

Getting Started with SecureView SA

The SecureView SA application provides a way to manage user access to multiple AOS switches. SecureView SA does this by enabling a network manager to configure Authenticated Switch Access for AOS switches. The Authenticated Switch Access feature authenticates users into a switch so that they can manage it. In contrast, the Authenticated VLANs feature authenticates users through the switch and out to a subnet.

Note: Even though user databases for both Authenticated Switch Access and Authenticated VLANs may be located on the same authentication server, the two features are independent. SecureView SA can be used to configure Authenticated Switch Access only. SecureView SA cannot be used to configure Authenticated VLANs.

Users can access AOS switches through several different interfaces:

- **Switch Console Port** - A direct connection to the switch console port can be established.
- **Telnet** - Any standard Telnet client may be used for logging into the switch. OmniVista's Telnet application enables you to establish Telnet sessions with switches.
- **HTTP** - The switch has a Web Browser management interface, WebView, which uses HTTP to access the switch.
- **FTP** - Any standard FTP client may be used for logging into the switch.
- **Secure Shell** - Any standard Secure Shell client may be used for logging into the switch. OmniVista's Telnet application enables you to establish Secure Shell (SSH) sessions with qualified switches.
- **SNMP** - Any standard SNMP browser may be used for logging into the switch. OmniVista uses SNMP to access switches.

A switch can be configured to allow or deny user access through any of these interfaces. A switch can also be configured to allow user access through one or more interfaces and to allow or deny that user the ability to read or write specific areas of the switch configuration. When a user logs into a switch, the switch "authenticates" the user by checking that the user has the right to access the switch via the interface used and determining what rights the user has to read or write the switch configuration.

By default, users are allowed to access a switch by connecting to its console port, and the switch's local user database is queried to determine the read/write privileges available to that user. However, user access and read/write privileges may be configured on external servers instead of the switch's local user database. (The exception is end-user profiles, which may only be configured on the switch). Such external servers are referred to as authentication servers, or AAA servers (authentication, authorization, and accounting). Authentication servers are used for storing information about users who want to manage the switch (for Authenticated Switch Access) and users who need access to a particular VLAN or VLANs (for Authenticated VLANs).

Authentication Servers

You can use an LDAP, RADIUS, ACE, or TACACS+ server as an external authentication server for Authenticated Switch Access to AOS switches. You can also use an LDAP, RADIUS, or a TACACS+ server as an external accounting server. However, only LDAP servers, TACACS+ servers or the local switch database can be used to authenticate SNMP access. RADIUS, LDAP, and TACACS+ servers can also be used for Authenticated VLANs (but not ACE servers). The following table summarizes how each type of server may be used.

How Different Authentication Servers Can Be Used

Server Type	Authenticated Switch Access	Authenticated VLANs
LDAP	Yes, including SNMP	Yes
RADIUS	Yes, except SNMP	Yes
ACE	Yes, except SNMP	No
TACACS+	Yes, including SNMP	Yes

Note that RADIUS and ACE servers do not support SNMP. However, OmniVista uses SNMP to manage switches. For this reason, if you specify a RADIUS, ACE, or TACACS+ server for Authenticated Switch Access, SecureView SA will require you to specify a second server for SNMP authentication.

The OmniVista LDAP Server

The OmniVista LDAP server is automatically installed along with SecureView SA. The OmniVista LDAP server is ready to use when installed and requires no user configuration. It is installed with the appropriate database schema for managing AOS switches. SecureView SA's One Touch mode enables you to easily create, modify, and delete users and user privileges in the OmniVista LDAP server.

Other Authentication Servers

If you wish to use an LDAP server other than the OmniVista LDAP server, a RADIUS server, an ACE server, or a TACACS+ server, you must install the server, configure it, and create all the users and user privileges on the server (if applicable) outside OmniVista. You must explicitly "add" such servers to OmniVista using SecureView SA's Expert mode. You can then use the Expert mode to assign switches to the servers.

Note: SecureView SA does not enable you to configure user accounts on any server other than the OmniVista LDAP server.

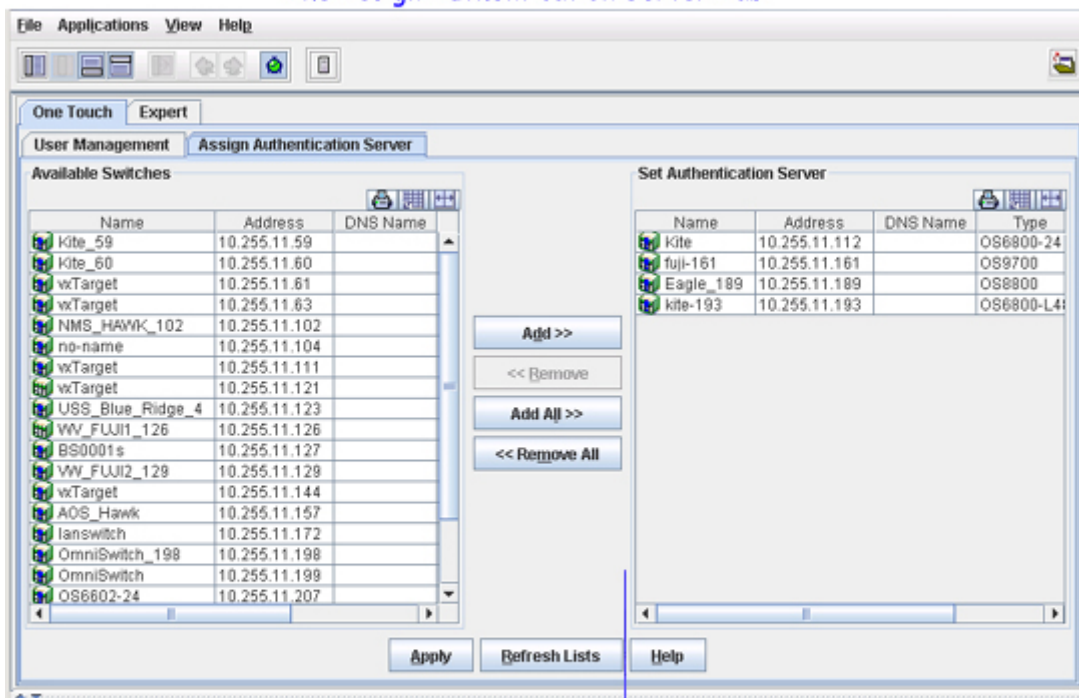
One Touch Mode

SecureView SA's One Touch mode makes configuring Authenticated Switch Access easy. The One Touch mode enables you to assign the OmniVista LDAP server or the switch local database for authentication. The One Touch mode does not allow you to assign other authentication servers. You can use the Expert mode if you need to use a server other than the OmniVista LDAP server or the local database.

Assigning Switches to the OmniVista LDAP Server

The One Touch mode's **Assign Authentication Server** tab, shown below, enables you to assign AOS switches to the OmniVista LDAP server for authentication. The **Available Switches** panel lists all the switches that are capable of using an authentication server. Select switches in this panel and move them to the **Set Authentication Server** panel. When you click the **Apply** button, all switches listed in the **Set Authentication Server** panel will be assigned to the OmniVista LDAP server for authentication of all switch access modes: FTP access, Telnet access, switch console access, SSH access, HTTP access, and SNMP access.

One Touch Mode
The Assign Authentication Server Tab

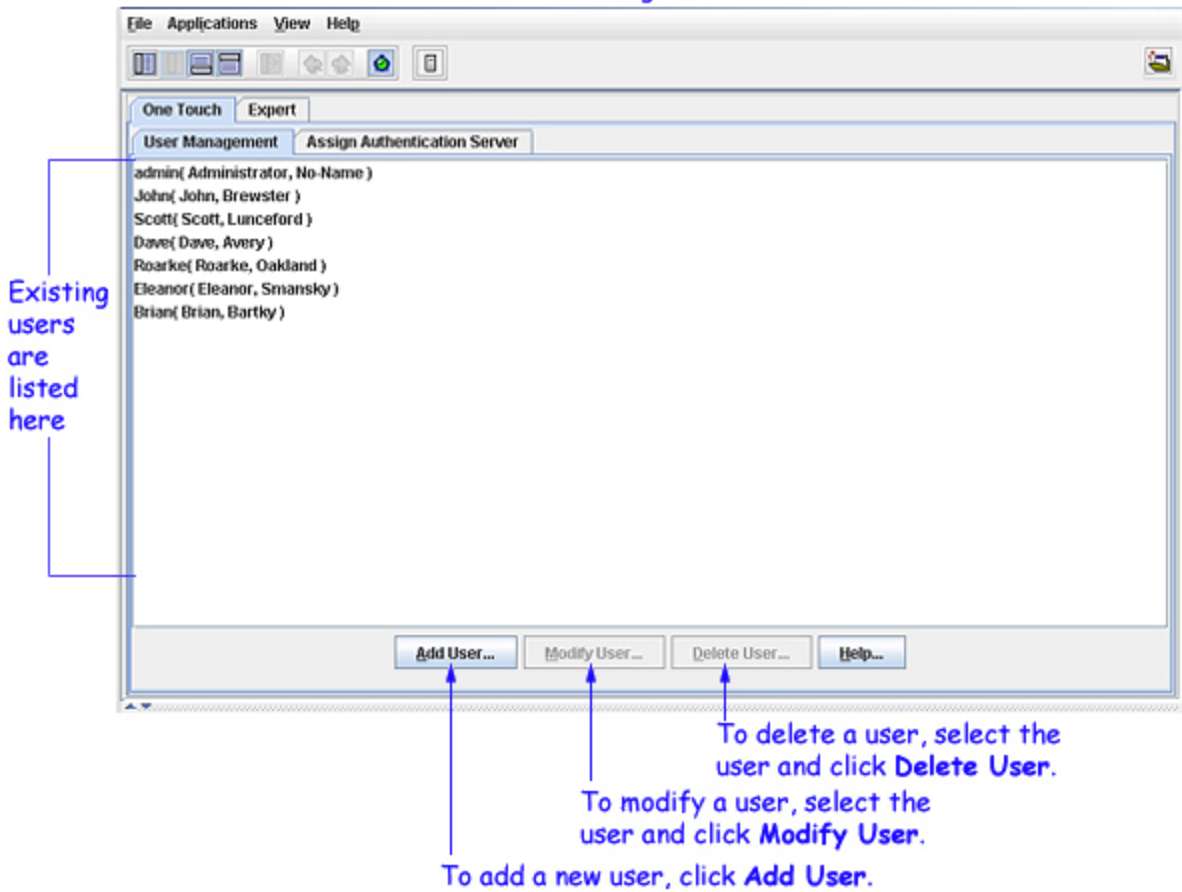


When **Apply** is clicked, all switches listed here will be assigned to the OmniVista server for authentication of all switch access modes.

Managing Users

The One Touch mode's **User Management** tab, shown below, lists all the existing users in the OmniVista LDAP server database and enables you to create, modify, and delete users within the OmniVista LDAP server database.

One Touch Mode
The User Management Tab



Adding a New User

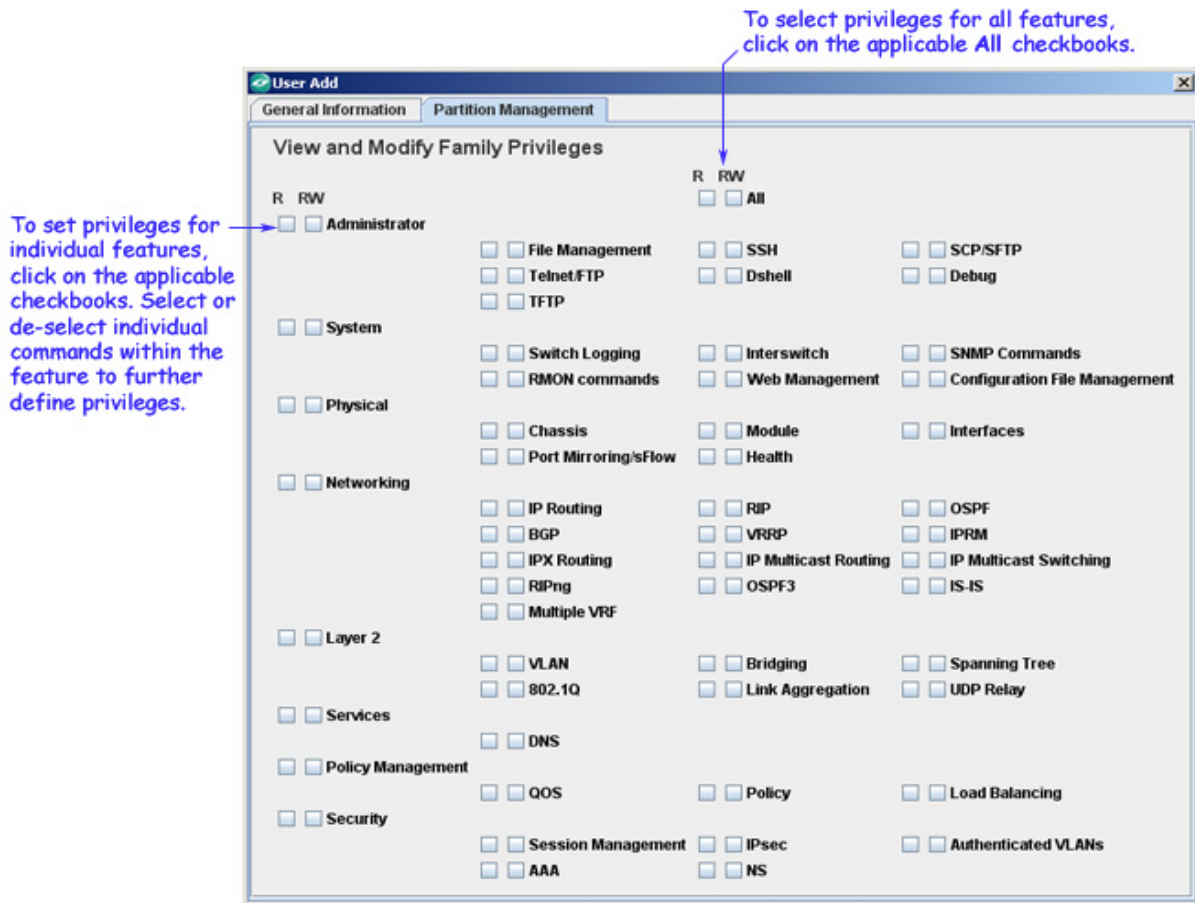
To add a new user in the One Touch mode, click the **Add User...** button in the **User Management** tab, as shown in the screen above. The **User Add** window is displayed. The **User Add** window has two tabs, **General Information** and **Partition Management**. The **General Information** tab, shown below, enables you to specify general information about a new user, including the type and version of SNMP available to the user and the time periods when the user is allowed to access switches.

The General Information Tab

The screenshot shows the 'User Add' dialog box with the 'General Information' tab selected. The 'Partition Management' tab is also visible. The 'General Information' section includes fields for 'User Name:', 'EUPM Profile Name:', 'Password:', 'Confirm Password:', 'First Name:', and 'Last Name:'. The 'SNMP Level' is set to 'No SNMP Access'. The 'Allowed Time' section is expanded, showing 'Allowed Date' with 'All Dates' checked and date pickers for 'Start Date' and 'End Date' (both set to 'Nov 30, 2005'). The 'Allowed Time' section has 'All Day' checked and time pickers for 'Start Time' and 'End Time' (both set to '04:47:44 PM'). The 'Allowed Days' section has 'All Week' checked and checkboxes for 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Sun'. A 'Description:' text area is at the bottom. At the very bottom are 'Apply', 'Cancel', and 'Help' buttons.

The **Partition Management** tab of the **User Add** window, shown below, enables you to define the switch access rights for the new user. You can define access for all command "families", selected command families, or individual commands within a family. (This is usually termed partitioned management.) For example, you can enable read/write access for all command families, or the Administrator command family only, or File Management commands only within the Administrator family of commands. For more information on the **Partition Management** tab go to "Adding or Modifying a User: Partition Management" on page 17.

Defining a User's Switch Access Rights



Expert Mode

In the One Touch mode, you are restricted to use the default OmniVista LDAP server for authentication. In the Expert mode, you can use any LDAP V3, RADIUS, ACE, or TACACS+ server for authentication. You can also use any LDAP V3, RADIUS, or TACACS+ server for accounting. However, the Expert mode does not allow you to manage users on such servers and all user accounts must be set up outside OmniVista. Unlike the One Touch mode, which allows you to specify only the single default authentication server, the Expert mode enables you to specify a primary server, a backup primary server, a secondary server, a backup secondary server, and a default server, each of which is tried in precedence order.

The Expert mode enables you to selectively allow or disallow individual types of switch access also. FTP, Telnet, switch console, SSH, and HTTP access to switches can be individually allowed or disallowed. However, in normal Expert mode all switch access types must be authenticated by the same server. For example, you cannot assign Telnet access to a RADIUS server and HTTP access to an LDAP server.

The Expert mode includes a special customization feature also that does allow you to take advantage of the full flexibility of the switch and individually assign each switch access mode to a different authentication server.

Note that assignments made in the Expert mode will override those made in the One Touch mode.

Managing Authentication Servers

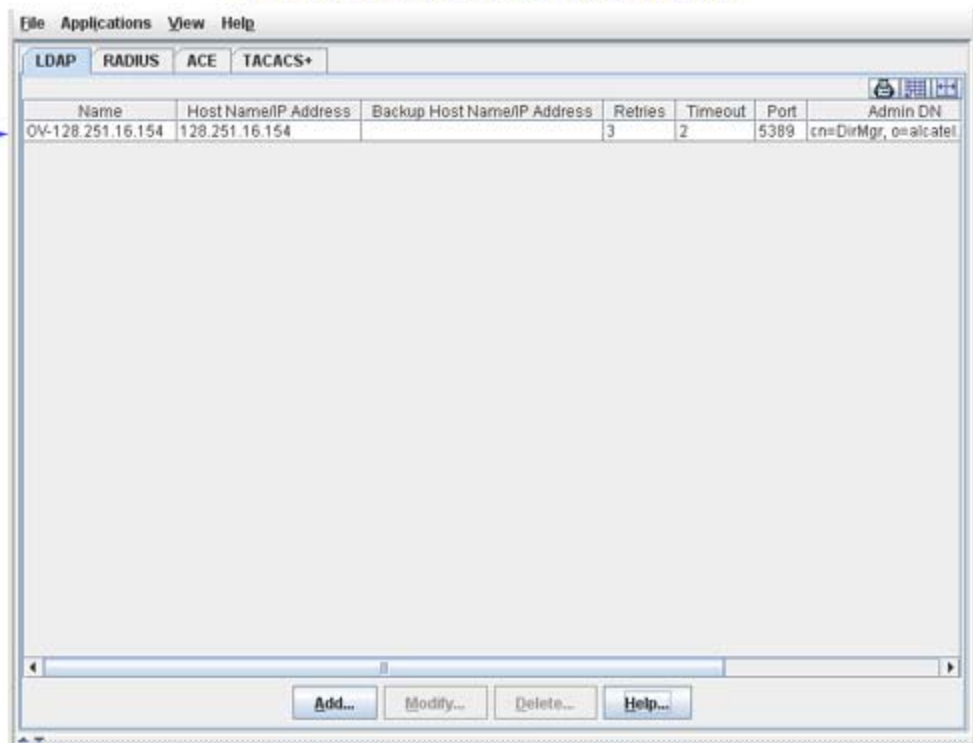
Any authentication server that you want to use, other than the default OmniVista LDAP server, must be added to OmniVista. Adding a server to OmniVista basically informs OmniVista that the server exists. OmniVista does not search the network to locate available authentication servers, so any server that you add to OmniVista should actually exist (or should exist in the near future).

To view the list of known authentication servers, click the **Config Auth Servers...** button. The **Authentication Servers** window is displayed. This window enables you to add, modify, and delete such servers. (The exception is an ACE server, which cannot be modified from OmniVista). When you add a server to OmniVista, you have the option of specifying a backup server that will be tried if the server becomes unavailable. (Again, the ACE server is an exception.) To add a server to OmniVista, click the **Add...** button at the bottom of the respective sub-tab. For more information on adding an Authentication Server, see the Authentication Servers application help.

Note: You must assign a unique name to each Authentication Server that you add to OmniVista. You cannot, for example, have an LDAP server named Server 1 and a RADIUS server named Server 1. (Again, the ACE server is an exception. The single ACE server you can add to OmniVista is always assigned the default name **ace**.)

The Authentication Servers Window

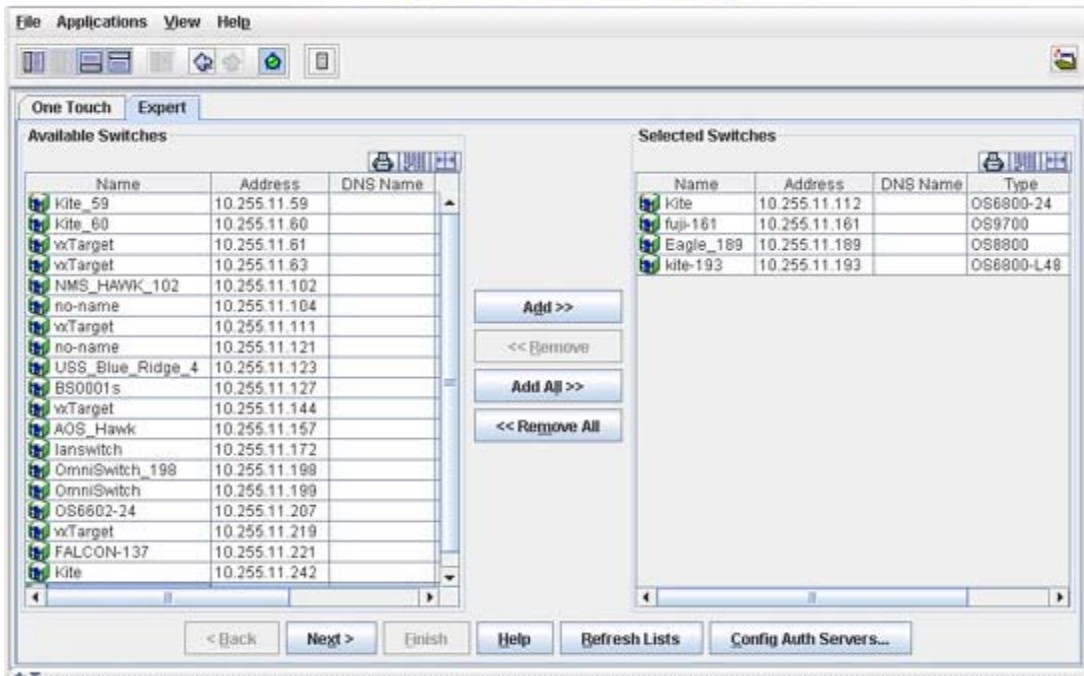
The OmniVista LDAP Server is provided by default. It cannot be deleted. →



Assigning Servers

The Expert mode has a wizard that enables you to select the switches from the **Available Switches** table, that you need to assign to authentication servers and accounting servers, and define the type(s) of switch access that the server will authenticate. The first screen of the Expert mode wizard, shown below, enables you to select the switches that you want to assign to an authentication server and accounting server. (Note that only AOS switches are displayed. SecureView SA does not support XOS switches.)

The Expert Mode Wizard - Page 1



The second screen of the Expert mode wizard, shown below, enables you to assign all the switches that you selected to a primary authentication server and, optionally, to a secondary authentication server, which will be used if the primary server is unavailable. It also enables you to define the default authentication for the selected switches as the local database or as no authentication.

The Expert Mode Wizard - Page 2

The switches selected for assignment

Name	Address	DNS Name	Type	Version	Backup Date	Backup Version	Last Known Up At
Kite	10.255.11.112		OS6800-24	6.1.2.74.R01			Nov 28, 2005 11:55:56 AM
Fuji-161	10.255.11.161		OS9700	6.1.2.90.R01			Nov 28, 2005 11:55:56 AM
Eagle_189	10.255.11.189		OS8800	5.1.6.87.R02			Nov 28, 2005 11:55:56 AM
Kite-193	10.255.11.193		OS6800-L48	5.3.1.7.R04			Nov 28, 2005 11:55:56 AM

These fields enable you to select the primary, secondary, and default authentication servers for the switches listed above

Select Authentication Server

Primary Authentication Server: OV-128.251.19.48

Secondary Authentication Server: local

default: local None

< Back Next > Finish Help

The third screen of the Expert mode wizard, shown below, enables you to assign all the switches that you selected to a primary accounting server and, optionally, to a secondary accounting server, which will be used if the primary server is unavailable. It also enables you to define the default accounting for the selected switches as the local database or as no accounting.

The Expert Mode Wizard - Page 3

The switches selected for assignment

Name	Address	DNS Name	Type	Version	Backup Date	Backup Version	Last Known Up At
Kite	10.255.11.112		OS6800-24	6.1.2.74.R01			Nov 28, 2005 11:55:56 AM
Fuji-161	10.255.11.161		OS9700	6.1.2.90.R01			Nov 28, 2005 11:55:56 AM
Eagle_189	10.255.11.189		OS8800	5.1.6.87.R02			Nov 28, 2005 11:55:56 AM
Kite-193	10.255.11.193		OS6800-L48	5.3.1.7.R04			Nov 28, 2005 11:55:56 AM

These fields enable you to select primary, and secondary accounting servers for the switches listed above

Select Accounting Server

Primary Accounting Server: OV-128.251.19.48

Secondary Accounting Server: local

< Back Next > Finish Help

The final screen of the Expert mode wizard, shown below, enables you to specify the type(s) of switch access that you want the servers you specified on the previous pages to allow,

authenticate, and account for the selected switches. When your selections are made, click the **Finish** button to apply your selections and server assignments to the selected switches.

The Expert Mode Wizard - Page 4

The switches selected for assignment

Name	Address	DNS Name	Type	Version	Backup Date	Backup Version	Last Known Up At
Kite	10.255.11.112		OS6800-24	6.1.2.74.R01			Nov 28, 2005 11:55:56 AM
fuji-161	10.255.11.161		OS9700	6.1.2.90.R01			Nov 28, 2005 11:55:56 AM
Eagle_189	10.255.11.189		OS8800	5.1.6.87.R02			Nov 28, 2005 11:55:56 AM
kite-193	10.255.11.193		OS6800-L48	5.3.1.7.R04			Nov 28, 2005 11:55:56 AM

A check means the corresponding switch access will be allowed and authenticated by the server(s) specified on the previous screen

Set Switch Access

- Allow FTP Access
- Allow Telnet Access
- Allow Console Access
- Allow SSH Access
- Allow HTTP Access

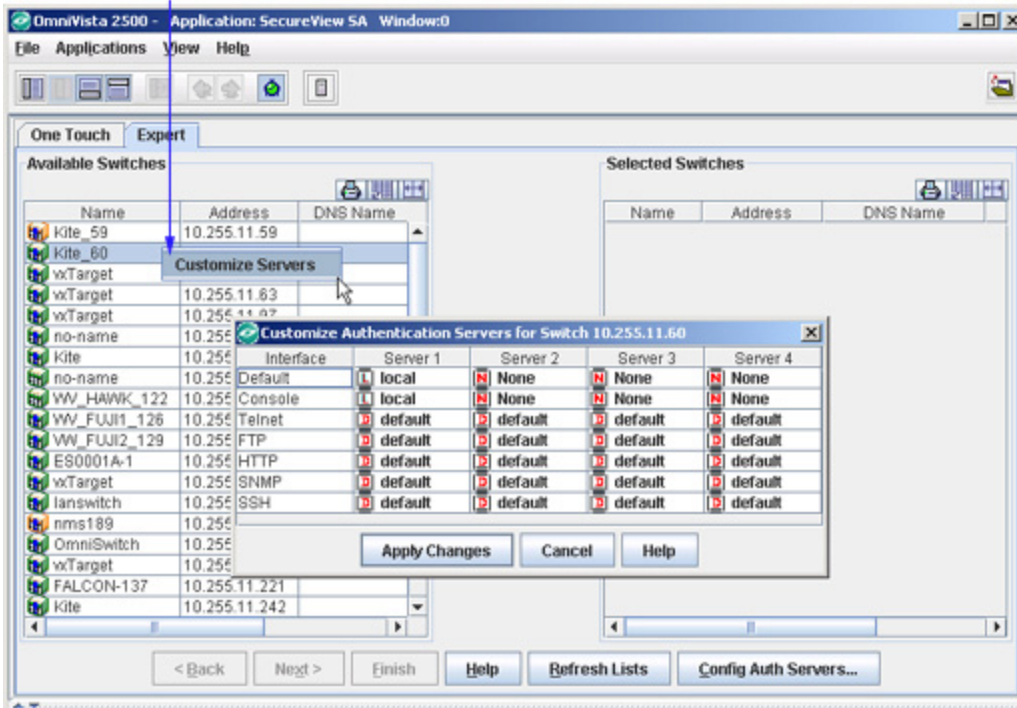
Note
SNMP access is always allowed.

< Back Next > Finish Help

Assigning Individual Access Modes to Different Servers

The One Touch mode always uses the default OmniVista LDAP server to authenticate all types of switch access. The Expert mode can use an LDAP, RADIUS, ACE, or TACACS+ server to authenticate all types of switch access. In contrast, the **Customize Authentication Servers** window makes it possible to take advantage of the full flexibility of the switch and individually assign each switch access mode to a different authentication server. The **Customize Authentication Servers** window also makes it possible to assign up to four authentication servers to each access mode (each with its own backup server with each server to be tried in order of precedence. Display the **Customize Authentication Servers** window as explained below.

1. Display Expert mode tab.
2. Click right on the switch displayed in the Available Switches panel. The **Customize Servers** menu item displays. Click on **Customize Servers** to display the **Customize Authentication Servers** window for the selected switch.



The **Customize Authentication Servers** window lists each switch access mode to its left. To assign a server, left-click in the respective field to display a drop-down box listing all the authentication servers known to OmniVista. Set each field to the desired server. Note that setting Server 1 to **None** for any access mode will turn off all access to that mode.

Click left in each field to display a combo box listing all known servers. Set each field to the desired server.



Using One Touch Mode

The One Touch mode uses the bundled OmniVista LDAP server to authenticate switch access. The OmniVista LDAP server is automatically installed along with **SecureView SA**. Since OmniVista knows the server's location and the server is installed with the appropriate database schema, there is no need for the user to configure this server. It is ready to use when installed. When you assign a switch to the OmniVista LDAP server, you are assigning all switch access modes to the server for authentication: FTP access, Telnet access, switch console access, SSH access, HTTP access, and SNMP access.

The One Touch mode provides two tabs that enable you to assign switches to the OmniVista LDAP server and set up user accounts on the server, respectively.

- The **Assign Authentication Server** tab, shown below, enables you to assign desired switches to the OmniVista LDAP server for authentication. This tab is described below.
- The **User Management** tab enables you to create users and specify their switch access rights, modify users and their access rights, and delete users. All users that you create or modify are written directly to the OmniVista LDAP server's database.

To use the One Touch mode, you can either assign switches to the server and then set up users, or you can set up users and then assign switches to the server. However, note that once you assign a switch to the server, only authorized users (i.e., users in the server's database) will be able to access the switch. If you set up users first, and then assign switches to the server, the users that you defined will be able to access the switches you assign immediately.

Assigning Switches to Servers

The **Assign Authentication Server** tab, shown below, enables you to assign switches to the OmniVista LDAP server for authentication of all the switch access modes. The **Set Authentication Server** panel lists all switches that are currently assigned to the OmniVista LDAP server for authentication. The **Available Switches** panel lists all the switches that are capable of using an authentication server. These switches may be currently assigned to the default local database for authentication, or they may have been assigned to other authentication servers via SecureView SA's Expert mode, WebView, or the CLI.

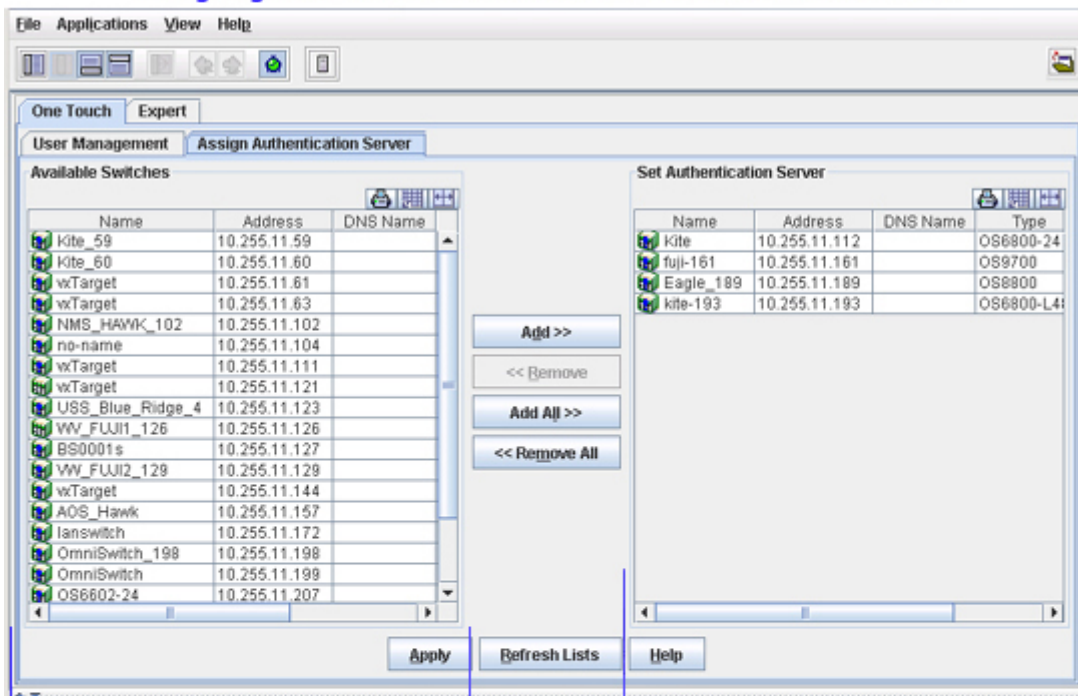
To assign switches to the OmniVista LDAP server for authentication, follow the steps below.

1. Select the desired switches in the **Available Switches** table, which you want to assign to the OmniVista LDAP server and move them to the **Set Authentication Server** table using the **<Add>** or **<Add All>** buttons. To select a switch, click it. You can select multiple contiguous switches by **Shift**-clicking and multiple non-contiguous devices by **Ctrl**-clicking. Click **Refresh Lists** to update lists with the currently active switches. For example, if a particular switch is off-line, it will not be added to the list until you click the **Refresh Lists** button.

Note: If a switch is currently assigned to the OmniVista server for authentication and is listed in the **Set Authentication Server** table, you can reassign it to the local database for authentication by selecting the switch in the **Set Authentication Server** table and moving it to the **Available Switches** table before you click **Apply**.

2. Click the **Apply** button. All switches in the **Set Authentication Server** table are assigned to the OmniVista LDAP server for authentication of all switch access modes. Any switch that is moved from the **Set Authentication Server** table to the **Available Switches** table is reassigned to the local database for authentication. Server assignments for all other switches listed in the **Available Switches** window are left as is.

One Touch Mode Assigning Switches to the OmniVista Authentication Server



When **Apply** is clicked, any switch that was moved here from the "Set Authentication Server" window will be reassigned to the local database for authentication of all switch access modes.

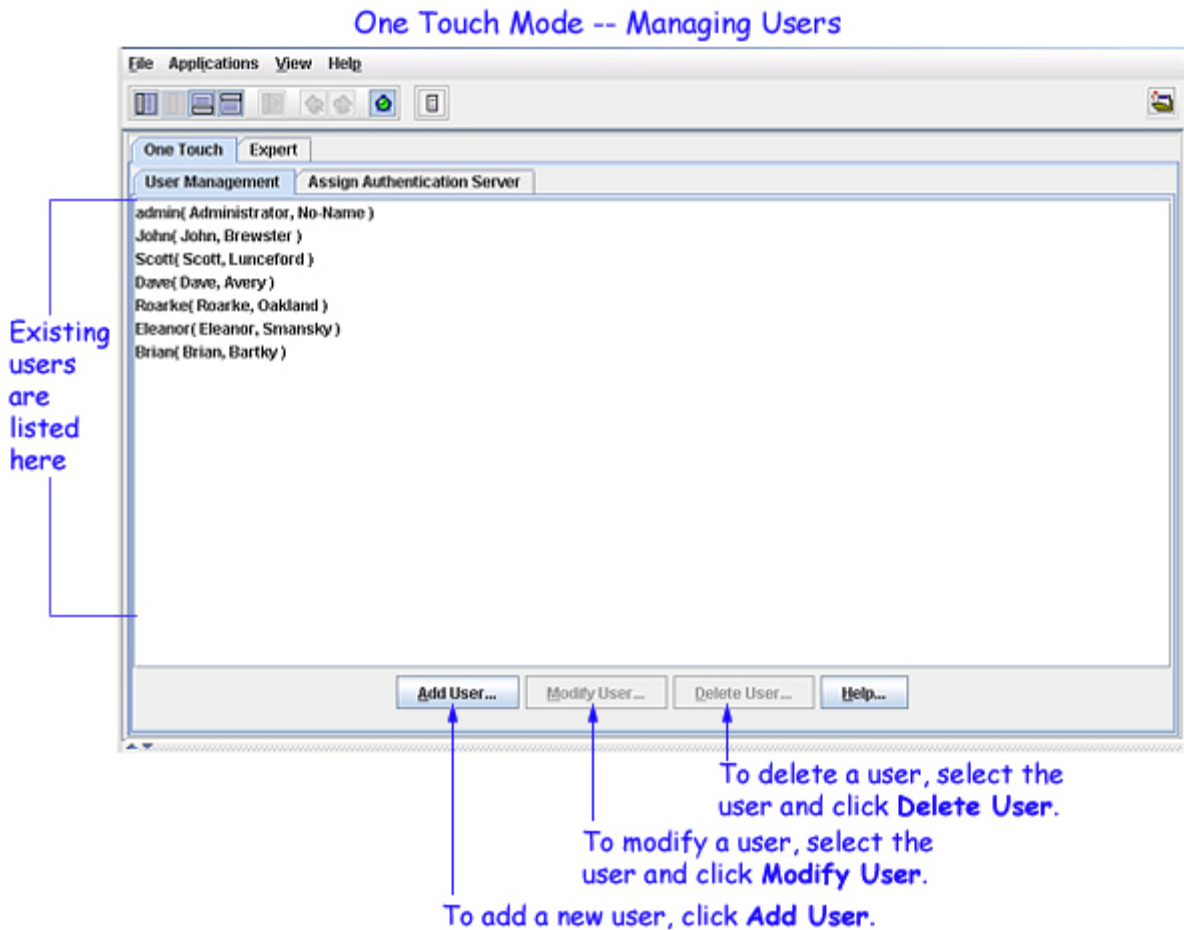
Server assignments for all other switches listed here (i.e., switches that were not moved from the "Set Authentication Server" window) will be left as is.

When **Apply** is clicked, all switches listed in the "Set Authentication Server" window will be assigned to the OmniVista server for authentication of all switch access modes.

Managing Users in One Touch Mode

The **User Management** tab in the One Touch mode, shown below, lists all users that are currently defined in the OmniVista LDAP authentication server. The **User Management** tab also enables you to add, modify, and delete users in the OmniVista LDAP authentication server.

- To add a new user, click the **Add User...** button.
- To modify an existing user, select the user and click the **Modify User...** button.
- To delete a user, select the user and click **Delete User...** button. You are asked to confirm the delete before it is performed. Note that deleting a user deletes all the information about the user from the OmniVista LDAP server database. Once the delete operation has been confirmed, there is no way to restore the deleted user (other than manually reentering the user information).



Adding or Modifying a User: General Information

The **General Information** tab of the **User Add** window enables you to specify general information about a new user, including type and version of SNMP available to the user and the time periods when the user is allowed to access switches. Each field is described below. When you complete all the fields, click the **Apply** button to write the information to the OmniVista server.

Note: The **General Information** tab includes fields that enable you to define the dates, times of day, and days of the week that the user can access switches. These fields reference the date and time as set **on the switch**. If a switch is set to the wrong date or time, authentication will not function in the expected manner.

Defining General User Information

General Information Fields

User Name

Enter a unique name to identify this user. This is the name that the user will enter to log in when accessing the switch via the console port, Telnet, SSH, FTP, HTTP (WebView), or SNMP (OmniVista). The user name should be between 1 - 31 characters in length.

EUPM Profile Name

If the user name specified above is associated with an end-user profile on the switch, enter the name of the profile in this field. End-user profiles determine access to specified command areas, and are attached to user login accounts. End-user profiles are configured and attached to user logins directly on the switch. See the *OmniSwitch 6800/7700/7800/8800/9000 Switch Management Guide* for more information on end-user profiles.

Note: If the user name specified above is associated with an end-user profile on the switch, and the name of the profile is not entered in this field, the user login fails.

Password

Enter the password for the user name defined above. The password should be between 1 - 47 characters in length.

Confirm Password

Enter the password defined above a second time for confirmation. If the two entries do not match you will receive a warning message and be prompted to reenter the passwords.

First Name

Enter the user's first name. This field is provided to make it easier for administrators to identify users, and the given name is stored on the server. The switch does not use this field.

Last Name

Enter the user's last name. This field is provided to make it easier for administrators to identify users, and the surname is stored on the server. The switch does not use this field.

SNMP Level

Set this drop-down box to specify the type and version of SNMP available to the user and the authentication and encryption scheme to be used for SNMP Version 3 access (if used).

MD5 (or HMAC-MD5-96) and SHA (or HMAC-SHA-96) are the two authentication protocols that have been defined for SNMP Version 3. Authentication uses a "secret key" to produce a "fingerprint" of the message. The fingerprint is included within the message. The device that receives the message uses the same secret key to validate that the fingerprint is correct. If it is, and if the message was received in a timely manner, then the message is considered authenticated. Otherwise, the message is discarded. The fingerprint is called a Message Authentication Code, or MAC. The MD5 and SHA authentication protocols produce the MAC in a similar, but not an identical, manner.

The string entered in the **Password** field is used as the "secret key" mentioned above. For MD5 the secret key should be 16 octets; for SHA the secret key should be 20 octets. Note that this implies that the stronger authentication is provided by the SHA protocol. Therefore, SHA should be used instead of MD5, whenever possible.

SNMP Version 3 uses the CBC-DES Symmetric Encryption Protocol for privacy. This protocol also uses a secret key. The string entered in the **Password** field is used as the secret key for CBC-DES Encryption as well as for MD5 and SHA authentication.

The possible values for the **SNMP Level** field are as follows:

No SNMP Access. The user will not have SNMP access to switches. This means that the user will not be able to use OmniVista to manage switches.

SNMPv1-v2c-v3 without Authentication. The user can access switches using SNMP Version 1, Version 2, or Version 3 without any required SNMP authentication or encryption protocol.

SNMPv3 with SHA and no Encryption. The user can access switches using SNMP Version 3 and the SHA authentication algorithm will be used for authenticating SNMP PDU for the user. No encryption will be used.

SNMPv3 with MD5 and no Encryption. The user can access switches using SNMP Version 3 and the MD5 authentication algorithm will be used for authenticating SNMP PDU for the user. No encryption will be used.

SNMPv3 with SHA and Encryption. The user can access switches using SNMP Version 3 and the SHA authentication algorithm and the DES encryption standard will be used for authenticating and encrypting SNMP PDU for the user.

SNMPv3 with MD5 and Encryption. The user can access switches using SNMP Version 3 and the MD5 authentication algorithm and the DES encryption standard will be used for authenticating and encrypting SNMP PDU for the user.

Allowed Date

This field determines the dates that the user is allowed to access switches. The **All Dates** checkbox is enabled by default, which means that the user is allowed to access switches all of the

time. If desired, you can define a specific start date and a specific end date for the user's ability to access switches. To do this, uncheck the **All Dates** checkbox to disable it. The **Start Date** and **End Date** fields are enabled when the **All Dates** checkbox is unchecked. Set the **Start Date** field to the desired start date **End Date** field to the desired end date.

Allowed Time

This field determines the times-of-day that the user is allowed to access switches. The **All Day** checkbox is enabled by default, which means that the user is allowed to access switches 24 hours per day. If desired, you can define specific start times and specific end times for the user's ability to access switches. To do this, uncheck the **All Day** checkbox to disable it. The **Start Time** and the **End Time** fields, and the **More** button are enabled when the **All Day** checkbox is unchecked.

If you want to define a single continuous period of time for switch access, set the **Start Time** field to the desired start time and set the **End Time** field to the desired end time. If you want to define two or more discontinuous periods of time for switch access (for example, from 8 AM to 11:45 AM and from 1 PM to 5 PM), click the **More** button. Each time you click **More**, an additional set of **Start Time** and **End Time** fields are displayed. Define each period of switch access by entering the start and end times in a set of **Start Time** and **End Time** fields. Note that you can click the **Less** button to remove the last set of **Start Time** and **End Time** fields displayed.

Allowed Days

This field determines the days of the week that the user is allowed to access switches. The **All Week** checkbox is enabled by default, which means that the user is allowed to access switches seven days a week. If desired, you can define specific days of the week for the user's ability to access switches. To do this, uncheck the **All Week** checkbox to disable it. The individual checkboxes are enabled by each day of the week when the **All Week** checkbox is unchecked. Check the day or days that you want the user to be allowed switch access.

Note: If you uncheck all the days of the week, the **All Week** checkbox will be enabled. It is not possible to specify "no days" of the week.

Description

Use this field to enter any useful information about the user; for example, you may want to enter the user's phone number or email address. The information in this field is stored on the server but is not used by the switch.

When you have complete all the fields, click the **Apply** button to write the information to the OmniVista LDAP server.

Modifying a User: General Information

To modify the general information for an existing user, select the user in the **User Management** tab and click the **Modify User...** button. The **User Modify** window is displayed. When you complete modifying the desired information, click the **Apply** button to write the modifications to the OmniVista LDAP server.

Adding or Modifying a User: Partition Management

The **Partition Management** tab of the **User Add** window enables you to define switch access right for a user. You can define access for a feature or features (e.g., Admin), which will include all command sets within that feature (e.g., File Management, Debug); or for individual command

sets within a feature. (This is usually termed partition management.) For example, you can enable read/write access for all the features, or for the Administrator feature only, or for the File Management commands within the Administrator feature only.

R stands for "read-only" access and **RW** stands for "read/write" access. You can set all the features to "read-only" or "read/write" by clicking the corresponding **All** checkbox, shown in the screen below. You can also set privileges for a single feature to "read-only" or "read/write" by clicking the corresponding feature checkbox (e.g., Administrator), shown in the screen below. Note that you can enable privileges for an individual feature, and then uncheck individual command sets as desired.

Note: If a user is allowed **All** commands, the user's command mask is set to allow all commands available on the switch. This is useful for creating an admin user who should be able to do everything on a switch.

When you have complete all the fields, click the **Apply** button to write the information to the OmniVista LDAP server.

Note: If you create a user without indicating switch access rights, the user will be given privileges based on the default user account in the switch.

Defining a User's Switch Access Rights

To select privileges for all features, click on the applicable **All** checkbooks.

To set privileges for individual features, click on the applicable checkbooks. Select or de-select individual commands within the feature to further define privileges.

The screenshot shows the 'User Add' dialog box with the 'Partition Management' tab selected. The main area is titled 'View and Modify Family Privileges' and lists various features and their sub-commands. Each feature has a checkbox for 'R' (read-only) and 'RW' (read/write) access, and an 'All' checkbox. The features listed are:

- Administrator
- System
- Physical
- Networking
 - IP Routing
 - BGP
 - IPX Routing
 - RIPng
 - Multiple VRF
- Layer 2
 - VLAN
 - 802.1Q
- Services
 - DNS
- Policy Management
 - QOS
- Security
 - Session Management
 - AAA
- File Management
- Telnet/FTP
- TFTP
- Switch Logging
- RMON commands
- Chassis
- Port Mirroring/sFlow
- VLAN
- 802.1Q
- DNS
- QOS
- Session Management
- AAA
- SSH
- Dshell
- Interswitch
- Web Management
- Module
- Health
- RIP
- VRRP
- IP Multicast Routing
- OSPF3
- Policy
- IPsec
- NS
- SCP/SFTP
- Debug
- SNMP Commands
- Configuration File Management
- Interfaces
- OSPF
- IPRM
- IP Multicast Switching
- IS-IS
- Load Balancing
- Authenticated VLANs

Modifying a User: Partition Management

To modify partition management information for an existing user, select the user in the **User Management** tab and click the **Modify User...** button. The User Modify window is displayed. Click the **Partition Management** tab and modify the fields as desired. When you complete modifying the desired information, click the **Apply** button to write the modifications to the OmniVista server.

Expert Mode

The Expert mode provides a wizard that enables you to select the switches that you want to assign to the authentication servers and accounting servers, and define the type(s) of switch access that the server will authenticate. You can assign switches to the default OmniVista LDAP server, other LDAP servers, a RADIUS server, an ACE server, or a TACACS+ server. Note that all authentication servers, and accounting servers (other than the default OmniVista LDAP server) must be added to OmniVista before switches can be assigned to the server. For more information on adding servers to OmniVista, see the Authentication Servers application help. Assigning authentication and accounting servers in the Expert mode consists of four steps:

Step 1. Selecting the Switches to be Assigned

The first screen of the Expert mode wizard, shown below, enables you to select the switches that you want to assign to authentication and accounting servers. (Note that only AOS switches are displayed. SecureView SA does not support XOS devices.)

Step 2. Assigning Primary and Secondary Authentication Servers

The second screen of the Expert mode wizard enables you to assign all the switches that you selected to a primary authentication server and, optionally, to a secondary authentication server that will be used if the primary server is unavailable. It also enables you to define the default authentication for the selected switches as the local database or as no authentication.

Step 3. Assigning Primary and Secondary Accounting Servers

The third screen of the Expert mode wizard enables you to assign all the switches that you selected to a primary accounting server and, optionally, to a secondary accounting server that will be used if the primary server is unavailable.

Step 4. Specifying the Type(s) of Switch Access to be Authenticated

The final screen of the Expert mode wizard enables you to specify the type(s) of switch access that the assigned server will allow and authenticate for the selected switches. The server can be configured to allow and authenticate FTP access, Telnet access, switch console access, SSH access, and/or HTTP access. (Note that SNMP access i.e., OmniVista access is always allowed.)

Note that server assignments that you make in the Expert mode will override server assignments made in the One Touch mode.

Step 1. Selecting the Switches to be Assigned

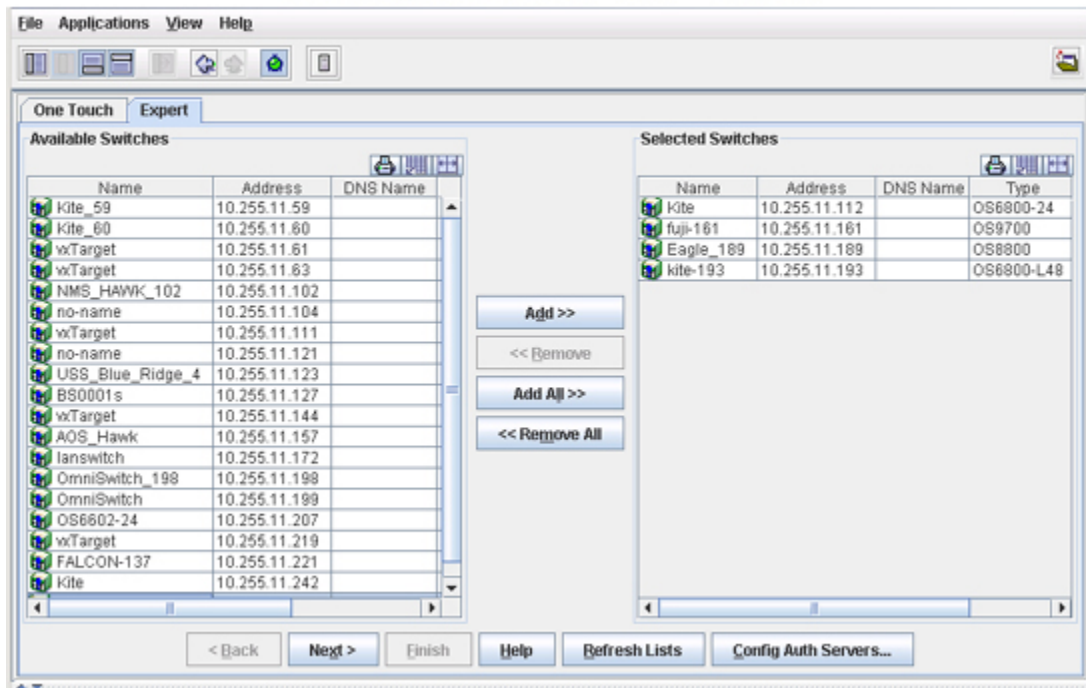
The first screen of the Expert mode wizard, shown below, enables you to select the switches that you want to assign to an authentication server and an accounting server. You will be able to assign the selected switches to a primary authentication server and, optionally, to a secondary authentication server. If assigned, the secondary server will be used for authentication when the primary server is not available. Similarly, you will be able to assign the selected switches to a

primary accounting server and, optionally, to a secondary accounting server. If assigned, the secondary server will be used for accounting when the primary server is not available.

Specify the switches to be assigned by selecting the switches in the **Available Switches** table and moving them to the **Selected Switches** table using the **Add>>** or **Add All>>** buttons.

Continue moving the switches until the **Selected Switches** table lists all the switches that you want to assign. To select a switch, click it. You can select multiple contiguous switches by **Shift**-clicking and multiple non-contiguous devices by **Ctrl**-clicking. Click **Refresh Lists** to update the lists with currently active switches and start the switches selection over.

Selecting the Switches to be Assigned

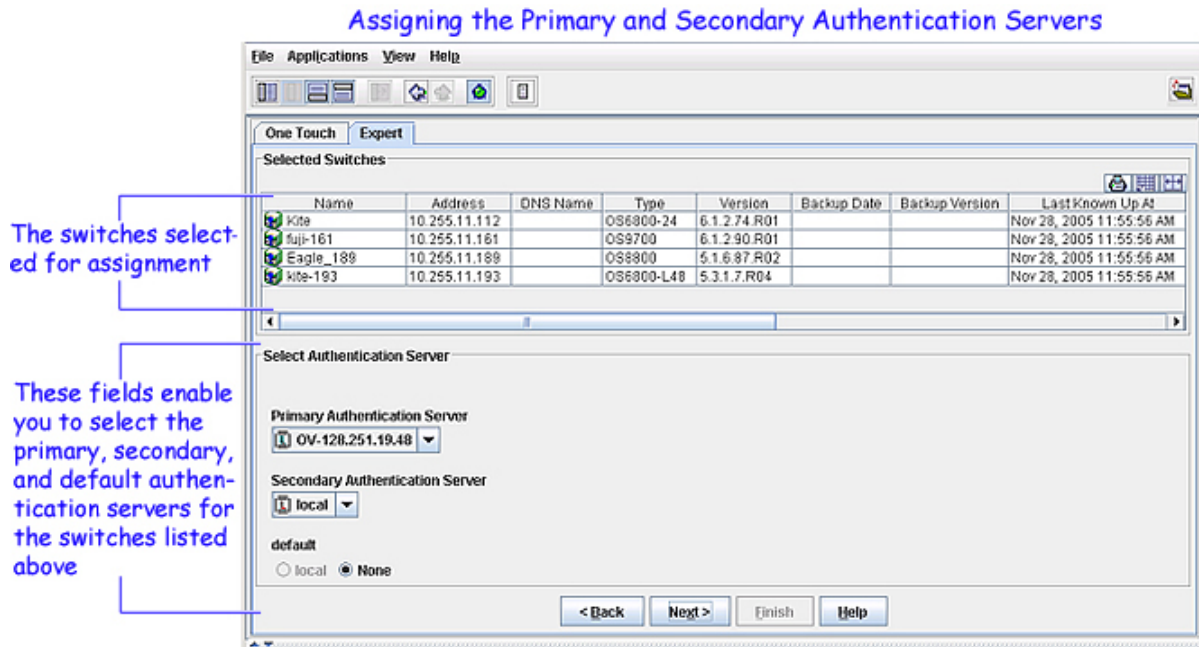


Click the **Next** button when your selections are complete.

Step 2. Assigning Primary and Secondary Authentication Servers

The second screen of the Expert mode wizard, shown below, enables you to assign all the switches that you selected in the first screen to a primary authentication server, a secondary authentication server, and a default authentication server. Remember, also, that when you added authentication servers to OmniVista you had the option of specifying a backup server for each server that you added. When the switch makes an authentication request, it tries these servers in the following order:

- The primary server is tried first. If the primary server is unavailable, the primary server's "backup" server is tried.
- If the primary server's backup server is unavailable, the secondary server is tried.
- If the secondary server is unavailable, the secondary server's "backup" server is tried.
- If the secondary server's backup server is unavailable, the default server is tried. The default server can be either **Local** (the local database) or **None** (as specified in the screen shown below). If the default is specified as None, the authentication request will fail.






ACE/Server Limitations

You can use only a single ACE server at any one time for switch authentication. This is because the **sdconf.rec** file must be FTPed from the ACE server to the switch's **/network** directory, which means that the switch can communicate only with the single ACE/Server of which it has knowledge. The **sdconf.rec** file informs the switch of the ACE server's IP address and other configuration information.

ACE servers (like RADIUS servers) do not support SNMP authentication. If you select an ACE server (or a RADIUS server) as either the primary or secondary authentication server, you will be prompted to select a second primary or secondary server to be used for SNMP authentication only. Refer to "Selecting an Additional Server for SNMP," below, for further information.

Selecting Authentication Server Fields

Note: The drop-down boxes in the **Select Authentication Server** panel list all the servers known to OmniVista. The type of each server listed is indicated by an icon. The  icon indicates an LDAP server. The  icon indicates a Radius server. The  icon indicates an ACE/Server.

Primary Authentication Server Field

Set this drop-down box to specify the primary authentication server. If you select a RADIUS server or an ACE server (neither of which support SNMP authentication), you will be prompted to select an additional server for SNMP access.

Secondary Authentication Server Field

Set this drop-down box to specify the secondary authentication server. Note that this field can also be set to **None** if you do not want to specify a secondary server. If you select a RADIUS server or an ACE server (neither of which support SNMP authentication), you will be prompted to select an additional server for SNMP access.

Default Field

Set this field to **Local** or **None** to specify the default authentication. If you specify **Local**, the local database will be used for authentication if the primary server, the backup primary server, the secondary server, and the backup secondary server are all unavailable. If you set this field to **None**, there will be no default authentication and the authentication will fail if the primary server, the backup primary server, the secondary server, and the backup secondary server are all unavailable.

Selecting an Additional Server for SNMP

SNMP access can only be authenticated by an LDAP or TACACS+ server or by the local database. If you select a RADIUS server or an ACE server as the primary or secondary authentication server, that server will be unable to authenticate SNMP access. Without SNMP access, OmniVista will be unable to manage the switch. For this reason, if you select a RADIUS server or an ACE/Server, you will be prompted to select an additional server that can authenticate SNMP access. An example of this prompt is shown in the screen below.

Note that the prompt shown below includes a **Primary SNMP Authentication Server** drop-down box. This drop-down box displays only servers that support SNMP: LDAP servers, TACACS+ servers, and the local database. Set this drop-down box to the desired authentication server for SNMP access. This server will be used **ONLY** for SNMP. The server selected in the **Primary Authentication Server** drop-down box will be used for all other types of access. The **Secondary Authentication Server** drop-down box functions in the same manner. If you select a secondary authentication server that does not support SNMP, you will be prompted to select a secondary server to be used for SNMP only.

Selecting an Additional Server for SNMP Authentication

The screenshot shows a configuration window with a table of switches and a dialog box for selecting authentication servers. The dialog box contains the following information:

Name	Address	DNS Name	Type	Version	Backup Date	Backup Version	Last Known Up At
Kite	10.255.11.112		OS6800-24	6.1.2.74.R01			Nov 30, 2005 11:19:12 AM
fuji-161	10.255.11.161		OS9700	6.1.1.620.R01			Nov 30, 2005 11:19:16 AM
Eagle_189	10.255.11.189		OS8800	5.1.6.87.R02			Nov 30, 2005 11:19:17 AM
kite-193	10.255.11.193		OS6800-L48	5.3.1.7.R04			Nov 30, 2005 11:19:17 AM

The dialog box also shows the following configuration options:

- Primary Authentication Server:** RADIUS 1
- Secondary Authentication Server:** ldap2
- default:** local None
- Primary SNMP Authentication Server:** OV-128.251.19.48

The dialog box includes a message: "You have selected an Authentication Server that does not support SNMP. You will need to select an addition Authentication Server to manage SNMP access." and buttons for "< Back", "Next >", "Finish", and "Help".

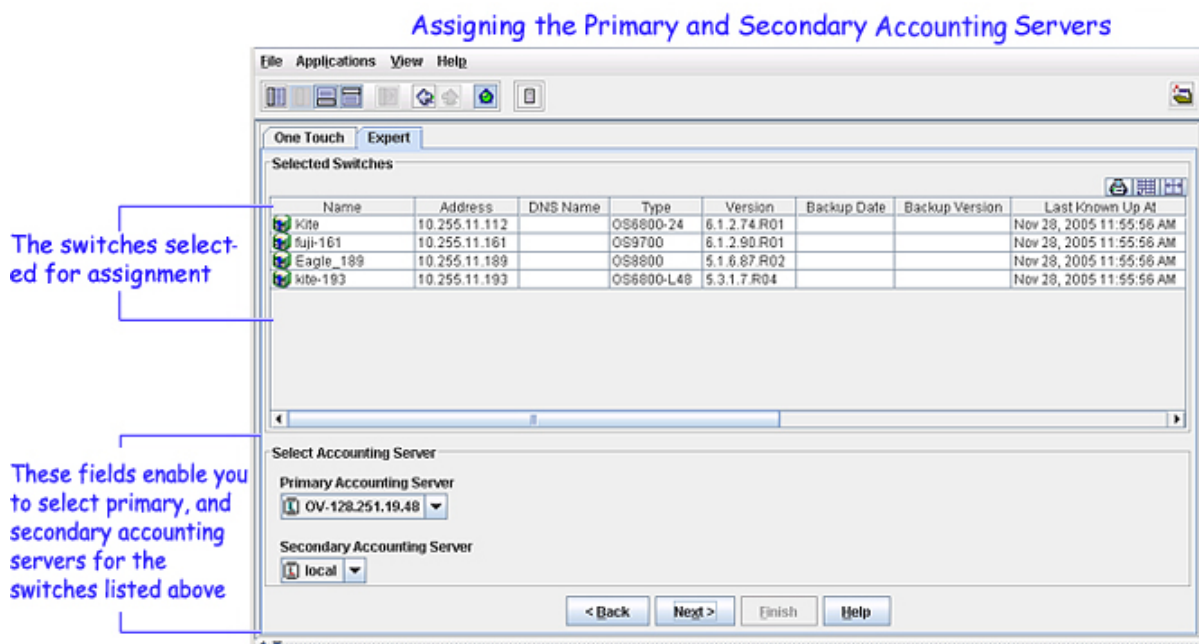
If the selected server doesn't support SNMP, you are prompted to select an additional server to manage SNMP authentication.

Click the **Next** button when your selections are complete.



Step 3. Assigning Primary and Secondary Accounting Servers

The third screen of the Expert mode wizard, shown below, enables you to assign all the switches that you selected to a primary accounting server and secondary accounting server. Remember, also, that when you added accounting servers to OmniVista you had the option of specifying a backup server for each server that you added. When the switch makes an accounting request, it tries these servers in the following order:

- The primary server is tried first. If the primary server is unavailable, the primary server's "backup" server is tried.
- If the primary server's backup server is unavailable, the secondary server is tried.
- If the secondary server is unavailable, the secondary server's "backup" server is tried. If the secondary server's backup server is not specified, the accounting request will fail.



Select Accounting Server Fields

Note: The drop-down boxes in the **Select Accounting Server** panel list all the servers known to OmniVista. The type of each server listed is indicated by an icon. The  icon indicates an LDAP server. The  icon indicates a Radius server.

Primary Accounting Server Field

Set this drop-down box to specify the primary accounting server.

Secondary Accounting Server Field

Set this drop-down box to specify the secondary accounting server. Note that this field can also be set to **None** if you do not want to specify a secondary server.

Click the **Next** button when your selections are complete.

Step 4. Specifying the Types of Switch Access to Be Authenticated

The final screen of the Expert mode wizard, shown below, enables you to specify the type(s) of switch access that you want the servers you specified in the previous screens to allow and authenticate for the selected switches. The switch access types are listed at the bottom of the **Set Switch Access** panel with corresponding checkboxes. When a checkbox is checked for a switch access, it means that the corresponding switch access will be allowed and authenticated. SNMP access is not part of the access types because SNMP access is always allowed. Each type of switch access is described in the sections below.

Specifying the Type(s) of Switch Access to be Allowed and Authenticated

The switches selected for assignment

Name	Address	DNS Name	Type	Version	Backup Date	Backup Version	Last Known Up At
kite	10.255.11.112		OS6800-24	6.1.2.74.R01			Nov 28, 2005 11:55:56 AM
fuji-161	10.255.11.181		OS9700	6.1.2.90.R01			Nov 28, 2005 11:55:56 AM
Eagle_189	10.255.11.189		OS8800	5.1.6.87.R02			Nov 28, 2005 11:55:56 AM
kite-193	10.255.11.193		OS6800-L48	5.3.1.7.R04			Nov 28, 2005 11:55:56 AM

A check means the corresponding switch access will be allowed and authenticated by the server(s) specified on the previous screen

Note
SNMP access is always allowed.

Allow FTP Access

If FTP access is not allowed, you will not be able to transfer files to the selected switches using FTP. If FTP access is allowed, you will be able to transfer files to the selected switches using FTP. OmniVista's Resource Manager application uses FTP to backup, restore, and install firmware configuration files.

Allow Telnet Access

If Telnet access is not allowed, you will not be able to Telnet to the selected switches. If Telnet access is allowed, you will be able to Telnet to the selected switches. OmniVista's Telnet application enables you to Telnet to switches and to maintain Telnet sessions with multiple switches simultaneously.

Allow Console Access

If switch console access is not allowed, CLI commands issued at the console ports of the selected switch will fail and the switch will report "authorization failed" for each command issued. OmniVista users can access switch console ports and issue CLI commands via Telnet or SSH.

Note: Access to the console port is important for switch recovery if the switch receives a bad configuration or if external authentication servers become unavailable. For this reason, user admin is ALWAYS authorized through the console port via the local

database (provided the correct password is supplied), even if access to the console port is not allowed.

Allow SSH Access

SSH, or Secure Shell, is a Telnet-like utility that provides encryption and is far more secure than Telnet. SSH is a requirement for some devices and is an option for AOS devices. If SSH access is not allowed, users will not be able to establish SSH sessions to the selected switches. If SSH access is allowed, users will be able to establish SSH sessions to the selected switches. SSH sessions can be established from OmniVista's Telnet application.

Note: Basically, SSH is a more secure replacement for both FTP and Telnet. Telnet is not as secure as SSH because Telnet passwords are transmitted in the clear, whereas SSH provides encryption. It is recommended that you allow SSH access if you do not allow FTP or Telnet access. You can encourage users to use SSH rather than Telnet or FTP by denying Telnet and FTP access and allowing SSH access.

Allow HTTP Access

HTTP is the means by which WebView accesses the switch. If HTTP access is not allowed, you will NOT be able to use WebView to manage the selected switches. If HTTP access is allowed, you will be able to use WebView to manage the selected switches. WebView is available as a menu item in several OmniVista popup menus.

Click the **Finish** button when your selections are complete. When the **Finish** button is clicked, OmniVista will configure the switches you selected for the authentication servers and accounting servers, and access types you specified. Any errors or problems that occur during this process will be reported by error messages. The successful completion of the process will also be reported.

Assigning Individual Access Modes to Different Servers

The One Touch mode always uses the default OmniVista LDAP server to authenticate all types of switch access. The Expert mode can use an LDAP, RADIUS, ACE, or TACACS+ sServer to authenticate all types of switch access. (An exception to this occurs when a RADIUS server or an ACE server is specified, since these servers do not support SNMP. In this case, the Expert mode requires you to use a second server for SNMP authentication.)

In contrast, SecureView SA's **Customize Authentication Servers** window makes it possible to take advantage of the full flexibility of the switch and individually assign each switch access mode to a different authentication server. The **Customize Authentication Servers** window also makes it possible to assign up to four authentication servers to each access mode (each with its own backup server), with each server to be tried in order of precedence.


Cautions: The **Customize Authentication Servers** window provides greater flexibility in server assignments than the normal Expert mode, including the flexibility to cut off OmniVista's communications with the switch. OmniVista will be unable to manage the switch if you set the primary server for SNMP access to **None** in the **Customize Authentication Servers** window. To recover, you would need to Telnet to the switch and issue CLI commands to turn SNMP access on.

The purpose of using an authentication server is to centralize the management of user accounts. Distributing user accounts among a large number of authentication servers

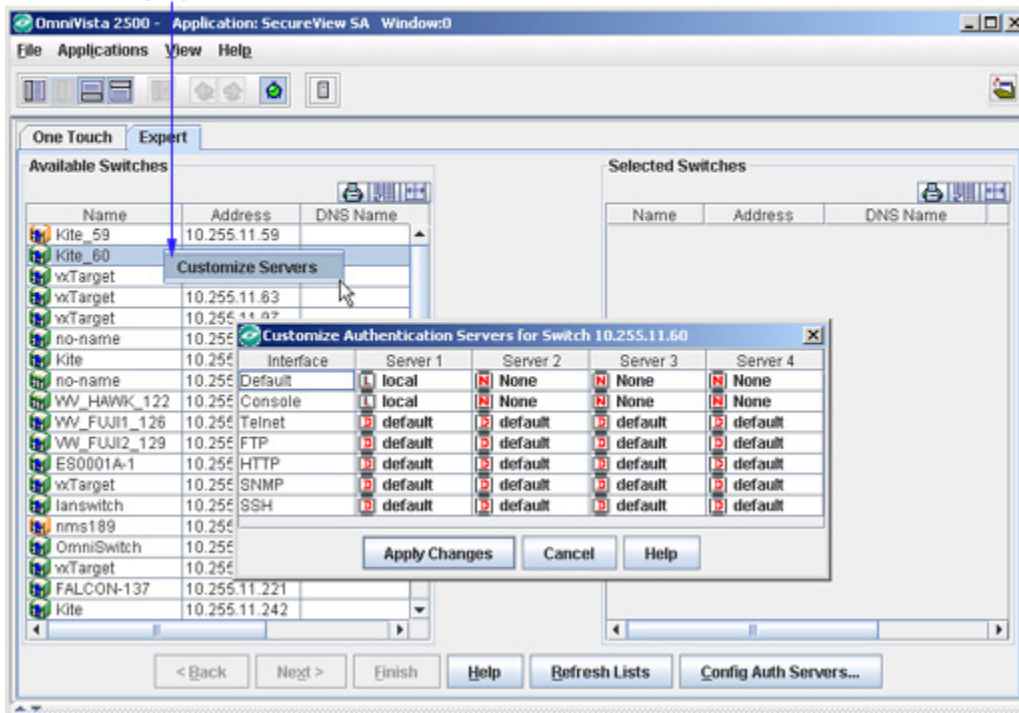
defeats this purpose and makes it more difficult to manage security. As a general rule, Alcatel-Lucent recommends that you configure all switch access modes for authentication by the same server.

To assign authentication of individual switch access modes to different servers, follow the steps below.

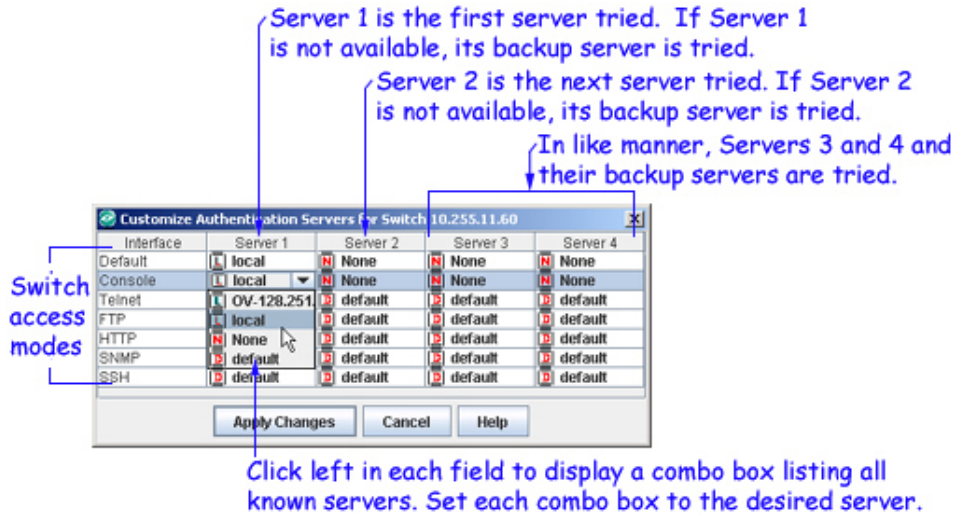
1. Display the Expert mode's **Assign Authentication Server** tab.
2. Right-click the desired switch in the **Available Switches** table to display the **Customize Servers** menu item, shown below. Click this menu item to display the **Customize Authentication Servers** window for the selected switch. The **Customize Authentication Servers** window enables you to individually assign each access mode for the selected switch to any authentication server known to OmniVista.

Note: When the **Customize Authentication Servers** window first comes up, it displays the authentication servers that the switch is actually set to use for each access mode. Since it is possible that servers were configured through means other than SecureView SA (such as the CLI), it is possible that the switch may be using a server that is unknown to OmniVista. Any such unknown server is indicated with an  icon. You can use the unknown server to authenticate access to the switch, but you cannot use the unknown server with any other switch.

1. Display Expert mode tab.
2. Click right on the switch displayed in the Available Switches panel. The **Customize Servers** menu item displays. Click on **Customize Servers** to display the **Customize Authentication Servers** window for the selected switch.



3. The **Customize Authentication Servers** window enables you to assign each switch access mode to up to four authentication servers (each with its own backup server), with each server to be tried in order of precedence. To assign a server to an access mode, click the corresponding field of the **Customize Authentication Servers** window, as shown below, and select the desired server from the list displayed.



Important Notes:

Setting Server 1 to **None** for any access mode will turn off all access to that mode. If you set Server 1 to **None** for SNMP, OmniVista will be unable to manage the switch.

The SNMP access mode can be authenticated by an LDAP server or the local switch database only. For this reason, RADIUS servers and ACE/Servers are not displayed in the SNMP access mode drop-down box.

If the **None** setting is used, it must be last in the precedence order of authentication servers. For example, if Servers 1, 2, and 3 are set to actual servers, Server 4 can be set to **None**. If Server 4 is set to an actual server, Servers 1, 2, and 3 cannot be set to **None**.

If the **Local** setting (the switch local database) is used, it must be last in the precedence order of authentication servers. For example, if Servers 1, 2, and 3 are set to actual servers, Server 4 can be set to **Local**. If Server 4 is set to an actual server, Servers 1, 2, and 3 cannot be set to **Local**.

4. When all the fields in the **Customize Authentication Servers** window are set to the desired server, or to **None**, click the **Apply Changes** button to apply the new server assignments.