APPENDIX C

Security Configuration with Cisco Secure ACS

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

Cisco Secure ACS Support

Service Monitor 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 separate from the one where Service Monitor is installed.

Service Monitor Integration Notes

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

When you register Cisco Prime Unified Service Monitor (and Common Services) with Cisco Secure ACS, the applications tasks—such as adding data source credentials to Service Monitor—and user roles—such as Network Administrator—for the application are imported into Cisco Secure ACS.

You only need to register 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.

Note The Service Monitor integration with Cisco Secure ACS does not enable you to selectively filter out specific devices. For example, a user in a role that includes the task:

- Data Source Credentials: add, edit and verify—Can add, edit, or verify credentials in Service Monitor for any NAM or any Unified Communications Manager.
- Cisco 1040: view details—Can view details from Service Monitor for any Cisco 1040.

Common Services Local Login Module Authentication Roles

Common Services login modules enable you to use a source other than the native mechanism for authentication, that is the Common Services Local login module.

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 six roles. 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	Privileges to view some information in Service Monitor and Common Services. Example: Generate and view reports and view details for Cisco 1040. (Cannot perform modifications.)
Network Operator	Privilege to perform all Service Monitor tasks and some Common Services tasks. Example: Set up Service Monitor; add, modify, verify data source credentials.
Network Administrator	Privilege to perform all Service Monitor tasks and several Common Services tasks. User can also perform Network Operator tasks. Example: Same as Network Operator.
System Administrator	Privilege to perform all system administration tasks. Example: Enable and disable debugging; set logging level.
Super Admin	This role is not supported in Service Monitor.

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

Note For more information, see Common Services online help.

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

Configuring the System Identity User in Common Services

Before you integrate the Service Monitor server with Cisco Secure ACS, ensure that you create and assign all privileges to a system identity user in Common Services. This topic explains how to 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 Common Services online help.*)*

1. Create a local user and assign all roles to the user. (See Configuring Users Using the Common Services Local Login Module, page 3-2.)

   Note 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 Service Monitor and Common Services.

2. Update the System Identity User, replacing the username with the one that you created in step 1. (Select **Administration > Server Administration (Common Services) > Security > Multi-Server Trust Management > System Identity Setup**.

For more information, see Common Services online help.

Setting Up the Cisco Secure ACS Server

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

1. Configure ACS Administrators.

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

   Note If you do not configure the administrator user with all privileges, Service Monitor registration with Cisco Secure ACS fails.

   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.

2. Add the Service Monitor server to Cisco Secure ACS as a AAA Client.

   Configure the Service Monitor server as a 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.

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

   You can create a group and add users to it.

4. Note whether the Service Monitor and Common Services applications are already registered with Cisco Secure ACS. To find out, select **Shared Profile Components** and look for:

   - Cisco Prime Unified Service Monitor
   - Common Services

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 Select **Administration > Server Administration (Common Services) > Security > AAA Mode Setup**. The AAA Mode Setup page appears.

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. (See 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 Service Monitor server to Cisco Secure ACS as a AAA client in step 2. (See Setting Up the Cisco Secure ACS Server, page C-3.)

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

Note If Service Monitor is registered with ACS and you register it again, you lose any custom roles that were previously configured in Cisco Secure ACS for Service Monitor. The same is true for 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 Service Monitor and Common Services tasks and users to ACS; overwrites any existing custom roles for 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. From the command line, enter these commands:

```
net stop crmdmgtd

net start crmdmgtd
```

Registering an Application to Cisco Secure ACS from the Command Line

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

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

Following are the available parameters when running the script from the CLI:

`AcsRegCli.pl -register <`*`application name`***`>`**

Replace application name with any of the following:

- qovr—Registers Service Monitor only
- cmf—Registers Common Services only
- all—Registers all applications on the server (Cisco Prime 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, select **Shared Profile Components > Cisco Prime Unified Service Monitor**. For more information, see these documents:

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

Verifying the Service Monitor and Cisco Secure ACS Configuration

After performing the tasks beginning with Assigning Roles to Users and User Groups in Cisco Secure ACS, page C-5 through Configuring the System Identity User in Common Services, page C-3, verify the configuration as follows:

1. Log in to Service Monitor with a 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 the role assigned to you in 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.

If you encounter difficulties, see Authentication Failure in ACS Mode in Common Services online help.