



APPENDIX **B**

Configuring Operations Manager with Cisco Secure ACS

This section describes how to configure Operations Manager with Cisco Secure ACS:

- [Login Module, page B-1](#)
- [Authentication Roles, page B-2](#)
- [Before You Begin: Integration Notes, page B-3](#)
- [Configuring Operations Manager on Cisco Secure ACS, page B-4](#)
- [Verifying the Operations Manager and Cisco Secure ACS Configuration, page B-4](#)

Login Module

Common Services provides security mechanisms for authenticating users of applications. You can configure the login module to use one of the following modes of user authentication and authorization:

- **Non-ACS**—In this mode, the Operations Manager server provides authentication and authorization services.
- **ACS**—In this mode, a Cisco Secure Access Control Server (ACS) provides authentication and authorization services. To use this mode, you must have a Cisco Secure ACS installed on your network. The supported versions of Cisco Secure ACS for Windows are 3.2, 3.2.3, 3.3.2, 4.0.

If you are using ACS 3.2.3, we recommend that you install the Admin HTTPS PSIRT patch:

1. Go to <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-ac-win>.
2. Click the Download Cisco Secure ACS Software (Windows) link. You will find the link to the Admin HTTPS PSIRT patch in the table.

You can integrate Operations Manager with Cisco Secure ACS only if they are installed on separate systems, because Operations Manager must be configured as an authentication, authorization, and accounting (AAA) client for Cisco Secure ACS.

In ACS mode, *fallback* is provided for authentication only. (Fallback options allow you to access Operations Manager if the login module fails, or you accidentally lock yourself or others out.) If authentication with ACS fails, Operations Manager does the following:

1. Tries authentication using non-ACS mode (CiscoWorks local mode).
2. If non-ACS authentication is successful, presents you with a dialog box with instructions to change the login mode to CiscoWorks local. (You can do so only if you have permission to perform that operation in non-ACS mode.)



Note You will not be allowed to log in if authentication fails in non-ACS mode.

For more information, see *User Guide for CiscoWorks Common Services* and Common Services online help.

Authentication Roles

In ACS mode, by default the Operations Manager server provides the five roles listed here, from least privileged to most privileged:

- **Help Desk**—A user with this role has the privileges to access network status information from the persisted data. This user does not have the privilege to contact any device or schedule a job that will reach the network.

For example, this user can search the Alert History database.

- **Network Operator**—A user with this role has the privilege to perform all tasks that involve collecting data from the network. The user can also perform all Approver tasks. The user does not have write access on the network.

For example, this user can configure logging parameters.



Note In Operations Manager, a user with this role by default can perform the same Operations Manager tasks as a Network Administrator.

- **Network Administrator**—A user with this role has the privilege to change the network. The user can also perform Network Operator tasks.

For example, this user can add devices to Operations Manager from the DCR.

- **System Administrator**—A user with this role has the privilege to perform all Operations Manager system administration tasks. See the Permissions report. From the Operations Manager home page, click **CiscoWorks** in the upper right-hand corner of the window, the CiscoWorks home page opens. Under Common Services, select Server > Reports > Permission Report.

For example, this user can configure SNMP trap forwarding (Administration > Preferences).



Note If you use Cisco Secure ACS to modify these roles, removing tasks or reassigning tasks from one role to another, the Permissions report will not reflect your changes.

You can modify roles on Cisco Secure ACS.

-
- Step 1** Select **Shared Profile Components > Cisco Unified Operations Manager**.
 - Step 2** Click the Operations Manager role that you want to modify.
 - Step 3** Select the Operations Manager tasks that suit your business workflow and needs.

Step 4 Click **Submit**.



Note

If desired, you can also create new roles on Cisco Secure ACS.

Before You Begin: Integration Notes

This section contains notes that you should read before you begin Cisco Secure ACS and Operations Manager server integration:

- Operations Manager server and Cisco Secure ACS integration should be performed only *after* installing all applications.
- If you have installed your application after configuring the CiscoWorks Login Module to ACS mode, then the application users are not granted any permissions; however, the application is registered to Cisco Secure ACS. On the Cisco Secure ACS server, you must assign the appropriate permissions to the application.

See [Configuring Operations Manager on Cisco Secure ACS, page B-4](#).

- Multiple instances of the same application using the same Cisco Secure ACS will share settings. Any changes will affect all instances of that application.
- If an application is configured with Cisco Secure ACS and then that application is reinstalled, it will inherit the old settings.



Note

This is applicable if you are using Cisco Secure ACS version 3.2.3 or earlier.

- You must create roles in Cisco Secure ACS for each Operations Manager application that is running on the Operations Manager server.

For example, you must create roles in Cisco Secure ACS for Cisco Unified Service Monitor. These roles are not shared by any other Operations Manager application.

- The roles that you create in Cisco Secure ACS are shared across all servers that are configured to the same Cisco Secure ACS.

For example, you have configured 10 servers with a Cisco Secure ACS, and you have created a role in Cisco Secure ACS for Operations Manager (say, *CUOMSU*). This role is shared by Operations Manager applications running on all 10 servers.

- A user can have different access privileges for different Operations Manager applications.

For example a user, *CWSU*, can have the following privileges:

- System Administrator for Common Services
- Approver for RME
- Network Operator for Campus Manager
- Network Administrator for Operations Manager
- Help Desk for Internet Performance Monitor (IPM)

- In CiscoWorks, you must do the following:
 - Set AAA Mode to ACS—You will need to supply the following information, obtained from Cisco Secure ACS, to complete this task: IP address or hostname, port, admin username and password, and shared secret key.
 - Set up System Identity Setup username.
- On Cisco Secure ACS, you must configure a user with the same username as the CiscoWorks server System Identity Setup user. For Operations Manager, this user must have Network Administrator privileges on Cisco Secure ACS. For CiscoWorks applications, this user must have System Administrator privileges on Cisco Secure ACS.

See the chapter “Configuring the Server” in *User Guide for CiscoWorks Common Services* for details on configuring the CiscoWorks server in ACS mode.

Configuring Operations Manager on Cisco Secure ACS

After you complete setting the Operations Manager server to ACS mode with Cisco Secure ACS, perform the following tasks on Cisco Secure ACS:

1. Click **Shared Profile Components** to verify that the Cisco Unified Operations Manager application entry is present.

**Note**

If you integrated CiscoWorks Common Services with Cisco Secure ACS *before* installing Operations Manager, you must configure ACS mode again and register all applications with ACS. See the Common Services online help. Also, if Operations Manager is reinstalled, the configurations in Cisco Secure ACS are not lost. After re-registering Operations Manager with Cisco Secure ACS, the configurations available in Cisco Secure ACS will be inherited by Operations Manager.

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

On Cisco Secure ACS, verify the per-user or per-group setting for Cisco Unified Operations Manager using **Interface Configuration > TACACS + (Cisco IOS)**.

3. Assign the appropriate Operations Manager privileges to the user or group.

For Operations Manager, you must ensure that a user with the same name as the CiscoWorks server System Identity Setup user is configured on Cisco Secure ACS and has Network Administrator privileges.

Verifying the Operations Manager and Cisco Secure ACS Configuration

After performing the tasks in [Configuring Operations Manager on Cisco Secure ACS, page B-4](#), verify the configuration as follows:

1. Log in to Operations Manager with the username defined in Cisco Secure ACS.
2. Try to perform tasks, to ensure that you can perform only those tasks that you are entitled to perform based on your privileges on Cisco Secure ACS.

For example, if your privilege is Help Desk, then:

- You should be able to view the device summary.
 - You should not be able to select devices for Operations Manager to manage.
3. 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.



Note For a list of Operations Manager displays that perform device-based filtering, see the Operations Manager-specific online help in Cisco Secure ACS.
