



CHAPTER 3

Configuring New Features in ACS 4.2

This chapter describes how to configure several new features provided with ACS 4.2.

For information on new features that accompany both ACS for Windows and the ACS SE, see:

- [New Global EAP-FAST Configuration Options, page 3-1](#)
- [Disabling of EAP-FAST PAC Processing in Network Access Profiles, page 3-3](#)
- [Disabling NetBIOS, page 3-4](#)
- [Configuring ACS 4.2 Enhanced Logging Features, page 3-5](#)
- [Configuring Group Filtering at the NAP Level, page 3-6](#)
- [Option to Not Log or Store Dynamic Users, page 3-7](#)
- [Active Directory Multi-Forest Support, page 3-7](#)

For information on new features that accompany ACS SE only, see:

- [Configuring Syslog Time Format in ACS 4.2, page 3-7](#)
- [RSA Support on the ACS SE, page 3-8](#)
- [Turning Ping On and Off, page 3-16](#)

New Global EAP-FAST Configuration Options

The EAP-FAST Configuration page in the Global Authentication Setup section contains several new options. [Figure 3-1](#) shows the new options on the EAP-FAST Configuration page.

Figure 3-1 New Global EAP-FAST Configuration Options

EAP-FAST Settings

EAP-FAST

Allow EAP-FAST

Active master key TTL: 1 months

Retired master key TTL: 3 months

Tunnel PAC TTL: 1 weeks

Client initial message:

Authority ID Info:

Allow full TLS renegotiation in case of Invalid PAC

Allow anonymous in-band PAC provisioning

Enable anonymous TLS renegotiation

Allow authenticated in-band PAC provisioning

Accept client on authenticated provisioning

Require client certificate for provisioning

When receiving client certificate, select one of the following lookup methods:

Certificate SAN lookup

Certificate CN lookup

270294

Table 3-1 describes the new EAP-FAST settings.

Table 3-1 New EAP-FAST Global Configuration Settings with Release 4.2

Option	Description
Allow Full TLS Renegotiation in Case of Invalid PAC	This option handles cases of an invalid or expired PAC. In this situation, the EAP server can select a different cipher than the one normally used with the invalid PAC to start the full TLS handshake and authentication. Check the Allow Full TLS Renegotiation in Case of Invalid PAC check box if you have clients that might attempt to authenticate by using certificates that are unusually old.
Allow Anonymous In-band PAC Provisioning	ACS provisions an end-user client with a PAC using EAP-FAST phase zero. If you check this check box, ACS establishes a secured connection with the end-user client to provide the client with a new PAC.
Enable anonymous TLS renegotiation	If you check the Allow Anonymous in-band PAC Provisioning check box, you can also check the Enable anonymous TLS renegotiation check box. Check the Enable anonymous TLS renegotiation check box if your network contains Vista clients, to prevent Vista users from being prompted twice for their password.

Disabling of EAP-FAST PAC Processing in Network Access Profiles

In the Protocols section for Network Access Profile (NAP) configuration, you can now set up a NAP that causes ACS to use EAP-FAST but not issue or accept tunnel or machine PACs.

Figure 3-2 shows the EAP-FAST section of the NAP Protocols page for ACS 4.2.

Figure 3-2 Use PAC and Do Not Use PAC Options

EAP-FAST

Allow EAP-FAST

Use PACs

Allow full TLS renegotiation in case of Invalid PAC

Allow anonymous in-band PAC provisioning

Enable anonymous TLS renegotiation

Allow authenticated in-band PAC provisioning

Accept client on authenticated provisioning

Require client certificate for provisioning

Allow Stateless session resume

Authorization PAC TTL

Do Not Use PACs

Require client certificate

Disable Client Certificate Lookup and Comparisons

Assign Group

When receiving client certificate, select one of the following lookup methods:

Certificate SAN lookup

Certificate CN lookup

Allowed inner methods

EAP-GTC

EAP-MSCHAPv2

EAP-TLS

Posture Validation:

None

Required

Optional - Client may not supply posture data. Use token

Posture only

270295

Figure 3-2 shows the new options on the NAP Protocols page.

Table 3-2 *New Options on the NAP Protocols Page*

Option	Description:
Use PACs	Click the Use PACs radio button if you want ACS to authenticate clients to which this NAP is applied by using EAP-FAST with PACs enabled. If you click the Use PACs radio button, then the same EAP-FAST configuration options that are available in the global EAP-FAST configuration are available.
Do Not Use PACs	Click the Do Not Use PACs radio button if you want ACS to authenticate clients to which this NAP is applied by using EAP-FAST without PACs enabled.
Require Client Certificate	If you click the Do Not Use PACs radio button, the Require Client Certificate option is available. Choose this option to require a client certification for EAP-FAST tunnel establishment.
Disable Client Certificate Lookup and Comparisons	If you click the Do Not Use PACs radio button, you can check the Disable Client Certificate Lookup and Comparisons check box to disable client certificate lookup and to enable EAP-FAST PKI Authorization Bypass. If you check the Disable Client Certificate Lookup and Comparisons check box, ACS establishes an EAP-FAST tunnel without authorizing the user based on user group data or a public key infrastructure (PKI) certificate in a user database; instead, ACS maps the user to a preconfigured user group.
Assign Group	If you check the Disable Client Certificate Lookup and Comparisons check box; then, from the drop-down list of user groups in the Assign Group field, select a user group to apply to the client.

Disabling NetBIOS

Because disabling NetBIOS might be desirable in some cases, you can run ACS 4.2 with NetBIOS disabled.

ACS SE 4.2 runs on a customized version of Windows 2003 that includes some but not all Windows 2003 services.



Note

Although you can use Windows 2000, Windows XP, and Windows Server 2003 to disable NetBIOS over TCP/IP (NetBT), many corporate networks do not, since most of them still have legacy (Windows 9.x or Windows NT) machines on their network. These machines need NetBIOS to function properly on a network, since they use NetBIOS to log in to domains, find one another, and establish sessions for accessing shared resources.

To disable NetBIOS over TCP/ IP in Windows 2000, XP, or 2003:

-
- Step 1** Right-click **My Network Places** and choose **Properties**.
 - Step 2** Right-click the appropriate Local Area Connection icon, and click **Properties**.
 - Step 3** Click **Internet Protocol (TCP/IP)** and choose **Properties**.
 - Step 4** Click **Advanced**, and click the **WINS** tab.
 - Step 5** On the WINS tab, enable or disable NetBIOS over TCP/IP.

The changes take effect immediately without rebooting the system.

Optionally, if you are using a DHCP server that can selectively enable and disable NetBIOS configurations through DHCP option types, you can choose the Use NetBIOS setting from the DHCP server. NetBIOS over TCP/IP can also be disabled for computers that are running Windows 2000/2003 by using the advanced DHCP option types that are supported by the Windows 2000/2003 DHCP Server service.

**Note**

Computers that are running an operating system prior to Windows 2000 will be unable to browse, locate, or create file and print share connections to a Windows 2000/XP/2003 computer with NetBIOS disabled.

Configuring ACS 4.2 Enhanced Logging Features

ACS 4.2 provides several new logging features. When you configure the CSV Failed Attempts and Passed Authentications reports, you can add several new fields:

- **Response Time**—Indicates how long it takes ACS to respond to a client after receiving an authentication request.
- **Framed-IP-address**—If ACS is configured to assign IP addresses when it receives Access-Request messages or if an incoming Access-Request contains an IP address, indicates the framed IP address.
- **Session-ID**—Indicates the session ID of a user session.

To add a field to the CSV Failed Attempts or Passed Authentications report:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**.
The Logging Configuration page opens.
 - Step 3** In the CSV column, click **Configure** next to the name of the report you want to configure.
The configuration page for the selected report opens.
 - Step 4** To add a field to the report, click the field name in the Attributes column and then click the right arrow button to move it to the Logged Attributes column.
 - Step 5** Click **Submit** to save the report configuration.
-

Configuring Group Filtering at the NAP Level

You can use ACS 4.2 to grant and deny access to users who are authenticated through a LDAP database based on the LDAP group to which the users belong. This feature is called group filtering at the NAP level.

To configure group filtering at the NAP level:

Step 1 Configure LDAP on the ACS server.

Step 2 Set up a Network Access Profile.

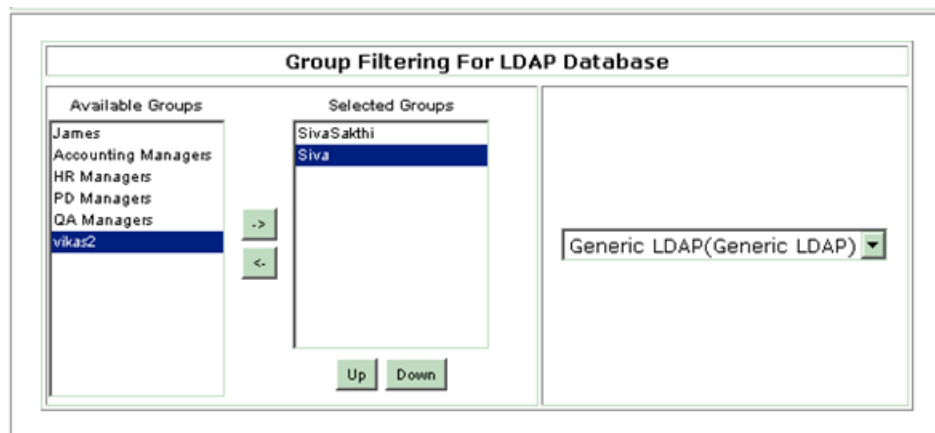
a. In the navigation bar, click **Network Access Profiles**.

The Network Access Profile page opens.

b. Click the **Authentication** link for the profile.

The Authentication page for the selected profile appears. The top of the Authentication page contains the Group Filtering for LDAP database section, as shown in [Figure 3-3](#).

Figure 3-3 Group Filtering for LDAP Database Configuration



c. From the drop-down list for LDAP databases, choose the LDAP database that you want to use to filter user access.

d. From the list of LDAP user groups in the Available Groups list, choose the groups for which to allow access.

Choose a group in the Available Groups list and click the right arrow (-->) button to move the group to the list of Selected Groups.

e. If you want to sort the lists, click the **Up** and **Down** buttons to move a group up or down in a list.

Step 3 Click **Submit**.

Option to Not Log or Store Dynamic Users

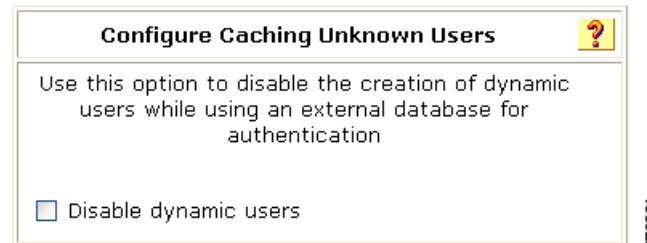
When ACS authenticates users by using external databases, such as Active Directory or LDAP, and a user is successfully authenticated with the external database, then, by default, ACS stores the information for the user in the ACS internal database. The users that ACS creates in this manner are called dynamic users.

With ACS 4.2, you can configure ACS not to create or store data on dynamic users.

To disable creation of dynamic users in the ACS internal database:

-
- Step 1** In the navigation bar, choose **External User Databases > Unknown User Policy**.
The Configure Unknown User Policy page opens.
- Step 2** Scroll down to the Configure Caching Unknown Users section, shown in [Figure 3-4](#):

Figure 3-4 Disabling Creation of Dynamic Users



- Step 3** Check the **Disable Dynamic users** check box.
- Step 4** Click **Submit**.
-

Active Directory Multi-Forest Support

ACS supports machine authentication in a multi-forest environment. Machine authentications succeed as long as an appropriate trust relation exists between the primary ACS forest and the requested domain's forest. When a requested user's or machine's domain is part of a trusted forest, machine authentication will succeed.

ACS supports user authentication between multiple forests for EAP-FAST, version 1a with PEAP, MSPEAP, and for EAP-TLS.



Note

The multi-forest feature works only where the username contains the domain information.

Configuring Syslog Time Format in ACS 4.2

ACS SE 4.2 provides a new option for configuring the time format that ACS uses to send messages to syslog servers.

In previous releases, ACS SE devices could only send syslog messages using the local time that is set on the ACS device. With release 4.2, you can configure the ACS SE to send syslog messages by using the local time setting or Greenwich Mean Time (GMT).

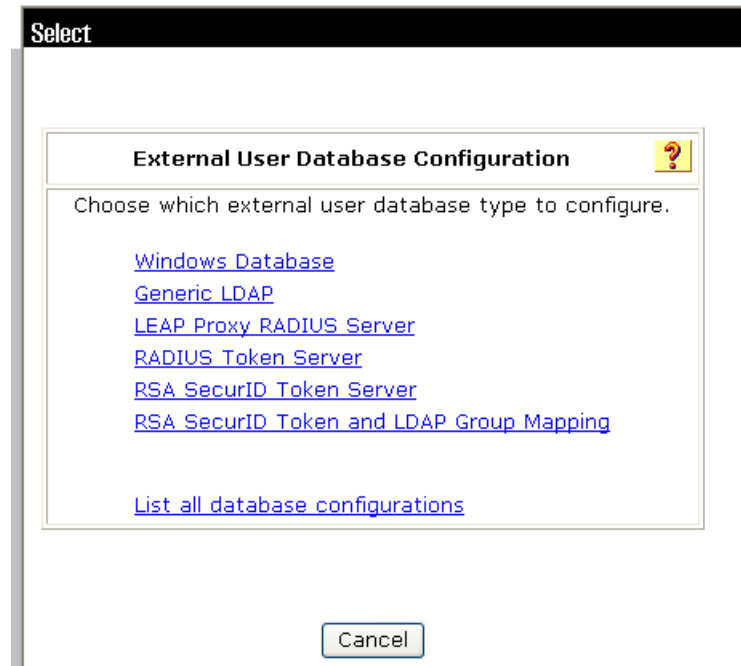
To configure the time format used for events sent to a syslog server:

-
- Step 1** In the navigation bar, choose **System Configuration > Date Format Control**.
The Date Format Control page opens.
- Step 2** In the Time Zone Selection for syslog section, specify the date format for events sent to syslog servers. To specify:
- Local time, click the **Use Local Time** radio button.
 - GMT time, click the **Use GMT Time** radio button.
- Step 3** Click **Submit and Restart**.
-

RSA Support on the ACS SE

ACS 4.2 adds support for RSA Token Server on the ACS SE. To add this support:

-
- Step 1** In the navigation bar, click **External User Databases**.
The External User Databases page opens.
- Step 2** Click **Database Configuration**.
The External User Databases Configuration page opens, as shown in [Figure 3-5](#).

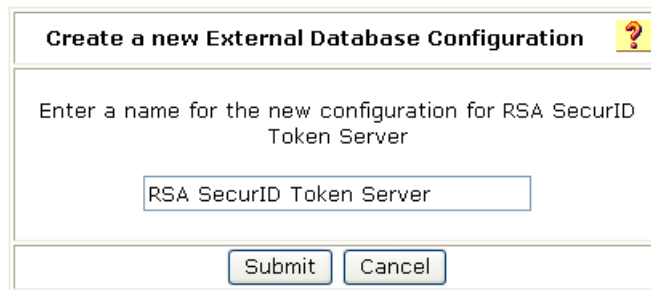
Figure 3-5 External User Databases Page (ACS SE)

Step 3 Click **RSA SecureID Token Server**.

The Database Configuration Creation page appears.

Step 4 Click **Create New Configuration**.

The Create a New External Database Configuration page appears, as shown in [Figure 3-6](#).

Figure 3-6 Create a New External Database Configuration Page.

Step 5 Enter the name for the RSA SecureID Token Server and then click **Submit**.

You are prompted to choose what to do with the Token Sever.

Step 6 Click **Configure**.

You are prompted to upload the *sdconf.rec* file.

Step 7 Click **Upload sconf.rec**.

Step 8 The Cisco Secure ACS to RSA SecurID Configuration page appears, as shown in [Figure 3-7](#).

Figure 3-7 Cisco Secure ACS to RSA SecurID Configuration Page

Cisco Secure ACS to RSA SecurID Configuration

FTP Setup

FTP Server:

Login:

Password:

Directory:

Decryption Password:

270289

Step 9 On the Cisco Secure ACS to RSA SecurID Configuration page, enter the information shown in [Table 3-3](#)

Table 3-3 RSA SecureID Server Configuration

Field	Description
FTP Server:	The IP address of the FTP server that contains the <i>sdconf.rec</i> file. This the configuration file for your RSA TokenID installation.
Login:	The login name for the FTP server.
Password:	The password for the FTP server.
Directory:	The directory on the FTP server where the <i>sdconf.rec</i> file is located.

Step 10 Click **Submit**.

Purging the RSA Node Secret File

When you change the RSA Token Server configuration, you must purge the existing Node Secret file. To purge the Node Secret file:

-
- Step 1** In the navigation bar, click **External User Databases**.
The External User Databases page opens.
 - Step 2** Click **Database Configuration**.
The External User Databases Configuration page opens.
 - Step 3** Click **RSA SecurID Token Server**.

The External User Database Configuration page opens.

Step 4 Click **Configure**.

The Cisco Secure ACS to RSA SecurID Configuration page opens.

Step 5 Click **Purge Node Secret**.

Configuring RSA SecurID Token and LDAP Group Mapping

You can perform authentication with RSA in native mode and also by using LDAP group mapping, with RSA. If you use RSA with LDAP group mapping, then the user's LDAP group membership controls authorization. When RSA native mode authentication succeeds, group mapping occurs with LDAP. The user's group is applied based on the group mapping configuration.



Note

Before you configure RSA authentication with LDAP Group Mapping, ensure that you have the correct installation or configuration of the third-party DLLs required to support this type of external database.

To configure RSA authentication with LDAP Group Mapping:

Step 1 [Enable RSA support as described in RSA Support on the ACS SE, page 3-8.](#)

Step 2 In the navigation bar, click **External User Databases**.

Step 3 Click **Database Configuration**.

ACS lists all possible external user database types.

Step 4 Click **RSA SecurID Token and LDAP Group Mapping**.

The External Database Configuration page appears.

Step 5 Click **Configure**.

The LDAP Native RSA Configuration page opens.

Step 6 Click **Configure LDAP**.

The RSA SecurID Token and LDAP Group Mapping Configuration page opens, as shown in [Figure 3-8](#).

Step 8 If you want to limit authentications processed by this LDAP configuration to usernames with a specific domain qualification:



Note For information about domain filtering, see “Domain Filtering” in chapter 12 of the *User Guide for Cisco Secure ACS, 4.2*.

- a. Under Domain Filtering, click the **Only process usernames that are domain qualified** radio button.
- b. From the Qualified by list, choose the applicable type of domain qualification: Suffix or Prefix. Only one type of domain qualification is supported per LDAP configuration.

For example, if you want this LDAP configuration to authenticate usernames that begin with a specific domain name, select **Prefix**. If you want this LDAP configuration to authenticate usernames that end with a specific domain name, select **Suffix**.

- c. In the Domain Qualifier box, type the name of the domain for which you this LDAP configuration should authenticate usernames. Include the delimiting character that separates the user ID from the domain name. Ensure that the delimiting character appears in the applicable position: at the end of the domain name if **Prefix** is selected on the Qualified by list; at the beginning of the domain name if Suffix is selected on the Qualified by list.

Only one domain name is supported per LDAP configuration. You can type up to 512 characters.

- d. If you want ACS to remove the domain qualifier before submitting it to the LDAP database, check the **Strip domain before submitting username to LDAP server** check box.
- e. If you want ACS to pass the username to the LDAP database *without* removing the domain qualifier, uncheck the **Strip domain before submitting username to LDAP server** check box.

Step 9 If you want to enable ACS to strip domain qualifiers from usernames before submitting them to an LDAP server:



Note For information about domain filtering, see “Domain Filtering” in chapter 12 of the *User Guide for Cisco Secure ACS, 4.2*.

- a. Under Domain Filtering, click the **Process all usernames after stripping domain name and delimiter** radio button.
- b. If you want ACS to strip prefixed domain qualifiers, check the **Strip starting characters through the last X character** check box, and then type the domain-qualifier delimiting character in the X box.



Note The X box cannot contain the following special characters: the pound sign (#), the question mark (?), the quote (“), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). ACS does not allow these characters in usernames. If the X box contains any of these characters, stripping fails.

- c. If you want ACS to strip suffixed domain qualifiers, check the **Strip ending characters from the first X character** check box, and then type the domain-qualifier delimiting character in the X box.



Note The *X* box cannot contain the following special characters: the pound sign (#), the question mark (?), the quote (“), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). ACS does not allow these characters in usernames. If the *X* box contains any of these characters, stripping fails.

- Step 10** Under Common LDAP Configuration, in the User Directory Subtree box, type the DN of the tree containing all your users.
- Step 11** In the Group Directory Subtree box, type the DN of the subtree containing all your groups.
- Step 12** In the User Object Type box, type the name of the attribute in the user record that contains the username. You can obtain this attribute name from your Directory Server. For more information, refer to your LDAP database documentation.



Note The default values in the UserObjectType and following fields reflect the default configuration of the Netscape Directory Server. Confirm all values for these fields with your LDAP server configuration and documentation.

- Step 13** In the User Object Class box, type the value of the LDAP `objectType` attribute that identifies the record as a user. Often, user records have several values for the `objectType` attribute, some of which are unique to the user, while others are shared with other object types. Choose a value that is not shared.
- Step 14** In the GroupObjectType box, type the name of the attribute in the group record that contains the group name.
- Step 15** In the GroupObjectClass box, type a value for the LDAP `objectType` attribute in the group record that identifies the record as a group.
- Step 16** In the GroupAttributeName box, type the name of the attribute of the group record that contains the list of user records who are a member of that group.
- Step 17** In the Server Timeout box, type the number of seconds that ACS waits for a response from an LDAP server before determining that the connection with that server has failed.
- Step 18** To enable failover of LDAP authentication attempts, check the **On Timeout Use Secondary** check box.
- Step 19** In the Failback Retry Delay box, type the number of minutes after the primary LDAP server fails to authenticate a user that ACS resumes sending authentication requests to the primary LDAP server first.



Note To specify that ACS should always use the primary LDAP server first, type zero (0) in the Failback Retry Delay box.

- Step 20** In the Max. Admin Connection box, enter the number of maximum concurrent connections with LDAP administrator account permissions.
- Step 21** For the Primary LDAP Server and Secondary LDAP Server tables:



Note If you did not check the **On Timeout Use Secondary** check box, you do not need to complete the options in the Secondary LDAP Server table.

- a. In the Hostname box, type the name or IP address of the server that is running the LDAP software. If you are using DNS on your network, you can type the hostname instead of the IP address.

- b. In the Port box, type the TCP/IP port number on which the LDAP server is listening. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information by viewing those properties on the LDAP server. If you want to use secure authentication, port 636 is usually used.
- c. To specify that ACS should use LDAP version 3 to communicate with your LDAP database, check the **LDAP Version** check box. If the LDAP Version check box is not checked, ACS uses LDAP version 2.
- d. If you want ACS to use SSL to connect to the LDAP server, check the **Use secure authentication** check box and complete the next three steps. If you do not use SSL, the username and password credentials are normally passed over the network to the LDAP directory in clear text.
- e. ACS SE only: If you checked the **Use Secure Authentication** check box, perform one of the following procedures:
 - Check the:
 - **Trusted Root CA** check box, and in the adjacent drop-down list, choose a **Trusted Root CA**.
 - **Certificate Database Path** check box, and download a *cert7.db* file.

**Note**

To download a *cert7.db* certificate database file to ACS now, complete the steps in “Downloading a Certificate Database (Solution Engine Only)” in Chapter 12 of the *User Guide for Cisco Secure ACS, 4.2*, and then continue with Step f. You can download a certificate database later. Until a certificate database is downloaded for the current LDAP server, secure authentication to this LDAP server fails.

- f. ACS for Windows only: If you checked the **Use Secure authentication** check box, perform one of the following procedures. Click the:
 - **Trusted Root CA** radio button, and in the adjacent drop-down list, choose a **Trusted Root CA**.
 - **Certificate Database Path** radio button, and in the adjacent box, type the path to the Netscape *cert7.db* file, which contains the certificates for the server to be queried and the trusted CA.
- g. The Admin DN box requires the fully qualified Distinguished Name (DN) of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory subtree.

In the Admin DN box, type the following information from your LDAP server:

```
uid=user id, [ou=organizational unit, ]
[ou=next organizational unit]o=organization
```

where *user id* is the username

organizational unit is the last level of the tree

next organizational unit is the next level up the tree.

For example:

```
uid=joesmith,ou=members,ou=administrators,o=cisco
```

**Tip**

If you are using Netscape DS as your LDAP software, you can copy this information from the Netscape console.

- h. In the Password box, type the password for the administrator account that is specified in the Admin DN box. The server determines password case sensitivity.

Step 22 Click **Submit**.

**Note**

ACS saves the generic LDAP configuration that you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication.

Turning Ping On and Off

With ACS 4.2, you can enable and disable pinging of the ACS SE device. Prior to release 4.2, when remote devices sent a ping request to an SE device, the ping was always rejected because, by default, the Cisco Security Agent (CSA) runs on the ACS SE device. CSA automatically rejects remote ping requests.

ACS 4.2 provides software patches for you to turn ping on and off by updating the policies in the CSA:

- **Ping Turn On Patch**—This patch turns on the ping option in the CSA, which makes it possible to ping the ACS SE.
- **Ping Turn Off Patch**—This patch turns off the ping option in the CSA, which causes the ACS SE to reject pings.

For detailed information on installing these patches, see “Turning Ping On and Off” in Chapter 3 of the the *Installation Guide for Cisco Secure ACS Solution Engine, 4.2*, “Installing and Configuring Cisco Secure ACS Solution Engine 4.2.”