Managing User Accounts

Managing user accounts involves account creation and user permissions:

- Account Creation, page 8-1. Your account can be a local account on the Security Manager Server, an ACS account on the CiscoWorks Common Services server, or a non-ACS account on the Common Services server.
- User Permissions, page 8-3. Your permissions (or privileges) are the tasks that you are authorized to perform. Your permissions are defined by your role within Security Manager. Your role within Security Manager is established after your username and password are authenticated. Authentication is done by Security Manager during login.

Account Creation

To use Cisco Security Manager, you must log in with the **admin** account that you created during installation and create an account for each user. You can create the following types of accounts:

- Local Account, page 8-1
- ACS Account, page 8-2
- Non-ACS Account, page 8-2

Local Account

To create a local account:

1. Do one of the following:
   - If you currently have the Security Manager client open and are logged in with an admin account, you can select **Tools > Security Manager Administration** and select **Server Security** from the table of contents. The Server Security page has buttons that link to and open specific pages in Common Services. Click **Local User Setup** to navigate to the Local User Setup page in Common Services.
   - Using your web browser, link to the Security Manager server using the URL https://*servername*, where *servername* is the IP address or DNS name of the server. This URL opens the Security Manager home page. Click **Server Administration** to open Common Services. Point to **Server > Single-Server Management > Local User Setup** to navigate to the Local User Setup page in Common Services.
2. Click **Add**.

ACS Account

To create an ACS account:

1. Do one of the following:
   - If you currently have the Security Manager client open and are logged in with an admin account, you can select **Tools > Security Manager Administration** and select **Server Security** from the table of contents. The Server Security page has buttons that link to and open specific pages in Common Services. Click **AAA Setup** to navigate to the Authentication Mode Setup page in Common Services.
   - Using your web browser, link to the Security Manager server using the URL https://*servername*, where *servername* is the IP address or DNS name of the server. This URL opens the Security Manager home page. Click **Server Administration** to open Common Services. Point to **Server > AAA Mode Setup** to navigate to the Authentication Mode Setup page in Common Services.
2. Select **ACS** under AAA Mode Setup.

Tip An ACS account uses (1) the ACS type of AAA Mode Setup (this is on the Authentication Mode Setup page) and (2) the ACS login module in CiscoWorks Common Services. However, you do not need to select the ACS login module; it is selected for you automatically when you select the ACS type of AAA Mode Setup.

Non-ACS Account

To create a non-ACS account:

1. Do one of the following:
   - If you currently have the Security Manager client open and are logged in with an admin account, you can select **Tools > Security Manager Administration** and select **Server Security** from the table of contents. The Server Security page has buttons that link to and open specific pages in Common Services. Click **AAA Setup** to navigate to the Authentication Mode Setup page in Common Services.
   - Using your web browser, link to the Security Manager server using the URL https://*servername*, where *servername* is the IP address or DNS name of the server. This URL opens the Security Manager home page. Click **Server Administration** to open Common Services. Point to **Server > AAA Mode Setup** to navigate to the Authentication Mode Setup page in Common Services.
2. Select **Local RBAC** under AAA Mode Setup.

Tip A non-ACS account uses (1) the Local RBAC type of AAA Mode Setup (this is on the Authentication Mode Setup page) and (2) one of the following login modules in CiscoWorks Common Services: CiscoWorks Local (the default login module), Local NT System, MS Active Directory, RADIUS, or TACACS+.

User Permissions

Cisco Security Manager authenticates your username and password before you can log in. After they are authenticated, Security Manager establishes your role within the application. This role defines your permissions (also called privileges), which are the set of tasks or operations that you are authorized to perform. If you are not authorized for certain tasks or devices, the related menu items, items in tables of contents, and buttons are hidden or disabled. In addition, a message tells you that you do not have permission to view the selected information or perform the selected operation.

Authentication and authorization for Security Manager is managed either by the CiscoWorks server or the Cisco Secure Access Control Server (ACS). By default, CiscoWorks manages authentication and authorization, but you can change to Cisco Secure ACS by using the AAA Mode Setup page in CiscoWorks Common Services. For more information on ACS integration, refer to the following sections of this chapter:

- Integrating Security Manager with Cisco Secure ACS, page 8-12
- Troubleshooting Security Manager-ACS Interactions, page 8-28

Prior to Security Manager 4.3, the major advantages of using Cisco Secure ACS were (1) the ability to create highly granular user roles with specialized permission sets (for example, allowing the user to configure certain policy types but not others) and (2) the ability to restrict users to certain devices by configuring network device groups (NDGs). These granular privileges (effectively "role-based access control," or RBAC) were not available in Security Manager 4.2 and earlier versions, unless you used Cisco Secure ACS. These granular privileges (RBAC) are available in Security Manager 4.3 and later because they use Common Services 4.0 or later, in which local RBAC is available without the use of ACS.

Security Manager 4.18 retains compatibility with ACS 4.2. See Integrating Security Manager with Cisco Secure ACS, page 8-12.

Note Users who wish to migrate their RBAC abilities from ACS to Common Services must do so manually; there are no migration scripts or other migration support.

Tip To view the complete Security Manager permissions tree, log in to Cisco Secure ACS, then click **Shared Profile Components** on the navigation bar. For more information, see Customizing Cisco Secure ACS Roles, page 8-10.

The following topics describe user permissions:

- Security Manager ACS Permissions, page 8-4
- Understanding CiscoWorks Roles, page 8-6
- Understanding Cisco Secure ACS Roles, page 8-9
- Default Associations Between Permissions and Roles in Security Manager, page 8-11

Security Manager ACS Permissions

Cisco Security Manager provides default ACS roles and permissions. You can customize the default roles or create additional roles to suit your needs. However, when defining new roles or customizing default roles, make sure that the permissions you select are logical within the context of the Security Manager application. For example, if you assign modify permissions without view permissions, you lock the user out of the application.

Security Manager classifies permissions into the following categories. For an explanation of individual permissions, see the online help integrated with Cisco Secure ACS (for information on viewing the permissions, see Customizing Cisco Secure ACS Roles, page 8-10).

- **View**—Allows you to view the current settings. These are the main view permissions:
  - **View > Policies**. Allows you to view the various types of policies. The folder contains permissions for various policy classes, such as firewall and NAT.
  - **View > Objects**. Allows you to view the various types of policy objects. The folder contains permissions for each type of policy object.
  - **View > Admin**. Allows you to view Security Manager administrative settings.
  - **View > CLI**. Allows you to view the CLI commands configured on a device and preview the commands that are about to be deployed.
  - **View > Config Archive.** Allows you to view the list of configurations contained in the configuration archive. You cannot view the device configuration or any CLI commands.
  - **View > Devices**. Allows you to view devices in Device view and all related information, including their device settings, properties, assignments, and so on. You can limit device permissions to particular sets of devices by configuring network device groups (NDGs).
  - **View > Device Managers**. Allows you to launch read-only versions of the device managers for individual devices.
  - **View > Topology**. Allows you to view maps configured in Map view.
  - **View > Event Viewer**. Allows you to view events in the Event Viewer in both the Real Time Viewer and the Historical Viewer.
  - **View > Report Manager**. Allows you to view reports in Report Manager.
  - **View > Schedule Reports**. Allows you to schedule reports in Report Manager.
  - **View > Health and Performance Manager**. Allows you to launch the Health and Performance Manager.
  - **View > Image Manager**. Allows you to launch the Image Manager.
- **Modify**—Allows you to change the current settings.
  - **Modify > Policies**. Allows you to modify the various types of policies. The folder contains permissions for various policy classes.
  - **Modify > Objects**. Allows you to modify the various types of policy objects. The folder contains permissions for each type of policy object.
  - **Modify > Admin**. Allows you to modify Security Manager administrative settings.
  - **Modify > Config Archive.** Allows you to modify the device configuration in the Configuration Archive. In addition, it allows you to add configurations to the archive and customize the Configuration Archive tool.

  - **Modify > Devices**. Allows you to add and delete devices, as well as modify device properties and attributes. To discover the policies on the device being added, you must also enable the Import permission. In addition, if you enable the Modify > Devices permission, make sure that you also enable the Assign > Policies > Interfaces permission. You can limit device permissions to particular sets of devices by configuring network device groups (NDGs).
  - **Modify > Hierarchy**. Allows you to modify device groups.
  - **Modify > Topology**. Allows you to modify maps in Map view.
  - **Modify > Manage Event Monitoring**. Allows you to enable and disable the monitoring in Security Manager for any device, so that Security Manager starts or stops event reception and processing from that device.
  - **Modify > Modify Image Repository**. Allows you to modify items in the Image Repository and to check for image updates from Cisco.com.
- **Assign**—Allows you to assign the various types of policies to devices and VPNs. The folder contains permissions for various policy classes.
- **Approve**—Allows you to approve policy changes and deployment jobs.
- **Control**—Allows you to issue commands to devices, such as ping. This permission is used for connectivity diagnostics.
- **Deploy**—Allows you to deploy configuration changes to the devices in your network and perform rollback to return to a previously deployed configuration.
- **Import**—Allows you to import the configurations that are already deployed on devices into Security Manager. You must also have view device and modify device privileges.
- **Submit**—Allows you to submit your configuration changes for approval.

Tips

- When you select modify, assign, approve, import, control or deploy permissions, you must also select the corresponding view permissions; otherwise, Security Manager will not function properly.
- When you select modify policy permissions, you must also select the corresponding assign and view policy permissions.
- When you permit a policy that uses policy objects as part of its definition, you must also grant view permissions to these object types. For example, if you select the permission for modifying routing policies, you must also select the permissions for viewing network objects and interface roles, which are the object types required by routing policies.
- The same holds true when permitting an object that uses other objects as part of its definition. For example, if you select the permission for modifying user groups, you must also select the permissions for viewing network objects, ACL objects, and AAA server groups.
- You can limit device permissions to particular sets of devices by configuring network device groups (NDGs). NDGs have the following effects on policy permissions:
  - To view a policy, you must have permissions for at least one device to which the policy is assigned.
  - To modify a policy, you must have permissions for all the devices to which the policy is assigned.
  - To view, modify, or assign a VPN policy, you must have permissions for all the devices in the VPN topology.

– To assign a policy to a device, you need permissions only for that device, regardless of whether you have permissions for any other devices to which the policy is assigned. (VPN policies are an exception, as noted above.) However, if a user assigns a policy to a device for which you do not have permissions, you cannot modify that policy.

Understanding CiscoWorks Roles

When users are created in CiscoWorks Common Services, they are assigned one or more roles. The permissions associated with each role determine the operations that each user is authorized to perform in Security Manager.

The following topics describe CiscoWorks roles:

- CiscoWorks Common Services Default Roles, page 8-6
- Selecting an Authorization Type and Assigning Roles to Users in Common Services, page 8-7

CiscoWorks Common Services Default Roles

CiscoWorks Common Services contains the following default roles for Security Manager:

- **Help Desk**—Help desk users can view (but not modify) devices, policies, objects, and topology maps.
- **Approver**—Can approve the modification of changes and CLI changes.
- **Network Operator**—In addition to view permissions, network operators can view CLI commands and Security Manager administrative settings. Network operators can also modify the configuration archive and issue commands (such as ping) to devices.
- **Network Administrator**—Can only deploy changes.

Note Cisco Secure ACS features a default role called Network Administrator that contains a different set of permissions. For more information, see Understanding Cisco Secure ACS Roles, page 8-9.

- **System Administrator**—System administrators have complete access to all Security Manager permissions, including modification, policy assignment, activity and job approval, discovery, deployment, and issuing commands to devices.

Tip In Security Manager, the System Administrator role has the highest level of permissions.

- **Super Admin—**Can perform all CiscoWorks operations including the administration and approval tasks. By default, this role has full privileges.

Tip In Security Manager, the Super Admin role does not have the highest level of permissions. Also, the Super Admin role is specific to Common Services and not to ACS.

- **Security Administrator—**Can only modify, assign, and submit changes.
- **Security Approver—**Can approve only the modification of changes.

Image Manager

Additional tasks for each of the default roles are defined for Image Manager, a feature that first appeared in Security Manager 4.3 and continues to be available in Security Manager 4.18:

- Launching Image Manager
- Adding images to the repository in Security Manager
- Creating image upgrade jobs

When using a local account (unique to Security Manager, defined on the Security Manager server), these additional tasks are assigned to different roles as listed in Table 8-1.

Table 8-1 Image Manager Tasks for Default Roles

	Tasks		
Role	**Launch and View**	**Add Images to Repository**	**Create Image Upgrade Jobs**
Help Desk	Yes	No	No
Approver	Yes	No	No
Network Operator	Yes	No	No
Network Administrator	Yes	Yes	Yes
System Administrator	Yes	Yes	Yes
Security Administrator	Yes	No	No

For details about which Security Manager permissions are associated with each CiscoWorks role, see Default Associations Between Permissions and Roles in Security Manager, page 8-11.

For a detailed series of tables that shows the RBAC permissions matrix for Image Manager, see Appendix B, "Permissions Matrix for Image Manager."

Tips

- Additional roles, such as Export Data, might be displayed in Common Services if additional applications are installed on the server. The Export Data role is for third-party developers and is not used by Security Manager.
- Although you cannot change the definition of CiscoWorks roles, you can define which roles are assigned to each user. For more information, see Selecting an Authorization Type and Assigning Roles to Users in Common Services, page 8-7.
- To generate a permissions table in CiscoWorks, select **Server > Reports > Permission** and click **Generate Report**.

Selecting an Authorization Type and Assigning Roles to Users in Common Services

In CiscoWorks Common Services 4.2.2, the Local User Setup > Add page is used (1) to select one of the three authorization types that are available for local users and (2) to assign roles to users. The three authorization types are the following:

- Full Authorization
- Enable Task Authorization

- Enable Device Authorization

You must select one of these three authorization types (Full Authorization, Enable Task Authorization, or Enable Device Authorization) when you add a local user in Common Services.

Selecting any of these three authorization types enables you to select the roles that the local user should have. Selecting the roles that the local user should have is important because it defines the operations that the user is authorized to perform.

For example, if you select the Help Desk role, the user is limited to view operations and cannot modify any data. For another example, if you assign the Network Operator role, the user is also able to modify the configuration archive. You can assign more than one role to a particular user.

By default the Help Desk role is enabled. You can also clear default roles, and you can set any roles to be default roles.

Tip You must restart the Security Manager client after making changes to user permissions.

Related Topics

- Security Manager ACS Permissions, page 8-4
- Default Associations Between Permissions and Roles in Security Manager, page 8-11
- Understanding CiscoWorks Roles, page 8-6

Step 1 Navigate to the Local User Setup page in Common Services by following this path:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

admin account login (or user account with sufficient privileges) >

Server Administration >

Server > [menu selector symbol] >

Security >

Single-Server Management >

Local User Setup

Step 2 Do one of the following:

- To create a user, click **Add** and enter the appropriate information in the following fields: Username, Password, Verify Password, and Email.
- To change the authorizations of an existing user, check the check box next to the username and click **Edit**.

Step 3 Select **Full Authorization** if you want the user to have all the roles (Help Desk, Approver, Network Operator, Network Administrator, System Administrator, Super Admin, Security Administrator, and Security Approver) that are available in Security Manager.

Tip If you select **Full Authorization**, you cannot also select **Enable Task Authorization** or **Enable Device Authorization** (as indicated by the radio button format).

Skip to Step 6 in this procedure.

Step 4 Select **Enable Task Authorization** if you want the new user to have only roles that you select (such as Network Operator only).

Tip If you select **Enable Task Authorization**, you cannot also select **Full Authorization** or **Enable Device Authorization** (as indicated by the radio button format).

a. Select one or more of the following roles: Help Desk, Approver, Network Operator, Network Administrator, System Administrator, Super Admin, Security Administrator, and Security Approver. For more information about each role, see CiscoWorks Common Services Default Roles, page 8-6.

b. Skip to Step 8 in this procedure.

Step 5 Select **Enable Device Authorization** if you want the new user to be authorized only for device groups that you select, not all of the device groups that are present in your Security Manager installation. (You can define device groups on the Device Groups page at Security Manager > Tools > Security Manager Administration > Device Groups.)

Tip If you select **Enable Device Authorization**, you cannot also select **Full Authorization** or **Enable Task Authorization** (as indicated by the radio button format).

a. Select the device group(s) that you want the new user to be authorized for.

b. Select one or more of the following roles: Help Desk, Approver, Network Operator, Network Administrator, System Administrator, Super Admin, Security Administrator, and Security Approver. For more information about each role, see CiscoWorks Common Services Default Roles, page 8-6.

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

Step 7 Restart the Security Manager client.

Understanding Cisco Secure ACS Roles

Prior to Common Services 4.0 (used with Security Manager 4.3 and 4.4) and Common Services 4.2.2 (used with Security Manager from version 4.5 to version 4.18), Cisco Secure ACS provided greater flexibility than Common Services for managing Security Manager permissions because it (ACS) supported application-specific roles (effectively “role-based access control,” or RBAC).

These granular privileges (RBAC) are available in Common Services 4.0 and 4.2.2, in which local RBAC is available without the use of ACS. Each role is made up of a set of permissions that determine the level of authorization to Security Manager tasks. In Cisco Secure ACS, you assign a role to each user group (and optionally, to individual users as well), which enables each user in that group to perform the operations authorized by the permissions defined for that role.

In addition, you can assign these roles to Cisco Secure ACS device groups, allowing permissions to be differentiated on different sets of devices.

Note Cisco Secure ACS device groups are independent of Security Manager device groups.

The following topics describe Cisco Secure ACS roles:

- Cisco Secure ACS Default Roles, page 8-10
- Customizing Cisco Secure ACS Roles, page 8-10

Cisco Secure ACS Default Roles

Cisco Secure ACS includes the same roles as CiscoWorks (see Understanding CiscoWorks Roles, page 8-6), plus these additional roles:

- **Security Approver**—Security approvers can view (but not modify) devices, policies, objects, maps, CLI commands, and administrative settings. In addition, security approvers can approve or reject the configuration changes contained in an activity.
- **Security Administrator**—In addition to having view permissions, security administrators can modify devices, device groups, policies, objects, and topology maps. They can also assign policies to devices and VPN topologies, and perform discovery to import new devices into the system.
- **Network Administrator**—In addition to view permissions, network administrators can modify the configuration archive, perform deployment, and issue commands to devices.

Note The permissions contained in the Cisco Secure ACS network administrator role are different from those contained in the CiscoWorks network administrator role. For more information, see Understanding CiscoWorks Roles, page 8-6.

Unlike CiscoWorks, Cisco Secure ACS enables you to customize the permissions associated with each Security Manager role. For more information about modifying the default roles, see Customizing Cisco Secure ACS Roles, page 8-10.

For details about which Security Manager permissions are associated with each Cisco Secure ACS role, see Default Associations Between Permissions and Roles in Security Manager, page 8-11.

Related Topics

- Integrating Security Manager with Cisco Secure ACS, page 8-12
- User Permissions, page 8-3

Customizing Cisco Secure ACS Roles

Cisco Secure ACS enables you to modify the permissions associated with each Security Manager role. You can also customize Cisco Secure ACS by creating specialized user roles with permissions that are targeted to particular Security Manager tasks.

Note You must restart Security Manager after making changes to user permissions.

Related Topics

- Security Manager ACS Permissions, page 8-4
- Default Associations Between Permissions and Roles in Security Manager, page 8-11

Step 1 In Cisco Secure ACS, click **Shared Profile Components** on the navigation bar.

Step 2 Click **Cisco Security Manager** on the Shared Components page. The roles that are configured for Security Manager are displayed.

Step 3 Do one of the following:

- To create a role, click **Add**. Enter a name for the role and, optionally, a description.
- To modify an existing role, click the role.

Step 4 Check and uncheck the check boxes in the permissions tree to define the permissions for this role.

Checking the check box for a branch of the tree selects all permissions in that branch. For example, selecting the **Assign** checkbox selects all the assign permissions.

Descriptions of the individual permissions are included in the window. For additional information, see Security Manager ACS Permissions, page 8-4.

Tip When you select modify, approve, assign, import, control or deploy permissions, you must also select the corresponding view permissions; otherwise, Security Manager does not function properly.

Step 5 Click **Submit** to save your changes.

Step 6 Restart Security Manager.

Default Associations Between Permissions and Roles in Security Manager

Table 8-2 shows how Security Manager permissions are associated with CiscoWorks Common Services roles and the default roles in Cisco Secure ACS. Some roles (Super Admin, Security Administrator, and Security Approver) are not listed because they are not specifically associated with the default roles in Cisco Secure ACS. For information about the specific permissions, see Security Manager ACS Permissions, page 8-4.

Table 8-2 Default Permission to Role Associations in Security Manager and CiscoWorks Common Services

	Roles						
Permissions	**System Admin.**	**Security Admin.**	**Security Approver**	**Network Admin.**	**Approver**	**Network Operator**	**Help Desk**
View Permissions							
View Device	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Policy	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Objects	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Topology	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View CLI	Yes	Yes	Yes	Yes	Yes	Yes	No
View Admin	Yes	Yes	Yes	Yes	Yes	Yes	No
View Config Archive	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View Device Managers	Yes	Yes	Yes	Yes	Yes	Yes	No
Modify Permissions							
Modify Device	Yes	Yes	No	No	No	No	No
Modify Hierarchy	Yes	Yes	No	No	No	No	No

Table 8-2 Default Permission to Role Associations in Security Manager and CiscoWorks Common Services

	Roles						
Permissions	**System Admin.**	**Security Admin.**	**Security Approver**	**Network Admin.**	**Approver**	**Network Operator**	**Help Desk**
Modify Policy	Yes	Yes	No	No	No	No	No
Modify Image	Yes	Yes	No	No	No	No	No
Modify Objects	Yes	Yes	No	No	No	No	No
Modify Topology	Yes	Yes	No	No	No	No	No
Modify Admin	Yes	No	No	No	No	No	No
Modify Config Archive	Yes	Yes	No	Yes	No	Yes	No
Additional Permissions							
Assign Policy	Yes	Yes	No	No	No	No	No
Approve Policy	Yes	No	Yes	No	No	No	No
Approve CLI	Yes	No	No	No	Yes	No	No
Discover (Import)	Yes	Yes	No	No	No	No	No
Deploy	Yes	No	No	Yes	No	No	No
Control	Yes	No	No	Yes	No	Yes	No
Submit	Yes	Yes	No	No	No	No	No

Integrating Security Manager with Cisco Secure ACS

This section describes how to integrate your Cisco Secure ACS with Cisco Security Manager.

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

Cisco Secure ACS uses TACACS+ to communicate with management applications. For Security Manager to communicate with Cisco Secure ACS, you must configure the CiscoWorks server in Cisco Secure ACS as a AAA client that uses TACACS+. In addition, you must provide the CiscoWorks server with (1) the administrator name and password that you use to log in to the Cisco Secure ACS and (2) the shared key configured in ACS on external user addition. Fulfilling these requirements ensures the validity of communications between Security Manager and Cisco Secure ACS.

Note For an understanding of TACACS+ security advantages, see *User Guide for Cisco Secure Access Control Server*.

When 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 Security Manager role and apply these roles to users and user groups.

The following topics describe how to use Cisco Secure ACS with Security Manager:

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14
- Integration Procedures Performed in Cisco Secure ACS, page 8-15
- Integration Procedures Performed in CiscoWorks, page 8-21
- Restarting the Daemon Manager, page 8-25
- Assigning Roles to User Groups in Cisco Secure ACS, page 8-25

ACS Integration Requirements

To use Cisco Secure ACS, make sure that the following steps are completed:

- You defined roles that include the permissions required to perform necessary functions in 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 Security Manager. This restriction applies to the display names, not the hostnames defined on the devices. ACS naming restrictions can be more limiting than those for Security Manager, so you should define the device in ACS first.
- There are additional device display name requirements that you must meet for ASA security contexts devices. These are described in Adding Devices as AAA Clients Without NDGs, page 8-17.
- Network Device Groups must be enabled.

Tips

- If you already have devices imported into Security Manager prior to ACS integration, we recommend adding those devices to ACS as AAA clients before the integration. The name of the AAA client must match the display name of the device in Cisco Security Manager. If you do not do so, the devices will not show up in the Device list of Security Manager after the ACS integration.
- We highly recommend that you create a fault-tolerant infrastructure that utilizes multiple Cisco Secure ACS servers. Having multiple servers helps to ensure your ability to continue work in Security Manager even if connectivity is lost to one of the ACS servers.
- You can integrate only one version of Security Manager with a Cisco Secure ACS. Therefore, if your organization is using two different versions of Security Manager at the same time, you must perform integration with two different Cisco Secure ACS servers. You can, however, upgrade to a new version of Security Manager without having to use a different ACS.
- Even when Cisco Secure ACS authentication is used, CiscoWorks Common Services software uses local authorization for CiscoWorks Common Services-specific utilities, such as Compact Database and Database Checkpoint. To use these utilities, you must be defined locally and be assigned the appropriate permissions.

Related Topics

- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14
- Integrating Security Manager with Cisco Secure ACS, page 8-12

Procedural Overview for Initial Cisco Secure ACS Setup

The following procedure summarizes the overall tasks you need to perform to use Cisco Secure ACS with Security Manager. The procedure contains references to more specific procedures used to perform each step.

Related Topics

- ACS Integration Requirements, page 8-13
- Integrating Security Manager with Cisco Secure ACS, page 8-12

Step 1 **Plan your administrative authentication and authorization model.**

You should decide on your administrative model before using Security Manager. This includes defining the administrative roles and accounts that you plan to use.

Tip When defining the roles and permissions of potential administrators, you should also consider whether to enable Workflow. This selection affects how you can restrict access.

For more information, see the following:

- Understanding Cisco Secure ACS Roles, page 8-9
- *User Guide for Cisco Security Manager*
- *User Guide for Cisco Secure Access Control Server*

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

Install Cisco Secure ACS. Install CiscoWorks Common Services and Cisco Security Manager on a different server. Do not run Cisco Secure ACS and Security Manager on the same server.

For more information, see the following:

- *Release Notes for Cisco Security Manager* (for information on the supported versions of Cisco Secure ACS)
- Installing Security Manager Server, Common Services, and AUS, page 5-3
- *Installation Guide for Cisco Secure ACS for Windows Server*

Step 3 **Perform integration procedures in Cisco Secure ACS.**

Define 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.

For more information, see Integration Procedures Performed in Cisco Secure ACS, page 8-15.

Step 4 **Perform integration procedures in CiscoWorks Common Services.**

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

For more information, see Integration Procedures Performed in CiscoWorks, page 8-21.

Step 5 **Restart the Daemon Manager.**

You must restart the Security Manager server Daemon Manager for the AAA settings you configured to take effect.

For more information, see Restarting the Daemon Manager, page 8-25.

Step 6 **Assign roles to user groups in Cisco Secure ACS.**

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

For more information, see Assigning Roles to User Groups in Cisco Secure ACS, page 8-25.

Integration Procedures Performed in Cisco Secure ACS

The following topics describe the procedures to perform in Cisco Secure ACS when integrating it with Cisco Security Manager. Perform the tasks in the listed order. For more information about the procedures described in these sections, see *User Guide for Cisco Secure Access Control Server*.

1. Defining Users and User Groups in Cisco Secure ACS, page 8-15
2. Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 8-17
3. Creating an Administration Control User in Cisco Secure ACS, page 8-20

Defining Users and User Groups in Cisco Secure ACS

All users of 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, assigning all the system administrators to one group, all the network operators to another group, and so on. For more information about the default roles in ACS, see Cisco Secure ACS Default Roles, page 8-10.

You must create an additional user that is assigned the system administrator role with full permissions to devices. The credentials established for this user are later used on the System Identity Setup page in CiscoWorks. See Defining the System Identity User, page 8-22.

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

Tip This procedure explains how to create user accounts during the initial Cisco Secure ACS integration. After you complete the integration, when you create a user account, you can assign it to the appropriate group as you create the account.

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14
- Assigning Roles to User Groups in Cisco Secure ACS, page 8-25

Step 1 Log in to Cisco Secure ACS.

Step 2 Configure a user with full permissions using the following procedure. For more information about the options available when configuring users and user groups, see *User Guide for Cisco Secure Access Control Server*.

a. Click **User Setup** on the navigation bar.

b. On the User Setup page, enter a name for the new user and click **Add/Edit**.

Tip Do not create a user named **admin**. The admin user is the fall-back user in Security Manager. If the ACS system stops working for some reason, you can still log in to CiscoWorks Common Services on the Security Manager server using the admin account to change the AAA mode to CiscoWorks local authentication and continue using the product.

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 should be assigned.

f. Click **Submit** to create the user account.

Step 3 Repeat this process for each Security Manager user. We recommend dividing the users into groups based on the role each user will be 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

For more information about the default permissions associated with each role, see Default Associations Between Permissions and Roles in Security Manager, page 8-11. For more information about customizing user roles, see Customizing Cisco Secure ACS Roles, page 8-10.

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 Assigning Roles to User Groups in Cisco Secure ACS, page 8-25.

Step 4 Create an additional user that you will use as the system identity user in CiscoWorks Common Services. Assign this user to the system administrators group and grant all privileges to devices. The credentials established for this user are later used on the System Identity Setup page in CiscoWorks. See Defining the System Identity User, page 8-22.

Step 5 Continue with Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 8-17.

Adding Managed Devices as AAA Clients in Cisco Secure ACS

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

If Security Manager is managing security contexts configured on firewall devices, each context must be added individually to Cisco Secure ACS.

The method for adding managed devices depends on whether you want to restrict users to managing a particular set of devices by creating network device groups (NDGs). Proceed as follows:

- If you want users to have access only to certain NDGs, add the devices as described in Configuring Network Device Groups for Use in Security Manager, page 8-18.

Note While devices do not need to be broken out into Network Device Groups, Security Manager expects the Security Manager Network Device to be in an NDG. "Not Assigned" is not an NDG. It is best to move all devices out of Not Assigned and into a Default NDG if multiple NDGs are not desired.

Adding Devices as AAA Clients Without NDGs

This procedure describes how to add devices as AAA clients of a Cisco Secure ACS. For complete information about all available options, see *User Guide for Cisco Secure Access Control Server*.

Tip Remember to add the CiscoWorks/Security Manager server as a AAA client.

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

Step 1 Click **Network Configuration** on the Cisco Secure ACS navigation bar.

Step 2 Click **Add Entry** beneath the AAA Clients table.

Step 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 Security Manager.

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

When naming the CiscoWorks server, we recommend using the fully qualified hostname. Be sure to spell the hostname correctly. (The hostname is not case sensitive.)

Additional naming conventions include the ASA security context:
<parent_display_name>_<context_name>

Step 4 Enter the IP address of the network device in the AAA Client IP Address field. If the device does not have an IP address (for example, a virtual sensor or a virtual context), enter the word **dynamic** instead of an address.

Note If you are adding a multi-homed device (a device with multiple NICs), enter the IP address of each NIC. Press **Enter** between each address. In addition, you must modify the gatekeeper.cfg file on the Security Manager server.

Step 5 Enter the shared secret in the Key field.

Step 6 Select **TACACS+ (Cisco IOS)** from the Authenticate Using list.

Step 7 Click **Submit** to save your changes. The device you added is displayed in the AAA Clients table.

Step 8 Repeat the process to add additional devices.

Step 9 To save the devices you have added, click **Submit + Restart**.

Step 10 Continue with Creating an Administration Control User in Cisco Secure ACS, page 8-20.

Configuring 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 Security Manager, NDGs enable you to provide users with different levels of permissions, depending on the devices they need to manage. For example, by using 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.

Tips

- Each device can be a member of only one NDG.
- NDGs are *not* related to the device groups that you can configure in Security Manager.
- For complete details about managing NDGs, see *User Guide for Cisco Secure Access Control Server*.

The following topics outline the basic information and steps for configuring NDGs:

- NDGs and User Permissions, page 8-18
- Activating the NDG Feature, page 8-19
- Creating NDGs, page 8-19
- Associating NDGs and Roles with User Groups, page 8-26

NDGs and User Permissions

Because NDGs limit users to particular sets of devices, they affect policy permissions, as follows:

- To view a policy, you must have permissions for at least *one* device to which the policy is assigned.
- To modify a policy, you must have permissions for *all* the devices to which the policy is assigned.
- To view, modify, or assign a VPN policy, you must have permissions for *all* the devices in the VPN topology.

- To assign a policy to a device, you need permissions only for that device, regardless of whether you have permissions for any other devices to which the policy is assigned. (VPN policies are an exception, as noted above.) However, if a user assigns a policy to a device for which you do not have permissions, you cannot modify that policy.

Note To modify an object, a user does *not* need modify permissions for all the devices that are using the object. However, a user must have modify permissions for a particular device in order to modify a device-level object override defined on that device.

Related Topics

- Configuring Network Device Groups for Use in Security Manager, page 8-18
- User Permissions, page 8-3

Activating the NDG Feature

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

Related Topics

- Creating NDGs, page 8-19
- Associating NDGs and Roles with User Groups, page 8-26
- NDGs and User Permissions, page 8-18
- Configuring Network Device Groups for Use in Security Manager, page 8-18

Step 1 Click **Interface Configuration** on the Cisco Secure ACS navigation bar.

Step 2 Click **Advanced Options**.

Step 3 Scroll down, then check the **Network Device Groups** check box.

Step 4 Click **Submit**.

Step 5 Continue with Creating NDGs, page 8-19.

Creating NDGs

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

Tip We highly recommend creating a special NDG that contains the CiscoWorks/Security Manager servers.

Before You Begin

Activate the NDG feature as described in Activating the NDG Feature, page 8-19.

Related Topics

- Associating NDGs and Roles with User Groups, page 8-26
- NDGs and User Permissions, page 8-18
- Configuring Network Device Groups for Use in Security Manager, page 8-18

Step 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. Please note that Not Assigned is *not* an NDG.

Step 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) Enter a key to be used by all 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** to save the NDG.

e. Repeat the process to create more NDGs.

Step 3 Populate the NDGs with devices. Keep in mind that each device can be a member of only one NDG.

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**. For more information, see Adding Devices as AAA Clients Without NDGs, page 8-17.

d. Repeat the process to add the remaining devices to NDGs. The only device you should consider leaving in the Not Assigned category is the default AAA server.

e. After you configure the last device, click **Submit + Restart**.

Step 4 Continue with Creating an Administration Control User in Cisco Secure ACS, page 8-20.

Tip You can associate roles with each NDG only after completing the integration procedures in Cisco Secure ACS and CiscoWorks Common Services. See Associating NDGs and Roles with User Groups, page 8-26.

Creating an Administration Control User in Cisco Secure ACS

Use the Administration Control page in Cisco Secure ACS to define the administrator account that is used when defining the AAA setup mode in CiscoWorks Common Services. Security Manager uses this account to access the ACS server and register the application, to query device group membership and group setup, and to perform other basic interactions with ACS. For more information, see Configuring the AAA Setup Mode in CiscoWorks, page 8-23.

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

Step 1 Click **Administration Control** on the Cisco Secure ACS navigation bar.

Step 2 Click **Add Administrator**.

Step 3 On the Add Administrator page, enter a name and password for the administrator.

Step 4 Select the following administrator privileges:

- Under Users and Group Setup
  - Read access to users in group
  - Read access of these groups
- Under Shared Profile Components
  - Create Device Command Set Type
- Network Configuration

Step 5 Click **Submit** to create the administrator. For more information about the options available when configuring an administrator, see *User Guide for Cisco Secure Access Control Server*.

Integration Procedures Performed in CiscoWorks

After you complete the integration tasks in Cisco Secure ACS (described in Integration Procedures Performed in Cisco Secure ACS, page 8-15), you must complete some tasks in CiscoWorks Common Services. Common Services performs the actual registration of any installed applications, such as Cisco Security Manager and Auto Update Server, into Cisco Secure ACS.

The following topics describe the procedures to perform in CiscoWorks Common Services when integrating it with Cisco Security Manager:

- Creating a Local User in CiscoWorks, page 8-21
- Defining the System Identity User, page 8-22
- Configuring the AAA Setup Mode in CiscoWorks, page 8-23
- Configuring an SMTP Server and System Administrator Email Address for ACS Status Notifications, page 8-24

Creating a Local User in CiscoWorks

Use the Local User Setup page in CiscoWorks Common Services to create a local user account that duplicates the system identity user you previously created in Cisco Secure ACS (as described in Defining Users and User Groups in Cisco Secure ACS, page 8-15). This local user account is later used for the system identity setup. For more information, see Defining the System Identity User, page 8-22.

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

Step 1 Navigate to the Local User Setup page in Common Services by following this path:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

admin account login >

Server Administration >

Server > [menu selector symbol] >

Security >

Single-Server Management >

Local User Setup

Step 2 Click **Add**.

Step 3 Enter the same name and password that you entered when creating the system identity user in Cisco Secure ACS. See Defining Users and User Groups in Cisco Secure ACS, page 8-15.

Step 4 Check all check boxes under Roles.

Step 5 Click **OK** to create the user.

Defining the System Identity User

Use the System Identity Setup page in CiscoWorks Common Services to create a trust user (called 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 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 to perform a subtask when the primary task has already been authorized for the logged in user.

The System Identity user you configure here must also be defined as a local user in CiscoWorks (assigned to all roles) and as a user with all privileges to devices in ACS. If you do not select a user with the required privileges, you might not be able to view all the devices and policies configured in Security Manager. Make sure that you performed the following procedures before continuing:

- Defining Users and User Groups in Cisco Secure ACS, page 8-15
- Creating a Local User in CiscoWorks, page 8-21

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

Step 1 Navigate to the System Identify Setup page in Common Services by following this path:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

admin account login >

Server Administration >

Server > [menu selector symbol] >

Security >

Multi-Server Trust Management >

System Identity Setup

Step 2 Enter the name of the system identity user that you created in Cisco Secure ACS. See Defining Users and User Groups in Cisco Secure ACS, page 8-15.

Step 3 Enter and verify the password for this user.

Step 4 Click **Apply**.

Configuring the AAA Setup Mode in CiscoWorks

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

This procedure performs the actual registration of CiscoWorks and Security Manager (and optionally, Auto Update Server) into Cisco Secure ACS.

Tip 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 re-installation. Therefore, if you upgrade to a new version of either application, you must reconfigure the AAA setup mode and re-register 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 re-register the new applications and Cisco Security Manager. In addition to re registering Security Manager with ACS, you must configure your existing system identity user and grant it the newly introduced permissions; otherwise, RBAC will not work properly. Please refer to Defining the System Identity User, page 8-22.

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

Step 1 Navigate to the AAA Mode Setup page in Common Services by following this path:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

admin account login >

Server Administration >

Server > [menu selector symbol] >

Security >

AAA Mode Setup

Step 2 Select **TACACS+** under Available Login Modules.

Step 3 Select **ACS** as the AAA type.

Step 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. All servers must be running the same version of Cisco Secure ACS.

Note If all the configured TACACS+ servers fail to respond, you must log in using 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.

Step 5 In the Login area, enter the name of the administrator that you defined on the Administration Control page of Cisco Secure ACS. For more information, see Creating an Administration Control User in Cisco Secure ACS, page 8-20.

Step 6 Enter and verify the password for this administrator.

Step 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 Adding Devices as AAA Clients Without NDGs, page 8-17.

Step 8 Check the **Register all installed applications with ACS** check box to register Security Manager and any other installed applications with Cisco Secure ACS.

Step 9 Click **Apply** to save your settings. A progress bar displays the progress of the registration. A message is displayed when registration is complete.

Step 10 Restart the Cisco Security Manager Daemon Manager service. See Restarting the Daemon Manager, page 8-25.

Step 11 Log back in to Cisco Secure ACS to assign roles to each user group. See Assigning Roles to User Groups in Cisco Secure ACS, page 8-25.

Configuring an SMTP Server and System Administrator Email Address for ACS Status Notifications

If all the ACS servers become unavailable, users cannot perform tasks in Security Manager. Users who are logged in can be abruptly logged out of the system (without an opportunity to save changes) if they try to perform a task that requires ACS authorization.

If you configure Common Services settings to identify an SMTP server and a system administrator, Security Manager sends an email message to the administrator if all ACS servers become unavailable. This can alert you to a problem that needs immediate attention. The administrator might also receive email messages from Common Services for non-ACS-related events.

Tip Security Manager can send email notifications for several other types of events such as deployment job completion, activity approval, or ACL rule expiration. The SMTP server you configure here is also used for these notifications, although the sender email address is set in Security Manager. For more information about configuring these other email addresses, see the *User Guide for Cisco Security Manager* for this version of the product, or the client online help.

Step 1 Navigate to the System Preferences page in Common Services by following this path:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

admin account login >

Server Administration >

Server > [menu selector symbol] >

Admin >

System Preferences

Step 2 On the System Preferences page, enter the hostname or IP address of an SMTP server that Security Manager can use. The SMTP server cannot require user authentication for sending email messages.

Step 3 Enter an email address that CiscoWorks can use for sending emails. This does not have to be the same email address that you configure for Security Manager to use when sending notifications.

If the ACS server becomes unavailable, a message is sent to (and from) this account.

Step 4 Click **Apply** to save your changes.

Restarting the Daemon Manager

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

Related Topics

- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14
- ACS Integration Requirements, page 8-13

Step 1 Log in to the machine on which the Security Manager server is installed.

Step 2 Select **Start > Programs > Administrative Tools > Services** to open the Services window.

Step 3 From the list of services displayed in the right pane, select **Cisco Security Manager Daemon Manager**.

Step 4 Click the **Restart Service** button on the toolbar.

Step 5 Continue with Assigning Roles to User Groups in Cisco Secure ACS, page 8-25.

Assigning Roles to User Groups in Cisco Secure ACS

After you have registered CiscoWorks, 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 Security Manager.

The procedure for assigning roles to user groups depends on whether NDGs are being used:

- Assigning Roles to User Groups Without NDGs, page 8-25
- Associating NDGs and Roles with User Groups, page 8-26

Note Cisco Security Manager and ACS integration works better by creating a special NDG that contains the CiscoWorks/Security Manager servers.

Assigning Roles to User Groups Without NDGs

This procedure describes how to assign the default roles to user groups when NDGs have not been defined. For more information, see Cisco Secure ACS Default Roles, page 8-10.

Before You Begin

- Create a user group for each default role. See Defining Users and User Groups in Cisco Secure ACS, page 8-15.
- Complete the procedures described in these topics:
  - Integration Procedures Performed in Cisco Secure ACS, page 8-15
  - Integration Procedures Performed in CiscoWorks, page 8-21

Related Topics

- Understanding CiscoWorks Roles, page 8-6
- Understanding Cisco Secure ACS Roles, page 8-9

Step 1 Log in to Cisco Secure ACS.

Step 2 Click **Group Setup** on the navigation bar.

Step 3 Select the user group for system administrators from the list (see Defining Users and User Groups in Cisco Secure ACS, page 8-15), then click **Edit Settings**.

Tip You can rename the groups with a more meaningful name to make it easier to identify the correct groups. Select a group and click **Rename Group** to change the name.

Step 4 Assign the system administrator role to this group:

a. Scroll down to the CiscoWorks area under TACACS+ Settings.

b. Select the first **Assign** option, then select **System Administrator** from the list of CiscoWorks roles.

c. Scroll down to the Cisco Security Manager Shared Services area.

d. Select the first **Assign** option, then select **System Administrator** from the list of Cisco Secure ACS roles.

e. Click **Submit** to save the group settings.

Step 5 Repeat the process for the remaining roles, assigning each role to the appropriate user group.

When selecting the Security Approver or Security Administrator roles in Cisco Secure ACS, we recommend selecting Network Administrator as the closest equivalent CiscoWorks role.

For more information about customizing the default roles in ACS, see Customizing Cisco Secure ACS Roles, page 8-10.

Associating NDGs and Roles with User Groups

When you associate NDGs with roles for use in 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 should match as closely as possible. When associating 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 that will be used with Security Manager. For example, if you have a user group containing support personnel for the Western region, you can select that user group, then associate the NDG containing the devices in that region with the Help Desk role.

Before You Begin

Activate the NDG feature and create NDGs. See Configuring Network Device Groups for Use in Security Manager, page 8-18.

Related Topics

- ACS Integration Requirements, page 8-13
- Procedural Overview for Initial Cisco Secure ACS Setup, page 8-14

Step 1 Click **Group Setup** on the navigation bar.

Step 2 Select a user group from the Group list, then click **Edit Settings**.

Tip You can rename the groups with a more meaningful name to make it easier to identify the correct groups. Select a group and click **Rename Group** to change the name.

Step 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 should be associated from the second list.
e. Click **Add Association**. The association appears in the Device Group box.
f. Repeat the process to create additional associations.
g. To remove an association, select it from the Device Group, then click **Remove Association**.

Step 4 Map NDGs and roles for use in Cisco Security Manager; you should create associations that match as closely as possible the associations defined in the previous step:

a. On the Group Setup page, scroll down to the Cisco Security Manager area under TACACS+ Settings.
b. Select **Assign a Cisco Security Manager on a per Network Device Group Basis**.
c. Select an NDG from the Device Group list.
d. Select the role to which this NDG should be associated from the second list.
e. Click **Add Association**. The association appears in the Device Group box.
f. Repeat the process to create additional associations.

Note When you are selecting the Security Approver or Security Administrator roles in Cisco Secure ACS, we recommend selecting Network Administrator as the closest equivalent CiscoWorks role.

Note CiscoWorks Common Services has a default role called "Network Administrator." Cisco Secure ACS has a default role called "Network Admin." These roles are not identical; they differ for a few of the permissions in Cisco Security Manager.

Step 5 Click **Submit** to save your settings.

Step 6 Repeat the process to define NDGs for the remaining user groups.

Step 7 To save the associations that you have created, click **Submit + Restart**.

For more information about customizing the default roles in ACS, see Customizing Cisco Secure ACS Roles, page 8-10.

Troubleshooting Security Manager-ACS Interactions

This following topics describe how to troubleshoot common problems that could occur because of how Security Manager and Cisco Secure ACS interact:

- Using Multiple Versions of Security Manager with Same ACS, page 8-28
- Authentication Fails When in ACS Mode, page 8-29
- System Administrator Granted Read-Only Access, page 8-29
- ACS Changes Not Appearing in Security Manager, page 8-30
- Devices Configured in ACS Not Appearing in Security Manager, page 8-30
- Working in Security Manager after Cisco Secure ACS Becomes Unreachable, page 8-30
- Restoring Access to Cisco Secure ACS, page 8-31
- Authentication Problems with Multihomed Devices, page 8-31
- Authentication Problems with Devices Behind a NAT Boundary, page 8-31

Using Multiple Versions of Security Manager with Same ACS

You cannot use the same Cisco Secure ACS with two different versions of Security Manager. For example, if you have integrated Security Manager 3.3.1 with a Cisco Secure ACS and another part of your organization plans to use Security Manager 4.0.1 *without* upgrading the existing installation, you must integrate Security Manager 4.0.1 with a different ACS than the one used for Security Manager 3.3.1.

If you upgrade an existing Security Manager installation, you can continue to use the same Cisco Secure ACS. The permission settings are updated as required.

Authentication Fails When in ACS Mode

If authentication keeps failing when you log in to Security Manager or CiscoWorks Common Services, even though you used Common Services to configure Cisco Secure ACS as the AAA server for authentication, do the following:

- Ensure that there is connectivity between the ACS servers and the server running Common Services and Security Manager.
- Ensure that the user credentials (username and password) you are using are defined in ACS and are assigned to the appropriate user group.
- Ensure that the Common Services server is defined as a AAA client on the Network Configuration page of ACS. Verify that the shared secret keys defined in Common Services (AAA Mode Setup page) and ACS (Network Configuration) match.
- Ensure that the IP address of each ACS server is correctly defined on the AAA Mode Setup page in Common Services.
- Ensure that the correct account is defined on the Administration Control page of ACS.
- Go to the AAA Mode Setup page in Common Services and verify that Common Services and Security Manager (as well as any other installed applications, such as AUS) are registered with Cisco Secure ACS.
- Go to Administration Control > Access Setup in ACS and ensure that the ACS is configured for HTTPS communication.
- If you receive “key mismatch” errors in the ACS log, verify whether the Security Manager server is defined as a member of a network device group (NDG). If it is, be aware that if you defined a key for the NDG, that key takes precedence over the keys defined for the individual devices in the NDG, including the Security Manager server. Ensure that the key defined for the NDG matches the secret key of the Security Manager server.

System Administrator Granted Read-Only Access

If you have read-only access to all policy pages of Security Manager even after logging in as a System Administrator with full permissions, do the following in Cisco Secure ACS:

- (When using network device groups (NDGs)) Click **Group Setup** on the Cisco Secure ACS navigation bar, then verify that the System Administrator user role is associated with all necessary correct NDGs for *both* CiscoWorks and Cisco Security Manager, especially the NDG containing the Common Services/Security Manager server.
- Click **Network Configuration** on the navigation bar, then do the following:
  - Verify that the Common Services/Security Manager server is not assigned to the Not Assigned (default) group.
  - Verify that the Common Services/Security Manager server is configured to use TACACS+ not RADIUS. TACACS+ is the only security protocol supported between the two servers.

Note You can configure the network devices (routers, firewalls, and so on) managed by Security Manager for either TACACS+ or RADIUS.

ACS Changes Not Appearing in Security Manager

When you are using Security Manager with Cisco Secure ACS 4.x, information from ACS is cached when you log in to Security Manager or CiscoWorks Common Services on the Security Manager server. If you make changes in the Cisco Secure ACS Network Configuration and Group Setup while logged in to Security Manager, the changes might not appear immediately or be immediately effective in Security Manager. You must log out of Security Manager and Common Services and close their windows, then log in again, to refresh the information from ACS.

If you need to make changes in ACS, it is best practice to first log out of and close Security Manager windows, make your changes, and then log back in to the product.

Note Although Cisco Secure ACS 3.3 is not supported, if you are using that version of ACS, you must open Windows Services and restart the Cisco Security Manager Daemon Manager service to get the ACS changes to appear in Security Manager.

Devices Configured in ACS Not Appearing in Security Manager

If the devices that you configured on the Cisco Secure ACS are not appearing in Security Manager, it is probably a problem with the device display name.

The device display names defined in Security Manager *must* match the names you configure in ACS when you add the devices as AAA clients. This is particularly important when you use domain names. If you intend to append a domain name to the device name in Security Manager, the AAA client hostname in ACS must be **<device_name>.<domain_name>**, for example, pixfirewall.cisco.com.

Working in Security Manager after Cisco Secure ACS Becomes Unreachable

Security Manager sessions are affected if the Cisco Secure ACS cannot be reached. Therefore, you should consider creating a fault-tolerant infrastructure that utilizes multiple Cisco Secure ACS servers. Having multiple servers helps to ensure your ability to continue work in Security Manager even if connectivity is lost to one of the ACS servers.

If your setup includes only a single Cisco Secure ACS and you wish to continue working in Security Manager in the event the ACS becomes unreachable, you can switch to performing local AAA authentication on the Security Manager server.

Procedure

To change the AAA mode, follow these steps:

Step 1 Log in to Common Services using the **admin** CiscoWorks local account.

Step 2 Select **Server > Security > AAA Mode Setup**, then change the AAA mode back to Non-ACS/CiscoWorks Local. This enables you to perform authentication and authorization using the local Common Services database and its built-in roles. Bear in mind that you must create local users in the AAA database to make use of local authentication.

Step 3 Click **Change**.

Restoring Access to Cisco Secure ACS

If you cannot access Security Manager because the Cisco Secure ACS is down, do the following:

- Open up Windows Services on the ACS server and check whether the CSTacacs and CSRadius services are up and running. Restart these services if required.
- Perform the following procedure in CiscoWorks Common Services:

Step 1 Log in to Common Services as the **admin** user.

Step 2 Open a DOS window and run *NMSROOT***bin\perl ResetLoginModule.pl**.

Step 3 Exit Common Services, then log in a second time as the **admin** user.

Step 4 Go to **Server > Security > AAA Mode Setup**, then change the AAA mode to Non-ACS > CW Local mode.

Step 5 Open Windows Services and restart the Cisco Security Manager Daemon Manager service.

Authentication Problems with Multihomed Devices

If you cannot configure a multihomed device (a device with multiple network interface cards (NICs)) that was added to the Cisco Secure ACS, even though your user role includes Modify Device permissions, there might be a problem with the way you entered the IP addresses for the device.

When you define a multihomed device as a AAA client of the Cisco Secure ACS, make sure to define the IP address of each NIC. Press **Enter** between each entry. For more information, see Adding Devices as AAA Clients Without NDGs, page 8-17.

Authentication Problems with Devices Behind a NAT Boundary

If you cannot configure a device with a pre-NAT or post-NAT IP address that was added to the Cisco Secure ACS, even though your user role includes Modify Device permissions, there might be a problem with the IP addresses that you configured.

When a device is behind a NAT boundary, make sure to define all IP addresses, including pre-NAT and post-NAT, for the device in the AAA client configuration settings in Cisco Secure ACS. For more information on how to add AAA client settings to ACS, see *User Guide for Cisco Secure Access Control Server*.

Local RBAC Using Common Services 4.2.2

Prior to Security Manager 4.3, the major advantages of using Cisco Secure ACS were (1) the ability to create highly granular user roles with specialized permission sets (for example, allowing the user to configure certain policy types but not others) and (2) the ability to restrict users to certain devices by configuring network device groups (NDGs). These granular privileges (effectively “role-based access control,” or RBAC) were not available in Security Manager 4.2 and earlier versions, unless you used Cisco Secure ACS. These granular privileges (RBAC) are available in Security Manager 4.3 and later because they use Common Services 4.0 or later, in which local RBAC is available without the use of ACS.

Security Manager 4.18 retains compatibility with ACS 4.2. See Integrating Security Manager with Cisco Secure ACS, page 8-12.

Note Users who wish to migrate their RBAC abilities from ACS to Common Services must do so manually; there are no migration scripts or other migration support.

Common Services 4.2.2 provides device-level RBAC, defining custom roles for users, and customizing existing roles for users. The following features are available:

- Managing users (add, remove, edit)
- Managing network device groups (NDGs) to provide device-level RBAC
- Managing custom roles
- Mapping roles to device groups
- Granular privileges for policy object types and policy types, such as “view network objects,” “modify service objects,” and “modify access rules.”

You can implement local RBAC using Common Services 4.2.2 by completing tasks in the following areas:

- Authentication Mode Setup, page 8-32
- User Management, page 8-32
- Group Management, page 8-33
- Role Management, page 8-33

Authentication Mode Setup

Follow the steps to set up a non-ACS account. See Non-ACS Account, page 8-2.

Then select the **CiscoWorks Local** login module.

Tip CiscoWorks Local is the default value for a clean installation of Security Manager.

User Management

Navigate to the Local User Setup page in Common Services:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

user account login >

Server Administration >

Home >

System Tasks >

Local User Setup

On the Local User Setup page, you can select a user and then choose one of the following actions:

- Import Users

- Export Users
- Edit
- Delete
- Add
- Modify My Profile

If you select more than one user, Edit is not available.

If you select no users, you can choose one of the following actions:

- Import Users
- Add
- Modify My Profile

If you select **Edit** or **Add**, you can select one of these three authorization types:

- Full Authorization
- Enable Task Authorization
- Enable Device Authorization

Group Management

Navigate to the Device Groups page in Security Manager:

Server where Security Manager is installed >

desktop icon for Configuration Manager application >

user account login >

Tools >

Security Manager Administration >

Device Groups

You cannot manage device groups through the Common Services interface (Server where Security Manager is installed > desktop icon for Cisco Security Manager application).

Role Management

Navigate to the Role Management Setup page:

Server where Security Manager is installed >

desktop icon for Cisco Security Manager application >

user account login >

Server Administration >

Server > [menu selector symbol] >

Security >

Single-Server Management >

Role Management Setup

The Role Management Setup page displays the default roles, which are Approver, Help Desk, Network Administrator, Network Operator, Security Administrator, Security Approver, Super Admin, and System Administrator. The Role Management Setup page also displays custom roles, if any, that you have added.

On the Role Management page, you can perform the following operations: Add, Edit, Delete, Copy, Export, Import, Set as default, and Clear default.