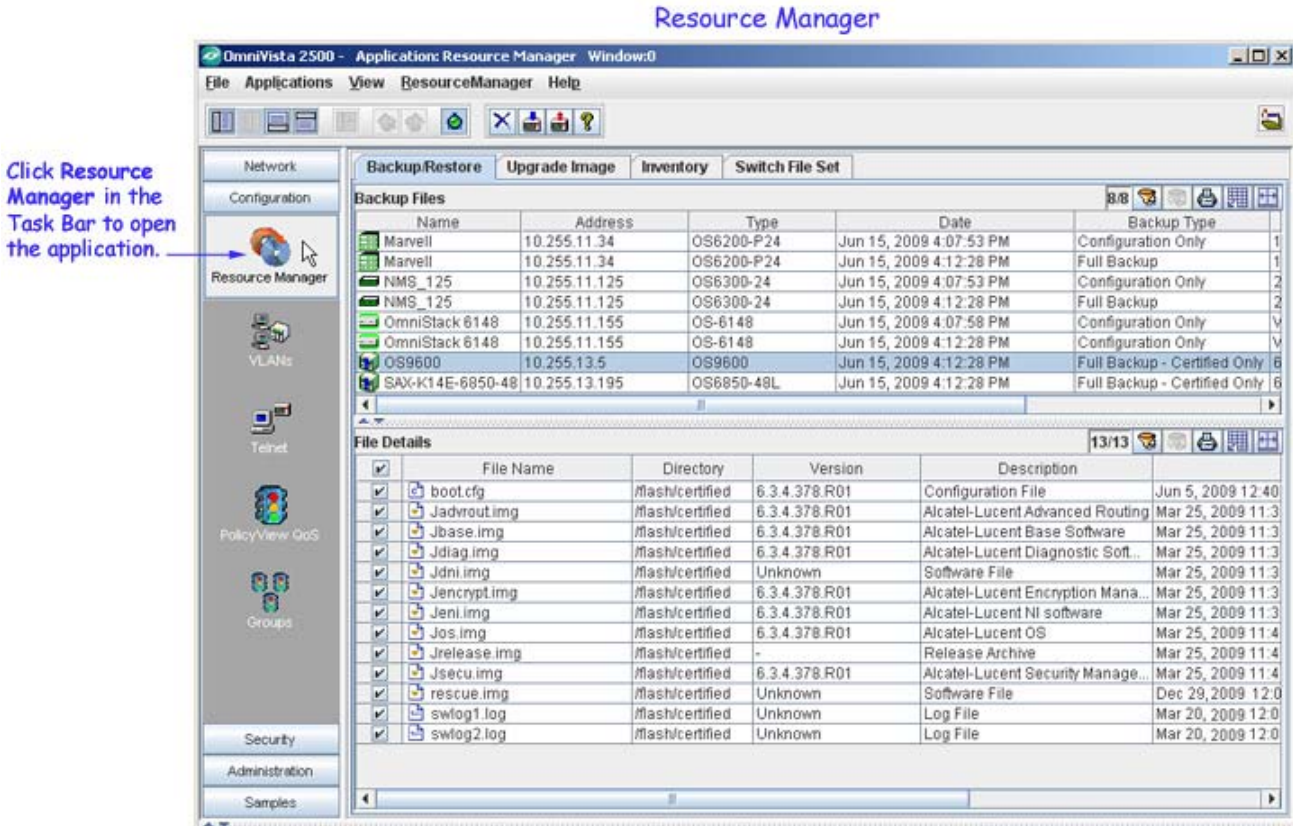


Getting Started with Resource Manager

The Resource Manager application, shown below, enables you to manage the firmware configuration files in network switches. The Resource Manager application makes it possible to:

- Backup the current firmware configuration files in network switches to the OmniVista server, and restore the configuration files to the switches when desired.
- Import new or upgraded image and firmware files into OmniVista, and install the new files in network switches when desired. (Note that all new image files must be provided by Alcatel-Lucent Customer Service.)
- Run Inventory Reports on network switches that enable you to examine a switch configuration before performing the functions described above.
- Assign customized Banner and Captive Portal Web Interface files to switches in the network.

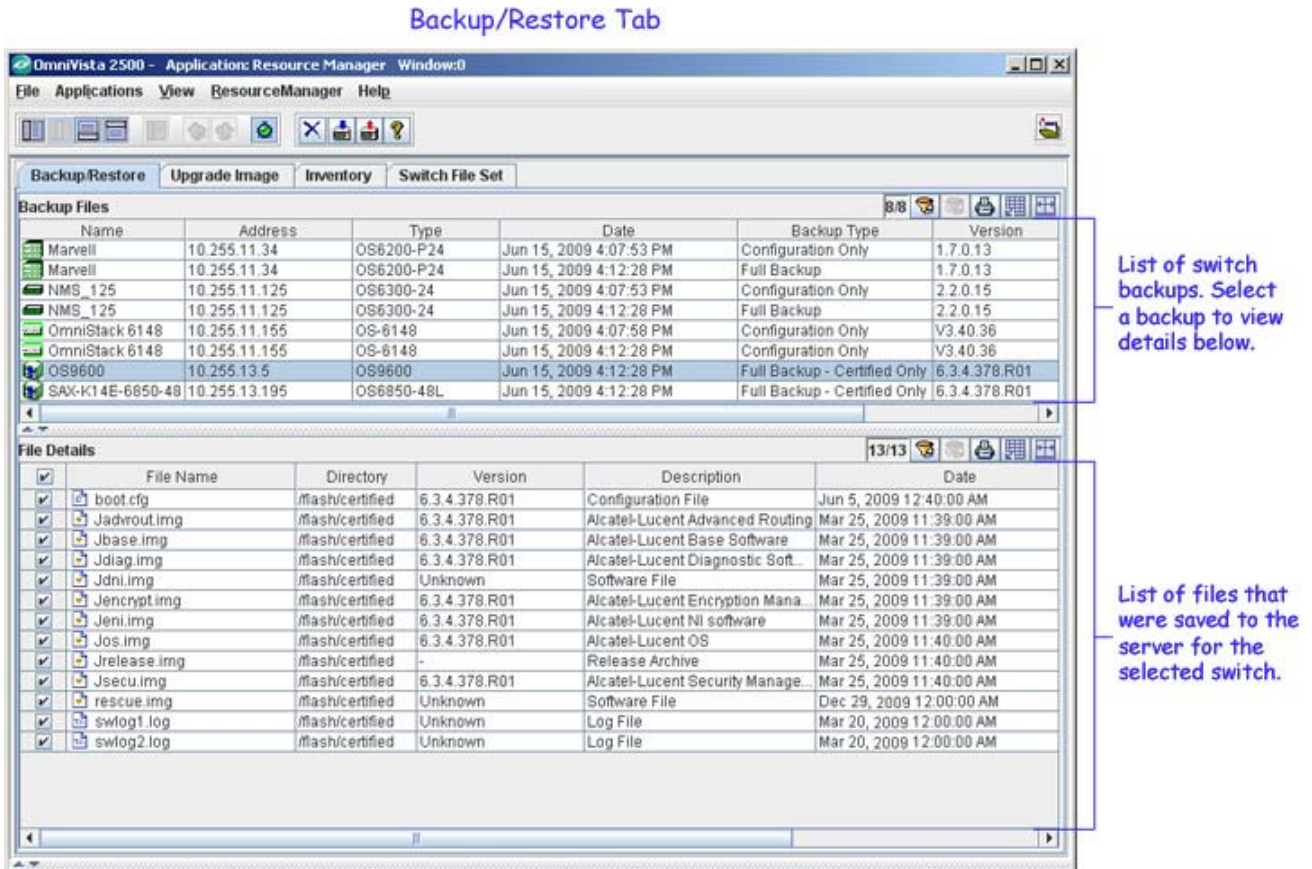
Resource Manager displays three tabs. The Backup/Restore tab enables you to manage the backing up and restoring of current firmware configurations. The Upgrade Image tab enables you to manage the importation and installation of new firmware files. The Inventory tab enables you to run switch Inventory Reports and, for convenience, also enables you to initiate switch backups.



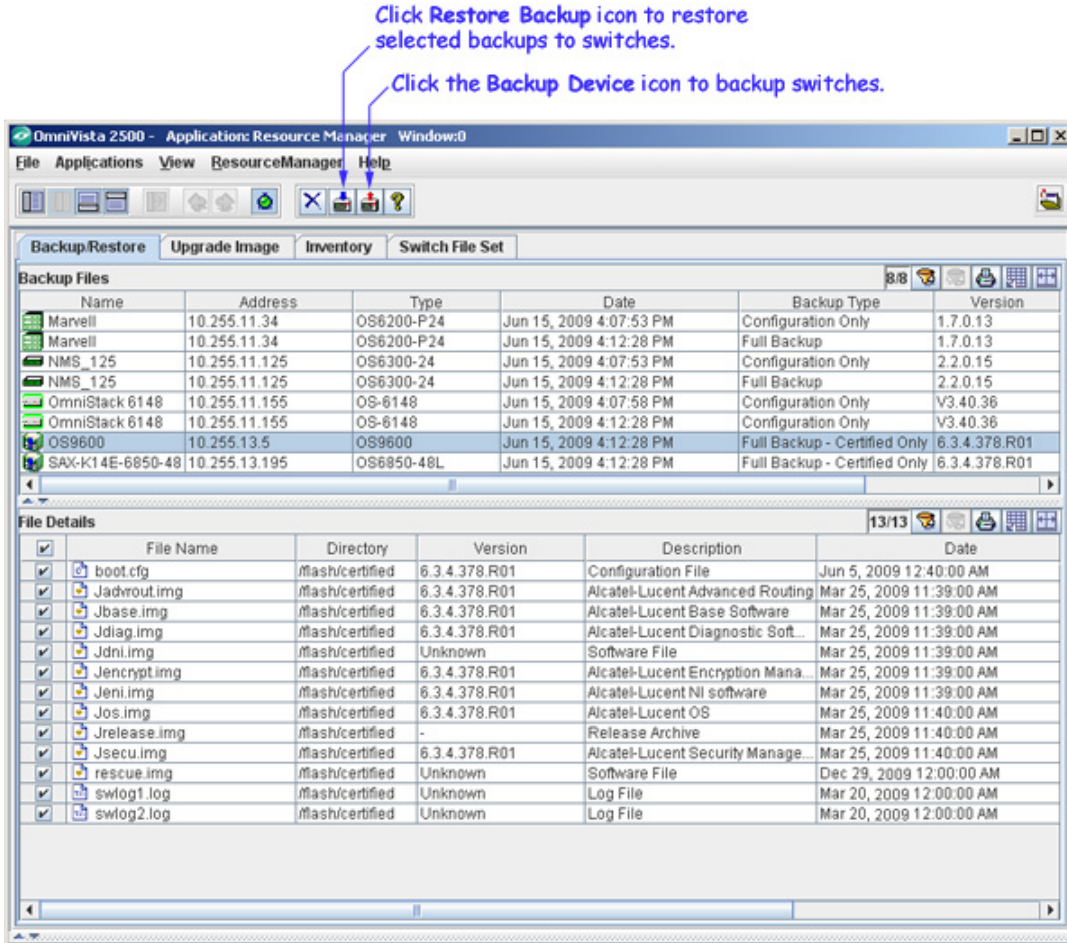
Backup/Restore Tab

The Backup/Restore tab enables you to backup configuration files to the OmniVista server, to view a detailed list of the files saved to the server during an individual backup, and to restore configuration files to the switches from which they were originally taken. As shown below, the top pane of the Backup/Restore tab, labeled "Backup Files," lists the switch backups that currently exist on the server. Select any backup listed and the bottom pane, labeled "File Details," lists the individual files that were saved to the server during the backup.

Note: Backup/Restore support using the Resource Manager application is currently available on OS6200 devices.



Icons in the Resource Manager Tool Bar, shown below, enable you to backup switches and restore the backups when desired. Backups are performed from the Backup Configuration Wizard, shown below, which opens when the Backup Device icon is clicked. See “Using the Backup/Restore Tab” on page 8 for more information on the functionality available from the Backup/Restore tab.

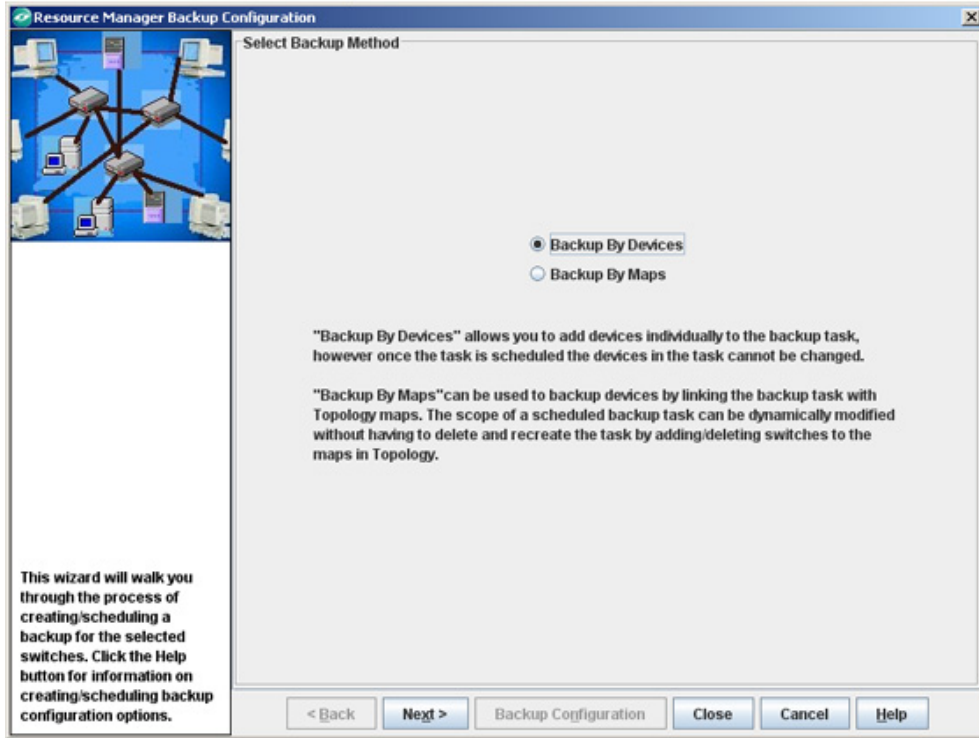


Backup Configuration Wizard

When you click the Backup Device icon to backup switches, Page One of the Backup Configuration wizard displays, as shown below. Page One of the wizard (shown below) displays two options, **Backup By Devices** and **Backup By Maps**. The **Backup By Devices** option lets you back up switches by devices and the **Backup By Maps** option lets you back up switches by regions. If you select the **Backup By Devices** option and click the **Next** button, Page Two of the wizard will display a list of all the devices known to OmniVista. However, if you select the **Backup By Maps** option and click the **Next** button, a list of all the regions defined in the Topology application will be displayed in Page Two.

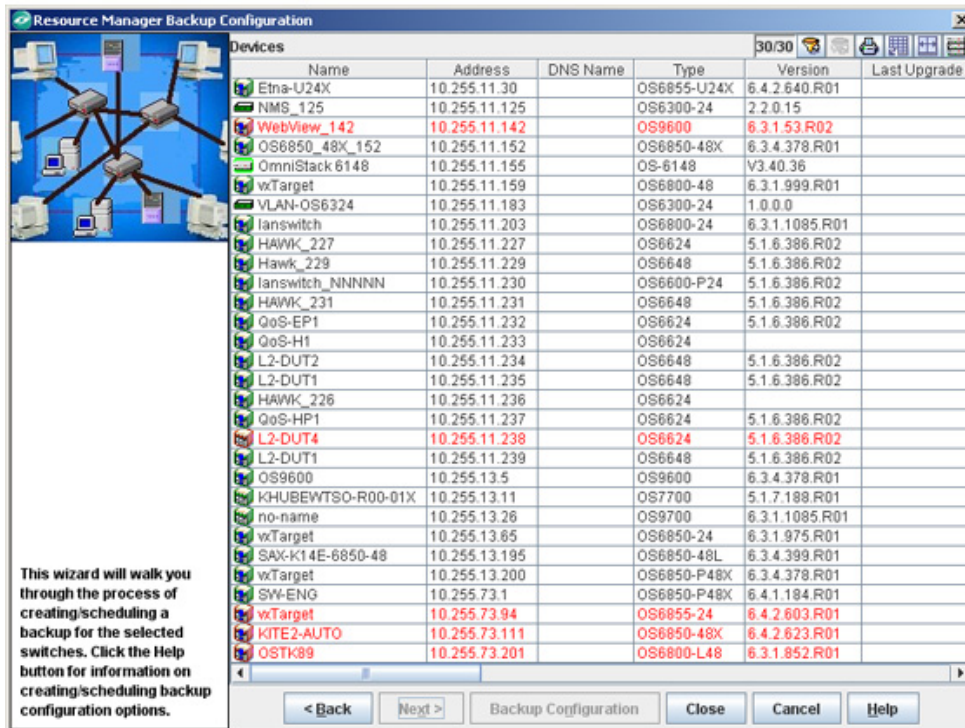
Select the desired option in Page One and click the **Next** button. Page Two of the Backup Configuration wizard displays.

Backup Configuration Wizard - Page 1

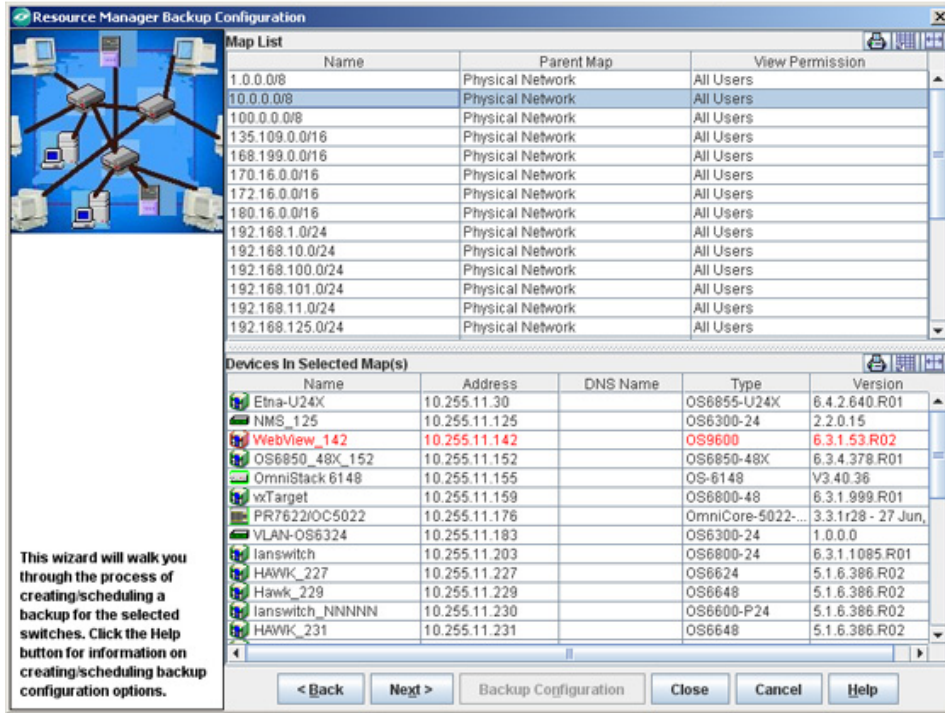


Page Two of the wizard (shown below) either displays a list of devices (note that the list does not include all devices in the list of All Discovered Devices) or a list of network maps to back up based on the option selected in Page One. Select one or more devices/maps that you want to backup and click the **Next** button. Page Three of the Backup Configuration wizard displays.

Backup Configuration Wizard - Page 2 (Devices)

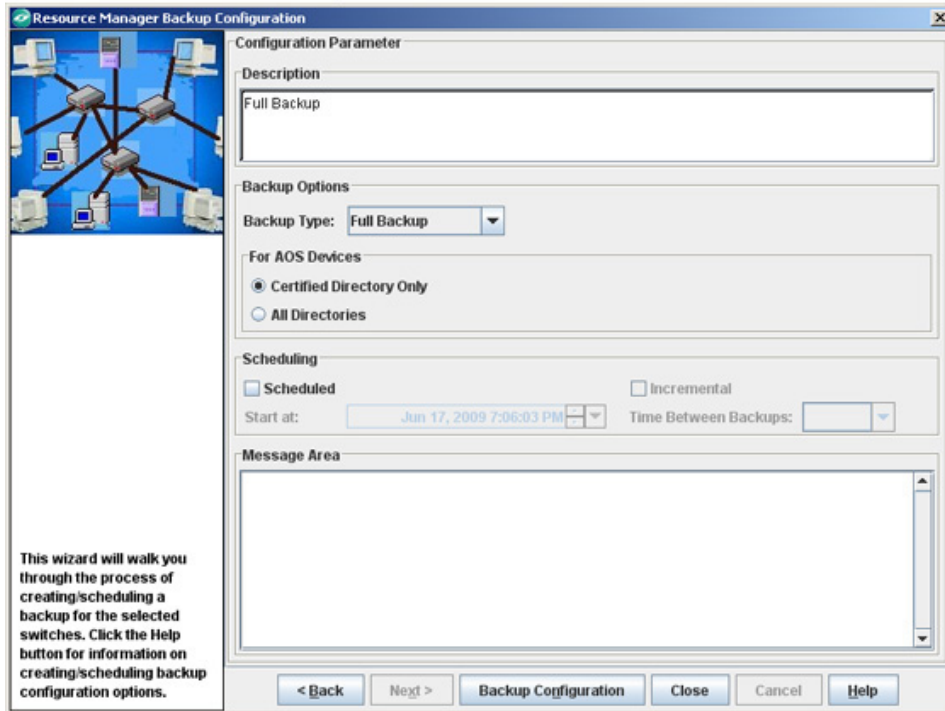


Backup Configuration Wizard - Page 2 (Maps)



Page Three of the Backup Configuration wizard (shown below) enables you to enter a description of the firmware to be saved, specify the type of backup you want performed, initiate the backup process, and monitor its progress. Page Three of the wizard also enables you to schedule the backup for a later time or date, if desired.

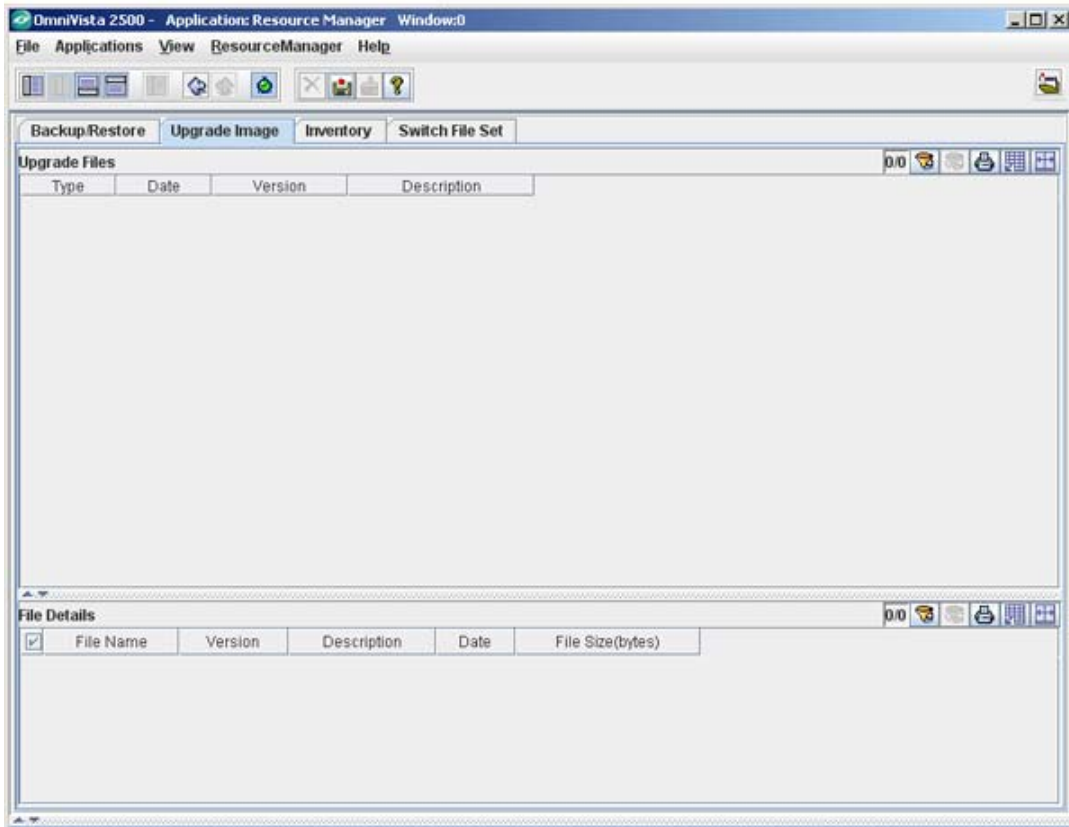
Backup Configuration Wizard - Page 3



Upgrade Image Tab

The Upgrade Image tab enables you to upgrade software, firmware, and FPGA (9000 series only) files. It is also used to perform an In-Service Software Upgrade (ISSU) on the CMM images (available only on 9000E Series Switches with redundant CMMs running AOS 6.4.1) Import the latest files from the Customer Support Web Site and use the "Upgrade Software" Wizard to upgrade a switch(es). As shown below, the top pane of the Upgrade Image tab, labeled "Upgrade Files," lists the imported firmware packages that currently exist on the server. When you select an import package in the "Upgrade Files" area the individual files will be listed in the bottom pane, labeled "File Details".

Upgrade Image Tab



Caution: Never attempt to import or install firmware files or upgrade packages acquired from any source other than Alcate-Lucent Customer Service. Image and Firmware files are specially packaged by Alcatel-Lucent Customer Server for importation into OmniVista, and contain an LSM file that describes the package contents to OmniVista. Installing new images files in XOS devices may cause configuration incompatibilities. Always check with Alcatel-Lucent Customer Support before installing new images files in XOS devices to ensure that the image files being installed are compatible.

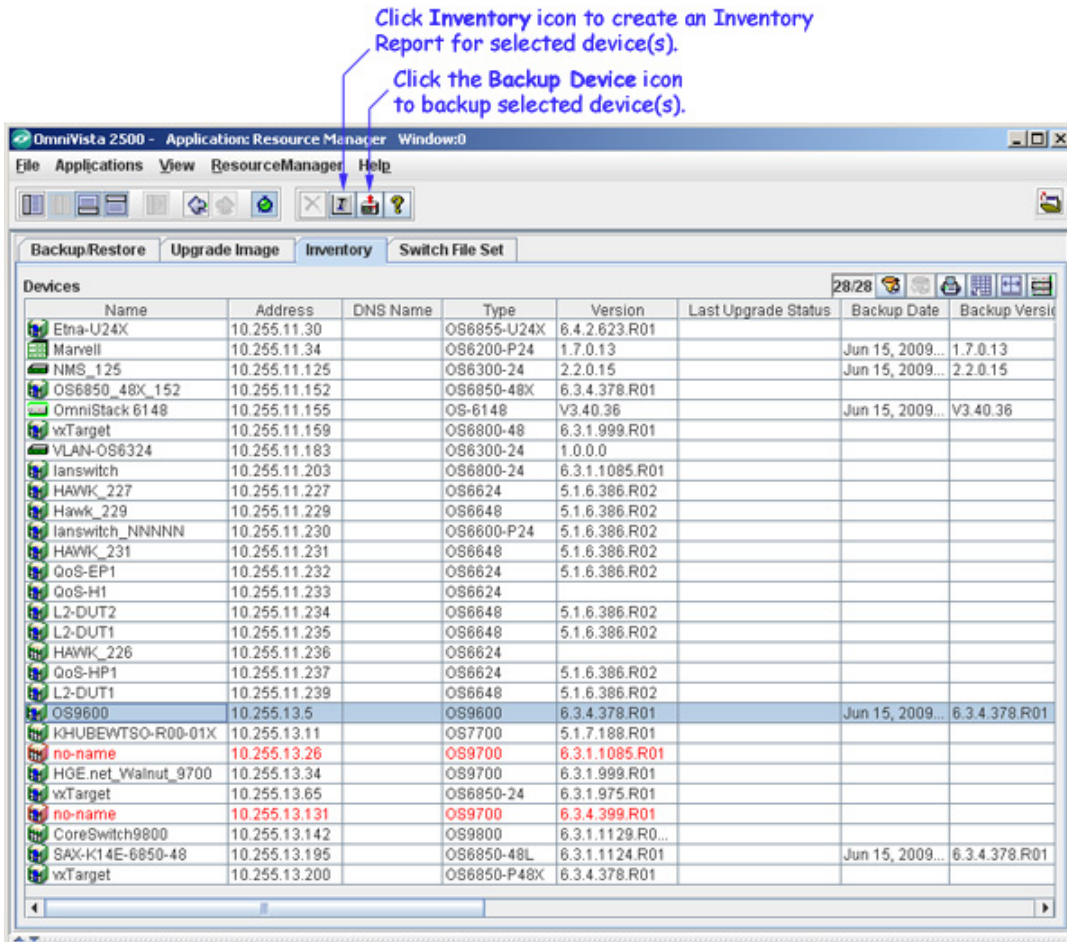
Resource Manager will prevent unsupported upgrades. When such an attempt is made, a message box informing that the upgrade has been rejected is displayed. This message box also displays details of the versions of the switch software required to successfully perform the upgrade.

Note: You must first complete the BootROM/Miniboot, U-Boot/Miniboot upgrade before upgrading the FPGA or image files. If you are upgrading a 6800 series switch, you must first upgrade the 5.3.1 software to 5.3.1.231.R02 or later.

Installation of firmware files takes place immediately when initiated; installation of firmware files cannot be scheduled for a later time or date. See “Using the Upgrade Image Tab” on page 18 for more information.

Inventory Tab

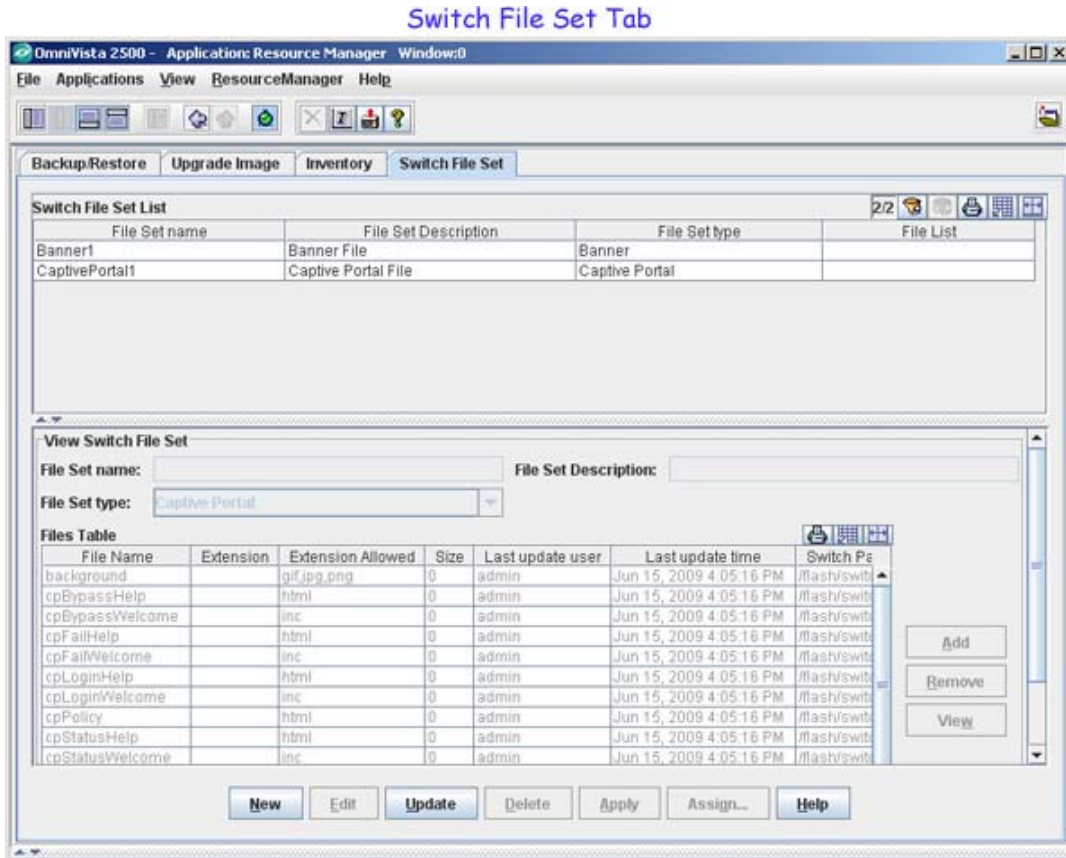
The Inventory tab, shown below, displays a list of the devices known to OmniVista that it is possible to inventory and back up. (Note that the list does not include all devices in the list of All Discovered Devices.) When the Inventory tab is displayed, icons in the Tool Bar enable you to create an Inventory Report for selected switches and to backup selected switches, as shown below. See “Using the Inventory Tab” on page 33 for more information.



Note: A new system file named "U-Boot" is available on OS9000 devices. This file is not supported on OmniVista 3.0. The Resource Manager can upload "Uboot" but it will not be automatically installed.

Switch File Set Tab

The Switch File Set Tab is used to "push" a command prompt banner and/or Captive Portal Web Page files to devices on the network. Banner files can be customized to display a unique command line banner for all devices on the network. Captive Portal, a web-based user authentication option within the Access Guardian application, presents the user with a web page for authentication. These web pages can also be customized by the user. See "Using the Switch File Set Tab" on page 37 for more information.

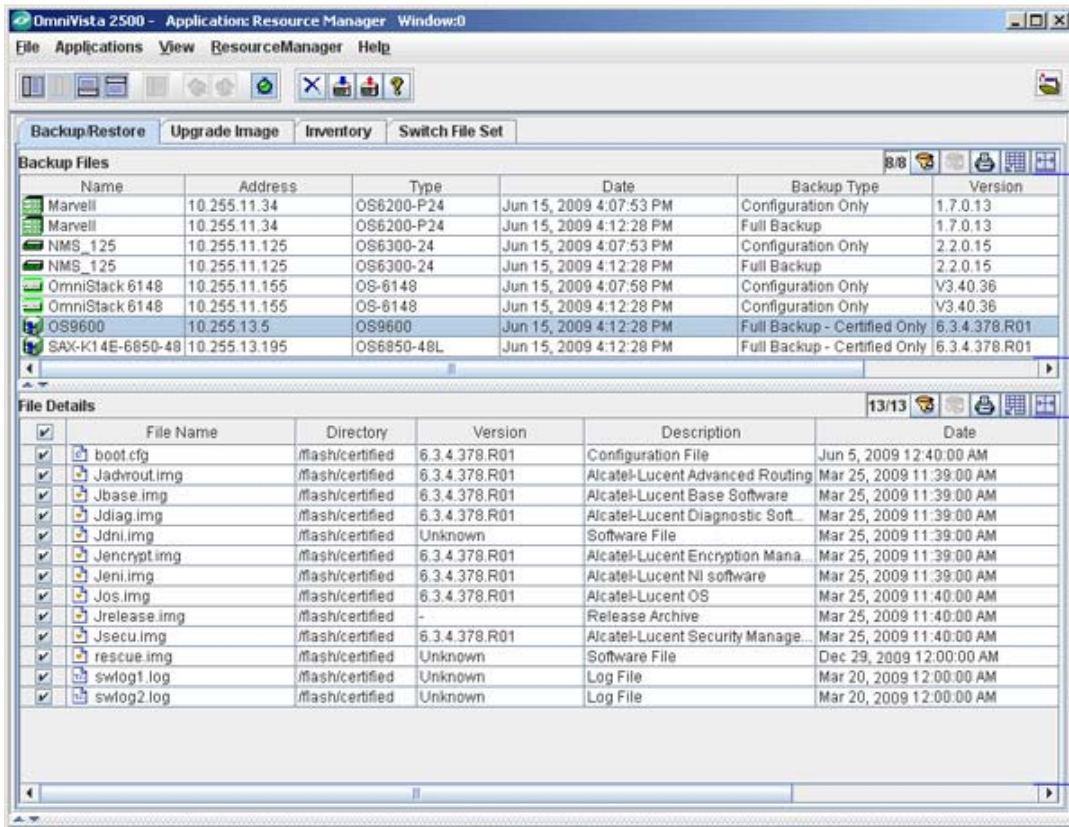


Using the Backup/Restore Tab

The Backup/Restore tab enables you to backup firmware configuration files to the OmniVista server, to view a detailed list of the files saved to the server during an individual backup, and to restore configuration files. As shown below, the top pane of the Backup/Restore tab, labeled "Backup Files," lists the switch backups that currently exist on the server. Select any backup listed and the bottom pane, labeled "File Details," lists the individual files that were saved to the server during the backup.

Note: Backup/Restore support using the Resource Manager application is currently available on OS6200 devices.

Backup/Restore Tab



List of switch backups. Select a backup to view details below.

List of files that were saved to the server for the selected switch.

"Backup Files" Fields

The fields in the "Backup Files" window pane are described below.

Name

The name of the switch that was backed up.

Address

The IP address of the switch that was backed up.

Type

The chassis type of the switch that was backed up.

Backup Date

The date and time that the backup was initiated.

Backup Type

The type of backup performed. The Backup type can be **Full Backup** (both configuration files and image files were backed up), **Configuration Only** (only configuration files were backed up), or **Image Only** (only image files were backed up).

Backup Version

The firmware version number of the files that were backed up. For AOS switches, this is read from the operating system's image file. For XOS switches, this is the version number of the primary MPM module's firmware. For the OmniStack 6024, 6048, 6124, 6148, 6300-24, and 8008, this is the version number of the Agent firmware.

User Description





A description entered by the OmniVista user who initiated the backup.

"File Details" Fields

The fields in the "File Details" window pane are described below.

File Name

The name of the individual file that was backed up and is currently stored on the OmniVista server. Each file name displays an icon to its left that identifies the type of the file. These icons indicate file types as follows:

- image file 
- configuration file 
- log file 
- other file types 

Version

The firmware version number of the file.

Description

An Alcatel-provided description of the file. This field will supply a standard description according to the filename extension, instead of displaying "Unknown". It will display the following values when the file itself is unknown, but uses a standard extension:

- .log - Log file
- .img - Software file
- .cmd - Command file


Date

The date the file was loaded into the switch.

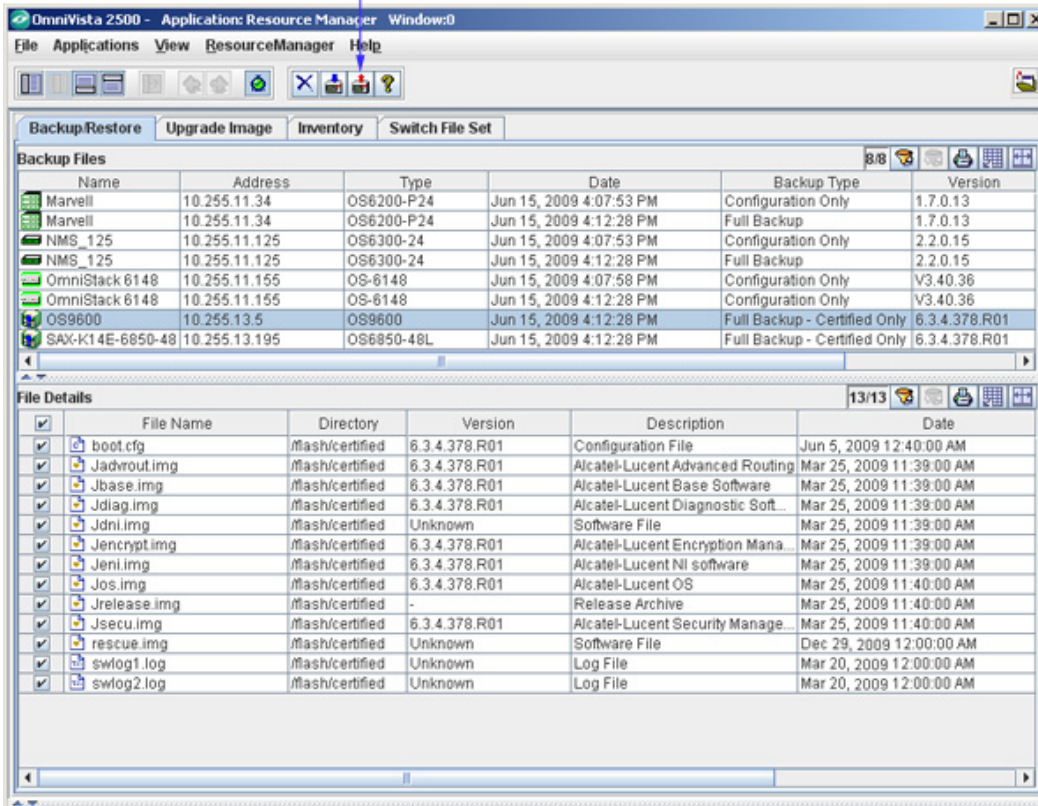
File Size (Bytes)

The size of the file, in bytes.

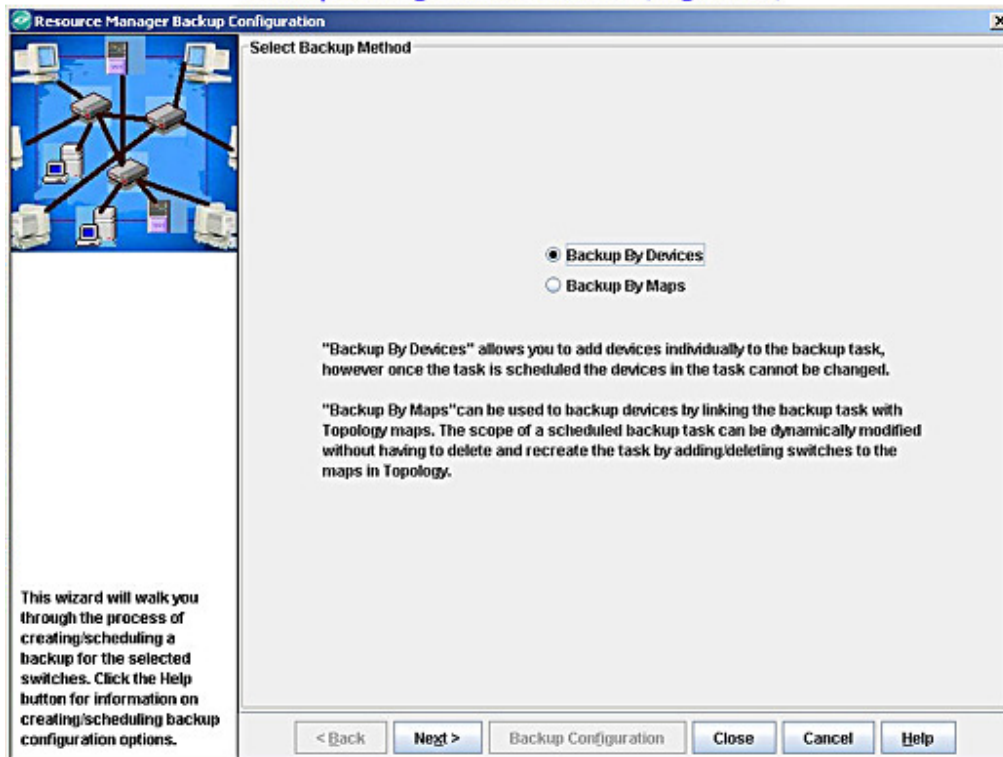
Initiating a Backup from the Backup/Restore Tab

To initiate backups for one or more switches from the Backup/Restore tab, merely click the Backup Device icon , or select **Backup** on the Resource Manager Menu, or press **Ctrl B**. The Backup Configuration Wizard opens. The first page of the Backup Configuration Wizard (shown below) enables you to select the switches that you want to backup. When the switches are selected, click the **Next** button to display page two of the Backup Configuration Wizard, which enables you to perform the backup and monitor its progress. See "Backup Configuration Wizard" on page 12 for further information on using the Backup Configuration Wizard.

Click on the Backup Device Image Files icon. The Backup Configuration Wizard is displayed, as shown below.



Backup Configuration Wizard (Page One)



Initiating a Backup from the List of All Discovered Devices

You can also initiate backups from the list of All Discovered Devices in the Topology application. To do this, follow the steps below.

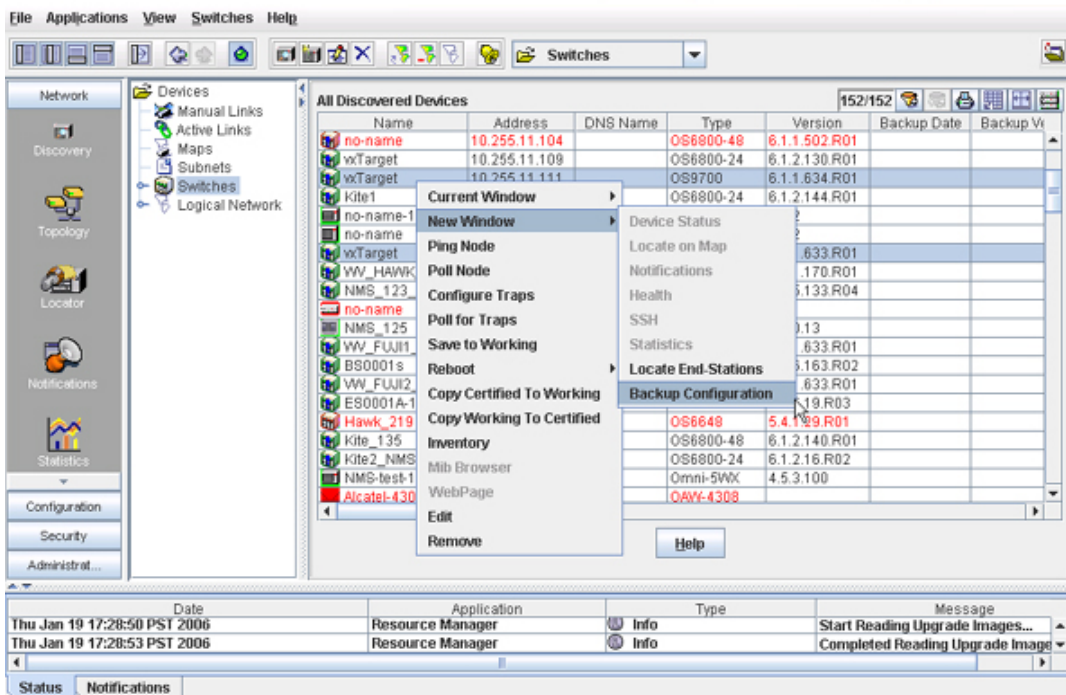
1. With the Topology application current, select **Switches** in the Tree, as shown below. The list of All Discovered Devices displays.
2. Select the switches in the list of All Discovered Devices that you want to back up. To select a single switch, merely click on it. **Shift**-click to select multiple contiguous switches. **Ctrl**-click to select multiple noncontiguous switches. Then click right to display a popup menu.
3. Select **Backup Configuration** on the popup menu. The Backup Configuration Wizard opens with page two displayed. Page two of the Backup Configuration Wizard enables you to back up the selected switches and monitor the backup process. See “Backup Configuration Wizard” on page 12 for further information on using the Backup Configuration Wizard.

1. Select switches in the tree.

2. Select the switches that you want to backup and click right. A popup menu displays.

3. Select Current Window or New Window.

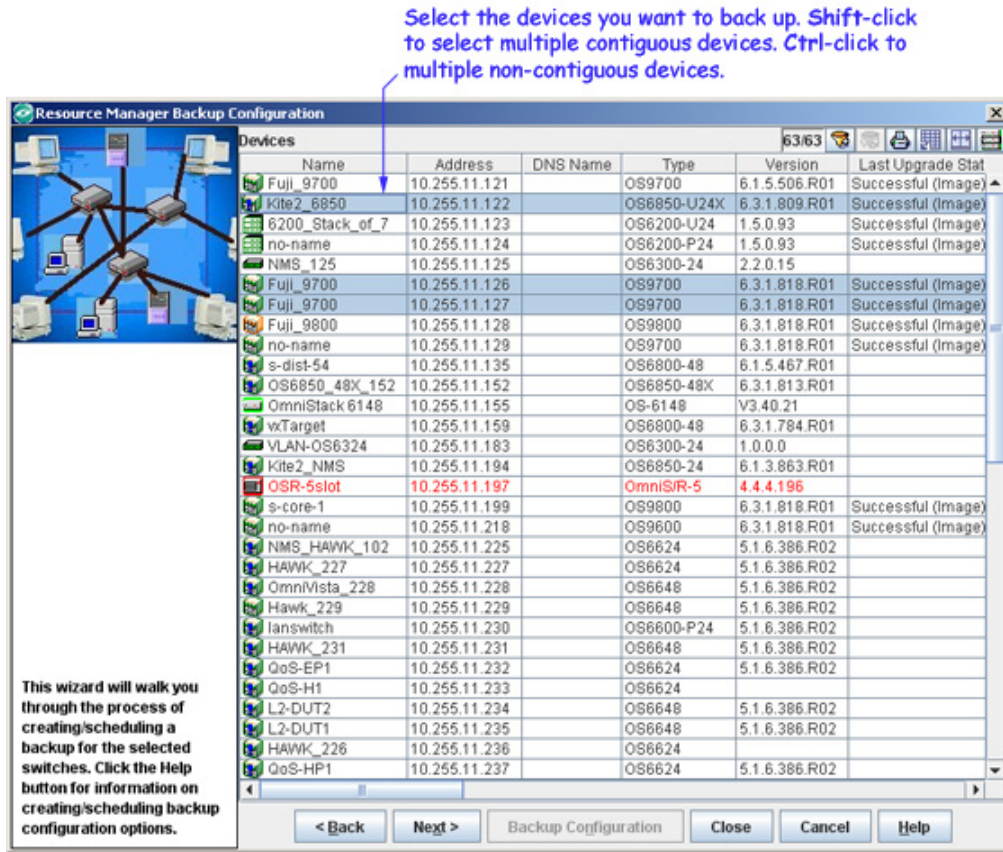
4. Select Backup Configuration. The Backup Configuration Wizard displays.



Backup Configuration Wizard

Page Two of the Backup Configuration wizard enables you to select either devices or regions that you want to backup. This page displays either a list of the devices known to OmniVista (note that the list does not include all devices in the list of All Discovered Devices) or a list of regions (as defined in the Topology application) that is possible to back up. To select a single device/region in the list, merely click on it. **Shift**-click to select multiple contiguous devices/regions. **Ctrl**-click to select multiple non-contiguous devices/regions. Click the **Next** button when you have made your selections.

Note: The information fields displayed for each device are identical to those displayed in the list of All Discovered Devices. For information on these fields, refer to the Topology help.



If **Backup By Maps** is selected in the Backup Configuration wizard, a list containing all maps defined in Topology will be displayed. Click on the desired map. All the devices belonging to the selected map will be displayed in **Device(s) in Selected Map(s)** section.

Select the region for which the backup has to be performed

All the maps defined in Topology will be displayed here

All the devices belonging to the selected map will be displayed here

This wizard will walk you through the process of creating/scheduling a backup for the selected switches. Click the Help button for information on creating/scheduling backup configuration options.

Name	Parent Map	View Permission
logical network	Logical Network	All Users
Subnet 10.10.10.0	Logical Network	All Users
1.0.0.0/8	Physical Network	All Users
10.0.0.0/8	Physical Network	All Users
111.0.0.0/8	Physical Network	All Users
120.0.0.0/8	Physical Network	All Users
130.0.0.0/16	Physical Network	All Users
130.201.0.0/16	Physical Network	All Users
136.18.0.0/16	Physical Network	All Users
140.0.0.0/16	Physical Network	All Users
151.96.0.0/16	Physical Network	All Users
153.18.0.0/16	Physical Network	All Users
172.100.0.0/16	Physical Network	All Users
172.16.0.0/16	Physical Network	All Users

Name	Address	DNS Name	Type	Version
falconCmm	10.255.11.100		OS7700	5.1.6.393.R01
Kite_Fiber_U24	10.255.11.101		OS6800-U24	5.3.1.181.R02
NMS_HAWK_102	10.255.11.102		OS6624	5.1.6.170.R02
nms-test-103	10.255.11.103		OmniS/R-9	4.4.5
vxTarget	10.255.11.104		OS6800-48	5.3.1.223.R02
vxTarget	10.255.11.111		OS9700	6.1.1.634.R01
Kite	10.255.11.112		OS6800-24	6.1.2.46.R03
no-name-119x	10.255.11.119		OmniS/R-6	4.5.2
no-name	10.255.11.120		OmniS/R-3	4.5.2
no-name	10.255.11.121		OS9700	6.1.3.105.R01
VV_HAWK_122-T	10.255.11.122		OS6648	5.1.6.164.R02
NMS_123_Hawk_1	10.255.11.123		OS6648	5.1.5.133.R04
no-name	10.255.11.124		OA-512	4.4.1

< Back Next > Backup Configuration Close Cancel Help

Select the devices you want to backup. Shift-click to select multiple contiguous devices. Ctrl-click to select multiple noncontiguous devices.


Note: This option is used to backup **all** devices in the selected region. You cannot backup selected devices. The devices displayed are for information purposes only. To backup select devices, select **Backup By Devices** on Page 1 of the Backup Wizard.

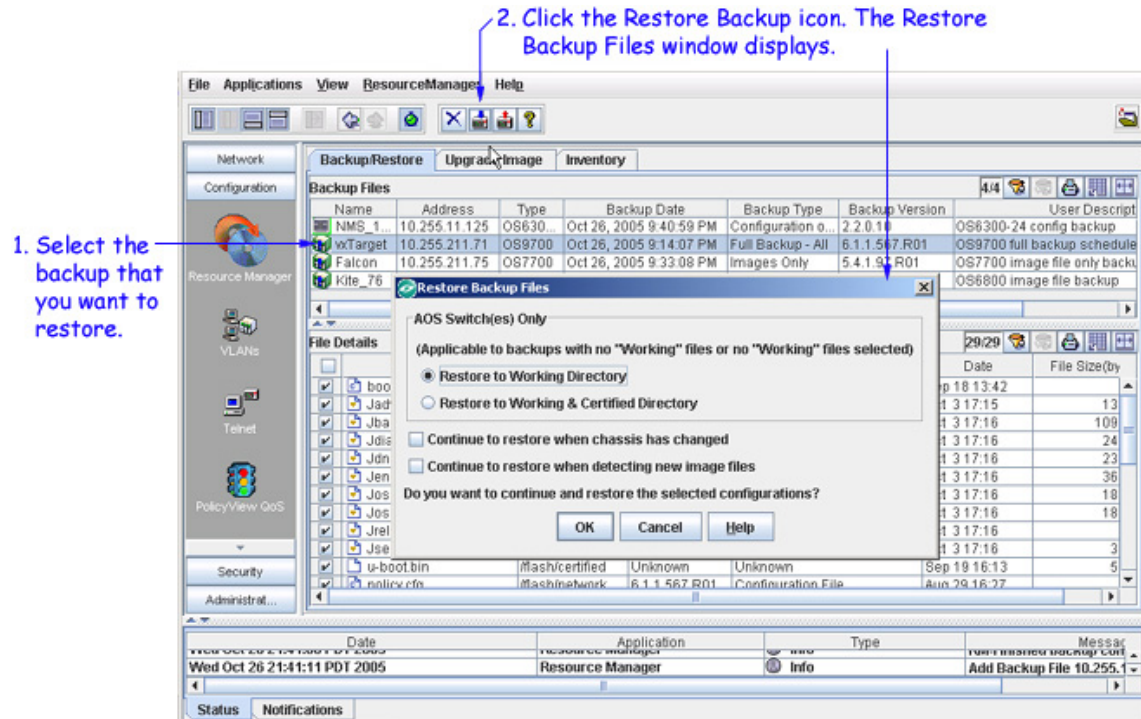
Note: If some devices in the region are not on-line, a dialog box will pop up warning you of the condition. Click **Yes** to continue the backup. Click **Cancel** to cancel the backup.

Click the **Next** button when you have made your selections.

Restoring a Backup

Backups can be restored to the original switch from which the backup was taken. (Backups cannot be restored to other switches, because doing so would cause mismatched IP addresses and other network problems.) To restore a backup, follow the steps below.

1. Select the backup that you want to restore in the "Backup Files" window pane, as shown below.
2. Click the Restore Backup icon , or select **Restore** on the Resource Manager Menu, or press **Ctrl R**. The Restore Backup Files window displays, as shown below.

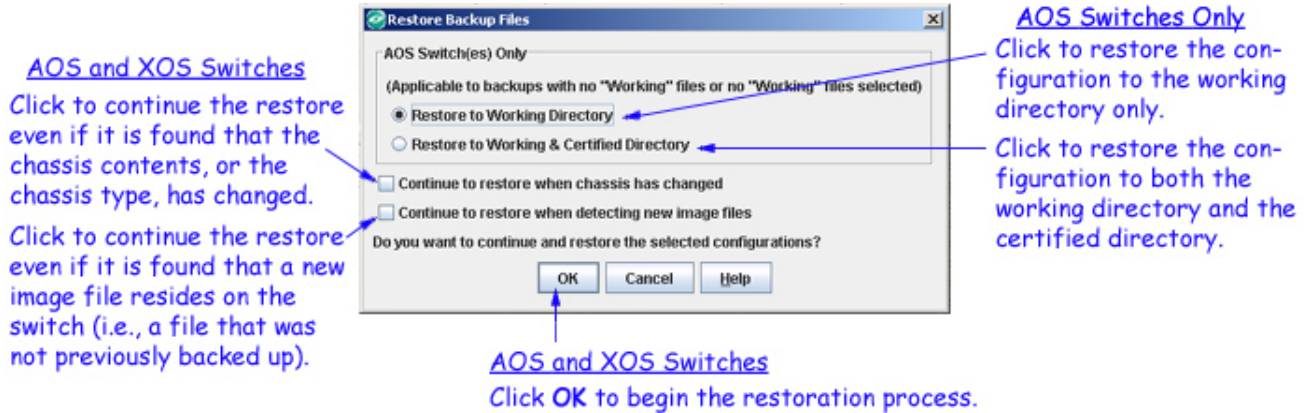


3. If the switch is an AOS switch, click **Restore to Working Directory** or **Restore to Working & Certified Directory** on the **Restore Backup Files** window to specify the directories to which you want the backup restored. These selections are not applicable to XOS devices. All the other selected files under "switch" and "network" will go back to their respective directories on the switch. If one or more working directory files are selected, then all the files selected will go back to their respective directories on the switch. By default, the **Restore to Working Directory** radio button is selected.

4. For both AOS and XOS switches, activate checkboxes on the Restore Backup Files window to indicate the action you want taken if the following changes are detected on the switch:

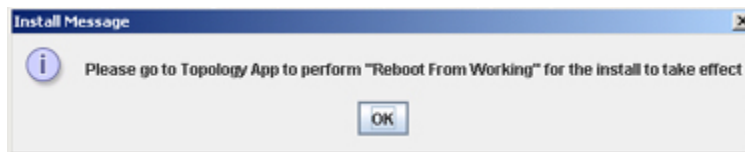
- Click the **Continue to restore when chassis has changed** checkbox if you want to continue the restore even if it is found that the chassis contents, or the chassis type, has changed since the backup. If you do not enable this checkbox, the restore will not take place if the chassis has changed.
- Click the **Continue to restore when detected new image files** checkbox if you want to continue the restore even if it is found that a new image file resides on the switch (i.e., a

file that were not previously backed up). If you do not enable this checkbox, the restore will not take place if a new image file is found on the switch.



5. For both AOS and XOS switches, click the **OK** button to start the restoration process. When the restore is complete, a message reports the success or failure of the operation in the status panel.

6. When the restore has successfully completed, you are prompted to reboot AOS and XOS switches to load the restored configuration into flash memory. A message similar to the following displays for AOS switches:



AOS switches can be rebooted from OmniVista's Topology application, by connecting to the switch and using the **Load From** command. Refer to the Topology help for more information. XOS switches can be rebooted via Telnet, etc. The OmniStack 6024, 6048, 6124, 6148, and 8008 will automatically reboot without user intervention when the file transfer is complete.

Understanding the Restoration Process

Restoration Errors

Note that the status messages will report any error that occurred during the restoration process. The term *error* refers to any problem that caused the restoration to fail -- perhaps because the switch went down during the restoration process. The worst-case error is a partial restoration, which could occur if a switch goes down between the server and the target switch. The network administrator must restore the file system manually if a partial restoration occurs. Network administrators should investigate and resolve any error listed, as the presence of an error means that the configuration was incompletely or imperfectly restored.

Pre-Restoration Checks

The restoration process checks the switch for compatibility before restoring any configuration files. The following checks are made:

- chassis type has not changed
- number of slots in the chassis has not changed
- MPM module type has not changed
- modules installed in individual slots have not changed
- new image files are not present on the switch

If any of the above changes are detected, the restore will proceed, or abort, according to the checkbox settings on the Restore Backup Files window (explained above).

Restored Files on the Switch

When files are restored, the existing configuration files on the switch are overwritten. However, restored files will overwrite existing files of the same name only. If other configuration files exist on the switch, they will NOT be automatically deleted by the restoration process.

Rebooting the Switch

When the restore process is completed, the switch must be rebooted to load the restored configuration into flash memory. You can reboot AOS switches via OmniVista's **Load From** command. You can reboot XOS switches via Telnet, etc. Note that OmniStack devices (the OmniStack 6024, 6048, 6124, 6148, 6300-24, and 8008) will automatically reboot without user intervention when the file transfer is complete.

Viewing Backup and Restore Status in the Audit Application

Whenever you backup or restore a configuration, entries are made in the audit log **config.log** that document the backup or restore process. You can view these entries by going to the Audit application and selecting **config.log** under **Current Log Files** in the Tree, as shown below. Select any entry in **config.log** to display further information such as its date, type, log ID, etc.

Audit Application Entries for Saved and Restored Configurations


Select **config.log** under **Current Log Files** to view Audit application entries for saved and restored configurations.

Entries in **config.log** document backups and restores.

Date	Client	User	Type	Message
Jan 23, 2006 6:15:36 PM	128.251.30.61	admin	Information	Removing file (flash/working/Fwebrou...
Jan 23, 2006 6:15:42 PM	128.251.30.61	admin	Information	copying (flash/working/Fwebrou...
Jan 23, 2006 6:15:42 PM	128.251.30.61	admin	Information	Removing remote file (flash/workin...
Jan 23, 2006 6:15:42 PM	128.251.30.61	admin	Information	Remote file (flash/working/Fwebse...
Jan 23, 2006 6:15:47 PM	128.251.30.61	admin	Information	copying (flash/working/Fwebse...
Jan 23, 2006 6:15:51 PM	128.251.30.61	admin	Information	copying (flash/working/Fwebse...
Jan 23, 2006 6:15:51 PM	128.251.30.61	admin	Information	Executing an Install Command
Jan 23, 2006 6:15:52 PM	128.251.30.61	admin	Information	Completed executing an install com...
Jan 23, 2006 6:15:52 PM	128.251.30.61	admin	Information	Restore configuration for device: 10...
Jan 23, 2006 6:15:52 PM	128.251.30.61	admin	Information	Please go to Topology App to perfor...
Jan 23, 2006 6:15:52 PM	128.251.30.61	admin	Information	Finished Restore configuration for:

Date	Application	Type	Message
Mon Jan 23 17:56:51 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Completed installing miniboot.def file
Mon Jan 23 17:56:51 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Removing miniboot.default file
Mon Jan 23 17:56:51 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Completed Removing miniboot.default file

Deleting Backups

To delete a saved backup, merely select the backup in the "Backup Files" window pane and click the **Delete** icon , or select **Delete** on the Resource Manager Menu, or press the **Del** key. Note that you can delete an entire backup, but you cannot selectively delete individual files in a backup.

Using the Upgrade Image Tab

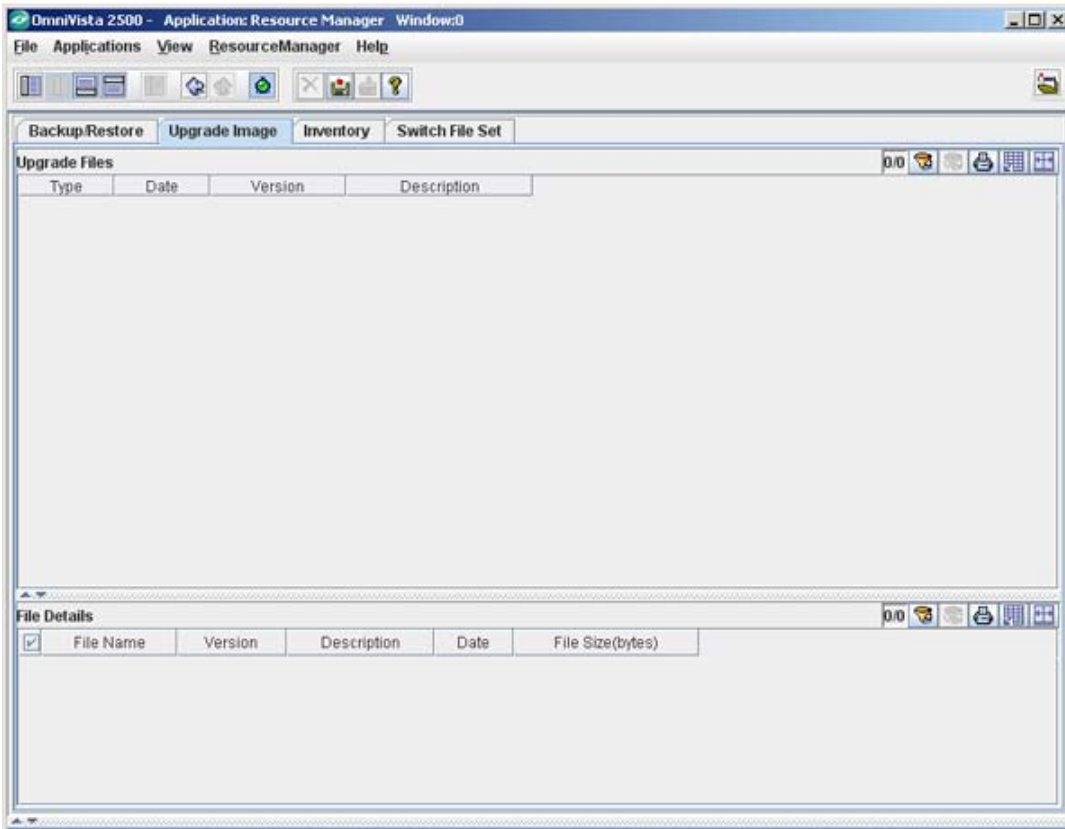
The Upgrade Image tab enables you to upgrade software, firmware, and FPGA (9000 series only) files. Import the latest files from the Customer Support Web Site and use the "Upgrade Software" Wizard to upgrade a switch(es). As shown below, the top pane of the Upgrade Image tab, labeled "Upgrade Files," lists the imported firmware packages that currently exist on the server. When you select an import package in the "Upgrade Files" area the individual files will be listed in the bottom pane, labeled "File Details".

Caution: Never attempt to import or install firmware files or upgrade packages acquired from any source other than Alcatel-Lucent Customer Service. Image and Firmware files are specially packaged by Alcatel Customer Server for importation into OmniVista, and contain an LSM file that describes the package contents to OmniVista. Installing new images files in XOS devices may cause configuration incompatibilities. Always check with Alcatel-Lucent Customer Service before installing new images files in XOS devices to ensure that the image files being installed are compatible.

Resource Manager will prevent unsupported upgrades. When such an attempt is made, a message box informing that the upgrade has been rejected is displayed. This message box also displays details of the versions of the switch software required to successfully perform the upgrade.

Note: You must first complete the BootROM/Miniboot, U-Boot/Miniboot upgrade before upgrading the FPGA or image files. If you are upgrading a 6800 series switch, you must first upgrade the 5.3.1 software to 5.3.1.231.R02 or later.

Upgrade Image Tab




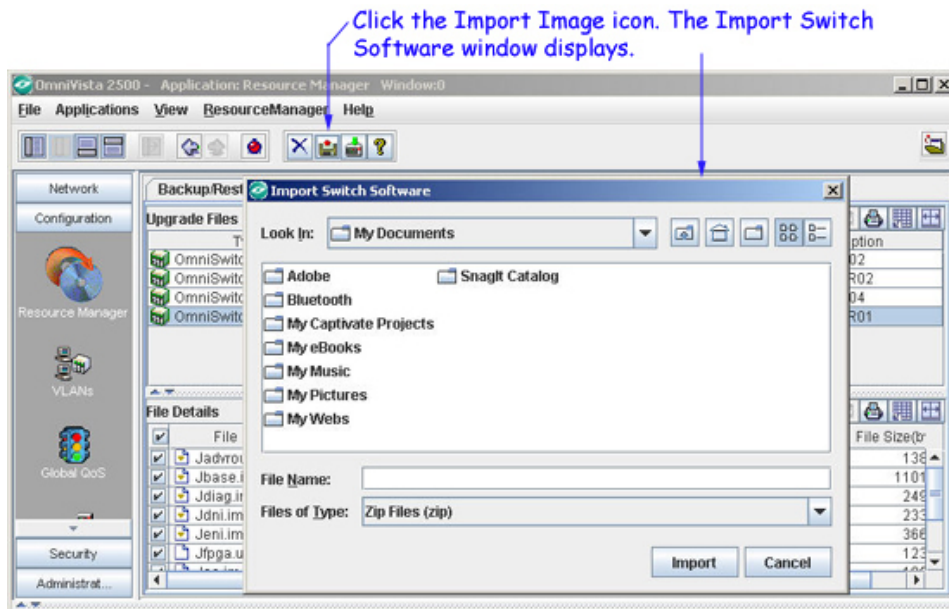
List of imports by device type. Select an import to view details below.

Individual files in the import selected above.

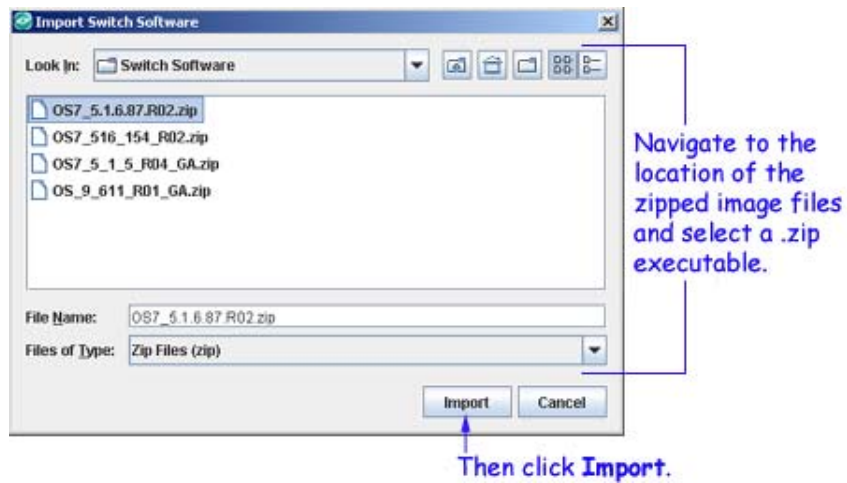
Importing the Upgrade Files

All upgrade files supplied by Alcatel-Lucent Customer Service are packaged as WinZip executables and have a .zip file extension. Do not attempt to unzip the firmware files manually. Import the WinZip executable and OmniVista will automatically unzip the executable as part of the import process.

1. Download the upgrade files to your PC.
2. With the Upgrade Image tab displayed, click the Import Image icon , or select **Import** on the Resource Manager menu, or press **Ctrl + I**. The Import Switch Software window is displayed.



3. In the Import Switch Software window, navigate to the location of the zipped firmware files and select a .zip executable. Then click the **Import** button. The import process begins immediately.



Messages in the Status Panel report the start, progress, and finish of the import process, and report any error that may occur. When the process is complete, the imported firmware files are listed in the Upgrade Image tab.

Import Status Messages in the Status Panel


Date	Application	Type	Message
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip:Starting Import
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-Copying OS_9_611_R01_GA.zip info ser
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-Done Copying OS_9_611_R01_GA.zip inf
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (softwa
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :Parsing (softwa
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (miniboo
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jadvrou
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jbase.ir
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jdiag.im
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jfpga.im
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jfpga.im
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jfpga.im
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jfpga.im
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jfpga.im
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jfpga.im
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jfpga.im
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :copied (Jfpga.im
Mon Jan 23 16:43:10 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :finished import
Mon Jan 23 16:43:13 PST 2006	Resource Manager	Info	RM-OS_9_611_R01_GA.zip :Add Upgrade Im
Mon Jan 23 16:43:13 PST 2006	Resource Manager	Info	Add Upgrade Image OmniSwitch9xxx

Installing the Upgrade Files

Follow the steps below to install the upgrade files.

1. In the "Upgrade Files" window pane, select the desired import. The individual image files contained in the import display in the "File Details" window pane. By default, the "select" checkbox by each image file (shown below) is enabled and the "select" checkbox by each BMF file on AOS switches is disabled. Only selected files will be installed.

2. Click to deactivate the "select" checkbox by any individual image file that you do NOT want installed.

3. Click the Install New Image Files icon , or select **Install** on the Resource Manager Menu, or press **Ctrl L**. The Install Upgrade Software Wizard opens. The first page of the Wizard (shown below) lists all devices that qualify for installation of the selected image files. Select the device or devices in which you want to install the files. When your selections are complete, click the **Next** button to display page two of the Wizard, which enables you to perform the installation and monitor its progress.

3. Click the Install New Image Files icon. The Install Upgrade Software Wizard displays (shown below).

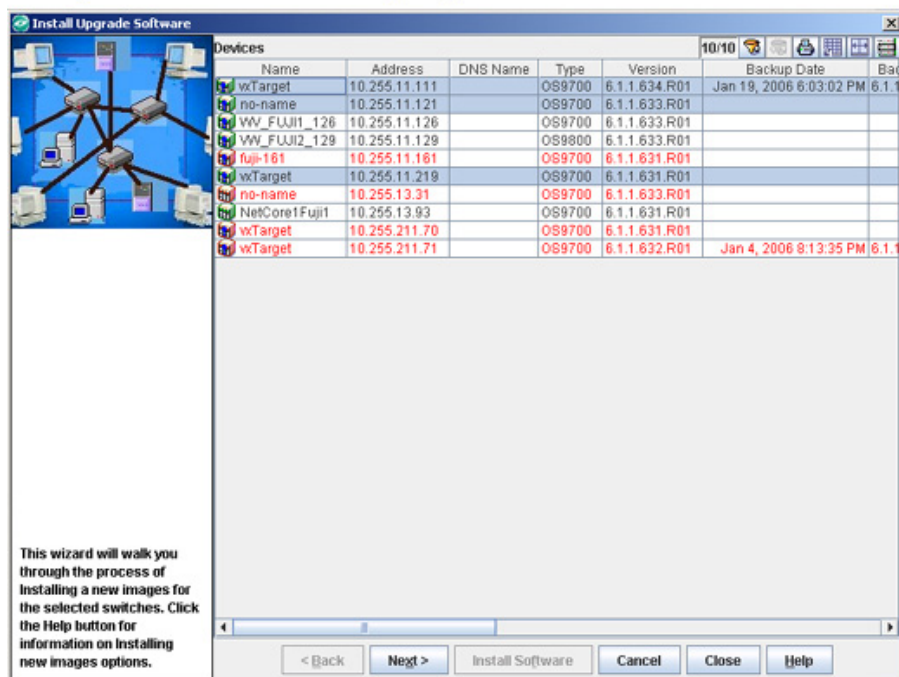
1. Select the import that contains the firmware files you want to install.

2. Click to deactivate the "select" checkbox by any firmware file you do not want to install.

Type	Date	Version	Description
OmniSwitch7xxx	Jan 23, 2006 4:40:42 PM	5.1.6.87.R02	AOS 5.1.6.87.R02
OmniSwitch7xxx	Jan 23, 2006 4:41:38 PM	5.1.6.154.R02	AOS 5.1.6.154.R02
OmniSwitch7xxx	Jan 23, 2006 4:42:12 PM	5.1.5.54.R04	AOS 5.1.5.54.R04
OmniSwitch9xxx	Jan 23, 2006 4:42:54 PM	6.1.1.633.R01	AOS 6.1.1.633.R01

File Name	Version	Description	Date	File Size(bytes)
<input type="checkbox"/> bootrom.bin	5.1.6.87.R02	bootrom firmware	Aug 11, 2004	422032
<input checked="" type="checkbox"/> Fadvrout.img	5.1.6.87.R02	CMM Advanced Routing	Jun 27, 2005	984801
<input checked="" type="checkbox"/> Fbase.img	5.1.6.87.R02	CMM Base	Jun 27, 2005	4300445
<input checked="" type="checkbox"/> Fdiag.img	5.1.6.87.R02	CMM Diagnostics	Jun 27, 2005	331338
<input checked="" type="checkbox"/> Feni.img	5.1.6.87.R02	NI image for all Ethernet-type NIs	Jun 27, 2005	1308842
<input checked="" type="checkbox"/> Ffpga_upgrade_kit	5.1.6.87.R02	ffpga upgrade kit firmware	Apr 27, 2005	1520343
<input checked="" type="checkbox"/> FI2eth.img	5.1.6.87.R02	CMM Layer 2 and Ethernet drivers	Jun 27, 2005	987208
<input checked="" type="checkbox"/> Fos.img	5.1.6.87.R02	CMM Operating System	Jun 27, 2005	1495009
<input checked="" type="checkbox"/> Fqos.img	5.1.6.87.R02	CMM Quality of Service	Jun 27, 2005	313011
<input checked="" type="checkbox"/> Frelease.img	5.1.6.87.R02	Release Archive	Jun 27, 2005	5521
<input checked="" type="checkbox"/> Froutrimg	5.1.6.87.R02	CMM Routing (IP and IPv6)	Jun 27, 2005	720233
<input checked="" type="checkbox"/> Fsecu.img	5.1.6.87.R02	CMM Security (AVLANs)	Jun 27, 2005	130240
<input checked="" type="checkbox"/> Fweb.img	5.1.6.87.R02	CMM Webview - Main	Jun 27, 2005	1433250
<input checked="" type="checkbox"/> Fwebadvrout.img	5.1.6.87.R02	CMM Webview - Advance Routing	Jun 27, 2005	249618

Install Upgrade Software Wizard (Page One)
Page One lists all devices that qualify for installation of the selected files.



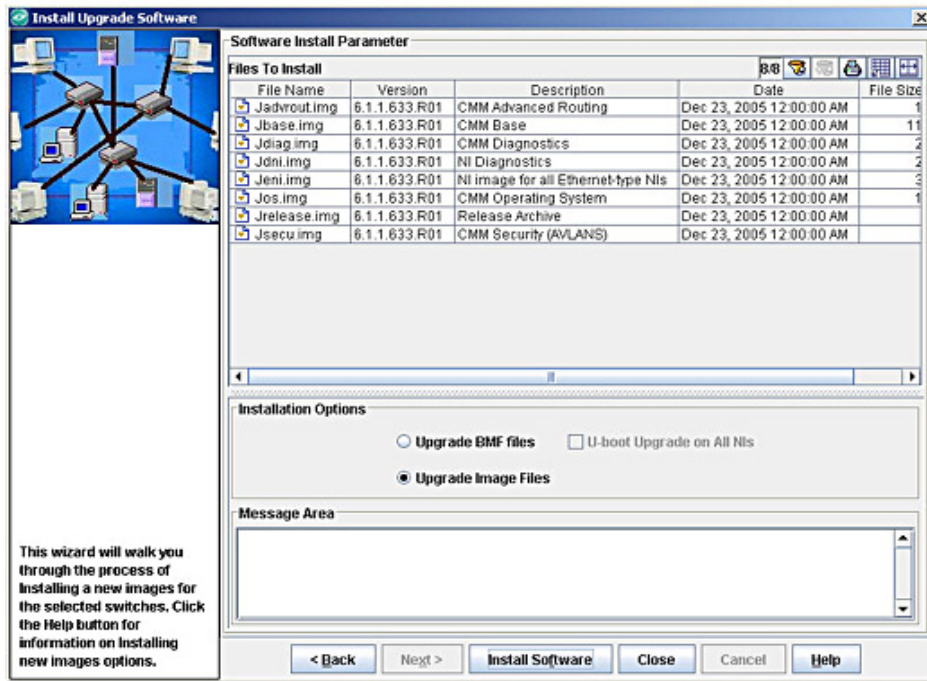
4. Select an **Installation Option**.

- **Upgrade BMF Files** - Upgrade the BootROM, MiniBoot, or FPGA files (AOS switches only).
- **Upgrade Images Files** - Upgrade the image files on the switch(es) (Default) .
- **U-Boot Upgrade on all NIs** - Perform u-boot upgrade for all the NIs on the switch(es) (9000 series switches only).
- **In-Service Software Upgrade (ISSU)** - Upgrade the image files on redundant CMMs with minimal data interruption. This option is only available (and displayed) for 9000E Series Switches (Release 6.4.1).

Note: If "OmniSwitch 9xxx-ISSU" files are imported and then selected in the "Upgrade Files" window (Step 1 above), only 9000E Series switches will be displayed in the "Devices" window. See "In-Service Software Upgrade" on page 29 for more information on ISSU.

- **6200 Device(es) Installation Options (6200 Devices Only).**
 - **Upgrade Master Unit Only** - Upgrade the image files on the master switch in the stack.
 - **Upgrade All NIs in Stack** - Upgrade the image files on all switches in a stack.

Install Upgrade Software Wizard (Page Two)
 Page Two enables you to perform the installation and monitor its progress.




Warning: Do **not** attempt to use the BMF option on an AOS switch unless it has already been upgraded to 5.1.5.R03 or later image files.

Note: The "U-boot Upgrade on All NIs" option will only be enabled when the imported software files to be installed on the switch are for OS9000 devices.

5. Select "Install Software" to begin the installation process immediately.

Deleting Imported Firmware Files

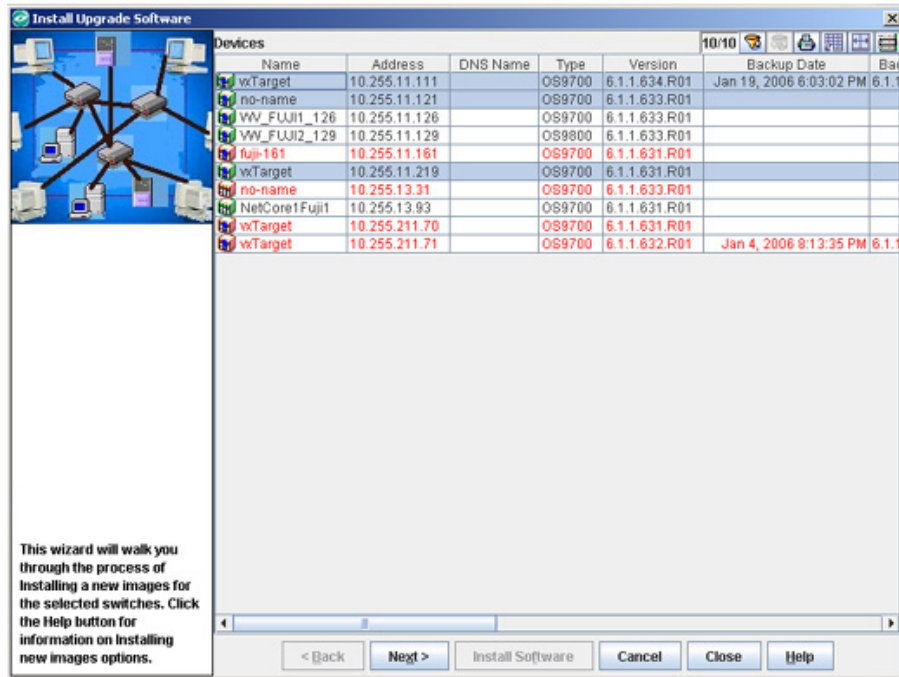
To delete imported firmware files from the OmniVista server, merely select the import in the "Upgrade Files" window pane and click the **Delete** icon , or select **Delete** on the Resource Manager Menu, or press the **Del** key. Note that you can delete an entire import, but you cannot selectively delete individual files in an import.

BMF Upgrades

The first page of the Install Upgrade Software Wizard, shown below, lists all known devices that qualify for installation of the selected BootROM, MiniBoot, and FPGA (BMF) files. Select the device or devices in which you want to install the files. To select a single device in the list, merely click on it. **Shift**-click to select multiple contiguous devices. **Ctrl**-click to select multiple non-contiguous devices. Click the **Next** button when you have made your selections.

Note: The information fields displayed for each device are identical to those displayed in the list of All Discovered Devices. For information on these fields, refer to the Topology help.

Install Upgrade Software Wizard (Page One)
 Page One lists all devices that qualify for installation of the selected files.



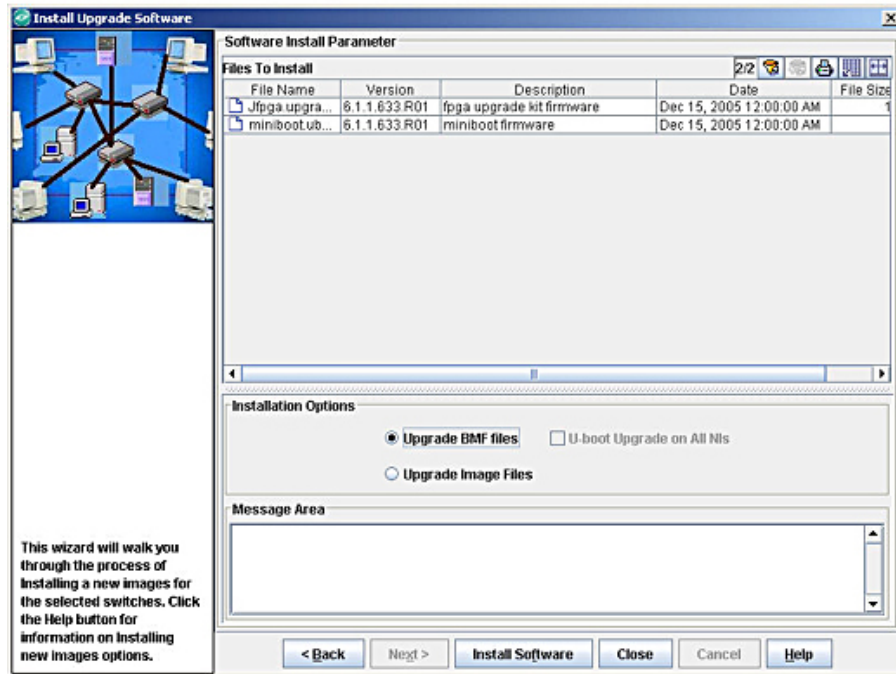
Click the **Next** button when you have made your selections.

Installing the BMF Files

The second page of the Install Upgrade Software Wizard, shown below, enables you to install the BootROM, MiniBoot, and FPGA (BMF) files and monitor the installation process for AOS switches with 5.1.5.R03 and later image files. Installation of BMF files takes place immediately when initiated; installation of BMF files cannot be scheduled for a later time or date. Note that BMF files will be loaded into the **/flash** directory during installation but are deleted after a successful installation.

Warning: Do not attempt to install BMF files on AOS switches unless they have already been upgraded to 5.1.5.R03 or later image files.

Install Upgrade Software Wizard (Page Two)
Page Two enables you to perform the installation and monitor its progress.



Before You Begin

Before you attempt to upgrade BootROM, MiniBoot, and FPGA (BMF) files the follow prerequisites must be met:

- All switches must be running Release 5.1.5.R03 (or later) image files.
- All CMMs should have at least 4.2 MB of free space in **/flash** memory.
- A shunt connecting pins 1 and 2 on jumper block J64 (OS9000), J21 (OS8800), J345 (OS7800), or J31 (OS7700) or must installed on all CMMs. (This is the factory default configuration.)

Installation Order

To ensure successful BootROM, MiniBoot, and FPGA (BMF) upgrades and to reduce possible network down time, BMF upgrades should be performed in the following order:

1. Upgrade the applicable BootROM/MiniBoot files (**bootrom.bin/miniboot.default** or **u-boot.bin/miniboot.uboot**).

Note: If you are upgrading the **bootrom.bin file**, wait a sufficient time to ensure that the BMF upgrade was successful. (Alcatel recommends two weeks.)

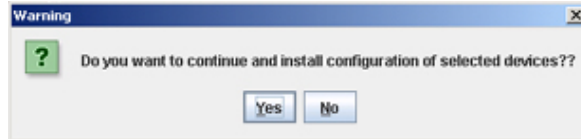
2. After successfully upgrading the BootRom/MiniBoot files, upgrade the FPGA.

Note: You must upgrade the BootROM/MinBoot files **before** upgrading the FPGA. Also note that you cannot upgrade **only** the U-Boot. You must update the U-Boot and MiniBoot at the same time.

Perform the steps described in How to Install BMF Files below.

How to Install BMF Files

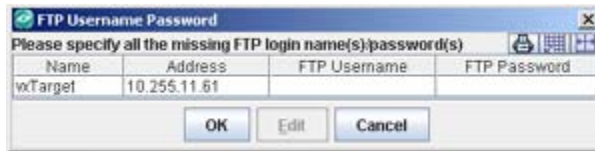
Click the **Install Software** button at the bottom of the Wizard. If the device FTP login names and passwords for the devices were previously defined to OmniVista via the Edit Discovery Manager Entry window, the confirmation query shown below displays.



Click **Yes** and the installation process begins.

If FTP User Names/Passwords are Undefined

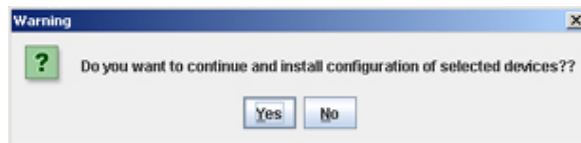
If the FTP user names and passwords for the devices were not previously defined to OmniVista via the Edit Discovery Manager Entry window, the FTP User Name Password window displays. An example is shown below. This window queries you to supply the FTP user names and passwords required for the backup.



To supply the FTP user name and password for a device, select the device in the FTP User Name Password window and click the **Edit** button. The Specify FTP Login window, shown below, displays. Enter the FTP user name and password for the selected device in the appropriate fields. If the user name and password you enter also apply to the other devices, click the **Same for all Unspecified** checkbox. Then click the **OK** button.



If necessary, continue to enter FTP user names and passwords until they have been specified for all devices listed. When all user names and passwords have been specified, the confirmation query shown below displays

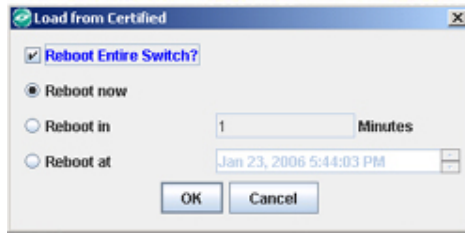


Click **Yes** to begin the installation process.

When the Installation Completes

When the install has successfully completed, you are prompted to reload the AOS switches. After the installation completes, you must reload the AOS switches by selecting the **Reboot Entire Switch** option using the **Load From Certified** or **Reboot From Certified** command. Either command will bring up the Load From Certified window, which is shown below. You can perform this task by connecting to the switch from OmniVista's Topology application. (To connect to a switch, merely select it in the Topology application's Tree. Refer to the Topology help for more information.)

The Load from Certified window enables you to schedule the reboot.

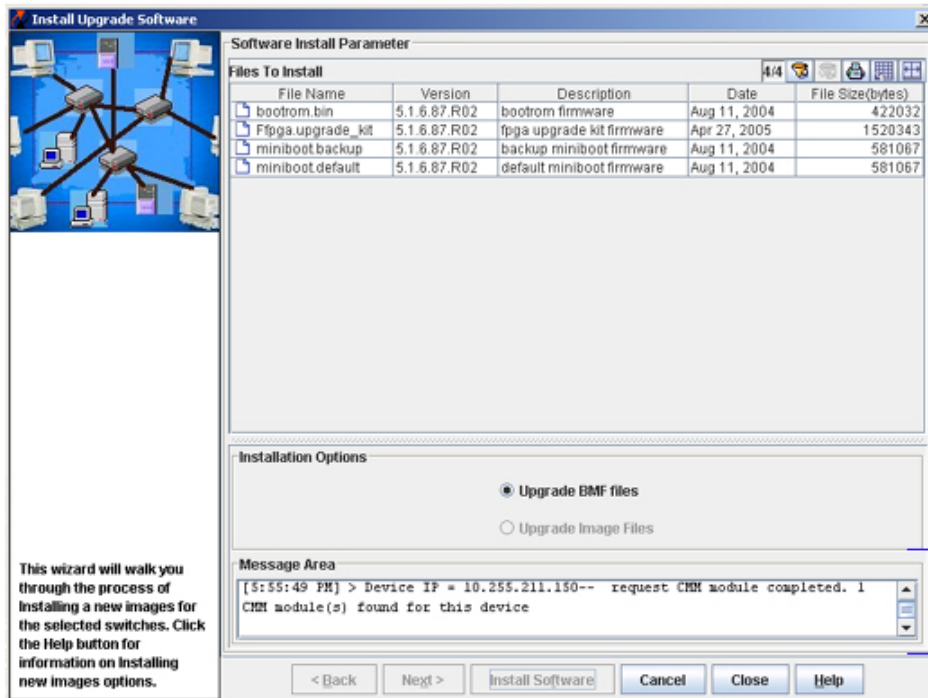


Note: When you select the **Reboot Entire Switch** option the operation does not necessarily take place immediately since OmniVista needs to propagate the command to all switches you have upgraded.

Monitoring the Installation Process

If you leave the Install Upgrade Software Wizard open, you can view status messages that document the installation process as it occurs. An example is shown below. Note that the install operation will continue even if the Wizard is closed.

Status Messages in the Install Upgrade Software Wizard



Status messages documenting the installation process as it occurs also display in the Status Panel. An example is shown below.

Status Messages in the Status Panel

Date	Application	Type	Message
Mon Jan 23 17:55:49 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Request CMM module information
Mon Jan 23 17:55:49 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- request CMM module completed. 1 CMM mod
Mon Jan 23 17:55:55 PST 2006	Resource Manager	Info	RM.copying (C:\Program Files\Alcatel OmniVista 2500\data\resourcemanagerv
Mon Jan 23 17:56:02 PST 2006	Resource Manager	Info	RM.copied (C:\Program Files\Alcatel OmniVista 2500\data\resourcemanagerv
Mon Jan 23 17:56:02 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Installing bootrom.bin file
Mon Jan 23 17:56:17 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Completed installing bootrom.bin file
Mon Jan 23 17:56:17 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Removing bootrom.bin file
Mon Jan 23 17:56:17 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Completed Removing bootrom.bin file
Mon Jan 23 17:56:25 PST 2006	Resource Manager	Info	RM.copying (C:\Program Files\Alcatel OmniVista 2500\data\resourcemanagerv
Mon Jan 23 17:56:34 PST 2006	Resource Manager	Info	RM.copied (C:\Program Files\Alcatel OmniVista 2500\data\resourcemanagerv
Mon Jan 23 17:56:34 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Installing miniboot.default file
Mon Jan 23 17:56:51 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Completed installing miniboot.def file
Mon Jan 23 17:56:51 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Removing miniboot.default file
Mon Jan 23 17:56:51 PST 2006	Resource Manager	Info	RM-Device IP = 10.255.211.150-- Completed Removing miniboot.default file

Status messages document the install process.

Note: There is a 10 minute FTP timeout built into OmniVista. If a switch goes down or there is a network interruption during an FTP session, OmniVista will continue to attempt to FTP the file(s) to the switch(es) for 10 minutes. If the FTP session is unsuccessful, OmniVista will return an error message at the end of the 10 minute period.

Viewing Install Entries in the Audit Application

Whenever you install new BMF files, entries are made in the audit log **config.log**. You can view these entries by going to the Audit application and selecting **config.log** under **Current Log Files** in the Tree, as shown below.

Audit Application Entries for Image File Installations

Select config.log under Current Log Files to view Audit application entries for image file installations.

Date	Client	User	Type	Message
Jan 23, 2006 5:56:17 PM	128.251.30.61	admin	Information	Device IP = 10.255.211.150-- Comp
Jan 23, 2006 5:56:17 PM	128.251.30.61	admin	Information	Device IP = 10.255.211.150-- Remc
Jan 23, 2006 5:56:25 PM	128.251.30.61	admin	Information	copying (C:\Program Files\Alcatel O
Jan 23, 2006 5:56:34 PM	128.251.30.61	admin	Information	copied (C:\Program Files\Alcatel Or
Jan 23, 2006 5:56:34 PM	128.251.30.61	admin	Information	Device IP = 10.255.211.150-- Install
Jan 23, 2006 5:56:51 PM	128.251.30.61	admin	Information	Device IP = 10.255.211.150-- Comp
Jan 23, 2006 5:56:51 PM	128.251.30.61	admin	Information	Device IP = 10.255.211.150-- Remc
Jan 23, 2006 5:56:51 PM	128.251.30.61	admin	Information	Device IP = 10.255.211.150-- Comp
Jan 23, 2006 5:56:58 PM	128.251.30.61	admin	Information	copying (C:\Program Files\Alcatel O
Jan 23, 2006 5:57:32 PM	128.251.30.61	admin	Information	copied (C:\Program Files\Alcatel O
Jan 23, 2006 5:57:32 PM	128.251.30.61	admin	Information	Device IP = 10.255.211.150-- Install

Important Facts About BMF File Installations

When performing an installation, BootROM, MiniBoot, and FPGA (BMF) files are FTPed from the OmniVista server to the switch. To gain access to the switch, the FTP user name and password must be known to OmniVista. (You can specify FTP user names and passwords via the Edit Discovery Manager Entry window.) If you did not define FTP login names and passwords via the Edit Discovery Manager Entry window, and you attempt to install BMF files, you will be queried for the FTP login name and password of each individual switch in which the files are being installed. This is described above. If the FTP login name and password are not supplied to OmniVista, the FTP process will return errors and the files will not be installed in the device. The process of installing the files in other switches will continue.

BMF files are installed via FTP, and any errors that can occur when using FTP outside of OmniVista are also possible when using OmniVista.

Note: The TFTP Setting tab in the Preferences window enables you to specify TFTP (Trivial File Transport Protocol) parameters that apply to all FTP file transfers performed from OmniVista. To display the Preferences window, select **Preferences** on the File menu.

If an install operation fails in the middle -- which could occur if a switch goes down between the server and the target switch -- the installation will be only partially completed. The user should check the status messages to determine the files that were actually installed and take any necessary corrective action.

When the install has successfully completed, you are prompted to reload the AOS switches. After the installation completes, you should reload AOS switches using the **Reboot Entire Switch** option in the **Load From Certified** or **Reboot From Certified** command. You can perform these tasks by connecting to the switch from OmniVista's Topology application. (To connect to a switch, merely select it in the Topology application's Tree. Refer to the Topology help for more information.)

Users should not attempt to copy BMF files installed on one machine to another machine. All BMF files should be installed on the desired machines from OmniVista, using the Install Upgrade Software Wizard.

Note: SFTP will be used when a device is configured in OmniVista to use SSH. If a device is configured to use SSH in OmniVista, SSH must be enabled on the device itself.


In-Service Software Upgrade

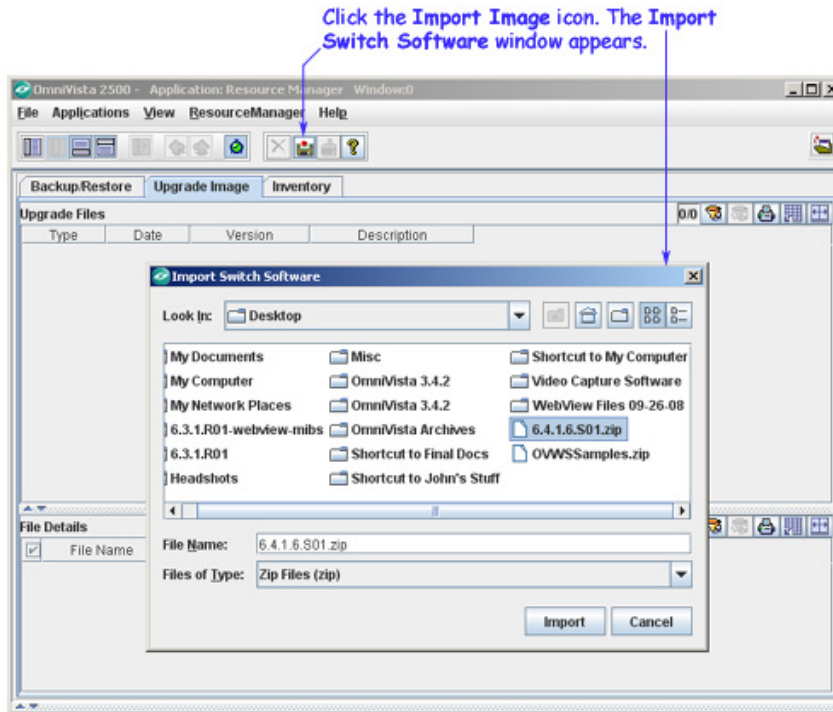
The In-Service Software Upgrade (ISSU) feature is used to upgrade the CMM images running on an OmniSwitch 9000E with minimal disruption to data traffic. The CMM images can be upgraded only on fully synchronized, certified, and redundant systems.

Note: A minimum of 25 MB flash space must be present in the switch to accommodate the image files that are used to upgrade existing image files. This feature is only supported on the OmniSwitch 9000E.

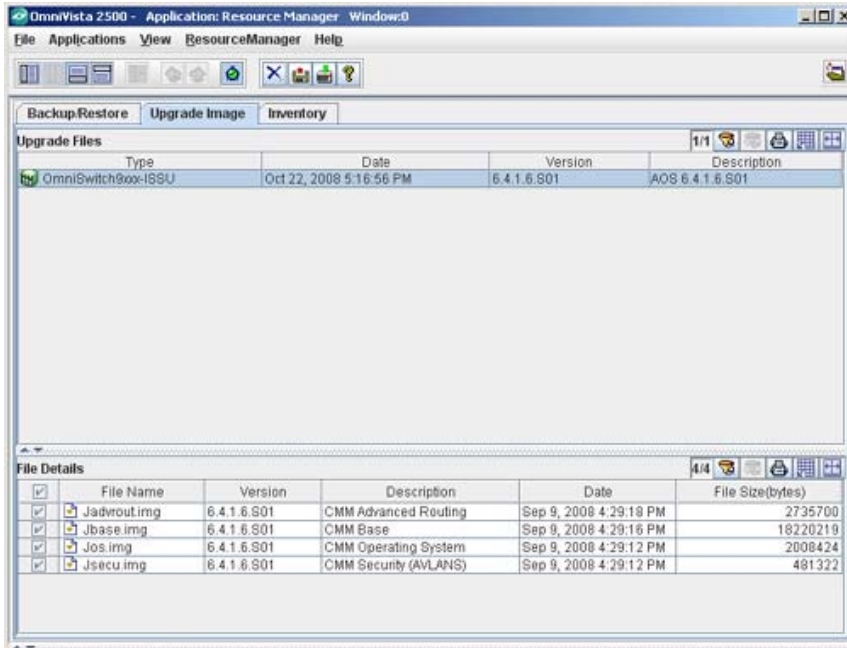
Importing the ISSU Files

Follow the steps below to import the ISSU files.

1. With the Upgrade Image tab displayed, click the Import Image icon , or select **Import** on the Resource Manager menu, or press **Ctrl + I**. The Import Switch Software window is displayed.




2. In the Import Switch Software window, navigate to the location of the zipped ISSU firmware files and select a .zip executable. Then click the **Import** button. The import process begins immediately. Once the ISSU package is imported into Resource Manager, it displays in the Upgrade Files Table as "OmniSwitch9xxx-ISSU", version "6.4.1.*.S0; with the individual files shown in the File Details area.

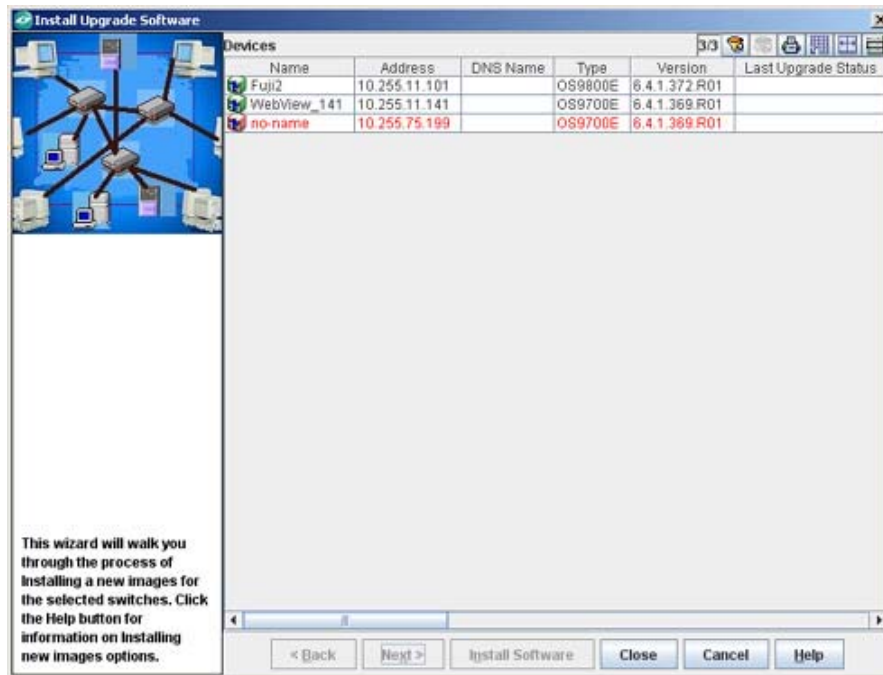


Note: As shown above, the following CMM images are ISSU capable: Jadvrout.img, Jbase.img, Jos.img, Jsecu.img. All of these files are installed in an ISSU upgrade. You cannot select individual files in the File Details area.

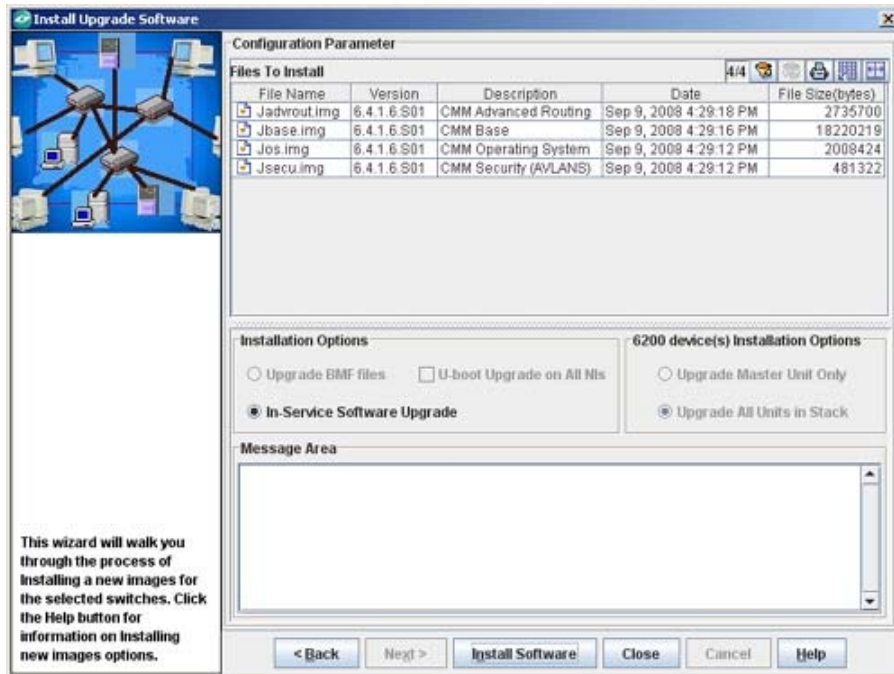
Installing the ISSU Files

Follow the steps below to install the upgrade files.

1. In the "Upgrade Files" window pane, select the desired import. The individual image files contained in the import display in the "File Details" window pane. By default, the "select" checkbox by each image file Only selected files will be installed.
2. Click to deactivate the "select" checkbox by any individual image file that you do NOT want installed.
3. Click the Install New Image Files icon , or select **Install** on the Resource Manager Menu, or press **Ctrl L**. The Install Upgrade Software Wizard opens. The first page of the Wizard lists all devices that qualify for installation of the selected image files. (In this case, only 9000E Series switches are displayed.)



4. Select the device or devices in which you want to install the files. When your selections are complete, click the **Next** button. The **In-Service Software Upgrade** option will be selected.



5. Click the **Install Software** button to begin the installation process immediately.

Prior to FTPing the images to switches, Resource Manager performs the following checks to make sure the selected device is ready for ISSU:

- Ensures the device is redundant, fully certified, and synchronized.
- Ensures that sufficient flash space is available on the primary CMM (a minimum of 25 MB of flash file system space is required for the upgrade).

Note: Although Resource Manager will make certain that the switch is ISSU capable, it will not perform any check whether selected ISSU images are compatible with the particular software version running on the switch. This information will be provided to customers by Customer Support when a new ISSU package is released.

If any of these checks fail for a device, Resource Manager logs the error message, and continues with the next device. Otherwise, Resource Manager checks for the existence of the /flash/issu directory on the primary CMM, and creates the directory if it is not present. If the directory already exists and is not empty, Resource Manager removes all files in the directory before replacing them with the new images.

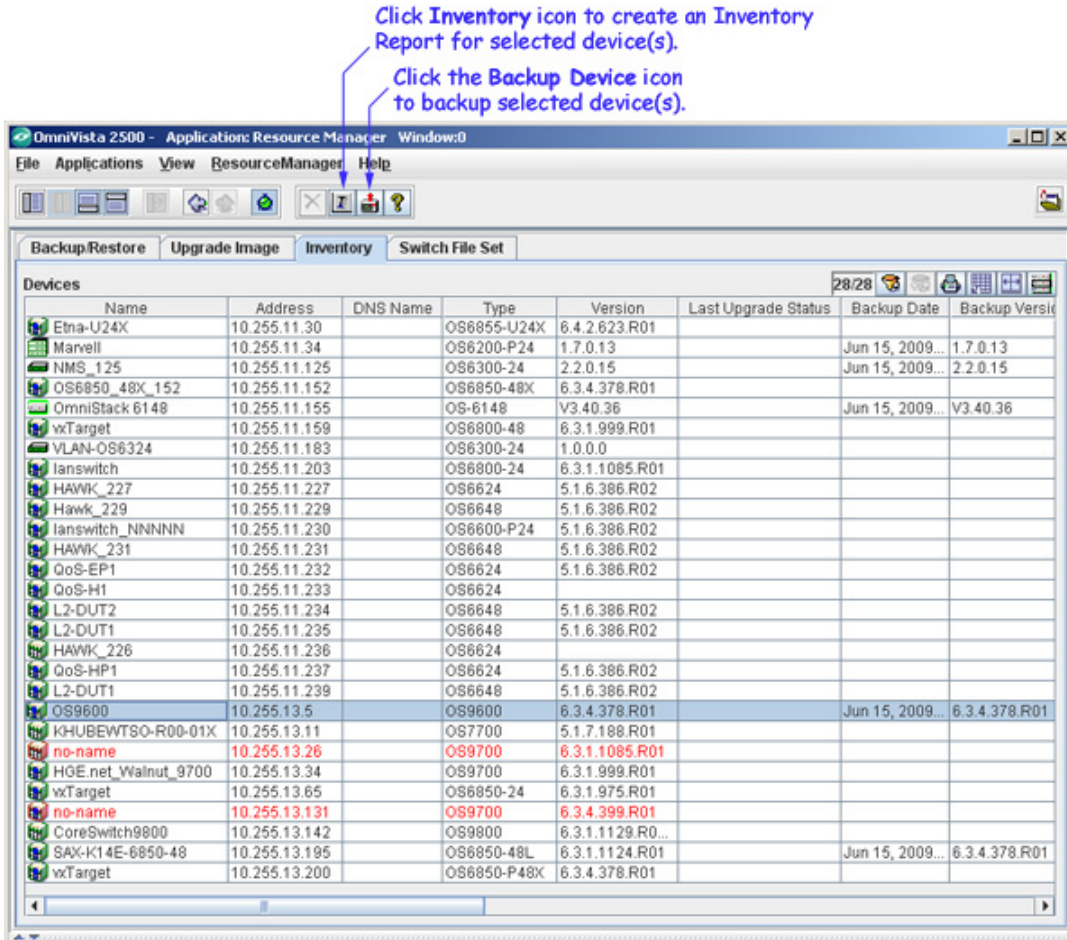
When Resource Manager finishes issuing the ISSU command to the selected switches, the user is asked to perform "Copy Working to Certified" using the Topology application after assessing the integrity of the upgrade software to complete the upgrade process.

Note: The Topology "Copy Working to Certified" function also performs "Flash-Synchro" to sync all the CMMs. If you wish to do this outside of the OmniVista Topology application, make sure you perform: "Copy Working to Certified" followed by "Flash-Synchro".

Using the Inventory Tab

The Inventory tab, shown below, displays a list of the devices known to OmniVista that is possible to inventory and back up. (Note that the list does not include all the devices in the list of All Discovered Devices.) When the Inventory tab is displayed, icons in the Tool bar enable you to quickly access the Inventory window and the Backup Configuration wizard, as explained below.

Note: Inventory support using the Resource Manager application is currently available on OS6200 devices.



Information Fields in the Devices List

As stated, the Inventory tab displays a list of the devices known to OmniVista that is possible to inventory and back up. Although this list does not include all the devices in the list of All Discovered Devices, the information fields displayed for each switch are identical to those displayed in the list of All Discovered Devices. The following section describes the information fields in the Devices table.

Name

The name of the device.

Address

The address of the device.

DNS Name

The DNS name of the device.

Type

The type of the device chassis.

Version

The version number of the device firmware. Version numbers are not displayed for certain non-XOS devices.

Last Upgrade Status

The status of the last firmware upgrade on the switch.

- "Successful" - Successful BMF and Image upgrade performed.
- "Successful (BMF)" - Successful BMF upgrade performed.
- "Successful (Image)" - Successful Image upgrade is performed.
- "Failed (BMF, Image)" - BMF and Image upgrade failed.
- "Failed (BMF)" - BMF upgrade failed.
- "Failed (Image)" - Image upgrade failed.

In all "Failed" cases, "Reload From Working" will be disabled on the switch until a successful upgrade is performed.

Backup Date

The date that the device's configuration and/or image files were last backed-up to the OmniVista server.

Backup Version

The firmware version of the configuration and/or image files that were last backed-up to the OmniVista server

Last Known Up At

The date and time when the last poll was initiated on the device.

Description

A description of the device, usually the vendor name and model.

Status

This field displays the operational status of the device. It displays **Up** if the device is up and responding to polls. (When a device is up, it displays green in both the List of All Discovered Devices and the tree.) It displays **Down** if the device is down and not responding to polls. (When a device is down, it displays red in both the List of All Discovered Devices and the tree.) This field displays **Warning** if the switch has sent at least one warning or critical trap and is thus in the warning state. (When a device is in the warning state, it displays orange in both the List of All Discovered Devices and the tree.)

Traps

This field indicates the status of trap configuration for the device. **On** means that traps are enabled. **Off** means that traps are disabled. **Not Configurable** means that traps for this device are not configurable from OmniVista. (Note that traps may have been configured for such devices outside of OmniVista.) **Unknown** means that OmniVista does not know the status of trap configuration on this switch. OmniVista will read the switch's trap configuration when traps are configured for the switch via the Configure Traps Wizard.

Seen By

This field lists the Security Groups that are allowed to view the device. (The Security Groups that are allowed to view a device can be defined when devices are autodiscovered, added manually, or edited.) The default Security Groups shipped with OmniVista are as follows:

- **Default** group. This group has read-only access to switches in the list of All Discovered Devices that are configured to grant access to this group.
- **Writers** group. This group has both read and write access to switches in the list of All Discovered Devices that are configured to grant access to this group. However, members of this group cannot run autodiscovery nor can they manually add, delete, or modify entries in the list of All Discovered Devices.
- **Network Administrators** group. This group has full administrative access rights to all switches on the network. Members of this group can run autodiscovery and can manually add, delete, and modify entries in the list of All Discovered Devices. Members of this group also have full read and right access to entries in the Audit application and the Control Panel application. Members of this group can do everything EXCEPT make changes to Security Groups.
- **Administrators** group. This group has all administrative access rights granted to the Network Administrators group AND full administrative rights to make changes to Security Groups.

Note that other Security Group names may display in this field if custom Security Groups were created. Refer to help for the Security application *Users and Groups* for further information on Security Groups.

Running From

For AOS devices, this field indicates whether the switch is running from the **certified** directory or from the **working** directory. This field is blank for all other devices. For AOS devices, the directory structure that stores the switch's image and configuration files in flash memory is divided into two parts:

- The certified directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory. (Note that you can specifically command a switch to reboot from either directory.)
- The working directory contains files that may or may not have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes


Note that the files in the certified directory and in the working directory may be different from the running configuration of the switch, which is contained in RAM. The running configuration is the current operating parameters of the switch, which are originally loaded from the certified or working directory but may have been modified through CLI commands, WebView commands, or OmniVista. Modifications made to the running configuration must be saved to the working directory (or lost). The working directory can then be copied to the certified directory if and when desired.

Changes

For AOS devices, this field indicates the state of changes made to the switch's configuration. This field is blank for all other devices. This field can display the following values:

- **Unsaved.** Changes have been made to the running configuration of the switch that have not been saved to the working directory.
- **Uncertified.** Changes have been saved to the working directory, but the working directory hasn't been copied to the certified directory. The working directory and the certified directory are thus different.
- **Blank.** When this field is blank for an AOS device, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.

OmniVista is now capable of tracking AOS configuration changes made through CLI commands or WebView, and so will reflect configuration changes made outside of OmniVista through these two interfaces in the Changes field. Information in the Changes field will be accurate as long as OmniVista has polled the switch since the last change was made (through any interface).

Note that it is possible a switch could be in a state where it is both Unsaved and Uncertified. In this situation **Unsaved** displays in the Changes field. Whenever an AOS device is in the Unsaved or Uncertified state, a blue exclamation mark displays on its icon ().


Discovered

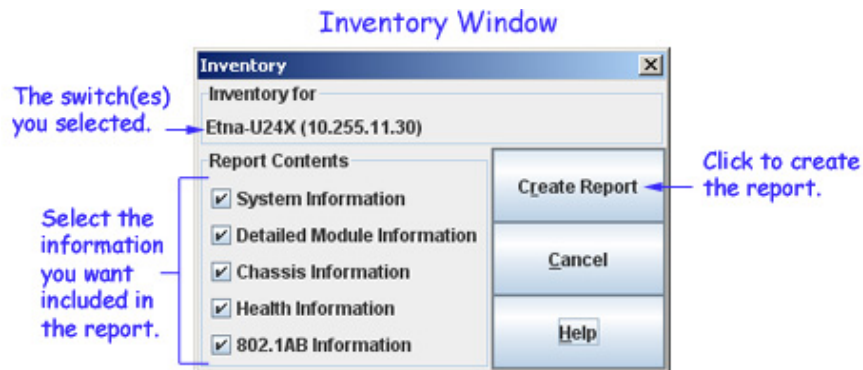
This field displays the date and time when OmniVista successfully pings or polls the switch for the first time. This value remains unchanged until the switch entry is deleted. This field will remain blank if OmniVista does not ping or poll the switch at all.

Creating an Inventory Report


A Switch Inventory Report includes system information, detailed module information, chassis data, and health information for an individual switch. You can request an Inventory Report for a single switch or for multiple switches simultaneously. To Create an Inventory Report, follow the steps below.

Note: Refer to the Inventory help to view a sample Inventory Report and information on the fields in Inventory Reports.

1. With the Inventory tab displayed, select the switches for which you want to generate an Inventory Report. To select a single switch, merely click on it. **Shift**-click to select multiple contiguous switches. **Ctrl**-click to select multiple noncontiguous switches.
2. Click the Inventory icon , or select **Inventory** on the Resource Manager Menu, or press **Ctrl I**. The Inventory window displays. The switches that you selected in step 1 are listed at the top of the window.
3. Click "Report Contents" checkboxes (shown below) to specify the types of information that you want included in the Inventory Report.
4. Click **Create Report** to create the report.



Initiating a Backup from the Inventory Tab

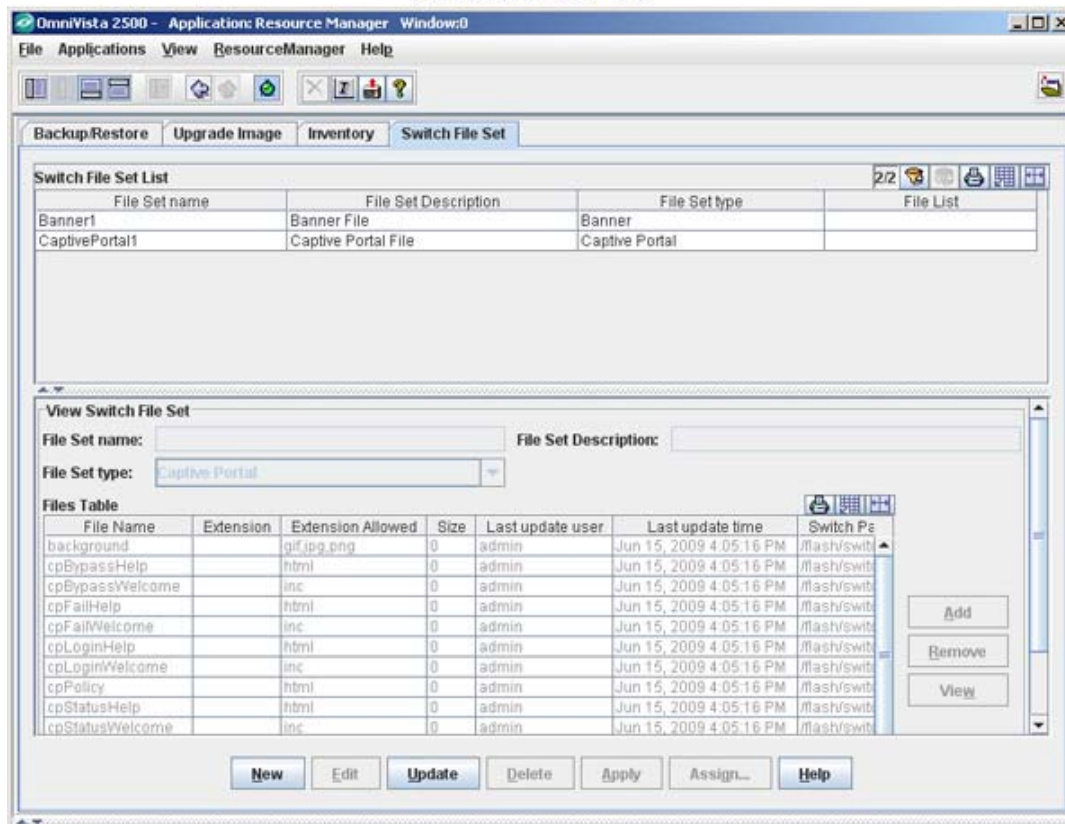
1. With the Inventory tab displayed, select the switches that you want to back up. To select a single switch, merely click on it. **Shift**-click to select multiple contiguous switches. **Ctrl**-click to select multiple noncontiguous switches.
2. Click the Backup Device icon , or select **Backup** on the Resource Manager Menu, or press **Ctrl B**. The Backup Configuration wizard displays. The wizard opens at Page Two. (Page One of the Wizard enables you to select the switches to backup, but in this case you have already selected the switches.) Page Two of the Backup Configuration wizard enables you to perform the backup and monitor its progress.

Using the Switch File Set Tab

The Switch File Set Tab is used to "push" a command prompt Login Banner and/or Captive Portal Web Page files to devices on the network. Banner files can be customized to display a unique command line banner for all devices on the network. Captive Portal, a web-based user authentication option within the Access Guardian application, presents the user with a web page for authentication. These web pages can also be customized by the user.

Note: Before "pushing" Banner or Captive Portal files to all devices in the network, it is recommended that you customize the file(s) and send the file(s) to a single switch on the network for verification. When you are satisfied with the customized file(s), you can then push the files to the network. Any subsequent changes to the files can be made on that same switch, and the new files imported and pushed to the network.

Switch File Set Tab



A list of the possible Banner file name and Captive Portal file names are displayed in the **Files Table** at the bottom of the page. These will be the Banner files and Captive Portal Web files (e.g., Login Page, Help Pages) that you will customize for your network. The files you create must use these file names. For example, if you create a Captive Portal Login Page, the file must be named *cpLoginWelcome.inc*. Once you have created all of the necessary files and verified them on a network device, you can then import those files from that device and "push" them to other devices on the network. The file names and their use are described below.

- **banner.txt** - A Banner file is a .txt file that is displayed when a user first logs into a network device using the command line interface.
- **background.gif/.jpg/.png** - Use this file to provide a page background image that Captive Portal will display on all pages.
- **cpLoginHelp.html** - Use this file to customize the Captive Portal login help page. A question-mark ("?") button links to this HTML help page, which is displayed in a separate browser window.
- **cpLoginWelcome/cpStatusWelcome/ cpFailWelcome/cpBypassWelcome.inc** - Use these files to customize the welcome message for the Captive Portal login, successful status, fail status, and bypass status page.
- **cpPolicy.html** - The User Acceptable Policy HTML file that is linked to the Captive Portal login page. The link provided opens a new browser window to display the policy information.
- **logo.gif/.jpg/.png** - Use these files to provide a company logo that Captive Portal will display on all pages.

Note: Create custom logo and background pages using the .gif, .jpg, or .png formats. Captive Portal checks the flash/switch directory on the switch for a .gif file, then a .jpg file, and finally a .png file. Whichever file type Captive Portal encounters first is the file used to display the custom logo or background.

The .inc files, which are used to present customized welcome messages, are partial HTML files that can include only text or text and other HTML tags, such as links. Note that these .inc files are wrapped in a paragraph HTML tag within the body of a Captive Portal default page.

Banner Files

A Banner file is a .txt file that is displayed when a user first logs into a network device using the command line interface (e.g., a company name, device name). You must first create the file, then assign ("push") the file to devices on the network.

Captive Portal Files

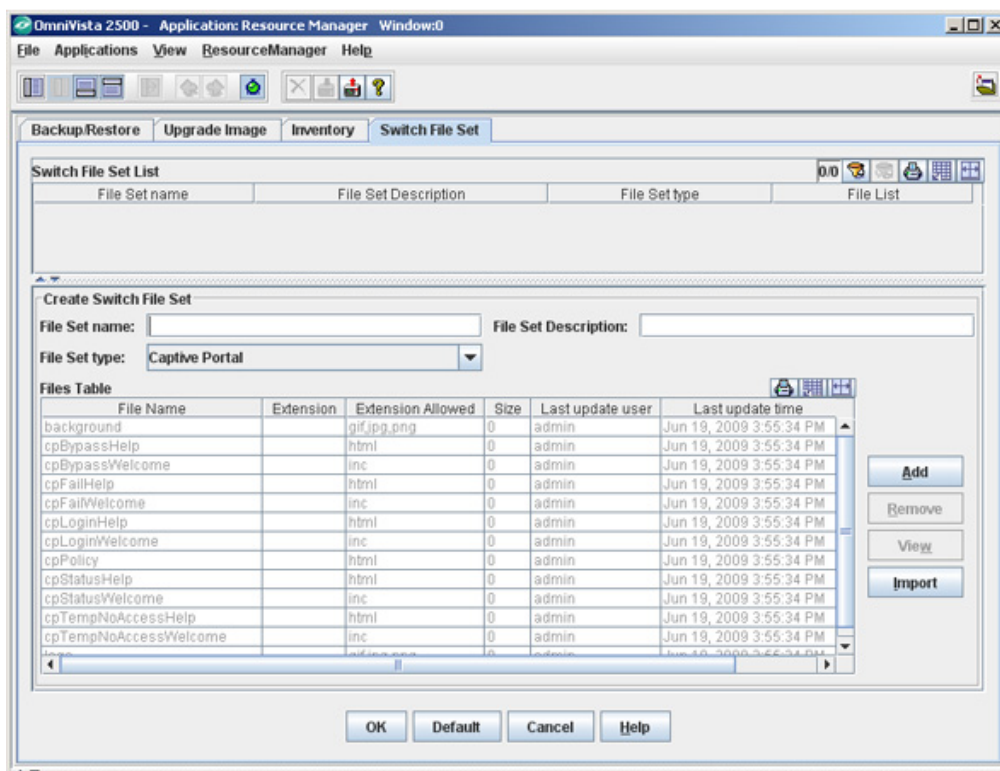
Captive Portal is a configurable option within the Access Guardian application that allows web-based clients to authenticate through switch using 802.1x or MAC authentication via a RADIUS Server. When the Captive Portal option is invoked, a Web page is presented to the user device to prompt the user to enter login credentials.

Creating a File

Follow the steps below to create a new Banner file.

1. Click on the **New** button. The "Create Switch File Set" pane is activated.

Creating a Switch File Set



2. Enter a **File Set Name** and **File Set Description**.
3. Click the **OK** button, then click **Apply**.
4. You can also add a file from your desktop by clicking on the **Add** button and locating and saving the file. You must rename the file to correspond to one of the pre-configured file names listed in the files table.
5. When you have created the file(s), you can push (assign) the files to devices on the network.

Note: You can also import files from a device on the network to your server, the push (assign) them to other devices on the network.

Importing Files

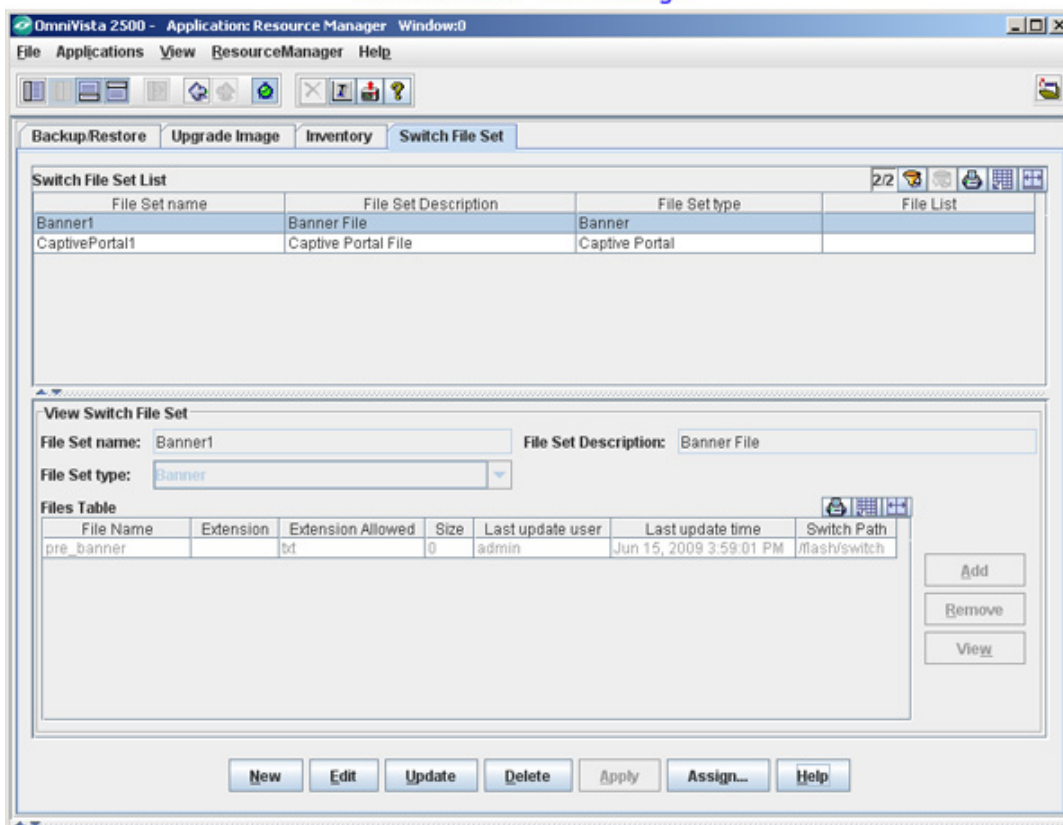
You can also create files by importing them from other switches on the network. Enter a name for the file set in the "File Set Name" field and a description in the "File Set Description" field. Click the **Import** button and select a switch with the files you want to import. The file set will appear in the "Switch File Set List".

Assigning a File

Follow the steps below to send the Captive Portal files to a switch or set of switches.

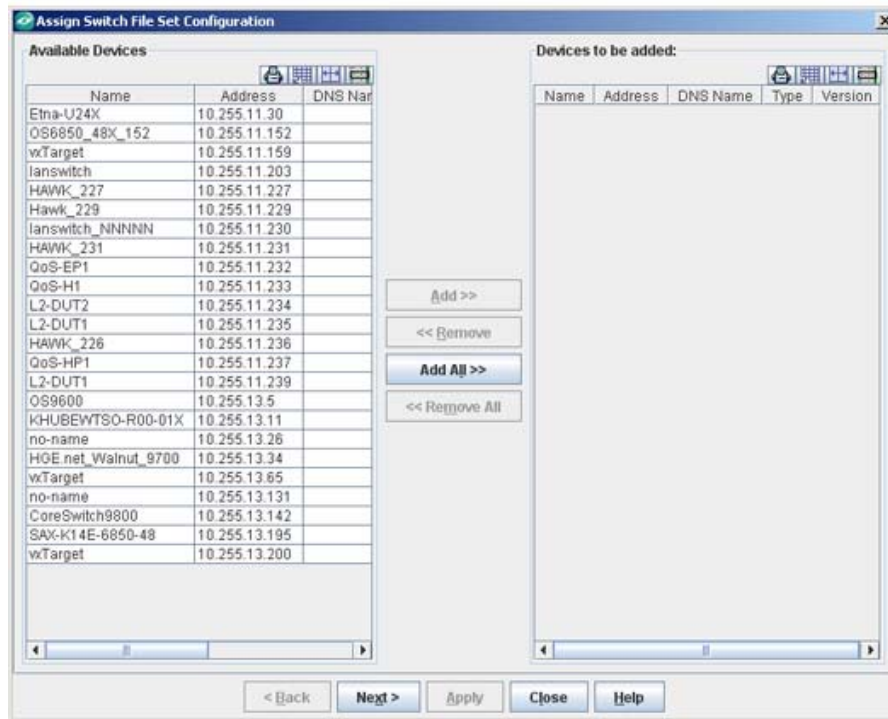
1. Select the file set you want to assign from the Switch File Set List".

Switch Fileset Tab - Assign



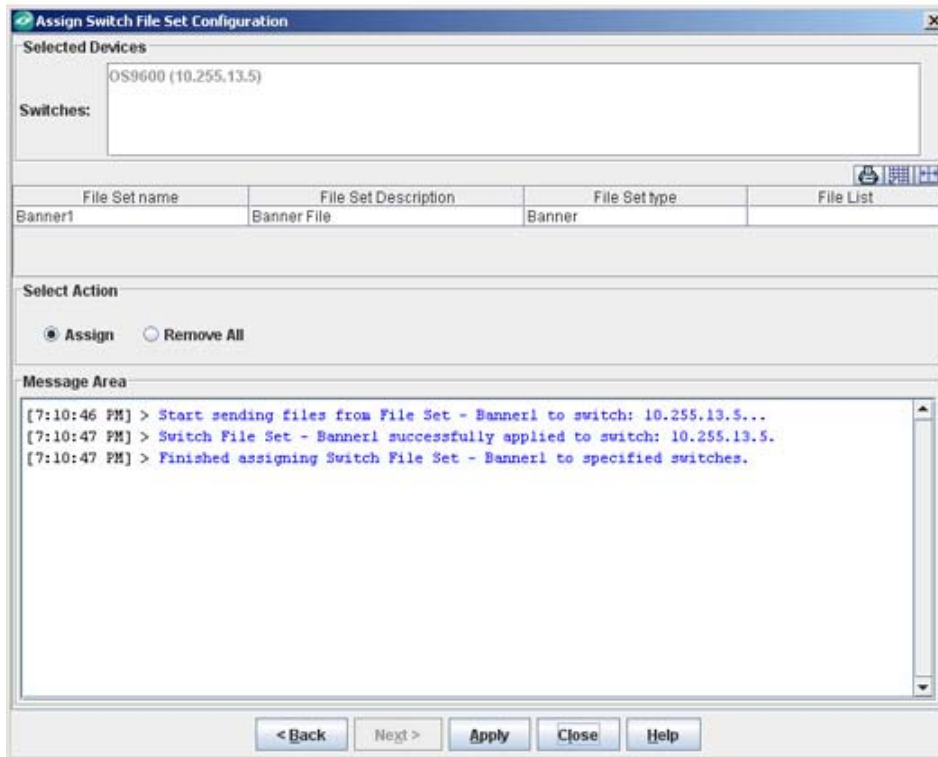
2. Click the **Assign** button. Page 1 of the "Assign File Set" Wizard appears.

Assign Fileset Wizard - Page 1



3. Select the switch(es) to which you want to send the file set and click the **Next** button. Page 2 of the "Assign File Set" Wizard appears.

Assign Fileset Wizard - Page 2



4. Click the **Apply** button to send the files to the switch(es).