Managing Users and Identity Stores

This chapter describes the following topics:

Overview

ACS manages your network devices and other ACS clients by using the ACS network resource repositories and identity stores. When a host connects to the network through ACS requesting access to a particular network resource, ACS authenticates the host and decides whether the host can communicate with the network resource.

To authenticate and authorize a user or host, ACS uses the user definitions in identity stores. There are two types of identity stores:

- Internal—Identity stores that ACS maintains locally (also called local stores) are called *internal identity stores*. For internal identity stores, ACS provides interfaces for you to configure and maintain user records.
- External—Identity stores that reside outside of ACS are called *external identity stores*. ACS requires configuration information to connect to these external identity stores to perform authentication and obtain user information.

In addition to authenticating users and hosts, most identity stores return attributes that are associated with the users and hosts. You can use these attributes in policy conditions while processing a request and can also populate the values returned for RADIUS attributes in authorization profiles.

Internal Identity Stores

ACS maintains different internal identity stores to maintain user and host records. For each identity store, you can define identity attributes associated with that particular store for which values are defined while creating the user or host records.

You can define these identity attributes as part of identity dictionaries under the System Administration section of the ACS application (**System Administration > Configuration > Dictionaries > Identity**).

Each internal user record includes a password, and you can define a second password as a TACACS+ enable password. You can configure the password stored within the internal user identity store to expire after a particular time period and thus force users to change their own passwords periodically.

Users can change their passwords over the RADIUS or TACACS+ protocols or use the UCP web service. Passwords must conform to the password complexity criteria that you define in ACS.

Internal user records consist of two component types: fixed and configurable.

Fixed components are:

- Name
- Description
- Password
- Enabled or disabled status
- Email Address
- Identity group to which users belong

Configurable components are:

- Enable password for TACACS+ authentication
- Sets of identity attributes that determine how the user definition is displayed and entered
- Disable Account if Date Exceeds
- Disable account after *n* successive failed attempts
- Enable Password Hash
- Password Never Expired/Disabled

Cisco recommends that you configure identity attributes before you create users. When identity attributes are configured:

- You can enter the corresponding values as part of a user definition.
- They are available for use in policy decisions when the user authenticates.
- They can be used to populate the values returned for RADIUS attributes in an authorization profile.

Internal user identity attributes are applied to the user for the duration of the user's session.

Internal identity stores contain the internal user attributes and credential information used to authenticate internal users.

Internal host records are similar to internal user records, except that they do not contain any password information. Hosts are identified by their MAC addresses. For information on managing internal identity stores, see Managing Internal Identity Stores, page 8-4.

External Identity Stores

External identity stores are external databases on which ACS performs authentications for internal and external users. ACS 5.8 supports the following external identity stores:

- LDAP
- Active Directory

- RSA SecurID Token Server
- RADIUS Identity Server

External identity store user records include configuration parameters that are required to access the specific store. You can define attributes for user records in all the external identity stores except the RSA SecurID Token Server. External identity stores also include certificate information for the ACS server certificate and certificate authentication profiles.

For more information on how to manage external identity stores, see Managing External Identity Stores, page 8-29.

Identity Stores with Two-Factor Authentication

You can use the RSA SecurID Token Server and RADIUS Identity Server to provide two-factor authentication. These external identity stores use an OTP that provides greater security. The following additional configuration options are available for these external identity stores:

- Identity caching—You can enable identity caching for ACS to use the identity store while processing a request in cases where authentication is not performed. Unlike LDAP and AD, for which you can perform a user lookup without user authentication, the RSA SecurID Token Server and RADIUS Identity Server does not support user lookup.

  For example, in order to authorize a TACACS+ request separately from the authentication request, taking into account that it is not possible for the identity store to retrieve the data because authentication is not performed, you can enable identity caching to cache results and attributes retrieved from the last successful authentication for the user. You can use this cache to authorize the request.

- Treat authentication rejects as—The RSA and RADIUS identity stores do not differentiate between the following results when an authentication attempt is rejected:
  - Authentication Failed
  - User Not Found

  This classification is very important when you determine the fail-open operation. A configuration option is available, allowing you to define which result must be used.

Identity Groups

Identity groups are logical entities that are defined within a hierarchy and are associated with users and hosts. These identity groups are used to make policy decisions. For internal users and hosts, the identity group is defined as part of the user or host definition.

When external identity stores are used, the group mapping policy is used to map attributes and groups retrieved from the external identity store to an ACS identity group. Identity groups are similar in concept to Active Directory groups but are more basic in nature.

Certificate-Based Authentication

Users and hosts can identify themselves with a certificate-based access request. To process this request, you must define a certificate authentication profile in the identity policy.

The certificate authentication profile includes the attribute from the certificate that is used to identify the user or host. It can also optionally include an LDAP or AD identity store that can be used to validate the certificate present in the request. For more information on certificates and certificate-based authentication, see:

- Configuring CA Certificates, page 8-97
- Configuring Certificate Authentication Profiles, page 8-103

Identity Sequences

You can configure a complex condition where multiple identity stores and profiles are used to process a request. You can define these identity methods in an Identity Sequence object. The identity methods within a sequence can be of any type.

The identity sequence is made up of two components, one for authentication and the other for retrieving attributes.

- If you choose to perform authentication based on a certificate, a single certificate authentication profile is used.
- If you choose to perform authentication on an identity database, you can define a list of identity databases to be accessed in sequence until the authentication succeeds. If the authentication succeeds, the attributes within the database are retrieved.

In addition, you can configure an optional list of databases from which additional attributes can be retrieved. These additional databases can be configured irrespective of whether you use password-based or certificate-based authentication.

If a certificate-based authentication is performed, the username is populated from a certificate attribute and this username is used to retrieve attributes from all the databases in the list. For more information on certificate attributes, see Configuring CA Certificates, page 8-97.

When a matching record is found for the user, the corresponding attributes are retrieved. ACS retrieves attributes even for users whose accounts are disabled or whose passwords are marked for change.

Note An internal user account that is disabled is available as a source for attributes, but not for authentication.

For more information on identity sequences, see Configuring Identity Store Sequences, page 8-105.

This chapter contains the following sections:

- Managing Internal Identity Stores, page 8-4
- Managing External Identity Stores, page 8-29
- Configuring CA Certificates, page 8-97
- Configuring Certificate Authentication Profiles, page 8-103
- Configuring Identity Store Sequences, page 8-105

Managing Internal Identity Stores

ACS contains an identity store for users and an identity store for hosts:

- The internal identity store for *users* is a repository of users, user attributes, and user authentication options.

- The internal identity store for *hosts* contains information about hosts for MAC Authentication Bypass (Host Lookup).

You can define each user and host in the identity stores, and you can import files of users and hosts.

The identity store for users is shared across all ACS instances in a deployment and includes for each user:

- Standard attributes
- User attributes
- Authentication information

Note ACS 5.8 supports authentication for internal users against the internal identity store only.

This section contains the following topics:

Authentication Information

You can configure an additional password, stored as part of the internal user record that defines the user's TACACS+ enable password which sets the access level to device. If you do not select this option, the standard user password is also used for TACACS+ enable.

If the system is not being used for TACACS+ enable operations, you should not select this option.

To use the identity store sequence feature, you define the list of identity stores to be accessed in a sequence. You can include the same identity store in authentication and attribute retrieval sequence lists; however, if an identity store is used for authentication, it is not accessed for additional attribute retrieval.

For certificate-based authentication, the username is populated from the certificate attribute and is used for attribute retrieval.

During the authentication process, authentication fails if more than one instance of a user or host exists in internal identity stores. Attributes are retrieved (but authentication is denied) for users who have disabled accounts or passwords that must be changed.

These types of failures can occur while processing the identity policy:

- Authentication failure; possible causes include bad credentials, disabled user, and so on.

- User or host does not exist in any of the authentication databases.
- Failure occurred while accessing the defined databases.

You can define fail-open options to determine what actions to take when each of these failures occurs:

- Reject—Send a reject reply.
- Drop—Do not send a reply.
- Continue—Continue processing to the next defined policy in the service.

The system attribute, *AuthenticationStatus*, retains the result of the identity policy processing. If you choose to continue policy processing when a failure occurs, you can use this attribute in a condition in subsequent policy processing to distinguish cases where identity policy processing did not succeed.

You can continue processing when authentication fails for PAP/ASCII, EAP-TLS, or EAP-MD5. For all other authentication protocols, the request is rejected and a message to this effect is logged.

Identity Groups

You can assign each internal user to one identity group. Identity groups are defined within a hierarchical structure. They are logical entities that are associated with users, but do not contain data or attributes other than the name you give to them.

You use identity groups within policy conditions to create logical groups of users to which the same policy results are applied. You can associate each user in the internal identity store with a single identity group.

When ACS processes a request for a user, the identity group for the user is retrieved and can then be used in conditions in the rule table. Identity groups are hierarchical in structure.

You can map identity groups and users in external identity stores to ACS identity groups by using a group mapping policy.

Creating Identity Groups

To create an identity group:

Step 1 Choose **Users and Identity Stores** > **Identity Groups**.

The Identity Groups page appears.

Step 2 Click **Create**. You can also:

- Check the check box next to the identity group that you want to duplicate, then click **Duplicate**.
- Click the identity group name that you want to modify, or check the check box next to the name and click **Edit**.
- Click **File Operations** to:
  - Add—Adds identity groups from the import to ACS.
  - Update—Overwrites the existing identity groups in ACS with the list from the import.
  - Delete—Removes the identity groups listed in the import from ACS.
- Click **Export** to export a list of identity groups to your local hard disk.

For more information on the File Operations option, see Performing Bulk Operations for Network Resources and Users, page 7-8.

The Create page or the Edit page appears when you choose the Create, Duplicate, or Edit option.

Step 3 Enter information in the following fields:

- Name—Enter a name for the identity group. If you are duplicating an identity group, you must enter a unique name; all other fields are optional.
- Description—Enter a description for the identity group.
- Parent—Click **Select** to select a network device group parent for the identity group.

Step 4 Click **Submit** to save changes.

The identity group configuration is saved. The Identity Groups page appears with the new configuration. If you created a new identity group, it is located within the hierarchy of the page beneath your parent identity group selection.

Related Topics

- Managing Users and Identity Stores, page 8-1
- Managing Internal Identity Stores, page 8-4
- Performing Bulk Operations for Network Resources and Users, page 7-8
- Identity Groups, page 8-3
- Creating Identity Groups, page 8-6
- Deleting an Identity Group, page 8-7

Deleting an Identity Group

To delete an identity group:

Step 1 Choose **Users and Identity Stores > Identity Groups**.

The Identity Groups page appears.

Step 2 Check one or more check boxes next to the identity groups you want to delete and click **Delete**.

The following error message appears:

```
Are you sure you want to delete the selected item/items?
```

Step 3 Click **OK**.

The Identity Groups page appears without the deleted identity groups.

Related Topic

- Managing Identity Attributes, page 8-7

Managing Identity Attributes

Administrators can define sets of identity attributes that become elements in policy conditions. For information about the ACS 5.8 policy model, see ACS 5.x Policy Model, page 3-1 During authentication, identity attributes are taken from the internal data store when they are part of a policy condition.

ACS 5.8 interacts with identity elements to authenticate users and obtain attributes for input to an ACS policy.

Attribute definitions include the associated data type and valid values. The set of values depends on the type. For example, if the type is *integer*, the definition includes the valid range. ACS 5.8 provides a default value definition that can be used in the absence of an attribute value. The default value ensures that all attributes have at least one value.

Related Topics

- Standard Attributes, page 8-8
- User Attributes, page 8-8
- Host Attributes, page 8-9

Standard Attributes

Table 8-1 describes the standard attributes in the internal user record.

Table 8-1 Standard Attributes

Attribute	Description
Username	ACS compares the username against the username in the authentication request. The comparison is case-insensitive.
Status	• Enabled status indicates that the account is active. • Disabled status indicates that authentications for the username will fail.
Description	Text description of the attribute.
Identity Group	ACS associates each user to an identity group. See Managing Identity Attributes, page 8-7 for information.

User Attributes

Administrators can create and add user-defined attributes from the set of identity attributes. You can then assign default values for these attributes for each user in the internal identity store and define whether the default values are required or optional.

You need to define users in ACS, which includes associating each internal user with an identity group, a description (optional), a password, an enable password (optional), and internal and external user attributes.

Internal users are defined by two components: fixed and configurable. Fixed components consist of these attributes:

- Name
- Description
- Password
- Enabled or disabled status
- Identity group to which they belong

Configurable components consist of these attributes:

- Enable password for TACACS+ authentication

- Sets of identity attributes that determine how the user definition is displayed and entered

Cisco recommends that you configure identity attributes before you create users. When identity attributes are configured:

- You can enter the corresponding values as part of a user definition.
- They are available for use in policy decisions when the user authenticates.

Internal user identity attributes are applied to the user for the duration of the user's session.

Internal identity stores contain the internal user attributes and credential information used to authenticate internal users (as defined by you within a policy).

External identity stores are external databases on which to perform credential and authentication validations for internal and external users (as defined by you within a policy).

In ACS 5.8, you can configure identity attributes that are used within your policies, in this order:

Step 1 Define an identity attribute (using the user dictionary).

Step 2 Define custom conditions to be used in a policy.

Step 3 Populate values for each user in the internal database.

Step 4 Define rules based on this condition.

As you become more familiar with ACS 5.8 and your identity attributes for users, the policies themselves will become more robust and complex.

You can use the user-defined attribute values to manage policies and authorization profiles. See Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-12 for information on how to create a user attribute.

Host Attributes

You can configure additional attributes for internal hosts. You can do the following when you create an internal host:

- Create host attributes
- Assign default values to the host attributes
- Define whether the default values are required or optional

You can enter values for these host attributes and can use these values to manage policies and authorization profiles. See Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-15 for information on how to create a host attribute.

Configuring Authentication Settings for Users

You can configure the authentication settings for user accounts in ACS to force users to use strong passwords. Any password policy changes that you make in the Authentication Settings page apply to all internal identity store user accounts. The User Authentication Settings page consists of the following tabs:

- Password complexity
- Advanced

To configure a password policy:

Step 1 Choose **System Administration > Users > Authentication Settings**.

The User Authentication Settings page appears with the Password Complexity and **Advanced** tabs.

Step 2 In the **Password Complexity** tab, check each check box that you want to use to configure your user password.

Table 8-2 describes the fields in the Password Complexity tab.

Table 8-2 Password Complexity Tab

Option	Description
Applies to all ACS internal identity store user accounts	
Minimum length	Required minimum length; the valid options are 4 to 32.
Password may not contain the username	Whether the password may contain the username or reverse username.
Password may not contain 'cisco'	Check to specify that the password cannot contain the word *cisco*.
Password may not contain	Check to specify that the password does not contain the string that you enter.
Password may not contain repeated characters four or more times consecutively	Check to specify that the password cannot repeat characters four or more times consecutively.
Change password failed reason message (for TACACS+ only)	Enter the error message that is displayed when a user enters a password that does not meet the password policy while trying to change the existing password. This option is applicable only for internal user TACACS+ authentication. The maximum length of this field is 50 characters. Using this option, you can display an appropriate error message for the internal users if their new password does not match the criteria that you have specified.
Password must contain at least one character of each of the selected types	
Lowercase alphabetic characters	Password must contain at least one lowercase alphabetic character.
Uppercase alphabetic characters	Password must contain at least one uppercase alphabetic character.
Numeric characters	Password must contain at least one numeric character.
Non-alphanumeric characters	Password must contain at least one non-alphanumeric character.

Step 3 In the **Advanced** tab, enter the values for the criteria that you want to configure for your user authentication process. The following table describes the fields in the **Advanced** tab.

Table 8-3 Advanced Tab

Options	Description
Account Disable	
Supports account disablement policy for internal users.	
Never	Default option where accounts never expire. All internal users who got disabled because of this policy, are enabled if you select this option.

Table 8-3 Advanced Tab

Options	Description
Disable account if Date exceeds	Internal user is disabled when the configured date exceeds. For example, if the configured date is 28th Dec 2010, all internal users will be disabled on the midnight of 28th Dec, 2010. The configured date can either be the current system date or a future date. You are not allowed to enter a date that is earlier than the current system date. All the internal users who get disabled due to Date exceeds option are enabled according to the configuration changes made in the Date exceeds option.
Disable account if Days exceed	Internal user is disabled when the configured number of days exceed. For example, if the configured number of days to disable the account of a user is 60 days, that particular user will be disabled after 60 days from the time account was enabled.
Disable account if Failed Attempts Exceed	Internal user is disabled when the successive failed attempts count reaches the configured value. For example, if the configured value is 5, the internal user will be disabled when the successive failed attempts count reaches 5.
Reset current failed attempts count on submit	If selected, failed attempts counts of all the internal users is set to 0. All internal users who were disabled because of **Failed Attempts Exceed** option are enabled.
Disable user account after *n* days of inactivity	Specifies that the user account must be disabled based on the number of days the user is not logged in to the network. This option is applicable only for the internal users. The days ranges between 1 and 365.
Password History	
Password must be different from the previous *n* versions.	Specifies the number of previous passwords for this user to be compared against. The number of previous passwords include the default password as well. This option prevents the users from setting a password that was recently used. Valid options are 1 to 99.
Password Lifetime	
Users can be required to periodically change password	
Disable user account after *n* days if password is not changed for *n* days	Specifies that the user account must be disabled after *n* days if the password is not changed; the valid options are 1 to 365. This option is applicable only for TACACS+ and RADIUS with MS-CHAPv2 authentication.
Expire the password after *n* days if the password is not changed for *n* days	Specifies that the user password must be expired after *n* days if the password is not changed; valid options are 1 to 365. This option is applicable only for TACACS+ and RADIUS with MS-CHAPv2 authentication.
Display reminder after *n* days	Displays a reminder after *n* days to change password; the valid options are 1 to 365. This option, when set, only displays a reminder. It does not prompt you for a new password. This option is applicable only for TACACS+ and RADIUS with MS-CHAPv2 authentication.

Table 8-3 Advanced Tab

Options	Description
Send Email for password expiry before *n* days	Check this check box and enter the number of days if you want ACS to send an email notification a day to the internal users starting from *n* th day before their password expires. This option helps the internal users change their password before it expires. ACS does not allow you to configure this option without configuring the "Expire the password after *n* days if the password is not changed for *n* days" or "Disable user account after *n* days if password is not changed for *n* days options."
TACACS Enable Password	
Select whether a separate password should be defined in the user record to store the Enable Password	
TACACS Enable Password	Check the check box to enable a separate password for TACACS+ authentication.

Step 4 Click **Submit**.

The user password is configured with the defined criteria. These criteria will apply only for future logins.

Note If one of the users gets disabled, the failed attempt count value needs to be reconfigured multiple times. In such a case, the administrators should either note separately the current failed attempt count of that user, or reset the count to 0 for all users.

Disabling User Account After *N* Days of Inactivity

Before you Begin:

- This feature is applicable only for the ACS internal users.
- ACS must be configured to send passed authentication messages to the log collector server.
- The log collector server must be running and receiving syslog messages from all ACS nodes in the deployment.
- The log recovery feature must be enabled.

ACS 5.8 allows the administrator to configure the maximum number of days from ACS web interface during which the internal users' accounts are enabled despite the users not having logged in to the network. Once the configured period is exceeded, the user's account is disabled if the user has not logged in to the network. The number of days ranges between 1 and 365. For this feature to work properly, the log collector server should be running and receiving the syslog messages from ACS nodes in the deployment. The last login date is not stored in the database and hence it will not be displayed in the web interface. Every day at 10 PM, ACS View runs a job to provide the list of active users to the primary management. The active user is one who has made at least one successful authentication for the configured period of time. You can view the last active date of an user from the passed authentication reports in ACS Reports web interface. Based on this list, the primary management identifies the inactive users list, disables them, and sends an audit log message to the log collector server. The administrator can enable the disabled user account. After enabling the user account, the subsequent calculation for inactivity will be calculated from the last enabled date.

Note When you change the log collector server, it is mandatory to restore the back up taken from the old log collector server in the new log collector server.

Note When you restore the ACS backup from one ACS instance to another ACS instance, the view back up also should be restored along with the ACS backup.

To disable user accounts after *n* days of inactivity:

Step 1 Choose **System Administration > Users > Authentication Settings**.

The User Authentication Settings page appears.

Step 2 Check **Disable user account after *n* days of inactivity** check box.

Step 3 Enter the number of days in the text box.

ACS disables the user account if it is not active for the configured number of days.

Creating Internal Users

In ACS, you can create internal users that do not access external identity stores for security reasons.

You can use the bulk import feature to import hundreds of internal users at a time; see Performing Bulk Operations for Network Resources and Users, page 7-8 for more information. Alternatively, you can use the procedure described in this topic to create internal users one at a time.

Step 1 Choose **Users and Identity Stores > Internal Identity Store > Users**.

The Internal Users page appears.

Step 2 Click **Create**. You can also:

- Check the check box next to the user that you want to duplicate, then click **Duplicate**.
- Click the username that you want to modify, or check the check box next to the name and click **Edit**.
- Check the check box next to the user whose password you want to change, then click **Change Password**. You can also change internal user password using REST API. See Changing internal user passwords using REST API to for more information.

The Change Password page appears.

Step 3 Complete the fields as described in Table 8-4 to change the internal user password.

Table 8-4 Internal User - Change Password Page

Option	Description
Password Information	
Password Type	Displays all configured external identity store names, along with Internal Users which is the default password type. You can choose any one identity store from the list. During user authentication, if an external identity store is configured for the user then internal identity store forwards the authentication request to the configured external identity store. If an external identity store is selected, you cannot configure a password for the user. The password edit box is disabled. You cannot use identity sequences as external identity stores for the Password Type. You can change Password Type using the **Change Password** button located in the **Users and Identity Stores > Internal Identity Stores > Users** page.
Password	User's current password, which must comply with the password policies defined under **System Administration > Users > Authentication Settings**. The valid range is 4 to 32 characters.
Confirm Password	User's password, which must match the Password entry exactly.
Change Password on Next Login	Check this box to start the process to change the user's password at the next user login, after authentication with the old password.
Enable Password Information	
Enable Password	(Optional) The internal user's TACACS+ enable password, from 4 to 128 characters. You can disable this option. See Authentication Information, page 8-5 for more information.
Confirm Password	(Optional) The internal user's TACACS+ enable password, which must match the Enable Password entry exactly.

- Click **File Operations** to:
  - Add—Adds internal users from the import to ACS.
  - Update—Overwrites the existing internal users in ACS with the list of users from the import.
  - Delete—Removes the internal users listed in the import from ACS.
- Click **Export** to export a list of internal users to your local hard disk.

For more information on the File Operations option, see Performing Bulk Operations for Network Resources and Users, page 7-8.

The User Properties page appears when you choose the Create, Duplicate, or Edit option. In the Edit view, you can see the information on the original creation and last modification of the user. You cannot edit this information.

Step 4 Complete the fields as described in Table 8-5.

Table 8-5 Users and Identity Stores > Internal Identity Store > User Properties Page

Option	Description
General	
Name	Username.
Status	Use the drop-down list box to select the status for the user: • Enabled—Authentication requests for this user are allowed. • Disabled—Authentication requests for this user fail.
Description	(Optional) Description of the user.
Identity Group	Click **Select** to display the Identity Groups window. Choose an identity group and click **OK** to configure the user with a specific identity group.
Email Address	Enter the internal user email address. ACS View sends alerts to this email address. ACS uses this email address to notify the internal users about their password expiry *n* days before their password expires.
Account Disable	
Disable Account if Date Exceeds	Check this check box to use the account disablement policy for each individual user. This option allows you to disable the user accounts when the configured date is exceeded. This option overrides the global account disablement policy of the users. This means that the administrator can configure different expiry dates for different users as required. The default value for this option is 60 days from the account creation date. The user account will be disabled at midnight on the configured date.
Disable account after *n* successive failed attempts	Check this check box to configure the failed attempts count for each user. You can enter the failed attempts count at the text box provided. The value ranges from 1 to 99. If a user enters an incorrect login credentials, ACS uses this failed attempts count to decide whether it has to disable the user account or allow the user to try again. If the failed attempts count reaches *n*, then ACS disables the user account. If you do not configure the failed attempt count here, ACS tries to check the failed attempt count configuration at identity group level. The user level failed attempt count takes the precedence.
Password Hash	
Enable Password Hash	Check this check box to enable password hashing using the PBKDF2 of Cisco SSL hashing algorithm to provide enhanced security to the user passwords. This option is only applicable for internal users. If you enable this option, the authentication types such as CHAP and MSCHAP will not work. This option is disabled by default. When you disable this option in the middle, you have to re-configure your password using the change password option immediately after disabling this option. For more information, see Enable and Disable Password Hashing for Internal Users, page 8-18.
Password Lifetime	
Password Never Expired/Disabled	Check the **Password Never Expired/Disabled** check box for the user account to be active when the password lifetime is completed. This option overrides the password lifetime settings configured on the **System Administration > Users > Authentication Settings > Advanced** page.
Password Information	
This section of the page appears only when you create an internal user.	
Password must contain at least 4 characters	

Table 8-5 Users and Identity Stores > Internal Identity Store > User Properties Page (continued)

Option	Description
Password Type	Displays all configured external identity store names, along with Internal Users which is the default password type. You can choose any one identity store from the list. During user authentication, if an external identity store is configured for the user then internal identity store forwards the authentication request to the configured external identity store. If an external identity store is selected, you cannot configure a password for the user. The password edit box is disabled. You cannot use identity sequences as external identity stores for the Password Type. You can change Password Type using the **Change Password** button located in the **Users and Identity Stores > Internal Identity Stores > Users** page.
Password	User's password, which must comply with the password policies defined under **System Administration > Users > Authentication Settings**.
Confirm Password	User's password, which must match the Password entry exactly.
Change Password on next login	Check this box to start the process to change the user's password when the user logs in next time, after authentication with the old password.
Enable Password Information	
This section of the page appears only when you create an internal user. Password must contain 4-128 characters.	
Enable Password	(Optional) Internal user's TACACS+ enable password, from 4 to 128 characters. You can disable this option. See Authentication Information, page 8-5 for more information.
Confirm Password	(Optional) Internal user's TACACS+ enable password, which must match the Enable Password entry exactly.
User Information	
If defined, this section displays additional identity attributes defined for user records.	
ManagementHierarchy	User's assigned access level of hierarchy. Enter the hierarchical level of the network devices that the user can access. Example: • Location:All:US:NY:MyMgmtCenter1 • Location:All:US:NY:MyMgmtCenter1|US:NY:MyMgmtCenter2 The attribute type is string and the maximum character length is 256.
Creation/Modification Information	
This section of the page appears only after you have created or modified an internal user.	

Table 8-5 Users and Identity Stores > Internal Identity Store > User Properties Page (continued)

Option	Description
Date Created	*Display only.* The date and time when the user's account was created, in the format *Day Mon dd hh:mm:ss* **UTC** *YYYY*, where: • *Day* = Day of the week. • *Mon* = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec • *DD* = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). • *hh*:*mm*:*ss* = Hour, minute, and second, respectively • *YYYY* = Four digits that represent the year
Date Modified	*Display only.* The date and time when the user's account was last modified (updated), in the format *Day Mon dd hh:mm:ss* **UTC** *YYYY*, where: • *Day* = Day of the week. • *Mon* = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec • *DD* = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). • *hh*:*mm*:*ss* = Hour, minute, and second, respectively • *YYYY* = Four digits that represent the year

Step 5 Click **Submit**.

The user configuration is saved. The Internal Users page appears with the new configuration.

Note The **Password Never Expired/Disabled** option on the Creating Internal Users page overrides only the password lifetime settings configured on the **System Administration > Users > Authentication Settings > Advanced** page. This option does not override the account disablement settings due to date exceeds, days exceeds, failed attempt count exceeds, or n days of account inactivity.

Related Topics

- Configuring Authentication Settings for Users, page 8-9
- Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-21
- Deleting Users from Internal Identity Stores, page 8-17

Deleting Users from Internal Identity Stores

To delete a user from an internal identity store:

Step 1 Choose **Users and Identity Stores > Internal Identity Store > Users**.

The Internal Users page appears.

Step 2 Check one or more check boxes next to the users you want to delete.

Step 3 Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

Step 4 Click **OK**.

The selected internal users are deleted.

Related Topics

- Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-21
- Creating Internal Users, page 8-13

Enable and Disable Password Hashing for Internal Users

ACS 5.8 provides enhanced security to the internal users' password by introducing the “Enable Password Hash” option in Creating Internal Users page of ACS web interface. Prior to Release 5.8, ACS stored the internal users’ password as clear text in the ACS internal user database. The ACS administrators can view the internal users’ passwords from internal user database. Therefore, to enhance security of internal users’ password, ACS 5.8 introduces the new feature “Enable Password Hash”. If you enable this option, the users’ password is converted into hashes using the PBKDF2 of Cisco SSL hashing algorithm and is stored in the internal user database as hashes. This feature is applicable only for password based authentications. Therefore, when this option is enabled, you cannot use CHAP and MSCHAP authentications. If you enable this option while creating internal users, ACS converts the passwords to hashes and stores the same in the internal user database. When a user tries to access the network using the login password, ACS converts that password to hashes using the PBKDF2 hashing algorithm and compares this hash entry with the entry that is stored in ACS internal user’s database. If the password hash value matches with the database hash value, then ACS allows the user to log in to the network. If the password hash value does not match with the database hash value, then ACS fails the authentication and the user cannot log in to the network. You can uncheck the Enable Password Hash check box to disable this option. Due to the iterations used in PDKDF2 algorithm to ensure stronger security, you can expect a delay in authentication response from ACS when there is a huge load on the server.

To enable password hashing for internal users in ACS:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Users**.

The Internal Users page appears with the list of available internal users.

Step 2 Perform one of the following:

- Click **Create**.
- Check the check box next to the user to whom you want to enable password hash and click **Edit**.

Step 3 Check the **Enable Password Hash** check box.

Step 4 Click **Submit**.

The Password hashing option is enabled for the selected internal user.

To disable password hashing for internal users in ACS:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Users**.

The Internal Users page appears with the list of available internal users.

Step 2 Check the check box next to the user to whom you want to disable password hash and click **Edit.**

Step 3 Uncheck the **Enable Password Hash** check box.

Step 4 Click **Submit**.

The Password hashing option is disabled for the selected internal user.

Note After disabling the **Enable Password Hash** option, you must change the user password immediately.

Step 5 Check the check box next to the user to whom you have disabled the password hash option and click **Change Password.**

Step 6 Enter the new password in the **Password** field.

Step 7 Enter the new password in the **Confirm Password** field.

Step 8 Click **Submit**.

Configuring Password Expiry Notification Emails to Users and Administrators

Before you Begin

- Email Settings must be configured under Monitoring Configuration. See Specifying E Mail Settings, page 15-16 for Email Settings.

ACS 5.8 allows you to configure password expiry notification email for internal users and administrators. You can configure the number of days before the password expiry notification email must be sent for internal users and administrators from Creating Internal Users page from ACS web interface. If you configure this feature, then ACS 5.8 notifies the internal users and administrators through an email a day starting from *nth* day before their password expires. ACS verifies the users' and administrators' password expiry immediately after 5 minutes of the management process being restarted. The subsequent verifications are performed every 24 hours from the last verified time. For this feature to work properly, the **Email Settings** option must be configured under Monitoring Configuration.

Configuring Password Expiry Reminder for Users

To send password expiry reminder email to internal users, you have to configure the following from ACS web interface.

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Users**.

The Internal Users page appears with the list of available internal users.

Step 2 Perform one of the following:

- Click **Create**.
- Check the check box next to the user to whom you want to configure the password expiry reminder and click **Edit**.

Step 3 Enter the users' email address in the **Email Address** text box.

Step 4 Click **Submit**.

Step 5 Choose **System Administration > Users > Authentication Settings > Advanced**.

The Advanced Authentication Settings page for users appear.

Step 6 Check the **Send Email for password expiry before *n* days** check box and enter the number of days.

Note The **Send Email for password expiry before *n* days** check box is disabled if the password lifetime is not configured.

Step 7 Click **Submit**.

The password expiry reminder is configured now. The users will receive an email a day starting from the *n*th day before their password expires. The email has the following message:

```
Dear User,
Your password is going to expire on day, date month year at time UTC. We recommend that
you reset your password immediately to avoid being locked out.
Regards,
CiscoSecureACS Administrator.
```

Configuring Password Expiry Reminder for Administrators

To send password expiry reminder email to internal administrators, you have to configure the following from ACS web interface.

Step 1 Choose **System Administration > Administrators > Accounts**.

The Administrators accounts page appear with the list of available internal administrators.

Step 2 Perform one of the following:

- Click **Create**.
- Check the check box next to the administrator to whom you want to configure the password expiry reminder and click **Edit**.

Step 3 Enter the administrators' email address in the **Email Address** text box.

Step 4 Click **Submit**.

Step 5 Choose **System Administration > Administrators > Settings > Authentication > Advanced**.

The Advanced Authentication Settings page for administrators appear.

Step 6 Check the **Send Email for password expiry before *n* days** check box and enter the number of days.

Note The **Send Email for password expiry before *n* days** check box is disabled if the **Disable administrator account after *n* days if password was not changed** option is not configured.

Step 7 Click **Submit**.

The password expiry reminder is configured now. The administrators will receive an email a day starting from the *n*th day before their password expires. The email has the following message:

```
Dear Administrator,

Your password is going to expire on day, date month year at time UTC. We recommend that
you reset your password immediately to avoid being locked out.

Regards,

CiscoSecureACS Administrator.
```

Related Topics

- Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-21
- Creating Internal Users, page 8-13

Viewing and Performing Bulk Operations for Internal Identity Store Users

To view and perform bulk operations to internal identity store users:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Users**.

The Internal Users page appears, with the following information for all configured users:

- Status—The status of the user
- User Name—The username of the user
- Identity Group—The identity group to which the user belongs
- Description—(Optional) A description of the user.

Step 2 Do one of the following:

- Click **Create**. For more information on creating internal users, see Creating Internal Users, page 8-13.
- Check the check box next to an internal user whose information you want to edit and click **Edit**. For more information on the various fields in the edit internal user page, see Creating Internal Users, page 8-13.
- Check the check box next to an internal user whose information you want to duplicate and click **Duplicate**. For more information on the various fields in the duplicate internal user page, see Creating Internal Users, page 8-13.
- Click **File Operations** to perform any of the following bulk operations:
  - Add—Choose this option to add internal users from the import file to ACS.
  - Update—Choose this option to replace the list of internal users in ACS with the list of internal users in the import file.
  - Delete—Choose this option to delete the internal users listed in the import file from ACS.

See Performing Bulk Operations for Network Resources and Users, page 7-8 for a detailed description of the bulk operations.

Related Topics

- Creating Internal Users, page 8-13
- Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-21

- Deleting Users from Internal Identity Stores, page 8-17

Configuring Authentication Settings for Hosts

ACS 5.8 introduces a new section “Authentication Settings” under “System Administration” for Configuring Authentication Settings for Hosts. Using this section, you can disable and delete host accounts based on their inactivity.

This section describes the following:

- Disabling and Deleting Host Accounts After N and N+x Days of Inactivity, page 8-22

Disabling and Deleting Host Accounts After *N* and *N+x* Days of Inactivity

Before you Begin:

- This feature is applicable only for the internal hosts that sends MAB authentication requests.
- ACS must be configured to send passed authentication messages to the log collector server.
- The log collector server must be running and receiving syslog messages from all ACS nodes in the deployment.
- The log recovery feature must be enabled.

ACS 5.8 allows the administrator to configure the maximum number of days from ACS web interface during which the internal hosts’ accounts are enabled despite the hosts not having logged in to the network. Once the configured period is exceeded, the host’s account is disabled if the host has not logged in to the network. Also, the administrator can configure the number of days in such a way that ACS can delete the host account from the database if the host has not logged in to the network after the host account is disabled.

The default value for disabling the host account is 30 days of inactivity. The default value for deleting the host account is 60 days of inactivity after the host account is disabled. For this feature to work properly, the log collector server should be running and receiving the syslog messages from all ACS nodes in the deployment.

ACS calculates the inactivity based on the last login date of MAB entry. Every day at 10 PM, ACS View runs a job to provide the list of active MAB entries to the primary management. An active host is one which has made at least one successful authentication for the configured period of time. You can observe the last active time of a host from the passed authentication reports in ACS Reports web interface. Based on this list, the primary management identifies the inactive MAB entries list, disables them, and sends an audit log message to the log collector server. The administrator can enable the disabled host account. After enabling the host account, the subsequent calculation for inactivity will be calculated from the last enabled date.

Note When you change the log collector server, it is mandatory to restore the back up taken from the old log collector server in the new log collector server.

Note When you restore the ACS backup from one ACS instance to another ACS instance, the view back up also should be restored along with the ACS backup.

To disable host accounts after *n* days of inactivity:

Step 1 Choose **System Administration > Hosts > Authentication Settings**.

The Host Authentication Settings page appears.

Step 2 Check the **Disable host account after *n* days of inactivity** check box.

Step 3 Enter the number of days in the text box.

ACS disables the host account if it is not active for the configured number of days.

To delete host accounts after *n* days of disablement:

Step 1 Choose **System Administration > Hosts > Authentication Settings**.

The Host Authentication Settings page appears.

Step 2 Check the **Delete host account after *n* days of disablement/inactivity** check box.

Step 3 Enter the number of days in the text box.

ACS deletes the host account if it is not active for the configured number of days after that account is disabled.

Creating Hosts in Identity Stores

To create, duplicate, or edit a MAC address and assign identity groups to internal hosts:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Hosts**.

The Internal Hosts page appears, listing any configured internal hosts.

Step 2 Click **Create**. You can also:

- Check the check box next to the MAC address you want to duplicate, then click **Duplicate**.
- Click the MAC address that you want to modify, or check the check box next to the MAC address and click **Edit**.
- Click **File Operations** to perform bulk operations. See Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-25 for more information on the import process.
- Click **Export** to export a list of hosts to your local hard drive.

The Internal Hosts General page appears when you click the Create, Duplicate, or Edit options.

Step 3 Complete the fields in the Internal MAC Address Properties page as described in Table 8-6:

Table 8-6 Internal Hosts Properties Page

Option	Description
General	
MAC Address	ACS 5.8 support wildcards while adding new hosts to the internal identity store. Enter a valid MAC address, using any of the following formats: • 01-23-45-67-89-AB/01-23-45-* • 01:23:45:67:89:AB/01:23:45:* • 0123.4567.89AB/0123.45* • 0123456789AB/012345* ACS accepts a MAC address in any of the above formats, and converts and stores the MAC address as six hexadecimal digits separated by hyphens; for example, 01-23-45-67-89-AB.
Status	Use the drop-down list box to enable or disable the MAC address.
Description	(Optional) Enter a description of the MAC address.
Identity Group	Enter an identity group with which to associate the MAC address, or click **Select** to display the Identity Groups window. Choose an identity group with which to associate the MAC address, then click **OK**.
MAC Host Information	*Display only.* Contains MAC host identity attribute information.
Creation/Modification Information	
This section of the page appears only after you have created or modified a MAC address.	
Date Created	*Display only.* The date that the host account was created, in the format *Day Mon dd hh:mm:ss* **UTC** *YYYY*, where: • *Day* = Day of the week. • *Mon* = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec • *DD* = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). • *hh***:***mm***:***ss* = Hour, minute, and second, respectively • *YYYY* = Four digits that represent the year
Date Modified	*Display only.* The date that the host account was last modified (updated), in the format *Day Mon dd hh:mm:ss* **UTC** *YYYY*, where: • *Day* = Day of the week. • *Mon* = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec • *DD* = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). • *hh***:***mm***:***ss* = Hour, minute, and second, respectively • *YYYY* = Four digits that represent the year

Step 4 Click **Submit** to save changes.

The MAC address configuration is saved. The Internal MAC list page appears with the new configuration.

Note Hosts with wildcards (supported formats) for MAC addresses are migrated from 4.x to 5.x.

Note You can add wildcard for MAC address which allows the entire range of Organization Unique Identifier (OUI) clients.
For example: If you add Cisco's MAC address 00-00-0C-*, the entire range of Cisco devices will be added to the host.

Related Topics

- Host Lookup, page 4-12
- Deleting Internal Hosts, page 8-25
- Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-25
- Policies and Identity Attributes, page 3-17
- Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17

Deleting Internal Hosts

To delete a MAC address:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Hosts**.

The Internal MAC List page appears, with any configured MAC addresses listed.

Step 2 Check one or more of the check boxes next to the internal hosts you want to delete.

Step 3 Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

Step 4 Click **OK**.

The Internal MAC List page appears without the deleted MAC addresses.

Related Topics

- Host Lookup, page 4-12
- Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-25
- Creating Hosts in Identity Stores, page 8-23
- Policies and Identity Attributes, page 3-17
- Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17

Viewing and Performing Bulk Operations for Internal Identity Store Hosts

To view and perform bulk operations for internal identity stores:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Hosts**.

The Internal Hosts page appears, with any configured internal hosts listed.

Step 2 Click **File Operations** to perform any of the following functions:

- Add—Choose this option to add internal hosts from an import file to ACS.
- Update—Choose this option to replace the list of internal hosts in ACS with the internal hosts in the import file.
- Delete—Choose this option to delete the internal hosts listed in the import file from ACS.

See Performing Bulk Operations for Network Resources and Users, page 7-8 for a detailed description of the bulk operations.

Related Topics

- Host Lookup, page 4-12
- Creating Hosts in Identity Stores, page 8-23
- Deleting Internal Hosts, page 8-25
- Policies and Identity Attributes, page 3-17
- Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17

Management Hierarchy

Management Hierarchy enables the administrator to give access permission to the internal users or internal hosts according to their level of hierarchy in the organizations management hierarchy. A hierarchical label is assigned to each device that represents the administrative location of that particular device within the organizations management hierarchy.

For example, the hierarchical label *All:US:NY:MyMgmtCenter* indicates that the device is in a MyMgmtcenter under NY city which is in U.S. The administrator can give access permission to the users based on their assigned level of hierarchy. For instance, if a user has an assigned level as *All:US:NY*, then that user is given permission when the user accesses the network through any device with a hierarchy that starts with *All:US:NY*. The same examples are applicable for internal hosts.

Attributes of Management Hierarchy

To use the Management Hierarchy feature, administrator needs to create the following attributes in the Internal Users Dictionary:

- ManagementHierarchy attribute—allows the administrator to define one or more hierarchies for each internal users or internal hosts. This attribute is of type string and the maximum character length is 256. See Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-12 and Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-15.
- UserIsInManagementHierarchy or HostIsInManagementHierarchy attribute—the value of this attribute is set to true when the hierarchy defined for the user or host equals or contained in the hierarchy defined for the network device and AAA clients. This attribute is of type Boolean and the default value is false. It is not displayed in the users or hosts page in ACS web interface. You can

view this attribute only in the identity attributes dictionary list. See Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-12 and Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-15.

Configuring AAA Devices for Management Hierarchy

The management centers and the correlated customer names should be configured within a Management Hierarchy for each AAA client. Any Network Device Group can be used as a Management Hierarchy for a AAA client. The Network Device Group used for this is known as the Management Hierarchy Attribute. The administrator can create a new Network Device Group which will be used as Management Hierarchy. The *Location* hierarchy is an example of a Management Hierarchy attribute.

Example:

Location:All Locations:ManagementCenter1:Customer1

Configuring Users or Hosts for Management Hierarchy

A specific level of access is defined to represent the top-most node in the Management Hierarchy assigned for each user or a host. This level is defined in the user's "ManagementHierarchy" attribute. Total value length is limited to 256 characters.

The administrator can configure any level of hierarchy while defining management centers or AAA client locations. The syntax for ManagementHierarchy attribute is:

<HierarchyName>: <HierarchyRoot>:<Value>

Examples:

- *Location:All Locations:ManagementCenter1*
- *Location:All Locations:ManagementCenter1:Customer 1*

The administrator can configure multiple values for management hierarchy. The syntax for multiple value attribute is:

<HierarchyName>: <HierarchyRoot>:<Value>|<Value>|...

Example:

Location:All Locations:ManagementCenter1:Customer1|ManagementCenter1:Customer2

Configuring and Using the UserIsInManagement Hierarchy Attribute

To configure and use the UserIsInManagementHierarchy attribute, complete the following steps:

Step 1 Create the ManagementHierarchy and UserIsInManagementHierarchy attributes for internal users. See Configuring Internal Identity Attributes, page 18-13.

Step 2 Create the network device groups for the network devices and AAA clients with the required hierarchies. See Creating, Duplicating, and Editing Network Device Groups, page 7-2.

Step 3 Create network devices and AAA clients and associate them with a network device group. See Creating, Duplicating, and Editing Network Devices, page 7-10.

Step 4 Create internal users and configure the ManagementHierarchy attribute. See Creating Internal Users, page 8-13.

Step 5 Choose **Access Policies > Access Services > Default Network Access > Authorization**.

The Authorization page appears.

Step 6 Click **Customize,** add the compound condition to the policy conditions, and click **OK**.

Step 7 Click **Create** to create a new policy, and do the following:

a. Enter an appropriate name for the policy, and set the status.

b. In the Conditions section, check the **Compound Condition** check box.

c. Select **Internal users** from the dictionary drop-down list.

d. Select the **UserIsInManagementHierarchy** attribute from the available attribute list.

e. Select **Static value** and enter **True** as a condition for the rule to be matched.

f. Click **Add** to add this compound condition to the policy.

g. Choose the policy result for the rule and click **OK**.

See Configuring a Session Authorization Policy for Network Access, page 10-31, for more information on creating an authorization policy for network access.

Step 8 After successfully creating the policy, try authenticating the user using the created policy. The user will be authenticated only if the hierarchy defined for the user equals or is contained in the AAA clients hierarchy. You can view the logs to analyze the authentication results.

Related Topics

Configuring and Using the HostIsInManagement Hierarchy Attribute, page 8-28.

Configuring and Using the HostIsInManagement Hierarchy Attribute

To configure and use the HostIsInManagementHierarchy attribute, complete the following steps:

Step 1 Create the ManagementHierarchy and HostIsInManagementHierarchy attributes for internal hosts. See Configuring Internal Identity Attributes, page 18-13.

Step 2 Create the network device groups for the network devices and AAA clients with the required hierarchies. See Creating, Duplicating, and Editing Network Device Groups, page 7-2.

Step 3 Create network devices and AAA clients and associate them with a network device group. See Creating, Duplicating, and Editing Network Devices, page 7-10.

Step 4 Create internal hosts and configure the ManagementHierarchy attribute. See Creating Internal Users, page 8-13.

Step 5 Choose **Access Policies > Access Services > Default Network Access > Authorization**.

The Authorization page appears.

Step 6 Click **Customize,** add the compound condition to the policy conditions, and click **OK**.

Step 7 Click **Create** to create a new policy, and do the following:

a. Enter an appropriate name for the policy, and set the status.

b. In the Conditions section, check the **Compound Condition** check box.

c. Select **Internal hosts** from the dictionary drop-down list.

d. Select **HostIsInManagementHierarchy** attribute from the available attribute list.

e. Select **Static value** and enter **True** as a condition for the rule to be matched.

f. Click **Add** to add this compound condition to the policy.

g. Choose the policy result for the rule and click **OK**.

See Configuring a Session Authorization Policy for Network Access, page 10-31, for more information on creating an authorization policy for network access.

Step 8 After successfully creating the policy, try authenticating the user using the created policy. The user will be authenticated only if the hierarchy defined for the user equals or is contained in the AAA clients hierarchy. You can view the logs to analyze the authentication results.

Related Topics

- Configuring and Using the UserIsInManagement Hierarchy Attribute, page 8-27.

Managing External Identity Stores

ACS 5.8 integrates with external identity systems in a number of ways. You can leverage an external authentication service or use an external system to obtain the necessary attributes to authenticate a principal, as well to integrate the attributes into an ACS policy.

For example, ACS can leverage Microsoft AD to authenticate a principal, or it could leverage an LDAP bind operation to find a principal in the database and authenticate it. ACS can obtain identity attributes such as AD group affiliation to make an ACS policy decision.

Note ACS 5.8 does not have a built-in check for the dial-in permission attribute for Windows users. You must set the msNPAllowDialin attribute through LDAP or Windows AD. For information on how to set this attribute, refer to Microsoft documentation at:
http://msdn.microsoft.com/en-us/library/ms678093%28VS.85%29.aspx

This section provides an overview of the external identity stores that ACS 5.8 supports and then describes how you can configure them.

This section contains the following topics:

LDAP Overview

Lightweight Directory Access Protocol (LDAP), is a networking protocol for querying and modifying directory services that run on TCP/IP and UDP. LDAP is a lightweight mechanism for accessing an x.500-based directory server. RFC 2251 defines LDAP.

ACS 5.8 integrates with an LDAP external database, which is also called an identity store, by using the LDAP protocol. See Creating External LDAP Identity Stores, page 8-34 for information about configuring an LDAP identity store.

This section contains the following topics:

Directory Service

The directory service is a software application, or a set of applications, for storing and organizing information about a computer network's users and network resources. You can use the directory service to manage user access to these resources.

The LDAP directory service is based on a client-server model. A client starts an LDAP session by connecting to an LDAP server, and sends operation requests to the server. The server then sends its responses. One or more LDAP servers contain data from the LDAP directory tree or the LDAP backend database.

The directory service manages the directory, which is the database that holds the information. Directory services use a distributed model for storing information, and that information is usually replicated between directory servers.

An LDAP directory is organized in a simple tree hierarchy and can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically.

An entry in the tree contains a set of attributes, where each attribute has a name (an attribute type or attribute description) and one or more values. The attributes are defined in a schema.

Each entry has a unique identifier: its Distinguished Name (DN). This name contains the Relative Distinguished Name (RDN) constructed from attributes in the entry, followed by the parent entry's DN. You can think of the DN as a full filename, and the RDN as a relative filename in a folder.

Authentication Using LDAP

ACS 5.8 can authenticate a principal against an LDAP identity store by performing a bind operation on the directory server to find and authenticate the principal. If authentication succeeds, ACS can retrieve groups and attributes that belong to the principal. The attributes to retrieve can be configured in the ACS web interface (LDAP pages). These groups and attributes can be used by ACS to authorize the principal.

To authenticate a user or query the LDAP identity store, ACS connects to the LDAP server and maintains a connection pool. See LDAP Connection Management, page 8-31.

Multiple LDAP Instances

You can create more than one LDAP instance in ACS 5.8. By creating more than one LDAP instance with different IP address or port settings, you can configure ACS to authenticate by using different LDAP servers or different databases on the same LDAP server.

Each primary server IP address and port configuration, along with the secondary server IP address and port configuration, forms an LDAP instance that corresponds to one ACS LDAP identity store instance.

ACS 5.8 does not require that each LDAP instance correspond to a unique LDAP database. You can have more than one LDAP instance set to access the same database.

This method is useful when your LDAP database contains more than one subtree for users or groups. Because each LDAP instance supports only one subtree directory for users and one subtree directory for groups, you must configure separate LDAP instances for each user directory subtree and group directory subtree combination for which ACS should submit authentication requests.

Failover

ACS 5.8 supports failover between a primary LDAP server and secondary LDAP server. In the context of LDAP authentication with ACS, failover applies when an authentication request fails because ACS could not connect to an LDAP server.

For example, as when the server is down or is otherwise unreachable by ACS. To use this feature, you must define primary and secondary LDAP servers, and you must set failover settings.

If you set failover settings and if the first LDAP server that ACS attempts to contact cannot be reached, ACS always attempts to contact the other LDAP server.

The first server ACS attempts to contact might not always be the primary LDAP server. Instead, the first LDAP server that ACS attempts to contact depends on the previous LDAP authentications attempts and on the value that you enter in the Failback Retry Delay box.

LDAP Connection Management

ACS 5.8 supports multiple concurrent LDAP connections. Connections are opened on demand at the time of the first LDAP authentication. The maximum number of connections is configured for each LDAP server. Opening connections in advance shortens the authentication time.

You can set the maximum number of connections to use for concurrent binding connections. The number of opened connections can be different for each LDAP server (primary or secondary) and is determined according to the maximum number of administration connections configured for each server.

ACS retains a list of open LDAP connections (including the bind information) for each LDAP server that is configured in ACS. During the authentication process, the connection manager attempts to find an open connection from the pool. If an open connection does not exist, a new one is opened.

If the LDAP server closed the connection, the connection manager reports an error during the first call to search the directory, and tries to renew the connection.

After the authentication process is complete, the connection manager releases the connection to the connection manager.

Authenticating a User Using a Bind Connection

ACS sends a bind request to authenticate the user against an LDAP server. The bind request contains the user's DN and user password in clear text. A user is authenticated when the user's DN and password matches the username and password in the LDAP directory.

- Authentication Errors—ACS logs authentication errors in the ACS log files.
- Initialization Errors—Use the LDAP server timeout settings to configure the number of seconds that ACS waits for a response from an LDAP server before determining that the connection or authentication on that server has failed.

  Possible reasons for an LDAP server to return an initialization error are:

  - LDAP is not supported.
  - The server is down.
  - The server is out of memory.
  - The user has no privileges.
  - Incorrect administrator credentials are configured.
- Bind Errors

  Possible reasons for an LDAP server to return bind (authentication) errors are:

  - Filtering errors—A search using filter criteria fails.
  - Parameter errors—Invalid parameters were entered.
  - User account is restricted (disabled, locked out, expired, password expired, and so on).

The following errors are logged as external resource errors, indicating a possible problem with the LDAP server:

- A connection error occurred.
- The timeout expired.
- The server is down.
- The server is out of memory.

The following error is logged as an Unknown User error:

A user does not exist in the database.

The following error is logged as an Invalid Password error, where the user exists, but the password sent is invalid:

```
An invalid password was entered.
```

Group Membership Information Retrieval

For user authentication, user lookup, and MAC address lookup, ACS must retrieve the group membership information from LDAP databases. LDAP servers represent the association between a subject (a user or a host) and a group in one of the following two ways:

- Groups Refer to Subjects—The group objects contain an attribute that specifies the subject. Identifiers for subjects can be stored in the group as:
  - Distinguished Names (DNs)
  - Plain usernames

- Subjects Refer to Groups—The subject objects contain an attribute that specify the group they belong to.

LDAP identity stores contain the following parameters for group membership information retrieval:

- Reference Direction—Specifies the method to use when determining group membership (either Groups to Subjects or Subjects to Groups).
- Group Map Attribute—Indicates which attribute contains the group membership information.
- Group Name Attribute—Indicates which attribute contains the group name information.
- Group Object Class—Determines that you recognize certain objects as groups.
- Group Search Subtree—Indicates the search base for group searches.
- Member Type Option—Specifies how members are stored in the group member attribute (either as DNs or plain usernames).

Attributes Retrieval

For user authentication, user lookup, and MAC address lookup, ACS must retrieve the subject attributes from LDAP databases. For each instance of an LDAP identity store, an identity store dictionary is created. These dictionaries support attributes of the following data types:

- String
- Integer 64
- IP Address (This can be either an IP version 4 [IPv4] or IP version 6 [IPv6] address.)
- Unsigned Integer 32
- Boolean

For unsigned integers and IP address attributes, ACS converts the strings that it has retrieved to the corresponding data types. If conversion fails, or if no values are retrieved for the attributes, ACS logs a debug message but does not fail the authentication or the lookup process.

You can optionally configure default values for the attributes that ACS can use when the conversion fails or when ACS does not retrieve any values for the attributes.

Certificate Retrieval

If you have configured certificate retrieval as part of user lookup, then ACS must retrieve the value of the certificate attribute from LDAP. To do this, you must have configured certificate attribute in the List of attributes to fetch while configuring an LDAP identity store.

LDAP Server Identity Check

Background

This feature prevents spoofing attacks when Cisco ACS performs user authentication or authorization against an LDAP server (in IPv4).

An LDAP server can be spoofed if an attacker establishes a rogue LDAP server using a real LDAP server IP address (which can be achieved by another attack on the network), and can get a valid LDAP server certificate issued by the same CA.

ACS is required to perform identify verification on the LDAP server's certificate according to RFC 4513—*Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms.*

Feature Overview

ACS matches the data retrieved from the LDAP server's certificate (usually found in the X.509 SAN section; otherwise it is in the CN section) against the data configured by the ACS administrator about that server. Once this authentication check succeeds, the LDAP connection is established; otherwise the ACS discontinues the connection.

The hostname data in the LDAP server's certificate may be in one of the following formats:

- IP address
- DNS
- DNS using the wildcard character "*"

In the first two cases, the matching is straight forward. If the wildcard character is detected, ACS performs two sanity checks to verify that:

- The reconstructed address is of the correct length.
- The reconstructed address has a "." immediately after the wildcard character.

Creating External LDAP Identity Stores

Note Configuring an LDAP identity store for ACS has no effect on the configuration of the LDAP database. ACS recognizes the LDAP database, enabling the database to be authenticated against. To manage your LDAP database, see your LDAP database documentation.

When you create an LDAP identity store, ACS also creates:

- A new dictionary for that store with two attributes, ExternalGroups and IdentityDn.
- A custom condition for group mapping from the ExternalGroup attribute; the condition name has the format LDAP:*ID-store-name* ExternalGroups.

You can edit the predefined condition name, and you can create a custom condition from the IdentityDn attribute in the Custom condition page. See Creating, Duplicating, and Editing a Custom Session Condition, page 9-5.

To create, duplicate, or edit an external LDAP identity store:

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

The LDAP Identity Stores page appears.

Step 2 Click **Create**. You can also:

- Check the check box next to the identity store that you want to duplicate, and then click **Duplicate**.
- Click the identity store name that you want to modify, or check the box next to the name and click **Edit**.

If you are creating an identity store, the first page of a wizard appears: General.

If you are duplicating an identity store, the **External Identity Stores > Duplicate:** *id-store* page General tab appears, where *id-store* is the name of the external identity store that you chose.

If you are editing an identity store, the **External Identity Stores > Edit:** *id-store* page General tab appears, where *id-store* is the name of the external identity store that you chose.

Step 3 Complete the Name and Description fields as required.

Step 4 Check the Enable Password Change check box to modify the password, to detect the password expiration, and to reset the password.

Step 5 Click **Next**.

Step 6 Continue with Configuring an External LDAP Server Connection, page 8-35.

Note A NAC guest server can also be used as an external LDAP server. For the procedure to use a NAC guest server as an external LDAP server: http://www.cisco.com/c/en/us/td/docs/security/nac/guestserver/configuration_guide/20/nacguestserver/g_guestpol.html

Related Topic

- Deleting External LDAP Identity Stores, page 8-42

Configuring an External LDAP Server Connection

Use the LDAP page to configure an external LDAP identity store.

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**, and then click any of the following:

- **Create** and follow the wizard.
- **Duplicate and then Next**. The Server Connection page appears.
- **Edit**, and then **Next**. The Server Connection page appears.

Table 8-7 LDAP: Server Connection Page

Option	Description
Server Connection	
Enable Secondary Server	Check to enable the secondary LDAP server, which is used as a backup in the event that the primary LDAP server fails. If you check this check box, you must enter configuration parameters for the secondary LDAP server.
Always Access Primary Server First	Click to ensure that the primary LDAP server is accessed first, before the secondary LDAP server is accessed.
Failback to Primary Server After *min.*Minutes	Click to set the number of minutes that ACS authenticates using the secondary LDAP server if the primary server cannot be reached, where ***min.***is the number of minutes. After this time period, ACS reattempts authentication using the primary LDAP server. (Default is 5.)

Table 8-7 LDAP: Server Connection Page (continued)

Option	Description
Enable Deployment Configuration	Check to enable the deployment configuration tab. The primary and secondary hostname fields in the server connection page become read-only fields when you enable the deployment configuration. You need to configure the primary and secondary LDAP server hostname details in the deployment configuration page; the hostname details of the current ACS will appear in the server connection page after saving it. If you check the Enable Secondary Server check box after configuring the primary LDAP server hostname in the deployment configuration page, the mandatory fields such as port number, server timeout, and maximum admin connections are set to zero. You need to fill in these fields with an appropriate value.
Primary Server	
Hostname	Enter the IP address or DNS name of the machine that is running the primary LDAP software. The hostname can contain from 1 to 256 characters or a valid IP address expressed as a string. The only valid characters for hostnames are alphanumeric characters (a to z, A to Z, 0 to 9), the dot (.), and the hyphen (-).
Port	Enter the TCP/IP port number on which the primary LDAP server is listening. Valid values are from 1 to 65,535. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information by referring to the administrator of the LDAP server.
Anonymous Access	Click to ensure that searches on the LDAP directory occur anonymously. The server does not distinguish who the client is and will allow the client read access to any data that is configured accessible to any unauthenticated client. In the absence of specific policy permitting authentication information to be sent to a server, a client should use an anonymous connection.
Authenticated Access	Click to ensure that searches on the LDAP directory occur with administrative credentials. If so, enter information for the Admin DN and Password fields.
Admin DN	Enter the distinguished name of the administrator; that is, the LDAP account which, if bound to, permits searching all required users under the User Directory Subtree and permits searching groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users that LDAP authenticates.
Password	Enter the LDAP administrator account password.
Use Secure Authentication	Click to use Secure Sockets Layer (SSL) to encrypt communication between ACS and the primary LDAP server. Verify the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must select a root CA.
Check Server Identity	Check this check box to allow ACS to perform the server identity check while establishing connection with the LDAP server.
Root CA	Select a trusted root certificate authority from the drop-down list box to enable secure authentication with a certificate.
Server Timeout <*sec.*> Seconds	Enter the number of seconds that ACS waits for a response from the primary LDAP server before determining that the connection or authentication with that server has failed, where <*sec.*> is the number of seconds. Valid values are 1 to 300. (Default = 10.)

Table 8-7 LDAP: Server Connection Page (continued)

Option	Description
Max Admin Connections	Enter the maximum number of concurrent connections (greater than 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. Valid values are 1 to 99. (Default = 8.)
Test Bind To Server	Click to test and ensure that the primary LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.
Secondary Server	
Hostname	Enter the IP address or DNS name of the machine that is running the secondary LDAP software. The hostname can contain from 1 to 256 characters or a valid IP address expressed as a string. The only valid characters for hostnames are alphanumeric characters (a to z, A to Z, 0 to 9), the dot (.), and the hyphen (-).
Port	Enter the TCP/IP port number on which the secondary LDAP server is listening. Valid values are from 1 to 65,535. 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 DS Properties on the LDAP machine.
Anonymous Access	Click to verify that searches on the LDAP directory occur anonymously. The server does not distinguish who the client is and will allow the client to access (read and update) any data that is configured to be accessible to any unauthenticated client. In the absence of specific policy permitting authentication information to be sent to a server, a client should use an anonymous connection.
Authenticated Access	Click to ensure that searches on the LDAP directory occur with administrative credentials. If so, enter information for the Admin DN and Password fields.
Admin DN	Enter the domain name of the administrator; that is, the LDAP account which, if bound to, permits searching for all required users under the User Directory Subtree and permits searching groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users that LDAP authenticates.
Password	Type the LDAP administrator account password.
Use Secure Authentication	Click to use Secure Sockets Layer (SSL) to encrypt communication between ACS and the secondary LDAP server. Verify the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must select a root CA.
Check Server Identity	Check this checkbox to allow ACS to perform the server identity check while establishing connection with the LDAP server.
Root CA	Select a trusted root certificate authority from the drop-down list box to enable secure authentication with a certificate.
Server Timeout <*sec.*> Seconds	Type the number of seconds that ACS waits for a response from the secondary LDAP server before determining that the connection or authentication with that server has failed, where <*sec.*> is the number of seconds. Valid values are 1 to 300. (Default = 10.)

Table 8-7 LDAP: Server Connection Page (continued)

Option	Description
Max Admin Connections	Type the maximum number of concurrent connections (greater than 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. Valid values are 1 to 99. (Default = 8.)
Test Bind To Server	Click to test and ensure that the secondary LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.

Step 2 Click **Next**.

Step 3 Continue with Configuring External LDAP Directory Organization, page 8-38.

Configuring External LDAP Directory Organization

Use this page to configure an external LDAP identity store.

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**, then click any of the following:

- **Create** and follow the wizard until you reach the Directory Organization page.
- **Duplicate**, then click **Next** until the Directory Organization page appears.
- **Edit**, then click **Next** until the Directory Organization page appears.

Table 8-8 LDAP: Directory Organization Page

Option	Description
Schema	
Subject Object class	Value of the LDAP *objectClass* attribute that identifies the subject. Often, subject records have several values for the *objectClass* attribute, some of which are unique to the subject, some of which are shared with other object types. This box should contain a value that is not shared. Valid values are from 1 to 20 characters and must be a valid LDAP object type. This parameter can contain any UTF-8 characters. (Default = Person.)
Group Object class	Enter the group object class that you want to use in searches that identify objects as groups. (Default = GroupOfUniqueNames.)
Subject Name Attribute	Name of the attribute in the subject record that contains the subject name. You can obtain this attribute name from your directory server. This attribute specifies the subject name in the LDAP schema. You use this attribute to construct queries to search for subject objects. For more information, refer to the LDAP database documentation. Valid values are from 1 to 20 characters and must be a valid LDAP attribute. This parameter can contain any UTF-8 characters. Common values are *uid* and *CN*. (Default = uid.*)*

Table 8-8 LDAP: Directory Organization Page (continued)

Option	Description
Group Map Attribute	For user authentication, user lookup, and MAC address lookup, ACS must retrieve group membership information from LDAP databases. LDAP servers represent an association between a subject (a user or a host) and a group in one of the following two ways: • Groups refer to subjects • Subjects refer to groups The Group Map Attribute contains the mapping information. You must enter the attribute that contains the mapping information: an attribute in either the subject or the group, depending on: • If you select the Subject Objects Contain Reference To Groups radio button, enter a subject attribute. • If you select Group Objects Contain Reference To Subjects radio button, enter a group attribute.
Group Name Attribute	Name of the attribute in the group record that contains the group name. You can obtain this attribute name from your directory server. This attribute specifies the group name in the LDAP schema. You use this attribute to construct queries to search for group objects. For more information, refer to the LDAP database documentation. Common values are DN and *CN*. (Default = DN.*)*.
Certificate Attribute	Enter the attribute that contains certificate definitions. These definitions can optionally be used to validate certificates presented by clients when defined as part of a certificate authentication profile. In such cases, a binary comparison is performed between the client certificate and the certificate retrieved from the LDAP identity store.
Subject Objects Contain Reference To Groups	Click if the subject objects contain a reference to groups.
Group Objects Contain Reference To Subjects	Click if the group objects contain a reference to subjects.
Subjects In Groups Are Stored In Member Attribute As	Use the drop-down list box to indicate if the subjects in groups are stored in member attributes as either: • Username • Distinguished name
Directory Structure	

Subject Search Base	Enter the distinguished name (DN) for the subtree that contains all subjects. For example:
	`o=corporation.com`
	If the tree containing subjects is the base DN, enter:
	`o=corporation.com`
	or
	`dc=corporation,dc=com`
	as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

Table 8-8 LDAP: Directory Organization Page (continued)

Option	Description

Group Search Base	Enter the distinguished name (DN) for the subtree that contains all groups. For example:
	`ou=organizational unit[,ou=next organizational unit]o=corporation.com`
	If the tree containing groups is the base DN, type:
	`o=corporation.com`
	or
	`dc=corporation,dc=com`
	as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

Test Configuration	Click to obtain the expected connection and schema results by counting the number of users and groups that may result from your configuration.
Username Prefix\Suffix Stripping	
Strip start of subject name up to the last occurrence of the separator	Enter the appropriate text to remove domain prefixes from usernames. If, in the username, ACS finds the delimiter character that is specified in the *start_string* box, it strips all characters from the beginning of the username through the delimiter character. If the username contains more than one of the characters that are specified in the *start_string* box, ACS strips characters through the last occurrence of the delimiter character. For example, if the delimiter character is the backslash (\) and the username is DOMAIN\echamberlain, ACS submits echamberlain to an LDAP server. The *start_string* 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.
Strip end of subject name from the first occurrence of the separator	Enter the appropriate text to remove domain suffixes from usernames. If, in the username, ACS finds the delimiter character that is specified in the Y box, it strips all characters from the delimiter character through the end of the username. If the username contains more than one of the character specified in the Y box, ACS strips characters starting with the first occurrence of the delimiter character. For example, if the delimiter character is the at symbol (@) and the username is *jwiedman@domain*, then ACS submits *jwiedman* to an LDAP server. The *end_string* 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 *end_string* box contains any of these characters, stripping fails.

Table 8-8 LDAP: Directory Organization Page (continued)

Option	Description
MAC Address Format	
Search for MAC Address in Format <*format*>	MAC addresses in internal identity stores are stored in the format xx-xx-xx-xx-xx-xx. MAC addresses in LDAP databases can be stored in different formats. However, when ACS receives a host lookup request, ACS converts the MAC address from the internal format to the format that is specified in this field. Use the drop-down list box to enable search for MAC addresses in a specific format, where <*format*> can be any one of the following: • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx • xxxx.xxxx.xxxx The format you select must match the format of the MAC address stored in the LDAP server.

Step 2 Click **Next**.

Continue with Configuring LDAP Hostnames in Deployment Configuration, page 8-41.

Related Topics

- Configuring LDAP Groups, page 8-43
- Deleting External LDAP Identity Stores, page 8-42

Configuring LDAP Hostnames in Deployment Configuration

ACS 5.8 supports configuring different LDAP hostnames for different ACS instances in your deployment. Configuring all ACS instances in your deployment to communicate to a single LDAP server may affect the performance of that LDAP server. Also, if your LDAP servers are deployed in different locations, you can configure the ACS instance with the LDAP server that is deployed geographically closer to it. This type of configuration results in better response time. Therefore, to manage the load and increase the performance level, configure in such a way that different ACS instances communicate to different LDAP servers, preferably with the LDAP server deployed in your local geographical location.

ACS introduces a new tab called Deployment Configuration to configure different LDAP server hostnames for every ACS instance. After saving the configuration in Deployment Configuration page, the LDAP server hostnames are auto-populated in the Server Connection page. This configuration can be performed only from the primary ACS instance in a deployment. From the secondary ACS instance, you can only view the details of the LDAP configurations.

If you enable the LDAP Deployment Configurations in your deployment, when a request comes to one of the ACS instances, the ACS instance searches for the configured primary LDAP server. After finding the configured LDAP server, it communicates with that LDAP server and fetches the required details.

Before You Begin

Check the **Enable Deployment Configuration** check box in the Server Connection page. When you check the Enable Deployment Configuration check box, the primary and secondary LDAP server hostname fields become read-only fields.

Use this page to configure different primary and secondary LDAP hostnames for different ACS instances in your deployment:

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP** and then click any of the following:

- **Create** and follow the wizard until you reach the Deployment Configuration page.
- **Duplicate** and then click **Next** until the Deployment Configuration page appears.
- **Edit** and then click **Next** until the Deployment Configuration page appears.

Note Check the Enable Deployment Configuration check box to enable the Deployment Configuration tab operations. You can see the Deployment Configuration tab even though you have not checked the Deployment Configuration check box. If this Enable Deployment Configuration check box is unchecked, you cannot configure different primary and secondary LDAP server hostnames for the ACS instances in your deployment.

The Deployment Configuration page appears, displaying the current list of ACS instances that are active in your deployment.

Step 2 Check the check box near the ACS instance name and click **Edit**.

The LDAP hostname setting dialog box appears.

This dialog box contains the following two fields:

- **Primary Hostname**—Enter the hostname of the primary LDAP server so that the selected ACS instance communicates with the specified primary LDAP server.
- **Secondary Hostname**—Enter the hostname of the secondary LDAP server so that the selected ACS instance communicates with the specified secondary LDAP server when the primary LDAP server is down.

Step 3 Click **OK**.

The LDAP hostname configuration is saved.

Step 4 Click **Finish**.

The external identity store that you have created is saved.

Related Topics

- Creating External LDAP Identity Stores, page 8-34
- Deleting External LDAP Identity Stores, page 8-42

Deleting External LDAP Identity Stores

You can delete one or more external LDAP identity stores simultaneously.

To delete an external LDAP identity store:

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

The LDAP Identity Stores page appears, with a list of your configured external identity stores.

Step 2 Check one or more check boxes next to the external identity stores you want to delete.

Step 3 Click **Delete**.

The following error message appears:

```
Are you sure you want to delete the selected item/items?
```

Step 4 Click **OK**.

The External Identity Stores page appears, without the deleted identity stores in the list.

Related Topic

- Creating External LDAP Identity Stores, page 8-34

Configuring LDAP Groups

Use this page to configure an external LDAP group.

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**, then click any of the following:

- **Create** and follow the wizard.
- **Duplicate**, then click the **Directory Groups** tab.
- **Edit**, then click the **Directory Groups** tab.

The Selected Directory Groups field displays a list of groups that are available as options in rule-table group-mapping conditions.

Step 2 Do one of the following:

- Click **Select** to open the Groups secondary window from which you can select groups and add them to the Selected Directory Groups list.
- You can alternatively enter the LDAP groups in the Group Name field and click **Add**.

To remove a selected group from the Selected Directory Groups list, select that group in the Selected Directory Groups list and Click **Deselect**.

Step 3 Click **Submit** to save your changes.

Viewing LDAP Attributes

Use this page to view the external LDAP attributes.

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

Step 2 Check the check box next to the LDAP identity store whose attributes you want to view, click **Edit**, and then click the **Directory Attributes** tab.

Step 3 In the Name of example Subject to Select Attributes field, enter the name of an example object from which to retrieve attributes, then click **Select**.

For example, the object can be an user and the name of the object could either be the username or the user's DN.

Step 4 Complete the fields as described in Table 8-9.

Table 8-9 LDAP: Attributes Page

Option	Description
Attribute Name	Type an attribute name that you want included in the list of available attributes for policy conditions.
Type	Select the type you want associated with the attribute name you entered in the Attribute Name field.
Default	Specify the default value you want associated with the attribute name you entered in the Attribute Name field. If you do not specify a default value, no default is used. When attributes are imported to the Attribute Name/Type/Default box via the Select button, these default values are used: • String—Name of the attribute • Integer 64 • IP Address—This can be either an IP version 4 (IPv4) or IP version 6 (IPv6) address. • Unsigned Integer 32 • Boolean
Policy Condition Name	(*Optional*) Specify the name of the custom condition for this attribute. This condition will be available for selection when customizing conditions in a policy.

Step 5 Click **Add** and the information you entered is added to the fields on the screen.

The attributes listed here are available for policy conditions.

Step 6 Click **Submit** to save your changes.

Configuring LDAP Deployments

Use this page to view the external LDAP attributes.

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

Step 2 Check the check box next to the LDAP identity store whose attributes you want to view, click **Edit**, and then click the **Directory Attributes** tab.

Step 3 In the Name of example Subject to Select Attributes field, enter the name of an example object from which to retrieve attributes, then click **Select**.

For example, the object can be an user and the name of the object could either be the username or the user's DN.

Step 4 Complete the fields as described in Table 8-9.

Table 8-10 LDAP: Attributes Page

Option	Description
Attribute Name	Type an attribute name that you want included in the list of available attributes for policy conditions.
Type	Select the type you want associated with the attribute name you entered in the Attribute Name field.

Table 8-10 LDAP: Attributes Page (continued)

Option	Description
Default	Specify the default value you want associated with the attribute name you entered in the Attribute Name field. If you do not specify a default value, no default is used. When attributes are imported to the Attribute Name/Type/Default box via the Select button, these default values are used: • String—Name of the attribute • Integer 64 • IP Address—This can be either an IP version 4 (IPv4) or IP version 6 (IPv6) address. • Unsigned Integer 32 • Boolean
Policy Condition Name	(*Optional*) Specify the name of the custom condition for this attribute. This condition will be available for selection when customizing conditions in a policy.

Step 5 Click **Add** and the information you entered is added to the fields on the screen.

The attributes listed here are available for policy conditions.

Step 6 Click **Submit** to save your changes.

Leveraging Cisco NAC Profiler as an External MAB Database

ACS communicates with Cisco NAC Profiler to enable non-802.1X-capable devices to authenticate in 802.1X-enabled networks. Endpoints that are unable to authenticate through 802.1X use the MAC Authentication Bypass (MAB) feature in switches to connect to an 802.1X-enabled network.

Typically, non-user-attached devices such as printers, fax machines, IP phones, and Uninterruptible Power Supplies (UPSs) are not equipped with an 802.1x supplicant.

This means the switch port to which these devices attach cannot authenticate them using the 802.1X exchange of device or user credentials and must revert to an authentication mechanism other than port-based authentication (typically endpoint MAC address-based) in order for them to connect to the network.

Cisco NAC Profiler provides a solution for identifying and locating the endpoints that are unable to interact with the authentication component of these systems so that these endpoints can be provided an alternative mechanism for admission to the network.

NAC Profiler consists of an LDAP-enabled directory, which can be used for MAC Authentication Bypass (MAB). Thus, the NAC Profiler acts as an external LDAP database for ACS to authenticate non-802.1X-capable devices.

Note You can use the ACS internal host database to define the MAC addresses for non-802.1X-capable devices. However, if you already have a NAC Profiler in your network, you can use it to act as an external MAB database.

To leverage Cisco NAC Profiler as an external MAB database, you must:

- Enable the LDAP Interface on Cisco NAC Profiler. See Enabling the LDAP Interface on Cisco NAC Profiler to Communicate with ACS, page 8-46.
- Configure NAC Profiler in ACS. See Configuring NAC Profile LDAP Definition in ACS for Use in Identity Policy, page 8-48.

Enabling the LDAP Interface on Cisco NAC Profiler to Communicate with ACS

Note Before you can enable the LDAP interface on the NAC Profiler, ensure that you have set up your NAC Profiler with the NAC Profiler Collector. For more information on configuring Cisco NAC Profiler, refer to the *Cisco NAC Profiler Installation and Configuration Guide*, available under http://www.cisco.com/c/en/us/support/security/nac-profiler/products-installation-and-configuration-guides-list.html.

To enable the LDAP interface on the NAC Profiler to communicate with ACS:

Step 1 Log into your Cisco NAC Profiler.

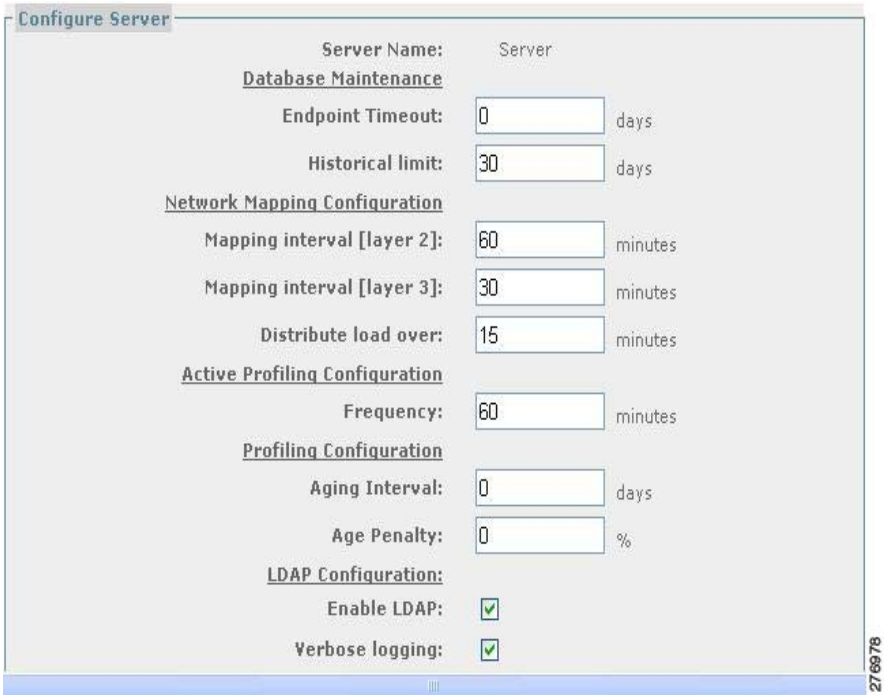
Step 2 Choose **Configuration > NAC Profiler Modules > List NAC Profiler Modules**.

Step 3 Click **Server**.

The Configure Server page appears.

Step 4 In the LDAP Configuration area, check the **Enable LDAP** check box as shown in Figure 8-1.

Figure 8-1 LDAP Interface Configuration in NAC Profiler



Step 5 Click **Update Server**.

Step 6 Click the **Configuration** tab and click **Apply Changes**.

The Update NAC Profiler Modules page appears.

Step 7 Click **Update Modules** to enable LDAP to be used by ACS.

You must enable the endpoint profiles that you want to authenticate against the Cisco NAC Profiler. For information on how to do this, see Configuring Endpoint Profiles in NAC Profiler for LDAP Authentication, page 8-47.

For proper Active Response Events you need to configure Active Response Delay time from your Cisco NAC Profiler UI. For this, choose **Configuration > NAC Profiler Modules > Configure Server > Advanced Options > Active Response Delay**.

Configuring Endpoint Profiles in NAC Profiler for LDAP Authentication

For the non-802.1X endpoints that you want to successfully authenticate, you must enable the corresponding endpoint profiles in NAC Profiler for LDAP authentication.

Note If the profile is not enabled for LDAP, the endpoints in the profile will not be authenticated by the Cisco NAC Profiler.

To enable the endpoint profiles for LDAP authentication:

Step 1 Log into your NAC Profiler.

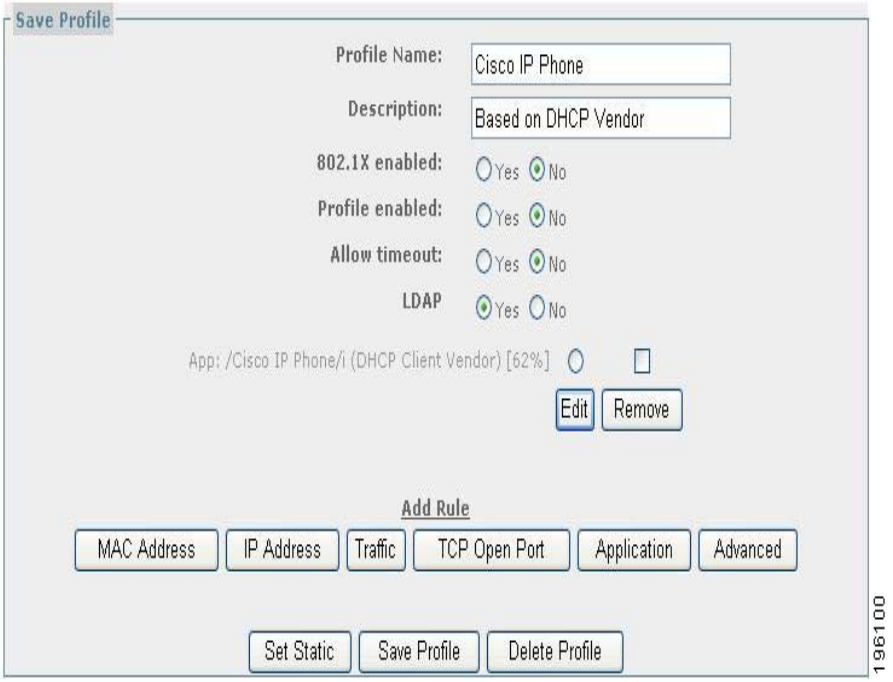
Step 2 Choose **Configuration > Endpoint Profiles > View/Edit Profiles List**.

A list of profiles in a table appears.

Step 3 Click the name of a profile to edit it.

Step 4 On the Save Profile page, ensure that the LDAP option is enabled by clicking the **Yes** radio button, if it is not already done as shown in Figure 8-2.

Figure 8-2 Configuring Endpoint Profiles in NAC Profiler



Step 5 Click **Save Profile**.

Configuring NAC Profile LDAP Definition in ACS for Use in Identity Policy

After you install ACS, there is a predefined LDAP database definition for NAC Profiler. This predefined database definition for NAC Profiler contains all the required data for establishing an initial connection. The only exception is the host information, which depends on your specific deployment configuration.

The steps below describe how to configure the host information, verify the connection, and use the profile database in policies.

Note Make sure that ACS NAC Profiler is chosen under **Access Policies > Access Services > Default Network Access > Identity**.

Note The **NAC Profiler** template in ACS, available under the LDAP external identity store, works with Cisco NAC Profiler version 2.1.8 and later.

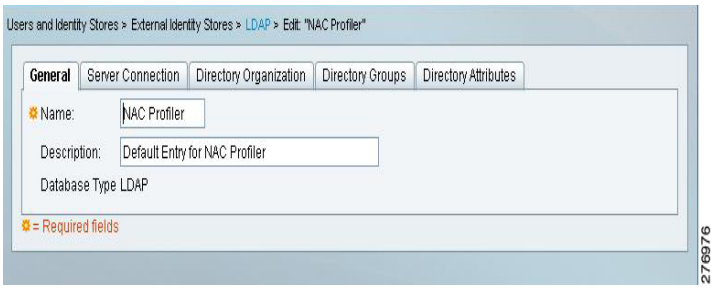
To edit the NAC Profiler template in ACS:

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

Step 2 Click on the name of the NAC Profiler template or check the check box next to the NAC Profiler template and click **Edit**.

The Edit NAC Profiler definition page appears as shown in Figure 8-3.

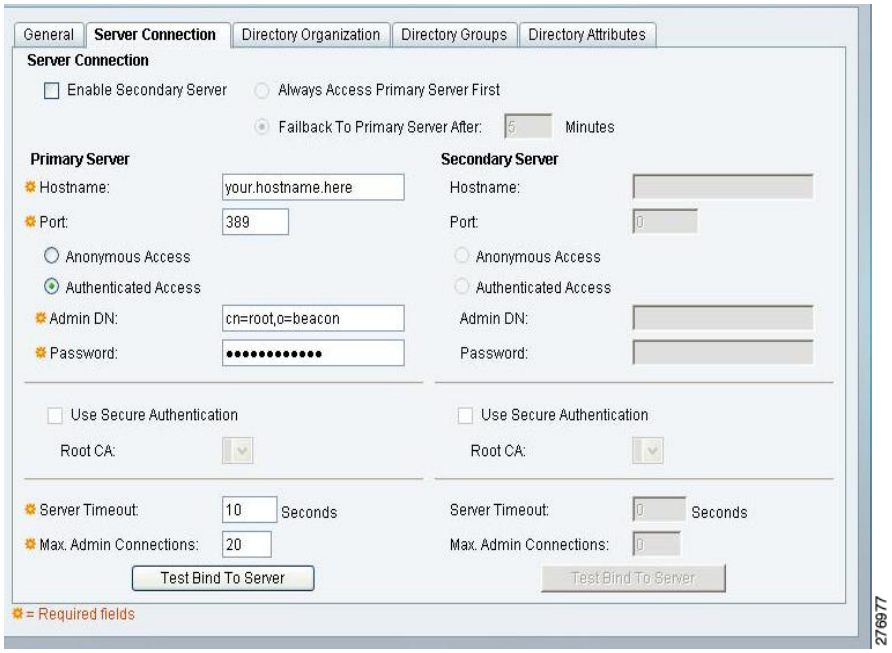
Figure 8-3 Edit NAC Profiler Definition — General Page



Step 3 Click the **Server Connection** tab.

The Edit page appears as shown in Figure 8-4.

Figure 8-4 Edit NAC Profiler Definition — Server Connection Page



Step 4 In the **Primary Server Hostname** field, enter the IP address or fully qualified domain name of the Profiler Server, or the Service IP of the Profiler pair if Profiler is configured for High Availability.

Step 5 Click **Test Bind to Server** to test the connection and verify ACS can communicate with Profiler through LDAP.

A small popup dialog, similar to the one shown in Figure 8-5 appears.

Figure 8-5 Test Bind to Server Dialog Box

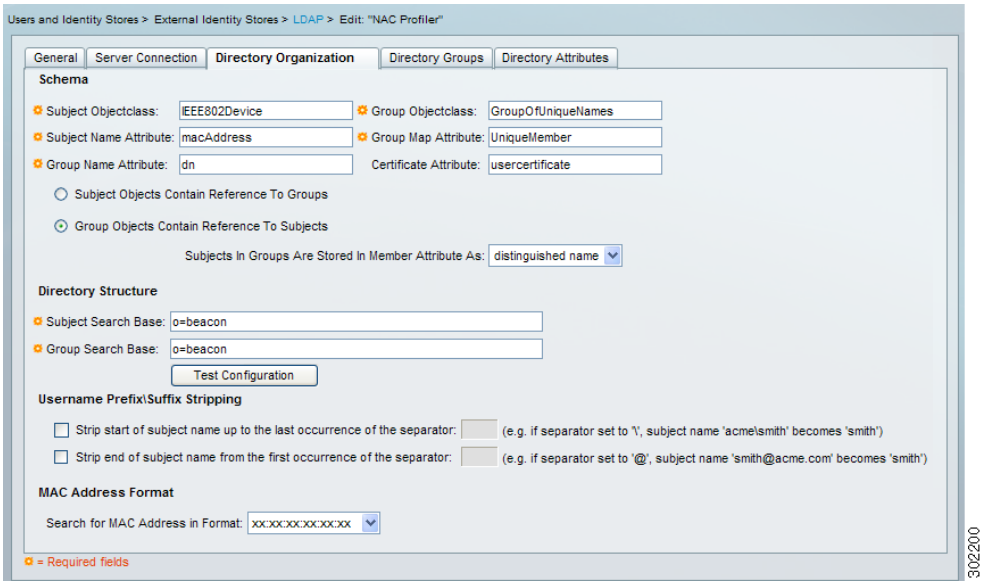
For more information, see Creating External LDAP Identity Stores, page 8-34.

Note The default password for LDAP is *GBSbeacon*. If you want to change this password, refer to the *Cisco NAC Profiler Installation and Configuration Guide*.

Step 6 If successful, go to the **Directory Organization** tab.

The Edit page appears as shown in Figure 8-6.

Figure 8-6 Edit NAC Profiler Definition — Directory Organization Page

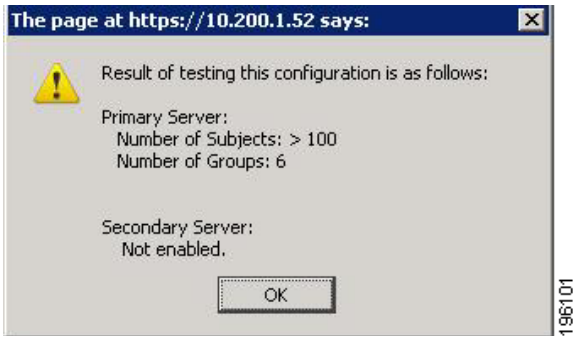


Step 7 Click **Test Configuration**.

A dialog box as shown in Figure 8-7 on page 50 appears that lists data corresponding to the Profiler. For example:

- Primary Server
- Number of Subjects: 100
- Number of Directory Groups: 6

Figure 8-7 Test Configuration Dialog Box



Number of Subjects—This value maps to the actual subject devices already profiled by the Cisco NAC Profiler (actual devices enabled for Profiler).

After the Profiler receives initial SNMP trap information from the switch, Profiler can poll the switch using SNMP to gather MIB (Management Information Base) information about the switch as well as the connecting endpoint.

After the Profiler has learned about the endpoint (e.g. MAC address, switch port), it adds the endpoint to its database. An endpoint added to the Profiler's database is considered 1 subject.

Number of Directory Groups—This value maps to the actual profiles enabled for LDAP on Profiler. When already running Profiler on your network, default profiles for endpoints are pre-configured.

However, all profiles are not enabled for LDAP, and must be configured as described in Configuring Endpoint Profiles in NAC Profiler for LDAP Authentication, page 8-47. Note that if setting up Profiler for the first time, once the Profiler is up and running, you will see zero groups initially.

The subjects and directory groups are listed if they are less than 100 in number. If the number of subjects or directory groups exceed 100, the subjects and directory groups are not listed. Instead, you get a message similar to the following one:

More than 100 subjects are found.

Step 8 Click the Directory Attributes tab if you want to use the directory attributes of subject records as policy conditions in policy rules. See Viewing LDAP Attributes, page 8-43 for more information.

Step 9 Choose NAC Profiler as the result (Identity Source) of the identity policy. For more information, see Viewing Identity Policies, page 10-23.

As soon as Endpoint is successfully authenticated from ACS server, ACS will do a CoA (Change of Authorization) and change VLAN. For this, you can configure static VLAN mapping in ACS server. For more information, see Specifying Common Attributes in Authorization Profiles, page 9-19.

When Endpoint is successfully authenticated the following message is displayed on the switch.

```
ACCESS-Switch# #show authentication sessions
Interface MAC Address Method Domain Status Session ID
Fa1/0/1 0014.d11b.aa36 mab DATA Authz Success 505050010000004A0B41FD15
```

For more information on features like Event Delivery Method and Active Response, see the *Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.*

Note You can use Microsoft Active Directory as an LDAP server and authenticate against ACS.

Troubleshooting MAB Authentication with Profiler Integration

To troubleshoot MAB authentication while integrating with NAC Profiler and to verify that the endpoint is successfully authenticated, complete the following steps:

Step 1 Run the following command on the switch which is connected to the endpoint devices:

```
ACCESS-Switch# show authentication sessions
```

The following output is displayed:

```
Interface  MAC Address    Method   Domain  Status         Session ID
Fa1/0/1    0014.d11b.aa36 mab      DATA    Authz Success  505050010000004A0B41FD15 reject
```

Step 2 Enable debugging for SNMP, AAA, and 802.1X on the switch.

Step 3 Verify the MAB authentication logs in **Monitoring and Reports Viewer > Troubleshooting**, for failure and success authentications.

Microsoft AD

ACS uses Microsoft Active Directory (AD) as an external identity store to store resources such as, users, machines, groups, and attributes. ACS authenticates these resources against AD.

Supported Authentication Protocols

- EAP-FAST and PEAP—ACS supports user and machine authentication and change password against AD using EAP-FAST and PEAP with an inner method of MSCHAPv2 and EAP-GTC.
- PAP—ACS supports authenticating against AD using TACACS PAP or ASCII method and also allows you to change AD users password.
- MSCHAPv1—ACS supports user and machine authentication against AD using MSCHAPv1. You can change AD users password using MSCHAPv1 version 2. ACS does not support MS-CHAP MPPE-Keys of a user, but does support MPPE-Send-Key and MPPE-Recv-Key.

Note ACS does not support changing user password against AD using MSCHAP version 1.

- MSCHAPv2—ACS supports user and machine authentication against AD using MSCHAPv2. ACS does not support MS-CHAP MPPE-Keys of a user, but does support MPPE-Send-Key and MPPE-Recv-Key.
- EAP-GTC—ACS supports user and machine authentication against AD using EAP-GTC.
- EAP-TLS—ACS uses the certificate retrieval option to support user and machine authentication against AD using EAP-TLS.

ACS 5.x supports changing the password for users who are authenticated against Active Directory in the TACACS+ PAP/ASCII, EAP-MSCHAP, and EAP-GTC methods. Changing the password for EAP-FAST and PEAP with inner MSCHAPv2 is also supported.

Changing the AD user password using the above methods must comply with the AD password policies. You must check with your AD administrator to determine the complete set of AD password policy rules. The most important AD password policies are:

- Enforce password history: N passwords are remembered.

- Maximum password age is N days.
- Minimum password age is N days.
- Minimum password length is N characters.
- Password must meet complexity requirements.

AD uses the "Maximum password age is N days" rule to detect password expiry. All other rules are used during attempts to change a password.

ACS supports these AD domains:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2012 R2 update 2

ACS machine access restriction (MAR) features use AD to map machine authentication to user authentication and authorization, and sets a the maximal time allowed between machine authentication and an authentication of a user from the same machine.

Most commonly, MAR fails authentication of users whose host machine does not successfully authenticate or if the time between machine and user authentication is greater than the specified aging time. You can add MAR as a condition in authentication and authorization rules as required.

While trying to join ACS to the AD domain, ACS and AD must be time-synchronized. Time in ACS is set according to the Network Time Protocol (NTP) server. Both AD and ACS should be synchronized by the same NTP server. If time is not synchronized when you join ACS to the AD domain, ACS displays a clock skew error. Using the command line interface on your appliance, you must configure the NTP client to work with the same NTP server that the AD domain is synchronized with.

The NTP process restarts automatically when it is down. You can check the NTP process status in two ways:

- Use the **`sh app status acs`** command in CLI interface.
- Choose **Monitoring and Reports > Reports > ACS Reports > ACS Instance > ACS_Health_Summary** in the ACS web interface.

For more information, see *CLI Reference Guide for Cisco Secure Access Control System 5.8*.

Note ACS supports two way trust between Active Directory domains.

The ACS appliance uses different levels of caching for AD groups, to optimize performance. AD groups are identified with a unique identifier, the Security Identifier (SID). ACS retrieves the SID that belongs to the user, and uses the cached mapping of the SID with the full name and path of the group. The AD client component caches the mapping for 24 hours. The run-time component of ACS queries the AD client and caches the results, as long as ACS is running.

Note To prevent ACS from using the outdated mappings, you should create new AD groups instead of changing or moving the existing ones. If you change or move the existing groups, you have to wait for 24 hours and restart the ACS services to refresh all the cached data.

Related Topics

- Prerequisites for Integrating Active Directory and ACS, page 8-54
- Network Ports That Must Be Open for Active Directory Communication, page 8-55

Prerequisites for Integrating Active Directory and ACS

The following are the prerequisites to integrate Active Directory with ACS.

- Use the Network Time Protocol (NTP) server settings to synchronize the time between the ACS server and Active Directory. You can configure NTP settings from ACS CLI.
- If your Active Directory structure has multi-domain forest or is divided into multiple forests, ensure that trust relationships exist between the domains to which ACS is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation.
- You must have at least one global catalog server operational and accessible by ACS, in the domain to which you are joining ACS.

Table 8-11 Active Directory Account Permissions Required for Performing Various Operations

Join Operations	Leave Operations	ACS Machine Accounts
For the account that is used to perform the join operation, the following permissions are required: • Search Active Directory (to see if a ACS machine account already exists) • Create ACS machine account to domain (if the machine account does not already exist) • Set attributes on the new machine account (for example, ACS machine account password, SPN, dnsHostname) **Note** It is not mandatory to be a domain administrator to perform a join operation.	For the account that is used to perform the leave operation, the following permissions are required: • Search Active Directory (to see if ACS machine account already exists) • Remove ACS machine account from domain **Note** If you perform a force leave (leave without domain credentials), it will not remove the machine account from the domain.	For the newly created ACS machine account, that is used to communicate to the Active Directory connection, the following permissions are required: • Ability to change own password • Read the user or machine objects corresponding to users or machines being authenticated • Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.) • Ability to read tokenGroups attribute **Note** You can precreate the machine account in Active Directory, and if the SAM name matches the ACS appliance hostname, it should be located during the join operation and re-used. **Note** If multiple join operations are performed, multiple machine accounts are maintained inside ACS, one for each join operation.

Note The credentials used for the join or leave operation are not stored in ACS. Only the newly created ACS machine account credentials are stored.

Related Topics

Network Ports That Must Be Open for Active Directory Communication, page 8-55

Network Ports That Must Be Open for Active Directory Communication

ACS supports certificate authorization. If there is a firewall between ACS and AD, certain ports need to be opened in order to allow ACS to communicate with AD. The following are the default ports to be opened:

Table 8-12 Network Ports That Must Be Open for Active Directory Communication

Protocol	Port (remote-local)	Target	Authenticated	Comments
DNS (TCP/UDP)	Random number greater than or equal to 49152	DNS Servers/AD Domain Controllers	No	—
MSRPC	445	Domain Controllers	Yes	—
Kerberos (TCP/UDP)	88	Domain Controllers	Yes (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	Domain Controllers	Yes	—
LDAP (GC)	3268	Global Catalog Servers	Yes	—
NTP	123	NTP Servers/Domain Controllers	No	—
KPASS	464	Domain Controllers	Yes (Kerberos)	MS AD/KDC
DNS (TCP/UDP)	53	DNS Servers/AD Domain Controllers	No	—
IPC	80	Other ACS nodes in the Deployment	Yes (Using RBAC credentials)	—

Note Dial-in users are not supported by AD in ACS.

This section contains the following topics:

- Machine Authentication, page 8-56
- Attribute Retrieval for Authorization, page 8-56
- Group Retrieval for Authorization, page 8-61
- Certificate Retrieval for EAP-TLS Authentication, page 8-61
- Concurrent Connection Management, page 8-62
- User and Machine Account Restrictions, page 8-62
- Machine Access Restrictions, page 8-62
- Dial-In Permissions, page 8-65
- Callback Options for Dial-In users, page 8-66
- Joining ACS to an AD Domain, page 8-67
- Selecting an AD Group, page 8-73
- Configuring AD Attributes, page 8-74

- Configuring Machine Access Restrictions, page 8-76
- Advanced Tunning, page 8-77
- Configuring Authentication Domains, page 8-78
- Diagnose Active Directory Problems, page 8-78
- Active Directory Alarms and Reports, page 8-80

Machine Authentication

Machine authentication provides access to network services to only these computers that are listed in Active Directory. This becomes very important for wireless networks because unauthorized users can try to access your wireless access points from outside your office building.

Machine authentication happens while starting up a computer or while logging in to a computer. Supplicants, such as Funk Odyssey perform machine authentication periodically while the supplicant is running.

If you enable machine authentication, ACS authenticates the computer before a user authentication request comes in. ACS checks the credentials provided by the computer against the Windows user database. If the credentials match, the computer is given access to the network.

Note When you perform Machine Authentication using EAP-TLS protocol, you should enable the "Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory" option and select the appropriate LDAP or Active Directory in the **Certificate Authentication Profile > CN User Name > Edit Page**.

Related Topics

- Attribute Retrieval for Authorization, page 8-56
- Boolean Attribute Support in Active Directory or LDAP, page 8-57
- Multi-Value Attribute Support in AD or LDAP, page 8-58
- Group Retrieval for Authorization, page 8-61
- Certificate Retrieval for EAP-TLS Authentication, page 8-61

Attribute Retrieval for Authorization

You can configure ACS to retrieve Active Directory user or machine attributes to be used in authorization and group-mapping rules. The attributes are mapped to the ACS policy results and determine the authorization level for the user or machine.

ACS retrieves the user and Active Directory machine attributes after a successful user or machine authentication; ACS can also retrieve the attributes for authorization and group-mapping purposes independent of authentication.

msRADIUSFramedIPAddress Attribute

In ACS, you can configure the Framed-IP-Address attribute as a dynamic value so that it takes the value dynamically from the AD attribute, msRADIUSFramedIPAddress during authentication. You can use the msRADIUSFramedIPAddress attribute that is retrieved from AD only as the IP address in ACS. You cannot convert this attribute type to string, integer, Boolean, and so on.

In AD, for every dial-in user, the AD administrator assigns a static IP address. When a dial-in user tries to connect to a network, the request is routed to ACS. ACS processes that request, authenticates the user against AD, and assigns the static IP address that is retrieved from AD to the dial-up client that is trying to connect to the network. In ACS 5.8, the msRADIUSFramedIPAdress attribute is of type IP Address.

You must configure the msRADIUSFramedIPAddress attribute in the Directory Attributes tab of Active Directory configuration in ACS and also use this attribute in the network access authorization profile for ACS to assign this value to the dial-up client. For more information on the network access authorization profile, see Authorization Profiles for Network Access, page 3-16.

Related Topics

- Boolean Attribute Support in Active Directory or LDAP, page 8-57
- Multi-Value Attribute Support in AD or LDAP, page 8-58
- Group Retrieval for Authorization, page 8-61
- Certificate Retrieval for EAP-TLS Authentication, page 8-61

Boolean Attribute Support in Active Directory or LDAP

ACS 5.8 allows you to configure Boolean attributes in AD or the LDAP Directory Attributes page and retrieves Boolean attributes from AD or LDAP during authentication against an AD or LDAP identity store. ACS retrieves the attributes specific to a user who is trying to authenticate against an AD or LDAP identity store.

ACS supports the following values for Boolean attributes:

- True—t, T, true, TRUE, True, and 1.
- False—f, F, false, FALSE, False, and 0.

You can configure Boolean attributes in AD or the LDAP Directory Attributes page and use them in authorization profiles. ACS does not recognize the Boolean attribute if you configure a value other than the supported values listed above.

- You can configure the Boolean attribute of AD or LDAP as a string. ACS converts the Boolean value of the specific attribute to a string value while retrieving it from AD or LDAP.

  For example, consider the Boolean attribute msTSAllowLogon.

  In AD or LDAP, the attribute msTSAllowLogon is a Boolean attribute. In ACS, you can configure the msTSAllowLogon attribute as string.
- If the value of a Boolean attribute in AD or LDAP is 0 or 1, you can convert that attribute to an integer.
- The Boolean attribute in AD or LDAP can be retrieved only as an attribute of type Boolean in ACS.
- You can also configure a string or an integer type AD or LDAP attribute as a Boolean attribute in ACS.

  For example, consider the attribute displayName.

  In AD or LDAP, the attribute displayName is a string or integer type attribute. In ACS, you can configure displayName as Boolean only when the value for the displayName attribute is one of the supported Boolean values listed above.

Note ACS does not support attribute substitution for Boolean attributes in RADIUS and TACACS+ authentications.

Related Topics

- Attribute Retrieval for Authorization, page 8-56
- Multi-Value Attribute Support in AD or LDAP, page 8-58
- Group Retrieval for Authorization, page 8-61
- Certificate Retrieval for EAP-TLS Authentication, page 8-61

Multi-Value Attribute Support in AD or LDAP

ACS 5.8 allows you to configure multi-value attributes in AD or the LDAP Directory Attributes page and retrieves multi-value attributes from AD or LDAP during authentication against an AD or LDAP identity store. ACS retrieves the attributes specific to a user who is trying to authenticate against an AD or LDAP identity store.

ACS supports the following AD or LDAP attribute types for multi-value attributes:

- String
- Integer
- IP Address

After you configure these multi-value attributes, you can use them in authorization profiles.

You can construct the following forms of conditions in access policies involving multiple value attributes:

- [Multiple value attribute] [operator] [Multiple value attribute]
- [Single value attribute] [operator] [Multiple value attribute]
- [Multiple value attribute] [operator] [Single value attribute]
- [Multiple value attribute] [operator] [Static value]

Operators for String-Type Multi-Value Attributes

ACS supports the following operators for String-type multi-value attributes:

- Equals
- Not Equals
- Starts with
- Ends with
- Contains
- Not contains

Table 8-13 displays the results of the conditions when you use the above operators among the multi-value, single value, and static value attribute operands.

Table 8-13 Results of the Operators Used Between the String Type Multi-Value Attributes

Left Operand	Right Operand	Equals	Not Equals	Starts with	Ends with	Contains	Not Contains
Multi-value attribute	Multi-value attribute	True if all values in the left operand are equal to at least one value in the right operand.	True if no value in the left operand is equal to any value in the right operand.	True if at least one value in the left operand starts with all values in the right operand.	True if at least one value in the left operand ends with all values in the right operand.	True if at least one value in the left operand contains all values in the right operand.	True if no value in the left operand contains any value in the right operand.
Single value attribute	Multi-value attribute						
Multi-value attribute	Single value attribute						
Multi-value attribute	Static value	True if at least one value in the left operand is equal to the value in the right operand.	True if no value in the left operand is equal to the value in the right operand.	True if at least one value in the left operand starts with the value in the right operand.	True if at least one value in the left operand ends with the value in the right operand.	True if at least one value in the left operand contains the value in the right operand.	True if no value in the left operand contains the value in the right operand.

Examples

- Left attribute value = 11 **Equals** Right attribute value = {22,11,33}

  Result = True
- Left attribute value = 11 **Equals** Right attribute value = {22,44}

  Result =False
- Left attribute value = 11 **Not Equals** Right attribute value = {22,33,44}

  Result = True
- Left attribute value = 11 **Not Contains** Right attribute value = {22,11,33}

  Result = False
- Left attribute value = 123 **Contains** Right attribute value = {12,23}

  Result = True

Operators for Integer-Type Multi-Value Attributes

ACS supports the following operators for Integer-type multi-value attributes:

- =
- !=
- >
- >=
- <
- <=

Table 8-14 displays the results of the conditions when you use the above operators among the multi-value, single value, and static value attribute operands.

Table 8-14 Results of the Operators Used Between the Integer-Type Multi-Value Attributes

Left Operand	Right Operand	=	!=	>	>=	<	<=
Multi-value attribute	Multi-value attribute	True if at least one value in the left operand is equal to one value in the right operand.	True if no value in the left operand is equal to any value in the right operand.	True if at least one value in the left operand is greater than one value in the right operand.	True if at least one value in the left operand is greater than or equal to one value in the right operand.	True if at least one value in the left operand is less than one value in the right operand.	True if at least one value in the left operand is less than or equal to one value in the right operand.
Single value attribute	Multi-value attribute						
Multi-value attribute	Single value attribute						
Multi-value attribute	Static value	True if at least one value in the left operand is equal to the value in the right operand.	True if no value in the left operand is equal to the value in the right operand.	True if at least one value in the left operand is greater than the value in the right operand.	True if at least one value in the left operand is greater than or equal to the value in the right operand.	True if at least one value in the left operand is less than the value in the right operand	True if at least one value in the left operand is less than or equal to the value in the right operand.

Examples

- Left attribute value = {11,22,33} **=** Right attribute value = 11

  Result = True
- Left attribute value = {11,22,33} **!=** Right attribute value = 11

  Result = False
- Left attribute value = {11,22,33} **>** Right attribute value = 11

  Result = True
- Left attribute value = {11,22,33} **<** Right attribute value = 11

  Result = False

Operators for IP-Address-Type Multi-Value Attributes

ACS supports the following operators for IP-Address type multi-value attributes:

- Equals
- Not Equals

Table 8-15 displays the results of the conditions when you use the above operators among the multi-value, single value, and static value attribute operands.

Table 8-15 Results of the Operators Used Between the IP-Address Type Multi-Value Attributes

Left Operand	Right Operand	Equals	Not Equals
Multi-value attribute	Multi-value attribute	True if at least one value in the left operand is equal to one value in the right operand.	True if no value in the left operand is equal to any value in the right operand.
Single value attribute	Multi-value attribute		
Multi-value attribute	Single value attribute		
Multi-value attribute	Static value		

Related Topics

- Attribute Retrieval for Authorization, page 8-56
- Boolean Attribute Support in Active Directory or LDAP, page 8-57
- Group Retrieval for Authorization, page 8-61
- Certificate Retrieval for EAP-TLS Authentication, page 8-61

Group Retrieval for Authorization

ACS can retrieve user or machine groups from Active Directory after a successful authentication and also retrieve the user or machine group independent of authentication for authorization and group mapping purposes. You can use the AD group data in authorization and group mapping tables and introduce special conditions to match them against the retrieved groups.

Related Topics

- Attribute Retrieval for Authorization, page 8-56
- Boolean Attribute Support in Active Directory or LDAP, page 8-57
- Multi-Value Attribute Support in AD or LDAP, page 8-58
- Certificate Retrieval for EAP-TLS Authentication, page 8-61

Certificate Retrieval for EAP-TLS Authentication

ACS 5.8 supports certificate retrieval for user or machine authentication that uses EAP-TLS protocol. The user or machine record on AD includes a certificate attribute of binary data type. This can contain one or more certificates. ACS refers to this attribute as userCertificate and does not allow you to configure any other name for this attribute.

ACS retrieves this certificate for verifying the identity of the user or machine. The certificate authentication profile determines the field (SAN, CN, SSN, SAN-Email, SAN-DNS, or SAN-other name) to be used for retrieving the certificates.

After ACS retrieves the certificate, it performs a binary comparison of this certificate with the client certificate. When multiple certificates are received, ACS compares the certificates to check if one of them match. When a match is found, ACS grants the user or machine access to the network.

Related Topics

- Concurrent Connection Management, page 8-62
- User and Machine Account Restrictions, page 8-62
- Machine Access Restrictions, page 8-62

Concurrent Connection Management

After ACS connects to the AD domain, at startup, ACS creates a number of threads to be used by the AD identity store for improved performance. Each thread has its own connection.

Related Topics

- User and Machine Account Restrictions, page 8-62
- Machine Access Restrictions, page 8-62

User and Machine Account Restrictions

While authenticating or querying a user or a machine, ACS checks whether:

- The user account disabled
- The user locked out
- The user's account has expired
- The query run outside of the specified logon hours

If the user has one of these limitations, the *AD1::IdentityAccessRestricted* attribute on the AD dedicated dictionary is set to indicate that the user has restricted access. You can use this attribute in group mapping and authorization rules.

Related Topics

- Machine Access Restrictions, page 8-62
- Distributed MAR Cache, page 8-64
- Dial-In Permissions, page 8-65
- Callback Options for Dial-In users, page 8-66
- Joining ACS to an AD Domain, page 8-67

Machine Access Restrictions

MAR helps tying the results of machine authentication to user authentication and authorization process. The most common usage of MAR is to fail authentication of users whose host machine does not successfully authenticate. The MAR is effective for all authentication protocols.

MAR functionality is based on the following points:

- As a result of Machine Authentication, the machine's RADIUS `Calling-Station-ID attribute (31)` is cached as an evidence for later reference.
- Administrator can configure the time to live (TTL) of the above cache entries in the AD settings page.
- Administrator can enable or disable MAR from AD settings page. However for MAR to work the following limitations must be taken into account:
  - Machine authentication must be enabled in the authenticating protocol settings
  - The AAA client must send a value in the Internet Engineering Task Force (IETF) RADIUS `Calling-Station-Id attribute (31).`
  - ACS does not replicate the cache of `Calling-Station-Id attribute` values from successful machine authentications.

  - ACS do not persevere the cache of `Calling-Station-Id attribute`. So the content is lost when ACS crashes unexpectedly. The content is not verified for consistency in case the administrator performs configuration changes that may effect machine authentication.
- When the user authenticates with either PEAP or EAP-FAST, against AD external ID store then ACS performs an additional action. It searches the cache for the users `Calling-Station-Id`. If it is found then **Was-Machine-Authenticated** attribute is set to true on the session context, otherwise set to false.

Note When you perform Machine Authentication using EAP-TLS protocol, you should enable the "Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory" option and select the appropriate LDAP or Active Directory in the **Certificate Authentication Profile > CN User Name > Edit** Page.

- For the above to function correctly, the user authentication request should contain the `Calling-Station-Id`. In case it does not, the **Was-Machine-Authenticated** attribute shall be set to false.
- The administrator can add rules to authorization policies that are based on AD GM attribute and on Machine authentication required attribute. Any rule that contains these two attributes will only apply if the following conditions are met:
  - MAR feature is enabled
  - Machine authentication in the authenticating protocol settings is enabled
  - External ID store is AD
- When a rule such as the one described above is evaluated, the attributes of AD GM and **Was-Machine-Authenticated** are fetched from the session context and checked against the rule's condition. According to the results of this evaluation an authorization result is set.
- Exemption list functionality is supported implicitly (in contrast to ACS 4.x). To exempt a given user group from the MAR the administrator can set a rule such that the column of **AD Group** consists of the group to exempt and the column of **Machine Authentication Required** consists of *No*. See the second rule in the table below for an example.

  For example, the administrator will add rules to the authorization policy as follows:

AD Group	Machine Authentication Required	…	ATZ profile
Engineers	Yes	…	VLAN X
Managers	No	…	VLAN B
…	…	…	DENY ACCESS

The Engineers' rule is an example of MAR rule that only allows engineers access if their machine was successfully authenticated against windows DB.

The Managers' rule is an example of an exemption from MAR.

Related Topics

- Distributed MAR Cache, page 8-64
- Dial-In Permissions, page 8-65
- Callback Options for Dial-In users, page 8-66

- Joining ACS to an AD Domain, page 8-67

Distributed MAR Cache

ACS 5.8 supports the Machine Access Restriction cache per ACS deployment. That is, machine authentication results can be cached among the nodes within a deployment.

MAR Cache Distribution Groups

ACS 5.8 has the option to group ACS nodes in MAR cache distribution groups. This option is used to control the impact of MAR cache distribution operations on ACS performance and memory usage.

A text label is assigned to each ACS node, which is called the MAR cache distribution group value. ACS nodes are grouped based on the MAR cache distribution group value. You can perform MAR cache distribution operations only between the ACS nodes that are assigned to the same MAR cache distribution group.

If the group value of an ACS node is empty, then it is considered as not assigned to any MAR cache distribution group. Such ACS nodes are not part of any MAR cache distribution operations.

Distributed MAR Cache Operation

The ACS runtime component combines two operations to implement a distributed MAR cache:

- MAR cache replication with no guaranteed delivery
- MAR cache distributed search

MAR Cache Replication

The ACS runtime component stores a MAR entry, `authenticated Calling-Station-ID`, in a MAR cache during machine authentication. Initially, ACS saves the MAR entry in the local MAR cache. Then, the ACS runtime component replicates the MAR entry to the ACS nodes that belong to the same MAR cache distribution group.

The replication is performed based on the cache entry replication attempts and the cache entry replication time-outs that are configured in the ACS web interface.

The replication operation is performed in the background and does not interrupt or delay the user authentication that triggered this replication.

MAR Cache Distributed Search

When an authentication request comes in, ACS searches for the MAR entry in the local MAR cache. If a MAR entry is not found in the local MAR cache, then ACS queries the ACS nodes that are assigned to the same MAR cache distribution group.

The distributed search is performed based on the cache entry query attempts and cache entry query time-outs that are configured in the ACS web interface. The MAR entry search is also delayed until the first successful response from any of the queried ACS nodes, up to the maximum of the configured cache entry query timeout period. You can see any of the following messages in ACS View for an authentication that involves querying the MAR Cache:

- 24422 - ACS has confirmed previous successful machine authentication for user in Active Directory.
- 24423 - ACS has not been able to confirm previous successful machine authentication for user in Active Directory.
- 24701 - ACS peer has confirmed previous successful machine authentication for user in Active Directory.

- 24702 - ACS peers have not confirmed previous successful machine authentication for user in Active Directory.

Distributed MAR Cache Reliability

The ACS runtime component provides a reliable mechanism to implement the distributed MAR cache operation.

The distributed search option provides a fallback facility when the replication messages for some reason are not delivered. In this case, you can find the MAR cache entry on the ACS node that performs the machine authentication or on any one of the ACS nodes from the same MAR cache distribution group. The distributed search option also provides a fallback facility when the ACS node that performs the machine authentication is restarted. In this case, also, you can find the MAR cache entry in any one of the ACS nodes from the same MAR cache distribution group.

Distributed MAR Cache Persistency

ACS 5.8 stores the MAR cache content, calling-station-ID list, and the corresponding time stamps to a file on its local disk when you manually stop the ACS run-time services. The other ACS instances in the MAR cache distribution group cannot access the MAR cache of an ACS instance when the run-time services of this ACS instance are down. ACS does not store the MAR cache entries of an instance when there is an accidental restart of its run-time services.

ACS reads the MAR cache entries from the file on its local disk based on the cache entry time to live when the ACS run-time services get restarted. When the run-time services of an ACS instance come up after a restart, ACS compares the current time of that instance with the MAR cache entry time. If the difference between the current time and the MAR entry time is greater than the MAR cache entry time to live, then ACS does not retrieve that entry from disk. Otherwise, ACS retrieves that MAR cache entry and updates its MAR cache entry time to live.

Related Topics

- Dial-In Permissions, page 8-65
- Callback Options for Dial-In users, page 8-66
- Joining ACS to an AD Domain, page 8-67

Dial-In Permissions

The dial-in permissions of a user are checked during authentications or queries from Active Directory. The dial-in check is supported only for user authentications and not for machines, in the following authentication protocols:

- PAP
- MSCHAPv2
- EAP-FAST
- PEAP
- EAP-TLS.

The following results are possible:

- Allow Access
- Deny Access

- Control Access through Remote Access Policy. This option is only available for Windows 2000 native domain, Windows server 2003 domain.
- Control Access through NPS Network Policy. This is the default result. This option is only available for Windows server 2008, Windows 2008 R2, and Windows 2012 domains.

Related Topics

- Callback Options for Dial-In users, page 8-66
- Joining ACS to an AD Domain, page 8-67

Callback Options for Dial-In users

If the callback option is enabled, the server calls the caller back during the connection process. The phone number that is used by the server is set either by the caller or the network administrator.

The possible callback options are:

- No callback
- Set by Caller (routing and remote access service only). This option can be used to define a series of static IP routes that are added to the routing table of the server running the Routing and Remote Access service when a connection is made.
- Always callback to (with an option to set a number). This option can be used to assign a specific IP address to a user when a connection is made

The callback attributes should be returned on the RADIUS response to the device.

Dial-In Support Attributes

The user attributes on Active Directory are supported on the following servers:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

ACS does not support Dial-in users on Windows 2000.

ACS Response

If you enable the dial-in check on ACS Active Directory and the user's dial-in option is 'Deny Access' on Active Directory, the authentication request is rejected with a message in the log, indicating that dial-in access is denied. If a user fails an MSCHAP v1/v2 authentication if the dial-in is not enabled, ACS should set on the EAP response a proper error code (NT error = 649).

In case that the callback options are enabled, the ACS RADIUS response contains the returned Service Type and Callback Number attributes as follows:

- If callback option is Set by Caller or Always Callback To, the service-type attribute should be queried on Active Directory during the user authentication. The service-type can be the following:
  - 3 = Callback Login
  - 4 = Callback Framed

  - 9 = Callback NAS Prompt

  This attribute should be returned to the device on Service-type RADIUS attribute. If ACS is already configured to return service-type attribute on the RADIUS response, the service-type value queried for the user on Active Directory replaces it.

- If the Callback option is Always Callback To, the callback number should also be queried on the Active Directory user. This value is set on the RADIUS response on the Cisco-AV-Pair attribute with the following values:
  - cisco-av-pair=lcp:callback-dialstring=[callback number value]
  - cisco-av-pair=Shell:callback-dialstring=[callback number value]
  - cisco-av-pair=Slip:callback-dialstring=[callback number value]
  - cisco-av-pair=Arap:callback-dialstring=[callback number value]

  The callback number value is also returned on the RADIUS response, using the RADIUS attribute CallbackNumber (#19).
- If callback option is Set by Caller, the RADIUS response contains the following attributes with no value:
  - cisco-av-pair=lcp:callback-dialstring=
  - cisco-av-pair=Shell:callback-dialstring=
  - cisco-av-pair=Slip:callback-dialstring=
  - cisco-av-pair=Arap:callback-dialstring=

Related Topics

- Joining ACS to an AD Domain, page 8-67
- Configuring an AD Identity Store, page 8-68

Joining ACS to an AD Domain

You can join the ACS nodes from same deployment to different AD domains that has two way trust between each other. However, each node can be joined to a single AD domain. The policy definitions of those ACS nodes are not changed and that uses the same AD identity store.

Note

- Previous releases of ACS disconnects the Active Directory domain and displays the status as “joined but disconnected” in the Active Directory connection details page, when you stop the ad-client process manually from ACS CLI. But in ACS 5.8, when you stop the ad-client process manually from ACS CLI, ACS disconnects Active Directory domain and displays the status as “None” in Active Directory connection details page. If you start the ad-client process again from ACS CLI, ACS gets connected to the Active Directory domain and displays the status as “joined and connected” in AD connection details page.
- In ACS 5.8, you must manually join ACS to Active Directory after upgrading ACS 5.x to ACS 5.8. See Installation and Upgrade Guide for Cisco Secure Access Control System for more information on upgrade methods.
- Prior to Release 5.8, ACS started the adclient process only after joining the Active Directory domain to ACS. But, ACS 5.8 starts the adclient process soon after installing it.
- The Windows AD account, which joins ACS to the AD domain, can be placed in its own organizational unit (OU). It resides in its own OU either when the account is created or later on, with a restriction that the appliance name must match the name of the AD account.

- ACS does not support user authentication in AD when a user name is supplied with an alternative UPN suffix configured in OU level. The authentication works fine if the UPN suffix is configured in domain level.

For information on how to configure an AD identity store, see Configuring an AD Identity Store, page 8-68.

Related Topics

- Configuring an AD Identity Store, page 8-68
- Selecting an AD Group, page 8-73
- Configuring AD Attributes, page 8-74
- Configuring Machine Access Restrictions, page 8-76

Configuring an AD Identity Store

The AD settings are not displayed by default, and they are not joined to an AD domain when you first install ACS. When you open the AD configuration page, you can see the list of all ACS nodes in the distributed deployment.

When you configure an AD identity store, ACS also creates the following:

- A new dictionary for that store with two attributes: the ExternalGroup attribute and another attribute for any attribute that is retrieved from the Directory Attributes page.
- A new attribute, IdentityAccessRestricted. You can manually create a custom condition for this attribute.
- A custom condition for group mapping from the ExternalGroup attribute—the custom condition name is AD1:ExternalGroups—and another custom condition for each attribute that is selected in the Directory Attributes page (for example, AD1:cn).

You can edit the predefined condition name, and you can create a custom condition from the Custom condition page. See Creating, Duplicating, and Editing a Custom Session Condition, page 9-5.

To authenticate users and join ACS with an AD domain:

Step 1 Choose **Users and Identity Stores > External Identity Stores > Active Directory**.

The Active Directory page appears.

The AD configuration page acts as a central AD management tool for all ACS nodes. You can perform the join and leave operations against a single ACS node or multiple ACS nodes on this page. You can also view the join results of all ACS nodes in the deployment at a single glance.

Step 2 Modify the fields in the General tab as described in Table 8-16.

Table 8-16 Active Directory: General Page

Option	Description
Connection Details	
Join	Click to join ACS with the AD domain for the given user, domain, and password entered. See Joining Nodes to an AD Domain, page 8-70.

Table 8-16 Active Directory: General Page (continued)

Option	Description
Leave	Click to disconnect a single node or multiple nodes from the AD domain for the given user, domain, and password entered. See Disconnecting Nodes from the AD Domain, page 8-71.
End User Authentication Settings	
Enable password change	Click to allow the password to be changed.
Enable machine authentication	Click to allow machine authentication.
Enable dial-in check	Click to examine the user's dial-in permissions during authentication or query. The result of the check can cause a reject of the authentication in case the dial-in permission is denied. The result is not stored on the AD dictionary.
Enable callback check for dial-in clients	Click to examine the user's callback option during authentication or query. The result of the check is returned to the device on the RADIUS response. The result is not stored on the AD dictionary.
Use Kerberos for Plain Text	Click to use Kerberos for plain-text authentications. For ACS 5.8, the default and recommended option is MS-RPC. Until ACS 5.7, Kerberos was used as a default option.
Identity Resolution—The identity resolution settings allows you to configure important settings to tune the security and performance balance to match your Active Directory deployment. You can use these settings to tune authentications for usernames and hostnames without domain markup.	
If identity does not include the AD domain	
Reject the request	Click this option to reject the authentication request for users those who do not have any domain markups, such as a SAM name. This is useful in case of multi join domains where ACS will have to look up for the identity in all the joined global catalogs, which might not be very secure. This option forces the users to use names with domain markups.
Only search in the "Authentication Domains" from the joined forest	Click this option to search for the identity only in the trusted domains in the forest which are specified in the authentication domains section. This is the default option and identical to ACS 5.7 behavior for SAM account names.
Search in all the "Authentication Domains" section	Click this option to search for the identity in all authentication domains in all the trusted forests. This might increase latency and impact performance.
Only search in the "Joined Domain"	(Introduced in ACS 5.8 patch 9 release) This option will search for the identity only in the joined domain. **Note** If you have selected the Only search in the "Joined Domain" option and are downgrading from an ACS 5.8 patch 9 or later release to a lower release, ensure that you deselect this option, and select one of the other three options (Reject the request, Only search in the "Authentication Domains", or Search in all the "Authentication Domains" sections).
If some of the domains are unreachable	
Proceed with available domains	Click this option to proceed with the authentication if it finds a match in any of the available domains when a few domains are not reachable.
Drop the request	Click this option to drop the authentication request if the identity resolution encounters some unreachable or unavailable domains.

Step 3 Click:

- **Save Changes** to save the configuration.
- **Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify the following:
  - There are no policy rules that use custom conditions based on the AD dictionary.
  - The AD is not chosen as the identity source in any of the available access services.
  - There are no identity store sequences with the AD.
- **Refresh** to update the data in Directory Groups, Authentication Domains, and Diagnostic Tool tabs after joining or leaving ACS to AD domain(s).

The Active Directory configuration is saved. The Active Directory page appears with the new configuration.

Note

- The AD configuration is affected (and sometimes gets disconnected) when there is a slow response from the server while you test the ACS connection with the AD domain. However the configuration works fine with the other applications.
- Active Directory page in ACS 5.8 is refreshed automatically for every 60 seconds. If you perform an operation in AD page, the status of the operation will be updated in AD page only after 60 seconds. If you want to see the updated status immediately, you must click **Refresh** option that is available at the bottom of the General tab.
- Due to NETBIOS limitations, ACS hostnames must contain less than or equal to 15 characters.

Note If “User change password at next logon” option is enabled for an AD user:
(a) If you use Kerberos for user authentication, the password gets changed immediately after you change the password on next login.
(b) If you use MSRPC for user authentication, you must wait for a reasonable time for the new password to get synchronized with ACS after you change the password on next login. During this time, the old password may work. see https://support.microsoft.com/en-us/kb/906305 for more information.

Joining Nodes to an AD Domain

You can join a single ACS node to only one AD domain. ACS does not support joining a single ACS node to multiple AD domains. But, ACS supports joining multiple ACS nodes to a single AD domain.

To join ACS nodes to an AD domain, complete the following steps:

Step 1 Choose **Users and Identity Stores > External Identity Stores > Active Directory.**

The Active Directory page appears.

Step 2 Select a single node or multiple nodes and click **Join**.

The Join page appears.

Step 3 Complete the fields in the Join page as described in Table 8-17.

Table 8-17 Join/Test Connection Page

Option	Description
Active Directory Domain Name	Name of the AD domain to which you want to join ACS.
Username	Enter the username of a predefined AD user. An AD account which is required for the domain access in ACS, should have either of the following: • Add workstations to the domain user in the corresponding domain. • Create Computer Objects or Delete Computer Objects permission on corresponding computers container where ACS machine's account is precreated (created before joining ACS machine to the domain). Cisco recommends that you disable the lockout policy for the ACS account and configure the AD infrastructure to send alerts to the administrator if a wrong password is used for that account. This is because, if you enter a wrong password, ACS will not create or modify its machine account when it is necessary and therefore possibly deny all authentications.
Password	Enter the user password. The password should have a minimum of 8 characters, using a combination of at least one lower case letter, one upper case letter, one numeral, and one special character. All special characters are supported.

Step 4 Click:

- **Join** to join the selected nodes to the AD domain. The status of the nodes are changed according to the join results.
- **Cancel** to cancel the connection.

Note After joining ACS to an Active Directory domain, if you delete the name server from ACS CLI, ACS prompts you to restart the services. If you enter No for restarting the services, ACS does not restart its services and deletes the name server from the configuration. But in the Active Directory General page, ACS displays the status of the Active Directory domain as None.

Disconnecting Nodes from the AD Domain

To disconnect a single node or multiple nodes from an AD Domain, complete the following steps:

Step 1 Choose **Users and Identity Stores > External Identity Stores > Active Directory**.

The Active Directory page appears.

Step 2 Select a single node or multiple nodes and click **Leave**.

The Leave Connection page appears.

Step 3 Complete the fields in the Leave Connection page as described in Table 8-18.

Table 8-18 Leave Connection Page

Option	Description
Username	Enter the username of a predefined AD user. An AD account which is required for the domain access in ACS, should have either of the following: • Add workstations to the domain user in the corresponding domain. • Create Computer Objects or Delete Computer Objects permission on corresponding computers container where ACS machine's account is precreated (created before joining ACS machine to the domain). Cisco recommends that you disable the lockout policy for the ACS account and configure the AD infrastructure to send alerts to the administrator if a wrong password is used for that account. This is because, if you enter a wrong password, ACS will not create or modify its machine account when it is necessary and therefore possibly deny all authentications.
Password	Enter the user password.
Do not try to remove machine account	Check this check box to disconnect the selected nodes from the AD domain, when you do not know the credentials or have any DNS issues. This operation disconnects the node from the AD domain and leaves an entry for this node in the database. Only administrators can remove this node entry from the database.

Step 4 Click:

- **Leave** to disconnect the selected nodes from AD domain.
- **Cancel** to cancel the operation.

Note

- Administrators can perform operations the join or leave operations from the secondary server. When you perform these operations from the secondary server, it affects only the secondary server.
- Authentications are not obligated to fail immediately when you disable ACS account from Active Directory domain. Authentications can work as long as there are established connections or TGT tickets. Authentications can fail with different errors based on LDAP, Kerberos or RPC depends upon which connection it is using to connect to ACS. It also depends on replication between Domain Controllers.

Related Topics

- Selecting an AD Group, page 8-73
- Configuring AD Attributes, page 8-74
- Configuring Machine Access Restrictions, page 8-76
- Advanced Tunning, page 8-77
- Configuring Authentication Domains, page 8-78
- Diagnose Active Directory Problems, page 8-78
- Active Directory Alarms and Reports, page 8-80

Selecting an AD Group

Use this page to select groups that can then be available for policy conditions.

Note To select groups and attributes from an AD, ACS must be connected to that AD.

Step 1 Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Directory Groups** tab.

The Groups page appears with corresponding Security Identifier (SID). The Selected Directory Groups field lists the AD groups you selected and saved. The AD groups you selected in the External User Groups page are listed and can be available as options in group mapping conditions in rule tables.

If you have more groups in other trusted domains or forests that are not displayed, you can use the search filter to narrow down your search results. You can also add a new AD group using the **Add** button.

Note

- ACS does not retrieve domain local groups. It is not recommended to use domain local groups in ACS policies. The reason is that the membership evaluation in domain local groups can be time consuming. So, by default, the domain local groups are not evaluated.
- ACS 5.5, 5.6, or 5.7 do not have SIDs associated with the directory groups. Therefore, after upgrading from ACS 5.5, 5.6, or 5.7 to ACS 5.8, the directory groups are displayed without the SID values. You can find a new column called SID against each directory groups and the value of SID will be empty for all the directory groups. You have to retrieve the directory groups again to set a SID value for the groups.

Step 2 Click **Select** to see the available AD groups on the domain and its child domains. To see the AD trusted domain groups in the same forest, you need to explicitly provide the trusted domain details in the search base DN field.

The External User Groups dialog box appears displaying a list of AD groups in the domain, as well as other trusted domains in the same forest.

If you have more groups that are not displayed, use the search filter to refine your search and click **Go**.

Step 3 Enter the AD groups or select them from the list, then click **OK**.

To remove an AD group from the list, click an AD group, then click **Deselect**.

Step 4 Click:

- **Save Changes** to save the configuration.
- **Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that there are no policy rules that use custom conditions based on the AD dictionary.

Note

- When configuring the AD Identity Store on ACS 5.x, the security groups defined on Active Directory are enumerated and can be used, but distribution groups are not shown. Active Directory Distribution groups are not security-enabled and can only be used with e-mail applications to send e-mail to collections of users. Please refer to Microsoft documentation for more information on distribution groups.
- Logon authentication may fail on Active Directory when ACS tries to authenticate users who belong to more than 1015 groups in external identity stores. This is due to the Local Security Authentication (LSA) limitations in Active Directory.

Related Topics

- Configuring AD Attributes, page 8-74
- Configuring Machine Access Restrictions, page 8-76
- Advanced Tunning, page 8-77
- Configuring Authentication Domains, page 8-78
- Diagnose Active Directory Problems, page 8-78
- Active Directory Alarms and Reports, page 8-80

Configuring AD Attributes

Use this page to select attributes that can then be available for policy conditions.

Step 1 Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Directory Attributes** tab.

Step 2 Complete the fields in the Active Directory: Attributes page as described in Table 8-19:

Table 8-19 Active Directory: Attributes Page

Option	Description
Name of example Subject to Select Attributes	Enter the name of a user or computer found on the joined domain. You can enter the user's or the computer's CN or distinguished name. The set of attributes that are displayed belong to the subject that you specify. The set of attributes are different for a user and a computer.
Select	Click to access the Attributes secondary window, which displays the attributes of the name you entered in the previous field.
Attribute Name List—Displays the attributes you have selected in the secondary Selected Attributes window. You can select multiple attributes together and submit them.	
Attribute Name	• Do one of the following: – Enter the name of the attribute. – You can also select an attribute from the list, then click **Edit** to edit the attribute. • Click **Add** to add an attribute to the Attribute Name list.

Table 8-19 Active Directory: Attributes Page (continued)

Option	Description
Type	Attribute types associated with the attribute names. Valid options are: • String • Integer 64 • IP Address—This can be either an IPv4 or IPv6 address. • Unsigned Integer 32 • Boolean
Default	Specified attribute default value for the selected attribute: • String—Name of the attribute. • Integer 64—0 • Unsigned Integer 64—0. • IP Address—No default set. • Boolean—No default set.
Policy Condition Name	Enter the custom condition name for this attribute. For example, if the custom condition name is *AAA*, enter **AAA** in this field and not **AD1:*att_name***.
Select Attributes Secondary Window	Available from the Attributes secondary window only.
Search Filter	Specify a user or machine name. • For user names, you can specify distinguished name, SAM, NetBios, or UPN format. • For machine names, you can specify one of the following formats: MACHINE$, NETBiosDomain\MACHINE$, host/MACHINE, or host/machine.domain. You can specify non-English letters for user and machine names.
Attribute Name	The name of an attribute of the user or machine name you entered in the previous field.
Attribute Type	The type of attribute.
Attribute Value	The value of an attribute for the specified user or machine.

Step 3 Do one of the following:

- **Click Save Changes** to save the configuration.
- **Click Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that there are no policy rules that use custom conditions based on the AD dictionary.

Related Topics

- Configuring Machine Access Restrictions, page 8-76
- Advanced Tunning, page 8-77
- Configuring Authentication Domains, page 8-78
- Diagnose Active Directory Problems, page 8-78
- Active Directory Alarms and Reports, page 8-80

Configuring Machine Access Restrictions

To configure the Machine Access Restrictions, complete the following steps:

Step 1 Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Machine Access Restrictions** tab.

Step 2 Complete the fields in the Active Directory: Machine Access Restrictions page as described in Table 8-20.

Table 8-20 Active Directory: Machine Access Restrictions Page

Option	Description
Enable Machine Access Restrictions	Check this check box to enable the Machine Access Restrictions controls in the web interface. This ensures that the machine authentication results are tied to user authentication and authorization. If you enable this feature, you must set the Aging time.
Aging time (hours)	Time after a machine was authenticated that a user can be authenticated from that machine. If this time elapses, user authentication fails. The default value is 6 hours. The valid range is from 1 to 8760 hours.
MAR Cache Distribution	
Cache entry replication timeout	Enter the time in seconds after which the cache entry replication gets timed out. The default value is 5 seconds. The valid range is from 1 to 10.
Cache entry replication attempts	Enter the number of times ACS has to perform MAR cache entry replication. The default value is 2. The valid range is from 0 to 5.
Cache entry query timeout	Enter the time in seconds after which the cache entry query gets timed out. The default value is 2 seconds. The valid range is from 1 to 10.
Cache entry query attempts	Enter the number of times that ACS has to perform the cache entry query. The default value is 1. The valid range is from 0 to 5.
Node	Lists all the nodes that are connected to this AD domain.
Cache Distribution Group	Enter the Cache Distribution Group of the selected node. This accepts any text string to a maximum of 64 characters. The Cache Distribution Group does not allow the special characters “(” and “)”.

Step 3 Do one of the following:

- **Click Save Changes** to save the configuration.
- **Click Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that there are no policy rules that use custom conditions based on the AD dictionary**.**

Related Topics

- Advanced Tunning, page 8-77
- Configuring Authentication Domains, page 8-78
- Diagnose Active Directory Problems, page 8-78
- Active Directory Alarms and Reports, page 8-80

Advanced Tunning

The advanced tuning feature provides node-specific changes and settings to adjust the parameters deeper in the system. This page allows configuration of preferred Domain Controllers, Global Catalogs, Domain Controller failover parameters, and timeouts. This page also provide troubleshooting options like disable encryption. These settings are not intended for normal administration flow and should be used only under Cisco Support guidance.

Active Directory Identity Search Attributes

Cisco Secure ACS (from Release 5.8 patch 9 onwards) identifies users using any one or both of the following attributes:

- sAMAccountName(SAM)
- CommonName (CN)

The default is set to SAM.

Prior to ACS 5.8 patch 9, both the SAM and CN attributes were searched by default. You can now configure ACS to identify users using SAM, CN, or both, based on your requirements.

The following procedure describes how to change the identity search attribute in Active Directory. ACS identifies AD users using the SAM and CN values. You can configure ACS to identify AD users by searching either one of these attributes, or both.

Note If you choose to use SAM and CN, and the value of SAM is not unique, ACS also compares the CN value.

To configure attributes for Active Directory identity search:

Step 1 Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Advanced Tuning** tab.

Step 2 Enter the following values:

- Name—Enter the name of the registry key that you are configuring. To change the Active Directory search attribute, enter:
  REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField
- Value—Enter one of the following values that ACS uses to identify a user:
  - SAM—To use only SAM in the query (default)
  - CN—To use only CN in the query
  - SAMCN—To use both SAM and CN in the query
- Comment—Enter a description about the change that you are making. Here in this example, you can enter *Changing the default behavior to SAM and CN*.

Step 3 Click **Update Value** to update the value in the GUI.

Step 4 Click **Restart Active Directory Connector** to update the registry.

A pop-up message appears. Read the message and accept the change. The Active Directory Connector service in ACS restarts.

Related Topics

- Configuring Authentication Domains, page 8-78
- Diagnose Active Directory Problems, page 8-78
- Active Directory Alarms and Reports, page 8-80

Configuring Authentication Domains

If you join ACS to an Active Directory domain, ACS has visibilities to other domains with which it has a trust relationship. By default, ACS permits authentication against all those trusted domains. You can restrict ACS to a subset of authentication domains while interacting with the Active Directory deployments. Configuring authentication domains enables you to select specific domains so that the authentications are performed against the selected domains only. Authentication domains improve security because they instruct ACS to authenticate users only from selected domains and not from all domains trusted from join point. Authentication domains also improve performance and latency of authentication request processing because authentication domains limit the search area (that is, where accounts matching to incoming username or identity will be searched). It is especially important when incoming username or identity does not contain domain markup (prefix or suffix). Due to these reasons, configuring authentication domains is a best practice, and we highly recommended it.

To configure Authentication Domains:

Before you Begin

Ensure that the ACS instance is joined to an Active Directory domain.

Step 1 Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Authentication Domains** tab.

A table appears with a list of your trusted domains. By default, ACS permits authentication against all trusted domains.

Step 2 To allow only specified domains, check the check box next to the domains for which you want to allow authentication, and click **Enable Selected**.

Step 3 Click **Save Changes**.

In the **Authenticate** column, the status of the selected domains are changed to **Yes**.

Related Topics

- Diagnose Active Directory Problems, page 8-78
- Active Directory Alarms and Reports, page 8-80

Diagnose Active Directory Problems

The Diagnostic Tool is a service that runs on every ACS node. It allows you to automatically test and diagnose the Active Directory deployment and execute a set of tests to detect issues that may cause functionality or performance failures when ACS uses Active Directory.

There are multiple reasons for which ACS might be unable to join or authenticate against Active Directory. This tool helps ensure that the prerequisites for connecting ACS to Active Directory are configured correctly. It helps detect problems with networking, firewall configurations, clock sync, user authentication, and so on. This tool works as a step-by-step guide and helps you fix problems with every layer in the middle, if needed.

You can run the following three test without joining ACS to Active Directory to check if the Active Directory Daemon is running properly:

- System health - check AD service
- System health - check DNS configuration
- System health - check NTP

You can run the following available tests after joining ACS to Active Directory:

- DNS A record high level API query
- DNS A record low level API query
- DNS SRV record query
- DNS SRV record size
- LDAP test AD site association
- LDAP test DCs availability
- LDAP test DCs response time
- LDAP test - DC locator
- LDAP test - GC locator
- Kerberos test obtaining join point TGT
- Kerberos test bind and query to ROOT DSE
- Kerberos check SASL connectivity to AD

To diagnose Active Directory problems:

Step 1 Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Diagnostic Tools** tab.

The Diagnostic Tools tab displays the list of all available tests that you can run on ACS to check Active Directory domain functions.

Step 2 Check the check box or check boxes next to the tests that you want to run.

Step 3 Click:

- **Run Selected Tests** to run only the selected tests.
- **Run All Tests** to run all the tests.
- **Stop All Running Tests** to stop ACS from running all tests.

You can see the test results in **Result and Remedy** columns.

Related Topics

Active Directory Alarms and Reports, page 8-80

Active Directory Alarms and Reports

Alarms

ACS 5.8 introduced various alarms and reports to monitor and troubleshoot Active Directory related activities.

The following alarms are triggered for Active Directory errors and issues:

- Configured name server not available
- Joined domain is unavailable
- Authentication domain is unavailable
- Active Directory forest is unavailable
- AD Connector had to be restarted
- AD: ACS account password update failed
- AD: Machine TGT refresh failed

Reports

You can monitor Active Directory related activities through the following two reports:

- RADIUS Authentications Report—This report shows detailed steps of the Active Directory RADIUS authentication and authorization. You can find this report here: **Launch Monitoring and Report Viewer > Monitoring and Reports > Reports > ACS Reports > AAA Protocol > RADIUS Authentications**.
- TACACS+ Authentications Report—This report shows detailed steps of the Active Directory TACACS+ authentication and authorization. You can find this report here: **Launch Monitoring and Report Viewer > Monitoring and Reports > Reports > ACS Reports > AAA Protocol > TACACS Authentications**.
- AD Connector Operations Report—The AD Connector Operations report provides a log of background operations performed by AD connector, such as ACS server password refresh, Kerberos ticket management, DNS queries, DC discovery, LDAP, and RPC connections management. If you encounter any Active Directory failures, you can review the details in this report to identify the possible causes. You can find this report here: **Launch Monitoring and Report Viewer > Monitoring and Reports > Reports > ACS Reports > ACS Instance > AD Connector Operations**.

Note The first authentication of a user belongs to the large number of groups may fail with a timeout error. But, the subsequent authentications of the same user or another user belongs to the same group works properly.

Joining ACS to Domain Controllers

When ACS needs to connect to a domain controller or a global catalog, it sends SRV requests to the configured DNS servers to find out the available list of domain controllers for a domain and the global catalogs for a forest.

If the Active Directory configuration on ACS machine is assigned to a subnet, which in turn is assigned to a site, then ACS sends the DNS queries scoped to the site. That is the DNS server is supposed to return the domain controllers and the global catalogs serving that particular site to which the subnet is assigned to.

If the ACS machine is not assigned to a site, then ACS does not send the DNS queries scoped to the site. That is the DNS server is supposed to return all available domain controllers and global catalogs with no regard to the sites.

ACS iterates the available list of domain controllers or global catalogs and tries to establish the connection according to the order of the domain controllers or the global catalogs in the DNS response received from the DNS server.

Related Topics

- RSA SecurID Server, page 8-81
- RADIUS Identity Stores, page 8-87

RSA SecurID Server

ACS supports the RSA SecurID server as an external database. RSA SecurID two-factor authentication consists of the user's personal identification number (PIN) and an individually registered RSA SecurID token that generates single-use token codes based on a time code algorithm.

A different token code is generated at fixed intervals (usually each at 30 or 60 seconds). The RSA SecurID server validates this dynamic authentication code. Each RSA SecurID token is unique, and it is not possible to predict the value of a future token based on past tokens.

Thus when a correct token code is supplied together with a PIN, there is a high degree of certainty that the person is a valid user. Therefore, RSA SecurID servers provide a more reliable authentication mechanism than conventional reusable passwords.

You can integrate with RSA SecurID authentication technology in any one of the following ways:

- Using the RSA SecurID agent—Users are authenticated with username and passcode through the RSA's native protocol.
- Using the RADIUS protocol—Users are authenticated with username and passcode through the RADIUS protocol.

RSA SecurID token server in ACS 5.8 integrates with the RSA SecurID authentication technology by using the RSA SecurID Agent.

Configuring RSA SecurID Agents

The RSA SecurID Server administrator can do the following:

- Create an Agent Record (sdconf.rec), page 8-81
- Reset the Node Secret (SecurID), page 8-82
- Override Automatic Load Balancing, page 8-82
- Manually Intervene to Remove a Down RSA SecurID Server, page 8-82
- Passcode Caching, page 8-82

Create an Agent Record (sdconf.rec)

To configure an RSA SecurID token server in ACS 5.8, the ACS administrator requires the *sdconf.rec* file. The *sdconf.rec* file is a configuration record file that specifies how the RSA agent communicates with the RSA SecurID server realm.

In order to create the *sdconf.rec* file, the RSA SecurID server administrator should add the ACS host as an Agent host on the RSA SecurID server and generate a configuration file for this agent host.

Note The *sdconf.rec* file is unique in a deployment. However, Cisco Secure ACS replicates the *sdconf.rec* file from the primary server to the secondary server while joining the secondary server with the primary server.

Reset the Node Secret (SecurID)

After the agent initially communicates with the RSA SecurID server, the server provides the agent with a node secret file called SecurID. Subsequent communication between the server and the agent relies on exchanging the node secret to verify the other's authenticity.

At times, you might have to reset the node secret. To reset the node secret:

- The RSA SecurID server administrator must uncheck the Node Secret Created check box on the Agent Host record in the RSA SecurID server.
- The ACS administrator must remove the SecurID file from ACS.

Override Automatic Load Balancing

RSA SecurID Agent automatically balances the requested loads on the RSA SecurID servers in the realm. However, you do have the option to manually balance the load. You can specify which server each of the agent hosts must use and assign a priority to each server so that the agent host directs authentication requests to some servers more frequently than others.

You must specify the priority settings in a text file and save it as sdopts.rec, which you can then upload to ACS.

Manually Intervene to Remove a Down RSA SecurID Server

When an RSA SecurID server is down, the automatic exclusion mechanism does not always work quickly. To speed up this process, you can remove the *sdstatus.12* file from ACS.

Passcode Caching

Passcode caching enables the user to perform more than one authentication with an RSA SecurID server using the same passcode.

ACS 5.8 stores users with passcode in a cache. User and passcode are entered into the cache after successful authentication with the RSA SecurID server. Upon authentication with the RSA SecurID server, ACS tries first to search for the authenticating user and passcode in the cache. If not found, ACS authenticates with the RSA SecurID server.

The passcode cache in ACS is available for a configurable amount of time from 1 to 300 seconds. The RSA SecurID server passcode entry in the cache is available for the amount of time that you configure. Within this period of time, the user can access the internet with the same passcode.

Creating and Editing RSA SecurID Token Servers

ACS 5.8 supports RSA SecurID Token Servers for authenticating users for the increased security that one-time passwords provide. RSA SecurID token servers provide two-factor authentication to ensure the authenticity of users.

To authenticate users against an RSA identity store, you must first create an RSA SecurID Token Server in ACS and configure the realm, ACS instance, and advanced settings.

ACS 5.8 supports only one RSA realm. You can configure the settings for the RSA realm. A single realm can contain many ACS instances.

Note You must obtain the *sdconf.rec* file from the RSA SecurID server administrator and store it in ACS.

To create or edit an RSA SecurID token server:

Step 1 Choose **Users and Identity Stores > External Identity Stores > RSA SecurID Token Servers**.

The RSA SecurID Token Servers page appears.

Step 2 Click **Create**.

You can also click the identity store name that you want to modify, or check the box next to the name and click **Edit**.

Step 3 Complete the fields in the RSA Realm Settings tab as described in Table 8-21.

Table 8-21 RSA Realm Settings Tab

Option	Description
General	
Name	Name of the RSA realm.
Description	(Optional) The description of the RSA realm.
Server Connection	
Server Timeout *n* seconds	ACS waits for *n* seconds to connect to the RSA SecurID token server before timing out.
Reauthenticate on Change PIN	Check this check box to reauthenticate on change PIN.
Realm Configuration File	
Import new 'sdconf.rec' file	Click **Browse** to select the *sdconf.rec* file from your machine.
Node Secret Status	Once the user is first authenticated against RSA SecurID Token Server, the Node Secret Status is shown as *Created*.

Step 4 Click the ACS Instance Settings tab. See Configuring ACS Instance Settings, page 8-84 for more information.

Step 5 Click the Advanced tab. See Configuring Advanced Options, page 8-86 for more information.

Step 6 Click **Submit** to create an RSA SecurID store.

The RSA SecurID Token Server page appears with the configured servers.

Related Topics:

- RSA SecurID Server, page 8-81
- Configuring ACS Instance Settings, page 8-84

- Configuring Advanced Options, page 8-86

Configuring ACS Instance Settings

The ACS Instance Settings tab appears with the current list of ACS instances that are active in the system. You cannot add or delete these entries. However, you can edit the available RSA Realm settings for each of these ACS instances.

Table 8-22 describes the fields in the ACS Instance Settings tab.

Table 8-22 ACS Instance Settings Tab

Option	Description
ACS Instance	Name of the ACS instance.
Options File	Name of the options file.
Node Secret Status	Status of Node Secret. This can be one of the following: • Created • Not created

You can edit the settings of the ACS instances that are listed on this page. To do this:

Step 1 Check the check box next to the ACS instance that you want to edit and click **Edit**.

The ACS instance settings dialog box appears. This dialog box contains the following tabs:

- RSA Options File—See Editing ACS Instance Settings, page 8-84 for more information.
- Reset Agents Files—See Editing ACS Instance Settings, page 8-84 for more information.

Step 2 Click **OK.**

Related Topics

- RSA SecurID Server, page 8-81
- Creating and Editing RSA SecurID Token Servers, page 8-82
- Editing ACS Instance Settings, page 8-84
- Editing ACS Instance Settings, page 8-84
- Configuring Advanced Options, page 8-86

Editing ACS Instance Settings

You can edit the ACS instance settings to:

- Enable the RSA Options File, page 8-84
- Reset Agent Files, page 8-85

Enable the RSA Options File

You can enable the RSA options file (*sdopts.rec*) on each ACS instance to control routing priorities for connections between the RSA agent and the RSA servers in the realm.

Table 8-23 describes the fields in the RSA Options File tab.

Table 8-23 RSA Options File Tab

Option	Description
The RSA options file (sdopts.rec) may be enabled on each ACS instance to control the routing priorities for connections between the RSA agent and the RSA servers in the realm. For detailed description of the format of the sdopts.rec, please refer to the RSA Documentation.	
Use the Automatic Load Balancing status maintained by the RSA Agent	Choose this option to use the automatic load balancing status that the RSA agent maintains.
Override the Automatic Load Balancing status with the sdopts.rec file selected below	Choose this option to use the automatic load balancing status that is specified in the sdopts.rec file.
Current File	Lists the sdopts.rec file that is chosen currently.
Time stamp	Time when sdopts.rec file was last modified.
File Size	Size of the sdopts.rec file.
Import new 'sdopts.rec' file	Click **Browse** to import the new sdopts.rec file from your hard drive.
Note Changes will not take effect until the page which launched this popup is submitted.	

Do one of the following:

- Click **OK** to save the configuration.
- Click the **Reset Agent Files** tab to reset the secret key information or the status of active and inactive servers in the realm.

Related Topics

- RSA SecurID Server, page 8-81
- Creating and Editing RSA SecurID Token Servers, page 8-82
- Configuring ACS Instance Settings, page 8-84
- Editing ACS Instance Settings, page 8-84
- Configuring Advanced Options, page 8-86

Reset Agent Files

Use this page to reset the following:

- Node Secret key file, to ensure that communication with the RSA servers is encrypted.
- Status of the servers in the realm.

Step 1 Choose either of the following options:

- To reset node secret on the agent host, check the **Remove secure id file on submit** check box.

  If you reset the node secret on the agent host, you must reset the agent host's node secret in the RSA server.
- To reset the status of servers in the realm, check the **Remove sdstatus.12 file on submit** check box.

Step 2 Click **OK**.

Related Topics

- RSA SecurID Server, page 8-81
- Creating and Editing RSA SecurID Token Servers, page 8-82
- Configuring ACS Instance Settings, page 8-84
- Editing ACS Instance Settings, page 8-84
- Configuring Advanced Options, page 8-86

Configuring Advanced Options

Use this page to do the following:

- Define what an access reject from an RSA SecurID token server means to you.
- Enable identity caching—Caching users in RSA is similar to caching users in RADIUS token with the logic and the purpose of the caching being the same. The only difference is that in RSA there is no attribute retrieval for users and therefore no caching of attributes. The user who is authenticated is cached, but without any attributes.
- Enable passcode caching—This option stores the passcodes after the first successful authentication with an RSA secure ID token server and uses the cached user credentials for the subsequent authentications if they happens within the configured time period.

To configure advanced options for the RSA realm:

Step 1 Do one of the following:

- Click the **Treat Rejects as Authentication failed** radio button—ACS interprets this as an authentication reject from an RSA SecurdID store and consider this as an authentication failure.
- Click the **Treat Rejects as User not found** radio button—ACS interprets this as an authentication reject from an RSA SecurID store and consider this as "user not found."

Step 2 Check the **Enable identity caching** check box.

Enable identity caching to allow ACS to process requests that are not authenticated through the RSA server.

The results obtained from the last successful authentication are available in the cache for the specified time period.

Step 3 Enter the aging time in minutes.

The identity cache stores the results of a successful login only for the time period specified here. The default value is 120 minutes. The valid range is from 1 to 1440 minutes.

Step 4 Check the **Enable passcode caching** check box.

Enable passcode caching to allow ACS to cache the passcodes and allow users to access the network with the same passcode for the specified time period.

Step 5 Enter the aging time in seconds.

The passcode cache stores the results of a successful login only for the time period specified here. The default value is 30 seconds. The valid range is from 1 to 300 seconds.

Step 6 Check the **Treat authorization is passed for internal user with password type set to this identity source** check box, if you want ACS to pass the authorization for an unknown user if the user is found in the internal identity store and the password type is set to RSA SecurID token server. When this option is enabled, authorization is passed always even if the user is not authenticated by this node previously and there is no corresponding entry in cache.

Note We strongly recommend that you enable this option only when you are using a NAS (such as, Cisco 5508 Wireless controller) that sends authentication and authorization requests to different AAA servers in a high-availability setup. Otherwise, we recommend that you always disable this option.

In a high-availability configuration, sometimes NAS sends TACACS+ authentication and authorization requests to different AAA servers. NAS sends authentication request to a AAA server and at the same time, sends the authorization/accounting request for the same user to another AAA server that is configured in the Authentication/Authorization Servers list on NAS. In this case, authentication succeeds, but the authorization fails with "User record was not found in the cache" message.

The user details are cached during authentication because User Lookups are not supported by RSA SecurID servers. ACS caches results of successful authentications and will process User Lookup requests against the cache. The authorization fails when the request is sent to a different ACS server (where authentication was not performed), because the cache (local to a server) is not replicated among ACS nodes in the deployment and hence user details would not be available in that cache. In such cases, you can enable this option to prevent this issue.

Note This option is available from ACS 5.8 patch 7 or later.

Step 7 Click **Submit**.

Note ACS displays the "InvalidPassword" error message in ACS view for the following scenarios when you authenticate users and administrators against RSA Identity Server and RSA SecurID Server as an external identity source:
1) Invalid Password is entered
2) User is disabled in external identity store
3) User does not exists in the external identity store

Related Topics

- RSA SecurID Server, page 8-81
- Creating and Editing RSA SecurID Token Servers, page 8-82
- Configuring ACS Instance Settings, page 8-84
- Editing ACS Instance Settings, page 8-84
- Configuring Advanced Options, page 8-86

RADIUS Identity Stores

RADIUS server is a third-party server that supports the RADIUS interface. RADIUS identity store, which is part of ACS, connects to the RADIUS server.

RADIUS servers are servers that come with a standard RADIUS interface built into them and other servers that support the RADUIS interface. ACS 5.8 supports any RADIUS RFC 2865-compliant server as an external identity store. ACS 5.8 supports multiple RADIUS token server identities.

For example, the RSA SecurID server and SafeWord server. RADIUS identity stores can work with any RADIUS Token server that is used to authenticate the user. RADIUS identity stores use the UDP port for authentication sessions. The same UDP port is used for all RADIUS communication.

Note For ACS to successfully send RADIUS messages to a RADIUS-enabled server, you must ensure that the gateway devices between the RADIUS-enabled server and ACS allow communication over the UDP port. You can configure the UDP port through the ACS web interface.

This section contains the following topics:

Supported Authentication Protocols

ACS supports the following authentication protocols for RADIUS identity stores:

- RADIUS PAP
- TACACS+ ASCII/PAP
- PEAP with inner EAP-GTC
- EAP-FAST with inner EAP-GTC

Failover

ACS 5.8 allows you to configure multiple RADIUS identity stores. Each RADIUS identity store can have primary and secondary RADIUS servers. When ACS is unable to connect to the primary server, it uses the secondary server.

Password Prompt

RADIUS identity stores allow you to configure the password prompt. You can configure the password prompt through the ACS web interface.

User Group Mapping

To provide the per-user group mapping feature available in ACS 4.x, ACS 5.8 uses the attribute retrieval and authorization mechanism for users that are authenticated with a RADIUS identity store.

For this, you must configure the RADIUS identity store to return authentication responses that contain the [009\001] cisco-av-pair attribute with the following value:

ACS:CiscoSecure-Group-Id=*N*, where *N* can be any ACS group number from 0 through 499 that ACS assigns to the user.

Then, this attribute is available in the policy configuration pages of the ACS web interface while creating authorization and group mapping rules.

Groups and Attributes Mapping

You can use the RADIUS attributes retrieved during authentication against the RADIUS identity store in ACS policy conditions for authorization and group mapping. You can select the attributes that you want to use in policy conditions while configuring the RADIUS identity store. These attributes are kept in the RADIUS identity store dedicated dictionary and can be used to define policy conditions.

Note You cannot query the RADIUS server for the requested attributes. You can only configure the RADIUS identity store to return the requested attributes. These attributes are available in the Access-Accept response as part of the attributes list.

You can use the attribute subscription feature of ACS 5.8 to receive RADIUS identity store attributes can on the ACS response to the device. The following RADIUS attributes are returned:

- Attributes that are listed in the RADIUS RFS
- Vendor-specific attributes

The following attribute types are supported:

- String
- Unsigned Integer
- IP Address
- Enumeration

If an attribute with multiple values is returned, the value is ignored, and if a default value has been configured, that value is returned. However, this attribute is reported in the customer log as a problematic attribute.

RADIUS Identity Store in Identity Sequence

You can add the RADIUS identity store for authentication sequence in an identity sequence. However, you cannot add the RADIUS identity store for attribute retrieval sequence because you cannot query the RADIUS identity store without authentication. ACS cannot distinguish between different error cases while authenticating with a RADIUS server.

RADIUS servers return an Access-Reject message for all error cases. For example, when a user is not found in the RADIUS server, instead of returning a User Unknown status, the RADIUS server returns an Access-Reject message.

You can, however, enable the Treat Rejects as Authentication Failure or User Not Found option available in the RADIUS identity store pages of the ACS web interface.

Authentication Failure Messages

When a user is not found in the RADIUS server, the RADIUS server returns an Access-Reject message. ACS provides you the option to configure this message through the ACS web interface as either Authentication Failed or Unknown User.

However, this option returns an Unknown User message not only for cases where the user is not known, but for all failure cases.

Table 8-24 lists the different failure cases that are possible with RADIUS identity servers.

Table 8-24 Error Handling

Cause of Authentication Failure	Failure Cases
Authentication Failed	• User is unknown. • User attempts to login with wrong passcode. • User logon hours expired.
Process Failed	• RADIUS server is configured incorrectly in ACS. • RADIUS server is unavailable. • RADIUS packet is detected as malformed. • Problem during sending or receiving a packet from the RADIUS server. • Timeout.
Unknown User	Authentication failed and the 'Fail on Reject' option is set to false.

Username Special Format with Safeword Server

Safeword token server supports authentication with the following username format:

Username—Username, OTP

ACS parses the username and converts this to:

Username—Username

Safeword token servers support both the formats. ACS works with various token servers. While configuring a Safeword server, you must check the Safeword Server check box for ACS to parse the username and convert it to the specified format.

This conversion is done in the RADIUS token server identity store before the request is sent to the RADIUS token server.

User Attribute Cache

RADIUS token servers, by default, do not support user lookups. However, the user lookup functionality is essential for the following ACS features:

- PEAP session resume—Happens after successful authentication during EAP session establishment
- EAP/FAST fast reconnect—Happens after successful authentication during EAP session establishment

- T+ Authorization—Happens after successful T+ Authentication

ACS caches the results of successful authentications to process user lookup requests for these features. For every successful authentication, the name of the authenticated user and the retrieved attributes are cached. Failed authentications are not written to the cache.

The cache is available in the memory at runtime and is not replicated between ACS nodes in a distributed deployment. You can configure the time to live (TTL) limit for the cache through the ACS web interface. You must enable the identity caching option and set the aging time in minutes. The cache is available in the memory for the specified amount of time.

Passcode Caching

Passcode caching enables the user to perform more than one authentication with an RADIUS identity server using the same passcode.

ACS 5.8 stores users with passcode in a cache. User and passcode are entered into the cache after successful authentication with the RADIUS Identity Server. Upon authentication with the RADIUS identity server, ACS tries first to search for the authenticating user and passcode in the cache. If not found, ACS authenticates with the RADIUS identity server.

The passcode cache in ACS is available for a configurable amount of time from 1 to 300 seconds. The RADIUS identity server passcode entry in the cache is available for the amount of time that you configure. Within this period of time, the user can access the internet with the same passcode.

Creating, Duplicating, and Editing RADIUS Identity Servers

ACS 5.8 supports the RADIUS identity server as an external identity store for the increased security that one-time passwords provide. RADIUS identity servers provide two-factor authentication to ensure the authenticity of the users.

To authenticate users against a RADIUS identity store, you must first create the RADIUS identity server in ACS and configure the settings for the RADIUS identity store. ACS 5.8 supports the following authentication protocols:

- RADIUS PAP
- TACACS+ ASCII\PAP
- PEAP with inner EAP-GTC
- EAP-FAST with inner EAP-GTC

For a successful authentication with a RADIUS identity server, ensure that:

- The gateway devices between the RADIUS identity server and ACS allow communication over the UDP port.
- The shared secret that you configure for the RADIUS identity server on the ACS web interface is identical to the shared secret configured on the RADIUS identity server.

To create, duplicate, or edit a RADIUS Identity Server:

Step 1 Choose **Users and Identity Stores > External Identity Stores > RADIUS Identity Servers**.

The RADIUS Identity Servers page appears with a list of RADIUS external identity servers.

Step 2 Click **Create**. You can also:

- Check the check box next to the identity store you want to duplicate, then click **Duplicate**.

- Click the identity store name that you want to modify, or check the box next to the name and click **Edit**.

Step 3 Complete the fields in the General tab. See Configuring General Settings, page 8-92 for a description of the fields in the General tab.

Step 4 You can:

- Click **Submit** to save the RADIUS Identity Server.
- Click the Shell Prompts tab. See Configuring Shell Prompts, page 8-94 for a description of the fields in the Shell Prompts tab.
- Click the Directory Attributes tab. See Configuring Directory Attributes, page 8-94 for a description of the fields in the Directory Attributes tab.
- Click the Advanced tab. See Configuring Advanced Options, page 8-95 for a description of the fields in the Advanced tab.

Step 5 Click **Submit** to save the changes.

Related Topics

- RADIUS Identity Stores, page 8-87
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-91

Configuring General Settings

Table 8-25 describes the fields in the General tab of the RADIUS Identity Servers page.

Table 8-25 RADIUS Identity Server - General Tab

Option	Description
Name	Name of the external RADIUS identity server.
Description	(Optional) A brief description of the RADIUS identity server.
SafeWord Server	Check this check box to enable a two-factor authentication using a SafeWord server.
Server Connection	
Enable Secondary Server	Check this check box to use a secondary RADIUS identity server as a backup server in case the primary RADIUS identity server fails. If you enable the secondary server, you must configure the parameters for the secondary RADIUS identity server and must choose one of the following options: • Always Access Primary Server First—Select this option to ensure that ACS always accesses the primary RADIUS identity server first before the secondary server is accessed. • Failback To Primary Server After *n* Minutes—Select this option to set the number of minutes ACS can use the secondary server for authentication. After this time expires, ACS should again attempt to authenticate using the primary server. The default value is 5 minutes.
Primary Server	

Table 8-25 RADIUS Identity Server - General Tab (continued)

Option	Description
Server IP Address	IP address of the primary RADIUS identity server.
Shared Secret	Shared secret between ACS and the primary RADIUS identity server. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Authentication Port	Port number on which the RADIUS primary server listens. Valid options are from 1 to 65,535. The default value is 1812.
Server Timeout *n* Seconds	Number of seconds, *n*, that ACS waits for a response from the primary RADIUS identity server before it determines that the connection to the primary server has failed. Valid options are from 1 to 300. The default value is 5.
Connection Attempts	Specifies the number of times that ACS should attempt to reconnect before contacting the secondary RADIUS identity server or dropping the connection if no secondary server is configured. Valid options are from 1 to 10. The default value is 3.
Secondary Server	
Server IP Address	IP address of the secondary RADIUS identity server.
Shared Secret	Shared secret between ACS and the secondary RADIUS identity server. The shared secret must be identical to the shared secret that is configured on the RADIUS identity server. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Authentication Port	Port number on which the RADIUS secondary server listens. Valid options are from 1 to 65,535. The default value is 1812.
Server Timeout *n* Seconds	Number of seconds, *n*, that ACS waits for a response from the secondary RADIUS identity server before it determines that the connection to the secondary server has failed. Valid options are from 1 to 300. The default value is 5.
Connection Attempts	Specifies the number of times that ACS should attempt to reconnect before dropping the request. Valid options are from 1 to 10. The default value is 3.

Related Topics

- RADIUS Identity Stores, page 8-87
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-91
- Configuring Shell Prompts, page 8-94
- Configuring Directory Attributes, page 8-94
- Configuring Advanced Options, page 8-95

Configuring Shell Prompts

For TACACS+ ASCII authentication, ACS must return the password prompt to the user. RADIUS identity server supports this functionality by the password prompt option. ACS can use the prompt that you configure in the Shell Prompts page on the ACS web interface. If the prompt is empty, the user receives the default prompt that is configured under TACACS+ global settings.

When establishing a connection with a RADIUS identity server, the initial request packets may not have the password. You must request a password. You can use this page to define the prompt that is used to request the password. To do this:

Step 1 Enter the text for the prompt in the Prompt field.

Step 2 Do one of the following:

- Click **Submit** to configure the prompt for requesting the password.
- Click the Directory Attributes tab to define a list of attributes that you want to use in policy rule conditions. See Configuring Directory Attributes, page 8-94 for more information.

Related Topics

- RADIUS Identity Stores, page 8-87
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-91
- Configuring General Settings, page 8-92
- Configuring Directory Attributes, page 8-94
- Configuring Advanced Options, page 8-95

Configuring Directory Attributes

When a RADIUS identity server responds to a request, RADIUS attributes are returned along with the response. You can make use of these RADIUS attributes in policy rules.

In the Directory Attributes tab, you can specify the RADIUS attributes that you use in policy rule conditions. ACS maintains a separate list of these attributes.

Step 1 Modify the fields in the Directory Attributes tab as described in Table 8-26.

Table 8-26 RADIUS Identity Servers - Directory Attributes Tab

Option	Description
Attribute List	Use this section to create the attracted list to include in policy conditions. As you include each attribute, its name, type, default value, and policy condition name appear in the table. To: • Add a RADIUS attribute, fill in the fields below the table and click **Add**. • Edit a RADIUS attribute, select the appropriate row in the table and click **Edit**. The RADIUS attribute parameters appear in the fields below the table. Edit as required, then click **Replace**.
Dictionary Type	RADIUS dictionary type. Click the drop-down list box to select a RADIUS dictionary type.

Table 8-26 RADIUS Identity Servers - Directory Attributes Tab

Option	Description
RADIUS Attribute	Name of the RADIUS attribute. Click **Select** to choose the RADIUS attribute. This name is composed of two parts: The attribute name and an extension to support AV-pairs if the attribute selected is a Cisco AV-Pair. For example, for an attribute, **cisco-av-pair** with an AV-pair name **some-avpair**, ACS displays **cisco-av-pair.some-avpair**. IETF and vendor VSA attribute names contain an optional suffix, *-nnn*, where *nnn* is the ID of the attribute.
Type	RADIUS attribute type. Valid options are: • String • Unsigned Integer 32 • IPv4 address
Default	(Optional) A default value that can be used if the attribute is not available in the response from the RADIUS identity server. This value must be of the specified RADIUS attribute type.
Policy Condition Name	Specify the name of the custom policy condition that uses this attribute.

Step 2 Do either of the following:

- Click **Submit** to save your changes and return to the RADIUS Identity Servers page.
- Click the Advanced tab to configure failure message handling and to enable identity caching. See Configuring Advanced Options, page 8-95 for more information.

Related Topics

- RADIUS Identity Stores, page 8-87
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-91
- Configuring General Settings, page 8-92
- Configuring Shell Prompts, page 8-94
- Configuring Advanced Options, page 8-95

Configuring Advanced Options

In the Advanced tab, you can do the following:

- Define what an access reject from a RADIUS identity server means to you.
- Enable identity caching.
- Enable passcode caching.

Table 8-27 describes the fields in the Advanced tab of the RADIUS Identity Servers page.

Table 8-27 RADIUS Identity Servers — Advanced Tab

Option	Description
This Identity Store does not differentiate between 'authentication failed' and 'user not found' when an authentication attempt is rejected. From the options below, select how such an authentication reject from the Identity Store should be interpreted by ACS for Identity Policy processing and reporting.	
Treat Rejects as 'authentication failed'	Click this option to consider all ambiguous access reject attempts as failed authentications.
Treat Rejects as 'user not found'	Click this option to consider all ambiguous access reject attempts as unknown users.
Identity caching is used to allow processing of requests that do not perform authentication against the server. The cache retains the results and attributes retrieved from the last successful authentication for the subject.	
Enable identity caching	Check this check box to enable identity caching. If you enable identity caching, you must enter the time in minutes for which you want ACS to retain the identity cache.
Aging Time *n* Minutes	Enter the time in minutes for which you want ACS to retain the identity cache. Valid options are from 1 to 1440.
Enable passcode caching	Check this check box to enable passcode caching. If you enable passcode caching, you must enter the time in seconds for which you want ACS to retain the passcode cache.

Table 8-27 RADIUS Identity Servers — Advanced Tab (continued)

Option	Description
Aging Time *n* Seconds	Enter the time in seconds for which you want ACS to retain the passcode cache. Valid options are from 1 to 300. The default value is 30 seconds.
Treat authorization is passed for internal user with password type set to this identity source	**Note** This option is available from ACS 5.8 patch 7 or later. Check this check box if you want ACS to pass the authorization for an unknown user if the user is found in the internal identity store and the password type is set to RADIUS identity server. When this option is enabled, authorization is passed always even if the user is not authenticated by this node previously and there is no corresponding entry in cache. **Note** Note: We strongly recommend that you enable this option only when you are using a NAS (such as, Cisco 5508 Wireless controller) that sends authentication and authorization requests to different AAA servers in a high-availability setup. Otherwise, we recommend that you always disable this option. In a high-availability configuration, sometimes NAS sends TACACS+ authentication and authorization requests to different AAA servers. NAS sends authentication request to a AAA server and at the same time, sends the authorization/accounting request for the same user to another AAA server that is configured in the Authentication/Authorization Servers list on NAS. In this case, authentication succeeds, but the authorization fails with "User record was not found in the cache" message. The user details are cached during authentication because User Lookups are not supported by RSA SecurID servers. ACS caches results of successful authentications and will process User Lookup requests against the cache. The authorization fails when the request is sent to a different ACS server (where authentication was not performed), because the cache (local to a server) is not replicated among ACS nodes in the deployment and hence user details would not be available in that cache. In such cases, you can enable this option to prevent this issue.

Click **Submit** to save the RADIUS Identity Server.

Related Topics

- RADIUS Identity Stores, page 8-87
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-91

Configuring CA Certificates

When a client uses the EAP-TLS protocol to authenticate itself against the ACS server, it sends a client certificate that identifies itself to the server. To verify the identity and correctness of the client certificate, the server must have a preinstalled certificate from the Certificate Authority (CA) that has digitally signed the client certificate.

If ACS does not trust the client's CA certificate, then you must install in ACS the entire chain of successively signed CA certificates, all the way to the top-level CA certificate that ACS trusts. CA certificates are also known as trust certificates.

You use the CA options to install digital certificates to support EAP-TLS authentication. ACS uses the X.509 v3 digital certificate standard. ACS also supports manual certificate acquisition and provides the means for managing a certificate trust list (CTL) and certificate revocation lists (CRLs).

Digital certificates do not require the sharing of secrets or stored database credentials. They can be scaled and trusted over large deployments. If managed properly, they can serve as a method of authentication that is stronger and more secure than shared secret systems.

Mutual trust requires that ACS have an installed certificate that can be verified by end-user clients. This server certificate may be issued from a CA or, if you choose, may be a self-signed certificate. For more information, see Configuring Local Server Certificates, page 18-16.

Note ACS builds a certificate chain with the CA certificates that you add to it and uses this chain during TLS negotiations. You must add the certificate that signed the server certificate to the CA. You must ensure that the chain is signed correctly and that all the certificates are valid.

If the server certificate and the CA that signed the server certificate are installed on ACS, ACS sends the full certificate chain to the client.

Note ACS does not support wildcard certificates.

Related Topics

- Adding a Certificate Authority, page 8-98
- Editing a Certificate Authority and Configuring Certificate Revocation Lists, page 8-99
- Deleting a Certificate Authority, page 8-101
- Renewing or Deleting a CA Certificate that is part of a Certificate Chain, page 8-102
- Exporting a Certificate Authority, page 8-103

Adding a Certificate Authority

The supported certificate formats are DER, PEM, or CER.

To add a trusted CA (Certificate Authority) certificate:

Step 1 Choose **Users and Identity Stores > Certificate Authorities**.

The Trust Certificate page appears.

Step 2 Click **Add**.

Step 3 Complete the fields in the Certificate File to Import page as described in Table 8-28:

Table 8-28 Certificate Authority Properties Page

Option	Description
Certificate File to Import	
Certificate File	Enter the name of the certificate file. Click **Browse** to navigate to the location on the client machine where the trust certificate is located.
Trust for client with EAP-TLS	Check this box so that ACS will use the certificate trust list for the EAP protocol.
Allow Duplicate Certificates	Allows you to add certificates with the same CN and SKI with different Valid From, Valid To, and Serial numbers.
Description	Enter a description of the CA certificate.

Step 4 Click **Submit**.

The new certificate is saved. The Trust Certificate List page appears with the new certificate.

Related Topics

- User Certificate Authentication, page C-6
- Overview of EAP-TLS, page C-6

Editing a Certificate Authority and Configuring Certificate Revocation Lists

Use this page to edit a trusted CA (Certificate Authority) certificate.

Step 1 Choose **Users and Identity Stores > Certificate Authorities.**

The Trust Certificate page appears with a list of configured certificates.

Step 2 Click the name that you want to modify, or check the check box for the Name, and click **Edit**.

Complete the fields in the Edit Trust Certificate List Properties Page as described in Table 8-29:

When ACS delays the CA CRL, the CA is retained on the local file system. The CA is not refreshed until you resubmit it.

By default ACS will fail all user certificates of a CA for which the CRL has expired.

- If the CA certificate is resubmitted, the following error is shown: `12514 EAP-TLS failed SSL/TLS handshake.` This is because of the unknown CA.
- If the CA certificate is not resubmitted, the following error is shown: `12515 EAP-TLS failed SSL/TLS handshake.`This is because of the expired CRL.

If you choose Ignore CRL Expiration, ACS fails authentication for the revoked certificates and passes the authentication for non-revoked certificates.

Table 8-29 Edit Certificate Authority Properties Page

Option	Description
Issuer	
Friendly Name	The name that is associated with the certificate.

Table 8-29 Edit Certificate Authority Properties Page (continued)

Option	Description
Description	(Optional) A brief description of the CA certificate.
Issued To	*Display only.* The entity to which the certificate is issued. The name that appears is from the certificate subject.
Issued By	*Display only.* The certification authority that issued the certificate.
Valid from	*Display only.* The start date of the certificate's validity. An X509 certificate is valid only from the start date to the end date (inclusive).
Valid To (Expiration)	*Display only.* The last date of the certificate's validity.
Serial Number	*Display only.* The serial number of the certificate.
Description	Description of the certificate.
Usage	
Trust for client with EAP-TLS	Check this box so that ACS will use the trust list for the TLS-related EAP protocols.
Certificate Status Validation	
OCSP Configuration	
Use this section to configure the OCSP service.	
Validate against OCSP service	Check this box and select the OCSP service from the drop-down list to validate the requests against the selected the OCSP service.
Reject the request if certificate status could not be determined by OCSP	Check this box to reject the request if the certificate status could not be determined by the OCSP service.
Certificate Revocation List Configuration	
Use this section to configure the CRL.	
Download CRL	Check this box to download the CRL.
CRL Distribution URL	Enter the CRL distribution URL. You can specify a URL that uses an HTTP or secure HTTPS connection. When you use a HTTPS URL, you must install the corresponding HTTPS server's CA certificate in ACS. You can configure a proxy server in ACS for CRL download so that ACS communicates with the CRL distribution server through the configured proxy server. For more information, see Configuring HTTP Proxy Settings for CRL Requests, page 18-4.
Retrieve CRL	ACS attempts to download a CRL from the CA. Toggle the time settings for ACS to retrieve a new CRL from the CA. • Automatically—Obtain the next update time from the CRL file. If unsuccessful, ACS tries to retrieve the CRL periodically after the first failure until it succeeds. • Every—Determines the frequency between retrieval attempts. Enter the amount in units of time.
If Download Failed Wait	Enter the amount of time to attempt to retrieve the CRL, if the retrieval initially failed.

Table 8-29 Edit Certificate Authority Properties Page (continued)

Option	Description
Bypass CRL Verification if CRL is not Received	If unchecked, all the client requests that use the certificate that is signed by the selected CA will be rejected until ACS receives the CRL file. When checked, the client request may be accepted before the CRL is received.
Ignore CRL Expiration	Check this box to check a certificate against an outdated CRL. • When checked, ACS continues to use the expired CRL and permits or rejects EAP-TLS authentications according to the contents of the CRL. • When unchecked, ACS examines the expiration date of the CRL in the Next Update field in the CRL file. If the CRL has expired, all authentications that use the certificate that is signed by the selected CA are rejected.

Step 3 Click **Submit**.

The Trust Certificate page appears with the edited certificate.

The administrator has the rights to configure CRL and OCSP verification. If both CRL and OCSP verification are configured at the same time, then ACS performs OCSP verification first. If it detects any communication problems with either the primary or secondary servers, or if the verification returns the status of a given certificate as unknown, then ACS moves on to perform the CRL validation.

Related Topics

- User Certificate Authentication, page C-6
- Overview of EAP-TLS, page C-6
- Configuring HTTP Proxy Settings for CRL Requests, page 18-4

Deleting a Certificate Authority

Use this page to delete a trusted CA (Certificate Authority) certificate:

Step 1 Choose **Users and Identity Stores > Certificate Authorities**.

The Trust Certificate List page appears with a list of configured certificates.

Step 2 Check one or more check boxes next to the certificates that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** to confirm.

The Trust Certificate page appears without the deleted certificate(s).

Related Topic

- Overview of EAP-TLS, page C-6

Renewing or Deleting a CA Certificate that is part of a Certificate Chain

When you try to delete a CA certificate which is part of a Certificate Chain, ACS displays the following error:

```
This System Failure occurred: Certificate Authority is in use by one of the ACS nodes
certificates. Your changes have not been saved. Click OK to return to the list page.
```

If you want to delete or renew a CA certificate which is part of EAP or management certificate chain, we must map or unbind the EAP or management protocols to another server certificate that is not issued by the CA certificate and then renew or delete it.

To renew or delete a CA certificate from ACS:

Step 1 Choose **System Administration > Configuration > Local Server Certificates > Local Certificates**.

Step 2 Check for the below conditions:

- If any of the server certificate listed are issued by the CA certificate that you want to renew or delete, you must check if EAP or management protocol is applied to the server certificates.
- If any of the server certificate issued by the CA certificate is mapped with EAP or management protocol, you must unbind the EAP or management protocol from the server certificate and map it to another server certificate that is not issued by the same CA certificate. For more information on unbinding EAP or management protocols from server certificate, see Unbinding EAP or Management Protocols from Server Certificate, page 8-102.

Step 3 You can renew or delete the CA certificate if none of the server certificate issued by this CA certificate is mapped with EAP or management protocol.

Unbinding EAP or Management Protocols from Server Certificate

To unbind EAP or management protocol from a server certificate:

Step 1 Install a new server certificate that is issued by a CA certificate other than the certificate that you want to delete or you can consider the default server certificate. For more information, see Adding Local Server Certificates, page 18-17.

Step 2 Perform one of the following action:

- Check the **EAP: Used for EAP protocols that use SSL/TLS tunneling** and **Management Interface: Used to authenticate the web server (GUI)** check boxes while adding the new server certificate.
- After adding the new server certificate, you can edit the certificate and check the **EAP: Used for EAP protocols that use SSL/TLS tunneling** and **Management Interface: Used to authenticate the web server (GUI)** check boxes.

This operation unbinds the EAP or management protocols from the old server certificate and binds it with the new server certificate.

Exporting a Certificate Authority

To export a trust certificate:

Step 1 Choose **Users and Identity Stores > Certificate Authorities**.

The Trust Certificate List page appears with a list of configured certificates.

Step 2 Check the box next to the certificates that you want to export.

Step 3 Click **Export**.

This operation exports the trusted certificate to the client machine.

Step 4 Click **Yes** to confirm.

You are prompted to install the exported certificate on your client machine.

Related Topics

- User Certificate Authentication, page C-6
- Overview of EAP-TLS, page C-6

Configuring Certificate Authentication Profiles

The certificate authentication profile defines the X509 certificate information to be used for a certificate-based access request. You can select an attribute from the certificate to be used as the username.

You can select a subset of the certificate attributes to populate the username field for the context of the request. The username is then used to identify the user for the remainder of the request, including the identification used in the logs.

You can use the certificate authentication profile to retrieve certificate data to further validate a certificate presented by an LDAP or AD client. The username from the certificate authentication profile is used to query the LDAP or AD identity store.

ACS compares the client certificate against all certificates retrieved from the LDAP or AD identity store, one after another, to see if one of them matches. ACS either accepts or rejects the request.

Note For ACS to accept a request, only one certificate from either the LDAP or the AD identity store must match the client certificate.

When ACS processes a certificate-based request for authentication, one of two things happens: the username from the certificate is compared to the username in ACS that is processing the request, or ACS uses the information that is defined in the selected LDAP or AD identity store to validate the certificate information.

You can duplicate a certificate authentication profile to create a new profile that is the same, or similar to, an existing certificate authentication profile. After duplication is complete, you access each profile (original and duplicated) separately, to edit or delete them.

ACS 5.8 now supports certificate name constraint extension. It accepts the client certificates whose issuers contain the name constraint extension. It checks the client certificates for CA and sub-CA certificates. This extension defines a name space for all subject names in the subsequent certificates in

a certificate path. It applies to both the subject distinguished name and the subject alternative name. These restrictions are applicable only when the specified name form is present in the client certificate. The ACS authentication fails if the client certificate is excluded or not permitted by the namespace.

Supported Name Constraints:

- Directory name
- DNS
- Email
- URL

Unsupported Name Constraints:

- IP address
- Other name

To create, duplicate, or edit a certificate authentication profile, complete the following steps:

Step 1 Choose **Users and Identity Stores > Certificate Authentication Profile**.

The Certificate Authentication Profile page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the certificate authentication profile that you want to duplicate, then click **Duplicate**.
- Click the certificate authentication profile that you want to modify, or check the check box next to the name and click **Edit**.

  The Certificate Authentication Profile Properties page appears.

Step 3 Complete the fields in the Certificate Authentication Profile Properties page as described in Table 8-30:

Table 8-30 Certificate Authentication Profile Properties Page

Option	Description
General	
Name	Enter the name of the certificate authentication profile.
Description	Enter a description of the certificate authentication profile.
Certificate Definition	

Table 8-30 Certificate Authentication Profile Properties Page (continued)

Option	Description
Principal Username X509 Attribute	Available set of principal username attributes for x509 authentication. The selection includes: • Common Name • Subject Alternative Name • Subject Serial Number • Subject • Subject Alternative Name - Other Name • Subject Alternative Name - EMail • Subject Alternative Name - DNS
Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory	Check this check box if you want to validate certificate information for authentication against a selected LDAP or AD identity store. If you select this option, you must enter the name of the LDAP or AD identity store, or click **Select** to select the LDAP or AD identity store from the available list.

Step 4 Click **Submit.**

The Certificate Authentication Profile page reappears.

Related Topics

- Viewing Identity Policies, page 10-23
- Configuring Identity Store Sequences, page 8-105
- Creating External LDAP Identity Stores, page 8-34

Configuring Identity Store Sequences

An access service identity policy determines the identity sources that ACS uses for authentication and attribute retrieval. An identity source consists of a single identity store or multiple identity methods. When you use multiple identity methods, you must first define them in an identity store sequence, and then specify the identity store sequence in the identity policy.

An identity store sequence defines the sequence that is used for authentication and attribute retrieval and an optional additional sequence to retrieve additional attributes.

Authentication Sequence

An identity store sequence can contain a definition for certificate-based authentication or password-based authentication or both.

- If you select to perform authentication based on a certificate, you specify a single Certificate Authentication Profile, which you have already defined in ACS.
- If you select to perform authentication based on a password, you can define a list of databases to be accessed in sequence.

When authentication succeeds, any defined attributes within the database are retrieved. You must have defined the databases in ACS.

Attribute Retrieval Sequence

You can optionally define a list of databases from which to retrieve additional attributes. These databases can be accessed regardless of whether you use password or certificate-based authentication. When you use certificate-based authentication, ACS populates the username field from a certificate attribute and then uses the username to retrieve attributes.

ACS can retrieve attributes for a user, even when:

- The user's password is flagged for a mandatory change.
- The user's account is disabled.

When you perform password-based authentication, you can define the same identity database in the authentication list and the attribute retrieval list. However, if the database is used for authentication, it will not be accessed again as part of the attribute retrieval flow.

ACS authenticates a user or host in an identity store only when there is a single match for that user or host. If an external database contains multiple instances of the same user, authentication fails. Similarly, ACS retrieves attributes only when a single match for the user or host exists; otherwise, ACS skips attribute retrieval from that database.

This section contains the following topics:

- Creating, Duplicating, and Editing Identity Store Sequences, page 8-106
- Deleting Identity Store Sequences, page 8-108

Creating, Duplicating, and Editing Identity Store Sequences

To create, duplicate, or edit an identity store sequence:

Step 1 Choose **Users and Identity Stores > Identity Store Sequences**.

The Identity Store Sequences page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the sequence that you want to duplicate, then click **Duplicate**.
- Click the sequence name that you want to modify, or check the check box next to the name and click **Edit**.

The Identity Store Sequence Properties page appears as described in Table 8-31.

Table 8-31 Identity Store Sequence Properties Page

Option	Description
General	
Name	Enter the name of the identity store sequence.
Description	Enter a description of the identity store sequence.
Authentication Method List	
Certificate Based	Check this check box to use the certificate-based authentication method. If you choose this option, you must enter the certificate authentication profile. Click **Select** to choose the profile from a list of available profiles.

Table 8-31 Identity Store Sequence Properties Page (continued)

Option	Description
Password Based	Check this check box to use the password-based authentication method. If you choose this option, you must choose the set of identity stores that ACS will access one after another until a match is found. If you choose this option, you must select a list of identity stores in the Authentication and Attribute Retrieval Search List area for ACS to access the identity stores one after another.
Authentication and Attribute Retrieval Search List	
Note This section appears only when you check the Password Based option.	
Available	Available set of identity stores to access.
Selected	Selected set of identity stores to access in sequence until first authentication succeeds. Use the Up and Down arrows at the right of the list to define the order of access. ACS automatically retrieves attributes from identity stores that you selected for authentication. You do not need to select the same identity stores for attribute retrieval.
Additional Attribute Retrieval Search List	
Available	Available set of additional identity stores for attribute retrieval.
Selected	(Optional) The selected set of additional identity stores for attribute retrieval. Use the Up and Down arrows at the right of the list to define the order of access. ACS automatically retrieves attributes from identity stores that you selected for authentication. You do not need to select the same identity stores for attribute retrieval.
Internal User/Host	
If internal user/host is not found or disabled then exit the sequence and treat as User Not Found	This option is applicable for the attribute phase and when the Internal Identity Store is in the Attribute retrieval list. ACS exists the sequence and treats it as User Not Found if this option is selected and the user not found or is disabled.
Advanced Options	
Break sequence	If this option is selected and if an authentication attempt against current Identity Store results in process error, the flow breaks the Identity Stores sequence. The flow then continues to the Fail-Open option configured in the Identity Policy. The same applies to attribute retrieval.
Continue to next identity store in the sequence	If this is checked and if authentication with the current Identity Store results in a process error, the flow tries to authenticate it with the next Identity Store in the authentication list. The same applies to attribute retrieval phase.

Step 3 Click **Submit**.

The Identity Store Sequences page reappears.

Related Topics

- Performing Bulk Operations for Network Resources and Users, page 7-8
- Viewing Identity Policies, page 10-23
- Managing Internal Identity Stores, page 8-4

- Managing External Identity Stores, page 8-29
- Configuring Certificate Authentication Profiles, page 8-103
- Deleting Identity Store Sequences, page 8-108

Deleting Identity Store Sequences

To delete an identity store sequence:

Step 1 Choose **Users and Identity Stores > Identity Store Sequences**.

The Identity Store Sequences page appears with a list of your configured identity store sequences.

Step 2 Check one or more check boxes next to the identity store sequences that you want to delete.

Step 3 Click **Delete**.

The following error message appears:

```
Are you sure you want to delete the selected item/items?
```

Step 4 Click **OK**.

The Identity Store Sequences page appears, without the deleted identity store sequence(s) listed.

Related Topics

- Performing Bulk Operations for Network Resources and Users, page 7-8
- Viewing Identity Policies, page 10-23
- Managing Internal Identity Stores, page 8-4
- Managing External Identity Stores, page 8-29
- Configuring Certificate Authentication Profiles, page 8-103
- Creating, Duplicating, and Editing Identity Store Sequences, page 8-106