



User Group Mapping and Specification

This chapter provides information about group mapping and specification. The the Cisco Secure Access Control Server Release 4.0 Solution Engine, hereafter referred to as ACS, uses these features to assign users who are authenticated by an external user database to a single ACS group.

This chapter contains the following topics:

- [About User Group Mapping and Specification, page 17-1](#)
- [Group Mapping by External User Database, page 17-1](#)
- [Group Mapping by Group Set Membership, page 17-3](#)
- [RADIUS-Based Group Specification, page 17-8](#)

About User Group Mapping and Specification

You can use the Database Group Mapping feature in the External User Databases section to associate unknown users with an ACS group for the purpose of assigning authorization profiles. For external user databases from which ACS can derive group information, you can associate the group memberships, which are defined for the users in the external user database, to specific ACS groups. For Windows user databases, group mapping is further specified by domain; because each domain maintains its own user database.

In addition to the Database Group Mapping feature, for some database types, ACS supports Remote Access Dial-In User Service (RADIUS)-based group specification.

Group Mapping by External User Database

You can map an external database to a ACS group. Unknown users who authenticate by using the specified database automatically belong to, and inherit the authorizations of, the group. For example, you could configure ACS so that all unknown users who authenticate with a certain token server database belong to a group called Telecommuters. You could then assign a group setup that is appropriate for users who are working away from home, such as `MaxSessions=1`. Or, you could configure restricted hours for other groups; but give unrestricted access to Telecommuters group members.

While you can configure ACS to map all unknown users in any external user database type to a single ACS group, the following external user database types are the external user database types whose users you can only map to a single ACS group:

- Open Database Connectivity (ODBC)
- Lightweight and Efficient Application Protocol (LEAP) Proxy RADIUS server
- Remote Access Dial-In User Service (RADIUS) token server
- Rivest, Shamir, and Adelman (RSA) SecurID token server

For a subset of the external user database types that were previously listed, group mapping by external database type is overridden on a user-by-user basis when the external user database specifies an ACS group with its authentication response. ACS supports specification of group membership for the following external user database types:

- LEAP Proxy RADIUS server.
- RADIUS token server.

For more information about specifying group membership for users who are authenticated with one of these database types, see [RADIUS-Based Group Specification, page 17-8](#).

Creating an ACS Group Mapping for a Token Server, ODBC Database, or LEAP Proxy RADIUS Server Database

To set or change a token server, ODBC, or LEAP Proxy RADIUS Server database group mapping:

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Group Mappings**.
- Step 3** Click the name of the token server, LEAP Proxy RADIUS Server, or ODBC database configuration for which you want to configure a group mapping.
- The Define Group Mapping table appears.
- Step 4** From the Select a default group for *database* list, click the group to which users who were authenticated with this database should be assigned.



Tip The Select a default group for *database* list displays the number of users who are assigned to each group.

- Step 5** Click **Submit**.

ACS assigns unknown and discovered users who are authenticated by the external database type that you selected in Step 3 to the ACS group that is selected in Step 4. For users who are authenticated by an ODBC, RADIUS token server, or LEAP Proxy RADIUS Server database, the mapping is only applied as a default if those databases did not specify an ACS group for the user.



Note For more information about group specification for RADIUS token servers, see [RADIUS-Based Group Specification, page 17-8](#).

Group Mapping by Group Set Membership

You can create group mappings for some external user databases based on the combination of external user database groups to which users belong. The following database types are the external user database types for which you can create group mappings based on group set membership:

- Windows domains.



Note Group mapping for Windows authentication supports only those users who belong to no more than 500 Windows groups.

- Generic Lightweight Directory Access Protocol (LDAP).

When you configure an ACS group mapping based on group set membership, you can add one or many external user database groups to the set. For ACS to map a user to the specified ACS group, the user must match *all* external user database groups in the set.

As an example, you could configure a group mapping for users who belong to the Engineering and Tokyo groups and a separate one for users who belong to Engineering and London. You could then configure separate group mappings for the combinations of Engineering-Tokyo and Engineering-London, and configure different access times for the ACS groups to which they map. You could also configure a group mapping that only included the Engineering group that would map other members of the Engineering group who were not members of Tokyo or London.

Group Mapping Order

ACS always maps users to a single ACS group; yet a user can belong to more than one group set mapping. For example, a user named *John* could be a member of the group combination Engineering and California, and at the same time be a member of the group combination Engineering and Managers. If ACS group set mappings exist for both these combinations, ACS has to determine to which group *John* should be assigned.

ACS prevents conflicting group set mappings by assigning a mapping order to the group set mappings. When a user who is authenticated by an external user database is assigned to an ACS group, ACS starts at the top of the list of group mappings for that database. ACS sequentially checks the user group memberships in the external user database against each group mapping in the list. When finding the first group set mapping that matches the external user database group memberships of the user, ACS assigns the user to the ACS group of that group mapping and terminates the mapping process.



Tip

The order of group mappings is important because it affects the network access and services that are allowed to users. When defining mappings for users who belong to multiple groups, ensure that they are in the correct order; so that users are granted the correct group settings.

For example, a user named *Mary* is assigned to the three-group combination of Engineering, Marketing, and Managers. *Mary* should be granted the privileges of a manager rather than an engineer. Mapping A assigns to ACS Group 2 users who belong to all three groups of which *Mary* is a member. Mapping B assigns to ACS Group 1 users who belong to the Engineering and Marketing groups. If Mapping B is listed first, ACS authenticates *Mary* as a user of Group 1 and she is assigned to Group 1, rather than Group 2 as managers should be.

No Access Group for Group Set Mappings

To prevent remote access for users who are assigned a group by a particular group set mapping, assign the group to the ACS No Access group. For example, you could assign all members of an external user database group *Contractors* to the No Access group so they could not dial in to the network remotely.

Default Group Mapping for Windows

For Windows user databases, ACS includes the ability to define a default group mapping. If no other group mapping matches an unknown user who is authenticated by a Windows user database, ACS assigns the user to a group based on the default group mapping.

Configuring the default group mapping for Windows user databases is the same as editing an existing group mapping, with one exception. When editing the default group mapping for Windows, instead of selecting a valid domain name on the Domain Configurations page, select **DEFAULT**.

For more information about editing an existing group mapping, see [Editing a Windows or Generic LDAP Group Set Mapping, page 17-6](#).

Windows Group Mapping Limitations

ACS has the following limits on group mapping for users who are authenticated by a Windows user database:

- ACS can only support group mapping for users who belong to 500 or fewer Windows groups.
- ACS can only perform group mapping by using the local and global groups to which a user belongs in the domain that authenticated the user. You cannot use group membership in domains that the authenticated domain trusts that is for ACS group mapping. This restriction is not removed by adding a remote group to a group that is local to the domain providing the authentication.

Creating an ACS Group Mapping for Windows or Generic LDAP Groups

Before You Begin

To map a Windows or generic LDAP group to an ACS group:

-
- Step 1** In the navigation bar, click **External User Databases**.
 - Step 2** Click **Database Group Mappings**.
 - Step 3** Click the external user database name for which you want to configure a group mapping.
If you are mapping a Windows group set, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.
 - Step 4** If you are mapping a Windows group set for a new domain:
 - a.** Click **New configuration**.
The Define New Domain Configuration page appears.
 - b.** If the Windows domain for which you want to create a group set mapping configuration appears in the Detected domains list, select the name of the domain.



Tip To clear your domain selection, click **Clear Selection**.

- c. If the Windows domain for which you want to create a group set mapping *does not appear* in the Detected domains list, type the name of a trusted Windows domain in the **Domain** box.
- d. Click **Submit**.

The new Windows domain appears in the list of domains in the Domain Configurations page.

Step 5 If you are mapping a Windows group set, click the domain name for which you want to configure a group set mapping.

The Group Mappings for Domain: *domainname* table appears.

Step 6 Click **Add Mapping**.

The Create new group mapping for *database* page opens. The group list displays group names that are derived from the external user database.

Step 7 For each group to be added to the group set mapping, select the name of the applicable external user database group in the group list, and then click **Add to selected**.



Note A user must match *all* the groups in the Selected list so that ACS can use this group set mapping to map the user to an ACS group; however, a user can also belong to other groups (in addition to the groups listed) and still be mapped to an ACS group.



Tip To remove a group from the mapping, select the name of the group in the Selected list, and then click **Remove from selected**.

The Selected list shows all the groups to which a user must belong in order to be mapped to an ACS group.

Step 8 In the ACS group list, select the name of the ACS group to which you want to map users who belong to all the external user database groups in the Selected list.



Note You can also select **No Access**. For more information about the **No Access** group, see [No Access Group for Group Set Mappings, page 17-4](#).

Step 9 Click **Submit**.

The group set you mapped to the ACS list appears at the bottom of the *database* groups column.



Note The asterisk (*) at the end of each set of groups indicates that users who are authenticated with the external user database can belong to other groups besides those in the set.

Editing a Windows or Generic LDAP Group Set Mapping

You can change the ACS group to which a group set mapping is mapped.



Note You cannot edit the external user database groups of an existing group set mapping. If you want to add or remove external user database groups from the group set mapping, delete the group set mapping and create one with the revised set of groups.

To edit a Windows or generic LDAP group mapping:

-
- Step 1** In the navigation bar, click **External User Databases**.
 - Step 2** Click **Database Group Mappings**.
 - Step 3** Click the external user database name for which you want to edit a group set mapping.
If you are editing a Windows group set mapping, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.
 - Step 4** If you are editing a Windows group set mapping, click the domain name for which you want to edit a group set mapping.
The Group Mappings for Domain: *domainname* table appears.
 - Step 5** Click the group set mapping to be edited.
The Edit mapping for *database* page opens. The external user database group or groups that are included in the group set mapping appear above the ACS group list.
 - Step 6** From the ACS group list, select the name of the group to which to map the set of external database groups, and then click **Submit**.



Note You can also select **No Access**. For more information about the **No Access** group, see [No Access Group for Group Set Mappings, page 17-4](#).

- Step 7** Click **Submit**.
The Group Mappings for *database* page opens again and includes the changed group set mapping.
-

Deleting a Windows or Generic LDAP Group Set Mapping

You can delete individual group set mappings.

To delete a Windows or generic LDAP group mapping:

-
- Step 1** In the navigation bar, click **External User Databases**.
 - Step 2** Click **Database Group Mappings**.
 - Step 3** Click the external user database configuration whose group set mapping you want to delete.
If you are deleting a Windows group set mapping, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.

- Step 4** If you are deleting a Windows group set mapping, click the domain name whose group set mapping you want to delete.
- The Group Mappings for Domain: *domainname* table appears.
- Step 5** Click the group set mapping that you want to delete.
- Step 6** Click **Delete**.
- ACS displays a confirmation dialog box.
- Step 7** Click **OK** in the confirmation dialog box.
- ACS deletes the selected external user database group set mapping.
-

Deleting a Windows Domain Group Mapping Configuration

You can delete an entire group mapping configuration for a Windows domain. When you delete a Windows domain group mapping configuration, you delete all group set mappings in the configuration.

To delete a Windows group mapping:

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Group Mappings**.
- Step 3** Click the name of the Windows external user database.
- Step 4** Click the domain name whose group set mapping you want to delete.
- Step 5** Click **Delete Configuration**.
- ACS displays a confirmation dialog box.
- Step 6** Click **OK** in the confirmation dialog box.
- ACS deletes the selected external user database group mapping configuration.
-

Changing Group Set Mapping Order

You can change the order in which ACS checks group set mappings for users who are authenticated by Windows and generic LDAP databases. To order group mappings, you must have already mapped them. For more information about creating group mappings, see [Creating an ACS Group Mapping for Windows or Generic LDAP Groups, page 17-4](#).

To change the order of group mappings for a Windows or generic LDAP group mapping:

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Group Mappings**.
- Step 3** Click the external user database name for which you want to configure group set mapping order.
- If you are ordering Windows group set mappings, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.

Step 4 If you are configuring a Windows group mapping order, click the domain name for which you want to configure group set mapping order.

The Group Mappings for Domain: *domainname* table appears.

Step 5 Click **Order mappings**.



Note The Order mappings button appears only if more than one group set mapping exists for the current database and does not apply to default group mapping.

The Order mappings for *database* page appears. The group mappings for the current database appear in the Order list.

Step 6 Select the name of a group set mapping that you want to move, and then click **Up** or **Down** until it is in the position that you want.

Step 7 Repeat Step 7 until the group mappings are in the correct order.

Step 8 Click **Submit**.

The Group Mappings for *database* page displays the group set mappings in the order that you defined.

Step 9 Click **Submit**.

ACS saves the SPT-to-user-group mapping.

RADIUS-Based Group Specification

For some types of external user databases, ACS supports the assignment of users to specific ACS groups based on the RADIUS authentication response from the external user database. ACS provides this assignment in addition to the unknown user group mapping described in [Group Mapping by External User Database, page 17-1](#). RADIUS-based group specification overrides group mapping. The database types that support RADIUS-based group specification are:

- LEAP Proxy RADIUS server
- RADIUS token server

ACS supports per-user group mapping for users who are authenticated with a LEAP Proxy RADIUS Server database. This group mapping support is provided in addition to the default group mapping described in [Group Mapping by External User Database, page 17-1](#).

To enable per user group mapping, configure the external user database to return authentication responses that contain the Cisco IOS/PIX RADIUS attribute 1, [009\001] *cisco-av-pair* with the following value:

```
ACS:CiscoSecure-Group-Id = N
```

where *N* is the ACS group number (0 through 499) to which ACS should assign the user. For example, if the LEAP Proxy RADIUS Server authenticated a user and included the following value for the Cisco IOS/PIX RADIUS attribute 1, [009\001] *cisco-av-pair*:

```
ACS:CiscoSecure-Group-Id = 37
```

ACS assigns the user to group 37 and applies authorization that is associated with group 37.