



Configuring DFM with Cisco Secure ACS

This section describes how to configure DFM with Cisco Secure ACS:

- [CiscoWorks Login Module, page C-1](#)
- [CiscoWorks Server Authentication Roles, page C-2](#)
- [Before You Begin: Integration Notes, page C-2](#)
- [Configuring DFM on Cisco Secure ACS, page C-4](#)
- [Verifying the DFM and Cisco Secure ACS Configuration, page C-4](#)

CiscoWorks Login Module

The CiscoWorks server provides the mechanism used to authenticate users for CiscoWorks applications. CiscoWorks Common Services supports two modes of user authentication and authorization:

- **ACS**—In this mode, authentication and authorization services are provided by an Access Control Server (ACS). To use this mode, you must have a Cisco Secure ACS installed on your network.

The supported Cisco Secure ACSs for Windows are:

- Cisco Secure ACS 3.2
 - Cisco Secure ACS 3.2.3
 - Cisco Secure ACS 3.3.2
 - Cisco Secure ACS 3.3.3
 - Cisco Secure ACS 4.0(1)
- **Non ACS**—In this mode, authentication and authorization services are provided by the CiscoWorks server.

The fallback option in ACS mode is different from that of non-ACS mode. Here, fallback is provided only for authentication.

- If the user authentication with ACS fails, the authentication is tried with CiscoWorks local mode.
- If user authentication succeeds, the user is allowed to change the login module to non-ACS mode, provided the user has permission to do so in non-ACS mode.

For more information, see *User Guide for CiscoWorks Common Services 3.0.5* and the CiscoWorks Common Services 3.0.5 online help.

CiscoWorks Server Authentication Roles

By default, the CiscoWorks server authentication provides five roles in ACS mode. They are listed here from least privileged to most privileged:

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

For example, this user can use the Alerts and Activities display.

2. **Approver**—User with this role has privileges to approve all DFM tasks and can perform all Help Desk tasks.

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

3. **Network Operator**—User with this role has privileges to perform all tasks that involve collecting data from the network. User does not have write access on the network. User can also perform all the Approver tasks.

For example, this user can configure logging parameters.



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

4. **Network Administrator**—User with this role has the privilege to change the network. User can also perform the Network Operator tasks.

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

5. **System Administrator**—User with this role has the privilege to perform all CiscoWorks system administration tasks. See the Permissions Report on the CiscoWorks server (**Common Services > Server > Reports > Permission Report**).

For example, this user can configure SNMP trap forwarding (**Configuration > Other Configurations > SNMP Trap Forwarding**).

We recommend that you do not modify the default CiscoWorks roles.

You can create your own custom roles on Cisco Secure ACS. See *User Guide for CiscoWorks Common Services 3.0.5* and the CiscoWorks Common Services 3.0.5 online help for further details.

Before You Begin: Integration Notes

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

- We recommend that you integrate the CiscoWorks server and Cisco Secure ACS after installing all of the LAN Management Solution applications.

If you have integrated the CiscoWorks server and Cisco Secure ACS before installing DFM 2.0.6, you are prompted with this message at the time of DFM 2.0.6 installation:

```
CiscoWorks Server is in ACS mode
The application that you are installing requires new tasks to be registered with ACS.
If you have already registered this application with ACS from another server, you do
not need to register it again. However if you re-register the application, you will
lose any custom roles that you had created earlier for this application in ACS.
```

Enter (Y)es to Register, (N)o to continue without registering, (Q)uit : [N]

- If you enter **Y**, DFM 2.0.6 gets registered with the ACS server.
- If you enter **N**, DFM 2.0.6 does not get registered with the ACS server.

After the installation, you can register DFM 2.0.6 with the ACS server, using the `AcsRegCli.pl` script:

```
NMSROOT\bin\perl NMSROOT\bin\AcsRegCli.pl -register dfm
```

For example (the following command is one line):

```
C:\Program-1\CSCOpX\bin\perl C:\Progra~1\CSCOpX\bin\AcsRegCli.pl -register dfm
```

- For DFM, you must ensure that the CiscoWorks server System Identity Setup user has the privilege to perform all DFM tasks on Cisco Secure ACS.
- 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 the Cisco Secure ACS. On the Cisco Secure ACS server, you must assign the appropriate permissions to the application.

See the information on server configuration in the *User Guide for Common Services 3.0.5*.

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

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

- The role that you create is not shared across all the LAN Management Solution applications. It is shared across all CiscoWorks servers that are configured to that particular Cisco Secure ACS.

You have to create new roles for each of the LAN Management Solution applications that are running on the CiscoWorks server.

For example, say you have configured 10 CiscoWorks servers with a Cisco Secure ACS, and you have created a role in DFM (for instance, DFMSU). This role is shared for the DFM application running in all 10 CiscoWorks servers. This role is not shared for any other LAN Management Solution applications that are running on the CiscoWorks server.

- You can have different users with different access privileges to the CiscoWorks applications.

For example, say you have a user, CWSU. This user can be a System Administrator for Common Services, an Approver for RME, a Network Operator for Campus, a Network Administrator for DFM, and a Help Desk user for IPM.

- For details on configuring the CiscoWorks server in ACS mode, see the information on server configuration in the *User Guide for Common Services 3.0.5*.

Configuring DFM on Cisco Secure ACS

After registering the CiscoWorks server with Cisco Secure ACS, perform the following on Cisco Secure ACS:

-
- Step 1** Click **Shared Profile Components** to verify that the Device Fault Manager application entry is present.
- Step 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, you can verify the per user or per group setting for DFM using Interface **Configuration > TACACS + (Cisco IOS)**.
- Step 3** Assign the appropriate privileges to the user or group to allow them to use DFM.
- For DFM, you must ensure that the CiscoWorks server System Identity Setup user has the privilege to perform all DFM tasks on Cisco Secure ACS.
-

Verifying the DFM and Cisco Secure ACS Configuration

Do the following after performing the above-mentioned tasks on the Cisco Secure ACS server.

-
- Step 1** Log in to CiscoWorks with the username defined in the Cisco Secure ACS.
- Step 2** Based on your privilege on the Cisco Secure ACS, verify that you can perform only certain tasks on the CiscoWorks server.
- For example, if you have only Help Desk privileges, then you can only view the device summary.
- Step 3** Based on the network device setting for the user or group on the Cisco Secure ACS, verify that you can view only certain devices in the CiscoWorks server.
-