



Configuring an LDAP AAA Server

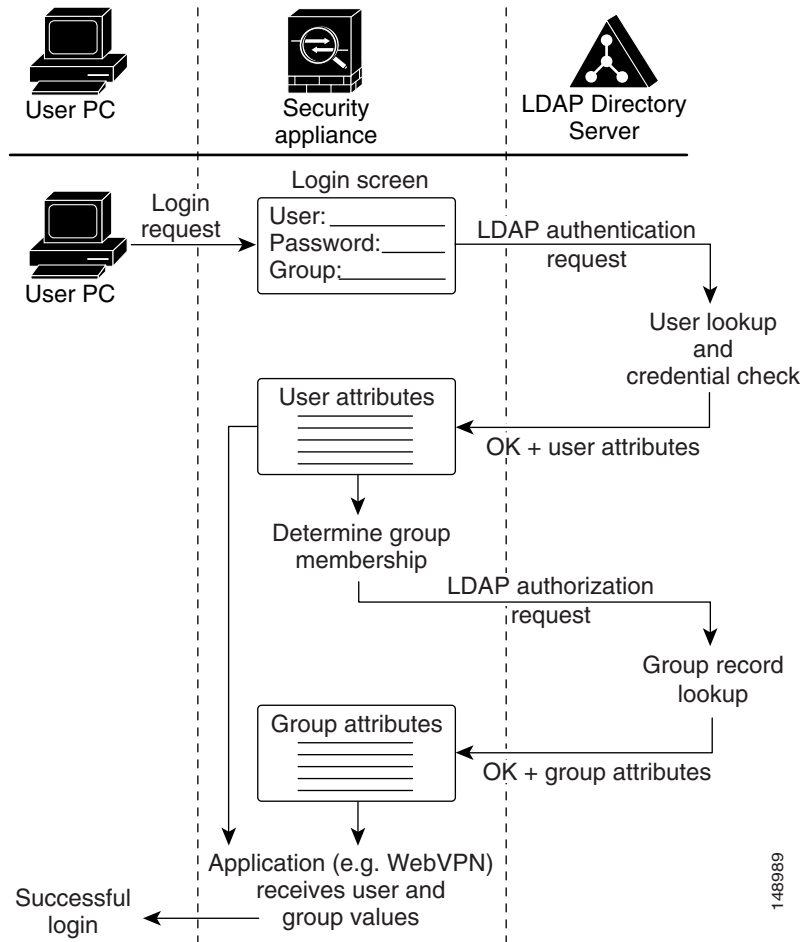
This chapter presents an example configuration procedure for configuring security appliance user authentication and authorization using a Microsoft Active Directory Server (LDAP) that is on the same internal network as the security appliance. It includes the following sections.

- [Overview of LDAP Transactions, page 6-2](#)
- [Creating an LDAP Attribute Map, page 6-2](#)
- [Configuring AAA Server Groups and Servers, page 6-5](#)
- [Configuring the Group Policy for LDAP Authorization, page 6-11](#)
- [Configuring a Tunnel Group for LDAP Authentication, page 6-12](#)

Overview of LDAP Transactions

Figure 6-1 shows the major transactions in security appliance user authentication and authorization using an LDAP directory server.

Figure 6-1 LDAP Authentication and Authorization Transaction Flow



148989

Creating an LDAP Attribute Map

To configure the security appliance for LDAP authentication and authorization, you must first create an LDAP attribute map which maps customer-defined attribute names to Cisco LDAP attribute names. This prevents you from having to rename your existing attributes using the Cisco names that the security appliance understands.



Note

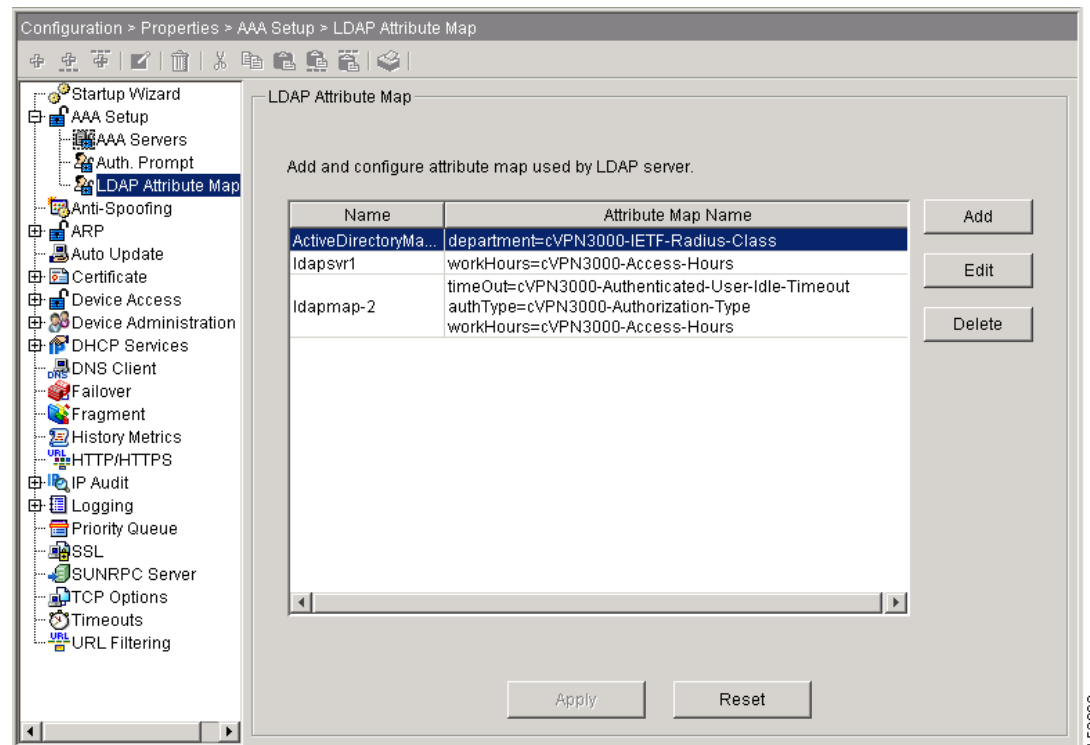
To use the attribute mapping features correctly, you need to understand the Cisco LDAP attribute names and values as well as the user-defined attribute names and values. See the *Cisco Security Appliance Command Line Configuration Guide* appendix, “Configuring an External Server for Authorization and Authentication” for the list of Cisco LDAP attributes.

To create a new LDAP attribute map, perform the following steps:

- Step 1** In the Cisco ASDM window, choose **Configuration > Properties > AAA Setup > LDAP Attribute Map**.

The LDAP Attribute Map area appears in the window on the right as shown in [Figure 6-2](#).

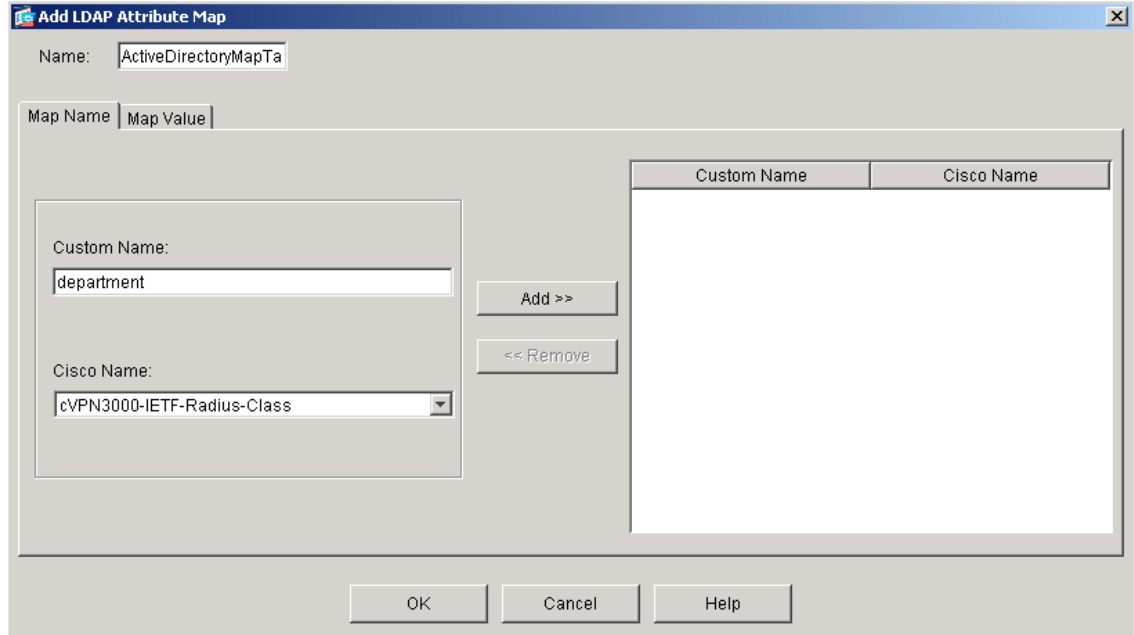
Figure 6-2 LDAP Attribute Map Area



- Step 2** In the LDAP Attribute Map area, click **Add**.

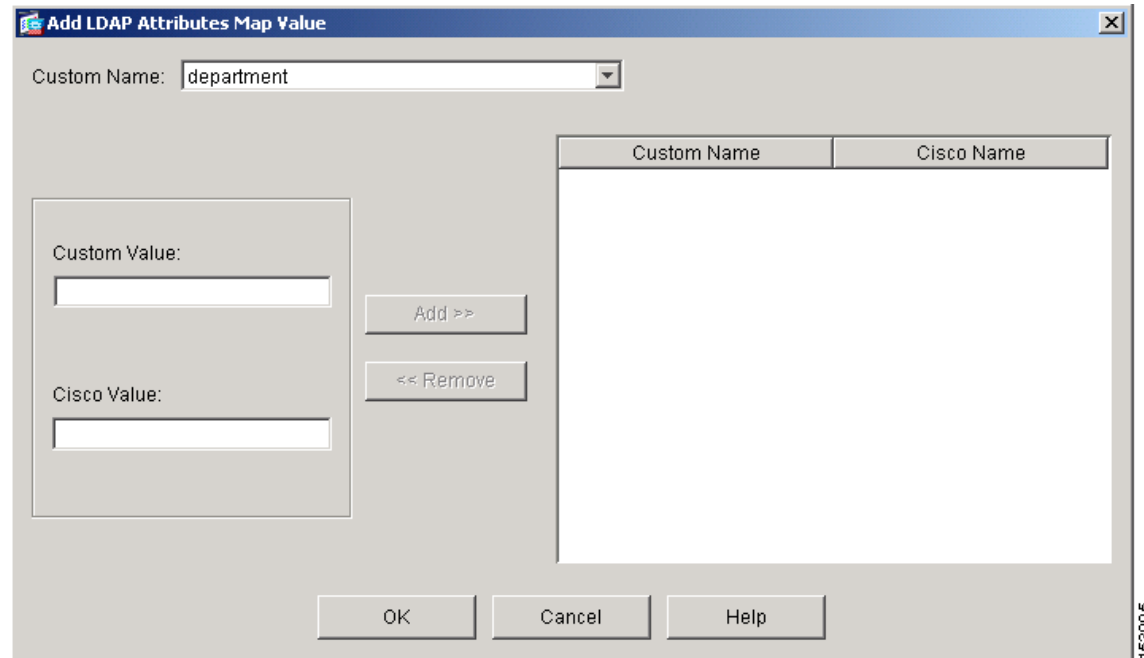
The Add LDAP Attribute Map dialog box appears as shown in [Figure 6-3](#).

Figure 6-3 Add LDAP Attribute Map Dialog Box - Map Name Tab Selected



- Step 3** In the Name field above the tabs, enter a name for the LDAP attribute map.
In this example, we name the attribute map `ActiveDirectoryMapTable`.
- Step 4** If the Map Name tab is not selected, choose it now.
- Step 5** In the Custom Name (user-defined attribute name) field on the Map Name tab, enter the name of an attribute that you want to map to a Cisco attribute name.
In this example, the custom name is *department*.
- Step 6** Choose a Cisco name from the Cisco Name menu. The custom name maps to this Cisco name.
In this example, the Cisco name is `cVPN3000-IETF-Radius-Class`. As shown in [Figure 6-1](#), the security appliance receives the user attributes from the authentication server upon validation of the user credentials. If a class attribute is among the user attributes returned, the security appliance interprets it as the group policy for that user, and it sends a request to the AAA server group configured for this group policy to obtain the group attributes.
- Step 7** Click **Add** to include the name mapping in the attribute map.
- Step 8** Click the **Map Value** tab and then click **Add** on the Map Value tab.
The Add LDAP Attributes Map Value dialog box appears as shown in [Figure 6-4](#).

Figure 6-4 Add LDAP Attributes Map Value Dialog Box



- Step 9** From the Custom Name menu, choose the custom attribute for which you want to map a value.
- Step 10** Enter the custom (user-defined) value in the Custom Value field.
- Step 11** Enter the Cisco value in the Cisco Value field.
- Step 12** Click **Add** to include the value mapping in the attribute map.
- Step 13** Repeat [Step 4](#) through [Step 12](#) for each attribute name and value to be mapped.
- Step 14** After you have completed mapping all the names and values, click **OK** at the bottom of the Add LDAP Attribute Map window.
- Step 15** Click **Apply** to complete the new LDAP attribute map and add it to the running security appliance configuration.

Configuring AAA Server Groups and Servers

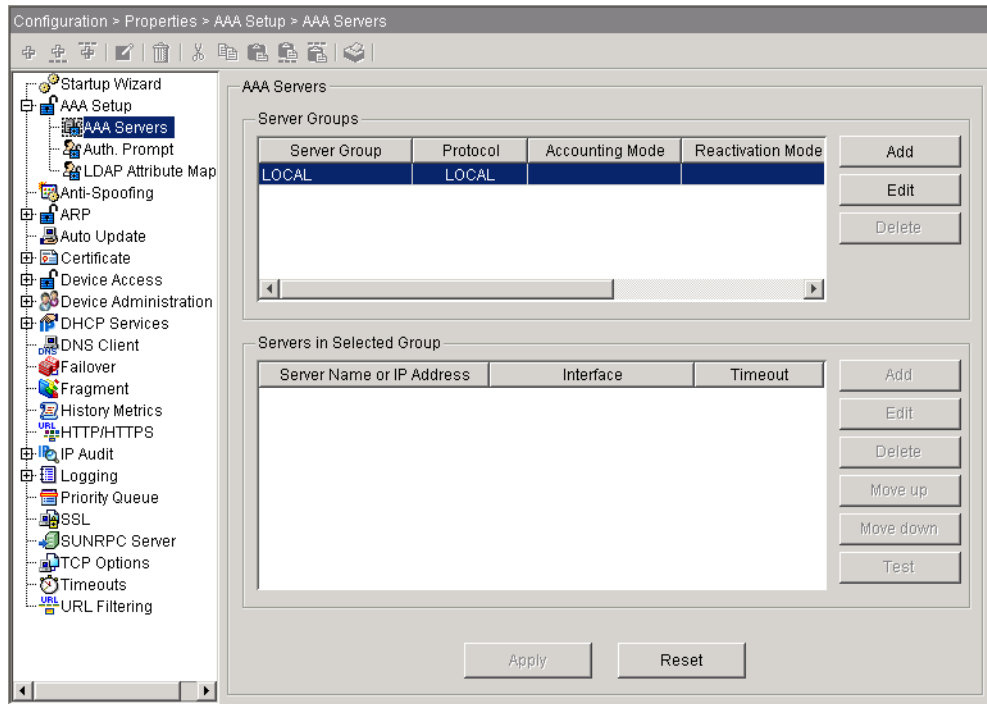
Next, you configure AAA server groups and the AAA servers that go into them. You must configure two AAA server groups. You configure one server group as an authentication server group containing an authentication server that requests an LDAP search of the user records. You configure the other server group as an authorization server group containing an authorization server that requests an LDAP search of the group records. One notable difference between the two groups is that the AAA servers have different base DN fields to specify different Active Directory folders to search.

Creating the LDAP AAA Server Groups

To configure the two server groups, perform the following steps:

- Step 1** In the Cisco ASDM window, choose **Configuration > Properties > AAA Setup > AAA Servers**. The AAA Servers area appears in the right half of the window as shown in [Figure 6-5](#).

Figure 6-5 The ASDM Window with AAA Servers Selected

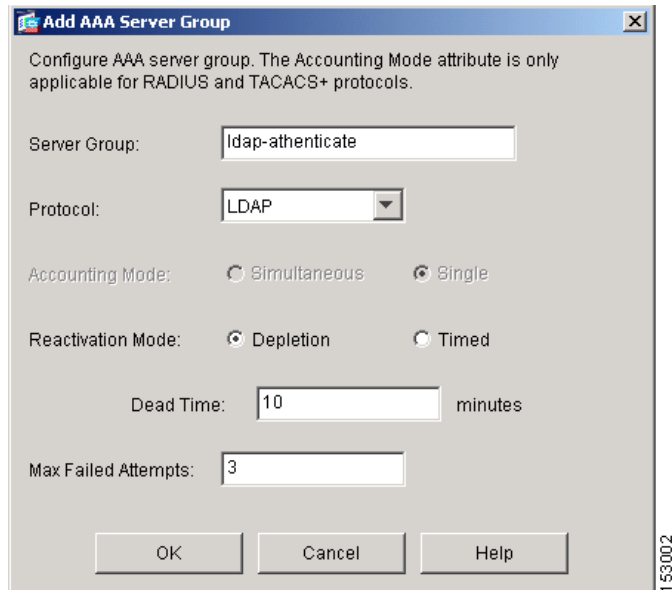


The fields in the AAA Servers area are grouped into two areas: the Server Groups area and the Servers In The Selected Group area. The Server Groups area lets you configure AAA server groups and the protocols the security appliance uses to communicate with the servers listed in each group.

- Step 2** In the Server Groups area, click **Add**.

The Add AAA Server Group dialog box appears as shown in [Figure 6-6](#).

Figure 6-6 The Add AAA Server Group Dialog Box



Step 3 Enter the name of the server group in the Server Group field.

Use different names for the authentication server group and the authorization server group. In this example, we name the authentication server group *ldap-authenticat* (authenticate is truncated because of a sixteen character maximum) and the authorization server group *ldap-authorize*.

Step 4 Choose **LDAP** from the Protocol menu.

Step 5 For the Reactivation Mode, choose one of the following:

- **Depletion**—Configures the security appliance to reactivate failed servers only after all of the servers in the group are inactive.
- **Timed**—Configures the security appliance to reactive failed servers after 30 seconds of down time.

Step 6 In the Dead Time field, enter the number of minutes that elapse between the disabling of the last server in the group and the subsequent reenabling of all servers.

This field is not available if you selected Timed mode in [Step 5](#).

Step 7 In the Max Failed Attempts field, enter the number of failed connection attempts (1 through 5) allowed before declaring a nonresponsive server inactive.

Step 8 Click **OK** to enter the newly configured server into the Server Groups table.

Step 9 Repeat [Step 2](#) through [Step 8](#) for the second AAA server group. When done, you should have an authentication server group and an authorization server group.

Configuring the LDAP AAA Servers

For each of the two AAA server groups, you next configure a AAA server. Again, one server is for authentication and one for authorization.

To add a new LDAP AAA server to each of the AAA server groups, perform the following steps:

- Step 1** In the Cisco ASDM window, choose **Configuration > Properties > AAA Setup > AAA Servers**. The AAA Servers area appears in the right half of the window.
- Step 2** In the Server Group table, click the LDAP server group to which you want to add the LDAP server. In this example, we configure the authentication server in the ldap-authenticat group and the authorization server in the ldap-authorize group.
- Step 3** In the Servers in Selected Group area, click **Add**. The Add AAA Server dialog box appears as shown in [Figure 6-7](#).

Figure 6-7 The Add AAA Server Dialog Box

The screenshot shows the 'Add AAA Server' dialog box with the following configuration:

- Server Group: ldap-authenticat
- Interface Name: inside
- Server Name or IP Address: 10.1.1.2
- Timeout: 10 seconds
- LDAP Parameters:
 - Enable LDAP over SSL
 - Server Port: 636
 - Server Type: Microsoft
 - Base DN: cn=users,dc=frdevtestad,dc=local
 - Scope: All levels beneath the Base DN
 - Naming Attribute(s): cn
 - Login DN: r,cn=users,dc=frdevtestad,dc=local
 - Login Password: anypassword
 - LDAP Attribute Map: ActiveDirectoryMapTable
 - SASL MD5 authentication
 - SASL Kerberos authentication
 - Kerberos Server Group: (empty)

Buttons: OK, Cancel, Help

Step 4 From the Interface Name menu, choose either:

- **Inside** if your LDAP server is on your internal network
- or-
- **Outside** if your LDAP server is on an external network

In our example, the LDAP server is on the internal network.

Step 5 Enter the server name or IP address in the Server Name or IP Address field.

In our example, we use the IP address.

Step 6 In the Timeout field, enter the timeout interval in seconds.

This is the time after which the security appliance gives up on the request to the primary AAA server. If there is a standby server in the server group, the security appliance sends the request to the backup server.

Step 7 In the LDAP Parameters area, check **Enable LDAP over SSL** if you want all communications between the security appliance and the LDAP directory to be encrypted with SSL.



Warning

If you do not check Enable LDAP over SSL, the security appliance and the LDAP directory exchange all data in the clear, including sensitive authentication and authorization data.

Step 8 Enter the server port to use in the Server Port field.

This is the TCP port number by which you access the server.

Step 9 From the Server Type menu, choose one of the following:

- **Sun Microsystems JAVA System Directory Server** (formerly the Sun ONE Directory Server)
- or -
- **Microsoft Active Directory**
- or -
- **Detect automatically**

The security appliance supports authentication and password management features only on the Sun Microsystems JAVA System Directory Server (formerly named the Sun ONE Directory Server) and the Microsoft Active Directory. By selecting Detect automatically, you let the security appliance determine if the server is a Microsoft or a Sun server.



Note

The DN configured on the security appliance to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.

Step 10 Enter one of the following into the Base DN field:

- The base DN of the Active Directory folder holding the user attributes (typically a users folder) if you are configuring the authentication server
- or -
- The base DN of the Active Directory folder holding the group attributes (typically a group folder) if you are configuring the authorization server

The base DN is the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request. For example, OU=people, dc=cisco, dc=com.

Step 11 From the Scope menu, select one of the following:

- **One level beneath the Base DN**
- or -
- **All levels beneath the Base DN**

The scope specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request. One Level Beneath the Base DN specifies a search only one level beneath the Base DN. This option is quicker. All Levels Beneath the Base DN specifies a search of the entire subtree hierarchy. This option takes more time.

Step 12 In the Naming Attribute(s) field, enter the Relative Distinguished Name attribute that uniquely identifies an entry on the LDAP server.

Common naming attributes are Common Name (cn) and User ID (uid).

Step 13 In the Login DN field, perform one of the following:

- Enter the name of the directory object for security appliance authenticated binding. For example, cn=Administrator, cn=users, ou=people, dc=Example Corporation, dc=com.
- or -
- Leave this field blank for anonymous access.

Some LDAP servers, including the Microsoft Active Directory server, require the security appliance to establish a handshake via authenticated binding before accepting requests for LDAP operations. The security appliance identifies itself for authenticated binding by including a Login DN field with the user authentication request. The Login DN field defines the security appliance authentication characteristics which should correspond to those of a user with administration privileges.

Step 14 Enter the password associated with the Login DN in the Login Password field.

The characters you type appear as asterisks.

Step 15 From the LDAP Attribute Map menu, choose the LDAP attribute map to apply to the LDAP server.

The LDAP attribute map translates user-defined LDAP attribute names and values into Cisco attribute names and values. To configure a new LDAP attribute map, see [Creating an LDAP Attribute Map, page 6-2](#).

Step 16 Check **SASL MD5 Authentication** to use the MD5 mechanism of the Simple Authentication and Security Layer (SASL) to secure authentication communications between the security appliance and the LDAP server.

Step 17 Check **SASL Kerberos Authentication** to use the Kerberos mechanism of the Simple Authentication and Security Layer to secure authentication communications between the security appliance and the LDAP server.



Note

If you configure more than one SASL method for a server, the security appliance uses the strongest method supported by both the server and the security appliance. For example, if both MD5 and Kerberos are supported by both the server and the security appliance, the security appliance selects Kerberos to secure communication with the server.

Step 18 If you checked SASL Kerberos authentication in [Step 17](#), enter the Kerberos server group used for authentication in the Kerberos Server Group field.

Step 19 Repeat [Step 3](#) through [Step 18](#) to configure a AAA server in the other AAA server group.

Configuring the Group Policy for LDAP Authorization

After configuring the LDAP attribute map, the AAA server groups, and the LDAP servers within the groups, you next create an external group-policy that associates the group-name with the LDAP authorization server.



Note

Comprehensive procedures for configuring group policies are provided elsewhere in this guide. The following steps are only those that apply to configuring AAA with LDAP.

To create a new group policy and assign the LDAP authorization server group to it, perform the following steps:

Step 1 In the Cisco ASDM window, select **Configuration > VPN > General > Group Policy**.

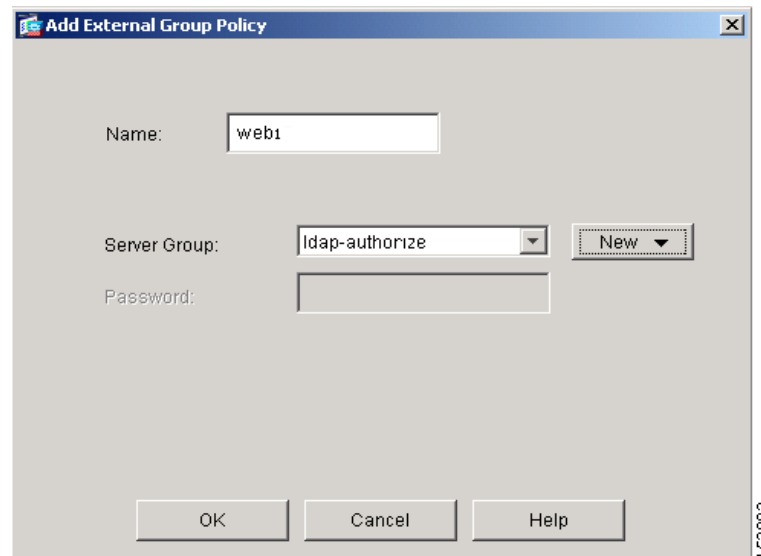
The Group Policy area appears in the right half of the window.

Step 2 Click **Add** and choose either **Internal Group Policy** or **External Group Policy**.

In this example, we choose External Group Policy because the LDAP server is external to the security appliance.

The Add Group Policy dialog box appears as shown in [Figure 6-8](#).

Figure 6-8 Add Group Policy Dialog Box



Step 3 Enter the name of the new group policy in the name field.

The group policy name is *web1* in our example.

Step 4 From the Server Group menu, choose the AAA authorization server group you created previously.

In our example, this is the server group named ldap-authorize.

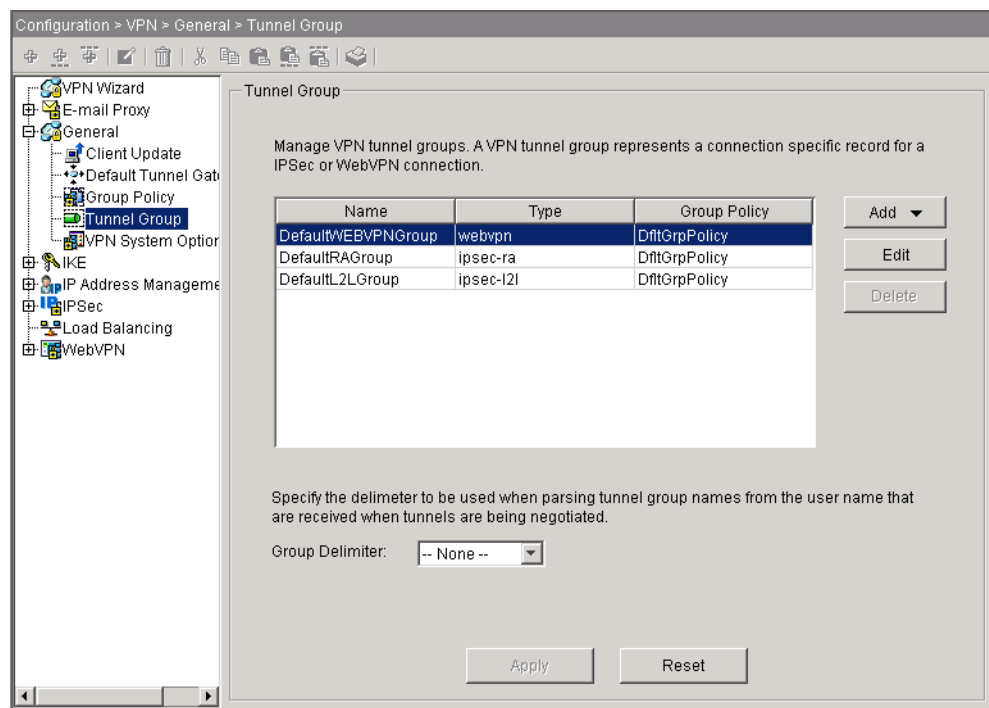
- Step 5** Click **OK** and then **Apply** to create the new group policy.

Configuring a Tunnel Group for LDAP Authentication

In the final major task, you create a tunnel group that specifies LDAP authentication by performing the following steps:

- Step 1** In the Cisco ASDM window, select **Configuration > VPN > General > Tunnel Group**.
The Tunnel Group area appears on the right side of the ASDM window as shown in [Figure 6-9](#).

Figure 6-9 Tunnel Group Area



- Step 2** Click **Add** in the tunnel Group area and choose the type of tunnel group.
In our example, we choose IPsec for Remote Access.
The Add Tunnel Group dialog box appears.
- Step 3** Choose the **General** tab, and then choose the **AAA** tab, as shown in [Figure 6-10](#).

Figure 6-10 Add Tunnel Group Dialog Box with General and AAA Tabs Selected

The screenshot shows the 'Add Tunnel Group' dialog box with the following configuration:

- Name:** ipsec-tunnelgroup
- Type:** ipsec-ra
- General Tab:**
 - AAA Sub-tab:**
 - Authentication Server Group:** ldap-authenticat
 - Use LOCAL if Server Group fails
 - Authorization Server Group:** -- None --
 - Users must exist in the authorization database to connect
 - Accounting Server Group:** -- None --
 - Authorization Settings:**
 - Use the entire DN as the username
 - Specify individual DN fields as the username
 - Primary DN Field:** CN (Common Name)
 - Secondary DN Field:** OU (Organization Unit)
 - Password Management:**
 - Override account-disabled indication from AAA server
 - Enable notification upon password expiration to allow user to change password
 - Enable notification prior to expiration
 - Notify days prior to expiration

- Step 4** Enter the name of the tunnel group in the Name field.
In our example, the tunnel group name is ipsec-tunnelgroup.
- Step 5** From the Authentication Server Group menu, chose the AAA server group you configured for authentication.
In our example, the authentication server group name is ldap-authenticat.
- Step 6** Click **OK** at the bottom of the Add Tunnel Group dialog box.
- Step 7** Click **Apply** at the bottom of the ASDM window to include the changes to the running configuration.
You have completed this example of the minimal steps required to configure the security appliance for LDAP authentication and authorization.

