

# Security Manager Integration With ACS

Document ID: 99749

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Integrate Cisco Security Manager with Cisco Secure ACS

#### Integration Procedures Performed in Cisco Secure ACS

- Define Users and User Groups in Cisco Secure ACS
- Add Managed Devices as AAA Clients in Cisco Secure ACS
- Add Devices as AAA Clients Without NDGs
- Configure Network Device Groups for Use in Security Manager

#### Integration Procedures Performed in CiscoWorks

- Create a Local User in CiscoWorks
- Define the System Identity User
- Configure the AAA Setup Mode in CiscoWorks
- Restart the Daemon Manager

#### Assign Roles to User Groups in Cisco Secure ACS

- Assign Roles to User Groups Without NDGs
- Associate NDGs and Roles with User Groups

#### Troubleshoot

#### Related Information

## Introduction

This document describes how to integrate the Cisco Security Manager with Cisco Secure Access Control Server (ACS).

Cisco Secure ACS provides command authorization for users who utilize management applications, such as Cisco Security Manager, in order to configure managed network devices. Support for command authorization is provided by unique command authorization set types, called roles in Cisco Security Manager, that contain a set of permissions. These permissions, also called privileges, determine the actions that users with particular roles can perform within Cisco Security Manager.

Cisco Secure ACS uses TACACS+ in order to communicate with management applications. For Cisco Security Manager to communicate with Cisco Secure ACS, you must configure the CiscoWorks server in Cisco Secure ACS as an AAA client that uses TACACS+. In addition, you must provide the CiscoWorks server with the administrator name and password that you use in order to log into the Cisco Secure ACS. When you fulfill these requirements, it ensures the validity of communications between Cisco Security Manager and Cisco Secure ACS.

When Cisco Security Manager initially communicates with Cisco Secure ACS, it dictates to Cisco ACS the creation of default roles, which appear in the Shared Profile Components section of the Cisco Secure ACS HTML interface. It also dictates a custom service to be authorized by TACACS+. This custom service appears on the TACACS+ (Cisco IOS®) page in the Interface Configuration section of the HTML interface. You can then modify the permissions included in each Cisco Security Manager role and apply these roles to users and user groups.

**Note:** It is not possible to integrate CSM with ACS 5.2 as it is not supported.

## Prerequisites

### Requirements

In order to use Cisco Secure ACS, make sure that:

- You define roles that include the commands required in order to perform necessary functions in Cisco Security Manager.
- The Network Access Restriction (NAR) includes the device group (or the devices) that you want to administer, if you apply a NAR to the profile.
- Managed device names are spelled and capitalized identically in Cisco Secure ACS and in Cisco Security Manager.

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco Security Manager version 3.0
- Cisco Secure ACS version 3.3

**Note:** Make sure that you choose the compatible CSM and ACS versions before you install on your network environment. For example, Cisco tested ACS 3.3 with only CSM 3.0 and stopped for later CSM versions. So, you are recommended to use CSM 3.0 with ACS 3.3. See the Compatibility Matrix table for more information on various software versions.

<b>Cisco Security Manager Versions</b>	<b>CS ACS Versions Tested</b>
3.0.0 3.0.0 SP1	Windows 3.3(3) and 4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	Solutions Engine 4.0(1) Windows 4.0(1)
3.1.0 3.0.2	Solutions Engine 4.0(1) Windows 4.1(1) and 4.1(3)
3.1.1 3.0.2 SP1 3.0.2 SP2	Solutions Engine v4.0(1) Windows 4.1(2), 4.1(3) and 4.1(4)
3.1.1 SP1	Solutions Engine 4.0(1) Windows 4.1(4)
3.1.1 SP2	Solutions Engine 4.0(1) Windows 4.1(4) and 4.2(0)
3.2.0	Solutions Engine 4.1(4) Windows 4.1(4) and 4.2(0)
3.2.1	Solutions Engine 4.1(4) Windows 4.2(0)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

# Integrate Cisco Security Manager with Cisco Secure ACS

This section describes the steps required to integrate Cisco Security Manager with Cisco Secure ACS. Some steps contain several substeps. These steps and substeps must be performed in order. This section also contains references to specific procedures used in order to perform each step.

Complete these steps:

### 1. Plan your administrative authentication and authorization model.

You must decide on your administrative model before you use Cisco Security Manager. This includes the definition of the administrative roles and accounts that you plan to use.

**Tip:** When you define the roles and permissions of potential administrators, also consider whether or not to enable Workflow. This selection affects how you can restrict access.

### 2. Install Cisco Secure ACS, Cisco Security Manager, and CiscoWorks Common Services.

Install Cisco Secure ACS version 3.3 on a Windows 2000/2003 server. Install CiscoWorks Common Services and Cisco Security Manager on a different Windows 2000/Windows 2003 server.

Refer to these documents for more information:

- ◆ Installation Guide for Cisco Security Manager 3.0
- ◆ Installation Guide for Cisco Secure ACS for Windows 3.3

**Note:** See the Compatibility Matrix table for more information before you choose the CSM and ACS software versions.

### 3. Perform integration procedures in Cisco Secure ACS.

Define Cisco Security Manager users as ACS users and assign them to user groups based on their planned role, add all your managed devices (as well as the CiscoWorks/Security Manager server) as AAA clients, and create an administration control user. See Integration Procedures Performed in Cisco Secure ACS for more information.

### 4. Perform integration procedures in CiscoWorks Common Services.

Configure a local user that matches the administrator defined in Cisco Secure ACS, define that same user for the system identity setup, and configure ACS as the AAA setup mode.

See Integration Procedures Performed in CiscoWorks for more information.

### 5. Assign Roles to User Groups in Cisco Secure ACS.

Assign roles to each user group configured in Cisco Secure ACS. The procedure you use depends on whether you have configured network device groups (NDGs).

See Assign Roles to User Groups in Cisco Secure ACS for more information.

# Integration Procedures Performed in Cisco Secure ACS

This section describes the steps you must complete in Cisco Secure ACS in order to integrate it with Cisco Security Manager:

1. Define Users and User Groups in Cisco Secure ACS
2. Add Managed Devices as AAA Clients in Cisco Secure ACS
3. Create an Administration Control User in Cisco Secure ACS

## Define Users and User Groups in Cisco Secure ACS

All users of Cisco Security Manager must be defined in Cisco Secure ACS and assigned a role appropriate to their job function. The easiest way to do this is to divide the users into different groups based on each default role available in ACS. For example, assign all the system administrators to one group, all the network operators to another group, and so on. Refer to Cisco Secure ACS Default Roles for more information about the default roles in ACS.

In addition, you must create an additional user that is assigned the system administrator role with full permissions. The credentials established for this user are later used on the System Identity Setup page in CiscoWorks. See Define the System Identity User for more information.

Note that at this stage you merely assign users to different groups. The actual assignment of roles to these groups is performed later, after CiscoWorks, Cisco Security Manager, and any other applications are registered to Cisco Secure ACS.

**Tip:** Before you proceed, install CiscoWorks Common Services and Cisco Security Manager on one Windows 2000/2003 server. Install Cisco Secure ACS on a different Windows 2000/2003 server.

1. Log in to Cisco Secure ACS.
2. Configure a user with full permissions:
  - a. Click **User Setup** on the navigation bar.
  - b. On the User Setup page, enter a name for the new user, then click **Add/Edit**.
  - c. Select an authentication method from the Password Authentication list under User Setup.
  - d. Enter and confirm the password for the new user.
  - e. Select **Group 1** as the group to which the user is assigned.
  - f. Click **Submit** in order to create the user account.
3. Repeat step 2 for each Cisco Security Manager user. Cisco recommends that you divide the users into groups based on the role each user is assigned:
  - ◆ Group 1 System Administrators
  - ◆ Group 2 Security Administrators
  - ◆ Group 3 Security Approvers
  - ◆ Group 4 Network Administrators
  - ◆ Group 5 Approvers
  - ◆ Group 6 Network Operators
  - ◆ Group 7 Help Desk

See the Table for more information about the default permissions associated with each role. Refer to Customizing Cisco Secure ACS Roles for more information about customizing user roles.

Permissions	Roles					
	System	Security	Security	Network	Network	Approver

	Admin	Admin(ACS)	Approver(ACS)	Admin(CW)	Admin(ACS)		
<b>View Permissions</b>							
<b>View Device</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>View Policy</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>View Objects</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>View Topology</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>View CLI</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>View Admin</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>View Config Archive</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>View Device Managers</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Modify Permissions</b>							
<b>Modify Device</b>	Yes	Yes	No	Yes	No	No	No
<b>Modify Hierarchy</b>	Yes	Yes	No	Yes	No	No	No
<b>Modify Policy</b>	Yes	Yes	No	Yes	No	No	No
<b>Modify Image</b>	Yes	Yes	No	Yes	No	No	No
<b>Modify Objects</b>	Yes	Yes	No	Yes	No	No	No
<b>Modify Topology</b>	Yes	Yes	No	Yes	No	No	No
<b>Modify Admin</b>	Yes	No	No	No	No	No	No
<b>Modify Config Archive</b>	Yes	Yes	No	Yes	Yes	No	Yes
<b>Additional Permissions</b>							
<b>Assign Policy</b>	Yes	Yes	No	Yes	No	No	No
<b>Approve Policy</b>	Yes	No	Yes	No	No	No	No
<b>Approve CLI</b>	Yes	No	No	No	No	Yes	No
<b>Discover(Import)</b>	Yes	Yes	No	Yes	No	No	No
<b>Deploy</b>	Yes	No	No	Yes	Yes	No	No
<b>Control</b>	Yes	No	No	Yes	Yes	No	Yes
<b>Submit</b>	Yes	Yes	No	Yes	No	No	No

**Note:** At this stage, the groups themselves are collections of users without any role definitions. You assign roles to each group after you complete the integration process. See Assign Roles to User Groups in Cisco Secure ACS for more information.

4. Create an additional user and assign this user to the system administrators group. The credentials established for this user are later used on the System Identity Setup page in CiscoWorks. See Define the System Identity User for more information.
5. Continue with Add Managed Devices as AAA Clients in Cisco Secure ACS.

## Add Managed Devices as AAA Clients in Cisco Secure ACS

Before you can begin to import devices into Cisco Security Manager, you must first configure each device as an AAA client in your Cisco Secure ACS. In addition, you must configure the CiscoWorks/Security Manager server as an AAA client.

If Cisco Security Manager manages security contexts configured on firewall devices, which includes security contexts configured on FWSMs for Catalyst 6500/7600 devices, each context must be added individually to Cisco Secure ACS.

The method you use in order to add managed devices depends on whether you want to restrict users to manage a particular set of devices with network device groups (NDGs). See one of these sections:

- If you want users to have access to all devices, add the devices as described in [Add Devices as AAA Clients Without NDGs](#).
- If you want users to have access only to certain NDGs, add the devices as described in [Configure Network Device Groups for Use in Security Manager](#).

### Add Devices as AAA Clients Without NDGs

This procedure describes how to add devices as AAA clients of a Cisco Secure ACS. Refer to the *AAA Client Configuration* section of Network Configuration for complete information about all available options.

**Note:** Remember to add the CiscoWorks/Security Manager server as an AAA client.

1. Click **Network Configuration** on the Cisco Secure ACS navigation bar.
2. Click **Add Entry** beneath the AAA Clients table.
3. Enter the AAA client hostname (up to 32 characters) on the Add AAA Client page. The hostname of the AAA client must match the display name you plan to use for the device in Cisco Security Manager.

For example, if you intend to append a domain name to the device name in Cisco Security Manager, the AAA client hostname in ACS must be **<device\_name>.<domain\_name>**.

When you name the CiscoWorks server, it is recommended to use the fully-qualified hostname. Be sure to spell the hostname correctly. The hostname is not case sensitive.

When you name a security context, append the context name (**\_<context\_name>**) to the device name. For FWSMs, this is the naming convention:

- ◆ FWSM blade **<chassis\_name>\_FW\_<slot\_number>**
  - ◆ Security context **<chassis\_name>\_FW\_<slot\_number>\_<context\_name>**
4. Enter the IP address of the network device in the AAA Client IP Address field.
  5. Enter the shared secret in the Key field.
  6. Select **TACACS+ (Cisco IOS)** from the Authenticate Using list.
  7. Click **Submit** in order to save your changes. The device you added appears in the AAA Clients table.
  8. Repeat steps 1 through 7 in order to add additional devices.
  9. After you add all the devices, click **Submit + Restart**.
  10. Continue with [Create an Administration Control User in Cisco Secure ACS](#).

# Configure Network Device Groups for Use in Security Manager

Cisco Secure ACS enables you to configure network device groups (NDGs) that contain specific devices to be managed. For example, you can create NDGs for each geographic region or NDGs that match your organizational structure. When used with Cisco Security Manager, NDGs enable you to provide users with different levels of permissions, based on the devices they need to manage. For example, with NDGs you can assign User A system administrator permissions to the devices located in Europe and Help Desk permissions to the devices located in Asia. You can then assign the opposite permissions to User B.

NDGs are not assigned directly to users. Rather, NDGs are assigned to the roles that you define for each user group. Each NDG can be assigned to a single role only, but each role can include multiple NDGs. These definitions are saved as part of the configuration for the selected user group.

These topics outline the basic steps required in order to configure NDGs:

- Activate the NDG Feature
- Create NDGs
- Associate NDGs and Roles with User Groups

## Activate the NDG Feature

You must activate the NDG feature before you can create NDGs and populate them with devices.

1. Click **Interface Configuration** on the Cisco Secure ACS navigation bar.
2. Click **Advanced Options**.
3. Scroll down, then check the **Network Device Groups** check box.
4. Click **Submit**.
5. Continue with Create NDGs.

## Create NDGs

This procedure describes how to create NDGs and populate them with devices. Each device can belong to only one NDG.

**Note:** Cisco recommends that you create a special NDG that contains the CiscoWorks/Security Manager server.

1. Click **Network Configuration** on the navigation bar.

All devices are initially placed under Not Assigned, which holds all devices that were not placed in an NDG. Keep in mind that Not Assigned is not an NDG.

2. Create NDGs:
  - a. Click **Add Entry**.
  - b. Enter a name for the NDG on the New Network Device Group page. The maximum length is 24 characters. Spaces are permitted.
  - c. **Optional when with version 4.0 or later:** Enter a key to be used by all the devices in the NDG. If you define a key for the NDG, it overrides any keys defined for the individual devices in the NDG.
  - d. Click **Submit** in order to save the NDG.
  - e. Repeat steps a through d in order to create more NDGs.
3. Populate the NDGs with devices:
  - a. Click the name of the NDG in the Network Device Groups area.

- b. Click **Add Entry** in the AAA Clients area.
  - c. Define the particulars of the device to add to the NDG, then click **Submit**. See Add Devices as AAA Clients Without NDGs for more information.
  - d. Repeat steps b and c in order to add the remainder of the devices to NDGs. The only device that you can leave in the Not Assigned category is the default AAA server.
  - e. After you configure the last device, click **Submit + Restart**.
4. Continue with Create an Administration Control User in Cisco Secure ACS.

## Create an Administration Control User in Cisco Secure ACS

Use the Administration Control page in Cisco Secure ACS in order to define the administrator account that is used when defining the AAA setup mode in CiscoWorks Common Services. See Configure the AAA Setup Mode in CiscoWorks for more information.

1. Click **Administration Control** on the Cisco Secure ACS navigation bar.
2. Click **Add Administrator**.
3. On the Add Administrator page, enter a name and password for the administrator.
4. Click **Grant All** in the Administrator Privileges area in order to provide full administrative permissions to this administrator.
5. Click **Submit** in order to create the administrator.

**Note:** Refer to Administrators and Administrative Policy for more information about the options available when you configure an administrator.

## Integration Procedures Performed in CiscoWorks

This section describes the steps to complete in CiscoWorks Common Services in order to integrate it with Cisco Security Manager:

- Create a Local User in CiscoWorks
- Define the System Identity User
- Configure the AAA Setup Mode in CiscoWorks

Complete these steps after you complete the integration procedures performed in Cisco Secure ACS. Common Services performs the actual registration of any installed applications, such as Cisco Security Manager, Auto-Update Server, and IPS Manager into Cisco Secure ACS.

### Create a Local User in CiscoWorks

Use the Local User Setup page in CiscoWorks Common Services in order to create a local user account that duplicates the administrator you previously created in Cisco Secure ACS. This local user account is later used for the system identity setup. See for more information.

**Note:** Before you proceed, create an administrator in Cisco Secure ACS. See Define Users and User Groups in Cisco Secure ACS for instructions.

1. Log into CiscoWorks with the default **admin** user account.
2. Choose **Server > Security** from Common Services, then choose **Local User Setup** from the TOC.
3. Click **Add**.
4. Enter the same name and password that you entered when you created the administrator in Cisco Secure ACS. See step 4 in Define Users and User Groups in Cisco Secure ACS.
5. Check all the check boxes under Roles except Export Data.
6. Click **OK** to create the user.

## Define the System Identity User

Use the System Identity Setup page in CiscoWorks Common Services in order to create a trust user, known as the System Identity user, that enables communication between servers that are part of the same domain and application processes that are located on the same server. Applications use the System Identity user in order to authenticate processes on local or remote CiscoWorks servers. This is especially useful when the applications must synchronize before any users have logged in.

In addition, the System Identity user is often used in order to perform a subtask when the primary task is already authorized for the logged in user. For example, in order to edit a device in Cisco Security Manager, interapplication communication is required between Cisco Security Manager and the Common Services DCR. After the user is authorized to perform the editing task, the System Identity user is used in order to invoke the DCR.

The System Identity user you configure here must be identical to the user with administrative (full) permissions that you configured in ACS. Failure to do so can result in an inability to view all the devices and policies configured in Cisco Security Manager.

**Note:** Before you proceed, create a local user with the same name and password as this administrator in CiscoWorks Common Services. See *Create a Local User in CiscoWorks* for instructions.

1. Choose **Server > Security**, then choose **Multi-Server Trust Management > System Identity Setup** from the TOC.
2. Enter the name of the administrator that you created for Cisco Secure ACS. See step 4 in *Define Users and User Groups in Cisco Secure ACS*.
3. Enter and verify the password for this user.
4. Click **Apply**.

## Configure the AAA Setup Mode in CiscoWorks

Use the AAA Setup Mode page in CiscoWorks Common Services in order to define your Cisco Secure ACS as the AAA server, which includes the required port and shared secret key. In addition, you can define up to two backup servers.

These steps perform the actual registration of CiscoWorks, Cisco Security Manager, IPS Manager (and optionally, Auto-Update Server) into Cisco Secure ACS.

1. Choose **Server > Security**, then choose **AAA Mode Setup** from the TOC.
2. Check the **TACACS+** check box under Available Login Modules.
3. Select **ACS** as the AAA type.
4. Enter the IP addresses of up to three Cisco Secure ACS servers in the Server Details area. The secondary and tertiary servers act as backups in case the primary server fails.

**Note:** If all the configured TACACS+ servers fail to respond, you must log in with the admin CiscoWorks Local account, then change the AAA mode back to Non-ACS/CiscoWorks Local. After the TACACS+ servers are restored to service, you must change the AAA mode back to ACS.

5. In the Login area, enter the name of the administrator that you defined on the Administration Control page of Cisco Secure ACS. See *Create an Administration Control User in Cisco Secure ACS* for more information.
6. Enter and verify the password for this administrator.
7. Enter and verify the shared secret key that you entered when you added the Security Manager server as a AAA client of Cisco Secure ACS. See step 5 in *Add Devices as AAA Clients Without NDGs*.
8. Check the **Register all installed applications with ACS** check box in order to register Cisco Security

Manager and any other installed applications with Cisco Secure ACS.

9. Click **Apply** in order to save your settings. A progress bar displays the progress of the registration. A message appears when registration is complete.
10. If you integrate Cisco Security Manager with any ACS version, restart the Cisco Security Manager Daemon Manager service. See *Restart the Daemon Manager* for instructions.

**Note:** After CSM 3.0.0, Cisco no longer tests with ACS 3.3(x) because it is heavily patched and its End-Of-Life (EOL) has been announced. Therefore, you need to use the appropriate ACS version for the CSM version 3.0.1 and later. See the *Compatibility Matrix* table for more information.

11. Log back into Cisco Secure ACS in order to assign roles to each user group. See *Assign Roles to User Groups in Cisco Secure ACS* for instructions.

**Note:** The AAA setup configured here is not retained if you uninstall CiscoWorks Common Services or Cisco Security Manager. In addition, this configuration cannot be backed up and restored after reinstallation. Therefore, if you upgrade to a new version of either application, you must reconfigure the AAA setup mode and reregister Cisco Security Manager with ACS. This process is not required for incremental updates. If you install additional applications, such as AUS, on top of CiscoWorks, you must reregister the new applications and Cisco Security Manager.

## Restart the Daemon Manager

This procedure describes how to restart the Daemon Manager of the Cisco Security Manager server. You must do this in order for the AAA settings you configured to take effect. You can then log back into CiscoWorks with the credentials defined in Cisco Secure ACS.

1. Log into the machine on which the Cisco Security Manager server is installed.
2. Choose **Start > Programs > Administrative Tools > Services** in order to open the Services window.
3. From the list of services displayed in the right pane, select **Cisco Security Manager Daemon Manager**.
4. Click the **Restart Service** button on the toolbar.
5. Continue with *Assign Roles to User Groups in Cisco Secure ACS*.

## Assign Roles to User Groups in Cisco Secure ACS

After you register CiscoWorks, Cisco Security Manager and other installed applications to Cisco Secure ACS, you can assign roles to each of the user groups that you previously configured in Cisco Secure ACS. These roles determine the actions that the users in each group are permitted to perform in Cisco Security Manager.

The procedure you use in order to assign roles to user groups depends on whether NDGs are used:

- Assign Roles to User Groups Without NDGs
- Associate NDGs and Roles with User Groups

### Assign Roles to User Groups Without NDGs

This procedure describes how to assign the default roles to user groups when NDGs are not defined. Refer to *Cisco Secure ACS Default Roles* for more information.

**Note:** Before you proceed:

- Create a user group for each default role. See *Define Users and User Groups in Cisco Secure ACS* for instructions.

- Complete the procedures described in Integration Procedures Performed in Cisco Secure ACS and Integration Procedures Performed in CiscoWorks.

Complete these steps:

1. Log in to Cisco Secure ACS.
2. Click **Group Setup** on the navigation bar.
3. Select the user group for system administrators from the list. See step 2 of Define Users and User Groups in Cisco Secure ACS, then click **Edit Settings**.

## Associate NDGs and Roles with User Groups

When you associate NDGs with roles for use in Cisco Security Manager, you must create definitions in two places on the Group Setup page:

- CiscoWorks area
- Cisco Security Manager area

The definitions in each area must match as closely as possible. When you associate custom roles or ACS roles that do not exist in CiscoWorks Common Services, try to define as close an equivalent as possible based on the permissions assigned to that role.

You must create associations for each user group to be used with Cisco Security Manager. For example, if you have a user group that contains support personnel for the Western region, you can select that user group, then associate the NDG that contains the devices in that region with the Help Desk role.

**Note:** Before you proceed, activate the NDG feature and create NDGs. See Configure Network Device Groups for Use in Security Manager for more information.

1. Click **Group Setup** on the navigation bar.
2. Select a user group from the Group list, then click **Edit Settings**.
3. Map NDGs and roles for use in CiscoWorks:
  - a. On the Group Setup page, scroll down to the CiscoWorks area under TACACS+ Settings.
  - b. Select **Assign a CiscoWorks on a per Network Device Group Basis**.
  - c. Select an NDG from the Device Group list.
  - d. Select the role to which this NDG is to be associated from the second list.
  - e. Click **Add Association**. The association appears in the Device Group box.
  - f. Repeat steps c through e in order to create additional associations.

**Note:** In order to remove an association, select it from the Device Group, then click Remove Association.

4. Scroll down to the Cisco Security Manager area and create associations that match as closely as possible the associations defined in step 3.

**Note:** When you select the Security Approver or Security Administrator roles in Cisco Secure ACS, it is recommended that you select Network Administrator as the closest equivalent CiscoWorks role.

5. Click **Submit** in order to save your settings.
6. Repeat steps 2 through 5 in order to define NDGs for the remainder of the user groups.
7. After you associate NDGs and roles with each user group, click **Submit + Restart**.

# Troubleshoot

1. Before you can begin to import devices into Cisco Security Manger, you must first configure each device as an AAA client in your Cisco Secure ACS. In addition, you must configure the CiscoWorks/Security Manager server as an AAA client.
2. If you receive a failed attempts log, author failed with error in the Cisco Secure ACS.

```
"service=Athena cmd=OGS authorize-deviceGroup*(Not Assigned) authorize-deviceGroup*  
Devices authorize-deviceGroup*HQ Routers authorize-deviceGroup*HQ Switches  
authorize-deviceGroup*HQ Security Devices authorize-deviceGroup*Agent Routers author
```

In order to resolve this issue, make sure that the name of the device in ACS needs to be a fully qualified domain name.

## Related Information

- [Cisco Security Access Control Server for Windows Support Page](#)
- [Cisco Security Manager Support Page](#)
- [Cisco Secure Access Control Server for Windows](#)
- [Configuration Guide for Cisco Secure ACS 4.1](#)
- [Cisco Secure ACS Online Troubleshooting Guide, 4.1](#)
- [Security Product Field Notices \(including CiscoSecure ACS for Windows\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Sep 25, 2008

Document ID: 99749

---