



CHAPTER 3

Setting Up the QPM Server

This chapter contains the following topics:

- [User Permissions for QPM, page 3-1](#)
- [CiscoWorks User Permissions, page 3-2](#)
- [ACS User Permissions, page 3-7](#)
- [Working with ACS Device Groups and User Permissions, page 3-10](#)

User Permissions for QPM

CiscoWorks Common Services provides management of QPM user roles and privileges. QPM can work with either CiscoWorks user permissions or Cisco Secure Access Control Server (ACS) user permissions.

QPM permissions for authentication and authorization are mapped to CiscoWorks permission roles or ACS permission roles, as specified.



Note

To use ACS authentication and authorization, ACS must be installed on the network.

Before you begin to work with QPM, you should ensure that you have the appropriate permissions.

ACS and CiscoWorks permissions in QPM rely on the usergroup or username, the command set or privileges associated with the usergroup or username, and the device or device group for which privileges are requested.

If your username or usergroup is not authorized for certain QPM actions, the related menu items, TOC items, and buttons will be hidden or disabled.

CiscoWorks User Permissions

QPM uses a separate set of permissions for each type of task.

[Table 3-1](#) shows how QPM permissions are mapped to CiscoWorks roles.

Table 3-1 QPM Permissions Mapped to CiscoWorks Roles

QPM Permissions	CiscoWorks Roles				
	System Admin	Network Admin	Network Operator	Approver	Help Desk
Device Inventory					
View	X	X	X	X	X
Add/Modify	X	X			
Policy Configuration					
View	X	X	X	X	X
Modify		X	X	X	
Deployment					
View	X	X	X	X	X
Deploy		X			
Delete jobs and logs	X				

Table 3-1 QPM Permissions Mapped to CiscoWorks Roles (continued)

QPM Permissions	CiscoWorks Roles				
	System Admin	Network Admin	Network Operator	Approver	Help Desk
Monitor					
Real Time Status					
View Report Card	X	X	X	X	X
Launch Real Time Chart	X	X	X	X	X
Launch Event browser	X	X	X	X	X
Historical Trends					
View	X	X	X	X	X
Delete	X				
Create Analysis Tasks		X	X	X	
Threshold Configuration					
View	X	X	X	X	X
Create Threshold Sets		X			
Assign Threshold Sets		X			
Delete Threshold Jobs	X				

Table 3-1 QPM Permissions Mapped to CiscoWorks Roles (continued)

QPM Permissions	CiscoWorks Roles				
	System Admin	Network Admin	Network Operator	Approver	Help Desk
Admin					
View Audit logs	X	X	X	X	X
Delete Audit logs	X				
Backup/Retrieve Backup	X				
SNMP Configuration Rights	X	X			
License	X				

To view the QPM tasks allowed for each CiscoWorks role in QPM, select **Administration > User Permissions Report**.

CiscoWorks roles have the following permissions in QPM:

- System Admin
 - View all information in QPM
 - Make changes to devices in the QPM device inventory
 - Delete policy deployment jobs and logs
 - Launch Real Time Charts and Event Browsers
 - Delete Monitoring Tasks (under Historical Trends)
 - Delete Threshold Assignment jobs
 - Delete Audit logs
 - Create and retrieve backups of the QPM database
 - Configure SNMP Configuration Rights
 - Add/remove licenses

System admin is the only user role that can delete logs, jobs, and reports in QPM.

- Network Admin
 - View all information in QPM
 - Make changes to devices in the QPM device inventory
 - Create and edit policies
 - Deploy policies on devices
 - Launch Real Time Charts and Event Browsers
 - Create Monitoring Tasks (under Historical Trends)
 - Create Threshold Sets and assign Threshold Sets to interfaces
 - Configure SNMP Configuration Rights

Network admin is the only user role that can deploy QoS policies on the devices in the network.

- Network Operator
 - View all information in QPM
 - Create and edit policies
 - Launch Real Time Charts and Event Browsers
 - Create Monitoring Tasks (under Historical Trends)
 - Create and run monitoring tasks
- Approver
 - View all information in QPM
 - Create and edit policies
 - Launch Real Time Charts and Event Browsers
 - Create Monitoring Tasks (under Historical Trends)
- Help Desk
 - View all information in QPM
 - Launch Real Time Charts and Event Browsers

Setting Up CiscoWorks Usernames and Permissions for QPM

You can add your username for CiscoWorks authentication from the CiscoWorks Homepage.

To select a role or a number of roles:

-
- Step 1** Select **Common Services > Server > Security** in the CiscoWorks homepage. The Security Settings page appears.
 - Step 2** Click **Local User Setup** in the TOC. The Local User Setup page appears.
 - Step 3** Click **Add**. The User Information dialog box appears.
 - Step 4** Enter the username in the Username field.
 - Step 5** Enter the password in the Password field.
 - Step 6** Re-enter the password in the Verify Password field.
 - Step 7** Enter the E-mail ID in the Email field, if the user has an Approver role.
 - Step 8** Go to the Roles pane and select the check box corresponding to the role(s) to be assigned to the user.

See the *User Guide for CiscoWorks Common Services 3.0.5* for more information about setting CiscoWorks usernames and permissions.

CiscoWorks permissions cannot be customized. However, you can create a role for a user with the permissions of more than one CiscoWorks role. For example, a user can have both System Admin and Approver roles.

**Tip**

You can create a superuser (permissions for everything) by giving both system administrator and network administrator roles to a user.

ACS User Permissions

When you configure CiscoWorks Common Services to use ACS authorization and authentication, QPM adds permissions in ACS.

Table 3-2 shows the default mapping of QPM permissions to ACS roles. This is the same as for the CiscoWorks roles. However, when using ACS authorization and authentication, you can modify the default roles.

Table 3-2 QPM Permissions Mapped to ACS Roles

QPM Permissions	ACS Roles				
	System Admin	Network Admin	Network Operator	Approver	Help Desk
Device Inventory					
View	X	X	X	X	X
Add/Modify	X	X			
Policy Configuration					
View	X	X	X	X	X
Modify		X	X	X	
Deployment					
View	X	X	X	X	X
Deploy		X			
Delete jobs and logs	X				
Monitor					
Real Time Status					
View Report Card	X	X	X	X	X
Launch Real Time Chart	X	X	X	X	X
Launch Event browser	X	X	X	X	X

Table 3-2 QPM Permissions Mapped to ACS Roles (continued)

QPM Permissions	ACS Roles				
	System Admin	Network Admin	Network Operator	Approver	Help Desk
Historical Trends					
View	X	X	X	X	X
Delete	X				
Create Analysis Tasks		X	X	X	
Threshold Configuration					
View	X	X	X	X	X
Create Threshold Sets		X			
Assign Threshold Sets		X			
Delete Threshold Jobs	X				
Admin					
View Audit logs	X	X	X	X	X
Delete Audit logs	X				
Backup/Retrieve Backup	X				
SNMP Configuration Rights	X	X			
License	X				

To modify global components, such as library components, global device settings, and so on, you must have appropriate permissions for the device group that contains the CiscoWorks Common Services server.

ACS roles have the following default permissions in QPM:

- System Admin
 - View all information in QPM
 - Make changes to devices in the QPM device inventory
 - Delete policy deployment jobs and logs
 - Launch Real Time Charts and Event Browsers
 - Delete Monitoring Tasks (under Historical Trends)
 - Delete Threshold Assignment jobs
 - Delete Audit logs
 - Create and retrieve backups of the QPM database
 - Configure SNMP Configuration Rights
 - Add/remove Licenses

System admin is the only user role that can delete logs, jobs, and reports in QPM.

- Network Admin
 - View all information in QPM
 - Make changes to devices in the QPM device inventory
 - Create and edit policies
 - Deploy policies on devices
 - Launch Real Time Charts and Event Browsers
 - Create Monitoring Tasks (under Historical Trends)
 - Create Threshold Sets and assign Threshold Sets to interfaces
 - Configure SNMP Configuration Rights

Network admin is the only user role that can deploy QoS policies on the devices in the network.

- Network Operator
 - View all information in QPM
 - Create and edit policies
 - Launch Real Time Charts and Event Browsers
 - Create Monitoring Tasks (under Historical Trends)
 - Create and run monitoring tasks
- Approver
 - View all information in QPM
 - Create and edit policies
 - Launch Real Time Charts and Event Browsers
 - Create Monitoring Tasks (under Historical Trends)
- Help Desk
 - View all information in QPM
 - Launch Real Time Charts and Event Browsers

If you intend to work with ACS device groups and user permissions, you must perform the setup configuration described in [Working with ACS Device Groups and User Permissions, page 3-10](#).

ACS allows you to modify the default permission roles. For details about modifying permissions in ACS, see the ACS Online help.

After you change the permission roles, you must restart the ACS server.

If QPM is open, log out and log in again to QPM for the changes to take effect.

Working with ACS Device Groups and User Permissions

The following topics describe how to configure CiscoWorks Common Services to use ACS authorization and authentication on a new QPM installation, and after upgrading from QPM 3.2.x.

- [Setting up ACS Device Groups and User Permissions for QPM, page 3-11](#)
- [Updating QPM 3.2.x User Permissions in ACS, page 3-15](#)

Setting up ACS Device Groups and User Permissions for QPM

If you want to use ACS device groups, user groups, and permissions, for QPM, ACS must be installed on the network.

To work with ACS device groups, user groups, and permissions, you must register the QPM server with ACS and configure CiscoWorks Common Services to use ACS authorization and authentication.

The following steps describe the process:

Step	Task	Procedure
Step 1	Register the QPM server with ACS.	<ol style="list-style-type: none"> 1. Login to ACS server. 2. In the navigation bar of the ACS home page, click Network Configuration. The Network Configuration page appears with a list of the Network Device Groups (NDGs). You can create your own QPM server Network Device Group, and add the QPM server as AAA client in it. The following steps describe this process. 3. Under the Network Device Groups table, click Add Entry. 4. In the Network Device Group Name box, type the name of the new NDG, for using QPM 5. In the Key box, enter a key for the Network Device Group. The maximum length is 32 characters 6. Click Submit. The Network Device Groups table displays the new NDG. 7. Click the name of the new NDG, and click Add Entry below the AAA Clients table 8. In the Add AAA Client page, enter the QPM client details like Hostname, IP Address, and Key. 9. Click Submit + Apply. <p>If you do not want to create a new NDG for QPM, you can click the Not Assigned link in the NDG table (instead of Step 3 and the subsequent steps above), and click Add Entry to define the QPM client in ACS.</p> <p>For details about all these steps, see the chapter <i>Network Configuration</i>, in the ACS User Guide.</p>

Step	Task	Procedure
Step 2	Register ACS with QPM.	<ol style="list-style-type: none"> 1. Login to CiscoWorks in the CMF Mode. 2. In the CiscoWorks homepage, select Common Services > Server > Security > AAA Mode Setup. 3. Click the TACACS+ radio button 4. Click Change. The Login Module Options window appears. 5. Enter the ACS server IP/Name and Key (the same Key that you entered in Step 1) in the corresponding fields, and click OK. The Login Module Change Summary page appears. 6. Click OK. 7. In the AAA Mode Setup page, click the ACS radio button. 8. Enter the ACS sever details. 9. Enter the login details including the Shared Secret Key (the same key that you entered in Step 1). 10. Check the Register all installed applications with ACS checkbox. 11. Click the HTTP or HTTPS radio button to specify the current ACS administrative protocol. 12. Click Apply. The Login Module Change Summary page appears with the following message: <i>ACS Server Credentials updated successfully</i> 13. Close down all the QPM and CS Windows, restart the deamon manager. <p>For details about these steps, see the section <i>Setting up the AAA mode</i> in the chapter <i>Configuring the Server</i>, in the User Guide for CiscoWorks Common Services 3.0.5.</p>

Step	Task	Procedure
Step 3	Synchronize device groups in ACS Server with QPM	<ol style="list-style-type: none"> 1. In QPM, select Devices > Device Grouping > Sync Privileges. The Sync Privileges page appears. 2. Check whether the Server mode is set to ACS, and click Sync.
Step 4	Define usernames and user groups and permissions, in ACS.	<ol style="list-style-type: none"> 1. In the navigation bar of the ACS homepage, click User Setup, and define usernames. 2. In the navigation bar of the ACS homepage, click Group Setup, and define user groups and their permissions. <p>For details about these steps, see the chapters <i>User Management</i> and <i>User Group Management</i>, in the ACS User Guide.</p>

To change the authorization and authentication mode back to CiscoWorks permissions, you must configure CiscoWorks Common Services to use local authorization and authentication.

For details of this procedure, see the *User Guide for CiscoWorks Common Services 3.0.5*.

Updating QPM 3.2.x User Permissions in ACS

If you are upgrading from QPM 3.2.x on the same QPM server, and you worked with ACS user groups and permissions, you must update ACS with the new QPM user permissions.



Note

If you are upgrading to a different server from QPM 3.2.x, follow the procedure in [Setting up ACS Device Groups and User Permissions for QPM, page 3-11](#).

Step	Task	Procedure
Step 1	Remove the old QPM permission roles from the ACS server.	<ol style="list-style-type: none"> 1. In the ACS server, select Shared Profile Components > CiscoWorks QPM. 2. Select the QPM user roles and delete them <p>For details about these steps, see the chapter <i>Shared Profile Components</i>, in the ACS User Guide.</p>
Step 2	Unregister the old QPM from ACS.	<ol style="list-style-type: none"> 1. In the CiscoWorks homepage, select Common Services > Server > Security > AAA Mode Setup. 2. Click the ACS radio button. 3. Uncheck the Register all installed applications with ACS checkbox. 4. Click Apply. 5. Logout of CiscoWorks desktop.

Step	Task	Procedure
Step 3	Reregister the new QPM in ACS	<ol style="list-style-type: none"> 1. Log into the CiscoWorks. 2. In the CiscoWorks Homepage, select Common Services > Server > Security > AAA Mode Setup. 3. Click the ACS radio button. 4. Check the Register all installed applications with ACS checkbox. 5. Click the HTTP or HTTPS radio button to specify the current ACS administrative protocol. 6. Click Apply. <p>For details about these steps, see the section <i>Setting up the AAA mode</i> in the chapter <i>Configuring the Server</i>, in <i>User Guide for CiscoWorks Common Services 3.0.5</i>.</p>
Step 4	Synchronize device groups in ACS Server with QPM	<ol style="list-style-type: none"> 1. In QPM, select Devices > Device Grouping > Sync Privileges. The Sync Privileges page appears. 2. Check whether the Server mode is set to ACS, and click Sync
Step 5	Define device groups, usernames, and user groups and permissions, in ACS.	<ol style="list-style-type: none"> 1. In the navigation bar of the ACS home page, click Network Configuration, and define Network Device Groups 2. In the navigation bar of the ACS homepage, click User Setup, and define usernames. 3. In the navigation bar of the ACS homepage, click Group Setup, and define user groups and their permissions. <p>For details about these steps, see the chapters <i>Network Configuration</i>, <i>User Management</i> and <i>User Group Management</i>, in the ACS User Guide.</p>