APPENDIX C

Security Configuration with Cisco Secure ACS

To configure Operations Manager to use Cisco Secure ACS for authentication and authorization, work through these topics in order:

Cisco Secure ACS Support

Operations Manager supports the ACS mode of authentication and authorization. To use this mode, you must have a Cisco Secure Access Control Server (ACS) installed in your network on a server other than the one on which Operations Manager is installed.

For details on supported devices and software, see Supported and Interoperable Devices and Software for Cisco Unified Operations Manager 8.5.

Operations Manager Integration Notes

Operations Manager, Service Monitor, and Common Services all integrate with Cisco Secure ACS as shared profile components. Multiple instances of the same application—for example, Operations Manager—can use the same Cisco Secure ACS server for authentication and authorization.

When you register Cisco Unified Operations Manager, Cisco Unified Service Monitor, and Common Services with Cisco Secure ACS, applications tasks and user roles are imported into Cisco Secure ACS.

You need to register only one instance of an application with Cisco Secure ACS for tasks and roles to be imported. If you register an application a second time, any changes that you have made to role settings, such as creating custom roles, are lost.

CiscoWorks Local Login Module Authentication Roles

Common Services login modules enable you to use a source of authentication other than the native mechanism, the Common Services Local Login Module. You can use the Cisco Secure ACS server for this purpose.

After you authenticate, authorization is controlled by your role. A role is a set of tasks that you have the privilege to perform. By default, the Common Services Local Login Module authorization scheme has five roles.

A sixth role, Super Admin, is available in ACS mode and visible on the Cisco Secure ACS system only. Roles are listed in Table C-1 from least privileged to most privileged.

Table C-1 Common Services User Roles and Privileges

Role	Description
Non-ACS Mode—Common Services Local Login Module	
Help Desk	User with this role has the privileges to view some information in Operations Manager and Common Services. Example: Can search the Alert History database.
Approver	User with this role does not have any privileges. (Operations Manager does not assign any tasks to this user role.)
Network Operator	User with this role has the privilege to perform all Operations Manager tasks and some Common Services tasks. Example: Can configure logging parameters. A user with this role by default can perform the same Operations Manager tasks as a Network Administrator.
Network Administrator	User with this role has the privilege to perform all Operations Manager tasks and several Common Services tasks. User can also perform Network Operator tasks. Example: Can add devices to Operations Manager from the DCR.
System Administrator	User with this role has the privilege to perform all system administration tasks. Example: Enable and disable debugging; set logging level.
ACS Mode	
Super Admin	User with this role has the privilege to perform all tasks when AAA mode is set to ACS and Cisco Secure ACS is used for authentication. You do not see the Super Admin role when you perform local user setup in Common Services. You can assign a user to this role only when you are logged into Cisco Secure ACS and only when your Common Services login module is set to ACS.

For tasks that are defined for Operations Manager and Common Services and the roles with the privilege to perform the tasks, see the Permission Report in Common Services. (Select **Administration > Service Administration (Common Services) > Reports > Permission Report**)

Note For more information, see CiscoWorks Online help.

We recommend that you do not modify the default Common Services roles. However, you can create your own custom roles for Operations Manager on Cisco Secure ACS.

Configuring the System Identity User in Common Services

Before you integrate the Operations Manager server with Cisco Secure ACS, ensure that you create and assign all privileges to a System Identity User in Common Services.

You can set up a local user as the System Identity User. (To use the Common Services admin user as the System Identity User, see the topic Setting up System Identity Account in the Online help for Common Services.

Step 1 Create a local user and assign all roles to this user.

If the System Identity User is not configured with all Common Services Local Login Module roles (see Table C-1), authorization fails when you try perform certain tasks in Operations Manager and Common Services.

Step 2 Update the System Identity User, replacing the username with the one that you created in step 1

To do this, choose **Administration > Service Administration** (**Common Services**) **> Security > Multi-Server Trust Management > System Identity Setup**. For more information, click the Help link.)

For more information, see Online help for Common Services.

Setting Up the Cisco Secure ACS Server

Perform these tasks in Cisco Secure ACS before you change the Common Services AAA mode to ACS:

Step 1 Configure ACS Administrators.

Configure an administrator user with all privileges in Cisco Secure ACS.

If you do not configure the administrator user with all privileges, Operations Manager registration with Cisco Secure ACS fails.

Step 2 Note the username and password for the administrator; you will need to enter them when you change the AAA mode to ACS in Common Services.

Step 3 Add the Operations Manager server to Cisco Secure ACS as an AAA Client.

Step 4 Configure the Operations Manager server as an AAA client in Cisco Secure ACS and do the following:

- Select authentication by TACACS + (CISCO IOS).
- Note the shared secret that you enter; you will need to enter it in Common Services when you change the AAA mode to ACS in Common Services.

Step 5 Add the System Identity User and Common Services users to Cisco Secure ACS.

You can create a group and add users to it.

Step 6 Note whether the Operations Manager, Service Monitor, and Common Services applications are already registered with Cisco Secure ACS:

To find out, select **Shared Profile Components** and look for:

- Cisco Unified Operations Manager
- Cisco Unified Service Monitor
- Common Services

Step 7 Based on your authentication setting (per user or per group) on Cisco Secure ACS, click either **User Setup** or **Group Setup**.

Step 8 Verify the per-user or per-group setting for Cisco Unified Operations Manager using **Interface Configuration > TACACS + (Cisco IOS)**.

For more information, see User Guide for Cisco Secure Access Control Server 4.x.

Changing the AAA Mode to ACS in Common Services

Before you perform this procedure, complete the tasks in Configuring the System Identity User in Common Services, page C-3 and Setting Up the Cisco Secure ACS Server, page C-3.

Step 1 Choose **Administration > Server Administration (Common Services) > Security > AAA Mode Setup**.

Step 2 Next to Select a Type, select the **ACS** radio button.

The page refreshes, displaying appropriate options.

Step 3 Under Server Details, enter an IP address for the Cisco Secure ACS server and enter a port.

Step 4 Under Login, enter:

- ACS Admin Name—Enter the name of the administrator you created in step 1 of Setting Up the Cisco Secure ACS Server, page C-3.
- ACS Admin Password—Enter the password for the administrator you created in step 1 (See Setting Up the Cisco Secure ACS Server, page C-3.)
- ACS Shared Secret Key— Enter the shared secret you entered when you added the Operations Manager server to Cisco Secure ACS as an AAA client in step 3 (See Setting Up the Cisco Secure ACS Server, page C-3.)

Step 5 Decide whether to select Register all installed applications with ACS.

If Operations Manager is registered with ACS and you register it again, you lose any custom roles that were previously configured in Cisco Secure ACS for Operations Manager.

The same is true for Service Monitor and Common Services. (To selectively register an application, see Registering an Application to Cisco Secure ACS from the Command Line, page C-5.)

Step 6 Select the appropriate radio button (HTTP or HTTPS) under Current ACS Administrative Access Protocol.

Step 7 Click **Apply** to complete the mode change.

An ACS verification status message is displayed; do one of the following:

- Click **OK**
  - Registers Operations Manager, Service Monitor, and Common Services tasks and users to ACS.
  - Overwrites any existing custom roles for Operations Manager, Service Monitor, and Common Services.
- Click **Cancel**—Prevents registration to ACS from occurring.

Step 8 Restart the daemon manager for the changes to take effect.

Step 9 From the command line, enter these commands:

```
net stop crmdmgtd
net start crmdmgtd
```

Registering an Application to Cisco Secure ACS from the Command Line

Registering an application with ACS imports the application tasks and overwrites any custom roles that exist for the application in Cisco Secure ACS.

If you did not select **Register all installed applications with ACS** when you changed the AAA mode to ACS in Common Services, you might want to use the information in this section to register an application to Cisco Secure ACS.

A script, *NMSROOT*\bin\AcsRegCli.pl, enables you to selectively register applications to Cisco Secure ACS.

Note *NMSROOT* is the directory where Operations Manager is installed. If you chose the default, it is C:\PROGRA~1\CSCOpx.

The following are the available parameters while running the script from the CLI:

`AcsRegCli.pl -register` *application name*

Replace *application name* with any of the following:

- itm—Registers Operations Manager only.
- qovr—Registers Service Monitor only.
- cmf—Registers Common Services only.
- all—Registers all applications on the server (Cisco Unified Operations Manager, Cisco Unified Service Monitor, and Common Services).

Assigning Roles to Users and User Groups in Cisco Secure ACS

You must ensure that the System Identity User in Cisco Secure ACS is assigned all roles and that Common Services users or user groups have been assigned the proper privileges.

In Cisco Secure ACS, choose **Shared Profile Components > Cisco Unified Operations Manager**. For more information, see the following:

- *User Guide for Cisco Secure Access Control Server 4.x*
- CiscoWorks Online help. Look for these topics:
  - Roles in ACS
  - Assigning Roles to Users and User Groups in ACS

Verifying the Operations Manager and Cisco Secure ACS Configuration

After performing the tasks beginning with Assigning Roles to Users and User Groups in Cisco Secure ACS, page C-6 through Configuring the System Identity User in Common Services, page C-3, verify the configuration as follows:

Step 1 Log intoOperations Manager with a username defined in Cisco Secure ACS.

Step 2 Try to perform tasks, to ensure that you can perform only those tasks that you are entitled to perform based on the role assigned to you in Cisco Secure ACS.

For example, if your privilege is Help Desk:

- You should be able to view Fault History reports.
- You should not be able to add devices to Operations Manager from the DCR.

Based on the Network Device setting for the user or group on Cisco Secure ACS, you can view only certain devices on the Operations Manager server.

For a list of Operations Manager tasks in which device-based filtering can be used, see the Operations Manager-specific Online help in Cisco Secure ACS.

If you encounter difficulties, see Authentication Failure in ACS Mode in CiscoWorks Online help.