



User Group Mapping and Specification

This chapter provides information about group mapping and specification. Cisco Secure Access Control Server (ACS) Solution Engine uses these features to assign users authenticated by an external user database to a single Cisco Secure ACS group.

This chapter contains the following topics:

- [About User Group Mapping and Specification, page 16-1](#)
- [Group Mapping by External User Database, page 16-2](#)
- [Group Mapping by Group Set Membership, page 16-4](#)
- [NAC Group Mapping, page 16-13](#)
- [RADIUS-Based Group Specification, page 16-14](#)

About User Group Mapping and Specification

The Database Group Mapping feature in the External User Databases section enables you to associate unknown users with a Cisco Secure ACS group for assigning authorization profiles. For external user databases from which Cisco Secure ACS can derive group information, you can associate the group memberships defined for the users in the external user database to specific Cisco Secure ACS groups. For Windows user databases, group mapping is further

specified by domain, because each domain maintains its own user database. For Novell NDS user databases, group mapping is further specified by trees, because Cisco Secure ACS supports multiple trees in a single Novell NDS user database.

In addition to the Database Group Mapping feature, for some database types, Cisco Secure ACS supports RADIUS-based group specification.

Group Mapping by External User Database

You can map an external database to a Cisco Secure ACS group. Unknown users who authenticate using the specified database automatically belong to, and inherit the authorizations of, the group. For example, you could configure Cisco Secure 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 Cisco Secure ACS to map all unknown users found in any external user database type to a single Cisco Secure ACS group, the following external user database types are the external user database types whose users you can only map to a single Cisco Secure ACS group:

- LEAP Proxy RADIUS server
- RADIUS token server

Additionally, for the external user database types listed above, group mapping by external database type is overridden on a user-by-user basis when the external user database specifies a Cisco Secure ACS group with its authentication response. For more information about specifying group membership for users authenticated with one of these database types, see [RADIUS-Based Group Specification, page 16-14](#).

Creating a Cisco Secure ACS Group Mapping for a Token Server or LEAP Proxy RADIUS Server Database

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

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Group Mappings**.
- Step 3** Click the name of the RADIUS token server or LEAP Proxy RADIUS Server 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 authenticated with this database should be assigned.



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

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

Cisco Secure ACS assigns unknown and discovered users authenticated by the external database type you selected in Step 3 to the Cisco Secure ACS group selected in Step 4. The mapping is only applied as a default if those databases did not specify a Cisco Secure ACS group for the user.



Note For more information about group specification for RADIUS token servers, see [RADIUS-Based Group Specification, page 16-14](#).

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 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.

- Novell NDS
- Generic LDAP

When you configure a Cisco Secure ACS group mapping based on group set membership, you can add one or many external user database groups to the set. For Cisco Secure ACS to map a user to the specified Cisco Secure 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 both the Engineering and Tokyo groups and a separate one for users who belong to both 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 Cisco Secure 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

Cisco Secure ACS always maps users to a single Cisco Secure ACS group, yet a user can belong to more than one group set mapping. For example, a user, 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 there are Cisco Secure ACS group set mappings for both these combinations, Cisco Secure ACS has to determine to which group John should be assigned.

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

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

For example, a user, 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 users who belong to all three groups Mary is in to Cisco Secure ACS Group 2. Mapping B assigns users who belong to the Engineering and Marketing groups to Cisco Secure ACS Group 1. If Mapping B is listed first, Cisco Secure ACS authenticates Mary as a user of Group 1, and she is be assigned to Group 1, rather than Group 2 like managers should be.

No Access Group for Group Set Mappings

To prevent remote access for users assigned a group by a particular group set mapping, assign the group to the Cisco Secure 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, Cisco Secure ACS includes the ability to define a default group mapping. If no other group mapping matches an unknown user authenticated by a Windows user database, Cisco Secure 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 VDEFAULT.

For more information about editing an existing group mapping, see [Editing a Windows, Novell NDS, or Generic LDAP Group Set Mapping](#), page 16-9.

Windows Group Mapping Limitations

Cisco Secure ACS has the following limits with respect to group mapping for users authenticated by a Windows user database:

- Cisco Secure ACS can only support group mapping for users who belong to 500 or less Windows groups.
- Cisco Secure ACS can only perform group mapping using the local and global groups a user belongs to in the domain that authenticated the user. Group membership in domains trusted by the authenticating domain cannot be used for Cisco Secure ACS group mapping. This restriction is not removed by adding a remote group to a group local to the domain providing authentication.

Creating a Cisco Secure ACS Group Mapping for Windows, Novell NDS, or Generic LDAP Groups

Before You Begin

To map a Windows, Novell NDS, or generic LDAP group to a Cisco Secure ACS group, follow these steps:

-
- 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. If you are mapping an NDS group set, the NDS Trees table appears. Otherwise, the Group Mappings for *database* Users table appears.

Step 4 If you are mapping a Windows group set for a new domain, follow these steps:

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 If you are mapping a Novell NDS group set, click the name of the Novell NDS tree for which you want to configure group set mappings.

The Group Mappings for NDS Users table appears.

Step 7 Click **Add Mapping**.

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

Step 8 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 Cisco Secure ACS can use this group set mapping to map the user to a Cisco Secure ACS group; however, a user can also belong to other groups (in addition to the groups listed) and still be mapped to a Cisco Secure 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 that a user must belong to in order to be mapped to a Cisco Secure ACS group.

Step 9 In the CiscoSecure group list, select the name of the Cisco Secure 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 16-5.

Step 10 Click **Submit**.

The group set you mapped to the Cisco Secure 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 authenticated with the external user database can belong to other groups besides those in the set.

Editing a Windows, Novell NDS, or Generic LDAP Group Set Mapping

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

**Note**

The external user database groups of an existing group set mapping cannot be edited. 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, Novell NDS, or generic LDAP group mapping, follow these steps:

-
- 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. If you are editing an NDS group set mapping, the NDS Trees table appears. Otherwise, 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** If you are editing a Novell NDS group set mapping, click the name of the Novell NDS tree for which you want to edit a group set mapping.

The Group Mappings for NDS Users table appears.
 - Step 6** Click the group set mapping to be edited.

The Edit mapping for *database* page opens. The external user database group or groups included in the group set mapping appear above the CiscoSecure group list.
 - Step 7** From the CiscoSecure group list, select the name of the group to which the set of external database groups should be mapped, 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 16-5.

Step 8 Click **Submit**.

The Group Mappings for *database* page opens again with the changed group set mapping listed.

Deleting a Windows, Novell NDS, or Generic LDAP Group Set Mapping

You can delete individual group set mappings.

To delete a Windows, Novell NDS, or generic LDAP group mapping, follow these steps:

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 need to delete.

If you are deleting a Windows group set mapping, the Domain Configurations table appears. If you are deleting an NDS group set mapping, the NDS Trees table appears. Otherwise, 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 If you are deleting a Novell NDS group set mapping, click the name of the Novell NDS tree whose group set mapping you want to delete.

The Group Mappings for NDS Users table appears.

Step 6 Click the group set mapping you want to delete.

- Step 7** Click **Delete**.
Cisco Secure ACS displays a confirmation dialog box.
- Step 8** Click **OK** in the confirmation dialog box.
Cisco Secure 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, all group set mappings in the configuration are deleted.

To delete a Windows group mapping, follow these steps:

-
- 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**.
Cisco Secure ACS displays a confirmation dialog box.
- Step 6** Click **OK** in the confirmation dialog box.
Cisco Secure ACS deletes the selected external user database group mapping configuration.
-

Changing Group Set Mapping Order

You can change the order in which Cisco Secure ACS checks group set mappings for users authenticated by Windows, Novell NDS, and generic LDAP databases. To order group mappings, you must have already mapped them. For more information about creating group mappings, see [Creating a Cisco Secure ACS Group Mapping for Windows, Novell NDS, or Generic LDAP Groups](#), page 16-6.

To change the order of group mappings for a Windows, Novell NDS, or generic LDAP group mapping, follow these steps:

-
- 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. If you are ordering NDS group set mappings, the NDS Trees table appears. Otherwise, the Group Mappings for *database* Users table appears.

- Step 4** If you are configuring 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** If you are configuring Novell NDS group set mapping order, click the name of the Novell NDS tree for which you want to configure group set mapping order.

The Group Mappings for NDS Users table appears.

- Step 6** Click **Order mappings**.



Note The Order mappings button appears only if more than one group set mapping exists for the current database.

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

- Step 7** Select the name of a group set mapping you want to move, and then click **Up** or **Down** until it is in the position you want.

- Step 8** Repeat Step 7 until the group mappings are in the order you need.

- Step 9** Click **Submit**.

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

NAC Group Mapping

Group mapping for Network Admission Control (NAC) databases provides the means to connect a system posture token (SPT) that is the result of posture validation to the user group whose authorizations you have configured to correspond to that SPT. Through the use of group mapping, the applicable downloadable IP ACLs and Cisco RADIUS cisco-av-pair attribute values are assigned to network sessions of a Network Admission Control (NAC)-client workstation. Each NAC database instance that you create has unique SPT-to-group mappings for each of the five SPTs.

For more information about posture tokens, see [Posture Tokens, page 14-4](#).

Configuring NAC Group Mapping

To configure NAC group mapping, follow these steps:

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Group Mappings**.
- Cisco Secure ACS displays a list of all external databases, including NAC databases.
- Step 3** Click the name of the NAC database whose SPT-to-group mappings you want to configure.
- Cisco Secure ACS displays the Token-to-User-Group Mapping page for the NAC database you selected.
- Step 4** For each SPT, follow these steps:
- From the **User Group** list, select a group or, if you want to deny access, select the <No Access> option, which is the default selection.
- When the result of posture validation is the SPT listed to the left of the User Group list, Cisco Secure ACS sends to the AAA client the authorizations associated with the selected group.
- (Optional) In the PA User Message box, type a message that the NAC client can show the user of the computer running the NAC client.



Note Whether the NAC client displays messages depends upon the configuration and design of the NAC client.

Step 5 Click **Submit**.

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

RADIUS-Based Group Specification

For some types of external user databases, Cisco Secure ACS supports the assignment of users to specific Cisco Secure ACS groups based upon the RADIUS authentication response from the external user database. This is provided in addition to the unknown user group mapping described in [Group Mapping by External User Database, page 16-2](#). RADIUS-based group specification overrides group mapping. The database types that support RADIUS-based group specification are as follows:

- LEAP Proxy RADIUS server
- RADIUS token server

Cisco Secure ACS supports per-user group mapping for users authenticated with a LEAP Proxy RADIUS Server database. This is provided in addition to the default group mapping described in [Group Mapping by External User Database, page 16-2](#).

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 Cisco Secure ACS group number (0 through 499) to which Cisco Secure 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
```

Cisco Secure ACS assigns the user to group 37 and applies authorization associated with group 37.

