Getting Started with Telnet

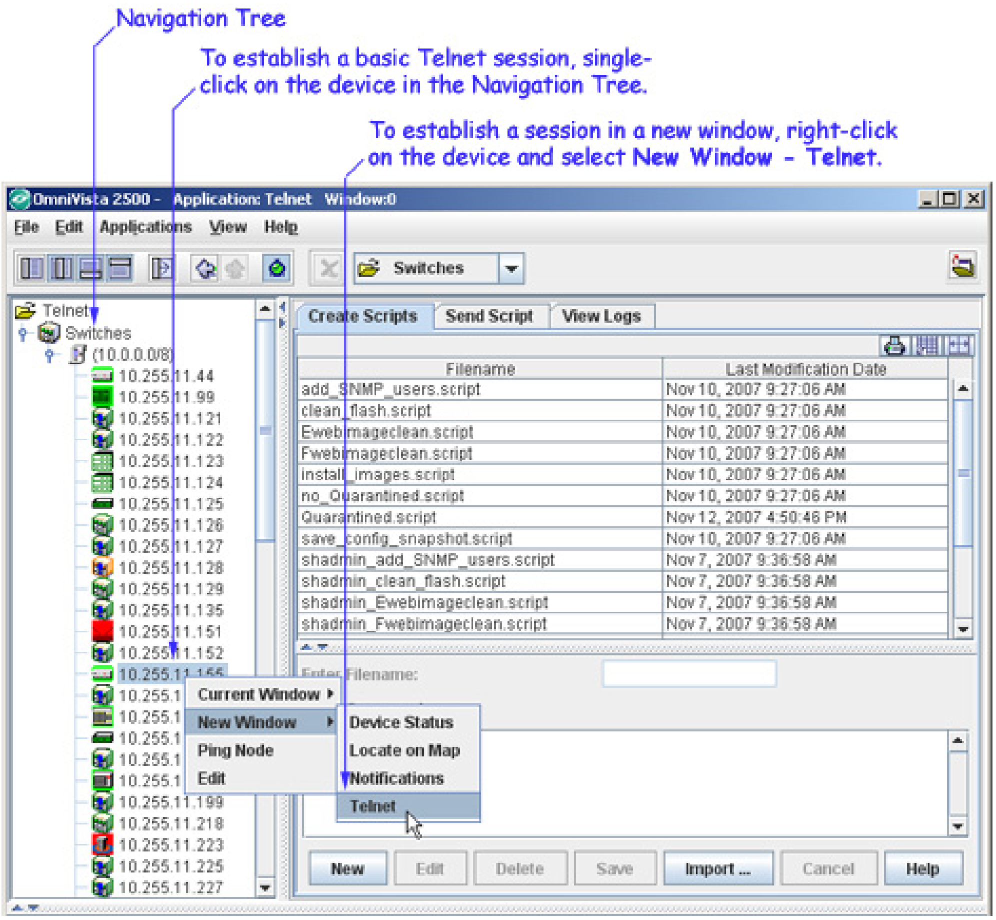
From the Telnet application window, two main Telnet functions can be accessed:

- **Establishing Telnet Sessions -** Establishing and managing Telnet sessions involves logging in to one or more devices and configuring the devices via supported CLI commands. Note that OmniVista Telnet also supports SSHv2 enhanced Telnet encryption.
- **Telnet Scripting -** Creating Telnet Scripting files involves manually creating a text-based script file within OmniVista and then configuring one or more devices by applying the file via Telnet. Users can also import existing text-based script files.

Establishing a Telnet Session

To establish a basic Telnet session with a device, begin by clicking open the **Switches** directory in the Navigation Tree. One or more **Subnet** directories displays in the Tree. Click open the applicable **Subnet** directory, then single-click on the icon or IP address of the desired device. A Telnet session for the device launches automatically.

To establish a basic Telnet session in a *new window*, right-click a device's icon or IP address in the Tree and select **New Window -> Telnet**. A new instance of OmniVista is opened and a Telnet session to the corresponding device is launched.



Filename	Last Modification Date
add_SNMP_users.script	Nov 10, 2007 9:27:06 AM
clean_flash.script	Nov 10, 2007 9:27:06 AM
Ewebimageclean.script	Nov 10, 2007 9:27:06 AM
Fwebimageclean.script	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM

> **Note:** If SSH has been configured as the preferred encryption type, the term **SSH** will be used in the place of **Telnet** in OmniVista's pop-up menus, application buttons, etc.

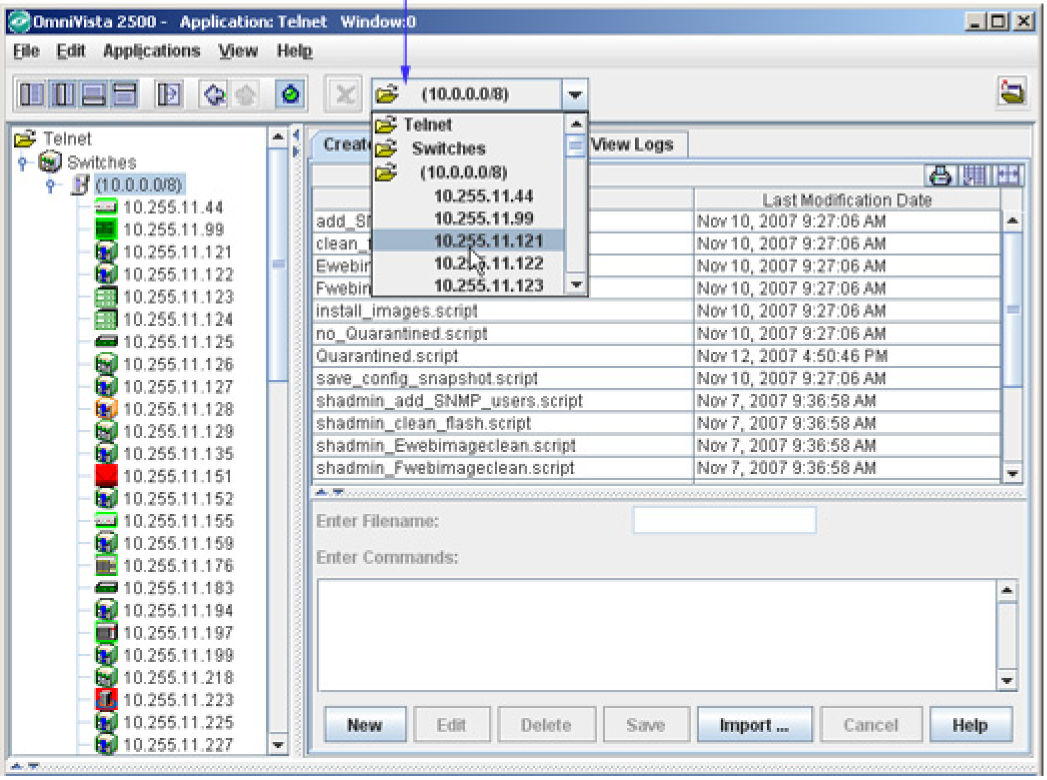
If Automatic Login has not been configured for the device, enter the login ID and password for the device in the Telnet window. If Automatic Login has been configured, OmniVista will enter the login ID and password automatically.

After login is complete, the CLI command prompt displays. A successful Telnet session has been established and the device is now ready to be managed and/or configured via the CLI.

Launching Telnet Sessions Using the Pull-Down Navigation Menu

Telnet sessions can also be launched from the pull-down menu located at the top of the main Telnet window. However, be sure that a particular subnet has first been selected in the Navigation Tree. When a subnet is selected, the pulldown menu lists all discovered devices in that subnet. Simply scroll and click to select a device from the menu; a Telnet session for the device launches automatically.

Telnet sessions can also be launched by selecting devices from this pull-down menu. Be sure that a subnet directory is highlighted in the Navigation Tree, then scroll and click to select a device. The session launches automatically.

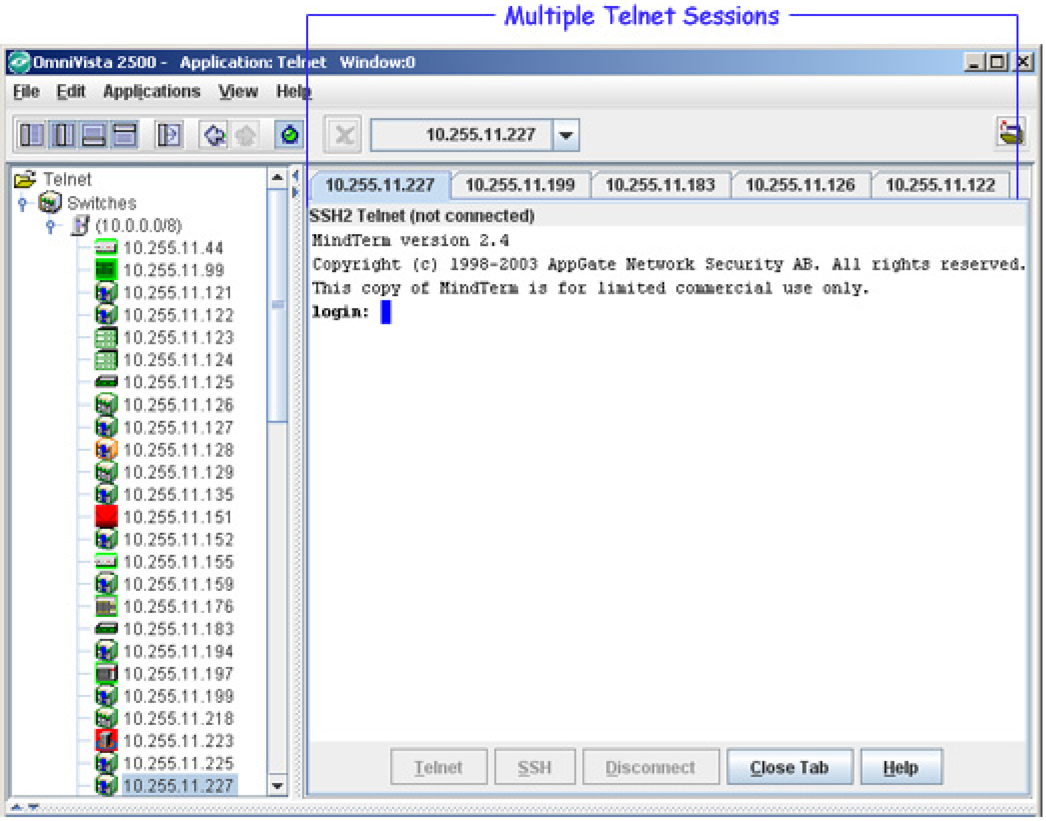


	Last Modification Date
add_Sl	Nov 10, 2007 9:27:06 AM
clean_	Nov 10, 2007 9:27:06 AM
Ewebir	Nov 10, 2007 9:27:06 AM
Fwebir	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM

> **Note:** Unlike the Navigation Tree, the pull-down navigation menu does not show additional status information, such as a device's type or whether it is reachable.

Managing Multiple Telnet Sessions

Multiple sessions can be launched and managed within the same instance of the Telnet application. To establish multiple Telnet sessions, simply select multiple devices, one at a time, from the Navigation Tree. A new tab displays for each session, with each tab indicating the IP address for its corresponding session.


Multiple Telnet Sessions

```
SSH2 Telnet (not connected)
MindTerm version 2.4
Copyright (c) 1998-2003 AppGate Network Security AB. All rights reserved.
This copy of MindTerm is for limited commercial use only.
login:
```

To access a particular Telnet session, click on the tab showing the device's IP address. The corresponding Telnet window displays.

Note: Multiple Telnet sessions can also be launched from the pull-down menu located at the top of the OmniVista window. Scroll and click to select devices from the pull-down menu; a Telnet session for each device launches automatically and a new tab for each session displays.

Closing Telnet Sessions

To close a Telnet session, click the **Disconnect** button at the bottom of the Telnet window or type **exit** at the command prompt.

If multiple sessions are being managed, clicking the **Close Tab** button disconnects a session and also closes its corresponding tab. (Note that the **Close Tab** button is not available if only one Telnet session is open.)

Reestablishing Closed Sessions

When a session has been disconnected, it can be quickly reconnected by clicking the **Telnet** button at the bottom of the Telnet window. If multiple sessions are being managed, be sure that the tab for the desired device is selected before clicking the **Telnet** button. Otherwise, sessions can be reestablished by following the steps described in "Establishing a Telnet Session" on page 1 and "Managing Multiple Telnet Sessions" on page 3.

Returning to the Main Telnet Window

To return to the main Telnet window (i.e., the window displayed when the Telnet application was first launched), single-click the **Switches** directory in the Navigation Tree. The main Telnet window, showing the **Create Scripts**, **Send Script**, and **View Logs** tabs displays.

Using Telnet Scripting

A Telnet script file is a text-based file used to configure one or more devices through OmniVista's Telnet Scripting feature. Telnet scripting is especially useful in applying batch updates or common configurations across multiple devices. A script file must contain only CLI commands supported on AOS switches. When a script file is applied, each CLI command in the file is sent to the device via Telnet.

> **Important Note:** Before attempting to apply a script, OmniVista must know the user name and password for each device being configured. Use Auto-Login to specify the login information.

Users are not required to create script files using a third-party text editor. OmniVista provides a text box where CLI commands can be manually entered from the Telnet application. During the Telnet Scripting steps, these commands are saved to a script file (which can be accessed for reference or future applications).

Creating Script Files

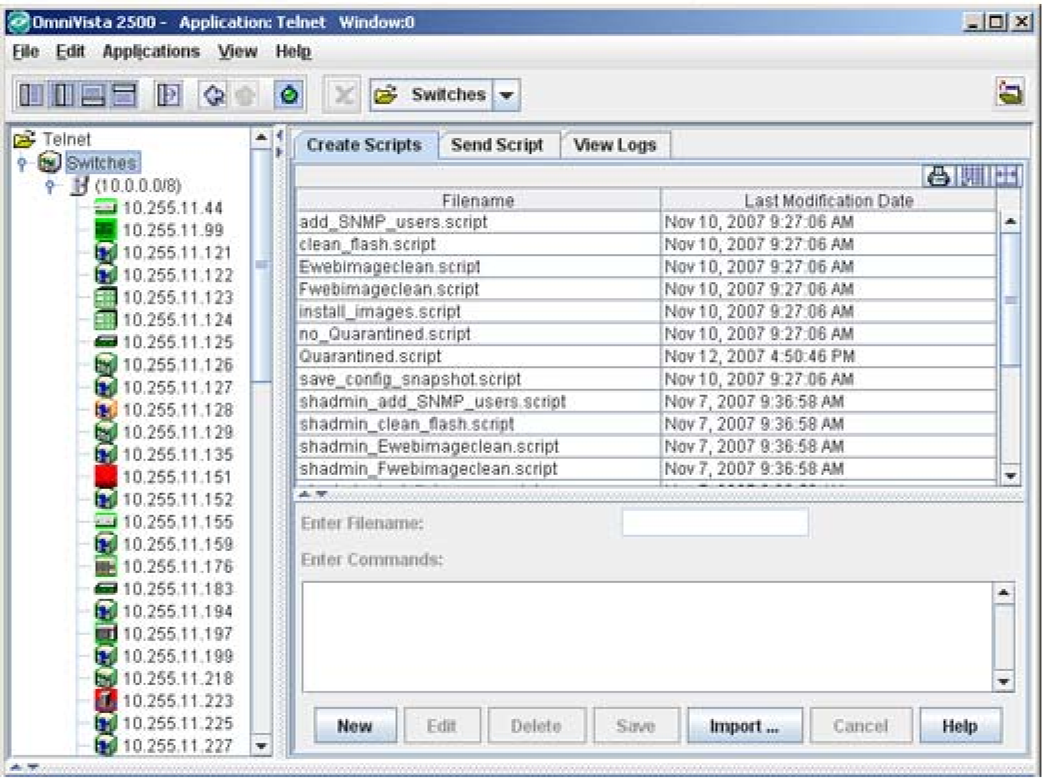
To create a script, click the **New** button. Enter a descriptive file name in the **Enter Filename** text field. For example, **new_vlan_config1**. (The file extension **.script** will be added automatically when the script file is saved.)

Press the **Tab** key or select the **Enter Commands** text box and enter the commands to be applied to the switch via this script. Enter on command per line. The script can be a combination of both CLI commands and JavaScript.

> **Note:** Use of JavaScript requires Java 1.6.
>
> **Important Note:** Operational commands that automatically issue a confirmation prompt and require the user to type a response (like Y or N) are not supported in CLI script files. Examples include **takeover**, **reload**, **fsck**, etc. Do not attempt to include these command types in the script file. Instead, manually issue them via the standard CLI command line prompt. These operations can also be issued on a device-by-device basis via WebView or OmniVista.

Verify that the syntax of all commands is correct before proceeding. When finished, click the **Save** button.

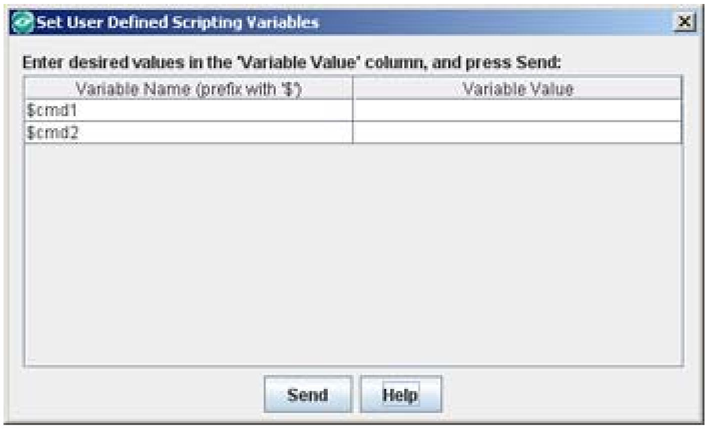
Pre-Configured Telnet Scripts



Filename	Last Modification Date
add_SNMP_users.script	Nov 10, 2007 9:27:06 AM
clean_flash.script	Nov 10, 2007 9:27:06 AM
Ewebimageclean.script	Nov 10, 2007 9:27:06 AM
Fwebimageclean.script	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM

User Defined Variables

If you have specified variables within the script, the **Set User Defined Scripting Variables** window is displayed when you click on the **Send Script** button. Click in the "Variable Value" field next to the variable and enter value to be used, then click **Send**.



Enter desired values in the 'Variable Value' column, and press Send:

Variable Name (prefix with '$')	Variable Value
$cmd1	
$cmd2	

Variables must be prefixed with '$' to show they are variables. The built-in variables are:

- **$IP_ADDRESS** - replaced automatically with target switch IP address.
- **$BOOT_DIR** - replaced automatically with target boot directory (ex: working).
- **$BASE_MAC** - replaced automatically with target base MAC address.
- **$CHASSIS_TYPE** - replaced automatically with target chassis type.
- **$SYSTEM_OID** - replaced automatically with target unique object ID.

- **$LOGIN_ID** - replaced automatically with target FTP/Telnet login ID.
- **$LOGIN_PWD** - replaced automatically with target FTP/Telnet login password.
- **$READ_PWD** - replaced automatically with target community string for SNMP reading.
- **$WRITE_PWD** - replaced automatically with target community string for SNMP writing.

Importing Existing Script Files

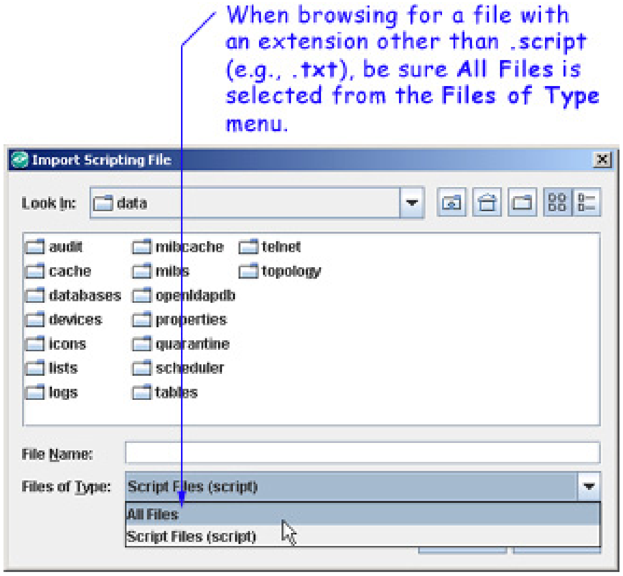
Although OmniVista allows users to manually create script files within the Telnet application, existing script files can also be imported. In other words, a file containing a set of CLI commands can be accessed from a server or local drive and then applied to one or more devices. This allows users to maintain a library of network configurations and then apply them to devices in their network as needed.

Before importing a file to one or more devices, consider the following important guidelines:

- Any script file being imported must be text-based (ASCII).
- Although file extensions such as **.txt** and **.ascii** are supported, the file extension **.script** is recommended.
- All CLI commands contained in the file must be AOS-supported. Also, operational commands that automatically issue a confirmation prompt and require the user to type a response (like Y or N) are not supported in CLI script files. Examples include **takeover**, **reload**, **fsck**, etc.
- CLI commands must also be entered into the text file *one command per line*.
- Only one script file can be imported at a time.

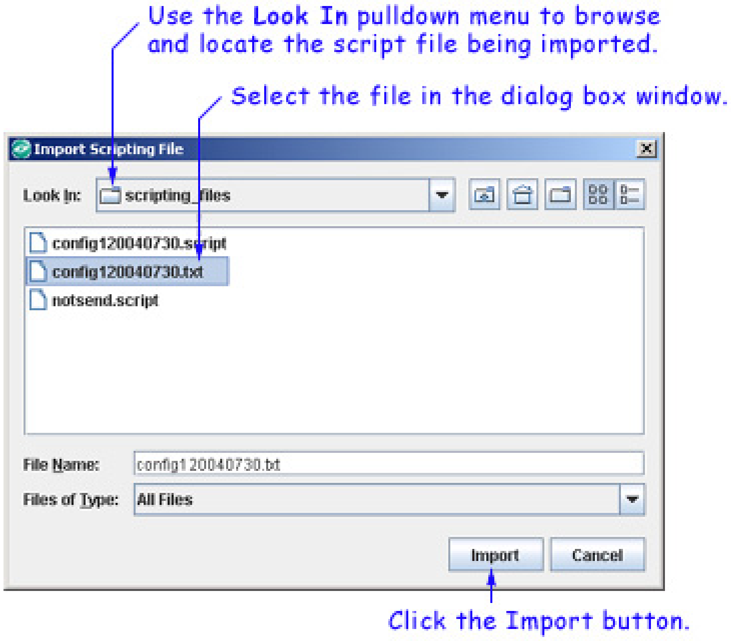
To import a script file, click the **Import** button at the bottom of the main Telnet window. The **Import Scripting File** dialog box displays. Use the dialog box's **Look In** pull-down menu to locate the file being imported.

> **Note:** If you are browsing for a file with an extension other than **.script**, be sure to select **Files of Type -> All Files** in the dialog box, as shown:



When browsing for a file with an extension other than .script (e.g., .txt), be sure All Files is selected from the Files of Type menu.

Once the script file has been located, select the file in the dialog box window; the file name displays in the **File Name** text field. Click the **Import** button.



Use the Look In pulldown menu to browse and locate the script file being imported.

Select the file in the dialog box window.

Click the Import button.

Import Scripting File

Look In: scripting_files

config120040730.script
config120040730.txt
notsend.script

File Name: config120040730.txt

Files of Type: All Files

Important Note: The script import procedure is *not* complete at this point. You must click on the **Send Script** tab in the main Telnet window and follow the remaining steps in order to send the script file to the device(s).

Editing Script Files

To edit a script file, select the file from the **Filename** list, then click **Edit**. The **Enter Scripts** text box (which was previously grayed out) becomes active. The CLI commands contained in the selected script file can now be deleted, modified, or appended. When the changes are complete, click the **Save** button.

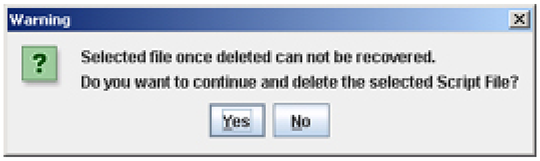
Important Note: When the changes are saved, the previous contents of the script file are overwritten. To preserve the original contents of the file, be sure to make a backup copy before editing.

Deleting Script Files

To delete a script file, select the file from the **Filename** list, then click **Delete**.

Note: When a file is deleted, it is permanently removed from the **scripting_files** directory. Once a script file is deleted, it cannot be recovered.

Click **Yes** in the **Warning** dialog box.



Warning

Selected file once deleted can not be recovered.
Do you want to continue and delete the selected Script File?

Deleting Multiple Script Files

Multiple log files can be deleted at once. To delete multiple script files, simply Control-click or Shift-click all applicable files in the list before clicking **Delete**. Remember, however, that once the files have been deleted, they cannot be recovered.

Using the OmniVista Telnet Application

OmniVista's Telnet application provides a feature set well beyond that of standard Telnet session support. Features include:

- Telnet support
- Automatic login for one or more devices
- Multiple Telnet session management
- Telnet Script file support for one or more AOS devices
- Secure Shell (SSHv2) support.

Opening the Telnet Application

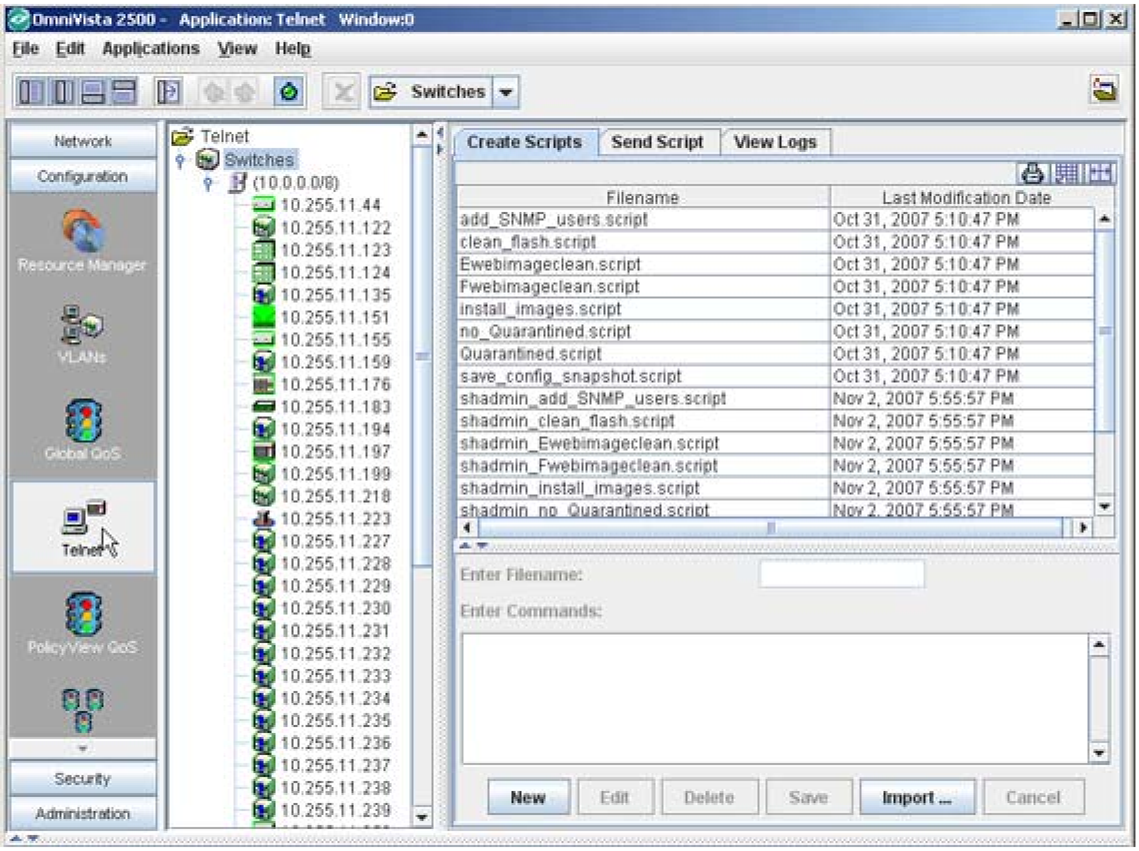
There are two different ways to open the Telnet application. Telnet can either be accessed from OmniVista's Task Bar, or from within another open OmniVista application, such as Topology, VLANs, etc.

When the Task Bar is used, the main Telnet window is displayed. Sessions are not automatically launched; instead, the user can choose a particular Telnet feature (e.g., Telnet Scripting) and launch sessions to one or more devices as needed.

When Telnet is accessed from another open OmniVista application, a Telnet session with the selected device launches automatically.

Opening Telnet from the Task Bar

To open the Telnet application from the Task Bar, click the **Configuration** group button, then click the **Telnet** button.



Filename	Last Modification Date
add_SNMP_users.script	Oct 31, 2007 5:10:47 PM
clean_flash.script	Oct 31, 2007 5:10:47 PM
Ewebimageclean.script	Oct 31, 2007 5:10:47 PM
Fwebimageclean.script	Oct 31, 2007 5:10:47 PM
install_images.script	Oct 31, 2007 5:10:47 PM
no_Quarantined.script	Oct 31, 2007 5:10:47 PM
Quarantined.script	Oct 31, 2007 5:10:47 PM
save_config_snapshot.script	Oct 31, 2007 5:10:47 PM
shadmin_add_SNMP_users.script	Nov 2, 2007 5:55:57 PM
shadmin_clean_flash.script	Nov 2, 2007 5:55:57 PM
shadmin_Ewebimageclean.script	Nov 2, 2007 5:55:57 PM
shadmin_Fwebimageclean.script	Nov 2, 2007 5:55:57 PM
shadmin_install_images.script	Nov 2, 2007 5:55:57 PM
shadmin_no_Quarantined.script	Nov 2, 2007 5:55:57 PM

The main Telnet window allows users to access the two main Telnet functions:

- Establishing and Managing Telnet Sessions
- Creating or Importing Telnet Scripting Files

For more information on these functions, refer to the Getting Started with Telnet section.

Opening Telnet from Other Applications

Telnet sessions can also be launched from other OmniVista applications by right-clicking devices in the Navigation tree. For example, from the **VLANs** application, right-click on a device listed in the tree and select **Current Window -> Telnet** or **New Window -> Telnet** from the popup menu. Telnet will be opened directly from VLANs and a session to the selected device will launch.

Note that launching a Telnet session in a new window allows users to preserve the current view in an open OmniVista application. So, for example, if a user is viewing detailed configuration information using the VLANs application and a Telnet session is needed for a quick configuration change, launching the session in a new window may be preferred.

Navigating Telnet

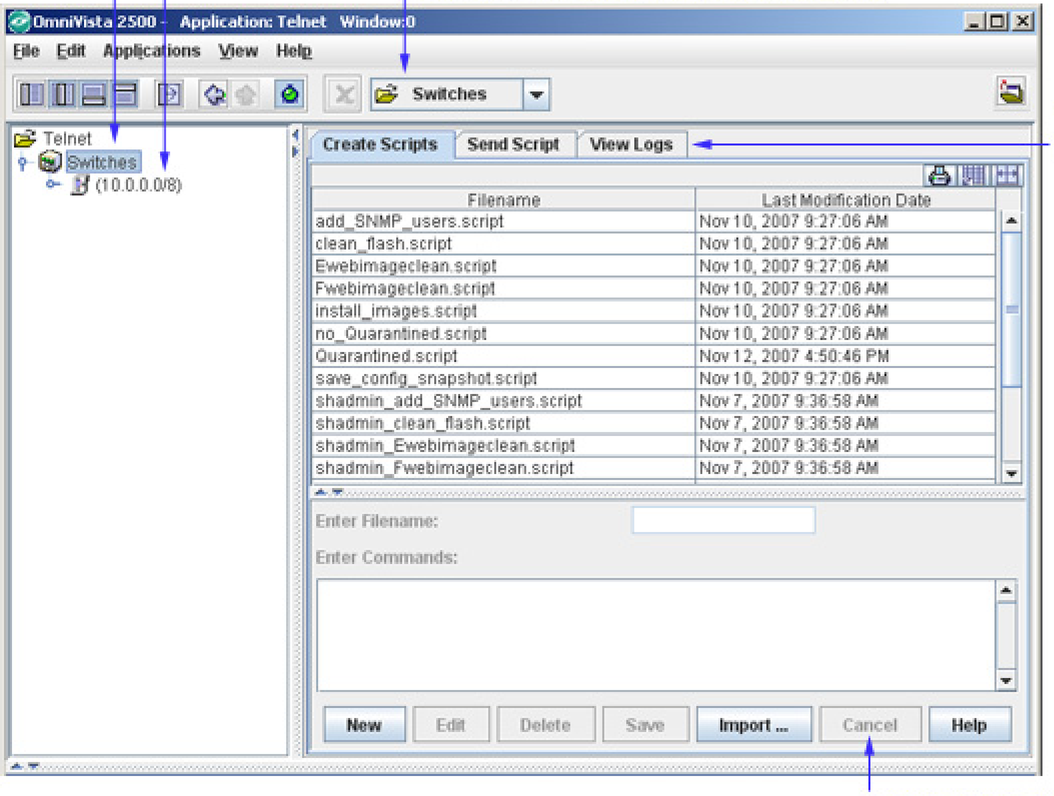
The screen below shows key navigation components of the Telnet application. The left side of the main Telnet window lists all discovered devices. To establish a telnet session, expand the tree and select a device. The tabs on the right side of the screen are used to configure, apply, and view telnet scripts.

- Create Scripts - A Telnet script file is a text-based file used to configure one or more devices through OmniVista's Telnet scripting feature. You can create new telnet scripts or import existing scripts.
- Send Scripts - Once you have created a script, you must send that script to a device or devices.
- View Logs - Log files are created when you send a script to a device or devices. You can view the log file by clicking on the View Logs tab and selecting the file.

To access the main Telnet window (shown), which provides access the Telnet Scripting feature, click Switches in the Navigation Tree.

To access a list of devices and directly launch a Telnet session, click and expand the applicable subnet in the Tree.

You can also access switches and launch Telnet sessions using the pull-down menu.



Filename	Last Modification Date
add_SNMP_users.script	Nov 10, 2007 9:27:06 AM
clean_flash.script	Nov 10, 2007 9:27:06 AM
Ewebimageclean.script	Nov 10, 2007 9:27:06 AM
Fwebimageclean.script	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM

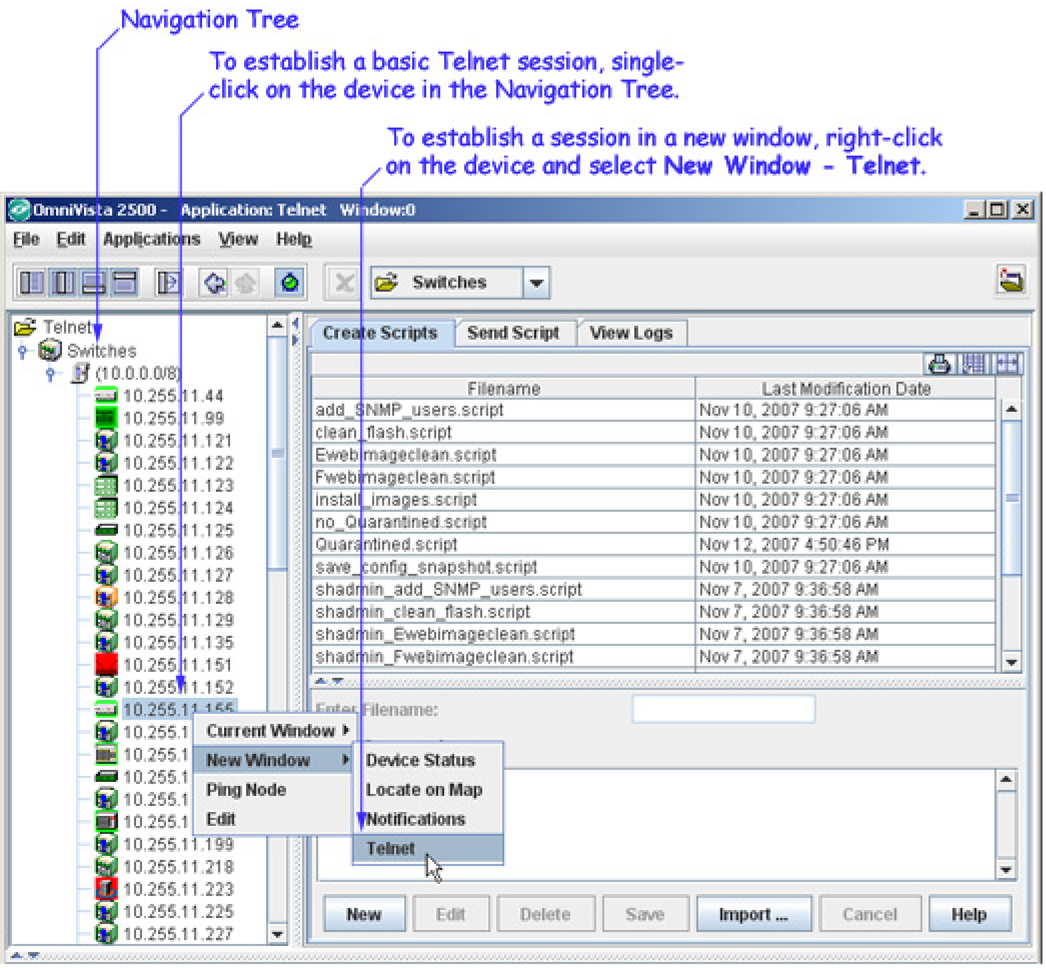
Telnet Scripting functions are accessed via these tabs.

To discontinue the current Telnet operation, click Cancel.

Establishing a Basic Telnet Session

To establish a basic Telnet session with a device, begin by clicking the **Switches** directory in the Navigation tree. One or more **Subnet** directories are displayed in the tree. Click the applicable **Subnet** directory, and then single-click the icon or IP address of the desired device. A Telnet session for the device launches automatically.

To establish a basic Telnet session in a *new window*, right-click a device's icon or IP address in the tree and select **New Window** -> **Telnet**. A new instance of OmniVista is opened and a Telnet session to the corresponding device is launched.



Navigation Tree

To establish a basic Telnet session, single-click on the device in the Navigation Tree.

To establish a session in a new window, right-click on the device and select New Window - Telnet.

Filename	Last Modification Date
add_SNMP_users.script	Nov 10, 2007 9:27:06 AM
clean_flash.script	Nov 10, 2007 9:27:06 AM
Ewebimageclean.script	Nov 10, 2007 9:27:06 AM
Fwebimageclean.script	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM

> **Note:** If SSH has been configured as the preferred encryption type, the term **SSH** will be used in the place of **Telnet** in OmniVista's pop-up menus, application buttons, etc.

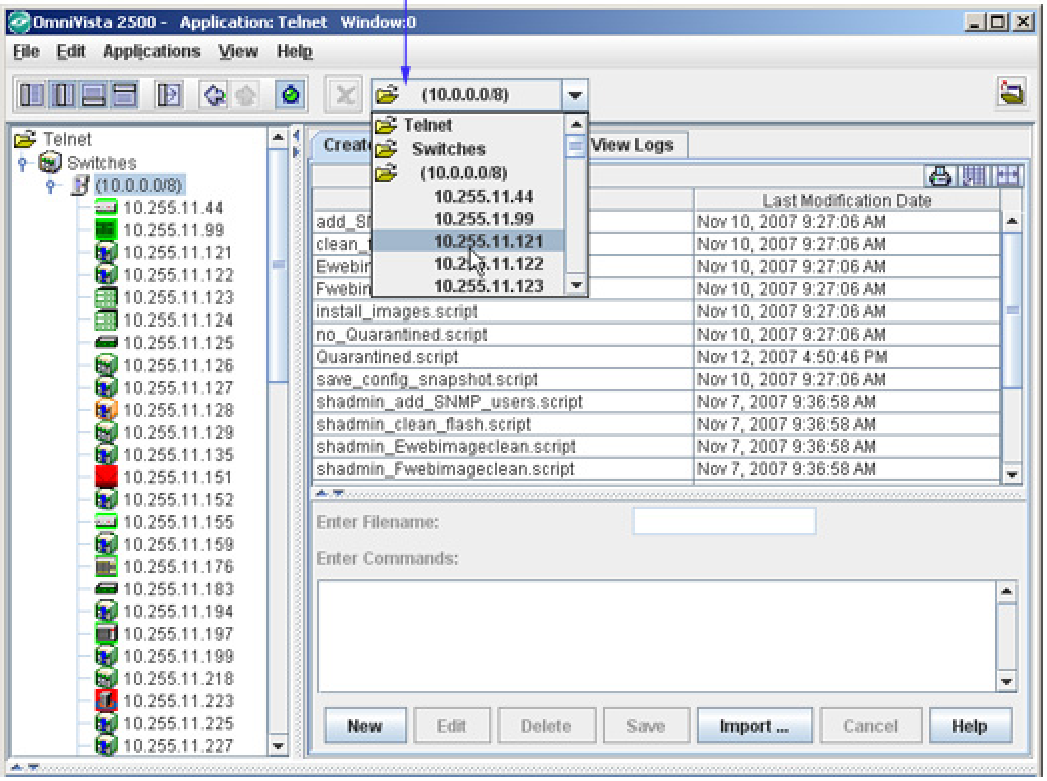
If Automatic Login has not been configured for the device, enter the login ID and password for the device in the Telnet window. If Automatic Login has been configured, OmniVista will enter the login ID and password automatically.

After login is complete, the CLI command prompt is displayed. A successful Telnet session has been established and the device is now ready to be managed and/or configured via the CLI.

Launching Telnet Sessions Using the Pull-Down Navigation Menu

Telnet sessions can also be launched from the pull-down menu located at the top of the main Telnet window. However, be sure that a particular subnet has first been selected in the Navigation tree. When a subnet is selected, the pull-down menu lists all discovered devices in that subnet. Simply scroll and click to select a device from the menu; a Telnet session for the device launches automatically.

Telnet sessions can also be launched by selecting devices from this pull-down menu. Be sure that a subnet directory is highlighted in the Navigation Tree, then scroll and click to select a device. The session launches automatically.

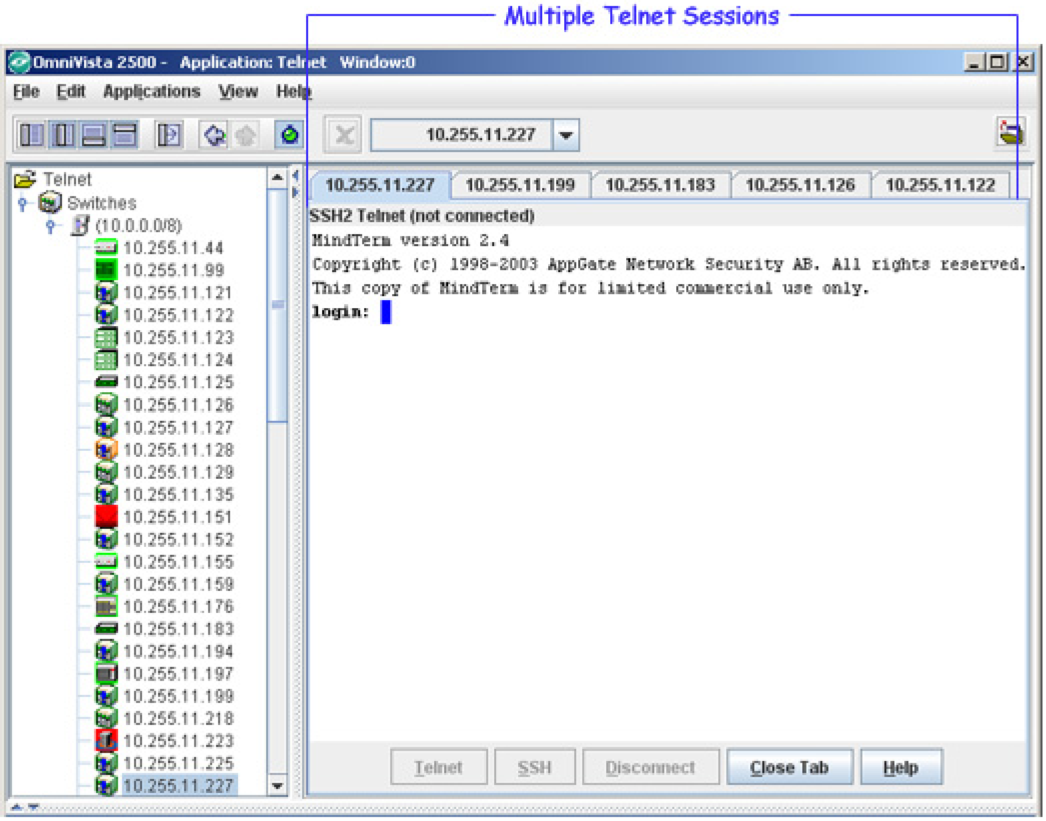


	Last Modification Date
add_S	Nov 10, 2007 9:27:06 AM
clean_	Nov 10, 2007 9:27:06 AM
Ewebir	Nov 10, 2007 9:27:06 AM
Fwebir	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM

Note: Unlike the Navigation tree, the pull-down navigation menu does not show additional status information, such as a device's type or whether it is reachable.

Managing Multiple Telnet Sessions

Multiple sessions can be launched and managed within the same instance of the Telnet application. To establish multiple Telnet sessions, simply select multiple devices, one at a time, from the Navigation tree. A new tab is displayed for each session, with each tab indicating the IP address for its corresponding session.



```
SSH2 Telnet (not connected)
MindTerm version 2.4
Copyright (c) 1998-2003 AppGate Network Security AB. All rights reserved.
This copy of MindTerm is for limited commercial use only.
login:
```

To access a particular Telnet session, click the tab showing the device's IP address. The corresponding Telnet window is displayed.

> **Note:** Multiple Telnet sessions can be launched from the pulldown menu located at the top of the OmniVista window also. Scroll and click to select devices from the pulldown menu; a Telnet session for each device launches automatically and a new tab for each session is displayed.

Closing Telnet Sessions

To close a Telnet session, click the **Disconnect** button at the bottom of the Telnet window or type **exit** at the command prompt.

If multiple sessions are being managed, clicking the **Close Tab** button disconnects a session and also closes its corresponding tab. (Note that the **Close Tab** button is not available if only one Telnet session is open.)

Reestablishing Closed Sessions

When a session has been disconnected, it can be quickly reconnected by clicking the **Telnet** button at the bottom of the Telnet window. If multiple sessions are being managed, be sure that the tab for the desired device is selected before clicking the **Telnet** button. Otherwise, sessions can be reestablished by following the steps described in the "Establishing a Basic Telnet Session" and "Managing Multiple Telnet Sessions" sections.

Configuring Automatic Login

Automatic Login (also referred to as Auto-Login) allows users to pre-configure the user ID and password for one or more devices. This allows OmniVista to automatically log into a device whenever a Telnet session is launched. In other words, the user is not required to type the user ID or password when the Telnet session reaches the login prompt. Instead, the information is entered automatically and the cursor is moved directly to the command prompt.

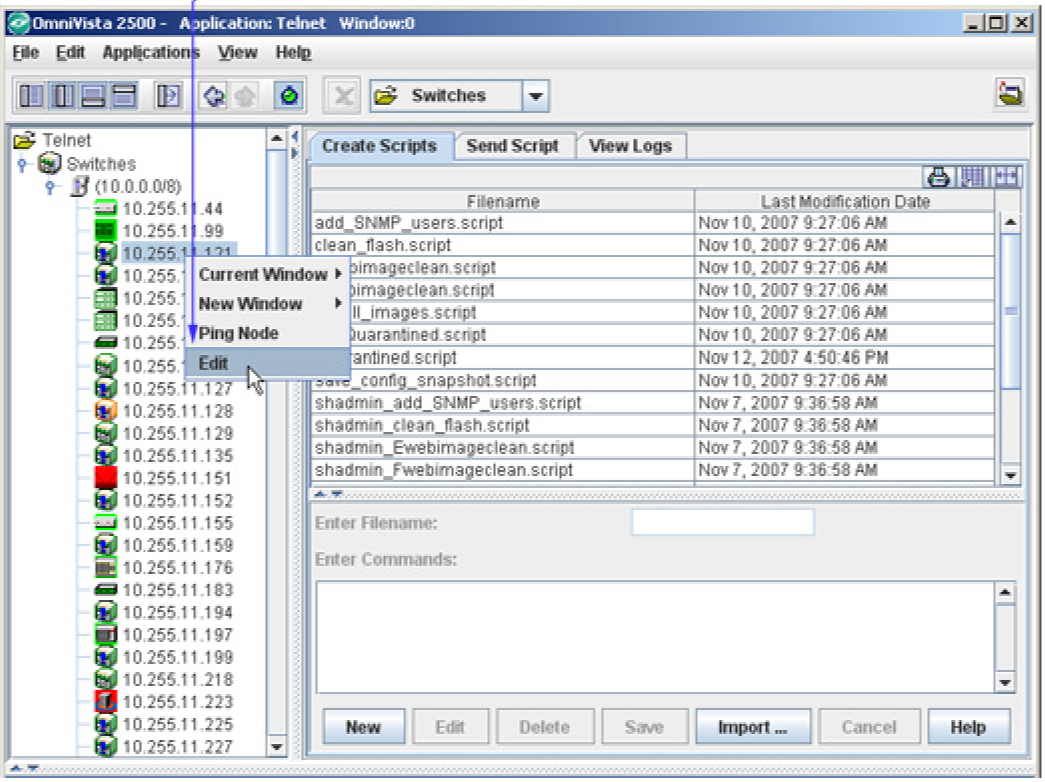
> **Important Note:** Auto-Login is required whenever applying scripts and importing scripts to a device. If Auto-login is not pre-configured for the device, a login error will result.

The Auto-Login feature can be configured on a device-by-device basis, or for multiple devices at once. Note that when Auto-Login is configured, the changes are only applied to OmniVista's Telnet login preferences. Login settings on the device itself are not affected.

Configuring Automatic Login for a Single Device

To configure Auto-Login for a single device, right-click the device in the Telnet navigation tree and select **Edit** from the popup menu that displays.

Right-click on a device in the Navigation Tree and select Edit from the drop-down menu.

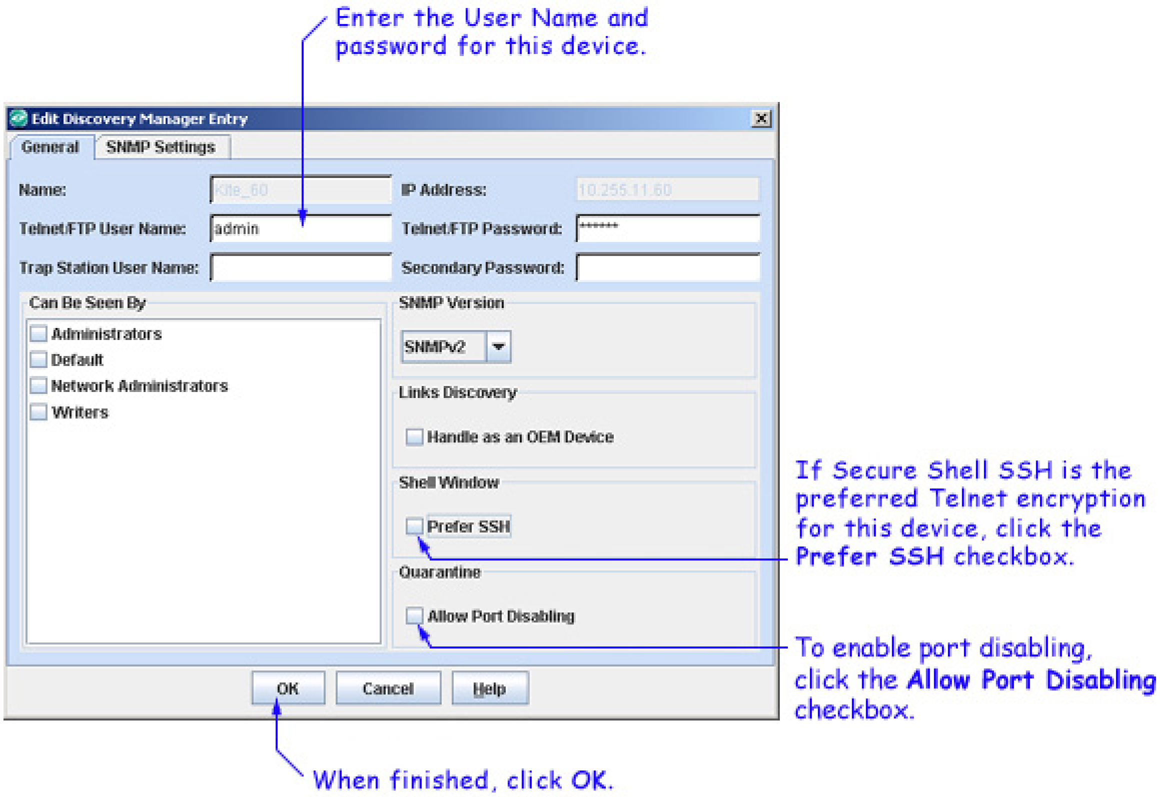


Filename	Last Modification Date
add_SNMP_users.script	Nov 10, 2007 9:27:06 AM
clean_flash.script	Nov 10, 2007 9:27:06 AM
bimageclean.script	Nov 10, 2007 9:27:06 AM
bimageclean.script	Nov 10, 2007 9:27:06 AM
ll_images.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 10, 2007 9:27:06 AM
antined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM

Enter Filename:

Enter Commands:

The **Edit-Discovery-Manager-entry** dialog box is displayed. Enter the user ID and password for the device in the **Telnet/FTP User Name** and **Telnet/FTP Password** text fields. If SSH (Secure Shell) is the preferred Telnet encryption type, click the **Prefer SSH** checkbox. (When this box is checked, future Telnet sessions for this device will use SSH.) Click the **Allow Port Disabling** checkbox to enable port disabling for a device. By default, all devices prohibit port disabling. When finished, click the **OK** button.



Enter the User Name and password for this device.

Edit Discovery Manager Entry

General | SNMP Settings

Name: Kite_60

IP Address: 10.255.11.60

Telnet/FTP User Name: admin

Telnet/FTP Password: ******

Trap Station User Name:

Secondary Password:

Can Be Seen By

□ Administrators
□ Default
□ Network Administrators
□ Writers

SNMP Version: SNMPv2

Links Discovery

□ Handle as an OEM Device

Shell Window

□ Prefer SSH

Quarantine

□ Allow Port Disabling

If Secure Shell SSH is the preferred Telnet encryption for this device, click the **Prefer SSH checkbox.**

To enable port disabling, click the **Allow Port Disabling** checkbox.

When finished, click OK.

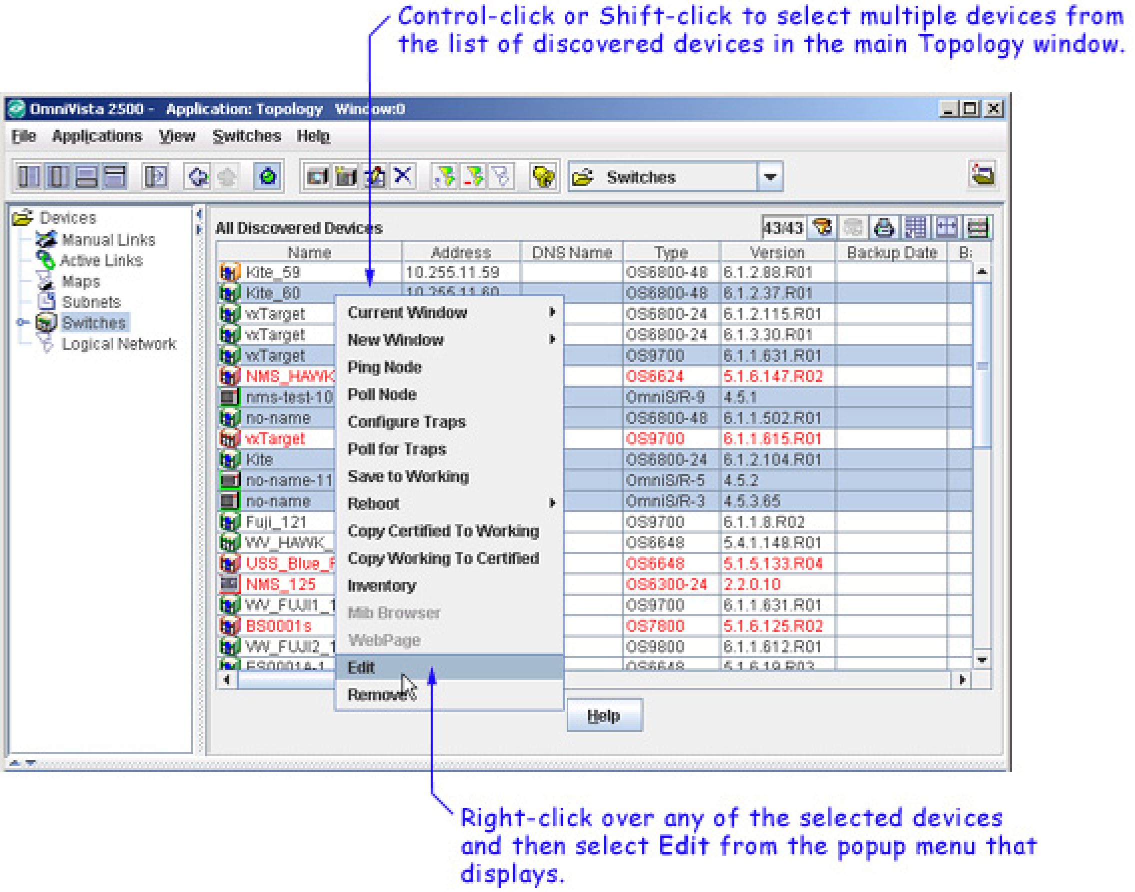
Note: For information on verifying Auto-Login for one or more devices, refer to the Verifying Automatic Login section.

Configuring Automatic Login for Multiple Devices

Auto-Login for multiple devices is configured through OmniVista's **Topology** application. Topology allows users to select multiple devices from a list and, in one step, specify the user ID and password to be used for future Telnet sessions. SSH (Secure Shell) can also be set as the default Telnet encryption for all selected devices.

To set up Auto-Login for multiple devices, start by opening the Topology application. (Topology can be accessed via the Task Bar by clicking the **Configuration** group button and then the **Topology** application button.)

When Topology launches, a list of all discovered devices is displayed. Using Control-click or Shift-click, select the devices from the list. Right-click any of the selected devices. A pop-up menu is displayed. Select **Edit** from the menu.

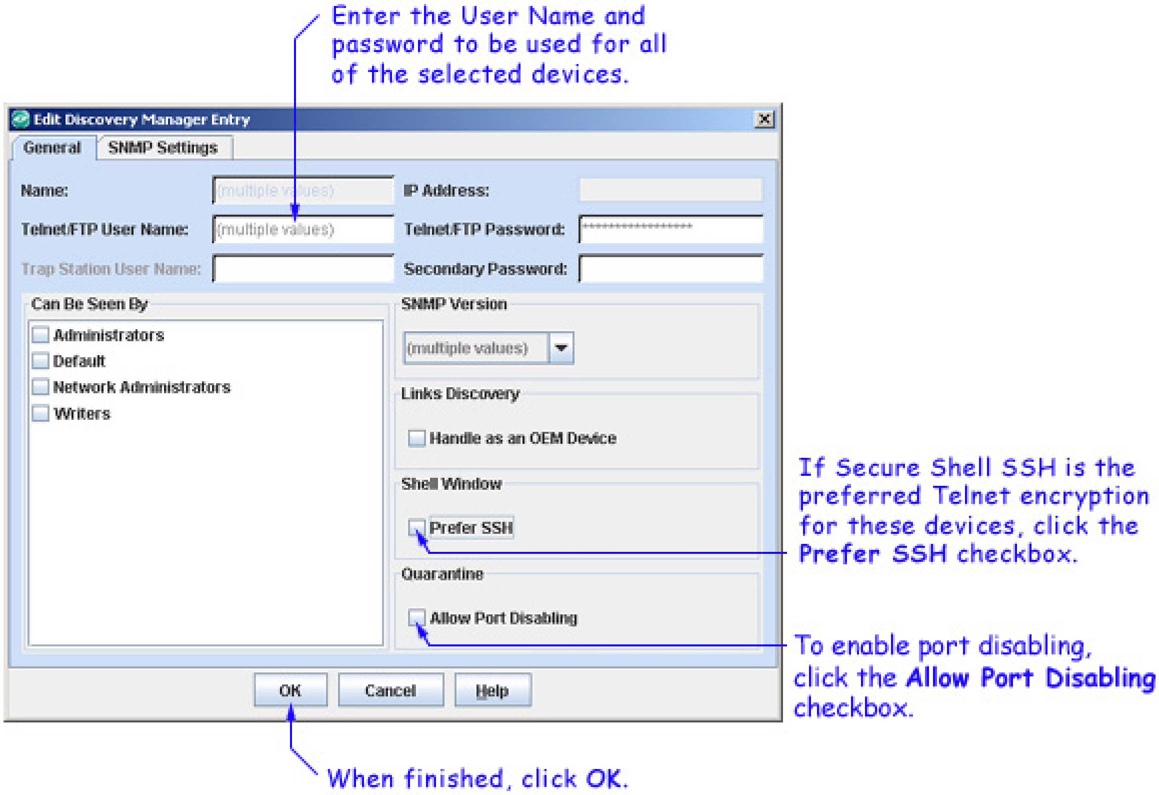


Name	Address	DNS Name	Type	Version	Backup Date	B:
Kite_59	10.255.11.59		OS6800-48	6.1.2.88.R01		
Kite_60	10.255.11.60		OS6800-48	6.1.2.37.R01		
vxTarget			OS6800-24	6.1.2.115.R01		
vxTarget			OS6800-24	6.1.3.30.R01		
vxTarget			OS9700	6.1.1.631.R01		
NMS_HAWK			OS6624	5.1.6.147.R02		
nms-test-10			OmniS/R-9	4.5.1		
no-name			OS6800-48	6.1.1.502.R01		
vxTarget			OS9700	6.1.1.615.R01		
Kite			OS6800-24	6.1.2.104.R01		
no-name-11			OmniS/R-5	4.5.2		
no-name			OmniS/R-3	4.5.3.65		
Fuji_121			OS9700	6.1.1.8.R02		
VV_HAWK_			OS6648	5.4.1.148.R01		
USS_Blue_F			OS6648	5.1.5.133.R04		
NMS_125			OS6300-24	2.2.0.10		
VV_FUJI1_1			OS9700	6.1.1.631.R01		
BS0001s			OS7800	5.1.6.125.R02		
VV_FUJI2_1			OS9800	6.1.1.612.R01		
ES0001A-1			OS6648	5.1.6.19.R03		

Control-click or Shift-click to select multiple devices from the list of discovered devices in the main Topology window.

Right-click over any of the selected devices and then select Edit from the popup menu that displays.

The **Edit Discovery Manager Entry** dialog box is displayed. Enter the user ID and password for the selected devices in the **Telnet/FTP User Name** and **Telnet/FTP Password** text fields. If SSH (Secure Shell) is the preferred Telnet encryption type, click the **Prefer SSH** checkbox . (By default, future Telnet sessions for the selected devices will use SSH.) Click the **Allow Port Disabling** checkbox to enable port disabling for the selected devices. By default, all devices prohibit port disabling. When finished, click the **OK** button.



Name: (multiple values)

IP Address:

Telnet/FTP User Name: (multiple values)

Telnet/FTP Password: ******************

Trap Station User Name:

Secondary Password:

Can Be Seen By

- □ Administrators
- □ Default
- □ Network Administrators
- □ Writers

SNMP Version: (multiple values)

Links Discovery

□ Handle as an OEM Device

Shell Window

□ Prefer SSH

Quarantine

□ Allow Port Disabling

Enter the User Name and password to be used for all of the selected devices.

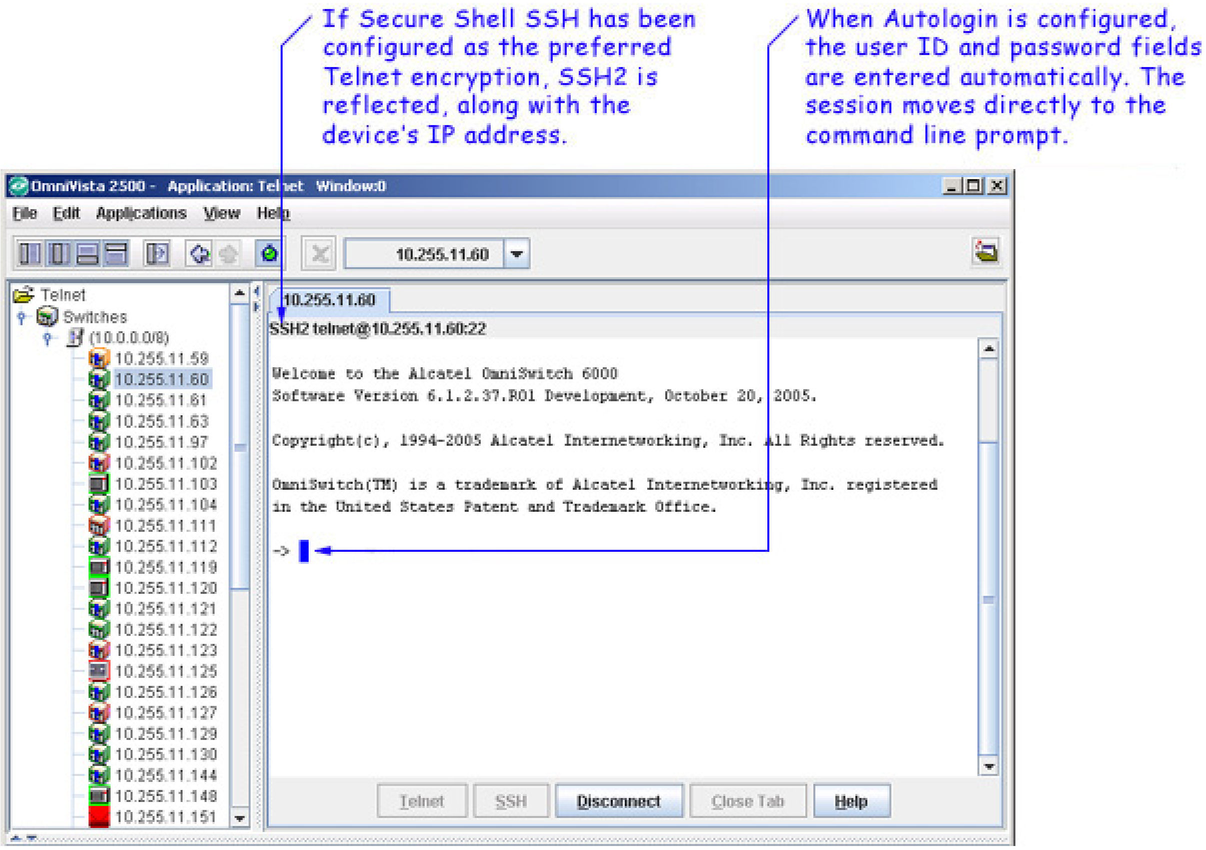
If Secure Shell SSH is the preferred Telnet encryption for these devices, click the **Prefer SSH** checkbox.

To enable port disabling, click the **Allow Port Disabling** checkbox.

When finished, click **OK**.

Verifying Automatic Login

Verify the Auto-Login setup by launching a Telnet session to a device where Auto-Login information has been specified. When the session is launched, the user ID and password fields should be populated automatically and the cursor should move directly to the command prompt.



If Secure Shell SSH has been configured as the preferred Telnet encryption, SSH2 is reflected, along with the device's IP address.

When Autologin is configured, the user ID and password fields are entered automatically. The session moves directly to the command line prompt.

SSH2 telnet@10.255.11.60:22

```
Welcome to the Alcatel OmniSwitch 6000
Software Version 6.1.2.37.R01 Development, October 20, 2005.

Copyright(c), 1994-2005 Alcatel Internetworking, Inc. All Rights reserved.

OmniSwitch(TM) is a trademark of Alcatel Internetworking, Inc. registered
in the United States Patent and Trademark Office.

->
```

Note: If an Auto-Login error occurs (i.e., the Telnet connection times out), be sure that the user ID and password for the device are correct and that the device is reachable. To check whether a device is reachable, right-click the device in the Navigation Tree and select **Ping Node** from the popup menu. The results of the ping are displayed in the Status pane at the bottom of the main OmniVista window.

Creating Script Files

A Telnet script file is a text-based file used to configure one or more devices through OmniVista's Telnet scripting feature. Telnet scripting is especially useful in applying batch updates or common configurations across multiple devices. A script file can contain can be a combination of both CLI commands and JavaScript. . When a script file is applied, each command in the file is sent to the device via Telnet.

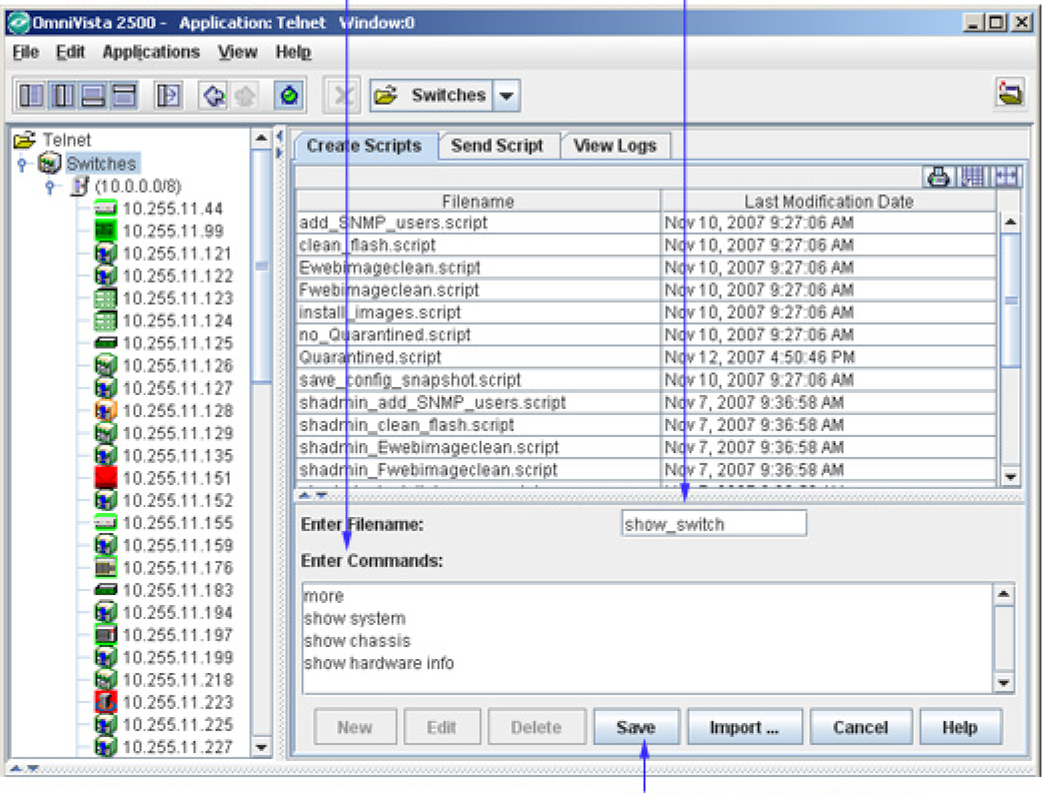
Important Note: Before attempting to apply a script, OmniVista must know the user name and password for each device being configured. Use Auto-Login to specify the login information.

Users are not required to create script files using a third-party text editor. OmniVista provides a text box where CLI commands can be manually entered from the Telnet application. During the Telnet Scripting steps, these commands are saved to a script file (which can be accessed for reference or future applications). In addition, a log file containing status and troubleshooting information is generated automatically. Follow the steps below to create a script.

1. Select the **Create Scripts** tab is selected and then click the **New** button.

Enter commands in the Enter Commands area.

Enter a descriptive filename in the Enter Filename field.



Filename	Last Modification Date
add_SNMP_users.script	Nov 10, 2007 9:27:06 AM
clean_flash.script	Nov 10, 2007 9:27:06 AM
Ewebimageclean.script	Nov 10, 2007 9:27:06 AM
Fwebimageclean.script	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM

Enter Filename: show_switch

Enter Commands:

```
more
show system
show chassis
show hardware info
```

Click Save when finished.

2. Enter a descriptive file name in the **Enter Filename** text field. For example, **show_switch**. (The file extension **.script** will be added automatically when the script file is saved.)

3. Press the **Tab** key or select the **Enter Commands** text box. Enter the commands to be applied to the switch via this script. Enter only one command per line.

Important Note: Operational commands that automatically issue a confirmation prompt and require the user to type a response (like Y or N) are not supported in CLI script files. Examples include **takeover**, **reload**, **fsck**, etc. Do not attempt to include these command types in the script file. Instead, manually issue them via the standard CLI command line prompt. These operations can also be issued on a device-by-device basis via WebView or OmniVista.

4. Verify that the syntax of all commands are correct before proceeding. When finished, click the **Save** button.

When the **Save** button is clicked, the script entries are automatically saved to a **.script** file. This file can be especially helpful if you want to save a particular configuration for later use. By default, the file is saved in OmniVista's **scripting_files** directory on the server or local system. This directory's location may vary, depending on the OmniVista installation, but can generally be found at a path similar to the following:

Alcatel OmniVista 2500\data\telnet\scripting_files

Click on the Send Script tab to send the script to specific switches.

Importing Existing Script Files

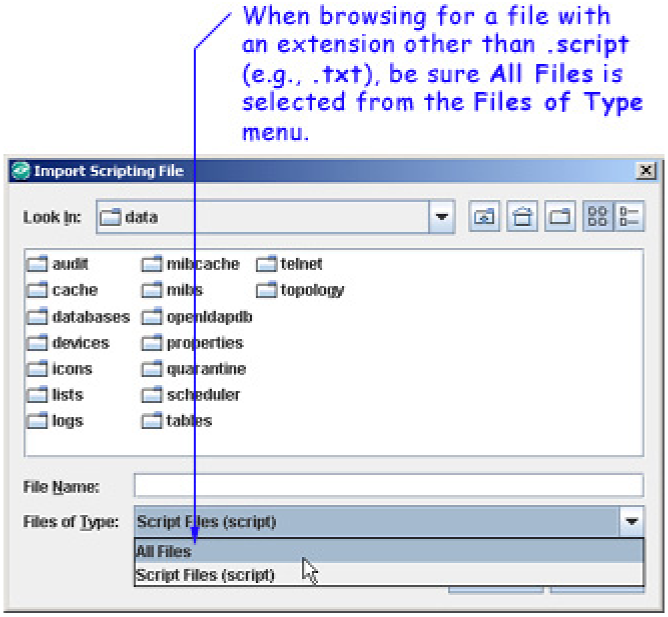
Although OmniVista allows users to manually create script files within the Telnet application, existing script files can also be imported. In other words, a file containing a set of CLI commands can be accessed from a server or local drive and then applied to one or more devices. This allows users to maintain a library of network configurations and then apply them to devices in their network as needed.

Before importing a file to one or more devices, consider the following important guidelines:

- Any script file being imported must be text-based (ASCII).
- Although file extensions such as **.txt** and **.ascii** are supported, the file extension **.script** is recommended for browsing purposes.
- All CLI commands contained in the file must be AOS-supported. Also, operational commands that automatically issue a confirmation prompt and require the user to type a response (like Y or N) are not supported in CLI script files. Examples include **takeover**, **reload**, **fsck**, etc. Do not attempt to include these command types in the script file. Instead, manually issue them via the standard CLI command line prompt. These operations can also be issued on a device-by-device basis via WebView or OmniVista.
- CLI commands must also be entered into the text file one command per line.
- Only one script file can be imported at a time.

To import a script file, click the **Import** button at the bottom of the main Telnet window. The **Import Scripting File** dialog box displays. Use the dialog box's **Look In** pulldown menu to locate the file being imported.

> **Note:** If you are browsing for a file with an extension other than **.script**, be sure to select **Files of Type -> All Files** in the dialog box, as shown:



When browsing for a file with an extension other than .script (e.g., .txt), be sure All Files is selected from the Files of Type menu.

Look In: data

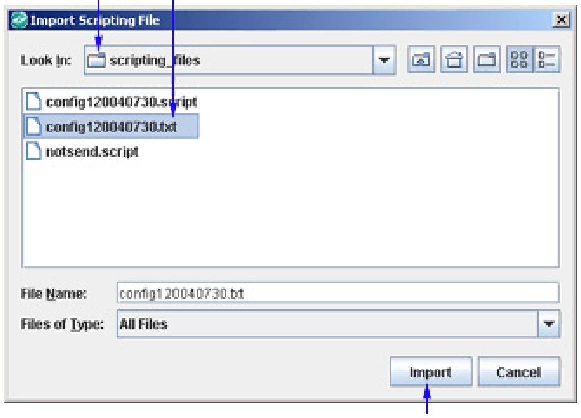
File Name:

Files of Type: Script Files (script)

Once the script file has been located, select the file in the dialog box window; the file name displays in the **File Name** text field. Click the **Import** button.

Use the Look In pulldown menu to browse and locate the script file being imported.

Select the file in the dialog box window.



Import Scripting File

Look In: scripting_files

config120040730.script
config120040730.txt
notsend.script

File Name: config120040730.txt

Files of Type: All Files

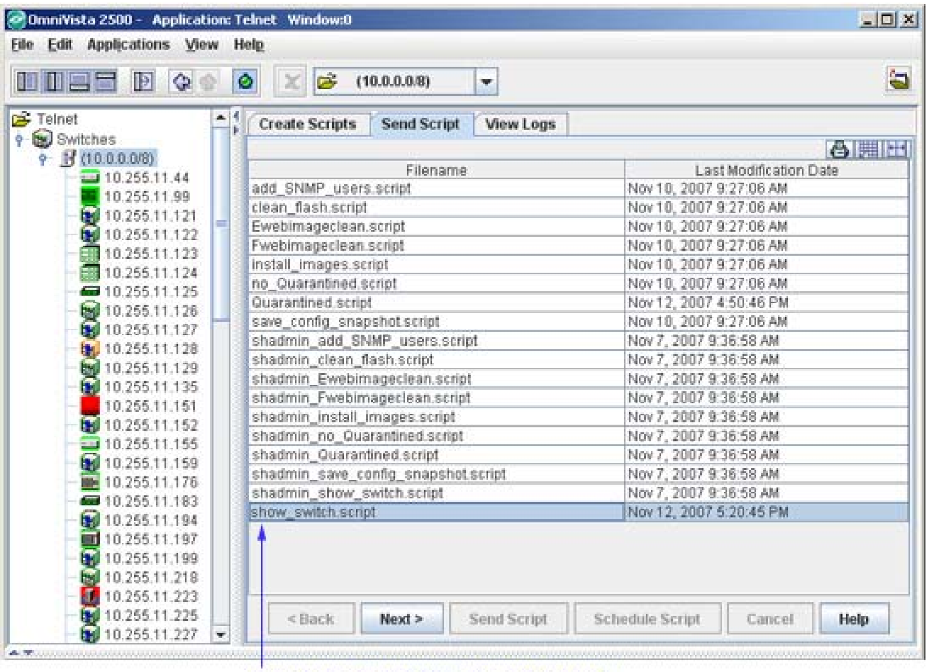
Click the Import button.

Important Note: The script import procedure is *not* complete at this point. You must complete the additional steps described below.

To continue the script import procedure, click the **Send Script** tab in the main Telnet window. The script file selected from the **Import Scripting File** dialog box is displayed in the **Filename** column.

> **Note:** If the **Filename** column does not display, be sure the **Send Script** tab is selected and, if needed, click the **Back** button until the column is displayed.

Select the script file in the **Filename** column and then click the **Next** button.



OmniVista 2500 - Application: Telnet Window:0

Filename	Last Modification Date
add_SNMP_users.script	Nov 10, 2007 9:27:06 AM
clean_flash.script	Nov 10, 2007 9:27:06 AM
Ewebimageclean.script	Nov 10, 2007 9:27:06 AM
Fwebimageclean.script	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_install_images.script	Nov 7, 2007 9:36:58 AM
shadmin_no_Quarantined.script	Nov 7, 2007 9:36:58 AM
shadmin_Quarantined.script	Nov 7, 2007 9:36:58 AM
shadmin_save_config_snapshot.script	Nov 7, 2007 9:36:58 AM
shadmin_show_switch.script	Nov 7, 2007 9:36:58 AM
show_switch.script	Nov 12, 2007 5:20:45 PM

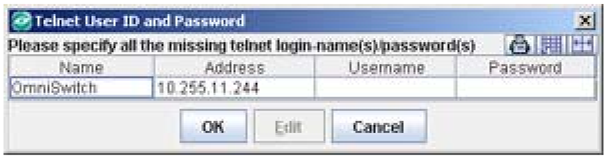
Select the script file, then click Next.

A list of discovered devices is displayed. From the list, select the device to which the file is being imported and then click the **Next** button.

> **Note:** Telnet Scripting's import file option supports multiple devices. If the script file is to be applied to more than one device, simply Control-click or Shift-click all applicable devices in the list before clicking **Next**. Remember, however, Auto-Login must first be configured for all devices to which a file is being imported.

The commands in the script file are displayed in the **Scripts Content** window.

If the selected device is without a Telnet username/password, then a dialog box will pop up, to allow you to enter the Telnet user name and password for the device. Enter the Telnet user name and password, and then click the **OK** button to close the popup dialog box.



Please specify all the missing telnet login-name(s)/password(s)

Name	Address	Username	Password
OmniSwitch	10.255.11.244		

Click the **Send Script** button in the **Send Script** tab. The script file is now imported and applied to the switch, and the status of the import operation is displayed.

Tip: If the file is not successfully imported (i.e., Percent Done does not reach 100), check the status pane at the bottom of the main Telnet window for troubleshooting information. The most common error when trying to import a file is missing login information. This can be corrected by configuring Auto-Login for the device.

Reminder: Changes made to a device using a script file are applied only to the device's *running memory* (i.e., RAM). If the device reboots or goes down unexpectedly, any unsaved changes will be lost. To save changes to the device's Working directory, you must either use the OmniVista Topology application or type **write memory** at the Telnet session command prompt. To save changes using the Topology application, right-click the device from the main Topology window and select **Save to Working** from the popup menu. If multiple devices have been configured using the script file, be sure to save changes for each device.

Editing Script Files

To edit a script file, select the file from the **Filename** list, then click **Edit**. The **Enter Scripts** text box (which was previously grayed out) becomes active. The CLI commands contained in the selected script file can now be deleted, modified, or appended. When the changes are complete, click the **Save** button.

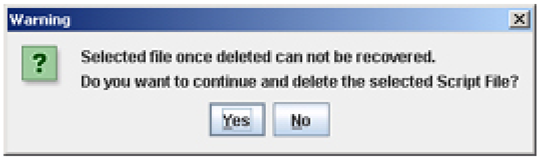
Important Note: When the changes are saved, the previous contents of the script file are overwritten. To preserve the original contents of the file, be sure to make a backup copy before editing.

Deleting Script Files

To delete a script file, select the file from the **Filename** list, then click **Delete**.

Note: When a file is deleted, it is permanently removed from the **scripting_files** directory. Once a script file is deleted, it cannot be recovered.

Click **Yes** in the Warning dialog box.



Selected file once deleted can not be recovered.
Do you want to continue and delete the selected Script File?

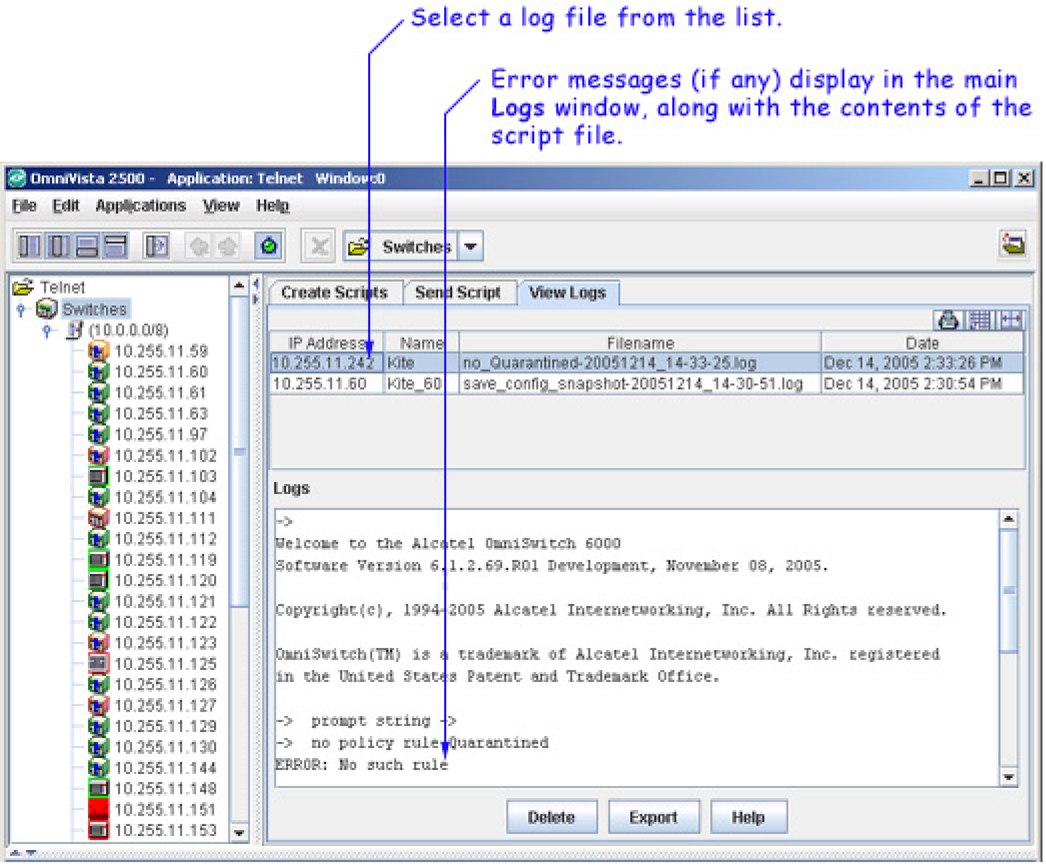
Deleting Multiple Script Files

Multiple log files can be deleted at once. To delete multiple script files, simply Control-click or Shift-click all applicable files in the list before clicking **Delete**. Remember, however, that once the files have been deleted, they cannot be recovered.

Viewing Log Files

The **View Logs** tab allows users, on a command-by-command basis, to view Telnet Scripting results. In other words, it displays whether the contents of a file were successfully applied to the device. A log file also provides a record of a particular configuration, as well as effective troubleshooting information, when applicable.

Unless an error has occurred, the log file will closely resemble the script file (i.e., it will list only the CLI commands that were applied to the device). If an error has occurred, an error notification displays in the log, following the CLI command that triggered the error. For more information, see the example below:



Select a log file from the list.

Error messages (if any) display in the main Logs window, along with the contents of the script file.

IP Address	Name	Filename	Date
10.255.11.242	Kite	no_Quarantined-20051214_14-33-25.log	Dec 14, 2005 2:33:26 PM
10.255.11.60	Kite_60	save_config_snapshot-20051214_14-30-51.log	Dec 14, 2005 2:30:54 PM

Logs

```
->
Welcome to the Alcatel OmniSwitch 6000
Software Version 6.1.2.69.R01 Development, November 08, 2005.

Copyright(c), 1994-2005 Alcatel Internetworking, Inc. All Rights reserved.

OmniSwitch(TM) is a trademark of Alcatel Internetworking, Inc. registered
in the United States Patent and Trademark Office.

->  prompt string ->
->  no policy rule Quarantined
ERROR: No such rule
```

As with the scripting files, log files are automatically stored on the server or local system. File locations may vary, depending on the OmniVista installation, but can generally be found at a path similar to the following:

Alcatel OmniVista 2500\data\telnet\scripting_logs

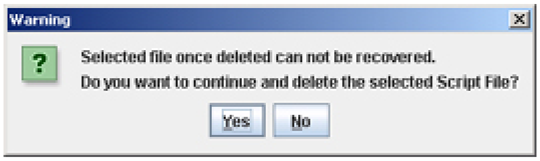
> **Note:** By default, log files are placed in a directory indicating the IP address of the corresponding device.

Deleting Log Files

To delete a log file, select the file from the **Filename** list, then click **Delete**.

> **Note:** When a file is deleted, it is permanently removed from the **scripting_logs** directory. Once a log file is deleted, it cannot be recovered.

Click **Yes** in the **Warning** dialog box.



Selected file once deleted can not be recovered.
Do you want to continue and delete the selected Script File?

Deleting Multiple Log Files

Multiple log files can be deleted at once. To delete multiple log files, simply Control-click or Shift-click all applicable files in the list before clicking **Delete**. Remember, however, that once the files have been deleted, they cannot be recovered.

Specifying SSH Session Preference

SSH (Secure Shell) provides Telnet sessions with enhanced encryption and security. SSH may be mandatory for some device types. OmniVista uses SSH by default for those devices requiring SSH. However, for AOS and other devices where SSH is optional, standard Telnet is the default setting. To use SSH, the user must specify SSH either on a device-by-device basis, or on multiple devices.

Specifying SSH on a Single Device

To specify SSH encryption on a single device, right-click the device in the Telnet Navigation Tree and select **Edit** from the popup menu that displays.

The **Edit-Discovery-Manager-entry** dialog box displays. Click the checkbox next to Prefer SSH. When this box is checked, future Telnet sessions for this device will use SSH. When finished, click the **OK** button.

Specifying SSH on Multiple Devices

As with Auto-Login, specifying SSH for multiple devices is done through OmniVista's Topology application. Topology allows users to select multiple devices from a list and, in one step, specify the SSH preference for future Telnet sessions.

To set up SSH for multiple devices, start by opening the Topology application. (Topology can be accessed via the Task Bar by clicking the **Configuration** group button and then the **Topology** application button.)

When Topology launches, a list of all discovered devices displays. Using **Control-click** or **Shift-click**, select the devices from the list. Right-click over any of the selected devices. A popup menu displays. Select **Edit** from the menu.

The **Edit Discovery Manager Entry** dialog box displays. Click the checkbox next to Prefer SSH. Future Telnet sessions for the selected devices will use SSH. When finished, click the **OK** button.

Creating and Using Telnet Scripts

A Telnet script file is a text-based file used to configure one or more devices through OmniVista's Telnet Scripting feature. Telnet scripting is especially useful in applying batch updates or common configurations across multiple devices. When a script file is applied, each command in the file is sent to the device via Telnet.

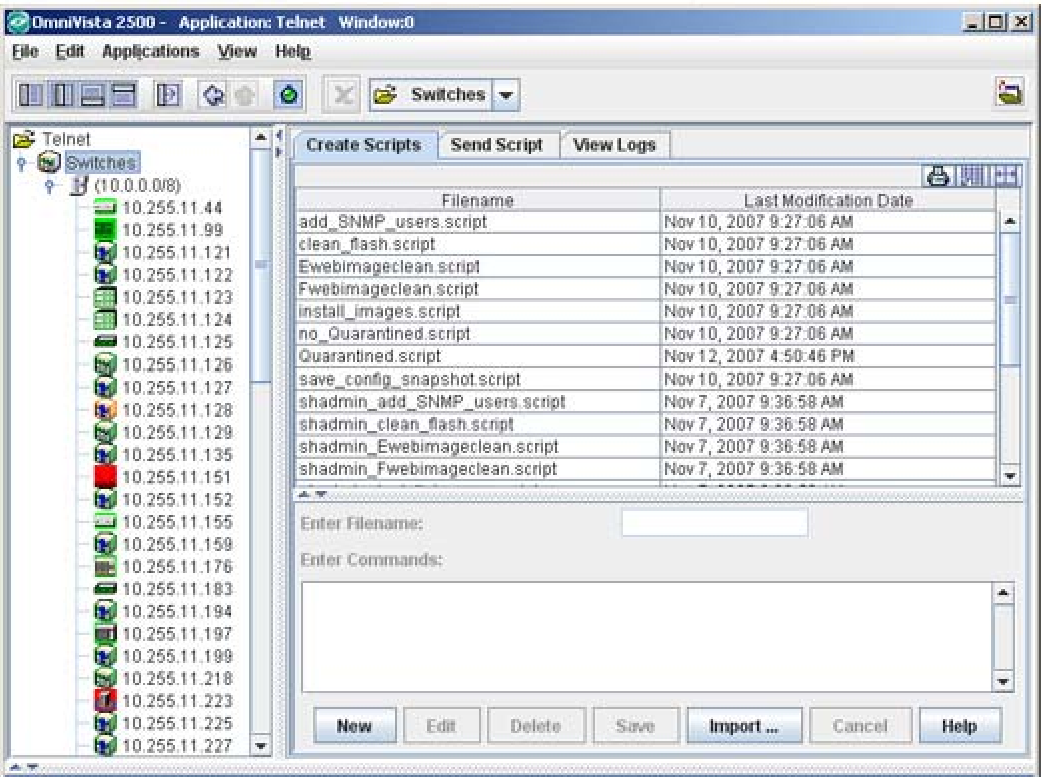
> **Note:** Before attempting to apply a script, OmniVista must know the user name and password for each device being configured. Use Auto-Login to specify the login information.

Users are not required to create script files using a third-party text editor. OmniVista provides a text box where CLI commands can be manually entered from the Telnet application. During the Telnet Scripting steps, these commands are saved to a script file (which can be accessed for reference or future applications).

Pre-Configured Script Files

OmniVista includes pre-configured Telnet script files to automate some tasks. A brief description of these scripts is provided below.

Pre-Configured Telnet Scripts



Filename	Last Modification Date
add_SNMP_users.script	Nov 10, 2007 9:27:06 AM
clean_flash.script	Nov 10, 2007 9:27:06 AM
Ewebimageclean.script	Nov 10, 2007 9:27:06 AM
Fwebimageclean.script	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM

shadmin_Ewebimageclean.script - Removes all the web image files from an OmniSwitch 8800 switch. Prior to an FPGA upgrade (AOS Release 5.1.6), the web image files must be removed due to flash size limitations. This script automates the removal process.

shadmin_Fwebimageclean.script - Removes all the web image files from an OmniSwitch 7700/7800 switch. Prior to an FPGA upgrade (AOS Release 5.1.6), the web image files must be removed due to flash size limitations. This script automates the removal process.

shadmin_install_images.script - Runs the install images script.

shadmin_save_config_snapshot.script - Creates a snapshot of the certified and working directory

shadmin_show_switch.script - Writes the switch information (System, Chassis, and Hardware information) to a log file, that can be viewed by clicking on the **View Logs** Tab.

shadmin_sFlowTool_configuration.script - Configures sFlow for a switch. The sample script below provides a syntax sample to show how a user can employ javascript for sending CLI commands, Regular Expressions, Arrays, loops, debugging (cli.trace), strings, and comments. See Creating New Script Files for more information.

> **Important Note:** Use caution when using the **shadmin_Ewebimageclean** and **shadmin_Fwebimageclean** scripts. Use the Resource Manager application to perform a full backup on the switch prior to an upgrade.

```
<js>
/*for a 'passive' sflow Collector modify the following line, otherwise comment out. Collector
configuration should precede Sampler and Poller*/

cli.sendCmd("sflow receiver 1 name sflowtool address 10.255.11.156 udp-port 6343 timeout 0
version 4");

/*The following lines determine which NI's are installed in the AOS device, so Samplers and
Pollers are only configured on the active slots*/

cli.sendCmd("show module");
var module = cli.lastResponse();
nilist = module.match(/NI-[0-9]{1,2}.*?/g);
cli.trace(nilist);
for (count=0; count < nilist.length; count++)
{
str = nilist[count].match("[0-9]{1,2}");
cli.trace(str);
for (i = 1; i <= 50; i++)
{
 cli.sendCmd("sflow sampler 1 "+str+"/"+i+" receiver 1 rate 56 sample-hdr-size 128");
 cli.sendCmd("sflow poller 1 "+str+"/"+i+" receiver 1 interval 5");
}
}
</js>
```

show sflow agent
show sflow sampler
show sflow poller

Creating New Script Files

Follow the steps below to create a new script file.

1. Click the **New** button and enter a descriptive file name in the **Enter Filename** text field. For example, **show_switch**. (The file extension **.script** will be added automatically when the script file is saved.)

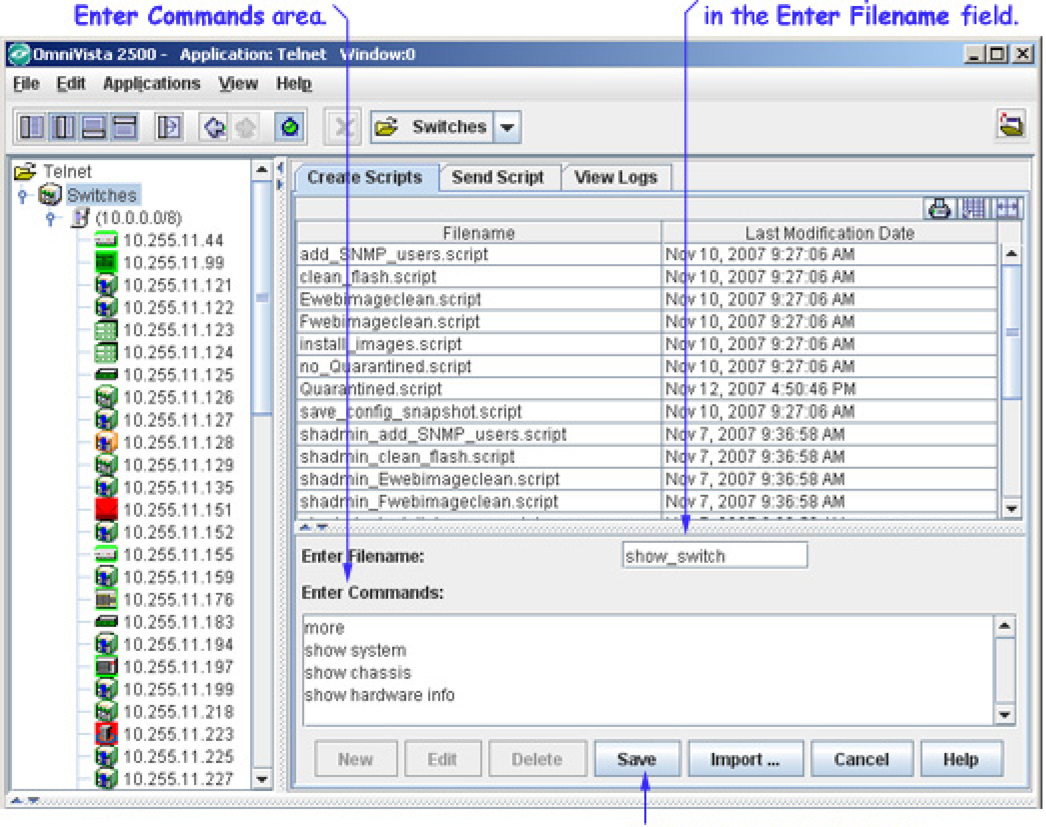
2. Press the **Tab** key or select the **Enter Commands** text box and enter the commands to be applied to the switch via this script. Enter on command per line. The script can be a combination of both CLI commands and JavaScript. You can also define variables to be used in the script.

> **Note:** Use of JavaScript requires Java 1.6.

3. Verify that the syntax of all the commands is correct, then click the **Save** button.

Enter commands in the Enter Commands area.

Enter a descriptive filename in the Enter Filename field.



Filename	Last Modification Date
add_SNMP_users.script	Nov 10, 2007 9:27:06 AM
clean_flash.script	Nov 10, 2007 9:27:06 AM
Ewebimageclean.script	Nov 10, 2007 9:27:06 AM
Fwebimageclean.script	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM

Enter Filename: show_switch

Enter Commands:

```
more
show system
show chassis
show hardware info
```

Click Save when finished.

CLI and Java Scripts

Scripts can be a combination of both CLI commands and JavaScript. The following is an example of a Telnet application CLI script containing JavaScript:

```
---------  script start -------------
<js>
var devtype = cli.deviceType();
if (devtype.indexOf("OS68") > -1)
cli.sendCmd("ls");
else if (devtype.indexOf("OS62") > -1)
cli.sendCmd("dir");
else
cli.sendCmd("files");
if (devtype.indexOf("OS68") > -1)
{
cli.setTimeout(3, 30);
cli.sendCmd("show log swlog");
}
else if (devtype.indexOf("OS66") > -1)
{
cli.setTimeout(5, 0);
cli.sendCmd("show log swlog");
}
println("I got: " + cli.lastResponse() );
cli.sendCmd("ls " + "$USERVAR" ); /* user defined variable! */

</js>
---------  script end -------------
```

Notice in the above example, the usage of the variable **‘cli’**. This is a built-in variable that can be used within the scripting blocks. CLI offers the following functions:

- **sendCmd(String cmd)** allows the user to send a CLI command to the switch.
- **lastResponse()** returns a string that represents the switch output from the last command the user sent to the switch (whether the command was sent via JavaScript or just entered as CLI in the cli script itself). deviceType() returns the same string as can be seen via the Topology applications “Type” column.
- **setTimeout(minutes, seconds)** allows a caller to specify a hint to the Telnet application about how long it could take for the next command to return a response. In the example above, the JavaScript specifies a timeout of 3 minutes and 30 seconds to apply to the next command (show log swlog) if the device is something like a OS6800-48. It specifies 5 minutes if the device is something like a OS6624. Some commands can be slow in returning output to the Telnet/SSH session, so this can help prevent the scripting session from timing out before a response is received. Once the session is receiving a response from the command (e.g., show log swlog), the default timeout will be automatically reset. The user specified timeout does not take affect for the entire session, just the CLI command used after the call to setTimeout(minutes, seconds). You may specify "0" for

minutes or seconds according to what is needed. Negative numbers are converted to '0' internally, thus ignored.

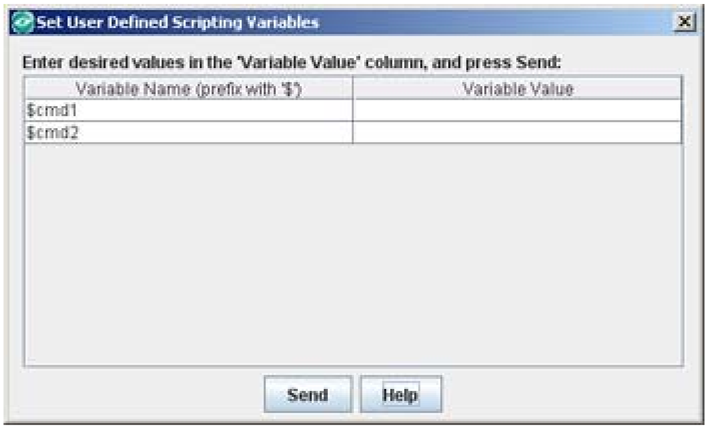
If both minutes and seconds contain either "0" and/or negative numbers, the timeout request will be ignored. Therefore the minimum timeout will be 1 second (ex: cli.setTimeout(0, 1);).

- **trace(String message)** logs any arbitrary string passed as its ‘message’ argument to the Telnet Audit Log. Can be contained in a variable for instance.
- **expectPrompt(String prompt)** sets-up the particular script (running on whatever devices) to expect a prompt that is not in the default collection of expected prompts. In other words, it allows the user to temporarily add to the set of prompts that Telnet scripting is hard-coded to recognize.
- **deviceType()** returns a string that contains the device’s type as seen in the Topology application.

Enter only one command per line. Operational commands that automatically issue a confirmation prompt and require the user to type a response (such as, Y or N) are not supported in CLI script files. Examples include **takeover**, **reload**, **fsck**, etc. Do not attempt to include these command types in the script file. Instead, manually issue them via the standard CLI command line prompt. These operations can also be issued on a device-by-device basis via WebView or OmniVista.

User Defined Variables

If you have specified variables within the script, the **Set User Defined Scripting Variables** window is displayed when you click on the **Send Script** button. Click in the "Variable Value" field next to the variable and enter value to be used, then click **Send**.



Set User Defined Scripting Variables

Enter desired values in the 'Variable Value' column, and press Send:

Variable Name (prefix with '$')	Variable Value
$cmd1	
$cmd2	

Variables must be prefixed with '$' to show they are variables. The built-in variables are:

- **$IP_ADDRESS** - replaced automatically with target switch IP address.
- **$BOOT_DIR** - replaced automatically with target boot directory (ex: working).
- **$BASE_MAC** - replaced automatically with target base MAC address.
- **$CHASSIS_TYPE** - replaced automatically with target chassis type.
- **$SYSTEM_OID** - replaced automatically with target unique object ID.
- **$LOGIN_ID** - replaced automatically with target FTP/Telnet login ID.

- **$LOGIN_PWD** - replaced automatically with target FTP/Telnet login password.
- **$READ_PWD** - replaced automatically with target community string for SNMP reading.
- **$WRITE_PWD** - replaced automatically with target community string for SNMP writing.

Script Directives

A tag, called <tapps> allows certain directives to the Telnet scripting application. <tapps> does not use a scripting engine. It is a set of supported commands that tell the Telnet application how to handle certain actions. For example, a user may write the following CLI script that uses all of the supported <tapps> commands:

<tapps> set timeout 5 </tapps>
qos apply
<tapps> import another.script </tapps>
<tapps> second password </tapps>

set timeout: The above script specifies a timeout for the *qos apply* command. It performs the same function as the previous Java Script example, but the user does not need to specify seconds. However the user must always specify minutes (the minutes can be "0" if the user wants to specify the timeout only in seconds).

Examples:
As shown above, to set a timeout of 5 minutes, only the *minutes* parameter is required:
<tapps> set timeout 5 </tapps>
qos apply

To set a timeout of 15 seconds, you must first specify 0 *minutes,* then 15 *seconds*:
<tapps> set timeout 0 15 </tapps>
qos apply

To set timeout of 5 minutes and 15 seconds, you would enter:
<tapps> set timeout 5 15 </tapps>
qos apply

> **Note:** The *set timeout* command only applies to the next command in the script (e.g., *qos apply*). Thereafter, the timeout reverts back to its default.

import script: The import script directive tells the Telnet application to insert the commands from the specified script at that spot in the current script. This allows re-use of scripts by other scripts. In the example above, if the Telnet application script named "another.script" contained only the command ls, then ls would be inserted at runtime at that point in the current script. The log output for a running of the current script would show the command 'qos apply' sent, followed by the command 'ls' being sent. Detection of loops takes place at strategic points in the Telnet application on both the client and server sides.

second password: The second password directive tells the Telnet application to prepare to send the password again. Some devices have a second login capability that requires the use of a second password. This second password for a given device is set by the user via Topology when a device is selected for Editing. The value in the Topology 'Secondary Password:' field will be used by this new <tapps> feature as the password to set when or if the device prompts for a password.

Importing Existing Script Files

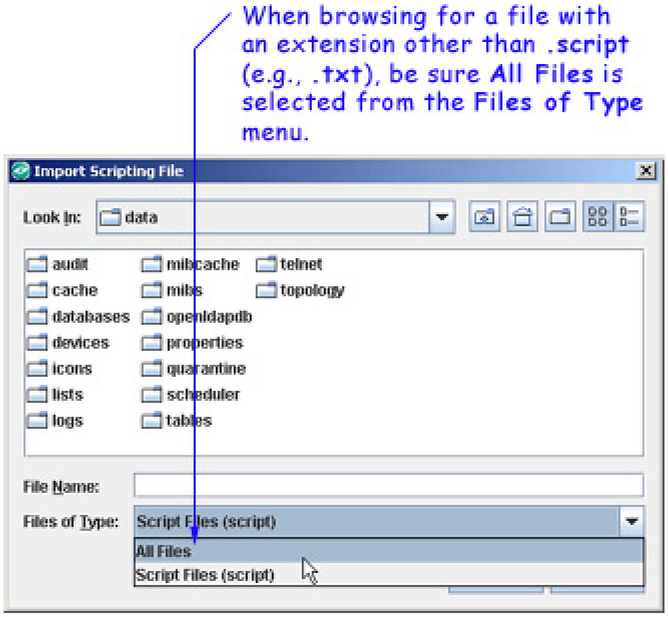
Although OmniVista allows users to manually create script files within the Telnet application, existing script files can also be imported. In other words, a file containing a set of CLI commands can be accessed from a server or local drive and then applied to one or more devices. This allows users to maintain a library of network configurations and then apply them to devices in their network as needed.

Before importing a file to one or more devices, consider the following important guidelines:

- Any script file being imported must be text-based (ASCII).
- Although file extensions such as **.txt** and **.ascii** are supported, the file extension **.script** is recommended.
- All CLI commands contained in the file must be AOS-supported. Also, operational commands that automatically issue a confirmation prompt and require the user to type a response (such as, Y or N) are not supported in CLI script files. Examples include **takeover**, **reload**, **fsck**, etc.
- CLI commands must also be entered into the text file *one command per line*.
- Only one script file can be imported at a time.

To import a script file, click the **Import** button at the bottom of the main Telnet window. The **Import Scripting File** dialog box displays. Use the dialog box's **Look In** pulldown menu to locate the file being imported.

> **Note:** If you are browsing for a file with an extension other than **.script**, be sure to select **Files of Type -> All Files** in the dialog box, as shown:

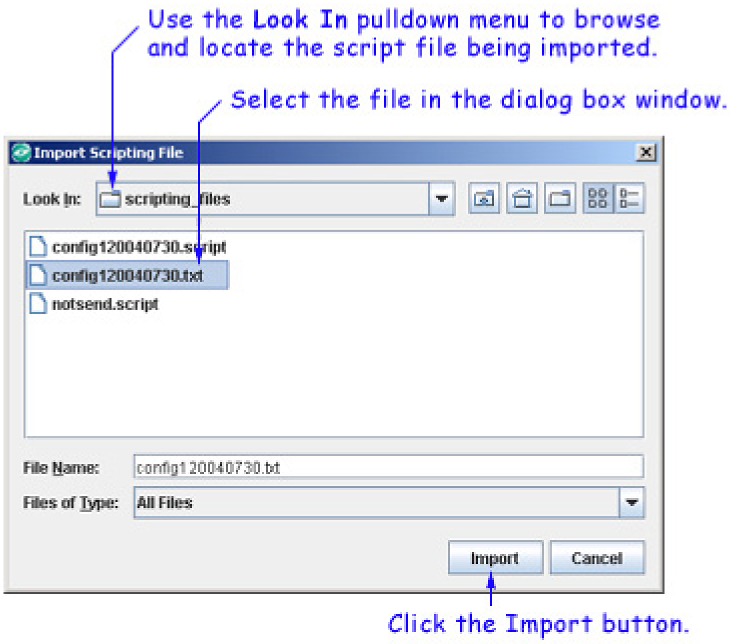

When browsing for a file with an extension other than .script (e.g., .txt), be sure All Files is selected from the Files of Type menu.

Look In: data

File Name:

Files of Type: Script Files (script)

Once the script file has been located, select the file in the dialog box window; the file name displays in the **File Name** text field. Click the **Import** button.



Use the Look In pulldown menu to browse and locate the script file being imported.

Select the file in the dialog box window.

Import Scripting File

Look In: scripting_files

config120040730.script
config120040730.txt
notsend.script

File Name: config120040730.txt

Files of Type: All Files

Click the Import button.

Note: The script import procedure is *not* complete at this point. You must click on the **Send Script** tab in the main Telnet window and follow the remaining steps in order to send the script file to the device(s).

Editing Script Files

To edit a script file, select the file from the **Filename** list, and then click **Edit**. The **Enter Scripts** text box (which was previously grayed out) becomes active. The CLI commands contained in the selected script file can now be deleted, modified, or appended. When the changes are complete, click the **Save** button.

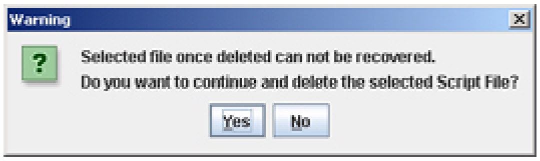
> **Note:** When the changes are saved, the previous contents of the script file are overwritten. To preserve the original contents of the file, be sure to make a backup copy before editing.

Deleting Script Files

To delete a script file, select the file from the **Filename** list, and then click **Delete**.

> **Note:** When a file is deleted, it is permanently removed from the **scripting_files** directory. Once a script file is deleted, it cannot be recovered.

Click **Yes** in the Warning dialog box:



Warning

Selected file once deleted can not be recovered.
Do you want to continue and delete the selected Script File?

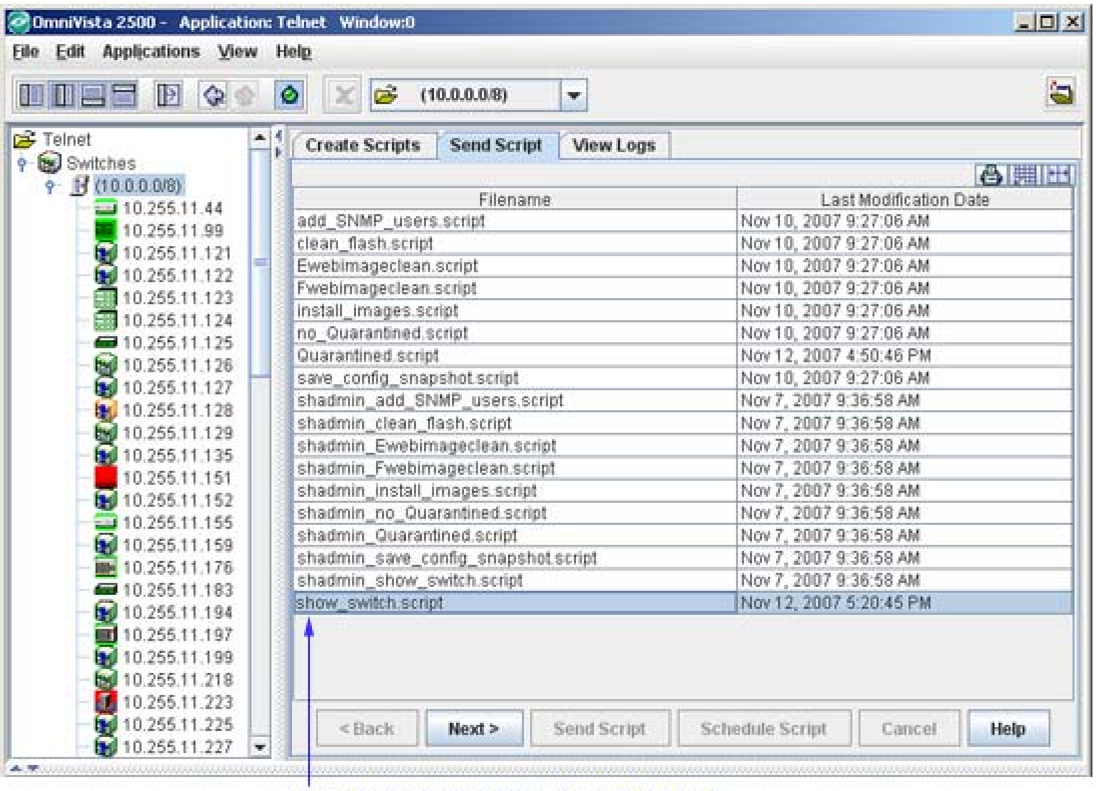
Deleting Multiple Script Files

Multiple log files can be deleted at once. To delete multiple script files, simply Control-click or Shift-click all applicable files in the list before clicking **Delete**. Remember, however, that once the files have been deleted, they cannot be recovered.

Sending Script Files

You can send a script file to a single device or multiple devices in the network. To send a script file to a device or devices, select the script file in the **Filename** column of the **Send Script** tab, then click the **Next** button.

Note: You can also schedule a script to run at a later time.

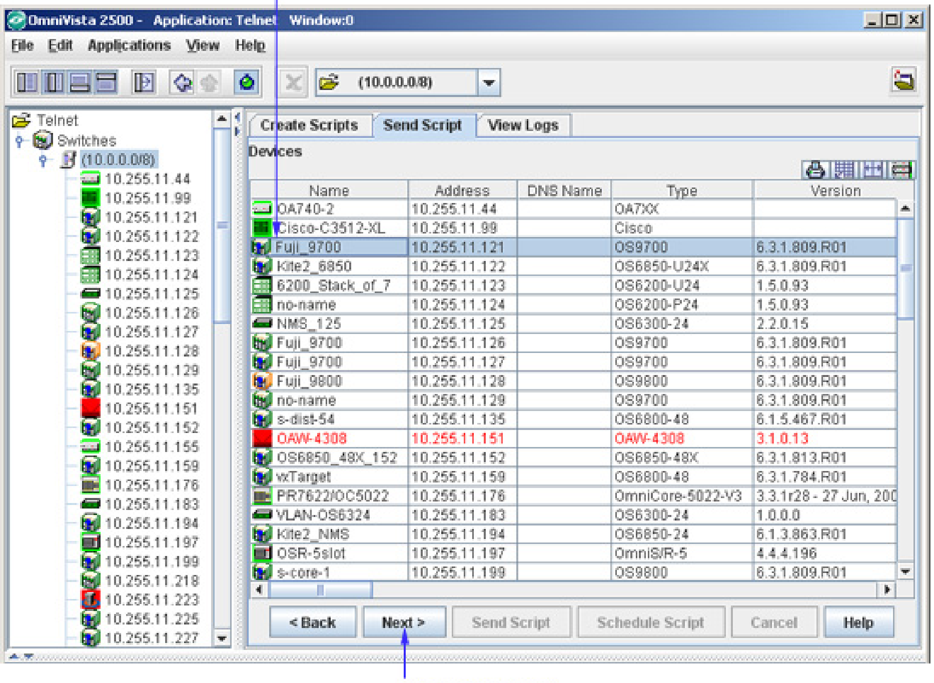


Filename	Last Modification Date
add_SNMP_users.script	Nov 10, 2007 9:27:06 AM
clean_flash.script	Nov 10, 2007 9:27:06 AM
Ewebimageclean.script	Nov 10, 2007 9:27:06 AM
Fwebimageclean.script	Nov 10, 2007 9:27:06 AM
install_images.script	Nov 10, 2007 9:27:06 AM
no_Quarantined.script	Nov 10, 2007 9:27:06 AM
Quarantined.script	Nov 12, 2007 4:50:46 PM
save_config_snapshot.script	Nov 10, 2007 9:27:06 AM
shadmin_add_SNMP_users.script	Nov 7, 2007 9:36:58 AM
shadmin_clean_flash.script	Nov 7, 2007 9:36:58 AM
shadmin_Ewebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_Fwebimageclean.script	Nov 7, 2007 9:36:58 AM
shadmin_install_images.script	Nov 7, 2007 9:36:58 AM
shadmin_no_Quarantined.script	Nov 7, 2007 9:36:58 AM
shadmin_Quarantined.script	Nov 7, 2007 9:36:58 AM
shadmin_save_config_snapshot.script	Nov 7, 2007 9:36:58 AM
shadmin_show_switch.script	Nov 7, 2007 9:36:58 AM
show_switch.script	Nov 12, 2007 5:20:45 PM

Select the script file, then click Next.

A list of discovered devices is displayed. Select the device(s) to which you want to send the script. Note that "Auto-Login" must first be configured for all devices to which a file is being sent.

Select the device(es) you want to send the script to.

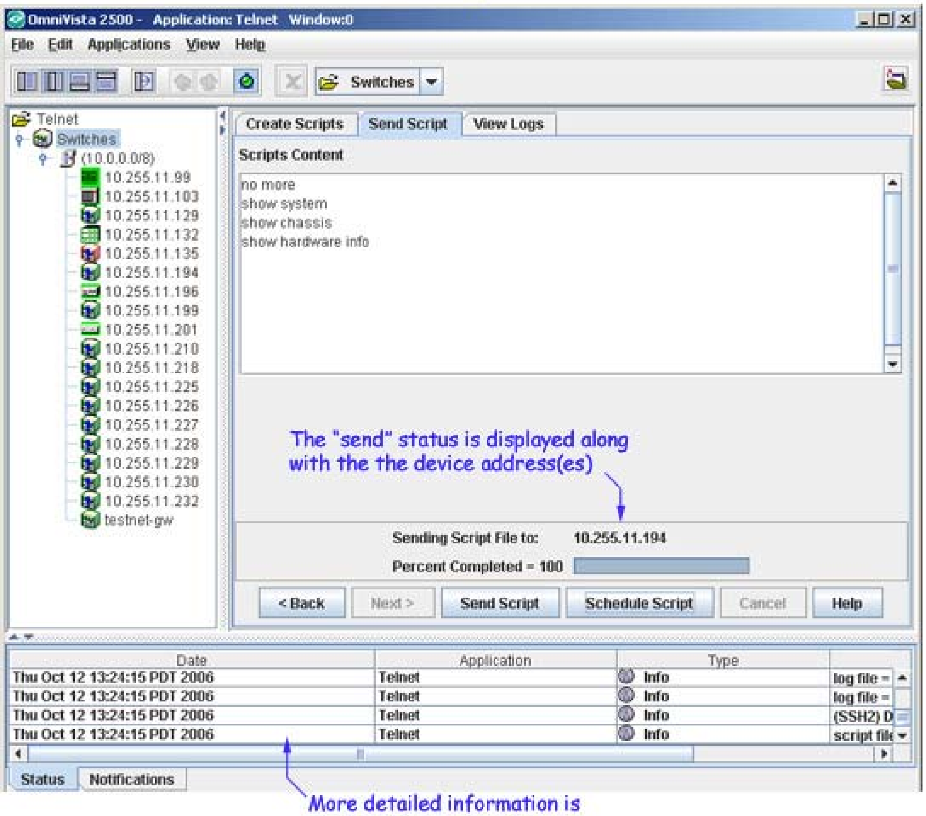


Name	Address	DNS Name	Type	Version
OA740-2	10.255.11.44		OA7XX	
Cisco-C3512-XL	10.255.11.99		Cisco	
Fuji_9700	10.255.11.121		OS9700	6.3.1.809.R01
Kite2_6850	10.255.11.122		OS6850-U24X	6.3.1.809.R01
6200_Stack_of_7	10.255.11.123		OS6200-U24	1.5.0.93
no-name	10.255.11.124		OS6200-P24	1.5.0.93
NMS_125	10.255.11.125		OS6300-24	2.2.0.15
Fuji_9700	10.255.11.126		OS9700	6.3.1.809.R01
Fuji_9700	10.255.11.127		OS9700	6.3.1.809.R01
Fuji_9800	10.255.11.128		OS9800	6.3.1.809.R01
no-name	10.255.11.129		OS9700	6.3.1.809.R01
s-dist-54	10.255.11.135		OS6800-48	6.1.5.467.R01
OAW-4308	10.255.11.151		OAW-4308	3.1.0.13
OS6850_48X_152	10.255.11.152		OS6850-48X	6.3.1.813.R01
vxTarget	10.255.11.159		OS6800-48	6.3.1.784.R01
PR7622/OC5022	10.255.11.176		OmniCore-5022-V3	3.3.1r28 - 27 Jun, 200
VLAN-OS6324	10.255.11.183		OS6300-24	1.0.0.0
Kite2_NMS	10.255.11.194		OS6850-24	6.1.3.863.R01
OSR-5slot	10.255.11.197		OmniS/R-5	4.4.4.196
s-core-1	10.255.11.199		OS9800	6.3.1.809.R01

Then click Next.

After selecting the device(s), click the **Next** button. The **Send Script Panel** is displayed:

The Send Script Panel



Scripts Content

```
no more
show system
show chassis
show hardware info
```

The "send" status is displayed along with the the device address(es)

Sending Script File to: 10.255.11.194

Percent Completed = 100

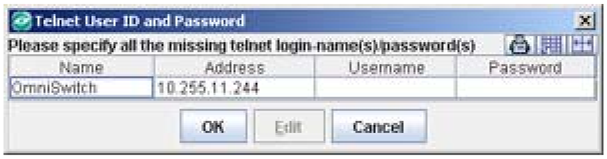
Date	Application	Type	
Thu Oct 12 13:24:15 PDT 2006	Telnet	Info	log file =
Thu Oct 12 13:24:15 PDT 2006	Telnet	Info	log file =
Thu Oct 12 13:24:15 PDT 2006	Telnet	Info	(SSH2) D
Thu Oct 12 13:24:15 PDT 2006	Telnet	Info	script file

More detailed information is displayed in the Status pane.

Click the **Send Script** button. If the selected device does not have a Telnet username/password, a dialog box will pop up to allow you to enter the Telnet username and password for the device. Enter the Telnet username and password, and then click the **OK** button.

> **Note:** The Telnet Scripting feature supports multiple devices. If the script file is to be applied to more than one device, simply **Control**-click or **Shift**-click all applicable devices in the list before clicking **Next**. Remember, however, Auto-Login must first be configured for all devices to which a file is being applied.

If the selected device is without a Telnet username/password, then a dialog box will pop up, to allow you to enter the Telnet user name and password for the device. Enter the user name and password, and then click the **OK** button to close the pop-up dialog box.

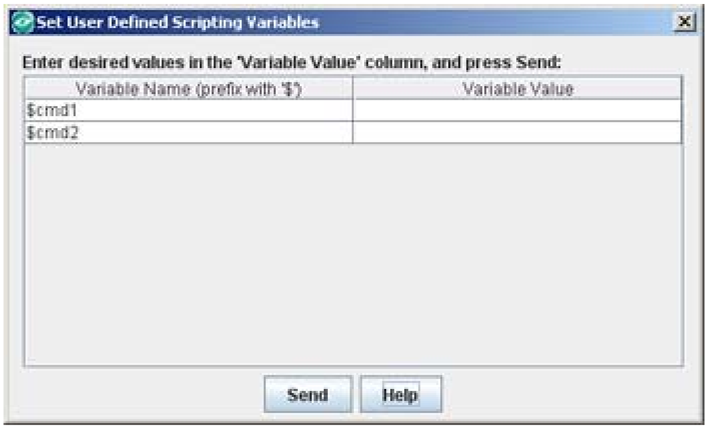


Please specify all the missing telnet login-name(s)/password(s)

Name	Address	Username	Password
OmniSwitch	10.255.11.244		

User Defined Variables

If you have specified variables within the script, the **Set User Defined Scripting Variables** window is displayed when you click on the **Send Script** button. Click in the "Variable Value" field next to the variable and enter value to be used, then click **Send**.



Enter desired values in the 'Variable Value' column, and press Send:

Variable Name (prefix with '$')	Variable Value
$cmd1	
$cmd2	

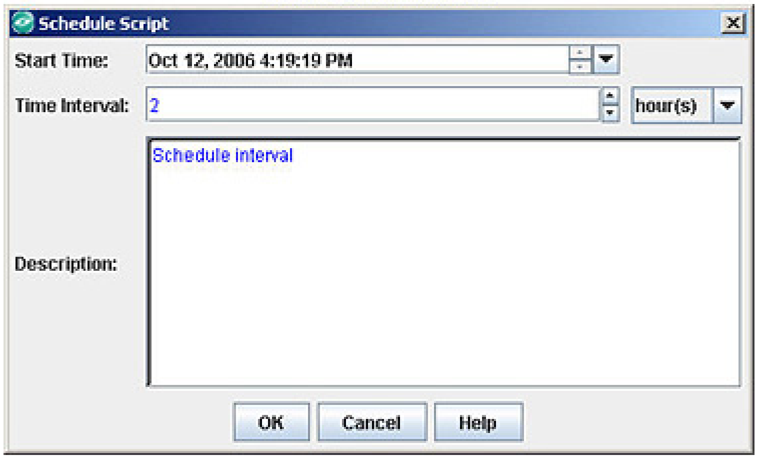
Variables must be prefixed with '$' to show they are variables. The built-in variables are:

- **$IP_ADDRESS** - replaced automatically with target switch IP address.
- **$BOOT_DIR** - replaced automatically with target boot directory (ex: working).
- **$BASE_MAC** - replaced automatically with target base MAC address.
- **$CHASSIS_TYPE** - replaced automatically with target chassis type.
- **$SYSTEM_OID** - replaced automatically with target unique object ID.
- **$LOGIN_ID** - replaced automatically with target FTP/Telnet login ID.
- **$LOGIN_PWD** - replaced automatically with target FTP/Telnet login password.
- **$READ_PWD** - replaced automatically with target community string for SNMP reading.
- **$WRITE_PWD** - replaced automatically with target community string for SNMP writing.

Scheduling a Script

OmniVista allows you to schedule scripts to run at a later time. You can schedule a script to run a single time, or schedule the script to run at regular intervals. To schedule a script to run at a later time, click the **Schedule Script** button at the bottom of the **Send Script** tab. The **Schedule Script** window appears.

Schedule Window



Start Time: Oct 12, 2006 4:19:19 PM

Time Interval: 2 hour(s)

Description: Schedule interval

Enter the date and time for the script to run in the **Start Time** field. To run the script just once, leave the **Time Interval** field black and click the **OK** button. To run the script at regular intervals, enter a value in the **Time Interval** field, and select a time period from the drop-down menu to the right (e.g., Hours, Days, Weeks), then click the **OK** button.

Note: If a time interval is not specified, there will not be any recurrence by default. To view, reschedule, or remove a scheduled job, use the **Schedule** application. Results from the running of a scheduled script are written to the Telnet Log.

Tips for Sending Scripts

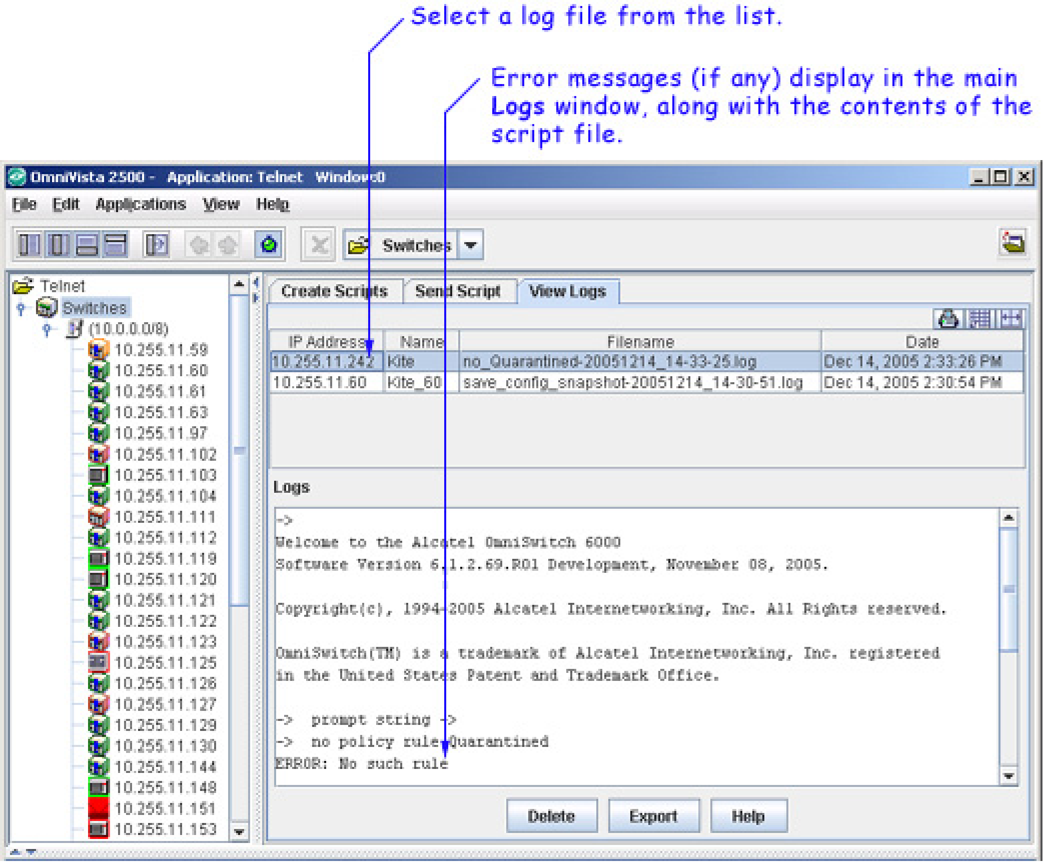
If the file is not successfully applied ("Percent Completed" does not reach 100), check the Status Pane at the bottom of the main Telnet window for troubleshooting information. The most common error when trying to apply a file is missing login information. This can be corrected by configuring Auto-Login for the device. Status information for each of the CLI commands applied can be viewed by clicking the **View Logs** tab in the main Telnet window.

> **Important Note:** Changes made to a device using a script file are applied only to the device's *running memory* (i.e., RAM). If the device reboots or goes down unexpectedly, any unsaved changes will be lost. To save changes to the device's Working directory, you must either use the OmniVista Topology application or type **write memory** at the Telnet session command prompt. To save changes using the Topology application, right-click the device from the main Topology window and select **Save to Working** from the pop-up menu. If multiple devices have been configured using the script file, be sure to save changes for each device.

Viewing Log Files

The **View Logs** tab allows users, on a command-by-command basis, to view Telnet Scripting results. In other words, it displays whether the contents of a file were successfully applied to the device. A log file also provides a record of a particular configuration, as well as effective troubleshooting information, when applicable.

Unless an error has occurred, the log file will closely resemble the script file (i.e., it will list only the CLI commands that were applied to the device). If an error occurs, an error notification is displayed in the log, following the CLI command that triggered the error. For more information, see the example below:



Select a log file from the list.

Error messages (if any) display in the main Logs window, along with the contents of the script file.

IP Address	Name	Filename	Date
10.255.11.242	Kite	no_Quarantined-20051214_14-33-25.log	Dec 14, 2005 2:33:26 PM
10.255.11.60	Kite_60	save_config_snapshot-20051214_14-30-51.log	Dec 14, 2005 2:30:54 PM

```
->
Welcome to the Alcatel OmniSwitch 6000
Software Version 6.1.2.69.R01 Development, November 08, 2005.

Copyright(c), 1994-2005 Alcatel Internetworking, Inc. All Rights reserved.

OmniSwitch(TM) is a trademark of Alcatel Internetworking, Inc. registered
in the United States Patent and Trademark Office.

->  prompt string ->
->  no policy rule Quarantined
ERROR: No such rule
```

As with the scripting files, log files are automatically stored on the server or local system. File locations may vary, depending on the OmniVista installation, but can generally be found at a path similar to the following:

Alcatel OmniVista 2500\data\telnet\scripting_logs

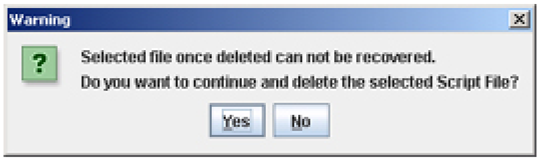
Note: By default, log files are placed in a directory indicating the IP address of the corresponding device.

Deleting Log Files

To delete a log file, select the file from the **Filename** list, and then click **Delete**.

> **Note:** When a file is deleted, it is permanently removed from the **scripting_logs** directory. Once a log file is deleted, it cannot be recovered.

Click **Yes** in the **Warning** dialog box.



Warning

Selected file once deleted can not be recovered.
Do you want to continue and delete the selected Script File?

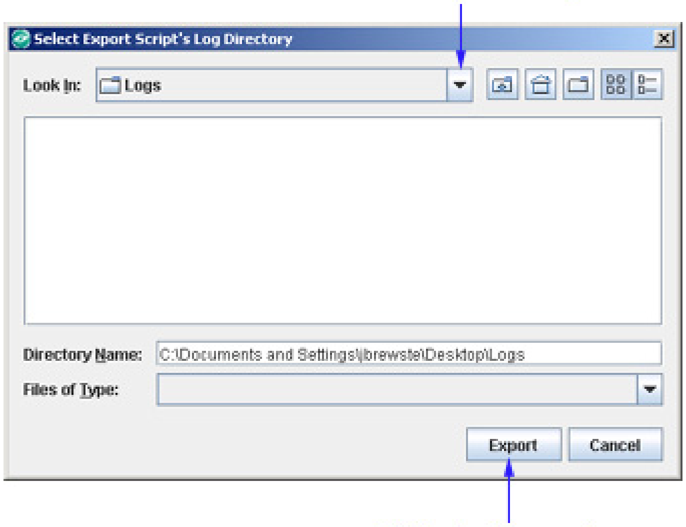
Deleting Multiple Log Files

Multiple log files can be deleted at once. To delete multiple log files, simply Control-click or Shift-click all applicable files in the list before clicking **Delete**. However, remember that once the files have been deleted, they cannot be recovered.

Exporting Log Files

To export a log file, select the file from the **Filename** list, and then click **Export**. A dialog box will be displayed. This dialog box will help you export the selected log file to a directory of your choice.

Use the **Look In** pulldown menu to browse and locate the Log file.



Select Export Script's Log Directory

Look In: Logs

Directory Name: C:\Documents and Settings\jbrewste\Desktop\Logs

Files of Type:

Click the **Export** button.