



CHAPTER 6

Agentless Host Support Configuration Scenario

This chapter describes how to configure the agentless host feature in Cisco Secure Access Control Server, hereafter referred to as ACS.



Note

The procedure in this chapter describes how to configure agentless host support by using ACS with a Lightweight Directory Access Protocol (LDAP) database. You can also configure agentless host support by using the ACS internal database; but, using an LDAP database is generally more efficient.

This chapter contains the following sections:

- [Overview of Agentless Host Support, page 6-1](#)
- [Summary of Configuration Steps, page 6-3](#)
- [Basic Configuration Steps for Agentless Host Support, page 6-4](#)
- [Configuration Steps for Audit Server Support, page 6-24](#)

Overview of Agentless Host Support

Many hosts that ACS authenticates run agent software that requests access to network resources and receives authorization from ACS. However, some hosts do not run agent software. For example:

- Many 802.1x port security deployments authenticate hosts that do not have appropriate security agent software, such as Cisco Trust Agent.
- When an agentless host is connected to a Layer 2 device and an Extensible Authentication Protocol over User Datagram Protocol timeout (EoU timeout) occurs, in-band posture validation cannot occur.

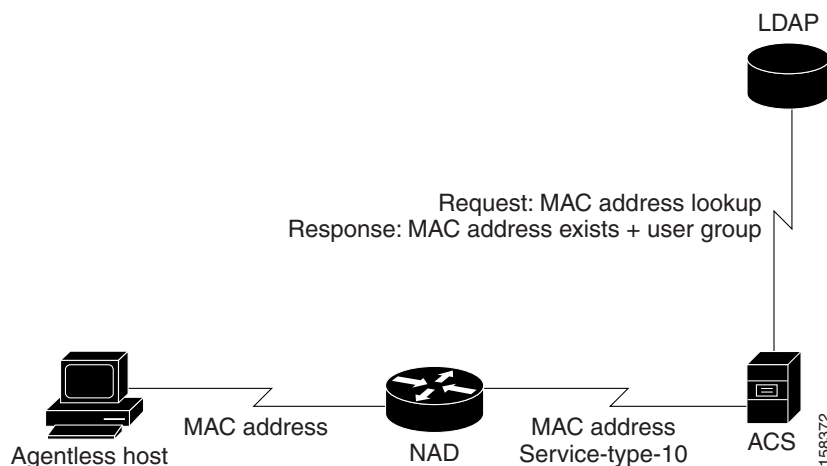
ACS solves this problem by using the MAC address of the host device to identify and authenticate the host. This technique is called MAC authentication bypass (MAB).

1. When an agentless host connects to a network access device (NAD), the NAD detects that the host does not have an appropriate software agent and uses the host's MAC address to identify it.
2. The NAD sends ACS a RADIUS authorization request with `servicetype=10` and the MAC address of the host contained in the `calling-station-id` attribute.

3. If you configure ACS for MAB, it searches the authentication database for the host's MAC address. The database can be:
 - ACS internal
 - LDAP (if you configure LDAP)
4. During the database lookup:
 - ACS looks up the MAC address in an identity store (the internal ACS database or an LDAP database).
 - ACS maps the MAC address to an ACS user group.
 - If ACS finds the MAC address, ACS associates the access request to an ACS user group.
 - If ACS does not find the MAC address, ACS assigns the access request to a default group that has been configured for failed MAB. At this stage, ACS proceeds with authorization as for all other access requests.
 - The expected value in the `calling-station-id` attribute is a MAC address; however, if the attribute contains a different value (IP address), ACS looks for the IP address in the access database.
 - ACS applies authorization rules based on the user group and associated policies that a Network Access Profile contains.

Figure 6-1 shows the flow of MAB information.

Figure 6-1 MAB Flow



Using Audit Servers and GAME Group Feedback

You can configure ACS to use audit servers. An audit server is a device that checks the information that the NAD provides against a list of predetermined device types.

The audit server can categorize an end device and provide additional information to ACS. ACS can then make a group assignment decision based on the categorization of the device. For example, if the device is a printer, ACS can assign the device to a user group that includes printers.

In a Cisco Network Admission Control (NAC) environment, ACS supports audit server authentication by enabling Generic Authorization Message Exchange (GAME) group feedback.

GAME group feedback provides an added security check for MAC address authentication by checking the device type categorization that ACS determines by associating a MAC address with a user group against information stored in a database on an audit server.

To use the GAME group feedback feature, you must add a NAC attribute-value pair to the ACS RADIUS dictionary before configuring a posture validation policy that uses GAME group feedback.

You then configure a posture validation policy in a NAP that requests device type authentication from the audit server. For details on configuring posture validation, see [Enable Posture Validation, page 9-74](#).

The detailed steps for configuring GAME group feedback are described in [Enable GAME Group Feedback, page 9-79](#) in Chapter 9, “NAC Configuration Scenario.”

Summary of Configuration Steps

To configure agentless host support in ACS:

Step 1 Install ACS for Windows or ACS Solution Engine (ACS SE).

See [Step 1: Install ACS, page 6-4](#) for details.

Step 2 Configure a RADIUS AAA client.

See [Step 2: Configure a RADIUS AAA Client, page 6-5](#) for details.

Configure restrictions on the admin user password.

Step 3 Install and set up an ACS security certificate:



Note This step is required to enable posture validation and Network Access Profiles.

- a. Obtain certificates and copy them to the ACS host.
- b. Run the Windows certificate import wizard to install the certificate
- c. Enable security certificates on the ACS installation.
- d. Install the CA certificate.
- e. Add a trusted certificate.

See [Step 3: Install and Set Up an ACS Security Certificate, page 6-6](#) for details.

Step 4 Configure LDAP support for MAB:

- a. Configure an external LDAP database for MAB support.
- b. Create One or More LDAP Database Configurations in ACS.

See [Step 4: Configure LDAP Support for MAB, page 6-10](#) for details.

Step 5 Configure user groups for MAB segments.

See [Step 5: Configure User Groups for MAB Segments, page 6-17](#) for details.

Step 6 Enable agentless request processing:

- a. Create a new Network Access Profile.
- b. Enable agentless host processing for the profile.
- c. Configure MAB.

See [Step 6: Enable Agentless Request Processing, page 6-18](#) for details.

Step 7 Configure logging and reports.

Add the **Bypass Info** attribute to the Passed Authentications and Failed Attempts reports. See [Step 7: Configure Logging and Reports, page 6-23](#).



Note

If you are using ACS with NAC, configure audit server support and, optionally, configure GAME group feedback. See [Configure GAME Group Feedback, page 6-24](#) for details.

Basic Configuration Steps for Agentless Host Support

This section describes the basic configuration steps for agentless host support.

Step 1: Install ACS

This section describes the installation process that you perform to run ACS, which runs on a Windows 2000 Server, a Windows 2003 system, or a Cisco Secure ACS SE.

To install ACS:

Step 1 Start ACS installation.

For detailed information on ACS installation, refer to the:

- *Installation Guide for Cisco Secure ACS for Windows 4.2*
- *Installation Guide for Cisco Secure ACS Solution Engine 4.2*

During the installation process, you are prompted to enter a password for encrypting the internal database.

Step 2 Enter a password that is at least 8 characters long, and contains letters and numbers.

The ACS installation process for ACS for Windows automatically creates a shortcut to the ACS administrative GUI on your desktop.



Note

If you are installing ACS on the ACS SE, you must manually create an administrative GUI user by using the **add-guiadmin** command to create a GUI account. For information on this command, see Appendix A of the *Installation Guide for Cisco Secure ACS Solution Engine 4.2*, “Command Reference.” You can then access the administrative GUI through a supported browser. For a list of supported browsers, see *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Release 4.1*.

Step 3 Double-click the ACS Admin icon to open a browser window to the ACS administrative GUI.

Step 4 If you do not see the ACS Admin icon on the desktop, open your browser from the machine on which you installed ACS and go to one of the following locations:

- `http://IP_address:2002`
- `http://hostname:2002`

where *IP_address* is the IP address of the host that is running ACS and *hostname* is the *hostname* of the host that is running ACS.

Step 2: Configure a RADIUS AAA Client

Before you can configure agentless host support, you must configure a RADIUS AAA client.

To configure a RADIUS AAA client:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using Network Device Groups (NDGs), click the name of the NDG to which you want to assign the AAA client. Then, click **Add Entry** below the AAA Clients table.
- To add AAA clients when you have not enabled NDGs, click **Add Entry** below the AAA Clients table.

The Add AAA Client page opens, shown in [Figure 6-2](#).

Figure 6-2 Add AAA Client Page

Add AAA Client

AAA Client Hostname

AAA Client IP Address

Shared Secret

Network Device Group

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format ASCII Hexadecimal

Authenticate Using

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

158375

- Step 3** In the AAA Client Hostname box, type the name assigned to this AAA client (up to 32 alphanumeric characters).
- Step 4** In the AAA Client IP Address box, type the AAA client IP address or addresses.
- Step 5** If you are using NDGs, from the Network Device Group list, select the name of the NDG to which this AAA client should belong, or select **Not Assigned** to set this AAA client to be independent of NDGs
- Step 6** From the Authenticate Using list, select **RADIUS (IOS/PIX)**.
- Step 7** Specify additional AAA client settings as required.
- Step 8** Click **Submit + Apply**.

Step 3: Install and Set Up an ACS Security Certificate

This section describes a simplified procedure for the ACS for Windows platform. For detailed information on installing certificates, and also for information on how to install certificates on the Cisco Secure ACS SE platform, see Chapter 9 of the *User Guide for Cisco Secure ACS 4.2*, “Advanced Configuration: Authentication and Certificates.”

The steps in this section are required to enable posture validation, which is used in Network Access Profiles.

Obtain Certificates and Copy Them to the ACS Host

To copy a certificate to the ACS host:

-
- Step 1** Obtain a security certificate.
- Step 2** Create a `\Certs` directory on the ACS server.
- Open a DOS command window.
 - To create a certificates directory, enter:

```
mkdir <selected_drive>:\Certs
```

where *selected_drive* is the currently selected drive.
- Step 3** Copy the following files to the `\Certs` directory:
- `server.cer` (server certificate)
 - `server.pvk` (server certificate private key)
 - `ca.cer` (CA certificate)
-

Run the Windows Certificate Import Wizard to Install the Certificate (ACS for Windows)

To run the Windows Certificate Import wizard to install the certificate on the server:

-
- Step 1** Start Windows Explorer.
- Step 2** Go to `<selected_drive>:\Certs`.
where *selected_drive* is the currently selected drive.
- Step 3** Double-click the `\Certs\ca.cer` file.
The Certificate dialog appears.

Step 4 Select **Install Certificate**.

The Windows Certificate Import wizard starts.

Step 5 To install the certificate, follow the instructions that the wizard displays.**Step 6** Accept the default options for the wizard.

Note Only perform this process once on a Windows 2000 Server.

Enable Security Certificates on the ACS Installation

To enable security certificates:

Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **ACS Certificate Setup**.**Step 3** Click **Install ACS Certificate**.**Step 4** The Install ACS Certificate page opens, shown in [Figure 6-3](#).

Figure 6-3 *Install ACS Certificate Page*

Install ACS Certificate

Step 5 Ensure that you click the **Read certificate from file** radio button.**Step 6** In the Certificate file text box, enter the server certificate location (path and name); for example `c:\Certs\server.cer`.**Step 7** In the Private Key File text box, type the server certificate private key location (path and name); for example: `c:\Certs\server.pvk`.**Step 8** In the Private Key password text box, type **1111**.**Step 9** Click **Submit**.**Step 10** ACS displays a message indicating that the certificate has been installed and instructs you to restart the ACS services.

Step 11 Do not restart the services at this time.

Restart the services later, after you have completed the steps for adding a trusted certificate. See [Add a Trusted Certificate](#), page 6-9.

Install the CA Certificate

To install the CA Certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.

Step 2 The ACS Certification Authority Setup page appears, shown in [Figure 6-4](#).

Figure 6-4 ACS Certification Authority Setup Page

ACS Certification Authority Setup

Step 3 In the CA certificate file box, type the CA certificate location (path and name). For example:
`c:\Certs\ca.cer`

Step 4 Click **Submit**.

Add a Trusted Certificate

After you add a server certificate and set up the certificate authority, install a trusted certificate.

To add a trusted certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > Edit Certificate Trust List**.

The Edit Certificate Trust List appears.

Step 2 Locate the trusted certificate that you want to install and check the corresponding check box by the certificate name. For example, find the **Stress** certificate and check the corresponding check box.

Step 3 Click **Submit**.

Step 4 To restart ACS, choose **System Configuration > Service Control**, and then click **Restart**.

Step 4: Configure LDAP Support for MAB

You can configure the ACS internal database to manage MAB used with the agentless host feature; however, if you have a large number of MAC addresses to process (for example, several thousand), it is more efficient to use an external LDAP database than to configure the MAC address mappings manually through the ACS GUI.

To configure LDAP support for MAB:

-
- Step 1** Configure an External LDAP database for MAB support.
See [Configure an External LDAP Database for MAB Support, page 6-10](#) for details.
- Step 2** Create one or more LDAP database configurations in ACS.
See [Create One or More LDAP Database Configurations in ACS, page 6-13](#) for details.
-

Configure an External LDAP Database for MAB Support

Configure one or more external LDAP databases for MAB support. In each LDAP database, create:

- Device records that describe the agentless hosts that ACS will authenticate.
- LDAP groups that define an LDAP schema to enable MAB for agentless host support.

[Example 6-1](#) shows portions of a sample Lightweight Directory Interchange Format (LDIF) file that defines an LDAP database for agentless host support.

Example 6-1 Sample LDAP Schema for MAB Support

```
dn: ou=MAB Segment, o=mycorp
ou: MAB Segment
objectClass: top
objectClass: organizationalUnit
description: MAC Authentication Bypass Sub-Tree

dn: ou=MAC Addresses, ou=MAB Segment, o=mycorp
ou: MAC Addresses
objectClass: top
objectClass: organizationalUnit

dn: ou=MAC Groups, ou=MAB Segment, o=mycorp
ou: MAC Groups
objectClass: top
objectClass: organizationalUnit

dn: cn=user00-wxp.emea.mycorp.com,ou=MAC Addresses, ou=MAB Segment, o=mycorp
ipHostNumber: 10.56.60.100
objectClass: top
objectClass: ipHost
objectClass: ieee802Device
macAddress: 00:11:22:33:44:55
cn: user00-wxp.emea.mycorp.com

dn: cn=user11-wxp.emea.mycorp.com,ou=MAC Addresses, ou=MAB Segment, o=mycorp
ipHostNumber: 10.56.60.111
objectClass: top
objectClass: ipHost
objectClass: ieee802Device
```

```

macAddress: 11-22-33-44-55-66
cn: user11-wxp.emea.mycorp.com

dn: cn=Group_1_colon,ou=MAC Groups, ou=MAB Segment, o=mycorp
objectClass: top
objectClass: groupofuniquenames
description: group of delimited MAC Addresses
uniqueMember: cn=user00-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
o=mycorp
uniqueMember: cn=user77a-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment
, o=mycorp
uniqueMember: cn=user88-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
o=mycorp
cn: Group_1_colon

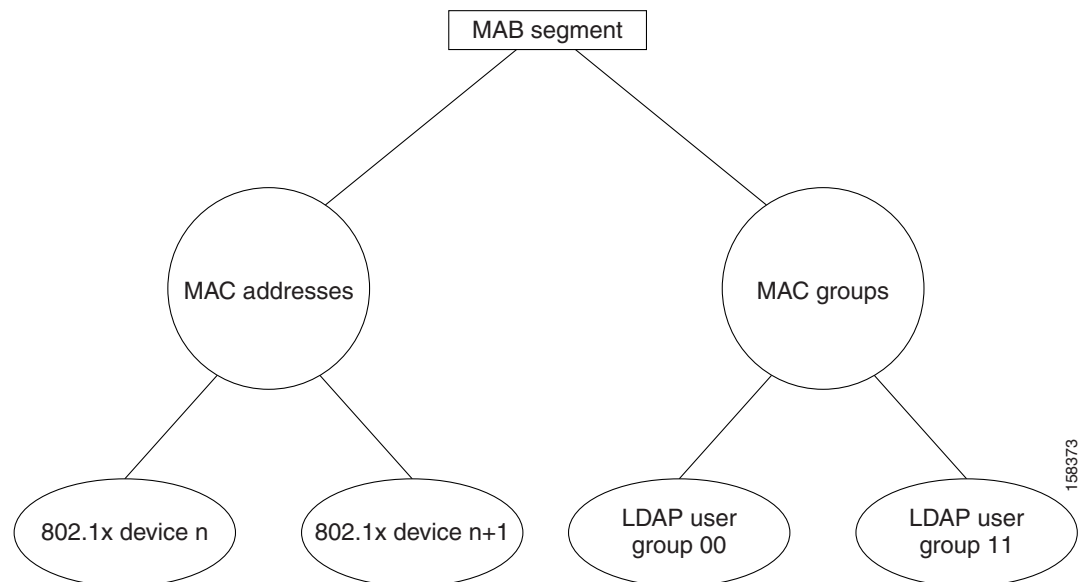
dn: cn=Group_2_dash,ou=MAC Groups, ou=MAB Segment, o=mycorp
objectClass: top
objectClass: groupofuniquenames
description: group of - delimited MAC Addresses
uniqueMember: cn=user11-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
o=mycorp
uniqueMember: cn=user77b-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment
, o=mycorp
cn: Group_2_dash

```

Description of the Settings in the Sample LDAP Schema

Figure 6-5 shows the tree structure of the LDAP schema that is presented in Example 6-1.

Figure 6-5 Tree Structure for a MAB Support LDAP Schema



156373

How the Subtrees Work

The sample LDAP schema in [Example 6-1](#) contains code to define two subtrees:

```
dn: ou=MAC Addresses, ou=MAB Segment, o=mycorp
ou: MAC Addresses
objectClass: top
objectClass: organizationalUnit

dn: ou=MAC Groups, ou=MAB Segment, o=mycorp
ou: MAC Groups
objectClass: top
objectClass: organizationalUnit
```

The LDAP subtrees are:

- **MAC Addresses**—A user directory subtree that contains device records that specify MAC addresses for agentless hosts (IEEE 802.1x devices that require agentless host authentication by ACS).

When you specify a user directory subtree during LDAP configuration in the ACS user interface, you enter the name assigned to the user directory subtree in your LDAP schema in the User Directory Subtree text box.

- **MAC Groups**—A group directory subtree that contains LDAP user groups of users who connect from specified MAC devices that are identified in the device records.

When you specify a group directory subtree during LDAP configuration in the ACS user interface, you enter the name assigned to the group directory subtree in your LDAP schema in the Group Directory Subtree text box.

How the LDAP User Groups Work

Each LDAP user group record sets up an LDAP user group that maps users connecting through one or more devices to the specified group.

For example, the LDAP user group identified as `cn=Group_1_colon` sets up an LDAP user group that will map users connecting from the host at 10.56.60.100 as well as from two other hosts:

```
dn: cn=Group_1_colon,ou=MAC Groups, ou=MAB Segment, o=mycorp
objectClass: top
objectClass: groupofuniquenames
description: group of delimited MAC Addresses
uniqueMember: cn=user00-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
o=mycorp
uniqueMember: cn=user77a-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment
, o=mycorp
uniqueMember: cn=user88-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
o=mycorp
cn: Group_1_colon
```

ACS queries the LDAP database to determine to which user groups to assign users who connect from a host with a specified MAC address. ACS then assign users in the LDAP user group to a specified ACS user group that you configure.

Table 6-1 describes the attributes of the sample LDAP groups.

Table 6-1 Attributes in LDAP User Groups for Agentless Host Support

Attribute Name	Description
objectClass	<p>The value in the example indicates that this is a “group of unique names.” The value that you specify here must match the name that you specify in the Group Object Class text box when you specify the Common LDAP configuration during ACS LDAP configuration.</p> <p>For information on configuring LDAP, see Configure an External LDAP Database for MAB Support, page 6-10.</p>
uniqueMember	<p>The value in the example is uniqueMember. One or more uniqueMember entries are used to specify one or more device type records that have been set up in the LDAP schema to define agentless hosts with specified MAC addresses. The objectClass field in the LDAP user group shown in the previous code sample includes user00, user77a, and user88.</p> <p>The name that you give to this field in your LDAP schema must match the value that you enter in the Group Attribute Name text box when you specify the common LDAP configuration during ACS LD configuration.</p> <p>For information on configuring LDAP, see Configure an External LDAP Database for MAB Support, page 6-10.</p>

Create One or More LDAP Database Configurations in ACS

After you have configured one or more LDAP databases to support MAB, configure ACS to query the LDAP databases.

The settings in the following procedure are based on the LDAP schema described in the previous section, [Configure an External LDAP Database for MAB Support, page 6-10](#). For your ACS installation, configure ACS based on the schema that you set up for your network.

To create a LDAP configuration in ACS:

-
- Step 1** In the navigation bar, click **External User Databases**.
The External User Databases page opens.
- Step 2** Click **Database Configuration**.
The External User Database Configuration page opens.
- Step 3** Click **Generic LDAP**.
The Database Configuration Creation table appears. If an LDAP configuration exists, the External User Database Configuration table also appears.
- Step 4** Do one of the following. If:
- There are no existing LDAP database configurations, click **Create New Configuration**.
 - The External User Database table appears, click **Configure**.
- Step 5** If you are creating a new LDAP configuration, enter the name of the new configuration for generic LDAP and then click **Submit**.
- Step 6** Click **Configure**.
The Generic LDAP Configuration page appears and contains four sections:
- **Domain Filtering**—Use to configure domain filtering, which is an optional configuration setting.

- **Common LDAP Configuration**—Configure the settings in this section to specify how ACS queries the LDAP database.
- **Primary LDAP Server**—Configure the settings in this section to specify the primary LDAP server.
- **Secondary LDAP Server**—Configure the settings in this section if you are setting up LDAP failback.

Step 7 If you want to set up Domain Filtering, refer to the “Configuring a Generic LDAP External User Database” section in Chapter 12 of the *User Guide for Cisco Secure Access Server 4.2*.

Step 8 Specify the common LDAP configuration

Figure 6-6 shows the Common LDAP Configuration section.

Figure 6-6 Common LDAP Configuration Section

Common LDAP Configuration	
User Directory Subtree	ou=MAC Addresses, ou=MAB Segment,
Group Directory Subtree	ou=MAC Groups, ou=MAB Segment, o=
UserObjectType	macAddress
UserObjectClass	ieee802Device
GroupObjectType	cn
GroupObjectClass	ieee802Device
Group Attribute Name	uniqueMember
Server Timeout	30 seconds
On Timeout Use Secondary	<input type="checkbox"/>
Failback Retry Delay	0 minutes
Max. Admin Connections	40

You must specify:

- **User Directory Subtree**—Enter the distinguished name (DN) of the user directory subtree that contains all users. In MAB configuration, the users are, in effect, host devices.
In the LDAP schema shown in Example 6-1, the DN of the User Directory Subtree is `ou=MAC Addresses, ou=MAB Segment, o=mycorp`.
- **Group Directory Subtree**—Enter the DN for the group directory subtree that contains all user groups as defined in your LDAP schema. In MAB configuration, the members of user groups are actually groups of MAC addresses.
In the LDAP schema shown in Example 6-1, the DN of the group directory subtree is `ou=MAC Groups, ou=MAB Segment, o=cisco`.
- **UserObjectType**—Enter the name of the user object type that is defined in your LDAP schema. In the LDAP schema shown in Example 6-1, the user object type is specified as `macAddress`.

- **UserObjectClass**—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, some of which are shared with other object types. In the LDAP schema shown in [Example 6-1](#), the user object class is specified as `ieee802Device`.
- **GroupObjectType**—The name of the attribute in the group record that contains the group name. In the LDAP schema shown in [Example 6-1](#), this is `cn`.
- **GroupObjectClass**—For MAB configuration, specify the name of a device record that you have set up in your LDAP schema. For example, in [Example 6-1](#), the group object class is `ieee802Device`.
- **GroupAttributeName**—For MAB configuration, specify the name of the LDAP attribute that specifies a LDAP user group. For example, in [Example 6-1](#), each member of a LDAP user group is specified in a `uniqueMember` attribute.
 - **Server Timeout**—The number of seconds that ACS waits for a response from an LDAP server before determining that the connection with that server failed.
 - **On Timeout Use Secondary**—Determines whether ACS performs failover of LDAP authentication attempts.
 - **Failback Retry Delay**—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. A value of zero (0) causes ACS to always use the primary LDAP server first.
 - **Max. Admin Connections**—The maximum number of concurrent connections (greater than zero (0)) with LDAP administrator account permissions that can run for a specific LDAP configuration. These connections are used to search the directory for users and groups under the User Directory Subtree and Group Directory Subtree.

Specify LDAP server configuration information:

[Figure 6-7](#) shows the Primary LDAP Server and Secondary LDAP Server configuration sections.

Figure 6-7 LDAP Server Configuration Sections

Primary LDAP Server	
Hostname	<input type="text"/>
Port	<input type="text" value="389"/> Default is 389
LDAP Version	<input checked="" type="checkbox"/> Use LDAP V3
Security	<input type="checkbox"/> Use Secure Authentication
<input type="radio"/> Trusted Root CA	<input type="text" value="--- none selected ---"/>
<input checked="" type="radio"/> Certificate DB Path	<input type="text"/>
Admin DN	<input type="text"/>
Password	<input type="text"/>
Secondary LDAP Server	
Hostname	<input type="text"/>
Port	<input type="text" value="389"/> Default is 389
LDAP Version	<input checked="" type="checkbox"/> Use LDAP V3
Security	<input type="checkbox"/> Use Secure Authentication
<input type="radio"/> Trusted Root CA	<input type="text" value="--- none selected ---"/>
<input checked="" type="radio"/> Certificate DB Path	<input type="text"/>
Admin DN	<input type="text"/>
Password	<input type="text"/>

a. For the primary LDAP server specify:

- **Hostname**—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.
- **Port**—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 the default.
- **LDAP Version**—ACS uses LDAP version 3 or version 2 to communicate with your LDAP database. If you check this check box, ACS uses LDAP version 3. If it is unchecked, ACS uses LDAP version 2.
- **Security**—ACS uses SSL to encrypt communication between ACS and the LDAP server. If you do not enable SSL, user credentials are passed to the LDAP server in clear text. If you select this option, then you must select **Trusted Root CA** or **Certificate Database Path**. ACS supports only server-side authentication for SSL communication with the LDAP server.

ACS SE Only:

You must ensure that the Port box contains the port number used for SSL on the LDAP server.

- **Trusted Root CA**—LDAP over SSL includes the option to authenticate by using the certificate database files other than the Netscape *cert7.db* file. This option uses the same mechanism as other SSL installations in the ACS environment. Select the certification authority that issued the server certificate that is installed on the LDAP server.
- **Certificate DB Path:** For ACS for Windows, this is the path to the Netscape *cert7.db* file. For the ACS SE, this option provides a link to the Download Certificate Database page.

For detailed information on this field, refer to the “LDAP Configuration Options” section in Chapter 12 of the *User Guide for Cisco Secure Access Control Server*, “User Databases.”

- **Admin DN**—The DN of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory Subtree. It must contain the following information about 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, and *next organizational unit* is the next level up the tree.

For example:

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

You can use anonymous credentials for the administrator username if the LDAP server is configured to make the group name attribute visible in searches by anonymous credentials. Otherwise, you must specify an administrator username that permits the group name attribute to be visible to searches.

**Note**

If the administrator *username* that you specify does not have permission to see the *group name* attribute in searches, group mapping fails for users whom LDAP authenticates.

- **Password**—The password for the administrator account that you specified in the Admin DN box. The LDAP server determines case sensitivity.
- b. If you want to set up LDAP server failback, then in the Secondary LDAP server section, specify information to identify the failback LDAP server.

The options and text input boxes in the Secondary LDAP Server section are the same as the ones in the Primary LDAP Server section.

Step 9 Click **Submit**.

Step 5: Configure User Groups for MAB Segments

During configuration of Network Access Profiles to enable agentless request processing, you will be required to map devices that have specified MAC addresses to one of the default user groups that ACS provides.

Before you assign the user groups, plan how to configure the user groups. For example, users associated with the user group can:

- Be denied access to the network
- Be limited by network access restrictions (NARs)
- Have specified password settings

For detailed information on how to set up user groups, refer to chapter 5 of the *User Guide for Cisco Secure ACS 4.2*, “User Group Management.”

Step 6: Enable Agentless Request Processing

To enable agentless request processing, you must set up a Network Access Profile that enables the feature. To create a NAP to enable agentless request processing:

-
- Step 1** Create a new NAP.
See [Create a New NAP, page 6-18](#) for details.
- Step 2** In the Protocols page, check the **Allow Agentless Request Processing** check box.
- Step 3** In the Authentication section, configure MAB.
See [Configure MAB, page 6-21](#) for details.
- Step 4** If you are using agentless request processing in a NAC environment, configure posture validation for the NAP.
See [Enable Agentless Request Processing for a NAP, page 6-20](#) for details.
-

Create a New NAP

To create a new NAP:

-
- Step 1** In the navigation bar, click **Network Access Profiles**.
The Network Access Profiles page opens, as shown in [Figure 6-8](#).

Figure 6-8 Network Access Profiles Page

Name	Policies	Description	Active
Add Profile Add Template Profile Up Down The Up/Down buttons submit and save the sort order to the database.			
<input type="radio"/> Deny access when no profile matches <input checked="" type="radio"/> Grant access using global configuration, when no profile matches			
Apply and Restart			

- Step 2** Click **Add Profile**,

The Profile Setup page opens, shown in [Figure 6-9](#).

Figure 6-9 Profile Setup Page

Profile Setup

Name:

Description:

Active:

Network Access Filter:

Protocol types

Allow any Protocol type

Allow Selected Protocol types

Protocol type	Selected
<input checked="" type="checkbox"/> RADIUS (IPass)	
<input type="checkbox"/> RADIUS (Nortel)	
<input type="checkbox"/> RADIUS (Juniper)	
<input type="checkbox"/> RADIUS (Ascend)	
<input type="checkbox"/> RADIUS (IETF)	
<input type="checkbox"/> RADIUS (Cisco VPN 5000)	
<input type="checkbox"/> RADIUS (Cisco VPN 3000)	
<input type="checkbox"/> RADIUS (Cisco IOS/PIX 6)	
<input type="checkbox"/> RADIUS (Cisco BBSM)	
<input type="checkbox"/> RADIUS (Cisco Aironet)	
<input type="checkbox"/> RADIUS (Cisco Airespace)	

158449

- Step 3** In the Name text box, enter the name of the NAP.
- Step 4** If you have set up network access filters (NAFs) and want to apply one, then from the drop-down list of NAFs, choose the appropriate NAF.
- Step 5** In the Protocol types section, select at least one RADIUS protocol type.
- Step 6** Configure additional NAP settings as required.
- Step 7** Click **Submit**.

The Edit Network Access Protocols page for the new profile appears, as shown in [Figure 6-10](#).

Figure 6-10 Edit Network Access Profiles Page

Network Access Profiles			
Name	Policies	Description	Active
<input type="radio"/> my_mac_auth_bypass	Protocols Authentication Posture Validation Authorization	Test profile to enable MAC authentication bypass for agentless host support	YES

The Up/Down buttons submit and save the sort order to the database.

Deny access when no profile matches
 Grant access using global configuration, when no profile matches

You are now ready to enable agentless request processing.

Enable Agentless Request Processing for a NAP

To enable agentless request processing for a NAP:

- Step 1** In the Edit Network Access Profiles page, click **Protocols**.

The Protocols Settings page for the selected NAP opens. Figure 6-11 shows the top portion of the Protocols Settings page.

Figure 6-11 Protocols Settings Page

Protocols Settings for my_mac_auth_bypass

Authentication Protocols

Allow PAP
 Allow CHAP
 Allow MS-CHAPv1
 Allow MS-CHAPv2
 Allow Agentless Request Processing

- Step 2** Check the check box for **Allow Agentless Request Processing**.
- Step 3** Configure additional protocol configuration options as required
- Step 4** If you are using ACS in a NAC environment, check the **Allow Posture Validation** check box in the EAP Configuration area.
- Step 5** Click **Submit**.

You are now ready to configure MAB settings.

Configure MAB

To configure MAB:

- Step 1** In the Edit Network Access Profiles page, click **Authentication**.

The Authentication page for the selected NAP opens. [Figure 6-12](#) shows the Authentication Settings page.

Figure 6-12 Authentication Settings Page

- Step 2** In the Credential Validation Databases section, choose the database(s) that ACS will use to authenticate agentless hosts.



Note If you clicked **Generic LDAP** or another LDAP database, choose **External User Databases > External User Database Configuration** and configure an LDAP database.

Step 3 If you specified an LDAP database in the Credential Validation Databases section, click **LDAP Server** and then select a LDAP database that you configured on the **External User Databases > External User Database Configuration** page.

Step 4 If you will validate MAC addresses by using the ACS internal database:

a. Click **Internal ACS DB**.

b. Click **Add**.

A text box for entering MAC addresses and associated user group mappings appears, as shown in [Figure 6-13](#).

Figure 6-13 MAC Address Input Area

c. In the MAC addresses input area, enter one or more MAC addresses to use in authenticating agentless hosts.

You can enter the MAC address in the following formats for representing MAC-48 addresses in human-readable form:

- Six groups of two hexadecimal digits, separated by hyphens (-) in transmission order; for example, *01-23-45-67-89-ab*.
- Six groups of two separated by colons (:); for example, *01:23:45:67:89:ab*.
- Three groups of four hexadecimal digits separated by dots (.); for example, *0123.4567.89ab*.

d. From the drop-down list of user groups in the User Group area, choose a user group to which devices having one of the specified MAC address are mapped.

e. To add additional groups of MAC addresses, click **Add** and enter additional groups and associated user groups as required.

Step 5 In the Default Action (If Agentless request was not assigned to a user group) area, from the drop-down list of user groups, choose a group to which to assign the MAC addresses if the MAC addresses are not found in the LDAP Server or the ACS Internal Database; or, if the LDAP Server is not reachable.

Step 6 If you enabled the EAP protocol and posture validation, set up posture validation rules in the Posture Validation section.

Step 7 As required, specify additional authorization rules in the Authorization section.

Step 8 Click **Submit**.

Step 7: Configure Logging and Reports

By default, the following information about MAB processing is logged to the *CSAuth* log file:

- The start of MAB request handling and what trigger is used to initiate MAB.

The format of this message is:

```
Performing Mac Authentication Bypass on <MAC_address>
```

where *MAC_address* is the MAC address that triggered the processing.

- User group mapping actions that indicate which MAC address in the authentication database was mapped to what user group. The format of this message is:

```
<MAC_address> was (not) found in <DB_name> and mapped to <user_group> user-group
```

where *MAC_address* is the MAC address that was mapped, *DB_name* is the name of the database that was used to match the *MAC_address*, and *user_group* is the name of the user group to which the MAC address was mapped.



Note

Because the results of MAC address lookup can influence the response that ACS returns to the NAD, the success or failure of the MAC address lookup has an effect on the user group that is mapped to an access request. Therefore, the MAC address lookup result might be listed in the Passed Authentications or Failed attempts report.

Configuring Reports for MAB Processing

When you configure reports, you can add a new attribute called `Bypass info` to the Passed Authentications and Failed Attempts reports.

To add this attribute:

-
- Step 1** In the navigation bar, click **System Configuration**.
The System Configuration page opens.
 - Step 2** Click **Logging**.
The Logging Configuration page opens.
The Logging Configuration page shows three columns of ACS reports: CSV, ODBC, and syslog.
 - Step 3** To add the Bypass attribute to a specified report:
 - a. Click **Configure** under the report type for one of the reports that you want to modify; for example, click the CSV report for the Passed Authentications report.
The Enable Logging page for the specified report opens.
 - b. Check the check box in the Enable Logging section.
 - c. In the Attributes column of the Select Columns to Log section, select the **Bypass Info** attribute.
 - d. Click the right arrow icon to move this attributed to the Logged Attributes column.
 - e. Select any other attributes that you want to log.
 - f. Set the other values on the Logging Configuration page as required.
 - g. Click **Submit**.

- Step 4** Repeat Step 3 for additional report types as required.
- Step 5** Repeat Steps 3 and 4 for the Failed Attempts report.
-

Configuration Steps for Audit Server Support

If you are using ACS with the NAC solution or with other applications that support the use of audit servers, you can set up agentless host support that uses an audit server.

An audit server runs a database that can enable further authentication of the information that is used to assign agentless host devices to user groups. For example, the categorization of devices in the LDAP schema might set up device categories such as *printer*, *PC*, or *FAX machine*. The database on the audit server can check whether a device with a specified MAC address or IP address is the type of device associated in the database with the specified MAC address or IP address. If it is not the correct device type, a specified authentication policy can be executed.

The mechanism that ACS 4.2 uses to communicate with audit servers in a NAC environment is called GAME group feedback. The GAME protocol defines the GAME groups. When you configure GAME group feedback for an audit server that is used in a NAP, you can enable the Request Device Type from Audit Server feature. If this feature is enabled, the audit feature can request a device type from the audit server and then check the device type against the device type that MAC authentication returns.

Configure GAME Group Feedback

To configure GAME group feedback:

- Step 1** Import an audit vendor file by using **CSUtil**.
- Step 2** Import a device-type attribute file by using **CSUtil**.
- Step 3** Import NAC attribute-value pairs.
- Step 4** Enable Posture Validation.
- Step 5** In the External Posture Validation Audit Server Setup page, configure an external audit server.
- Step 6** Enable GAME group feedback.
- Step 7** In the external audit server posture validation setup section, configure:
- Which hosts are audited section.
 - GAME group feedback.
 - Device-type retrieval and mapping for vendors who have a device attribute in the RADIUS dictionary.
- Step 8** Set up a device group policy.

The detailed steps for configuring GAME group feedback are described in [Enable GAME Group Feedback, page 9-79](#) in [Chapter 9, “NAC Configuration Scenario.”](#)
