



APPENDIX **F**

Security Configuration with Cisco Secure ACS

This section describes how to configure Service Monitor with Cisco Secure ACS:

- [Before You Begin: Integration Notes, page F-1](#)
- [Configuring Service Monitor on Cisco Secure ACS, page F-2](#)
- [Verifying the Service Monitor and Cisco Secure ACS Configuration, page F-3](#)

Before You Begin: Integration Notes



Note

You can integrate Service Monitor with Cisco Secure ACS only if they are installed on separate systems because Service Monitor must be configured as an AAA client for Cisco Secure ACS.

For information about Common Services login modules and user roles, see [Configuring Users \(ACS and Non-ACS\), page 6-10](#).

This section contains the following notes, which you should read before you begin Cisco Secure ACS and Service Monitor integration:

- Multiple instances of the same application using the same Cisco Secure ACS will share settings. Any changes will affect all instances of that application.

For example: You have configured three Service Monitor servers with a Cisco Secure ACS, and you have created a role in Cisco Secure ACS for Service Monitor (say, *SMSU*). This role is shared by licensed versions of Service Monitor running on all three servers.

- A user can have different access privileges for different Cisco Unified Communications Management Suite applications.

For example: A user, *SMSU*, can have the following privileges:

- System Administrator for Service Monitor
 - Network Operator for Operations Manager
 - Network Administrator for Service Monitor
 - Help Desk for Operations Manager
- 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.

- Using Common Services, 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.



Note When you set Common Services AAA mode to ACS, all Cisco Unified Communications Management Suite applications running on the same server register with Cisco Secure ACS and use it for authentication and authorization. If Service Monitor and Operations Manager are installed on a server in ACS mode, all of the following use Cisco Secure ACS: Service Monitor, Operations Manager, and Common Services.

- Set up System Identity Setup username. This user was configured during Service Monitor installation. For more information, click the CiscoWorks link on the Service Monitor home page and select **Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup**.
- On Cisco Secure ACS, you must configure a user with the same username as the System Identity Setup user. For Service Monitor, that user must have Network Administrator privileges on Cisco Secure ACS.
- In ACS mode, fallback is provided for authentication only. (Fallback options allow you to access Service Monitor if the login module fails, or you accidentally lock yourself or others out.) If authentication with ACS fails, Service Monitor 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 details on configuring ACS mode, click the CiscoWorks link on the Service Monitor home page and select **Common Services > Server > Security > AAA Mode** and click **Help**.

Configuring Service Monitor on Cisco Secure ACS

After you complete setting the CiscoWorks 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 Service Monitor (Service Monitor) application entry is present.
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 Service Monitor using **Interface Configuration > TACACS + (Cisco IOS)**.

3. Assign the appropriate Service Monitor privileges to the user or group.

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



Note You configured the System Identity Setup user during Service Monitor installation. For more information, click the CiscoWorks link on the Service Monitor home page and select **Common Services > Server > Security > Multi-Server Trust Management > System Identity Setup**.

You can modify roles on Cisco Secure ACS.

-
- Step 1** Select **Shared Profile Components > Cisco Unified Service Monitor**.
 - Step 2** Click the Service Monitor role that you want to modify.
 - Step 3** Select the Service Monitor 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.

Verifying the Service Monitor and Cisco Secure ACS Configuration

After performing the tasks in [Configuring Service Monitor on Cisco Secure ACS, page F-2](#), verify the configuration as follows:

1. Log in to Service Monitor 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 Cisco 1040s that are managed by Service Monitor.
- You should not be able to add Cisco 1040s for Service Monitor to manage, and you should not be able to delete them.

