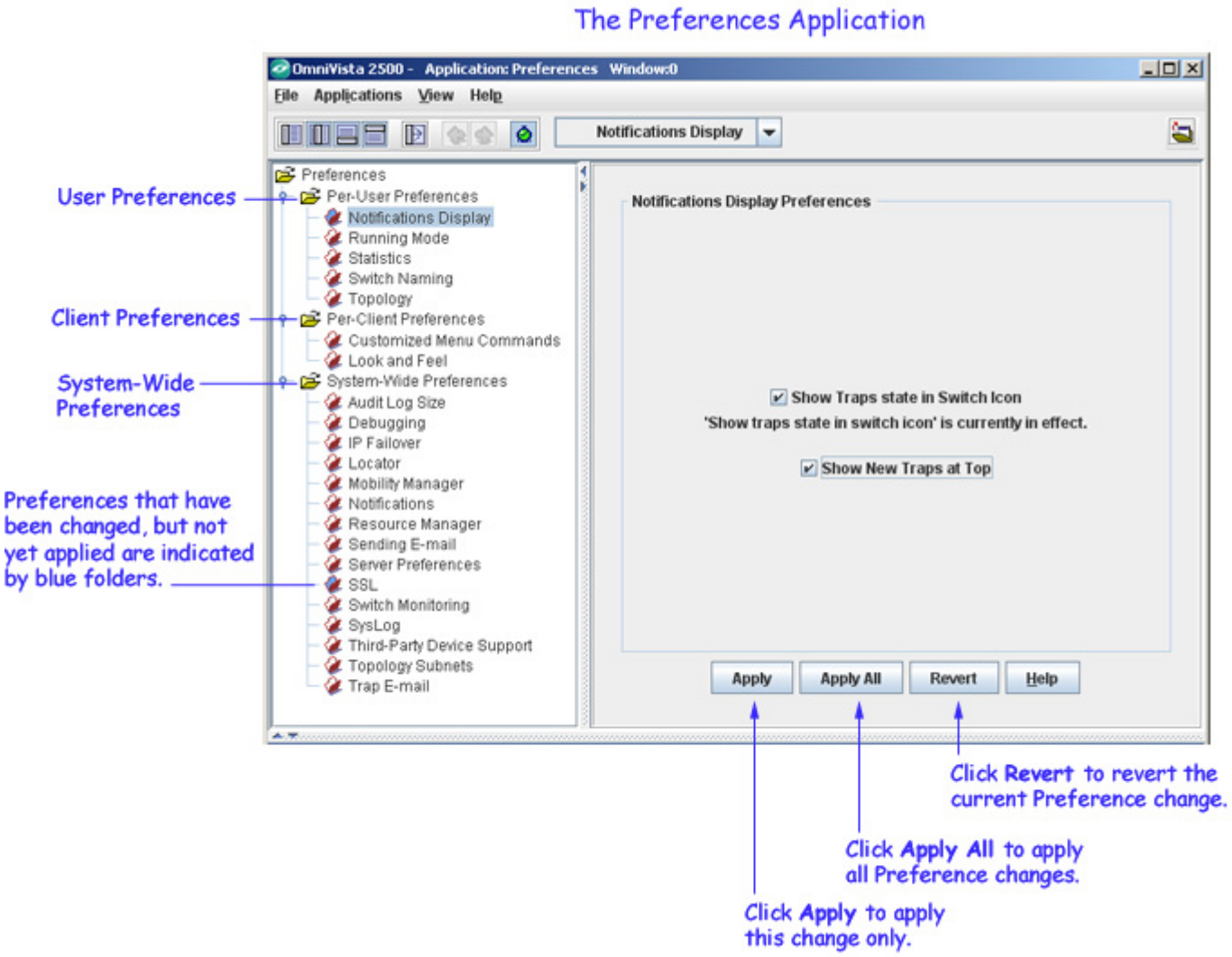
Getting Started with Preferences

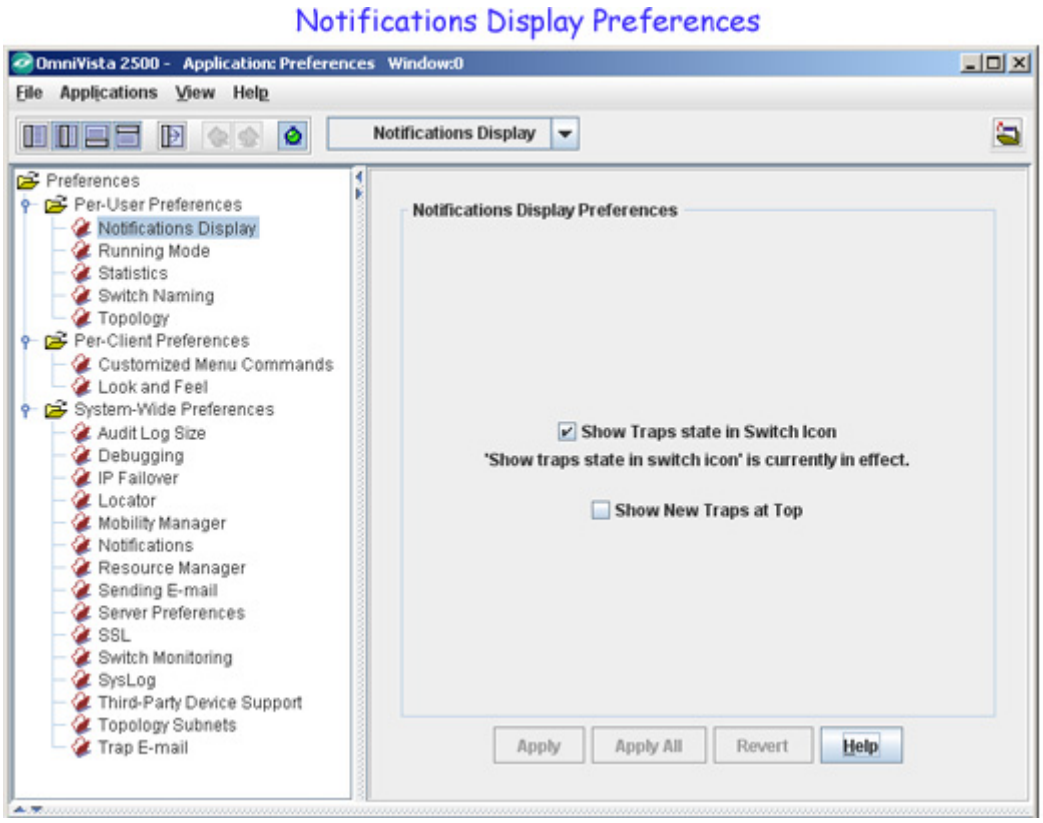
The Preferences application enables you to set preferences for OmniVista behavior that apply to the individual OmniVista user, the individual OmniVista client, and the OmniVista system as a whole. All Preference items have appropriate default values, so there is no need to change Preference settings unless you wish to.

You can navigate to each preference option and apply that change by clicking the **Apply** button (the buttons at the bottom of the window activate when you make a change). You can also change several preferences before applying them. When you change a preference, the folder for that preference is highlighted in blue. To apply all of preference changes, click the **Apply All** button. Click the **Revert** button to return a preference to its initial value. Note that you cannot revert all of the changes at once. You must navigate to each preference window to return that preference to its original value.



Notifications Display Preferences

The Notifications Display Preferences window is used to set trap display settings. By default, the **Show Traps state in Switch** icon is selected. If you change the preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.



Show Traps State in Switch Icon

When this checkbox is enabled, a switch icon will turn orange when a trap is received for the device that has any severity level other than "Normal". When the trap is acknowledged, the switch icon will turn back from orange to green. When this checkbox is disabled, switch icons will not turn orange when a trap with severity other than "Normal" is received. Note the following:

- Even when enabled, this setting is not applicable to the traps with "Normal" severity. Receipt of a trap with "Normal" severity will not cause a switch icon to turn orange.
- Whether enabled or disabled, this setting does not affect switch icons that display red because a switch is down or unreachable. Icons for these switches will display red irrespective of this setting being enabled or disabled.

Show New Traps at Top

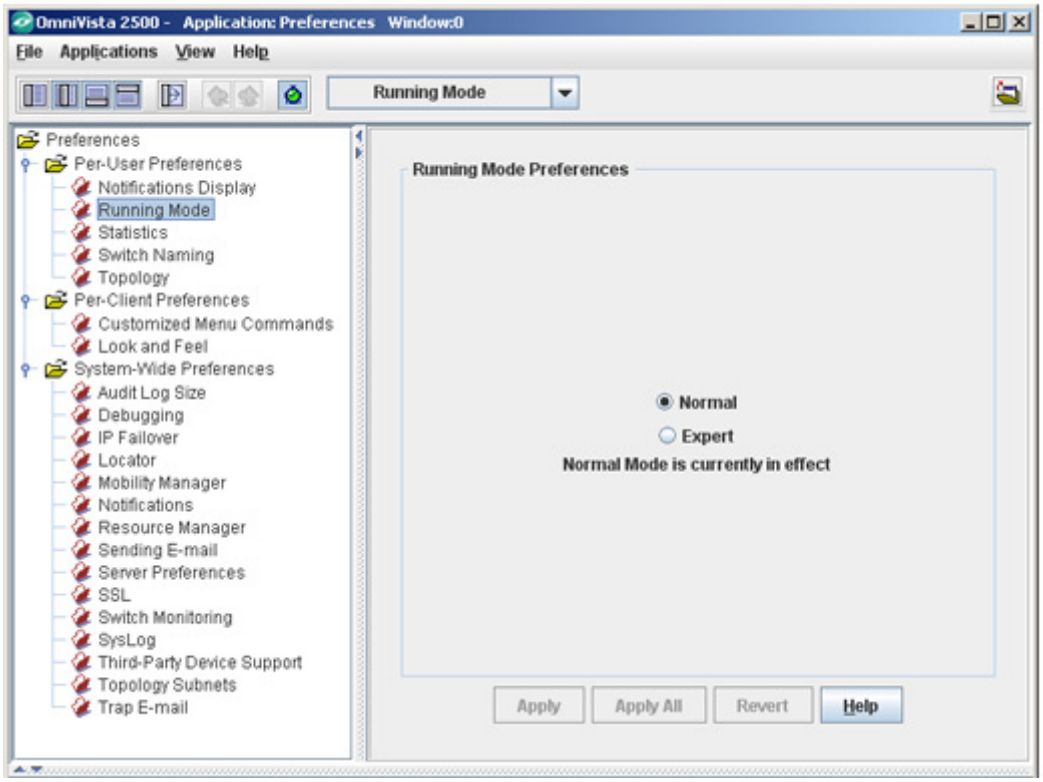
If this checkbox is enabled, the newest traps will be displayed at the beginning of the **Notifications for All Switches** table in the Notifications application, by default.

Running Mode Preferences

The Running Mode Preferences window is used to set the OmniVista running mode. Normal running mode is the normal way to run OmniVista. Expert running mode is a diagnostic tool for developers. Always use Normal running mode unless you are advised otherwise by Customer Service.

If you change the preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.

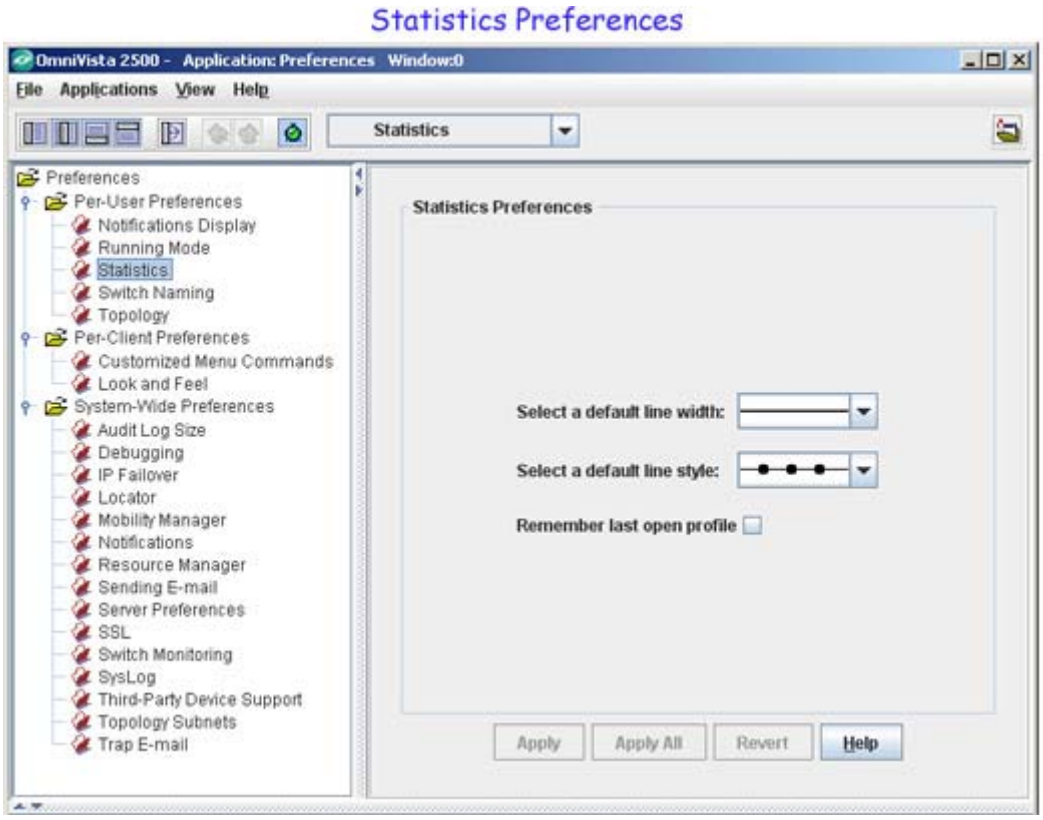
Running Mode Preferences



Statistics Preferences

The Statistics Preferences window is used to specify the default line widths and styles that will display in the Statistics application. To set a line preference, select the line width and/or style from the drop-down menu(s). You can also set the Statistics application to remember the last Statistics profile you viewed by clicking the **Remember last open profile** checkbox. If you enable this feature, the Statistics application will always open the last profile you viewed. See the Statistics application Help for more information.

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.



Switch Name Preferences

The Switch Name Preferences window is used to specify the display mode of the switch in the OmniVista user interface. The following are the display modes:

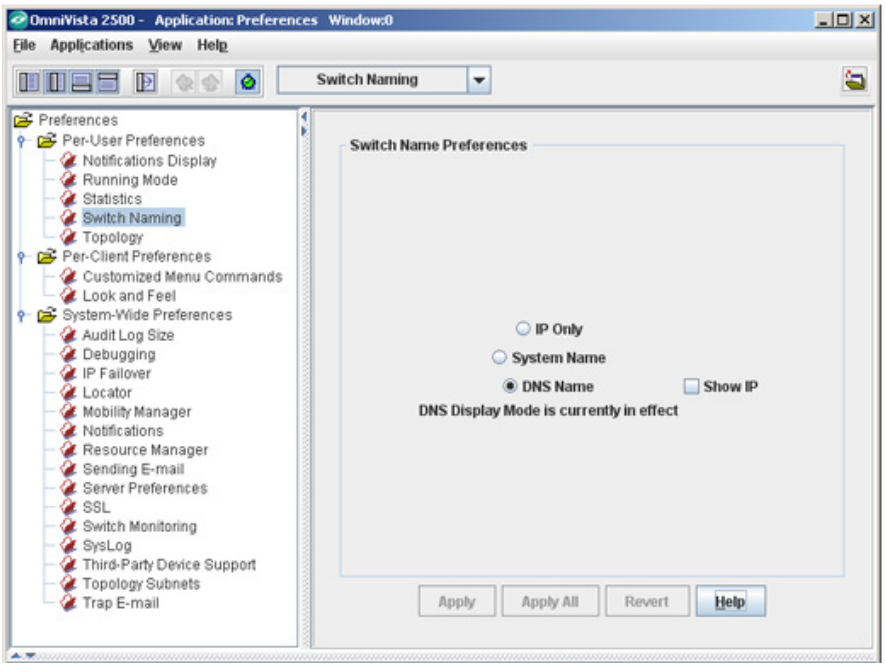
- IP Only
- System Name
- DNS Name.

The **DNS Name** radio button is selected by default. To set the display mode to IP Only or System Name, click the corresponding radio button. If you want to display the system name or the DNS name along with the IP address, click the **Show IP** check box.

> **Note:** The **Show IP** check box is enabled only if either **System Name** or **DNS Name** is selected.

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.

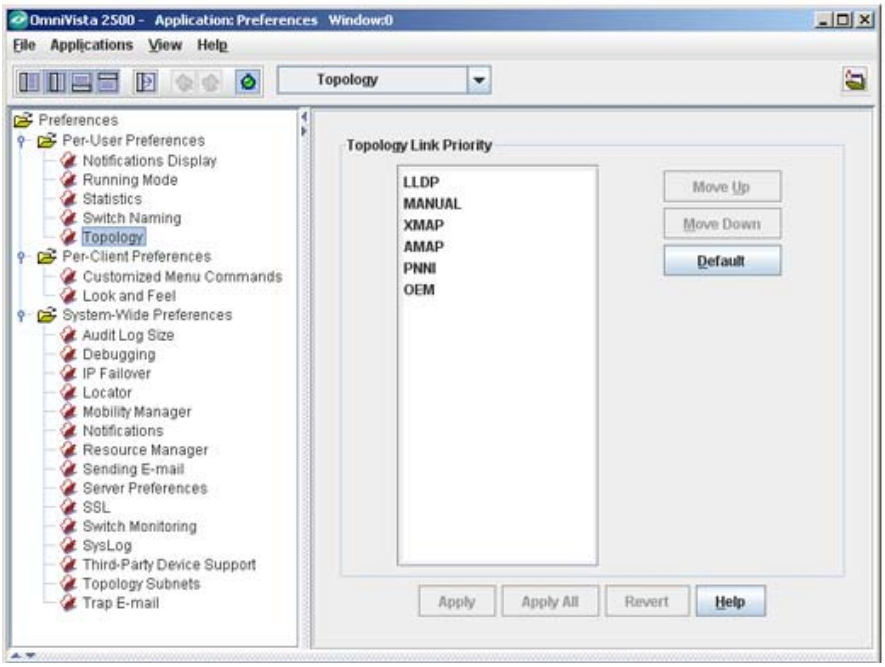
Switch Naming Preferences



Topology Preferences

The Topology Preferences window is used to specify the order of preference for link displays in Topology if the same link is discovered/defined in multiple ways. Select a Link Type and use the **Move Up** or **Move Down** buttons to change the order. Click the **Default** button to return to the default settings. If you change the preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.

Topology Preferences

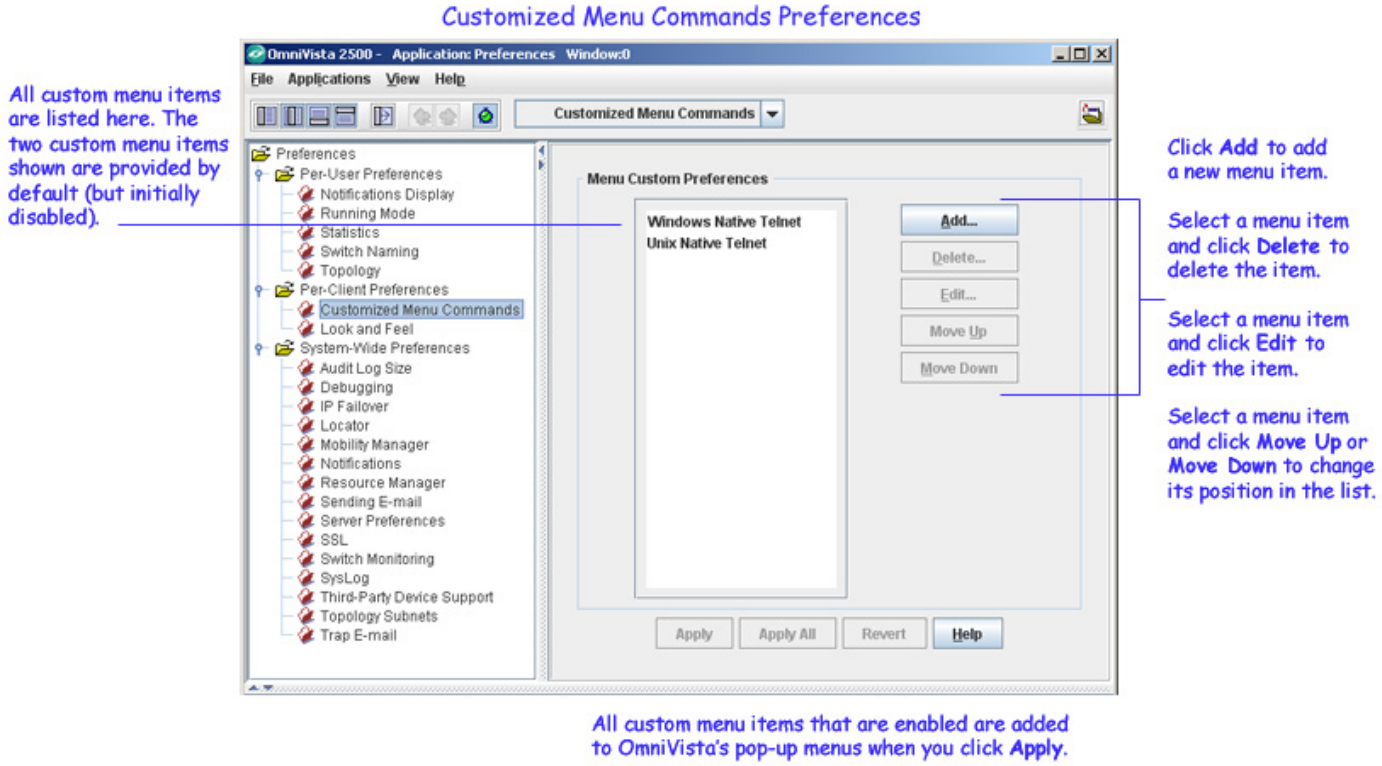


Customized Menu Command Preferences

The Customized Menu Commands Preferences window is used to add custom menu items to OmniVista pop-up menus. You can add a custom menu item for any native command that already exists on the workstation. To display a custom menu item on OmniVista pop-up menus, you must both create it and enable it. When you click the **OK** button on the Customized Menu Commands Preferences window, all custom menu items that are enabled will be added to OmniVista pop-up menus.

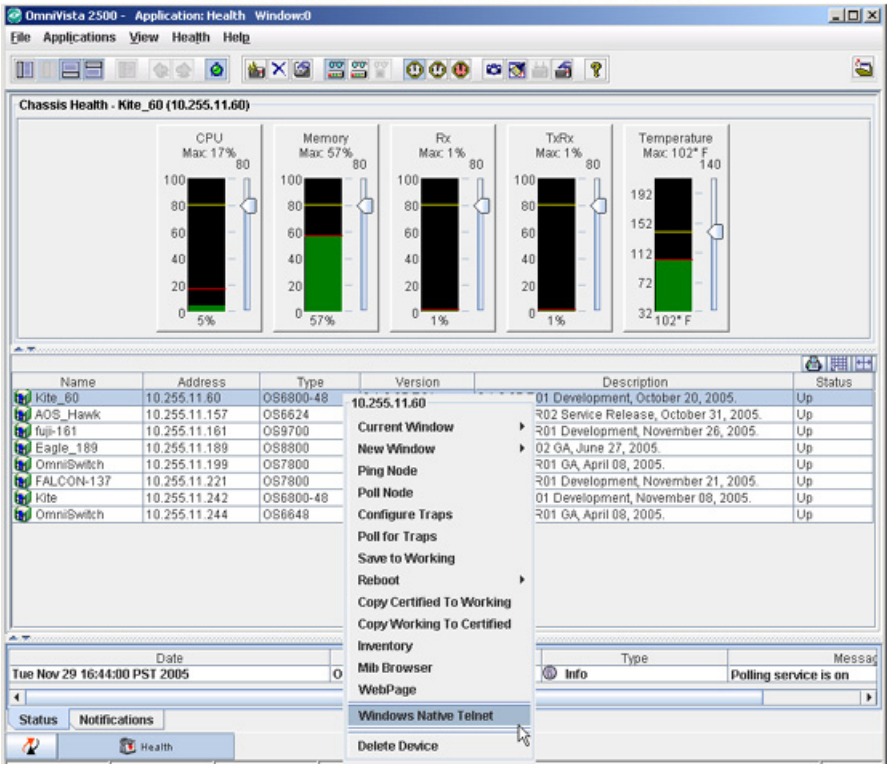
If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.

Note: Two custom menu items are provided by default, but are initially disabled: **Unix Native Telnet** and **Windows Native Telnet**. To use these default custom menu items, you must first enable them.



The screen below shows an OmniVista pop-up menu with the **Windows Native Telnet** custom menu item enabled.

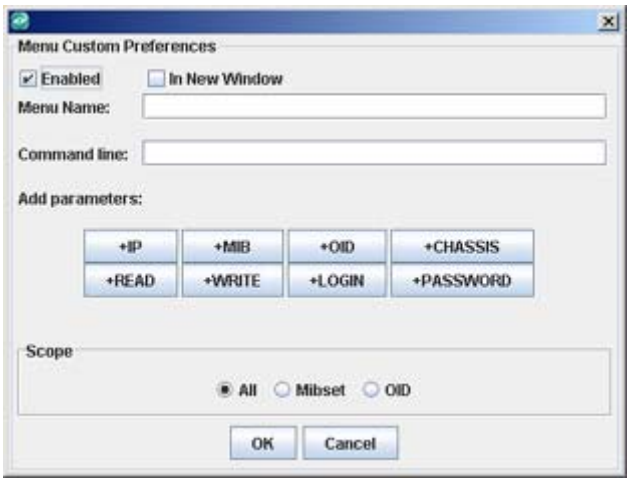
Example of a Custom Menu Item on a Pop-Up Menu



Creating a New Custom Menu Item

You can add a custom menu item for any native command that already exists on the workstation. Follow the steps below to add a new custom menu item.

1. Click the **Add** button on the Customized Menu Commands Preferences window. A window is displayed as shown below. This window enables you to define the new custom menu item.

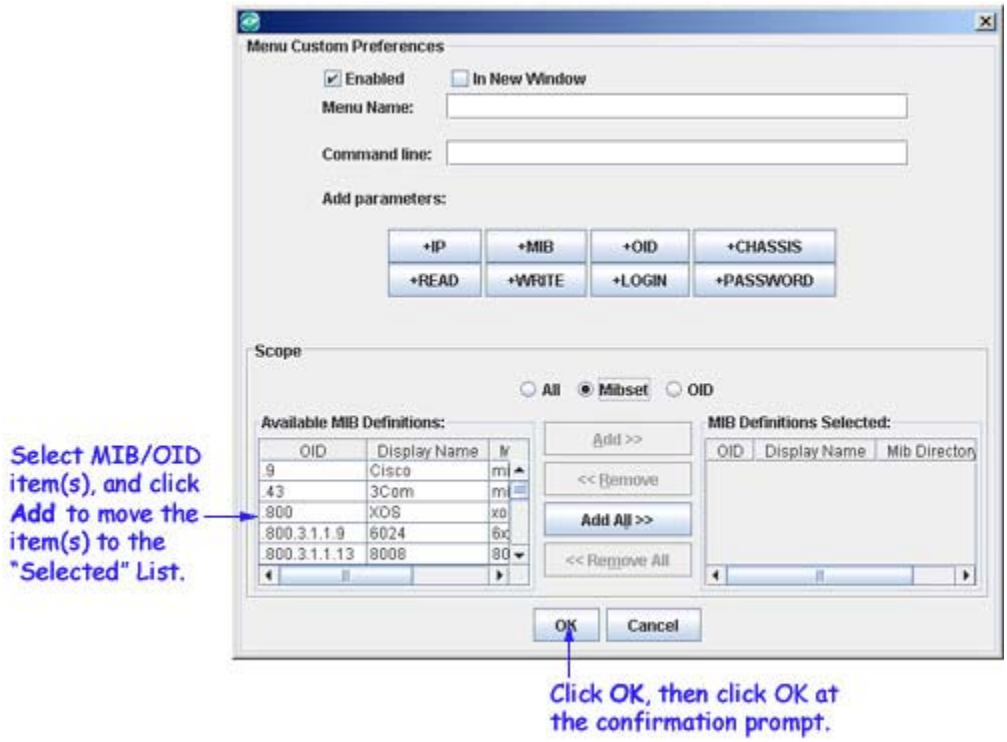


2. The **Enabled** checkbox determines whether the new custom menu item will be enabled after it is created. If a custom menu item is not enabled, it will NOT display on the pop-up menus. The **Enabled** checkbox is checked and active by default. If you wish to create a custom menu item but you do not want it to be displayed at the present time, click the **Enabled** checkbox to

deactivate it. You can edit the custom menu item at a later time to reactivate the **Enabled** checkbox.

3. If you want the new custom menu item to execute in a new window, click the **In New Window** checkbox. Note that this option must be enabled for some commands (e.g., FTP).

4. In the **Scope** area you can define a menu item to appear on **All** devices (Default), or you can define a menu item to appear only in those devices that support the new item, as shown below. If you select **Mibset**, all devices that use the Mibset will include the new menu item. If you select **OID**, all devices whose "sysObjectID" value starts with the OID value will include the new menu item.



Note: You can specify a menu item to appear on specific device types only (e.g., Falcon) by adding the device to the Third Party Device Mibset List in the Third Party Device Support Preferences window. Go to the Third Party Device Support Preferences window and add the device's OID by entering enter the device's "sysObjectID" value in the OID field. The OID for that device will be added to the available MIB Definitions list above.

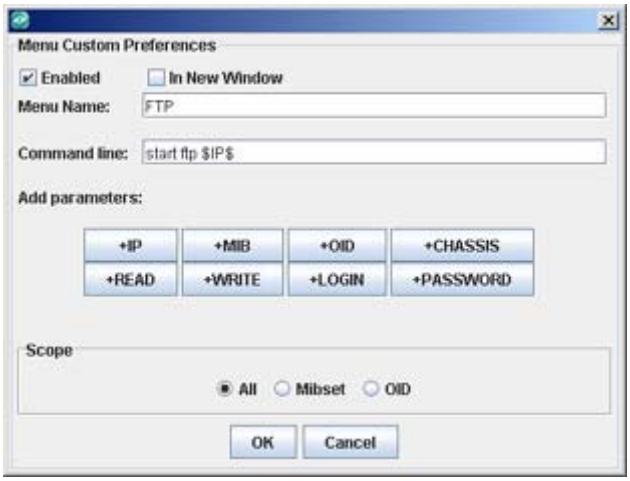
The "sysObjectID" value for the switch can be found by using a Mib browser. To use the OmniVista MIB browser, right-click on a switch in the OmniVista Device tree or the list of discovered devices, then select **Mib Browser**. Click on the "sysObjectID" value in the **org\dod\internet\mgmt\mib-2\system** directory to display the switch's Object ID.

5. In the **Menu Name** field, enter the custom menu item exactly as you want it to appear on pop-up menus.

6. In the **Command Line** field, type the executable that will run when the custom menu item is selected.

7. Add variables to the **Command Line** field by clicking on the desired **Add parameters** buttons. Each **Add parameters button** adds an individual variable to the command line. Each variable translates into an item of information about the switch that is selected when the custom menu item is executed from a pop-up menu.

For example, the screen below shows a custom menu item named **ftp**. The command line for **ftp** is **start ftp**. If you click the **+IP** Add parameter button, **IP** is added to the command line, as shown. The **IP parameter** represents the IP address of the switch that is selected when the custom menu item is executed. The result is that, when the **ftp** custom menu item is executed from a pop-up menu, the following command will execute: **start ftp *ip address***, where ***ip address*** is the IP address of the selected switch. This will open an FTP session directly to the selected switch without the need to type in the IP address.



You can add any of the following variables to the command line:

+IP. Adds the IP address of the selected switch.

+MIB. Adds the name of the MIB set in the selected switch.

+OID. Adds the system object ID of the selected switch.

+CHASSIS. Adds the chassis type of the selected switch.

+READ. Adds the read password of the selected switch.

+WRITE. Adds the write password of the selected switch.

+LOGIN. Adds the FTP user login for the selected switch.

+PASSWORD. Adds the FTP password for the selected switch.

For example, in the CLI, there is a "user" command that takes a username and password for parameters. In that case, you would use the +LOGIN and +PASSWORD when defining the command for Preferences (e.g., > user +LOGIN +PASSWORD). The "user" command can also be used to set Partitioned Management permissions for families of commands. In that case you would use the +READ and +WRITE parameters when defining the command (e.g. > user <partitioned mgmt family> +READ +WRITE).

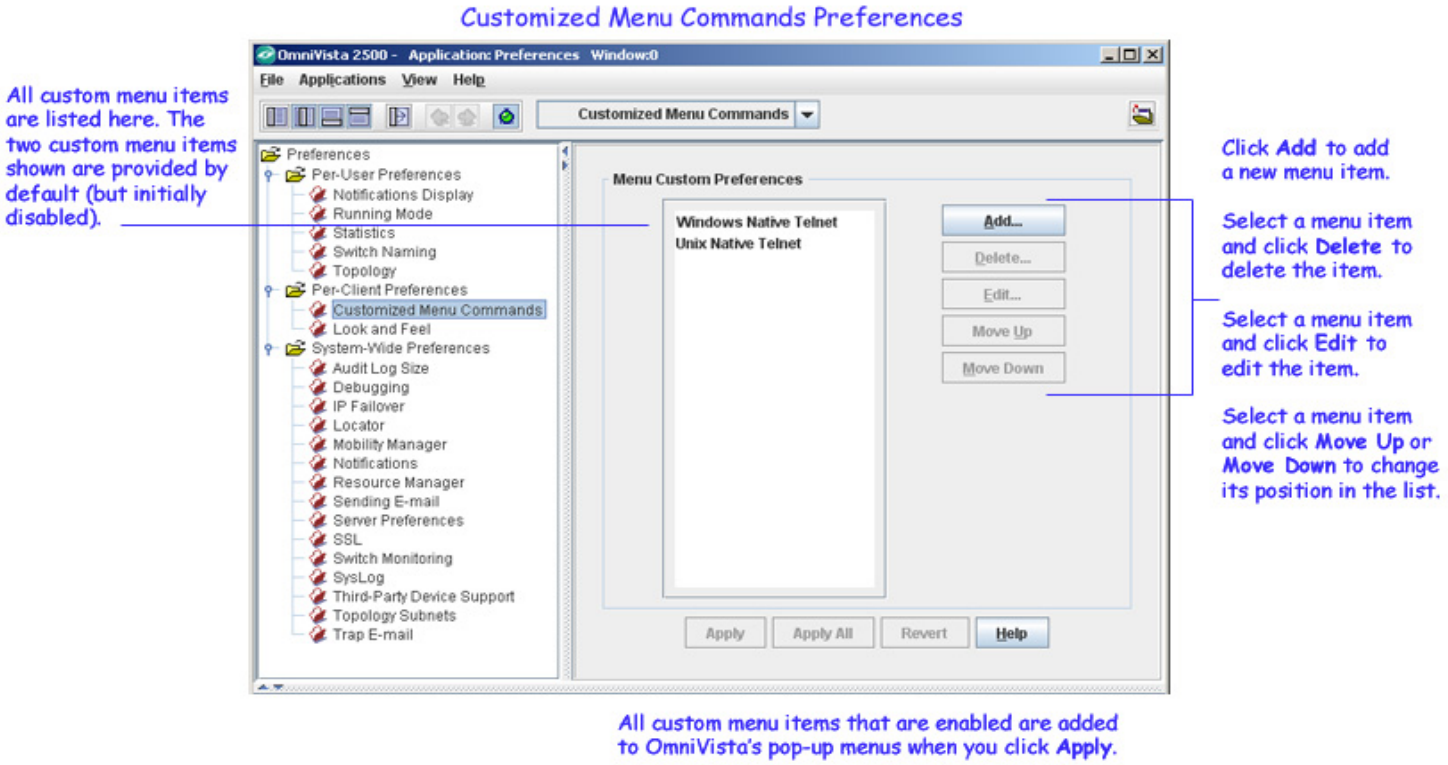
8. Click the **OK** button. You are returned to the **Customized Menu Commands** Preferences window. The new custom menu item is listed in the window.

9. Click the **Apply** button on the Customized Menu Command Preferences Window. You will be prompted to logout of OmniVista and login again. When you do so, all enabled custom menu items will display in pop-up menus.

Enabling a Custom Menu Item

To activate a custom menu item (including the default items), you must enable it. Follow the steps below to enable a custom menu item.

1. Select the menu item that you wish to enable in the Customized Menu Commands Preferences window and click the **Edit** button. The window below displays the selected menu item in the Menu Name field (e.g., Windows Native Telnet).



2. Click the **Enabled** checkbox to activate the menu item. If you want the new custom menu item to execute in a new window, click the **In New Window** checkbox. Note that this option must be enabled for certain commands (e.g., FTP).

3. Click the **OK** button. You are returned to the Customized Menu Commands Preferences window.

4. Click the **Apply** button on the **Customized Menu Commands** Preferences window. You will be prompted to logout of OmniVista and login again. When you do so, all enabled custom menu items will display in pop-up menus.

Editing a Custom Menu Item

You can edit any existing custom menu items. Select the desired menu item in the Customized Menu Commands Preferences window and click the **Edit** button. You can change any field. When your changes are complete, you will be prompted to logout of OmniVista and login again.

Deleting a Custom Menu Item

To delete a custom menu item, select it in the Customized Menu Commands Preferences window and click the **Delete** button. You will be prompted to logout of OmniVista and login again.

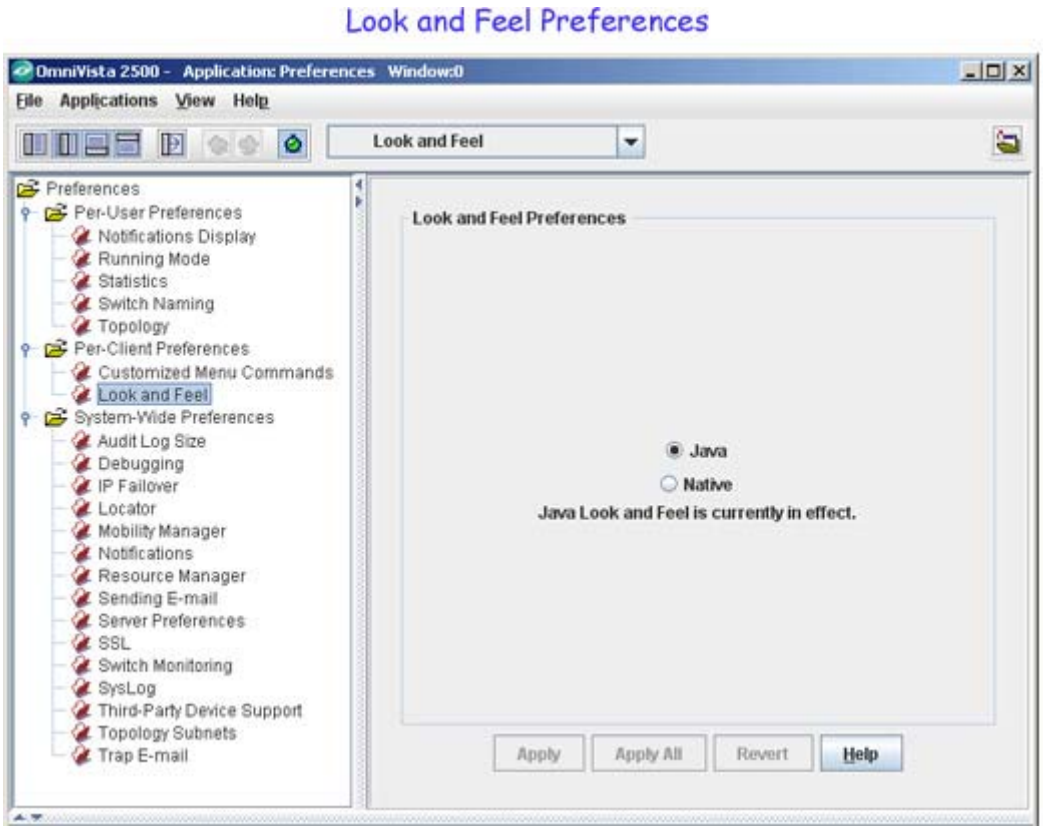
Moving Up/Down a Custom Menu Item

When you add multiple custom menu commands in the Customized Menu Commands Preferences window, you can organize the order in which they appear in the list. To move a menu command up the order, select the custom menu item in the **Menu Custom Preferences** panel and click the **Move Up** button. Similarly, to move a menu command down the order, select the custom menu item in the **Menu Custom Preferences** panel and click the **Move Down** button.

Look and Feel Preferences

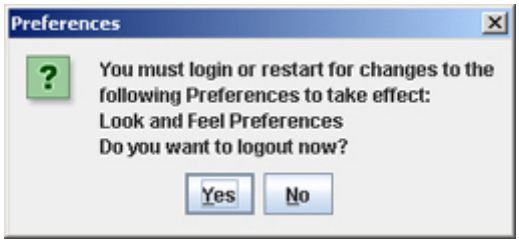
The Look and Feel Preferences window is used to set the overall OmniVista display. OmniVista can display with a Java "look and feel" or with a native look and feel (the look and feel of your current operating system). Java look and feel is the default.

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.



1. Click one of the look and feel options: **Java** (the default) or **Native** (the look and feel of your current operating system). The buttons at the bottom of the page will activate.

2. Click the **Apply** button. A confirmation prompt displays.

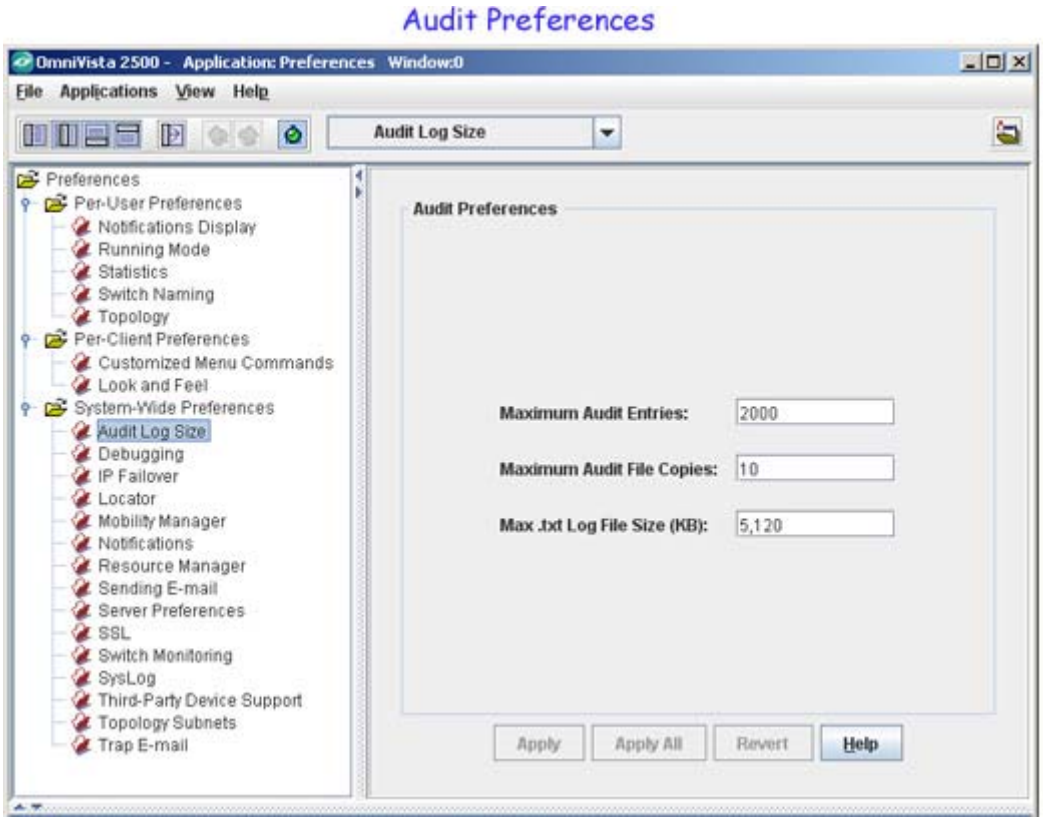


3. Click **Yes** to close all applications, logout, and log back into OmniVista. The new look and feel will take effect when you log back in. Click **No** to exit the window and continue using the current look and feel.

Audit Log Size Preferences

The Audit Log Size Preferences window is used to specify the maximum number of entries that can exist in any one log file listed in the Audit Application. You can also specify the maximum size, in KB, of the server.txt file. (Log files and the server.txt file are accessed from the Audit Application.)

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.



Maximum Audit Entries

The value in this field specifies the maximum number of entries that can exist in any one log file. The minimum value for this field is 50. Any entry in excess of the value in this field will cause the current log file to be archived. For example, if the field is set to 1,000 entries, and the

login.log file contains 1,000 entries, when the next login entry is received the following will occur:

- The current login.log file will be archived with 1,000 entries.
- A new version of the login.log file will be created that contains the one (latest) entry.

Maximum Audit File Copies
The value in this field specifies the maximum number of audit files that can be created. When the audit file reaches the configured maximum number of audit entries, the file is saved and a new file is started.

Max .txt Log File Size (KB)
The value in this field specifies the maximum size, in KB, of the server.txt and traps.txt files. The minimum value for this field is 1. Any entry in the file that increases the file size beyond the value in this field will cause current server.txt and traps.txt files to be archived. For example, if the field is set to 5120 KB, and the server.txt file is at a file size of 5120 KB, when the next entry is received the following will occur:

- The current server.txt file will be archived with 5120 KB of information. The archive file will be located at *installation directory*/data/logs.
- A new version of the server.txt file will be created that contains the latest entry.

Debugging Preferences

The Debugging Preferences window is used to set and clear traces that are used for debugging purposes. The two main traces you may want to set are "SNMP" and "Polling".

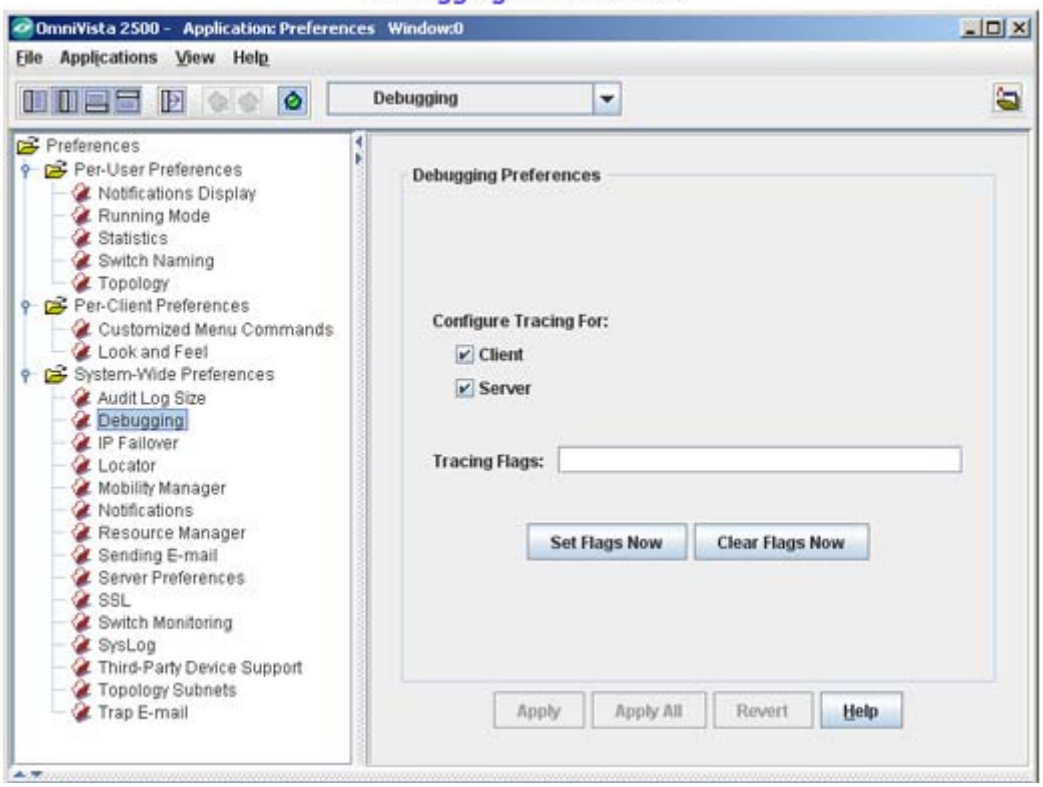
- **snmp.** When the SNMP trace is set, a debugging trace for all SNMP activity is recorded.
- **polling.** When the Polling trace is set, a debugging trace for all regular polling is recorded. The trace shows which OmniVista application is performing the polling (e.g., VLAN, Locator).

Note: The Debugging Preferences Window is functional only if you are logged in as user **admin** or **netadmin** (or as a user that has equivalent security permissions).

When tracing is configured for the client, the trace output is written to the client console. (In Windows, a client console is opened if you **CTRL**+double-click the application icon. In UNIX, applications are opened from a client console.) When tracing is configured for the server, the trace output is written to the server.txt file (which can be viewed from the Audit application).

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.

Debugging Preferences



Setting Traces

1. Click the **Client** checkbox, the **Server** checkbox, or both to specify the output location of the traces you want to set.

2. In the **Tracing Flags** field, type the name of one or more traces that you want to set. Enter a space between each flag. For example, to set the SNMP and Polling traces, type **snmp polling**). You can also type in **all** to set all possible traces.

Caution: Do not set **all** traces unless instructed by Alcatel Customer Service. Setting **all** traces will slow the server.

3. Click the **Set Flags Now** button.

> **Note:** It is important to note that when you set flags using the Preferences application, the flags set for a client will be in effect until that client is closed, and the flags set for the server will be in effect until the server is shutdown. You can permanently set the flags by configuring xydebug settings in the OVServer.lax file.

Clearing Traces

1. Click the **Client** checkbox, the **Server** checkbox, or both to specify the output location of the trace you want to clear.

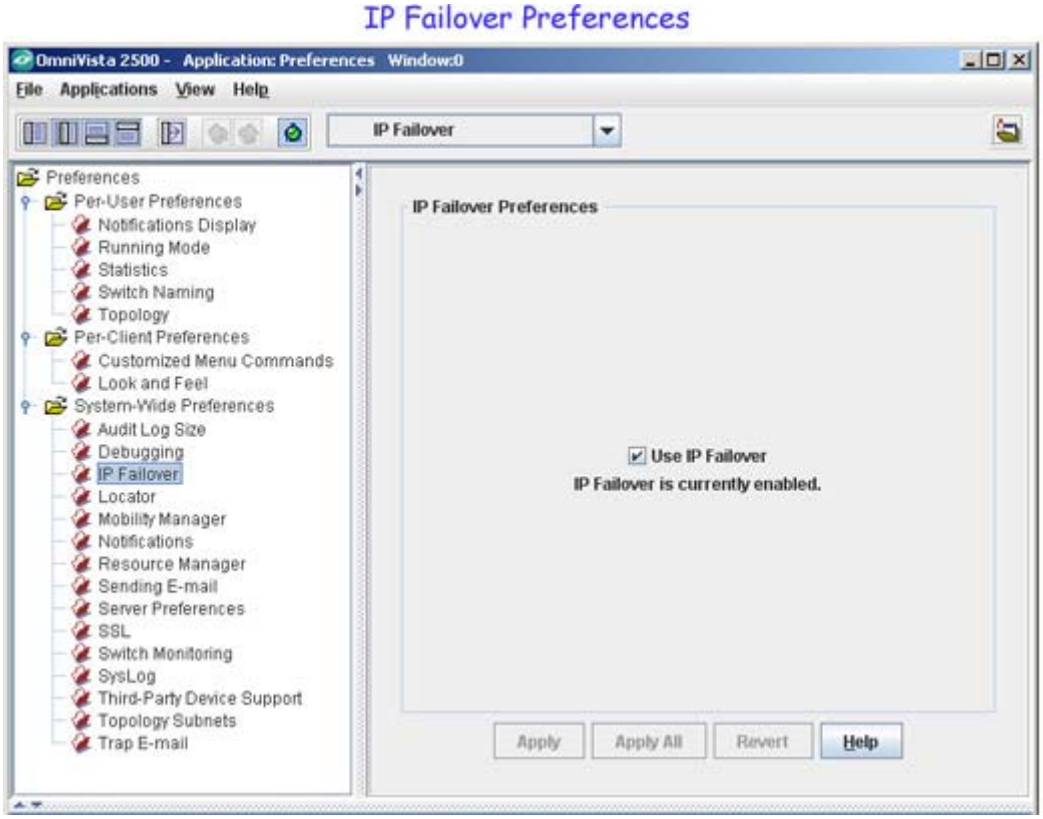
2. In the **Tracing Flags** field, type the name of a single flag that you want to clear. You can also type in **all** to clear all flags.

3. Click the **Clear Flags Now** button.

IP Failover Preferences

The IP Failover Preferences window is used to specify whether or not OmniVista will use a switch's alternate IP address for SNMP traffic, if the primary IP address fails. If the **Use IP Failover** checkbox is enabled and a switch fails to respond to SNMP requests, the OmniVista server tries to reach the switch using the alternate IP address. If the attempt is successful on the switch, then all the subsequent management traffic is diverted to this new address.

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.

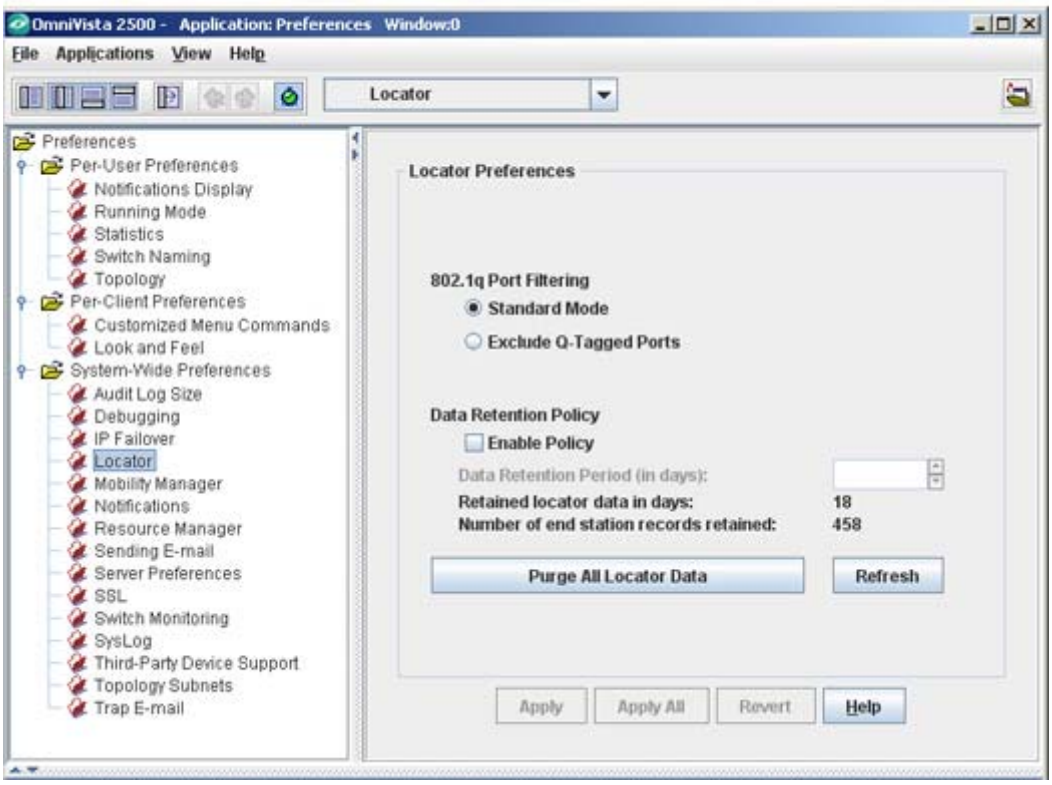


Note: In the IP Failover mode, the display still shows the original IP address of the switch. However, when you run the SNMP debug tracing, the alternate IP address of the switch used for the SNMP traffic is displayed.

Locator Preferences

The Locator Preferences window is used to Filter 802.1q Tagged Ports from polling results and live searches and Configure Locator Data Retention Policy. If you change a preference setting, click the **Apply** button at the bottom of the page to save the changes. To discard the new settings and return to the previous settings, click the **Revert** button.

Locator Preferences



802.1q Port Filtering

This feature allows you to exclude 802.1q tagged ports from polling results and live searches when AMAP / XMAP is not operating or a link is not present on the tagged port By default, it is disabled, which indicates 802.1q ports are included in polling and searches. Filtering modes are described below.

- **Standard Mode:** 802.1q Ports are included in polling and searches.
- **Exclude Q-Tagged Ports:** 802.1q Ports are excluded from polling and searches.

Data Retention Policy

If Data Retention Policy is disabled, Locator will not remove data during polling and will accumulate unbounded data. To enable the Data Retention policy:

1. Select the **Enable Policy** checkbox.

2. In the **Data Retention Period** field, specify the number of days that Locator data will be retained (Default = 30).

When Data Retention is enabled, information that is older than the number of days specified in the **Data Retention Period** field is automatically deleted from the database. In addition, the number of days the data has been retained as well as the number of end station records being retained is listed. To refresh this information, click the **Refresh** button. To purge all Locator data, click the **Purge All Locator Data** button, then click **Yes** at the confirmation prompt.

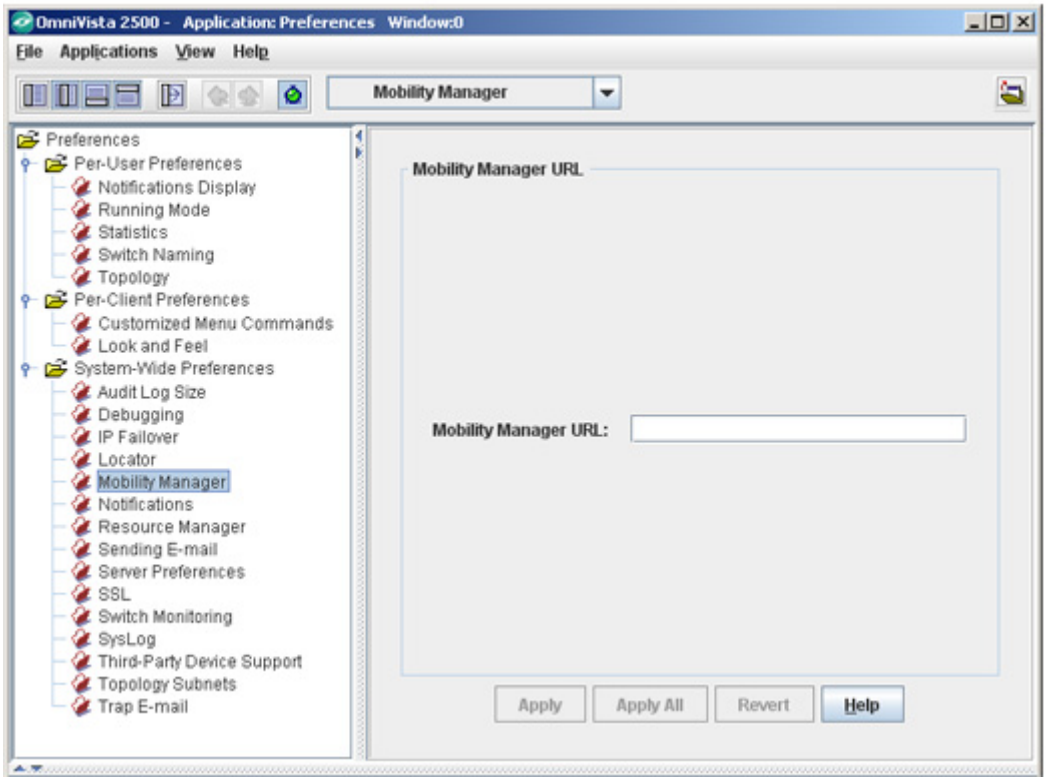
Mobility Manager Preferences

The Mobility Manager Preferences window is used to specify the URL where the Mobility Manager is located. Mobility Manager manages all the wireless devices in the network and can be accessed from a Web browser, which uses the Java Web Start capability to launch the application on a remote client.

If the Mobility Manager URL is not defined in Preferences, then when a wireless switch is launched from the Topology application for the first time, you will be prompted to define the Mobility Manager URL. Refer to the Topology application for further information on setting the Mobility Manager URL.

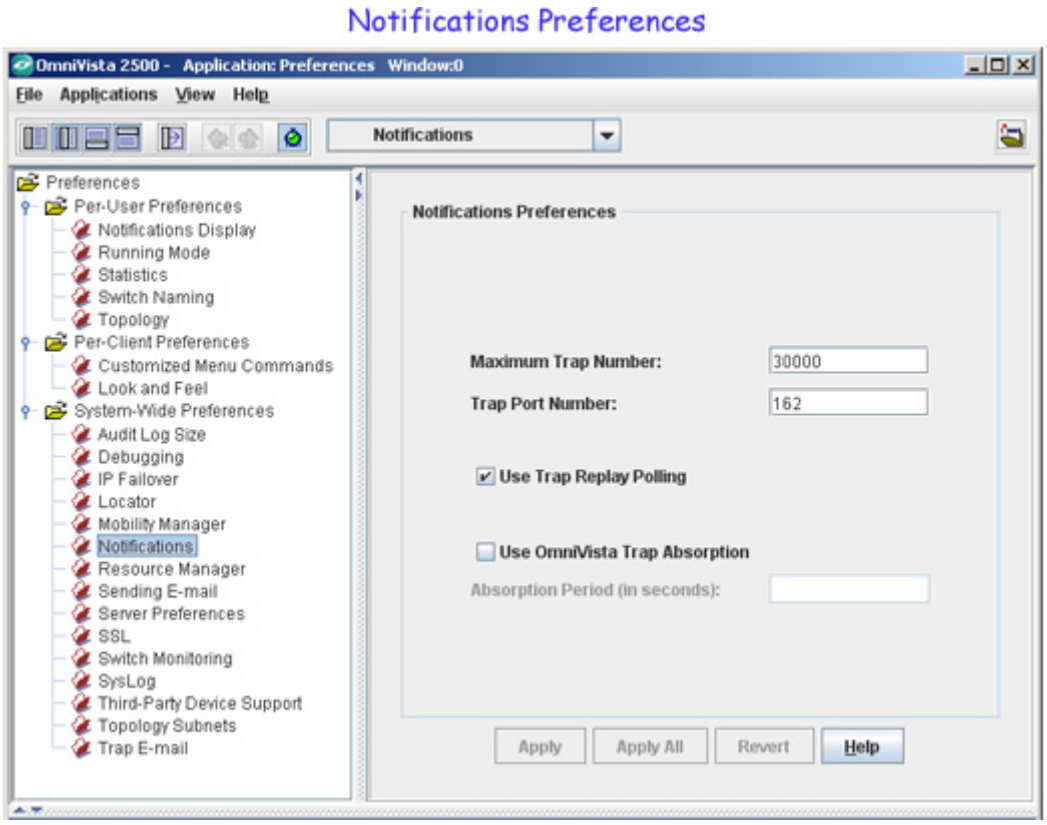
If you change the preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.

Mobility Manager Preferences



Notifications Preferences

The Notifications Preferences window is used to configure trap notifications parameters. This includes a new Trap Absorption feature for non-AOS devices. If you change the preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.



The **Maximum Trap Number** field enables you to specify the total number of received traps that can be stored on the OmniVista server. When a trap is received that exceeds the value in this field, the newly-received trap overwrites the oldest trap stored on the server. The minimum value for the **Maximum Trap Number** field is 1000 traps.

The **Trap Port Number** field enables you to specify the destination trap port number on the OmniVista server that receives alarms and traps. The number entered in the Trap Port Number field must match the port number that the switch is configured to send traps to.

If the **Use Trap Replay Polling** checkbox is enabled, OmniVista will poll all discovered AOS switches for missing traps at startup, and will continue to periodically poll the switches for missing traps.

If you change the preference setting, the buttons at the bottom of the screen will be activated. Click the **Apply** button to apply the change.

Trap Absorption

The Trap Absorption feature extends trap absorption to non-AOS devices. When this feature is enabled, similar traps received from non-AOS devices during the trap absorption period are 'absorbed,' and a 'trapAbsorbtionTrap' trap is generated similar to existing AOS traps. This trap contains details, such as the total number of 'sufficiently-similar' traps received since the original trap.

For example, if OmniVista receives a 'ChassisTrapsAlert' trap from a switch, OmniVista will 'absorb' all of the traps it receives from the same switch that are 'sufficiently similar' to 'ChassisTrapsAlert', until the trap absorption period expires.

> **Note:** Two traps are considered to be 'sufficiently similar' when their names, agent IP address, trap OID, severity, and enterprise OID (if defined) are same, and all their trap variables (if any) are also same.

OmniVista extends the trap absorption period when a 'trapAbsorbtionTrap' trap is generated. For example, if a trap absorption period is set to 15 seconds and a 'sufficiently-similar' trap is received on the 8th second, the period for that trap is extended for another 15 seconds. If no 'sufficiently-similar' traps for a trap is received during an entire trap absorption period, the trap absorption period expires for that trap.

> **Note:** If trap absorption is enabled for non-AOS devices, the "Forward Trap" responder configured in the Notifications application will not forward absorbed traps. It sees only the original unmodified trap stream, and forwards it to the forward destination.

Use OmniVista Trap Absorption - This check box allows you to enable or disable the trap absorption feature. By default, this checkbox is disabled. If you select this checkbox, the Absorption Period (in seconds) text box is set to 15 seconds automatically.

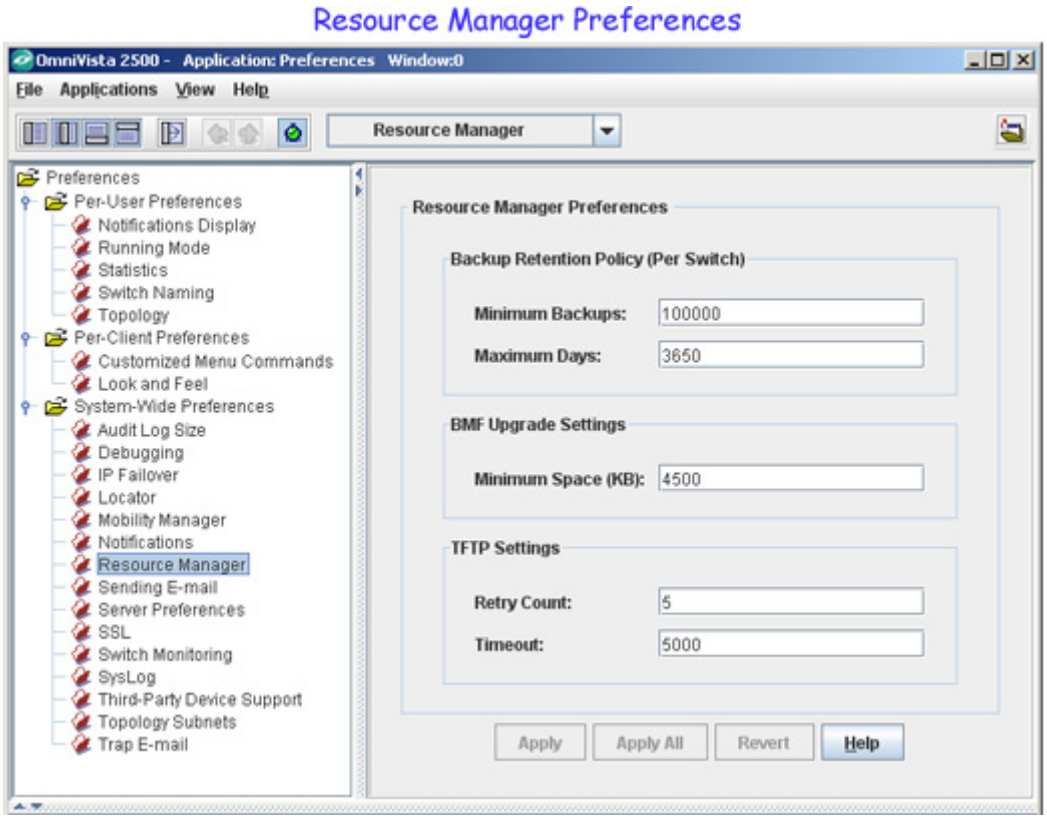
Absorption Period (in seconds) - This text box enables you to set a trap absorption period in seconds. By default, the trap absorption period is set to 15 seconds. You can change this value based on your requirements.

If you change a preference setting, the buttons at the bottom of the screen will be activated. Click the **Apply** button to apply the change.

Resource Manager Preferences

The Resource Manager Preferences window is used to set the amount of space that must be available on the CMM before an upgrade is allowed, and specify Trivial File Transport Protocol (TFTP) parameters that apply to all TFTP file transfers performed from OmniVista.

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.



Backup Retention Policy
These settings are used to specification of a maximum number of days and a minimum number of backups to keep per switch.

- **Minimum Backups -** The minimum number of backups you want to retain per switch. (Range = 1 - 100,000)
- **Backup Retention Period -** The maximum number of days that you want to retain those backups. (Range = 1 - 3,650)

If a backup for a switch is older than the maximum number of days, and the total number of backups is at least the minimum number specified, older backups will be deleted in accordance with the retention policy. The backup retention policy is applied when a new backup is successfully created.

For example, Let ‘b’ denotes the minimum number of backups to retain, ‘d’ the retention period in days, and ‘n’ the number of backups that are less than ‘d’ days old. For each device, the larger of the two numbers, ‘b’ and ‘n’, shall be retained. If 'b' = 3 and 'd' = 60 days:

- Switch 1: there are 6 backups, 4 of them are more than 60 days old, the 2 other ones are less than 60 days old: => 3 backups will be retained.
- Switch 2: there are 6 backups, 1 of them is more than 60 days old, the 5 other ones are less than 60 days old: => 5 backups will be retained.

BMF Upgrade Settings

- **Minimum Space -** The amount of space that must be available on the CMM before an upgrade is allowed. (Default = 4.5 MB)

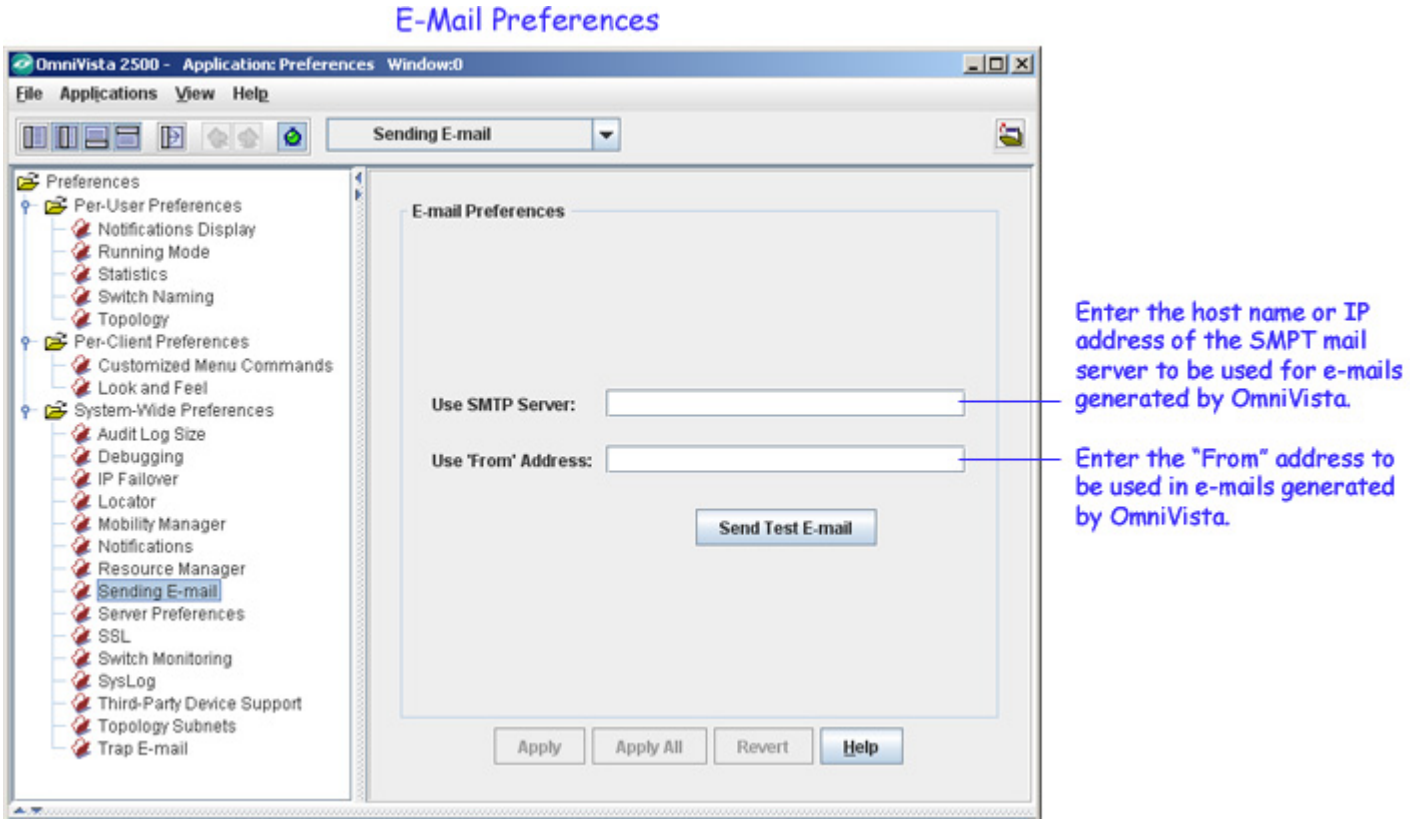
TFTP Settings

- **Retry Count -** The number of times OmniVista is allowed to retry packet transmission.
- **Timeout -** The time period, in milliseconds, that OmniVista will wait for a switch to respond with a data packet before assuming the request has timed out.

E-Mail Preferences

The E-Mail Preferences window is used to specify the Simple Mail Transfer Protocol (SMTP) mail server that you want to use to send e-mails generated by OmniVista. You can also specify the "From" address that will be used for these e-mails.

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.



OmniVista can be configured to generate and send an e-mail upon receipt of user-specified traps. This can be configured from the Automatic Trap Responders window in the Notifications application. The "To" address for Trap Responder e-mails is specified in the Automatic Trap

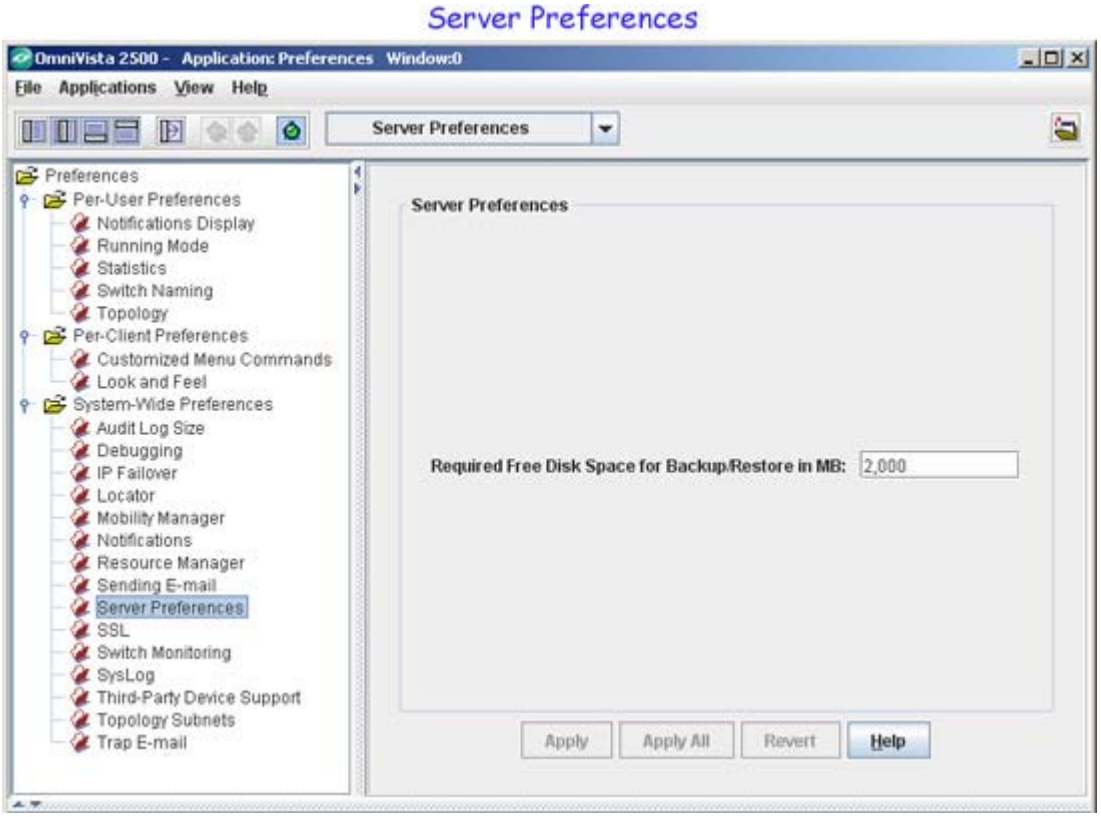
Responders window. The "From" address and the mail server to be used are specified in the **E-Mail Preferences** panel, as shown above.

You can click the **Send Test E-mail** button to send a test e-mail.

> **Note:** ALL the fields in the **E-Mail Preferences** panel must be filled or the e-mails you define will not be sent. Mail servers usually require the "From" address to be a valid e-mail address. If it is not, the mail server is likely to discard the request.

Server Preferences

The Server Preferences window is used to set the maximum amount of disk space, in MB, available on the CMM for Backup/Restore operations. If you change the setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.



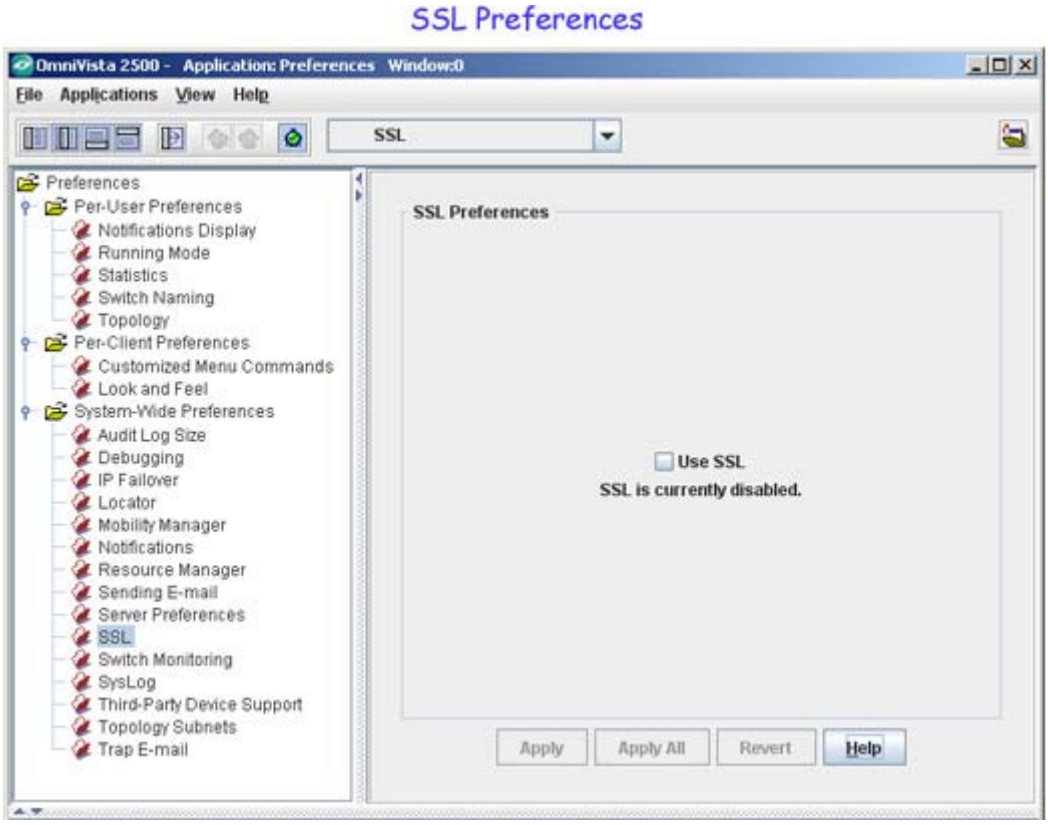
SSL Preferences

The SSL Preferences window is used to specify whether or not communication between the OmniVista server and OmniVista clients is encrypted for greater security. When the **Use SSL** checkbox is enabled, communications between the OmniVista server and all OmniVista clients will be encrypted using the Secure Socket Layer (SSL) protocol; and all clients that log into the server will be forced to use SSL, beginning with the client login process.

When SSL is not enabled, communications between the OmniVista server and OmniVista clients are not encrypted. However, even when SSL is not enabled, the login exchange will be encrypted to provide password security. Encrypting the login exchange makes it much more difficult to discover passwords by monitoring network traffic.

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.

> **Note:** Note that if you change the SSL setting, you will be prompted to reboot the server to make the change effective. The OmniVista implementation of SSL uses the Java Secure Socket Extension (JSSE) package that is now a part of JDK1.4. This package uses 128-bit RC4 encryption.

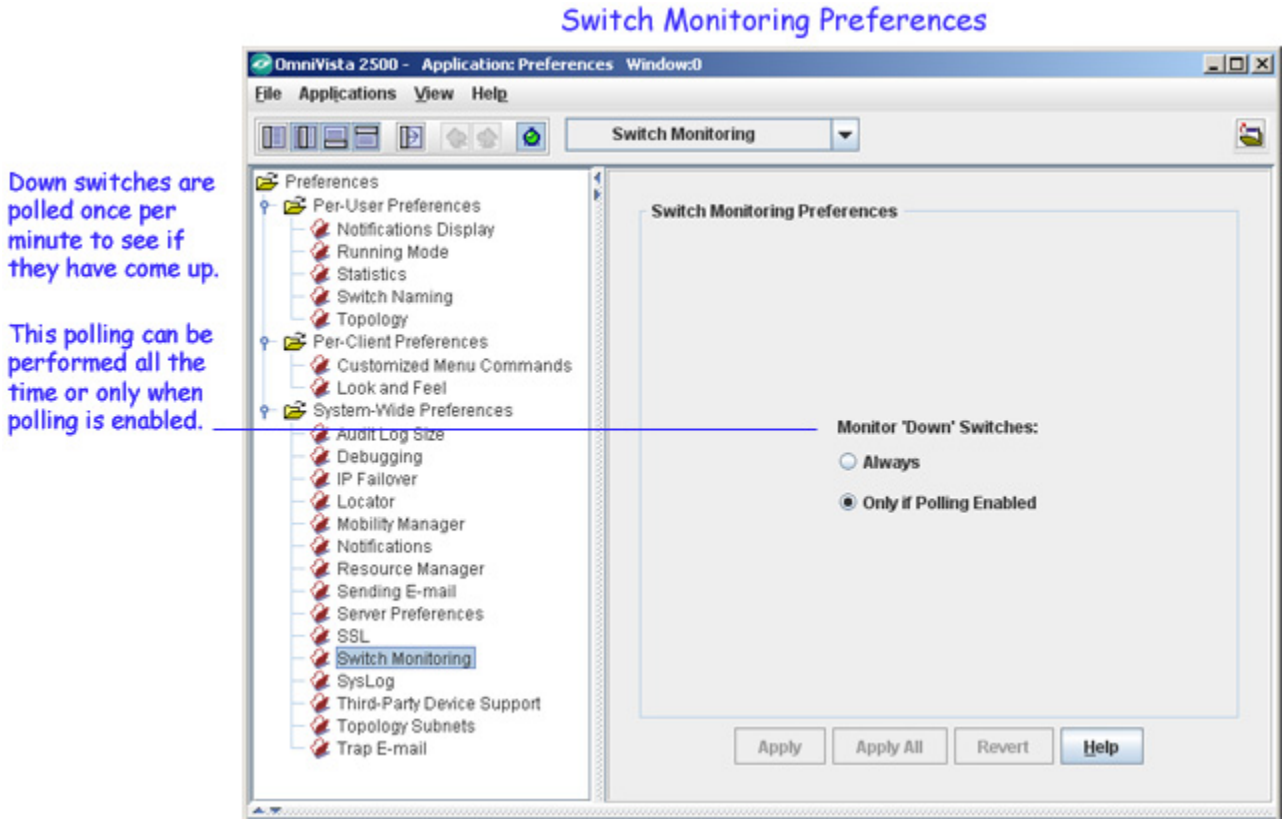


The SSL Status Indicator

If SSL is enabled, a padlock icon will display in the Status Bar in the lower right corner of the OmniVista Window. If a client is not logged into a server, or is logged into a server not using SSL, the padlock icon will not display.

Switch Monitoring Preferences

The Switch Monitoring Preferences window is used to configure the switch monitoring options described below. If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.



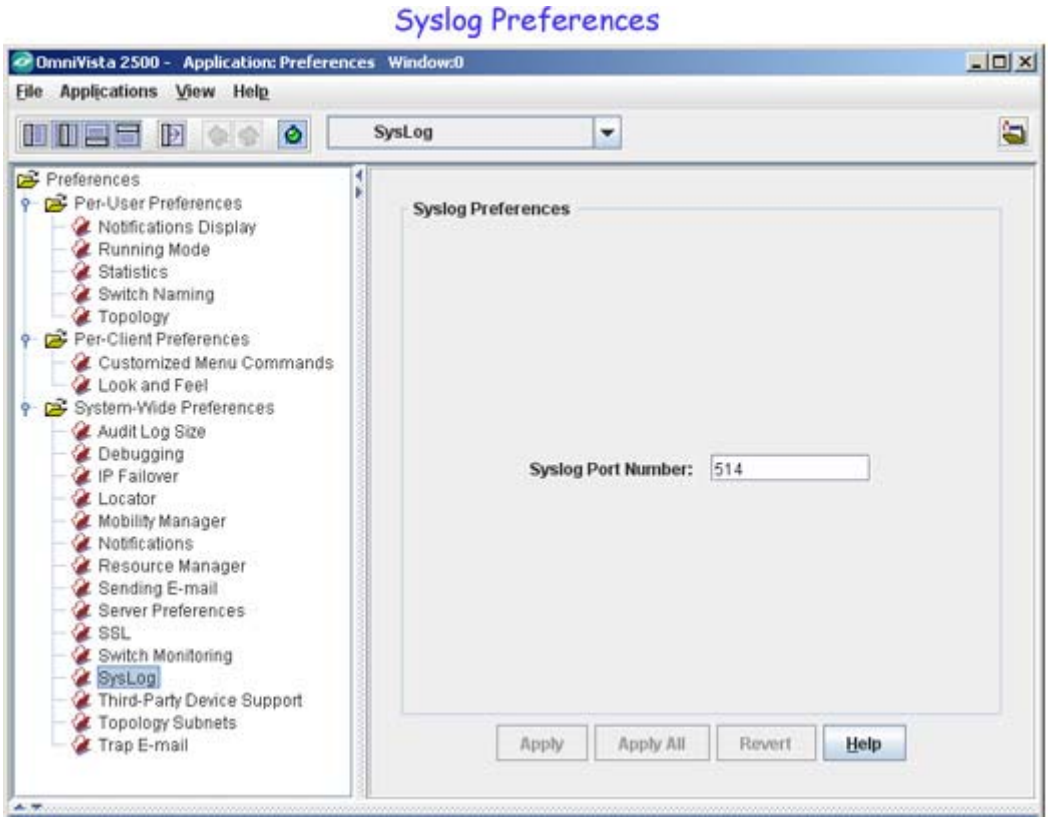
Monitor Down Switches Options

OmniVista polls down switches once per minute to check if the switches have come back up. Enable the **Always** button if you want such monitoring to occur all the time. Enable the **Only if Polling Enabled** button if you want such monitoring to occur only when normal OmniVista polling is enabled.

SysLog Preferences

The SysLog Preferences window is used to specify the port number used for SysLog messages. SysLog messages are used by the Quarantine Manager application to trigger rules that quarantine the devices that threaten the network. The default port is 514.

If you change the preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.

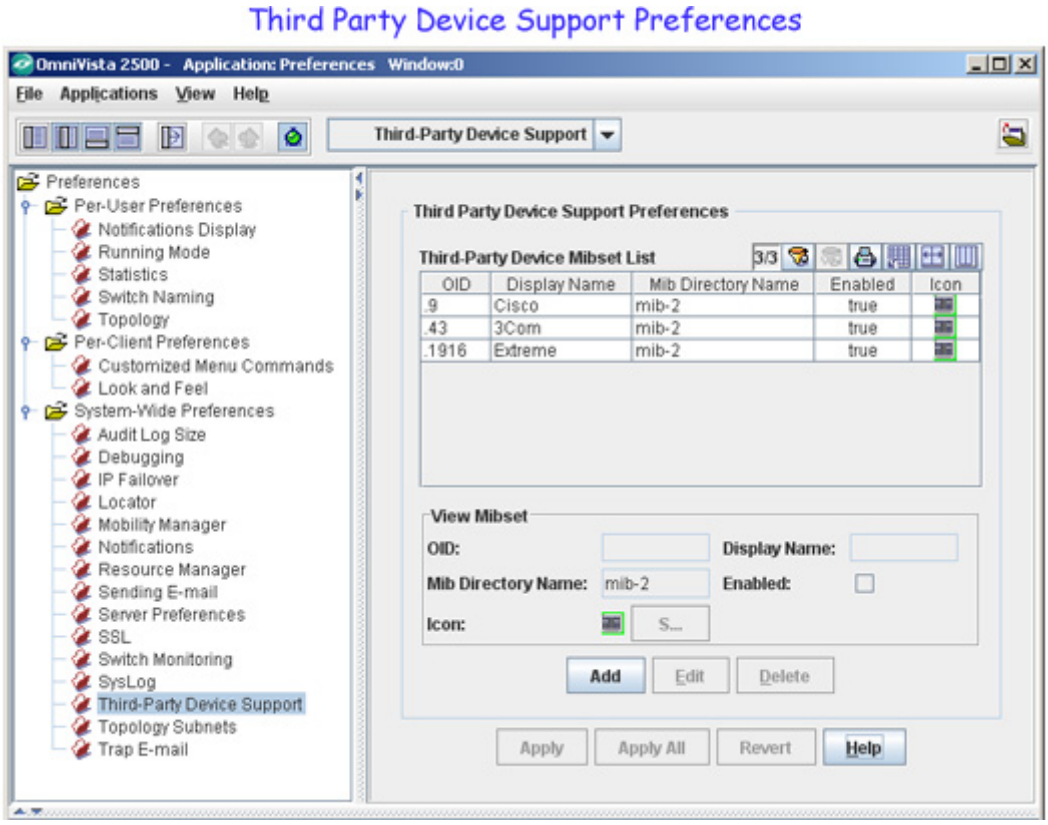


Third-Party Device Support Preferences

The Third-Party Device Support Preferences window is used to manage support for third-party devices. OmniVista ships with generic MIB-II support for Cisco, Extreme, 3Com, and Netscreen devices. Third-Party Device Support Preferences enable you to manage this default third-party device support, add support for additional third-party devices, edit third-party device support, delete support for unwanted third-party devices, and alter the generic default support for Cisco, Extreme, 3Com, or Netscreen devices to make that support more device-specific.

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.

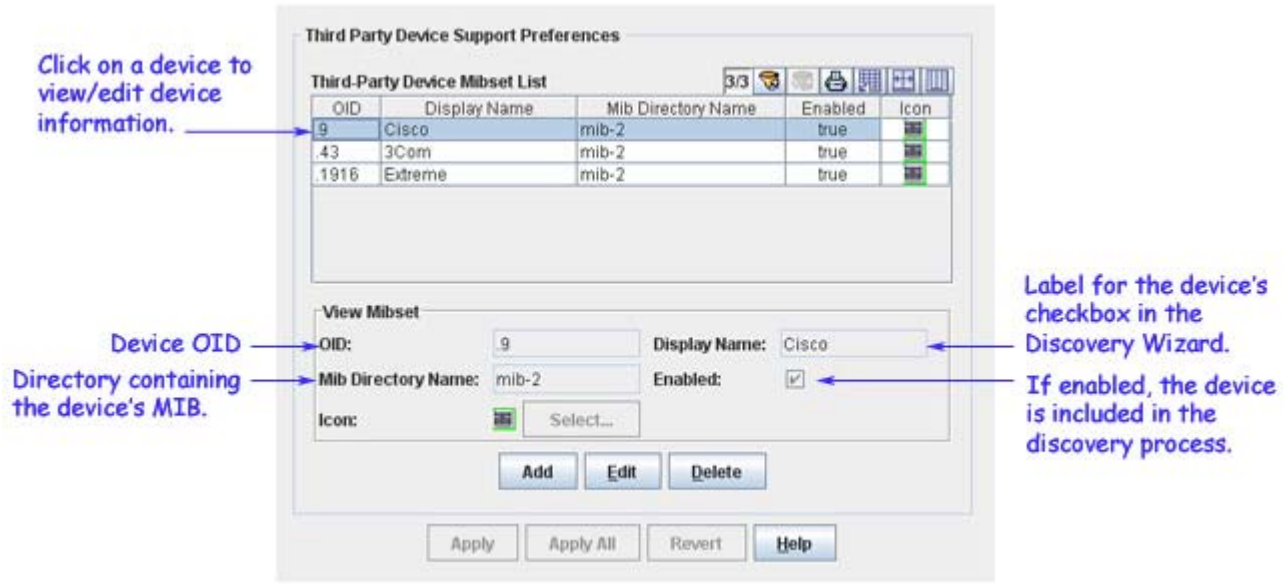
> **Note:** Altering third-party generic default support will require importation of the appropriate MIBs. All third-party devices must use MIB-II.



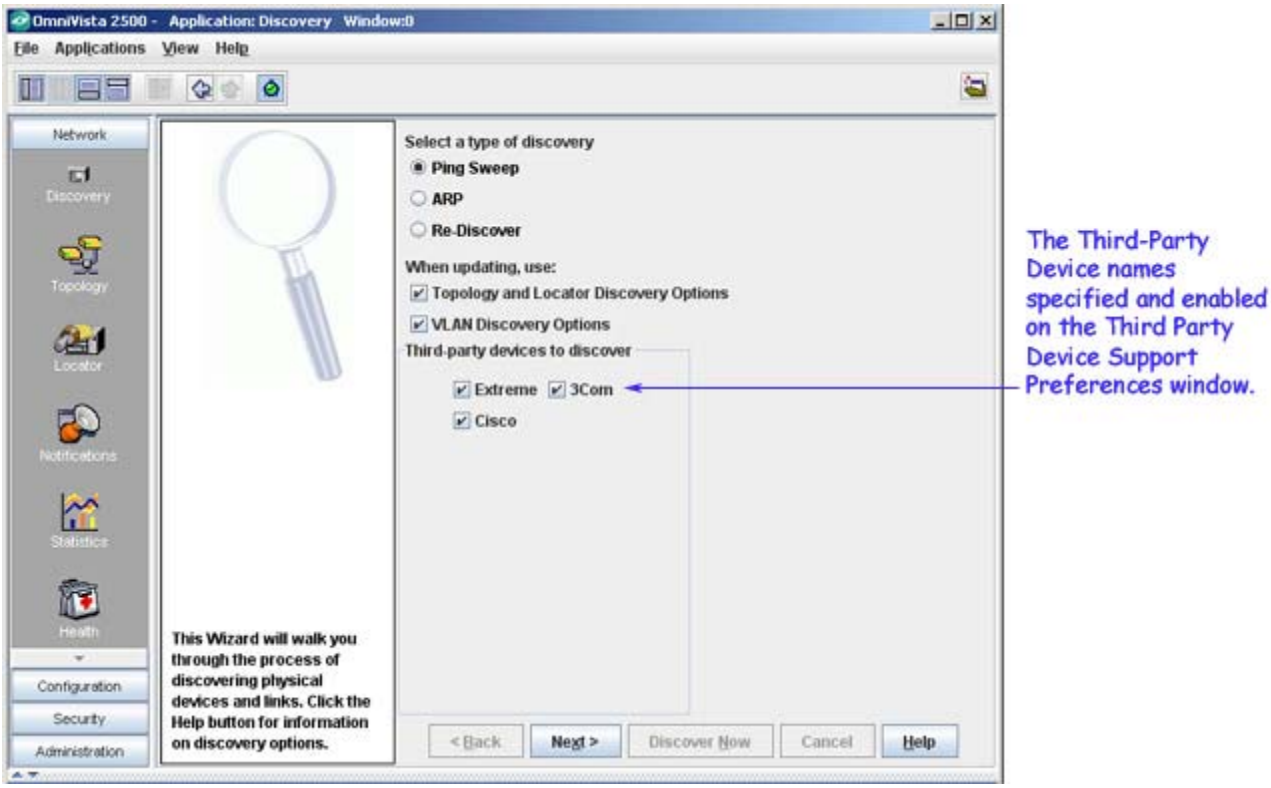
Understanding Third-Party Device Support

Click on any third-party device listed in the Third-Party Device Support Preferences window to view support information for the device. The fields are displayed below.

- **OID.** Device's Object ID.
- **Display Name.** Label that is used for the device's checkbox in the Discovery Wizard window.
- **MIB Directory Name.** Directory that contains the device's MIB.
- **Enabled.** Default state of the device's checkbox in the Discovery Wizard Window. When this field is enabled (indicated by a checkmark), the device is included in the discovery process. When this field is not enabled, the device is not included in the discovery process.



The first page of the Discovery Wizard displays a checkbox for each supported third-party device. As stated, the label for each checkbox is specified by the **Display Name** field on the Third-Party Device Support Preferences Window and the default state of the checkbox (enabled or disabled) is determined by the **Enabled** field.



Note that if the device checkbox is disabled by default, you can still check the box manually to enable it before performing a discovery. If the checkbox is manually enabled in this fashion, and if the discovery process is completed, OmniVista will set the **Enable** field on the Third-Party Device Support Window to **true**.

Adding Support for a Third Party Device

Adding support for a new third party device consists of two tasks, which should be performed in the following sequence:

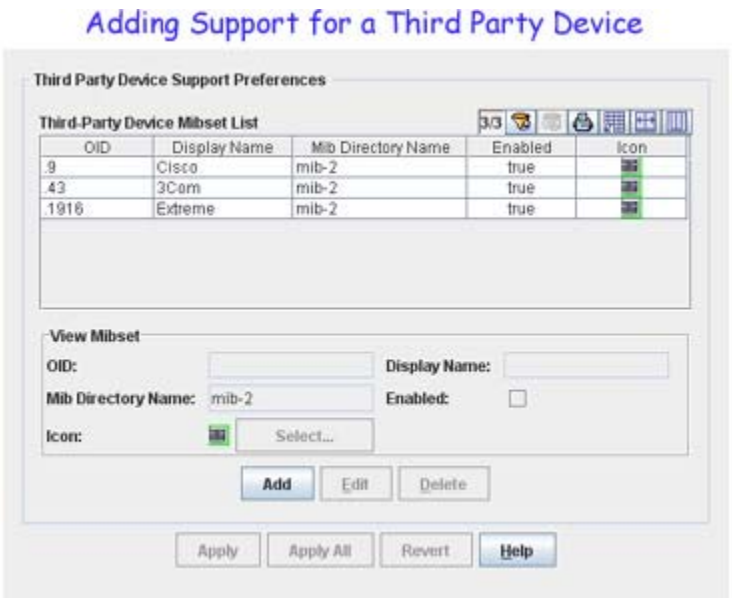
Task 1. Add support for the new device using the Third-Party Device Support Preferences Window.

Task 2 (Optional). Import device-specific MIBs for the new device using the Import MIBs Window in the Topology Application. All third-party devices must use MIB-II. If generic MIB-II support for the device is sufficient, this step can be omitted.

Note: It is no longer necessary to distribute imported MIBs to OmniVista clients. The OmniVista MIB Browser now resides on the server, and, when a client makes a request to use the MIB Browser, the necessary components (including imported MIBs) are transferred to the client and cached there for subsequent use.

Add Support for the New Device

1. From the Third-Party Device Support Preferences Window, click the **Add** button. The Third-Party Device Support Preferences Window goes into add mode, as shown below.



2. Enter the device's Object ID in the **OID** field. Enter only the portion of the OID relative to the ".1.3.6.1.4.1." (".iso.org.dod.internet.private.enterprises") branch. For example, enter only '9' for Cisco devices rather than '.1.3.6.1.4.1.9', or '1916' for Extreme devices, rather than '.1.3.6.1.4.1.1916". Using this vendor value (e.g., 9, 1916) will enable OmniVista to recognize all devices from the vendor.

> **Note:** You can also enter specific vendor device values (e.g., '1916.800.1.1.2.1.5.1') for each vendor device if you want each device to have a different name while using the same mibset.

3. Enter the directory name of the device's MIB in the **MIB Directory Name** field. If you are not using standard MIB-II, you should enter a new directory name for the MIB. When you import the MIB for the device, the directory name that you enter here will display for your selection in

the Import MIB window. Note that the directory does not have to actually exist; it will be created automatically when you import the MIB.

4. If you have a unique **Icon** that you want to display for the device, click **Select** and browse to the icon file.

5. In the **Display Name** field, enter the label that will appear on the device's checkbox on the Discovery Wizard.

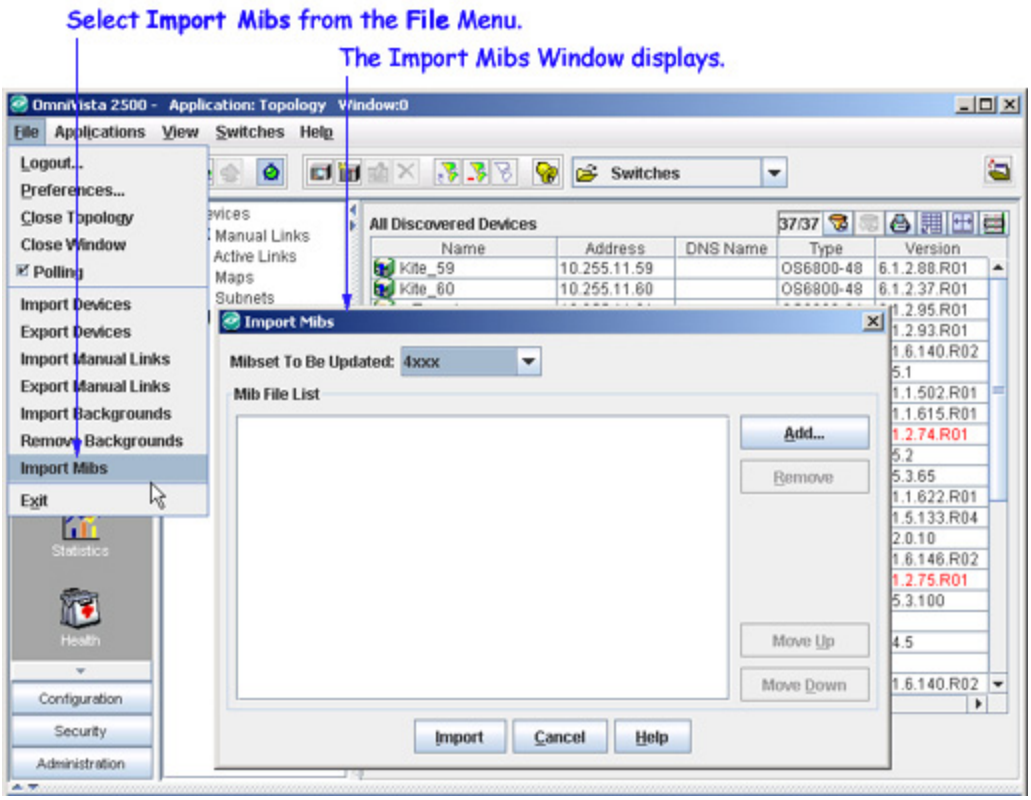
6. Set the **Enabled** field to **true** or **false**, as desired, to specify the default state of the device's checkbox on the Discovery Wizard. Setting the **Enabled** field to **true** will enable the checkbox by default, and the device will be included in the polling process.

7. Click the **OK** button below the Add panel.

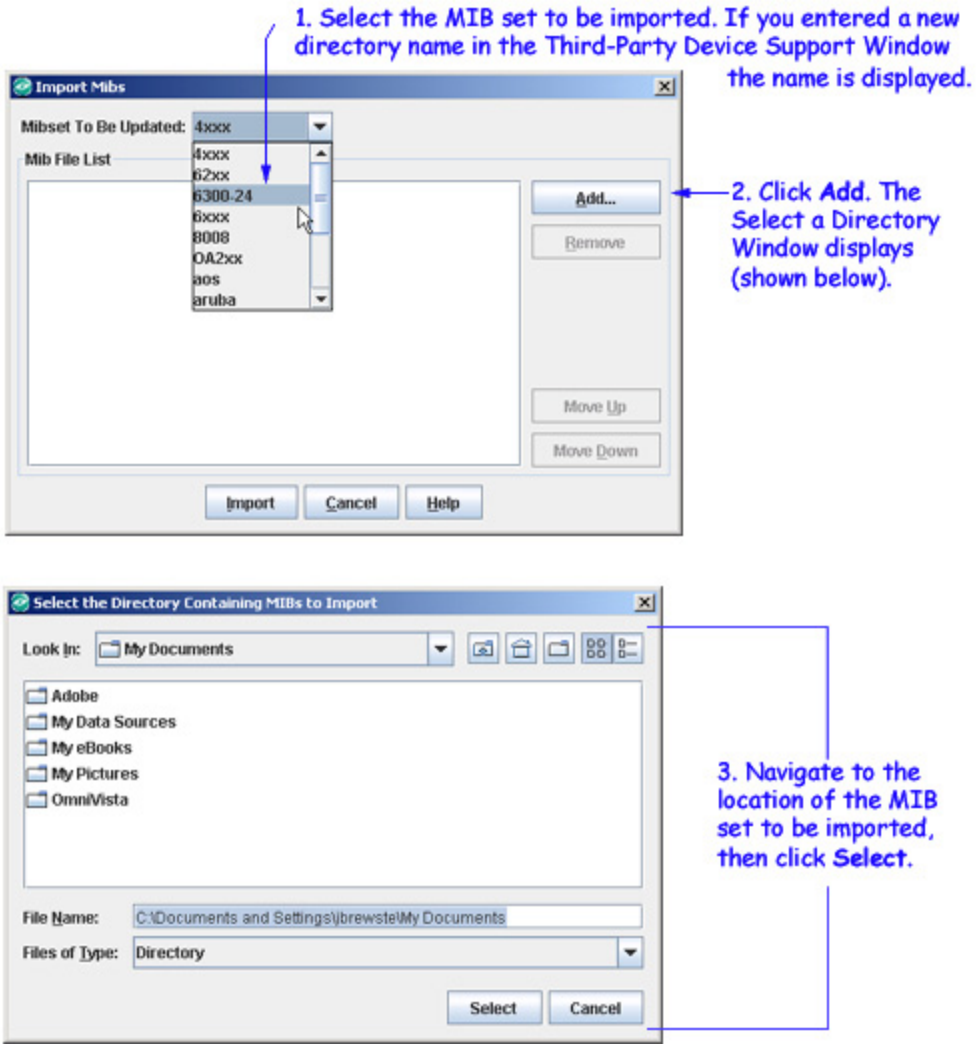
8. Click the **Apply** button at the bottom of the window to write the new device support to the server. The new device name will now display on the Discovery Wizard.

Import MIBs for the New Device Via the Import MIB Window

1. Open the Topology Application and select **Import MIBs** from the **File** menu. The Import MIBs window displays, shown below.



2. From the **Mibset To Be Updated** drop-down menu, select the MIB set to be imported. (If you entered a new directory name in the Third-Party Device Support Window, the name is displayed.). Then click the **Add** button. The Select a Directory Window displays.



3. Within the Select a Directory Window, navigate to the location where the MIB set resides. When the correct MIB directory is displayed in the window, click the **Select** button. The Select a Directory Window closes and the MIB files are listed in the Import MIBs Window.

4. If any files listed in the Import Mibs Window are unnecessary, select them and click the **Remove** button. Files that you remove will not be imported.

5. The MIB files will be loaded into OmniVista in the order the files are listed in the the Import MIBs Window. You can adjust this order by selecting individual files and clicking the **Move Up** and **Move Down** buttons until files are listed in the correct order.

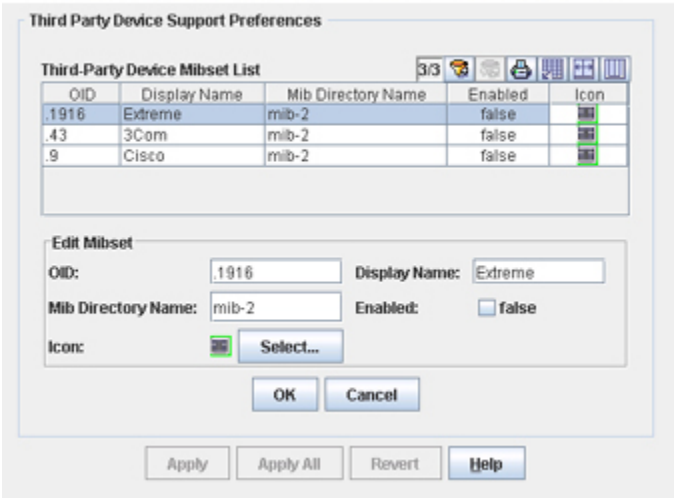
6. Click the **Import** button. The MIB files are imported. A message displays in the Status Panel when the import operation is complete.

Editing Support for a Third-Party Device

1. From the Third-Party Device Support Preferences Window, select the device you want to edit, then click the **Edit** button. The Third-Party Device Support Preferences Window goes into edit mode, as shown below.

2. You can edit any field. When your changes are complete, click the **OK** button, then click the **Apply** button at the bottom of the Third-Party Device Support Preferences Window to write the change to the server.

Editing Support for a Third-Party Device



Deleting Support for a Third-Party Device

To delete support for an existing third-party device, select the device in the Third-Party Device Support Preferences window and click the **Delete** button. The device is deleted from the Third-Party Device Support Preferences window. Click the **Apply** button to write the change to the server.

Making Support More Device-Specific

OmniVista ships with generic MIB-II support for third-party devices. It is possible to make this generic support more device-specific. (However, note that doing so requires importation of the appropriate MIBs.) Follow the steps below to make OmniVista's third-party device support more device-specific.

1. Use the Third-Party Device Support Preferences Window to add device-specific display names and appropriate MIB directory names. For example, you may wish to delete the **Cisco** display name and add display names for the **Cisco 6509** and the **Cisco 4006**. If you are not using standard MIB-II, you should enter new MIB directory names for the Cisco devices as appropriate.

2. Use the Import Mibs Window to import the appropriate device-specific MIBs. (To display the Import MIBs window, go to the Topology application and select **Import MIBs** on the **File** menu.) To continue the example above, you would import device-specific MIBs for the Cisco 6509 and the Cisco 4006.

Traps for Third-Party Devices

By default, OmniVista supports generic MIB II traps for third-party devices. If you import a new, custom MIB for a third-party device, OmniVista will automatically scan the MIB for new traps and integrate any traps it finds. It is no longer necessary to manually integrate traps for

third-party devices, as it was in previous releases of OmniVista. Note that MIBs do not include synopses for traps. OmniVista will create a synopsis "on the fly" for any new trap it integrates.

> **Note:** You can go to the Notifications Application and edit the synopses or severity levels that OmniVista assigns to new traps. To do this, select **Trap Definition** in the Notification Application's Tree.

Third-Party Device Support After Discovery

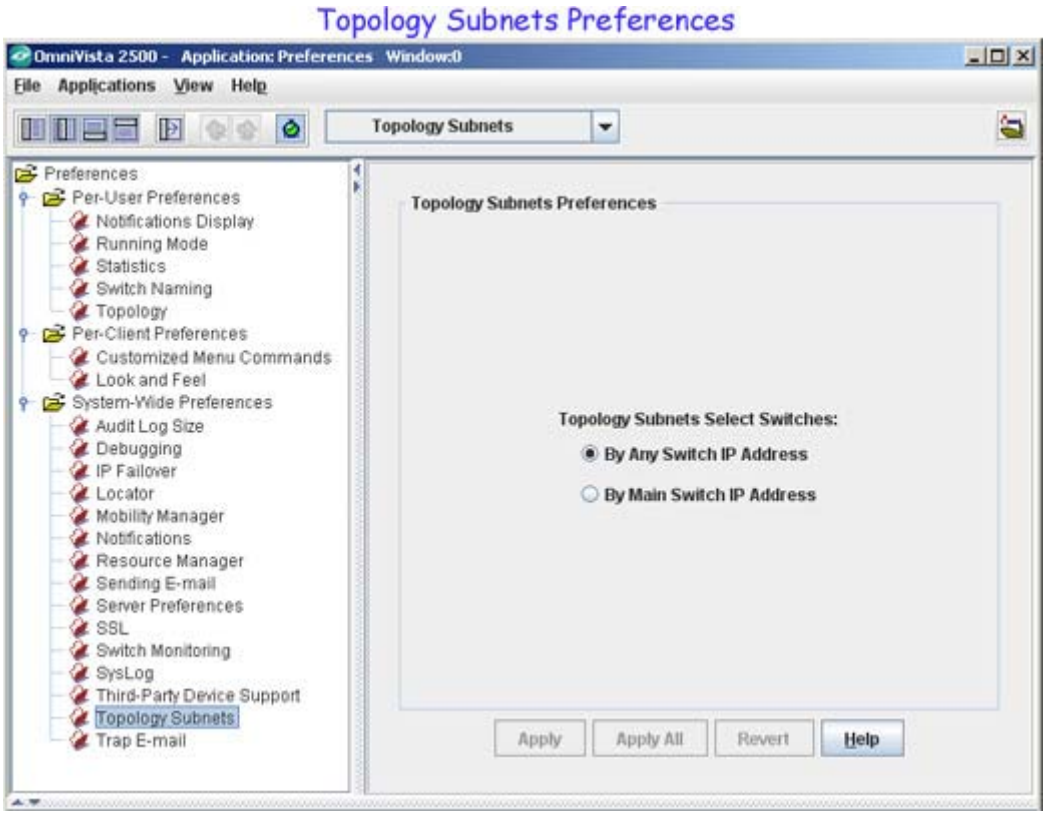
Once third-party devices have been discovered, OmniVista supports the following functionality for the devices:

- **Web Browser.** OmniVista enables you to launch web-based element managers for third-party devices from OmniVista pop-up menus.
- **Telnet or SSH (as applicable).** OmniVista enables you to initiate Telnet or SSH sessions to third-party devices from OmniVista pop-up menus.
- **Custom MIBs.** OmniVista allows you to import custom MIBs for third-party devices (as described above).
- **Custom Icons.** OmniVista enables you to import a custom icon that will be used to represent a specific third-party device.
- **Custom Menu Items.** OmniVista enables you to add custom menu items to OmniVista pop-up menus. You can add a custom menu item for any native command that already exists on the workstation. You can configure OmniVista to display the custom menu item when a specific third-party device is selected (but not when other devices are selected).
- **MIB Browser.** The OmniVista MIB Browser can be used with third-party devices. The OmniVista MIB Browser is available from OmniVista pop-up menus.
- **Traps.** By default, OmniVista supports generic MIB II traps for third-party devices. In addition, whenever you import a new, custom MIB for a third-party device, OmniVista will scan the MIB for new traps and automatically integrate any traps it finds.
- **Statistics.** OmniVista's Statistics Application supports third-party devices.
- **Locator.** OmniVista's Locator Application supports third-party devices.

Topology Subnet Preferences

The Topology Subnet Preferences window is used to set the preference of selecting a switch in a subnet by the main IP address or any IP address associated with the switch. To select switches by the main IP address of a switch, enable **By Main Switch IP Address**. To select switches by any IP address associated with a switch, enable **By Any Switch IP Address**.

If you change a preference setting, the buttons at the bottom of the screen will activate. Click the **Apply** button to apply the change. To discard the new settings and return to the previous settings, click the **Revert** button.



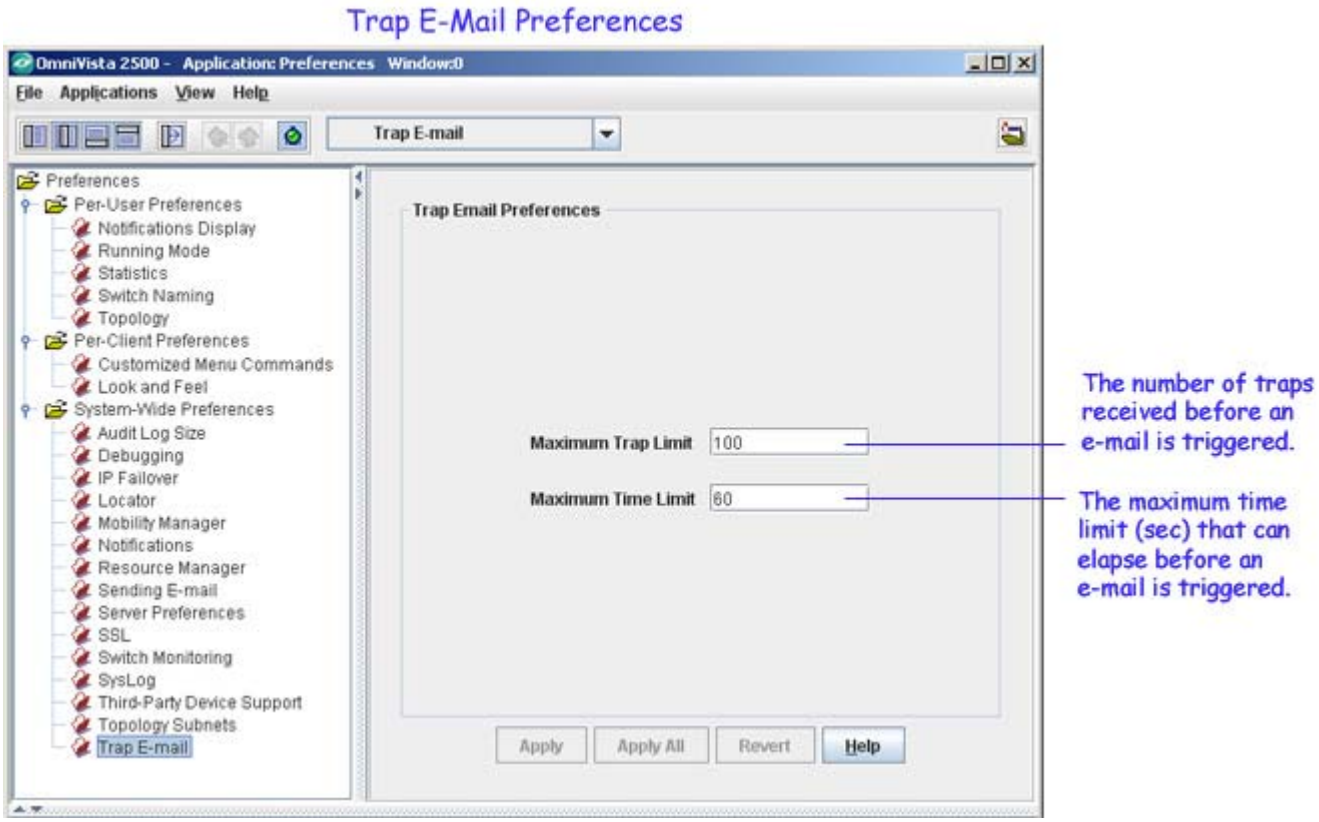
Trap E-Mail Preferences

The Trap E-Mail Preferences window is used to define the default values for OmniVista "trap responder" e-mails. Trap responder e-mails are e-mails that OmniVista generates automatically when specified traps are received from network devices.

The Automatic Trap Responders window in the Notifications application enables you to configure OmniVista to send an e-mail when a specified trap is received. (Traps can be specified by severity level, or by use of a filter.) However, to prevent e-mail storms that would result from receipt of multiple traps, OmniVista does NOT send one e-mail per trap received. Rather, OmniVista "combines" responder e-mails to prevent storms. By default, OmniVista will send a "combined" responder e-mail when:

- One minute has passed since the first trap was received for which an e-mail was not generated, OR
- 100 traps have been received.

If you change a preference setting, the buttons at the bottom of the screen will be activated. Click the **Apply** button to apply the change.



Maximum Trap Limit
This field enables you to redefine the number of received traps that will trigger a trap responder e-mail. Enter the number of received traps that will trigger a trap responder e-mail.

Maximum Time Limit
This field enables you to redefine the maximum time period, in seconds, that can elapse before a trap responder e-mail is triggered. The time period begins when a trap is received for which an e-mail was not generated.

Refer to the Notifications application Help for further information on trap responder e-mails.