

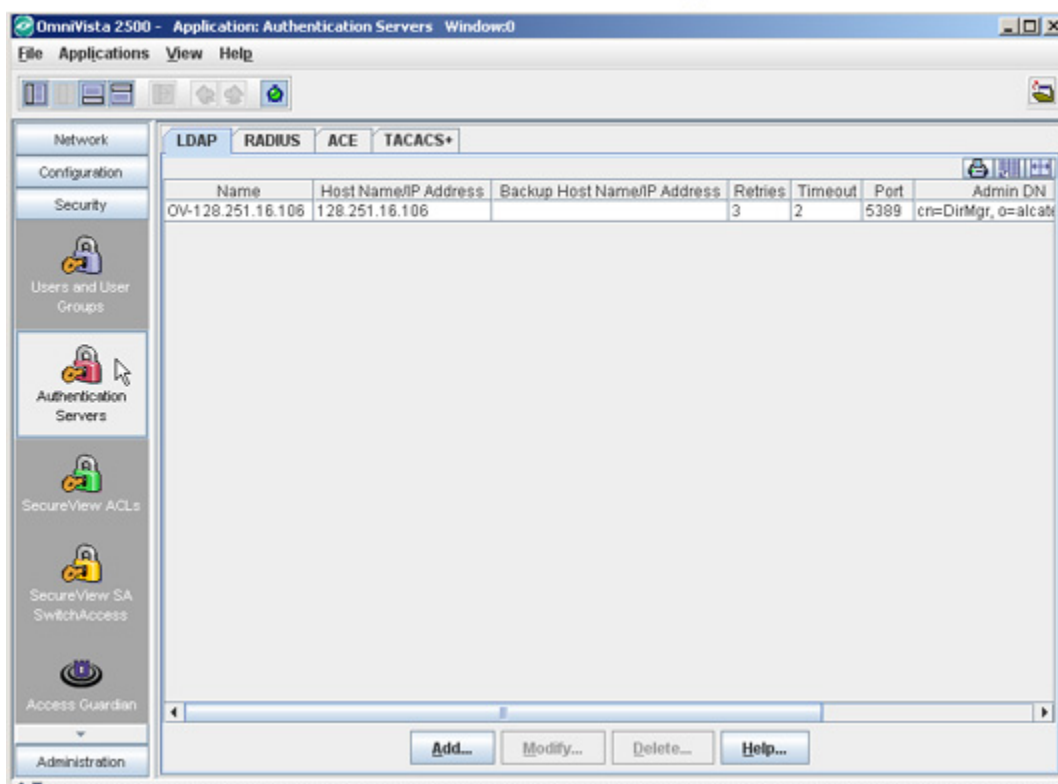
Getting Started With Authentication Servers

The Authentication Servers application enables you to create, modify, and delete authentication servers in OmniVista. An authentication server could be an LDAP, RADIUS, ACE, or TACACS+ Server. 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). When you add a server, you can also specify other information such as:

- Operating parameters for switches that will use the server for authentication, such as the number of retries the switch will attempt while communicating with the server.
- The user name and password used to login to the server (if applicable).
- The location of the server to be used as a "backup" server if the added server becomes unavailable.

When you start the Authentication Servers application, the **LDAP**, **RADIUS**, **ACE**, and **TACACS+** tabs are displayed.

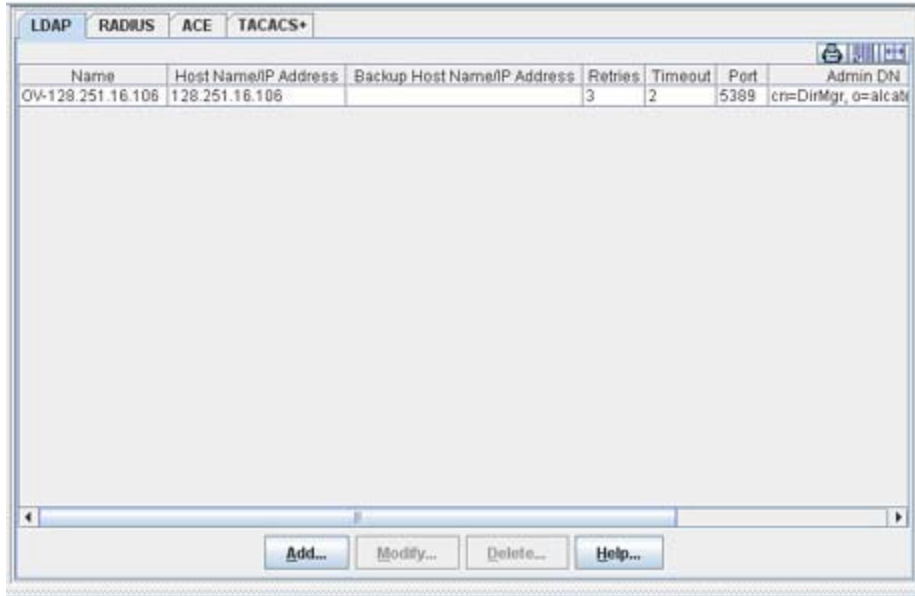
The Authentication Servers Application



LDAP Mode Overview

The **LDAP** tab, shown below, enables you to add an existing LDAP Version 3 authentication server to OmniVista's list of available LDAP authentication servers, modify an existing LDAP Server, and delete an LDAP Server from the list of LDAP Servers known to OmniVista.

LDAP Tab



RADIUS Mode Overview

The **RADIUS** tab, shown below, lists all the RADIUS authentication servers known to the OmniVista. It also enables you to add RADIUS Servers, modify existing RADIUS Servers, and delete RADIUS Servers from the list of RADIUS Servers known to OmniVista.

RADIUS Tab

Name	Host Name/IP Address	Backup Host Name/IP Address	Retries	Timeout	Auth Port	Account Port
RADIUS 1	Engineering	174.34.3.33	3	2	1812	1813
RADIUS 2	Testing	196.22.3.092	3	2	1812	1813

ACE Mode Overview

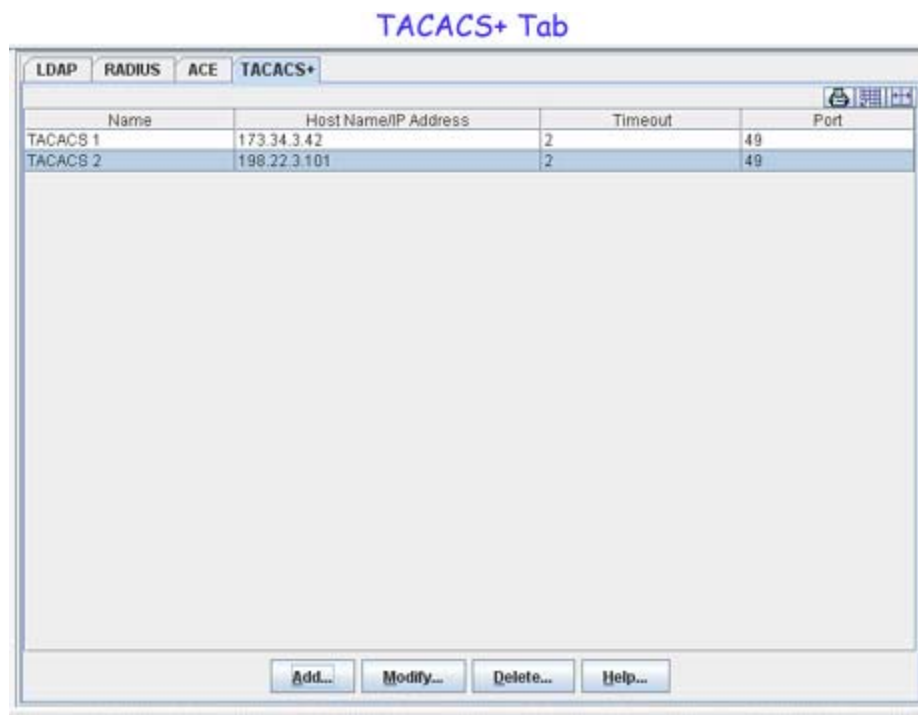
The **ACE** tab, shown below, enables you to add a single ACE Server to OmniVista. It also enables you to delete an ACE Server. An ACE Server cannot be configured or modified from OmniVista because all configuration information is contained in **sdconf.rec** file.

ACE Tab

Name	Description
ace	Configuration Information contained in sdconf.rec file

TACACS+ Mode Overview

The **TACACS+** tab, shown below, lists all the TACACS+ authentication servers known to the OmniVista. It also enables you to add, modify, and delete TACACS+ Servers from the list of TACACS+ Servers known to OmniVista.



Managing LDAP Servers

Lightweight Directory Access Protocol (LDAP) is a standard directory server protocol. The LDAP Client in the switch is based on several RFCs: 1798, 2247, 2251, 2252, 2253, 2254, 2255, and 2256. The protocol was developed as a way to use directory services over TCP/IP and to simplify the Directory Access Protocol (DAP) defined as part of the Open Systems Interconnection (OSI) effort. Originally, LDAP was a front-end for X.500 DAP.

The LDAP protocol synchronizes and governs the communications between the LDAP Client and the LDAP Server. The protocol also dictates how database information, which is normally stored in hierarchical form, is searched from the root directory down to distinct entries.

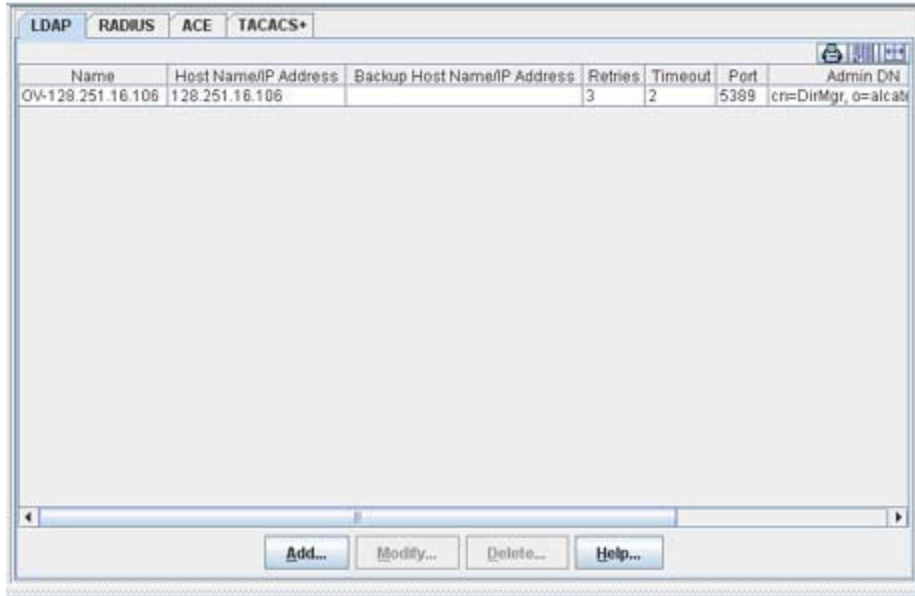
In addition, LDAP has its own format that permits LDAP-enabled Web browsers to perform directory searches over TCP/IP.

The LDAP Tab

The **LDAP** tab, shown below, enables you to add an existing LDAP Version 3 authentication server to OmniVista's list of available LDAP Authentication servers, modify an existing LDAP Server, and delete an LDAP Server from the list of LDAP Servers known to OmniVista. However, before you add an LDAP Server to OmniVista, you must do the following:

- Install the LDAP Server
- Modify the LDAP Server's schema to add required objects
- Set up user accounts on the LDAP Server

LDAP Tab



Installing and Configuring an LDAP Server

Before you add an LDAP Server to OmniVista's list of available authentication servers, you must first install the LDAP Server based on the instructions provided by the LDAP Server's vendor. You must then modify the LDAP Server's schema to add the LDAP objects required to manage Alcatel switches. The following section provides a list of the required objects.

Required LDAP Schema Objects

The following objects must be added to an LDAP Server's schema so that it can manage Alcatel switches. To modify the schema, follow the vendor's instructions. Each LDAP vendor provides a different way of modifying the schema.

- attribute accountfailtime oid-ataccountfailtime cis**
- attribute accountstarttime oid-ataccountstarttime cis**
- attribute accountstoptime oid-ataccountstoptime cis**
- attribute numberofswitchgroups oid-atnumberofswitchgroups int single**
- attribute switchgroups oid-atswitchgroups int**
- attribute switchserialnumber oid-atswitchserialnumber cis**
- attribute switchslotport oid-atswitchslotport cis**
- attribute clientipaddress oid-atclientipaddress cis**
- attribute clientmacaddress oid-atclientmacaddress cis**
- attribute userPermissions oid-atuserPermissions int single**
- attribute pm-access-priv-read-1 oid-atpm-access-priv-read-1 cis single**
- attribute pm-access-priv-read-2 oid-atpm-access-priv-read-2 cis single**
- attribute pm-access-priv-write-1 oid-atpm-access-priv-write-1 cis single**

attribute pm-access-priv-write-2 oid-atpm-access-priv-write-2 cis single
attribute pm-access-priv-global-1 oid-atpm-access-priv-global-1 cis single
attribute pm-access-priv-global-2 oid-atpm-access-priv-global-2 cis single
attribute bop-asa-func-priv-read-1 oid-atbop-asa-func-priv-read-1 int single
attribute bop-asa-func-priv-read-2 oid-atbop-asa-func-priv-read-2 int single
attribute bop-asa-func-priv-write-1 oid-atbop-asa-func-priv-write-1 int single
attribute bop-asa-func-priv-write-2 oid-atbop-asa-func-priv-write-2 int single
attribute allowedTime oid-atallovedTime cis single
attribute bop-asa-geo-priv-profile-number oid-atbop-asa-geo-priv-profile-number int single
attribute bop-md5key oid-atbop-md5key cis single
attribute bop-shakey oid-atbop-shakey cis single
attribute bop-asa-snmp-level-security oid-atbop-asa-snmp-level-security int single

Configuring User Accounts on the Server

When you use an LDAP Server other than the OmniVista LDAP Server, you must set up all user accounts on the server based on the instructions provided by the LDAP Server's vendor. You cannot set up user accounts from OmniVista for any authentication server other than the OmniVista LDAP Server, which is automatically installed with the Authentication Servers application.

Adding an LDAP Server to OmniVista

Once you have installed the LDAP authentication server, modified its schema to add required objects, and set up user accounts on the server, you are ready to add the server to OmniVista's list of available LDAP authentication servers. You can use the Authentication Servers application's **Add LDAP Server** window to add the new server. Complete each field in the **Add LDAP Server** window as explained below.



Server Name

Enter a unique name for the LDAP authentication server. This name will be used by OmniVista and the switch to identify the server.

Host Name/IP Addr

Enter the name of the computer where the server is located OR enter the IP address of the computer where the server is located.

Backup Host Name/IP Addr

Each LDAP authentication server may optionally have a backup server. If you wish to define a

backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup server is located.

Retries

Enter the number of retries that you want the switch to attempt when trying to contact the LDAP authentication server.

Timeout(Sec)

Enter the number of seconds that you want the switch to wait before a request to the LDAP authentication server is timed out.

Search Base

Enter the search base in the LDAP authentication server where authentication information can be found (e.g., o=alcatel.com).

SSL

Set this field to **Enabled** or **Disabled** to inform the switch whether SSL (Secure Socket Layer) is enabled or disabled on the LDAP authentication server. SSL can be set up on the server for additional security. (This usually involves adding digital certificates to the server.) When SSL is enabled, the server's identity will be authenticated. Refer to "Managing Authentication Servers" in your *Network Configuration Guide* and to the instructions provided by the LDAP Server's vendor for further information on setting up SSL on the LDAP Server.

Admin Name

Enter the Distinguished name used to login to the LDAP authentication server (e.g., cn=Directory Manager).

Password

Enter the password configured for the Admin name specified above. The switch must have both the Admin name and the password to log into the LDAP authentication server.

Port Number

Enter the port number used as the LDAP port address. This is the port at which the LDAP Server "listens". By default, the port number is 389. However, note that the switch automatically sets the port number to 636 when SSL is enabled. (Port number 636 is typically used on LDAP Servers for SSL.) The port number on the switch must match the port number configured on the server.

Note: When you complete all required fields in the **Add LDAP Server** window, click the **Apply** button. The new LDAP authentication server will be known to OmniVista and will be displayed in the list of known LDAP Servers in the **LDAP** tab.

Modifying an LDAP Server

You can modify a known LDAP Server by selecting it in the list of known LDAP Servers and clicking the **Modify...** button. The **Modify LDAP Server** window appears, as shown below.



You can modify any field displayed. Refer to the Adding an LDAP Server to OmniVista section for an explanation of each field. However, it is important to note that you cannot modify values indiscriminately. The values must match those of the actual LDAP Server. For example, if you want to change the LDAP port address, you must first use the tools provided by your LDAP Server's vendor to change the port on the LDAP Server itself. You can then inform OmniVista that the port number has changed by modifying the **Port Number** field in the **Modify LDAP Server** window.

Deleting an LDAP Server

You can delete an LDAP Server by selecting it in the list of known LDAP Servers and clicking the **Delete...** button.

Note: Deleting an authentication server from the list of LDAP Servers known to OmniVista will not cause switches that currently use that LDAP Server to cease using it. Switches using the deleted LDAP Server will continue to use it until the switches are reassigned.

Enabling SSL on the OmniVista LDAP Server

If you want to enable SSL on the OmniVista LDAP Server that is installed with the Authentication Servers application, you need to select the server in the list of known LDAP Servers and click the **Modify...** button to display the **Modify LDAP Server** window. Note that enabling or disabling SSL may affect PolicyView QoS (if it is installed), Groups (if it is installed), as well as SecureView SA.

Managing RADIUS Servers

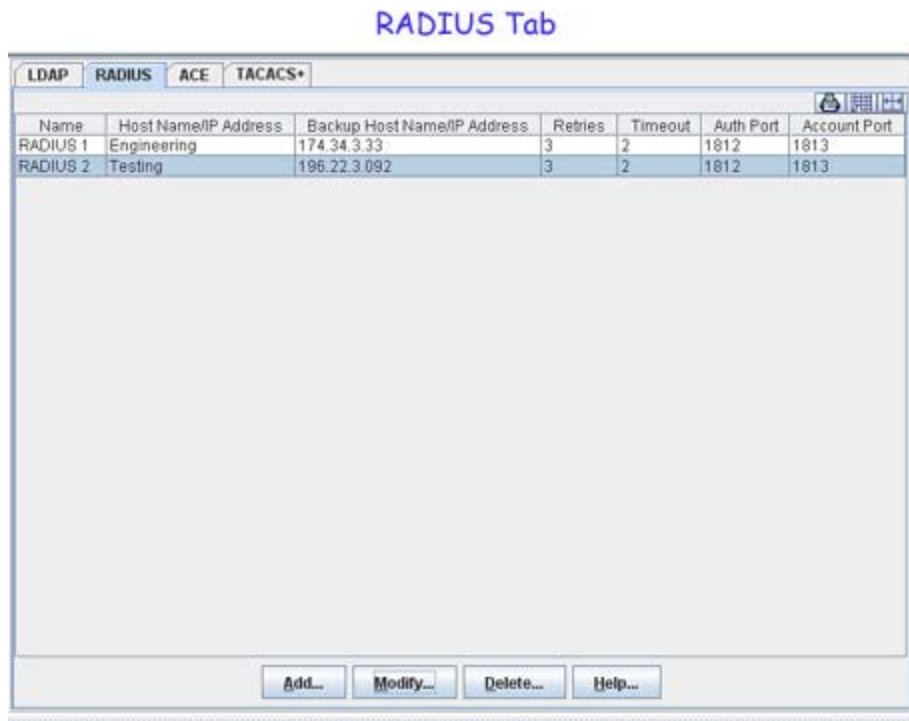
Remote Authentication Dial-in User Service (RADIUS) is a standard authentication and accounting protocol defined in RFC 2865 and RFC 2866. A built-in RADIUS Client is available in the switch. A RADIUS Server that supports Vendor Specific Attributes (VSAs) is required. VSAs carry specific authentication, authorization, and configuration details about RADIUS requests to and replies from the server. Refer to "Managing Authentication Servers" in your *Network Configuration Guide* for specific information on the VSAs required.

The RADIUS Tab

The **RADIUS** tab, shown below, lists all the RADIUS Authentication Servers known to OmniVista. It also enables you to add RADIUS Servers, modify existing RADIUS Servers, and delete RADIUS Servers from the list of RADIUS Servers known to OmniVista. However, before you add a RADIUS Server to OmniVista, you must do the following:

- Install and configure the RADIUS Server
- Set up user accounts on the RADIUS Server

Note: You cannot add, modify, or delete users and user privileges from RADIUS Servers in OmniVista.



Installing and Configuring a RADIUS Server

Before you add a RADIUS Server to OmniVista's list of available authentication servers, you must first install the RADIUS Server based on the instructions provided by the RADIUS Server's vendor. Then, you must configure the RADIUS Server with the vendor specific attributes. These attributes carry specific authentication, authorization, and configuration details about RADIUS requests to and replies from the server. Refer to "Managing Authentication Servers" in your Network Configuration Guide for specific information on the VSAs required.

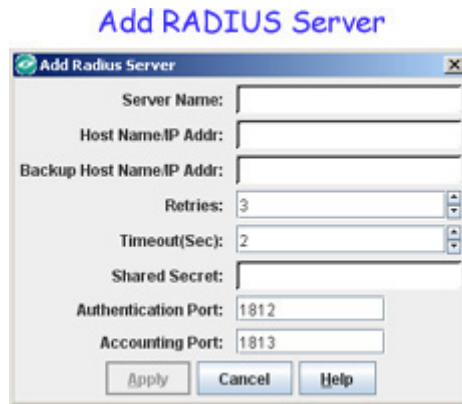
Note: The Alcatel-NMS-Group attribute must be assigned to vendor number 800 to successfully authenticate the OmniVista users through the RADIUS Server. If the vendor number is not defined for this attribute, or the vendor number is set to a different number other than 800, the user logs in, but is assigned to the "Default" group.

Configuring User Accounts on a RADIUS Server

When you use a RADIUS Server for User Authentication, you must set up all user accounts on the server based on the instructions provided by the RADIUS Server's vendor. However, the authorization which includes the access level associated with each user will be controlled by the OmniVista server, based on the group a user is associated with. You cannot set up user accounts from OmniVista for any authentication server other than the OmniVista LDAP server, which is automatically installed with the Authentication Servers application.

Adding a RADIUS Server to OmniVista

Once you have installed, configured, and set up the user accounts on the RADIUS Server, you are ready to add the server to OmniVista. You can use the Authentication Servers application's **Add Radius Server** window to add the new server. When you assign the new RADIUS Server to switches, the authentication server will automatically configure the switches to operate with the server.



Complete each field in the **Add Radius Server** window as explained below.

Server Name

Enter a unique name for the RADIUS authentication server. This name will be used by OmniVista and the switch to identify the server.

Host Name/IP Addr

Enter the name of the computer where the server is located OR enter the IP address of the computer where the server is located.

Backup Host Name/IP Addr

Each RADIUS authentication server may optionally have a backup server. If you wish to define a backup server that will be used if this server is unavailable, enter the name of the computer where the backup server is located OR enter the IP address of the computer where the backup server is located.

Retries

Enter the number of retries that you want the switch to attempt when trying to contact the RADIUS authentication server.

Timeout(Sec)

Enter the number of seconds that you want the switch to wait before a request to the RADIUS authentication server is timed out.

Shared Secret

Enter the password to the server. (The "shared secret" is essentially the server password.) Note that the password you enter must be configured identically on the server.

Authentication Port

Enter the port you to access the server.

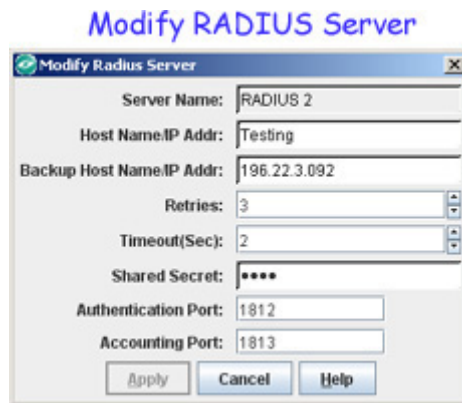
Accounting Port

Enter the port for accounting information.

Note: When you complete all required fields in the **Add Radius Server** window, click the **Apply** button. The new RADIUS authentication server will be known to OmniVista and will be displayed in the list of known RADIUS Servers in the **RADIUS** tab.

Modifying a RADIUS Server

You can modify a known RADIUS Server by selecting the desired server from the list of known RADIUS Servers and clicking the **Modify...** button. The **Modify Radius Server** window appears, as shown below.



You can modify any field displayed. Refer to the Adding a RADIUS Server to OmniVista section for an explanation of each field. However, it is important to note that you cannot modify values indiscriminately. The values must match those of the actual RADIUS Server. For example, if you want to change the RADIUS authentication port, you must first use the tools provided by your RADIUS Server's vendor to change the port on the RADIUS Server itself. You can then inform OmniVista that the port number has changed by modifying the **Authentication Port** field in the **Modify RADIUS Server** window.

Deleting a RADIUS Server

You can delete a RADIUS Server by selecting it the list of known RADIUS Servers and clicking the **Delete...** button.

Note: Deleting an authentication server from the list of RADIUS Servers known to the OmniVista will not cause switches that currently use that RADIUS Server to cease using it. Switches using the deleted RADIUS Server will continue to use it until the switches are reassigned.

Configuring a RADIUS Server for User Authentication

OmniVista includes an option to select RADIUS authentication of all OmniVista login users. In this mode all OmniVista user accounts and passwords will be created and maintained external to OmniVista. When this mode is selected, the authentication of a user at login time will be performed using the remote RADIUS Server, but the authorization will continue to be controlled within OmniVista.

Note: To select RADIUS authentication of all OmniVista login users go to **Users and User Groups** application and select RADIUS Server as the **Authentication Server**.

Authorization includes the access levels associated with each user, what switches can be seen, whether access is read-only, read-write, admin, and so forth. In the remote authentication mode OmniVista will continue to be used to create all the groups, but creating user accounts will only create local users.

The access and permission levels are controlled by user group, not by an individual user. The RADIUS accounts include the group affiliations for each user as an authorization attribute of a standard name to be defined.

The RADIUS group attribute will be a multi-valued string attribute, containing the list of groups to which this user belongs. When the authentication is performed at login, OmniVista fetches this authorization attribute and record the group membership for the current user, and the resulting access attributes. If no RADIUS group attribute is provided for the authenticated user, OmniVista sets the membership to the pre-defined "Default" group.

Three other attribute names will be defined that can optionally be provided from the external server for use by OmniVista:

- First Name
- Last Name
- Description

These attributes are not used by OmniVista for authorization, but are user-specific attributes that can be stored with for reporting in the Control Panel Application. The Attributes have the following definition in the FUNK vendor specific attribute file:

```
ATTRIBUTE Alcatel-Nms-Group Alcatel-Attr(20, string) R
```

```
ATTRIBUTE Alcatel-Nms-First-Name Alcatel-Attr(21, string) r
```

```
ATTRIBUTE Alcatel-Nms-Last-Name Alcatel-Attr(22, string) r
```

```
ATTRIBUTE Alcatel-Nms-Description Alcatel-Attr(23, string) r
```

When the remote authentication option is enabled OmniVista will attempt to authenticate the user from the remote server. If the user is not found on the remote server or the password is not valid then the user will not be authenticated. If a backup remote server has been specified and OmniVista cannot contact the remote server then it will attempt to contact the backup Remote Server.

When a user attempts to login, the server will use which error login system has been specified by the administrator in the Users and Group application. If a remote server has been selected and neither the remote server nor the remote backup server can be reached, then login will fallback to the local OmniVista users. This will allow a network administrator to login even if the authentication server is down.

Managing ACE Servers

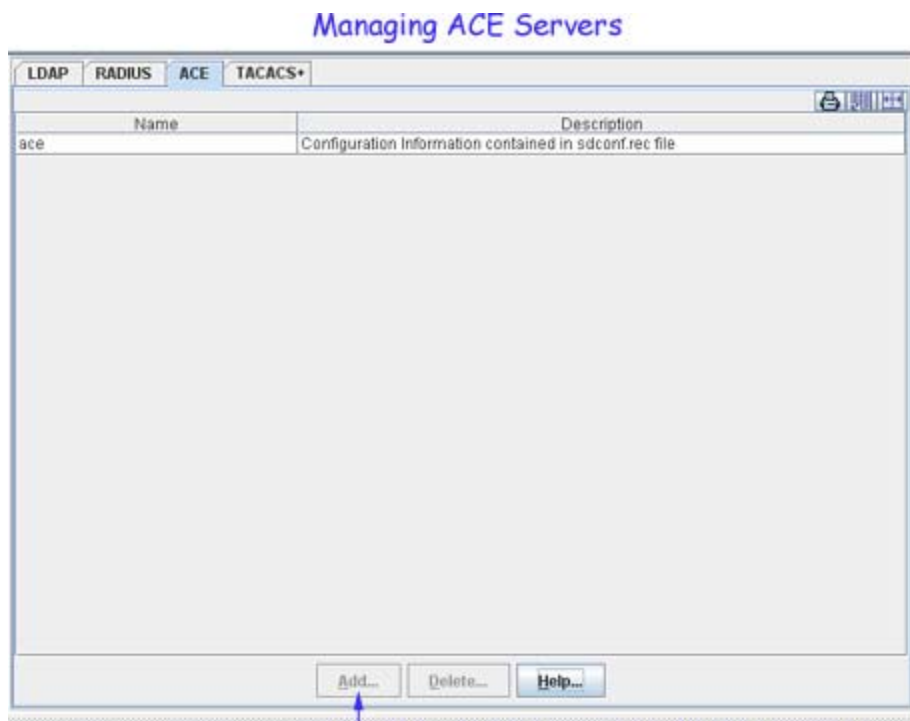
The ACE Tab

You can use a single external ACE Server for authentication of all switch access types. You are limited to a single ACE Server, because file **sdconf.rec** must be FTPed from the ACE Server to the switch's **/network** directory, to inform the switch of the ACE Server's IP address and other

configuration information. This requirement means that the switch can communicate with only a single ACE Server at any one time.

Note: An ACE Server cannot be used for Layer 2 authentication or for policy.

The **ACE** tab, shown below, enables you to add a single ACE Server to OmniVista. It also enables you to delete an ACE Server. An ACE Server cannot be configured or modified from OmniVista because all configuration information is contained in **sdconf.rec** file.



To add an ACE Server, click Add. Only a single ACE Server can be added. The Add button is active only when an ACE Server does not exist.

Before You Add an ACE Server to OmniVista

Before you add the ACE Server to OmniVista, you must first install the ACE Server, based on the instructions provided by your ACE Server's vendor. You must also set up user accounts on the ACE Server. There are no server-specific parameters that must be configured for the switch to communicate with an attached ACE Server; however, you must FTP the **sdconf.rec** file from the server to the switch's **/network** directory. This file is required so that the switch will know the IP address of the ACE Server and other configuration information. For information about loading files into the switch, see the *OmniSwitch 6800/6850/7700/7800/8800/9000 Switch Management Guide*.

Note: An ACE Server stores and authenticates switch user accounts (i.e., user IDs and passwords), but does NOT store or send user privilege information to the switch. User privileges for logins are determined by the switch itself. When a user attempts to log into the switch, the user ID and password are sent to the ACE Server. The server determines whether the login is valid or not. If the login is valid, the user privileges must be determined. The switch checks its user database for the user's privileges. If the user is not

in the database, the switch uses the default privilege, which is determined by the default user account. For information about the default user account, see the "Switch Security" chapter of the *OmniSwitch 6800/6850/7700/7800/8800/9000 Switch Management Guide*.

The ACE client in the switch is version 4.1; it does not support the replicating and locking feature of ACE 5.0, but it may be used with an ACE 5.0 server if a legacy configuration file is loaded on the server. The legacy configuration must specify authentication to two specific servers (master and slave). See the RSA Security ACE Server documentation for more information.

Adding an ACE Server

Once you have installed and configured the ACE Server, you are ready to add the new server to OmniVista. To add an ACE Server to OmniVista, click the **Add...** button in the **ACE** tab, as shown in the screen above. When you assign the ACE Server to switches, the authentication server will automatically configure the switches to operate with the server.

Deleting an ACE Server

To delete an ACE Server from OmniVista, select the server in the **ACE** tab and click the **Delete...** button.

Note: Deleting an authentication server from the list of ACE Servers known to OmniVista will not cause switches that currently use that ACE Server to cease using it. Switches using the deleted ACE Server will continue to use it until the switches are reassigned.

Managing TACACS+ Servers

Terminal Access Controller Access Control System (TACACS+) is a standard authentication and accounting protocol defined in RFC 1321 that employs TCP for reliable transport. A built-in TACACS+ Client is available in the switch. A TACACS+ Server allows access control for routers, network access servers, and other networked devices through one or more centralized servers. The protocol also allows separate authentication, authorization, and accounting services. By allowing arbitrary length and content authentication exchanges, it allows clients to use any authentication mechanism.

The TACACS+ Client offers the ability to configure multiple TACACS+ Servers. When the primary server fails, the client tries the subsequent servers. Multiple server configurations are applicable only for backup and not for server chaining.

- **Authentication.** TACACS+ protocol provides authentication between the client and the server. It also ensures confidentiality because all the exchanges are encrypted. The protocol supports fixed passwords, one-time passwords, and challenge-response queries. Authentication is not a mandatory feature, and it can be enabled without authorization and accounting. During authentication if a user is not found on the primary TACACS+ Server, the authentication fails. The client does not try to authenticate with the other servers in a multiple server configuration. If the authentication succeeds, then authorization is performed.
- **Authorization.** Enabling authorization determines if the user has the authority to execute a specified command. TACACS+ authorization cannot be enabled independently. The

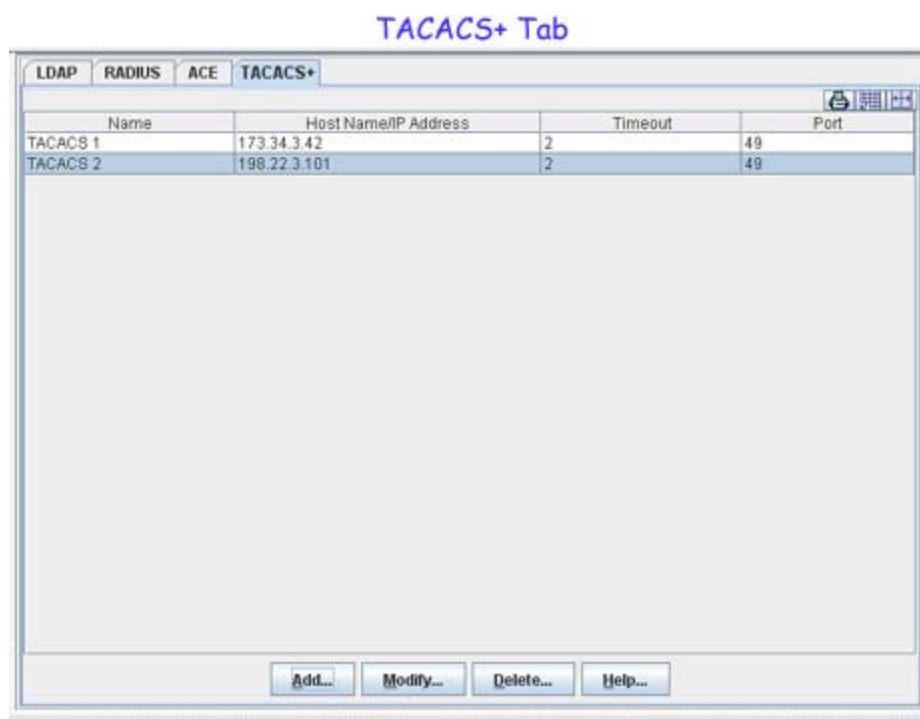
TACACS+ authorization is enabled automatically when the TACACS+ authentication is enabled.

- **Accounting.** The process of recording what the user is attempting to do or what the user has done is “Accounting”. The TACACS+ accounting must be enabled on the switches for accounting to succeed. Accounting can be enabled irrespective of authentication and authorization.

Refer to "Managing Authentication Servers" in your *Network Configuration Guide* for more information.

The TACACS+ Tab

The **TACACS+** tab, shown below, lists all the TACACS+ Servers known to OmniVista. It also enables you to add TACACS+ Servers, modify existing TACACS+ Servers, and delete TACACS+ Servers from the list of TACACS+ Servers known to OmniVista.



Adding a TACACS+ Server to OmniVista

Once you have installed, configured, and set up the user accounts on the TACACS+ Server, you are ready to add the server to OmniVista. You can use the Authentication Servers application's **Add TACACS Server** window to add the new server. When you assign the new TACACS+ Server to switches, the authentication server will automatically configure the switches to operate with the server.



Complete each field in the **Add TACACS Server** window as explained below.

Server Name

Enter a unique name for the TACACS+ Server. This name will be used by OmniVista and the switch to identify the server.

Host Name/IP Addr

Enter the name of the computer where the server is located OR enter the IP address of the computer where the server is located.

Timeout (Sec)

Enter the number of seconds that you want the switch to wait before a request to the TACACS+ Server is timed out (Default = 2).

Port Number

Enter the port you to access the server (Default = 49).

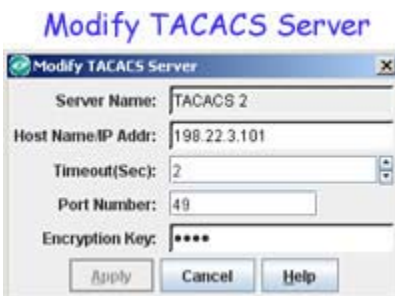
Encryption Key

Enter the password to the server. (The "Encryption Key" is essentially the server password.) Note that the password you enter must be configured identically on the server.

Note: When you complete all required fields in the **Add TACACS+ Server** window, click the **Apply** button. The new TACACS+ Server will be known to OmniVista and will be displayed in the list of known TACACS+ Servers in the **TACACS+** tab.

Modifying a TACACS+ Server

You can modify a known TACACS+ Server by selecting the desired server from the list of known TACACS+ Servers and clicking the **Modify...** button. The **Modify TACACS Server** window appears, as shown below.



You can modify any field displayed. Refer to the Adding a TACACS+ Server to OmniVista section for an explanation of each field. However, it is important to note that you cannot modify values indiscriminately. The values must match those of the actual TACACS+ Server. For example, if you want to change the TACACS+ authentication port, you must first use the tools

provided by your TACACS+ Server's vendor to change the port on the TACACS+ Server itself. You can then inform OmniVista that the port number has changed by modifying the **Authentication Port** field in the **Modify TACACS+ Server** window.

Deleting a TACACS+ Server

You can delete a TACACS+ Server by selecting it the list of known TACACS+ Servers and clicking the **Delete...** button.

Note: Deleting a TACACS+ Server will not cause switches that currently use that TACACS+ Server to cease using it. Switches using the deleted TACACS+ Server will continue to use it until the switches are reassigned.