections detail what's new in Nortel Visualization Configuration (NN48014-500) for release 2.1.

Features

See the following sections for information about the new features described in this guide:

Discovery problem reports

You can now see error and warning messages from the last discovery, on the Network Discovery page in your browser. Previously, this feature was only available with the VPFM Administrative Client. For more information, see "Network Discovery" (page 10).

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. For more information, see "Moving icons in the topology view" (page 12).

MLT/SMLT schematic layout details in campus details view

The topology map is enhanced to keep the groups of devices participating in an MLT/SMLT together on the campus detail view so that the SMLT configuration (triangle, square, or mesh) is evident.

Addition of Nortel Legacy devices monitoring scopes

This document includes an example of a Nortel legacy devices monitoring scope. For more information, see "Nortel legacy devices monitoring scopes" (page 20).

Other information

See the following section for information about VPFM that is not feature related:

Multimedia content

Some conceptual and procedural topics covered in the documentation are now available in a multimedia format. Links to the multimedia content are provided contextually in the documentation.

“WATCH THE VIDEO” identifies a link to multimedia content.

Fundamentals

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

Navigation

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. This includes status propagation, fault, and performance information. Every object that is a MO counts towards the license count. The license number decreases each time you add a new MO.

Once the maximum MO license count is reached, VPFM no longer discovers new objects until the MO count is reduced, 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, may appear on the interface as a gray icon, but does not process any information on the device, including status information, faults, and performance management. An UMO is not counted 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 Nortel Visualization Performance and Fault Manager (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 UCM. For more information see, *Nortel Unified Communications Management Common Services Fundamentals* (NN48014-100).
- Add a new discovery domain.

- Configure the discovery options for the discovery domain.
- Discover the domain.

Attention: 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 click the Network Discovery link located on the Welcome page.

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.
- Create - 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 - 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 - 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.

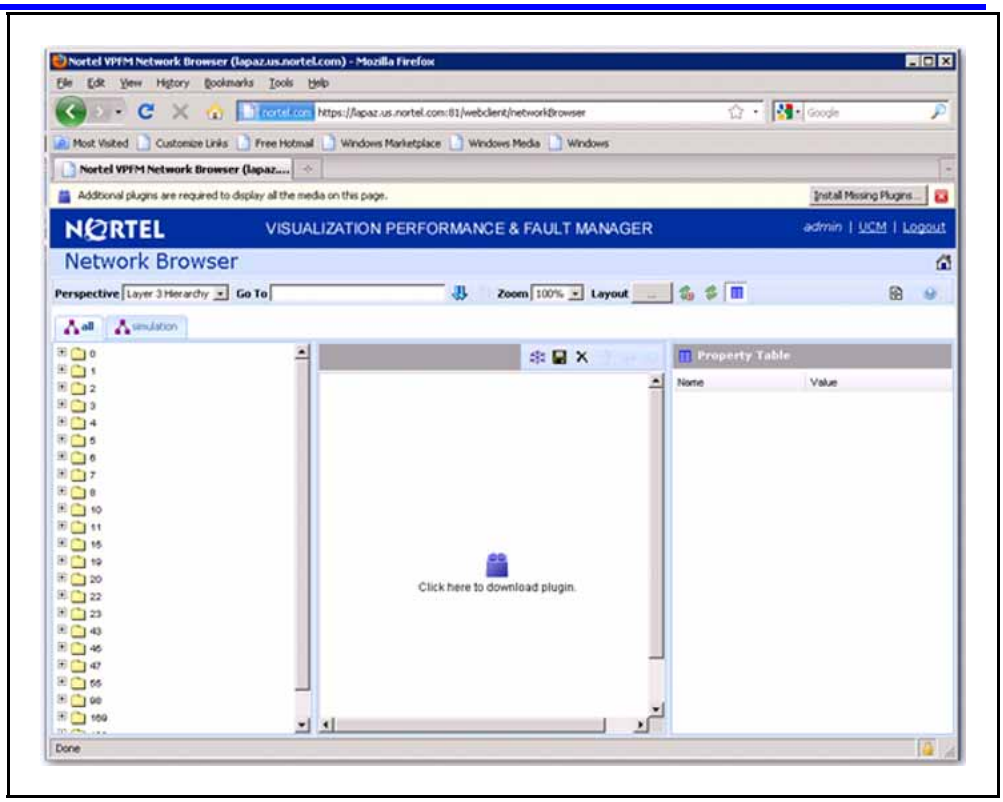
- Discovery Problem Report—Takes you to the Discovery Problem Report screen where you can choose to view the discovery report for one or all domains.
- Save—Saves the domain. Larger domains require longer save times.
- Set Refresh—Turns on or off servlet refresh or changes the refresh interval. The default is auto refresh every 15 seconds.
- Refresh Now—Refreshes the servlet once. The refresh is performed immediately.
- Start/Stop Monitoring—Starts or stops monitoring of the discovery domain. By default when the domain is discovered only Start Monitoring is available.

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. The controls are provided in the bar on the right hand top, next to the navigation arrows. You can freeze a view (to stop movements), save a layout view, or 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 2.1, 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 shows what the user sees if the Adobe Flash browser plug-in is not installed.



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.
- Nortel Only Discovery (selected) - Ignores any devices that are not on the approved Nortel list.

Domain, campus, and seeds

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

With Nortel 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.

Attention: 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.

Attention: 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 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.nortel.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.

Attention: 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 four options to configure your discovery:

- Seeds - The starting point of a discovery (router or DNS name).
- 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, and Nortel only discovery.

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

Media application discovery

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

- Nortel Multimedia Conferencing Release 6.0
- Nortel Interactive Communications Portal Release 1.0

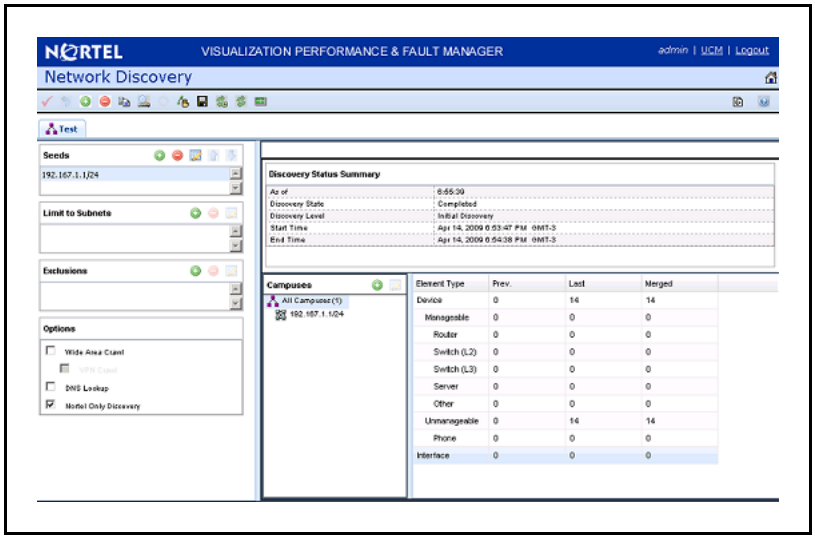
To have VPFM automatically discover these applications, you must include the media application server in the discovery recipe. You must also configure the device credentials for the media application server in the Device Credentials panel. The applications discovered are displayed in the Network Browser;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

Layer 3 subnet partitioning

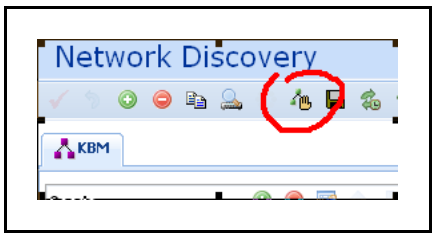
The layer 3 subnet partitioning feature is a discovery phase that you can execute prior to performing a normal network discovery. When you use the layer 3 partitioning feature, the VPFM executes a discovery phase that takes as its starting input one or more large subnet seeds. From these seeds, it analyzes 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.



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.

Attention: 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.

- Design view/text view toggle - 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:

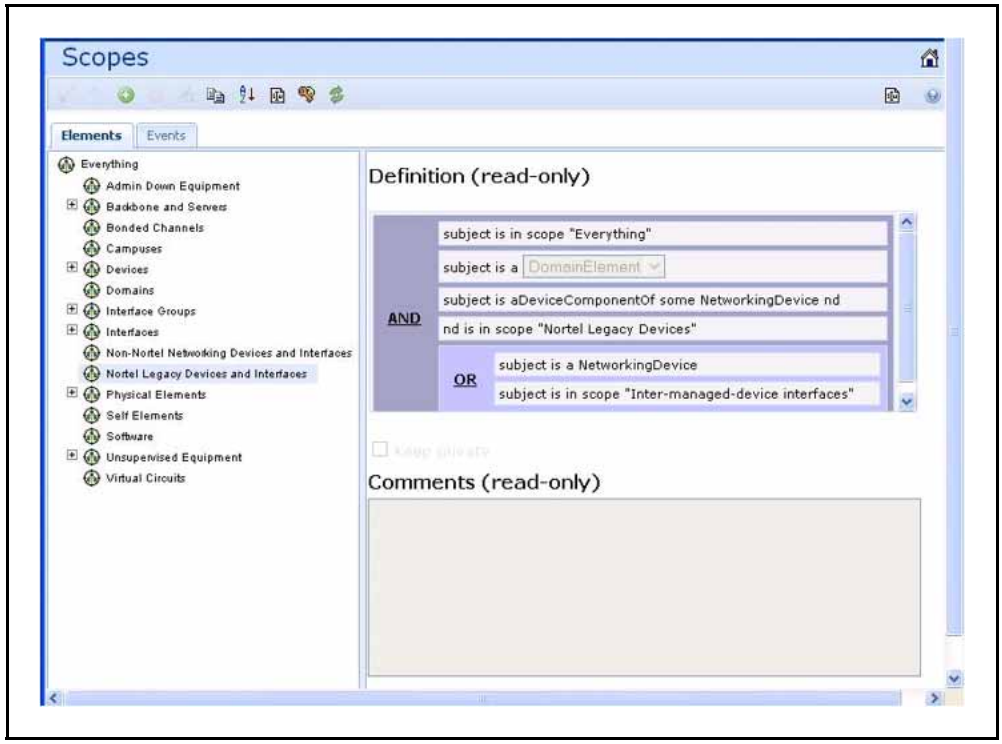
- Constraint-based scopes are defined by a set of elements that meet specified criteria. Both domain element scopes and event scopes may be of the constraint-based scope type.
- Enumerated member scopes are defined by an explicit list of individual elements. Only domain element scopes can be of the enumerated 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.
- 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.

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.

Nortel 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 Nortel legacy devices are available in the Nortel legacy device scope.

The following is an example of the Nortel legacy device scope.



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.

Attention: 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:

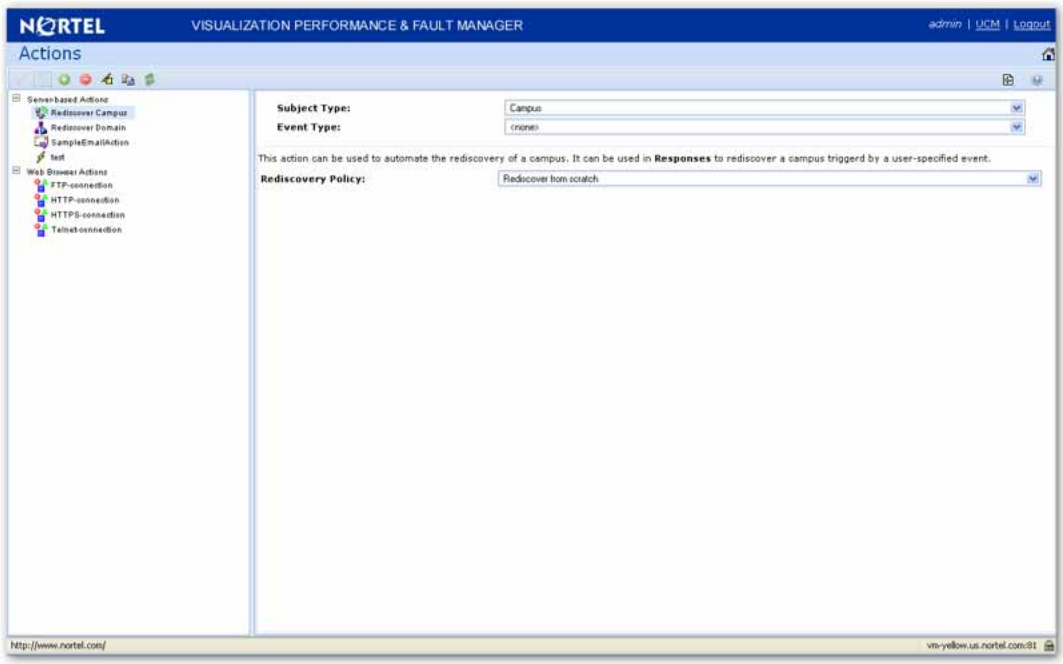
- Enabled – (Default is on) Indicates whether or not the event processing override is active (enabled).

- 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 can be executed through the user interface either interactively, by selecting a domain element and initiating the command, or automatically, using a predefined response or action schedule. VPFM supports a number of different action types.

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



- 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.
- 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.
- 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.
- 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), and SMTP Password (the password for the SMTP user account that sends the message).
- Backup SMTP - enables you to specify the backup 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), and SMTP Password (the password for the SMTP user account that sends the message).

- 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.

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 Domain - Automates the rediscovery of a domain.
- SampleEmailAction- Provides a sample email action.

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-connection - Opens an FTP connection.
- HTTP-connection - Opens an HTTP connection.
- HTTPS-connection - Opens an HTTPS connection.
- Telnet-connection - 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

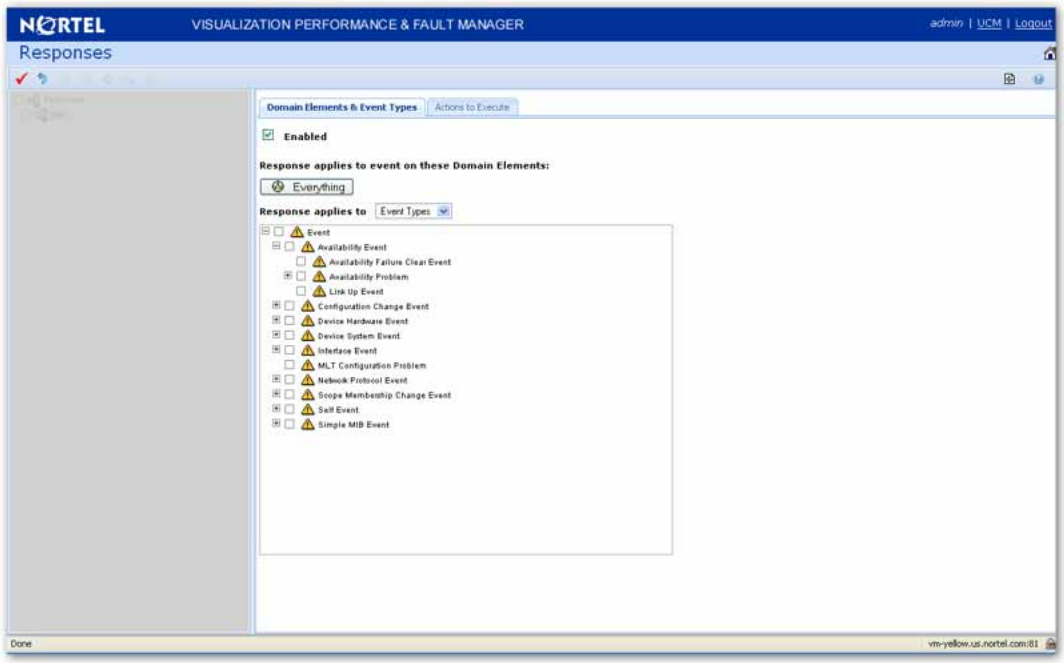
You can sometimes just use an identifier directly when it has a simple value such as ${trigger}, and at other times when the identifier is an object, you must specify a property such as ${event.type}. Sometimes the property of an object is another object in which case you must chain your dot notation as in ${device.campus.location}.

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

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:



- 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)

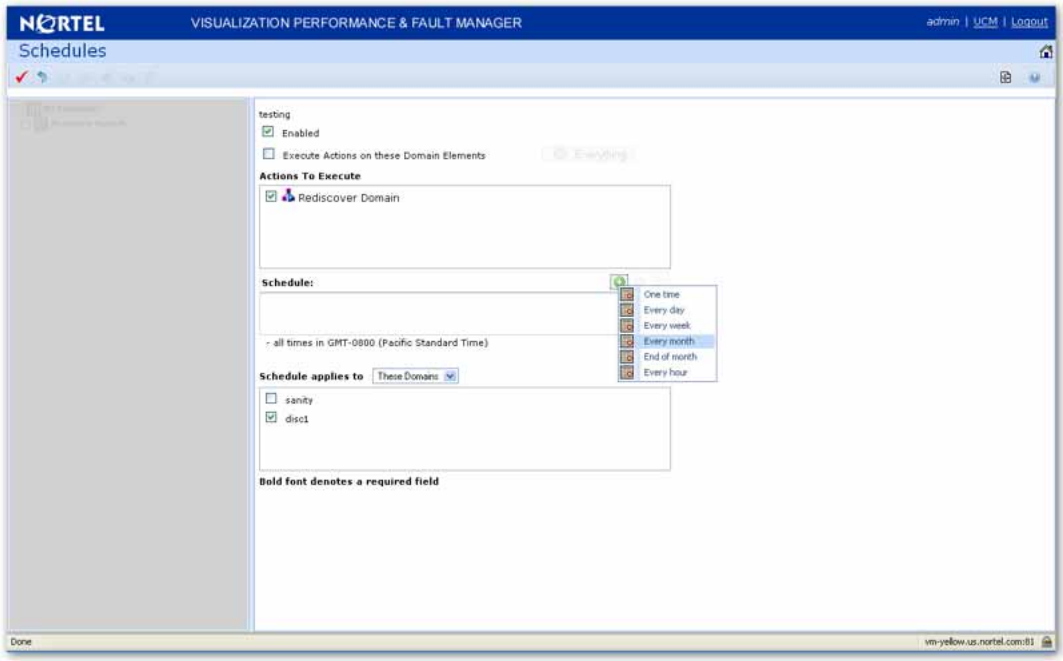
- An event is correlated (triggers a response when the event is correlated)
- Execute the Following Actions - Displays a list of existing actions that are valid for the currently specified scope.

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, log into VPFM and click the By Schedules link located on the Welcome page.

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.

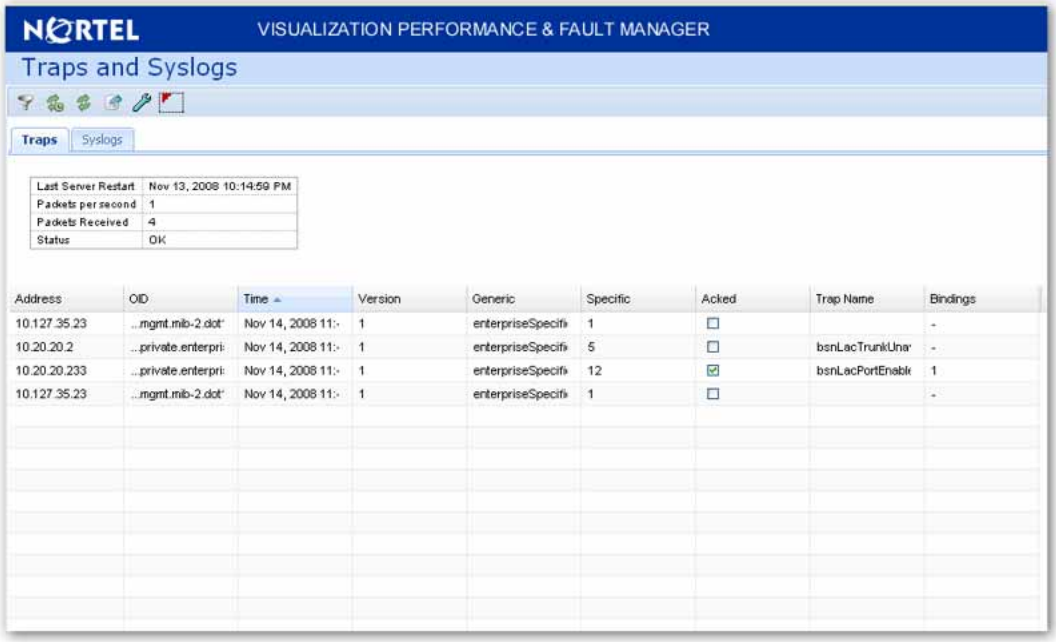
The following fields display on the right-side panel of the Action Scheduler page when editing or viewing an action schedule:

- 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)

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, log on to VPFM and click the Traps and Syslogs link located on the Welcome page.

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



- 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.
- 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.

Syslogs tab

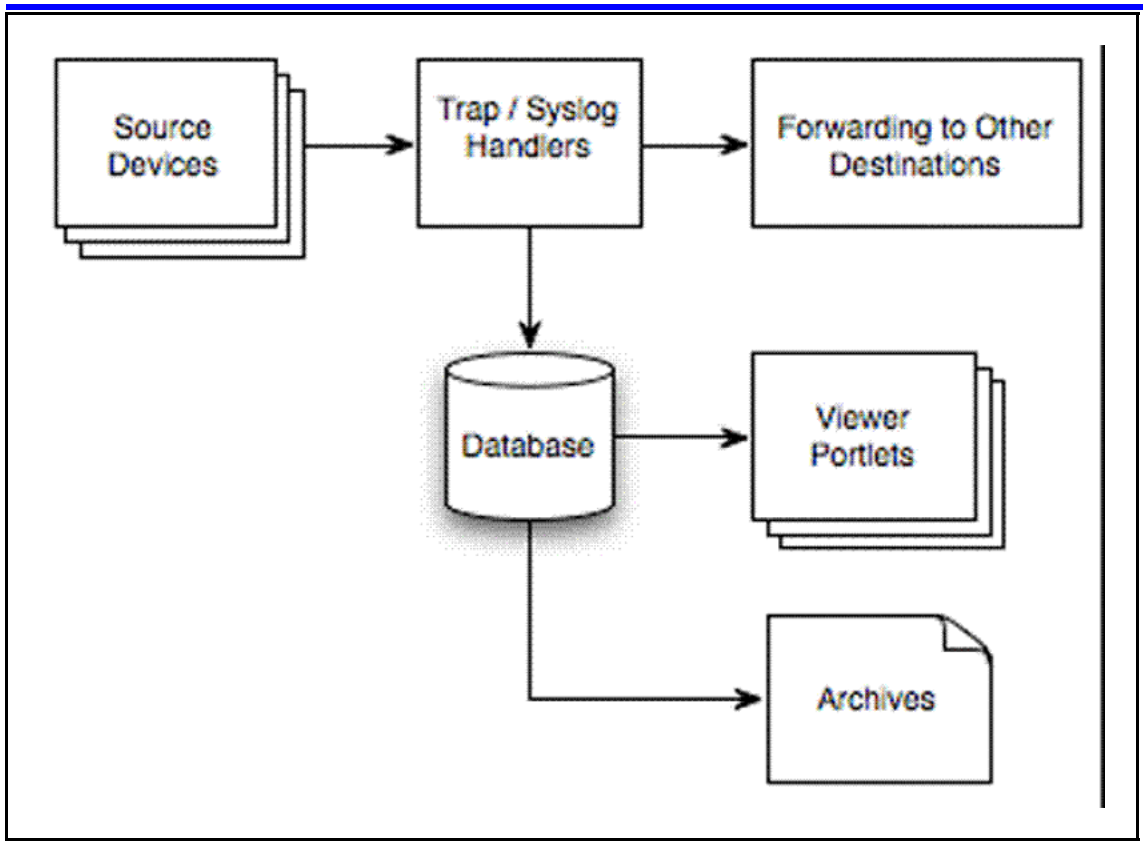
The communication protocol for traps supports specification of original source address. This is not true for Syslogs, the subject address cannot be reliably parsed from a syslog message because of the different formats in use.

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. The general flow of information is as follows:



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

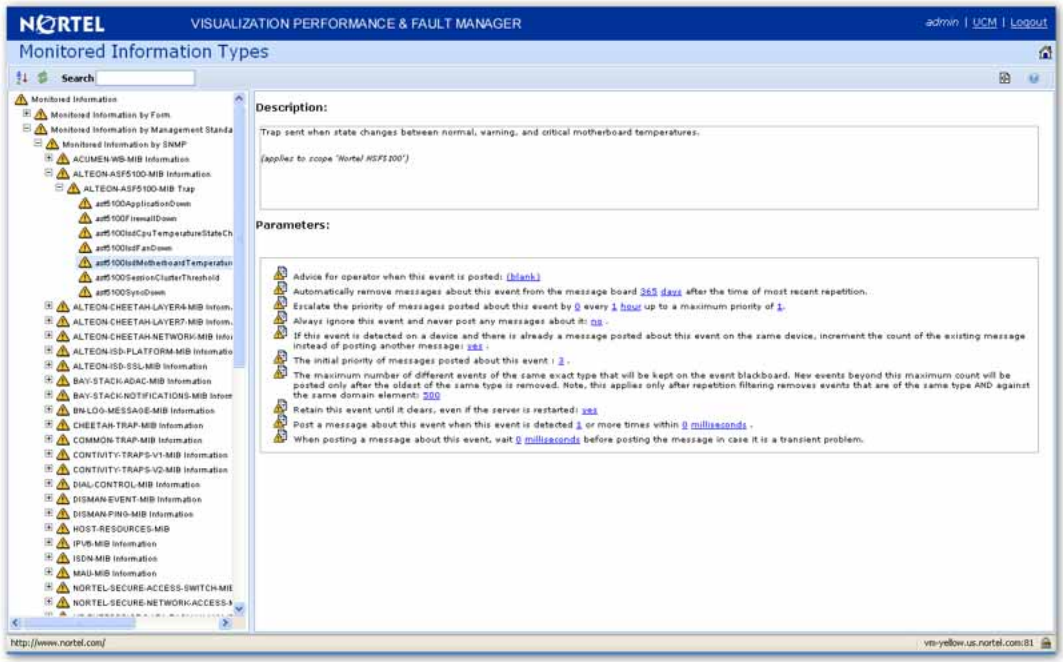
- Listening - You can configure the VPFM through the Traps/Syslogs Configuration to listen to non-default ports. If you do this, the VPFM listens on default ports 162/514 if they are available and the VPFM can get them from the operating system.
- Forwarding - You can configure VPFM to forward to multiple destinations. The original source address that is encoded in the trap/syslog is not affected by the forwarding, so a forwarded trap does not appear to have come from the VPFM server.
- 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.

You configure MIT by selecting Monitoring Information Types at the Welcome page.

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



- 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

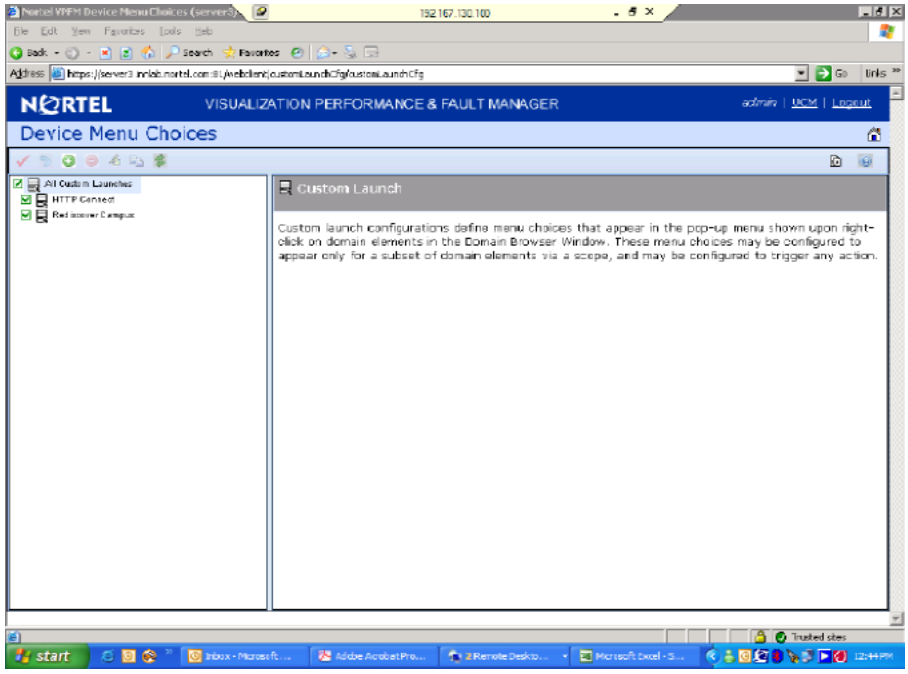
Device Menu Choices

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.

You configure Device Menu Choices by selecting By Device Menu Choice on the Welcome page. The following general controls are available on the Device Menu Choices page:



- 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, select the Monitoring link on the Welcome page. 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.

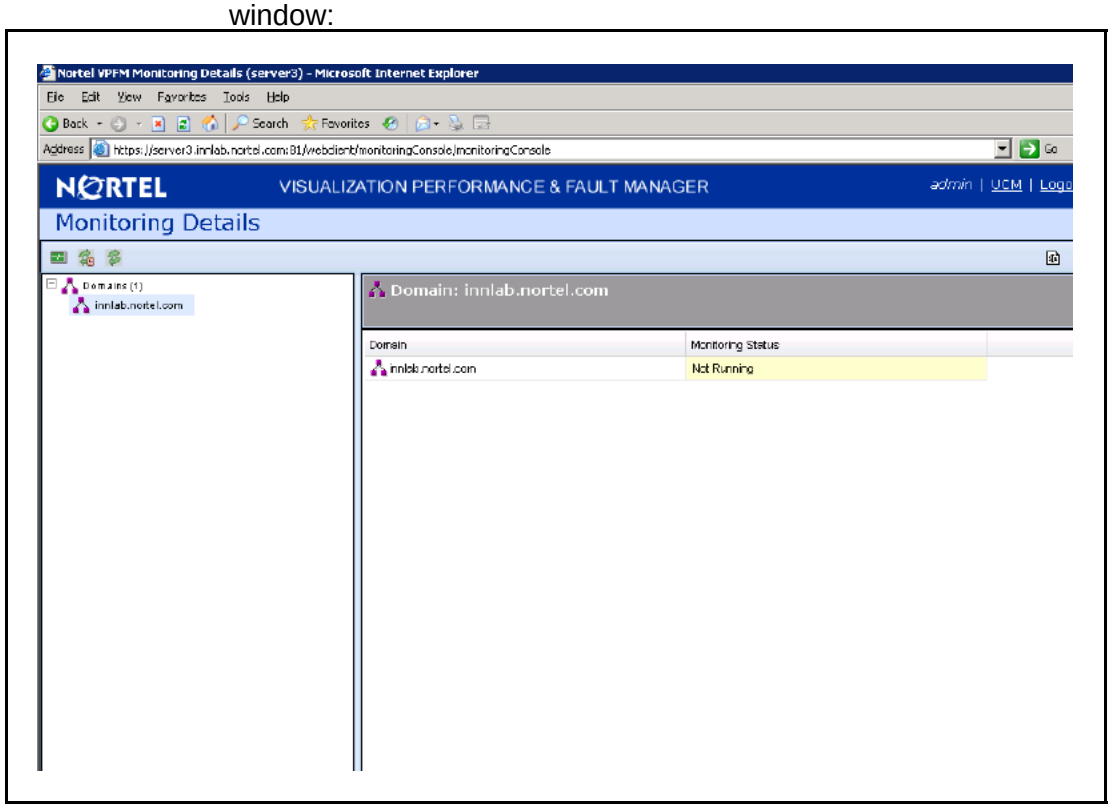
Monitoring details browser

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 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.

Network Discovery configuration

Perform the following procedures to configure network discoveries on your VPFM. For information about how to perform a discovery, see *VPFM Fault and Performance* (NN48014-700).

Click the link below to view a multimedia demonstration about configuring a discovery recipe. http://www31.nortel.com/webcast.cgi?id=8913

Navigation

Perform the following procedures to configure network discoveries.

For more information about network discovery, see "Network Discovery" (page 10). For information about performing a network discovery, see the *Nortel VPFM Fault and Performance Guide* (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 Nortel VPFM. A discovery domain is a virtual representation of part or all of a network.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **Network Discovery** link. 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.

--End--

Cloning discovery domains

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

Attention: 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.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM Welcome page, click the **Network Discovery** link. The Network Discovery page appears.
2	Select the domain you want to clone.
3	From the Network Discovery menu bar, click the **Clone the 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.

--End--

Deleting discovery domains

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

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM Welcome page, click the **Network Discovery** link. The Network Discovery page appears.
2	Select the domain you want to delete.
3	From the Network Discovery menu bar, click on the **Delete selected domain** button. A dialog box appears to confirm deletion.
4	Click **Ok**.

--End--

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.

Click the link below to view a multimedia demonstration about creating a partitioning seed. http://www31.nortel.com/webcast.cgi?id=8910

Prerequisites

- Log on to VPFM.
- Click the Network Discovery link.
- Add a network discovery domain.

Procedure Steps

Step	Action
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. A dialog box appears.
3	Select either **Router** or **IP Subnet** to indicate the type of seed you want to add.
4	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.
5	Select the **Enabled** checkbox.
6	If you want VPFM to partition the selected subnet to find router-based seeds, select the **Partition** checkbox.

7	Click **OK**. The system adds a list of router-based seeds to the seed list.
8	To save the changes, click **Apply your changes** button.

--End--

Editing seeds

Edit a seed to modify the value of the seed.

Prerequisites

- Log on to VPFM.
- Click the Network Discovery link.
- Add a discovery domain and a seed.

Procedure Steps

Step	Action
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 the **Edit** button.
4	Modify the seed as needed.
5	Click **OK**.
6	To save the changes, click **Apply your changes** button.

--End--

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.

Prerequisites

- Log on to VPFM.
- Click the Network Discovery link.
- Add a network discovery domain and a seed.

Procedure Steps

Step	Action
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**.

--End--

Deleting seeds

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

Prerequisites

- Log on to VPFM.
- Click the Network Discovery link.
- Add a network discovery domain and a seed.

Procedure Steps

Step	Action
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 the **Delete** button located at the top of the Seeds box.
	There is no delete confirmation, the seed is deleted immediately
4	To save the change, click the **Apply your changes** button.

--End--

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.

Prerequisites

- Log on to VPFM.

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

Procedure Steps

Step	Action
1	Click the **Network Discovery** link. The Network Discovery page appears.
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. A dialog box appears.
4	Type a Subnet value. Subnet value must be in network prefix notation or a range. For example, 172.16.67.0/24 is a valid network prefix notation. Alternatively, 172.16.67.0-172.16.255.255 is an example of a valid range.
5	Click **Ok**. The new limit appears in the Limit to subnet box.
6	To save the change, click the **Apply your changes** button.

--End--

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.

Prerequisites

- Log on to VPFM.

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

Procedure Steps

Step	Action
1	Click the **Network Discovery** link. The Network Discovery page appears.
2	From the Limit to subnet box select the limit that you want to edit.
3	In the **Limit to Subnets** box, click the **Edit** button. A dialog box appears.
4	Edit the limit as needed.
5	Click **Ok**.
6	To save the changes, click the **Apply your changes** button.

--End--

Deleting limits to subnets

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

Prerequisites

- Log on to VPFM.

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

Procedure Steps

Step	Action
1	Click the **Network Discovery** link. The Network Discovery page appears.
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 the **Delete** button. There is no delete confirmation, the limit is deleted immediately.
5	To save the changes, click the **Apply your changes** button.

--End--

Adding exclusions

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

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **Network Discovery** link. The Network Discovery page appears.
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 the **Add** button. A dialog box appears.
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 the **Apply your changes** button.

--End--

Variable definitions

Variable	Value
Filter Type	
Device Type	Exclude all devices of a certain type.
IP address/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.*.
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.

Variable	Value
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
Server	Network-connected computer hardware that provides specific services onto the network.
Switch	Layer-2 switch
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

Editing exclusions

Edit an exclusion to modify the discovery of your network.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **Network Discovery** link.
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. Enter an exclude filter definition dialog box appears.

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 the **Apply your changes** button.

--End--

Variable definitions

For information about variables for Editing exclusions, see the variable definitions table for "Adding exclusions" (page 53).

Deleting exclusions

You can delete an exclusion if it is not required.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **Network Discovery** link.
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 the **Delete** button located at the top of the Exclusions box. There is no delete confirmation, the exclusion is deleted immediately.

--End--

Setting the network discovery options

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

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **Network Discovery** link.
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.
4	To save the changes, click the **Apply your changes** button.

--End--

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: 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.

Variable	Value
DNS Lookup	VPFM performs DNS lookup on all devices.
Nortel Only Discovery	Ignores any devices that are not on the approved Nortel list. Includes devices with IDs that begin with one of the following: 15 (Xylogics), 18 (Wellflee), 45 (Synoptics), 335 (Micom, 562 (Nortel), 569 (Armon), 930 (Centillion), 1424 (Performance Technology), 1872 (Alteon), 2272 (Rapid City), 2505 (New Oak), 2865 (Opteron)

Renaming a campus

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

Prerequisites

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

Procedure Steps

Step	Action
1	Click the **Network Discovery** link. The Network Discovery page appears.
2	On the **Network Discovery** page, highlight the campus you would like to rename and click the **Rename campus** button. A dialog box appears.
3	Type a new name for the campus.
4	Click **OK**.

--End--

Manual device discovery

Perform the following procedures to start a manual device discovery.

Navigation

Adding a device to an existing discovery

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

Prerequisites

- You must configure the device to respond to SNMP queries from VPFM.
- Must have an existing pre-discovered domain containing a pre-discovered LAN (routed subnet) to which the new device can be added.

Procedure Steps

Step	Action
1	Click the **Network Discovery** link. The Network Discovery page appears.
2	On the Network Discovery page, click the **Manual Discovery** icon. The Manual Discovery dialog box appears.

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.

--End--

Editing a manual device discovery

Perform the following procedure to edit a manual discovery.

Prerequisites

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

Procedure Steps

Step	Action
1	Click the **Network Discovery** link. The Network Discovery page appears.
2	On the Network Discovery page, click the **Manual Discovery** icon. The Manual Discovery dialog box appears.
3	In the **Previous Requests** panel, select the device to be modified.
4	In the Previous requests panel click the **Edit** button.
5	Modify the value as required.
6	Click **Ok** to save the changes.

--End--

Starting the manual device discovery again

Perform the following procedure to start the manual discovery again.

Prerequisites

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

Procedure Steps

Step	Action
1	Click the **Network Discovery** link. The Network Discovery page appears.
2	On the Network Discovery page, click the **Manual Discovery** icon. The Manual Discovery dialog box appears.
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.
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.

--End--

Deleting a manual device discovery

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

Prerequisites

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

Procedure Steps

Step	Action
1	Click the **Network Discovery** link. The Network Discovery page appears.
2	On the Network Discovery page, click the **Manual Discovery** icon. The Manual Discovery dialog box appears.
3	In the New Requests panel, select the device to be deleted.
4	Click the **Delete** button located at the top of the New Requests panel.

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

--End--

Cancelling a manual device discovery

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

Procedure Steps

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

--End--

Viewing a manual discovery report file

For information on how to view a discovery report, see "Network Discovery" (page 10).

Viewing manual discovery results

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

Procedure Steps

Step	Action
1	Click the **Network Browser** link. 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 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.

--End--

Scope configuration

Perform the following procedures to create scopes on your VPFM system.

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.

Click here to view a multimedia demonstration about creating scopes http://www31.nortel.com/webcast.cgi?id=8005.

Navigation

Perform the following procedures to create scopes.

- "Adding constraint based scopes" (page 63)
- "Adding enumerated member scopes" (page 66)
- "Adding union based scopes" (page 67)
- "Editing scopes" (page 68)
- "Renaming scopes" (page 69)
- "Cloning scopes" (page 70)
- "Deleting scopes" (page 70)

For more information about scopes, see "Scopes" (page 18).

Adding constraint based scopes

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

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM Web Agent Welcome page, select the **Scopes** link.
2	From the Scopes window, click the **Elements** tab to select the Elements domain or Click the **Events** tab to select the Events tab.
3	Click the **Add** button.
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 the **Apply your changes** button.

--End--

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.

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

Variable	Value
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.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM Web Agent Welcome page, select the **Scopes** link.
2	From the Scopes window, click the **Elements** tab to select the Elements domain or Click the **Events** tab to select the Events tab.
3	Click the **Add** button.
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 the **Add** button 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** button.

--End--

Variable definitions

Variable	Value
Scope Members	Specify the domain elements to include in the scope.
Keep Private	Indicates whether or not the scope is to be hidden. A private scope does not show in the list of public scopes and is not seen in the network browser scope perspective.
Comments	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.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM Web Agent Welcome page, select the **Scopes** link.

2 From the Scopes window, click the **Elements** tab to select the Elements domain

or

Click the **Events** tab to select the Events tab.

3 Click the **Add** button.

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** button.

--End--

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.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM Web Agent Welcome page, select the **Scopes** link.
2	From the Scopes window, click the **Elements** tab to select the Elements domain or Click the **Events** tab to select 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 the **Apply your changes** button.

--End--

Renaming scopes

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

Prerequisites

- Log onto VPFM.

Procedure Steps

Step	Action
1	From the VPFM Web Agent Welcome page, select the **Scopes** link.
2	From the Scopes window, click the **Elements** tab to select the Elements domain or Click the **Events** tab to select the Events tab.
3	Select the scope you want to rename.
4	Click the **Rename** button. A Prompt dialog box appears.
5	Enter the new name.
6	Click **OK**.

--End--

Cloning scopes

You can clone an existing scope.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM Web Agent Welcome page, select the **Scopes** link.
2	From the Scopes window, click the **Elements** tab to select the Elements domain or Click the **Events** tab to select the Events tab.
3	Select the scope you want to clone.
4	Click the **Clone** button. A Prompt dialog box appears.
5	Enter a new name for the cloned scope.
6	Click **OK**.

--End--

Deleting scopes

You can delete an existing scope.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM Web Agent Welcome page, select the **Scopes** link.
2	From the Scopes window, click the **Elements** tab to select the Elements domain or Click the **Events** tab to select the Events tab.
3	Select the scope you want to delete.

4 Click the **Delete** button.

A Confirmation dialog box appears.

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

--End--

Monitoring configuration

Perform the following procedures to set up monitoring for your VPFM system.

Navigation

Perform the following procedures to set up monitoring for your VPFM system.

For more information about configuring monitoring, see "Monitoring overrides" (page 20) and "Monitoring configuration" (page 40).

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.

Prerequisites

- Log on to VPFM.
- Select the Monitoring link.

Procedure Steps

Step	Action
1	From the Monitoring window, click the **Add** button. A prompt dialog box appears.
2	Enter the name of the new configuration.
3	Click **OK**.
4	There are two tabs, Basics and Domains. Select the **Basics** tab.
5	In the Basics tab, select the **Enabled** option to enable polling for the configuration.
6	From the **Polling period** list, specify the interval at which the polling must occur.
7	From the **Data retention period** list, specify the duration for which the data can be retained.
8	From the **These Elements** list, select a scope. The information type list shows the modified monitoring information.
9	From the **Monitor for these information types** section, select the appropriate events or categories of events.
10	Select the **Domains** tab.
11	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.
12	To save the changes, click the **Apply your changes** button.

--End--

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.

Variable	Value
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.

Prerequisites

- Log on to VPFM.
- Select the Monitoring link.

Procedure Steps

Step	Action
1	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.
2	Edit the settings as needed.
3	To save the change, click the **Apply your changes** button.

--End--

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.

Variable	Value
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.

Prerequisites

- Log on to VPFM.
- Select the Monitoring link.

Procedure Steps

Step	Action
1	From the Monitoring window, select the configuration you want to rename.
2	Click the **Rename** button. A Prompt dialog box appears.
3	Enter the new name.
4	Click **OK**.
5	To save the change, click the **Apply your changes** button.

--End--

Deleting a monitoring configuration

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

Prerequisites

- Log on to VPFM.
- Select the Monitoring link.

Procedure Steps

Step	Action
1	From the Monitoring window, select the configuration you wish to delete.
2	Click the **Delete** button. A Prompt dialog box appears to confirm the deletion.
3	Click **OK**.

--End--

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" (page 42) and "Viewing active monitoring configurations" (page 78).

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **Monitoring Details Browser** link. The Monitoring Details 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 the **Start Monitoring button**. Monitoring begins for the selected domain. When monitoring starts for a selected domain, the expandable list of domains and agents is refreshed.

--End--

Variable definitions

Variable	Value
Domains	A container element for the list of domains for your system.

Variable	Value
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.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **Monitoring Details Browser** link. The Monitoring Details page appears.
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.
	--End--

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" (page 20).

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click the **Monitoring Overrides** link. 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 the **Add** button. The Enter Desired Override Entry Name window appears.
3	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	For event processing overrides, from the **Overrides Applies to** box, select whether the override applies to an event scope or event type. After you select an option, you can then use the tree selection list to specify the appropriate event scope or event type.

7 Click the **Add domain element scope** link. The Select a scope window appears.

8 Expand the tree structure and select the scope to which you want the monitoring override to apply.

9 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.

10 Click **Ok**.

The Parameter Override window appears.

11 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.

12 Select the parameter for which you want to define the override. The parameter description and value appear in the bottom right box.

13 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.

14 After you select the desired override value click **Ok**.

15 To save your changes, click **Apply**.

--End--

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.
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

Variable	Value
	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.

Editing an override

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

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click the **Monitoring Overrides** link. The Monitoring Overrides page appears. 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 the **Apply your changes** button.

--End--

Renaming an override

After you create an override you can change the name.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click the **Monitoring Overrides** link. The Monitoring Overrides page appears.
2	Select the override you want to rename.
3	Click the **Rename** button.

A Prompt dialog box appears.

4 Enter the new name.

5 Click **OK**.

--End--

Cloning an override

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

Prerequisite

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click the **Monitoring Overrides** link. The Monitoring Overrides page appears.
2	Select the override you want to clone.
3	Click the **Clone** button. A Prompt dialog box appears.
4	Enter a new name for the cloned override.
5	Click **OK**.

--End--

Deleting an override

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

Prerequisites

- Log onto VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click the **Monitoring Overrides** link. The Monitoring Overrides page appears.
2	Select the override you want to delete.
3	Click the **Delete** button.

A Confirmation dialog box appears.

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

--End--

Trap and syslog configuration

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

Navigation

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

- "Configuring Traps Viewer settings" (page 85)
- "Configuring Syslog Viewer settings" (page 86)

For more information about traps and syslog, see"Traps, Syslogs, and Events" (page 31).

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.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **Trap and Syslog Browser**.
2	Select the **Traps** tab.
3	On the Traps and Syslogs page, click **Settings**.
	The Traps Configuration Settings window appears.
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, enter the destination IP address for trap information.
12	Click **Ok** to save the changes.

--End--

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.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **Trap and Syslog Browser**. The Traps and Syslogs page appears.
2	Select the **Syslogs** tab.
3	On the Traps and Syslogs page, click **Settings**. The Syslog Configuration Settings window appears.
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 syslog 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, enter the destination IP address for syslog information.

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

--End--

MIB configuration

If you have a new device that you want to monitor you can import the required MIBs using the VPFM Administrator client. After you load the MIB, VPFM generates a new event type for each SNMP notification and trap defined within the MIB.

Adding a MIB

You can add a MIB using the VPFM Administrator Client.

Procedure Steps

Step	Action
1	On your computer go to **Start >Programs>Nortel> 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.
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**.

--End--

MIT configuration

Perform the following procedures for MIT configuration.

Navigation

Perform the following procedures for MIT configuration.

- "Configuring Monitored Information Types" (page 91)
- "Viewing Monitored Information Types" (page 92)

For more information about MIT configuration, see "MIT " (page 36).

Configuring Monitored Information Types

You can modify the parameters of the MITs.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **Monitored Information Types** link. The Monitored Information Types page appears.
2	Select the hierarchical or alphabetical view using the view toggle.
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.

--End--

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 MITs.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **Monitored Information Types** link. The Monitored Information Types page appears.
2	Select the hierarchical or alphabetical view using the view toggle.
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.

--End--

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.

Automating configuration tasks

VPFM allows you to automate actions, responses, and schedules. The procedures in this section show how to configure these tasks.

Navigation

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" (page 22).

Click here to view a multimedia demonstration about creating actions. http://www31.nortel.com/webcast.cgi?id=8004.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **Actions**. The Actions page appears.
2	On the Actions page, select the action group to which you want to add an action by highlighting its folder in the left panel of the Actions page.
3	Click the **Add** button. A drop-down menu displays the available action types.
4	Select the appropriate action type. A Prompt dialog box appears.
5	Type a name for the action you are creating in the box and 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.**.

--End--

Renaming an action

After you create an action you can change the name.

Prerequisites

Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **Actions**. The Actions page appears.
2	Select the action you want to rename.
3	Click the **Rename** button. A Prompt dialog box appears.

4 Enter the new name.

5 Click **OK**.

--End--

Cloning an action

After you create an action you can clone it.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **Actions**.
	The Actions page appears.
2	Select the action you want to clone.
3	Click the **Clone** button.
	A Prompt dialog box appears.
4	Enter a new name for the cloned action.
5	Click **OK**.

--End--

Deleting an action

You can delete an action if you do not need it.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **Actions**.
	The Actions page appears.
2	Select the action you want to delete.
3	Click the **Delete** button.
	A Confirmation dialog box appears.

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

--End--

Creating a response

Responses define the ways in which 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" (page 28).

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **By Event Response**.
2	On the By Event Response page, click **Add**. A Prompt dialog box appears.
3	Type a name for the response and click **Ok**. The Domain Elements and Event Types and Actions to Execute tabs appear.
4	Select the **Domain Elements and 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.
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**.

--End--

Renaming a response

After you create a response you can change the name.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **By Event Response**. The Responses page appears.
2	Select the response you want to rename.
3	Click the **Rename** button. A Prompt dialog box appears.
4	Enter the new name.
5	Click **OK**.

--End--

Cloning a response

After you create a response you can clone it.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **By Event Response**. The Responses page appears.
2	Select the response you want to clone.
3	Click the **Clone** button. A Prompt dialog box appears.

4 Enter a new name for the cloned response.

5 Click **OK**.

--End--

Deleting a response

You can delete a response if you do not need it.

Prerequisites

- Log onto VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **By Event Response**. The Responses page appears.
2	Select the response you want to delete.
3	Click the **Delete** button. A Confirmation dialog box appears.
4	Click **OK** to confirm the deletion.

--End--

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" (page 30).

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **By Schedule**.
2	Click **Add**.

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 To select the interval for the schedule to execute the defined actions, click **Add**.

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.

9 Specify the applicable domains.

10 Click **Apply your changes**.

--End--

Renaming an action schedule

You can rename an action schedule after you create it.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **By Schedule**.
	The Schedules page appears.
2	Select the schedule you want to rename.
3	Click the **Rename** button.
	A Prompt dialog box appears.
4	Enter the new name.
5	Click **OK**.

--End--

Cloning an action schedule

After you create an action schedule you can clone it.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **By Schedule**.
	The Schedules page appears.
2	Select the schedule you want to clone.
3	Click the **Clone** button.
	A Prompt dialog box appears.
4	Enter a new name for the cloned schedule.
5	Click **OK**.

--End--

Deleting an action schedule

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

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **By Schedule**.
	The Schedules page appears.
2	Select the schedule you want to delete.
3	Click the **Delete** button.
	A Confirmation dialog box appears.
4	Click **OK** to confirm the deletion.

--End--

Creating a domain rediscovery schedule

A domain rediscovery schedule enables you to automate the rediscovery of your domain.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **By Schedule**.
	The Schedules appears.
2	On the Schedules page, click **Add**.
	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**.

--End--

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" (page 38).

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **By Device Menu Choice** link. The Device Menu Choices page appears.
2	Click the **Add** button. A dialog box appears.
3	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**.

--End--

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.
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.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	Click the **By Device Menu Choice** link. The Device Menu Choices page appears.
2	Click the **Add** button. A dialog box appears.
3	Type a name for the device menu choice in the dialog box. For example, telnet_https.
4	In the right panel, click the **Everything** button.
5	From the list in the dialog box, select **Devices** and click **Ok**.
6	Select **Enabled** check box.
7	Select **Obtain user confirmation before executing** check box.
8	From the **Make these actions available** list, select the actions you want to launch.
9	Click **Apply your changes**.
10	Go back to the Welcome page and click the **Network Browser** link.
11	Right click on any device for which you want to launch a Telnet/Http/Https/Ftp session.
12	From the list, select **Tools** and click the option you want to launch.

--End--

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.

Prerequisites

- Log on to VPFM.

Procedure Steps

Step	Action
1	From the VPFM main page, click **Actions**. The Actions page appears.
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. A Prompt dialog box appears.
5	Type a name for the action you are creating in the box and click **OK**.
6	Specify values for all mandatory parameters and for any optional parameters you want to use.
7	Click **Apply your changes.**.

--End--

Variable definitions

Variable	Value
Name	The name for this action.
Subject type	The scope to which the web browser action will apply.
Event type	—

Variable	Value
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.

Supported Nortel devices

The following table lists Nortel devices that VPFM supports.

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

Device name	Release
Enterprise 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
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)	4.2
ERS 4500 series (4526-FX, 4550T, 4550T-PWR, 4548GT, 4548GT-PWR, 4524GT, 4526GTX, 4526GTX-PWR, 4526T, 4526T-PWR)	5.2
ERS 1424 T	2.1.6
ERS 3510 T	4.0.4
ERS 5510, ERS 5520, ERS 5530-24TFD	5.1, 6.0
ERS 8300	4.0
ERS 8600	4.2/5.0
Business Secure Router 222	2.6
Business Secure Router 252	2.6
Secure Router 1001 and 1001S	9.3
Secure Router 1002, 1004	9.3

Secure Router 3120	9.3
Secure Router 4134	10.1
SNAS 4050	1.0
VPN Router 600 / 1750 / 2700 / 2750 / 5000	8.0
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
Enterprise Voice Devices	
CS1000 E, 1000 S,	5.0
Business Communication Manager 200 , 400	4.0
Business Communication Manager 50	3.0
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 SS 2380	5.0

Nortel Visualization Performance and Fault Manager

Configuration

Printed in Canada
Release: 2.1
Publication: NN48014-500
Document revision: 03.01
Document release date: March 2010

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com