



APPENDIX **C**

User Roles and Permissions

Your username and password must be authenticated for you to use AUS. Your username and password pair are compared with either the CiscoWorks Server or Cisco Secure Access Control Server (ACS) database, depending on which you configured.

After authentication, your authorization is based on the privileges that were assigned to you. A privilege is a task or operation defined within the application. The set of privileges assigned to you defines your role and dictates how much and what type of system access you have.

When you installed CiscoWorks Common Services, the CiscoWorks Server was chosen to provide AAA services by default. You can change this to ACS before or after installing AUS. See *Using CiscoWorks Common Services* for details.

These topics provide details about the user roles and permissions associated with the two types of authentication methods:

- [AUS Privileges, page C-1](#)
- [CiscoWorks Server Roles and AUS Privileges, page C-2](#)
- [Cisco Secure ACS Roles and AUS Privileges, page C-4](#)

AUS Privileges

AUS privileges are the major actions that you can perform. The privileges AUS provides are listed in [Table C-1](#). These privileges are assigned to the CiscoWorks Server and ACS roles described in the following sections:

- [CiscoWorks Server Roles and AUS Privileges, page C-2](#)

- [Cisco Secure ACS Roles and AUS Privileges, page C-4](#)

Table C-1 **AUS Privileges**

Privilege	Description
API_View_Device GUI_View_Device	Allows you to view device information.
API_View_Images GUI_View_Images	Allows you to display information about software images.
API_View_Assignment GUI_View_Assignment	Allows you to gather and display information about device-to-file and file-to device assignments.
API_View_Reports GUI_View_Reports	Allows you to display system summary information and event reports.
API_View_Admin GUI_View_Admin	Allows you to display AUS administrative information.
API_Modify_Device GUI_Modify_Device	Allows you to force a device to contact AUS.
API_Modify_Images GUI_Modify_Image	Allows you to add images to and delete images from AUS.
API_Modify_Assignment GUI_Modify_Assignment	Allows you to assign a file to devices and devices to a file.
API_Modify_Admin GUI_Modify_Admin	Allows you to change some AUS administrative configuration settings, such as database passwords.

CiscoWorks Server Roles and AUS Privileges

When you perform an action to devices using the CiscoWorks Server authentication method, the action is authorized according to the selected device.

The CiscoWorks Server has five roles that correspond to likely functions within your organization. Roles are not set up hierarchically, with each role including all privileges of the role “below” it. Instead, these roles are based on user needs.

[Table C-2](#) lists roles for use with AUS.

Table C-2 CiscoWorks Roles

Role	Description
System Administrator	Can perform all CiscoWorks Server and AUS tasks, for example, add users, set user passwords, add or delete images, and delete assignments.
Network Administrator	Can perform CiscoWorks Server administrative tasks, for example, add or edit administrative settings.
Network Operator	Has read-only access to all information in AUS.
Approver	Can modify devices. Has read-only access for images, assignments, reports, and admin tasks.
Help Desk ¹	Has read-only access to all information in AUS.

1. All CiscoWorks Server roles allow you to perform Help Desk tasks.

Table C-3 lists AUS roles and their supported privileges.

Table C-3 CiscoWorks Roles and AUS Privileges

AUS Privilege ¹	CiscoWorks Role				
	System Admin	Network Admin	Network Operator	Approver	Help Desk
API_View_Device GUI_View_Device	X	X	X	X	X
API_View_Images GUI_View_Images	X	X	X	X	X
API_View_Assignment GUI_View_Assignment	X	X	X	X	X
API_View_Reports GUI_View_Reports	X	X	X	X	X
API_View_Admin GUI_View_Admin	X	X	X	X	X
API_Modify_Device GUI_Modify_Device	X	X	–	X	–

Table C-3 CiscoWorks Roles and AUS Privileges (continued)

AUS Privilege ¹	CiscoWorks Role				
	System Admin	Network Admin	Network Operator	Approver	Help Desk
API_Modify_Images GUI_Modify_Image	X	X	–	–	–
API_Modify_Assignment GUI_Modify_Assignment	X	X	–	–	–
API_Modify_Admin GUI_Modify_Admin	X	X	–	–	–
API_Modify_Admin GUI_Modify_Admin	X	X	–	–	–

1. See [Table C-1](#) for descriptions.

Cisco Secure ACS Roles and AUS Privileges

Cisco Secure ACS supports roles that are application-specific. A higher-level role includes all privileges associated with lower-level roles. Unlike other applications that use ACS for authentication, AUS checks authorization with itself, not on a per-device basis.

You can use the AUS roles already defined in ACS, or you can create your own, customized roles.

For more information about using ACS and for an understanding of ACS security advantages, see the *User Guide for Cisco Secure ACS for Windows Server 3.3* and *Release Notes for Cisco Secure Access Control Server for Windows Server 3.3*.

[Table C-4](#) lists default roles for use with AUS.

Table C-4 ACS Roles

Role	Description
System Administrator	Full privileges (superuser).
Network Administrator	Full privileges (superuser).
Network Operator	Read privileges for the GUI.

Table C-4 ACS Roles (continued)

AUS Remote Interface	Privileges to access only the external interface and not the GUI.
Help Desk ¹	Read-only privileges for nonsensitive data.
API Reader	Read privileges for external interface.
API Writer	Read and write privileges for external interface.
GUI Reader	Read privileges for viewing information on the GUI.
GUI Writer	Read and write privileges for viewing and modifying information on the GUI.

1. All CiscoWorks Server roles allow you to perform Help Desk tasks.

**Note**

For communication between Security Manager and AUS to be successful, the username and password entered for AUS in Security Manager must be associated with the API_Writer role, a role that has the same privileges, or the AUS remote interface.

Table C-5 lists default AUS roles and their supported privileges.

Table C-5 ACS Roles and AUS Privileges

AUS Privilege ¹	ACS Role							
	System Admin	Network Admin	Network Operator	Help Desk	API Reader	GUI Reader	API Writer	GUI Writer
API_View_Device	X	X	X	–	X	–	X	–
GUI_View_Device	X	X	X	X		X	–	X
API_View_Images	X	X	X	–	X	–	X	–
GUI_View_Images	X	X	X	X		X	–	X
API_View_Assignment	X	X	X	–	X	–	X	–
GUI_View_Assignment	X	X	X	X		X	–	X
API_View_Reports	X	X	X	–	X	–	X	–
GUI_View_Reports	X	X	X	X		X	–	X

Table C-5 ACS Roles and AUS Privileges (continued)

AUS Privilege ¹	ACS Role							
	System Admin	Network Admin	Network Operator	Help Desk	API Reader	GUI Reader	API Writer	GUI Writer
API_View_Admin	X	X	X	X	X	–	X	–
GUI_View_Admin	X	X	X	–	–	X	–	X
API_Modify_Device	X	X	–	–	–	–	X	–
GUI_Modify_Device	X	X	–	–	–	–	–	X
API_Modify_Images	X	X	–	–	–	–	X	–
GUI_Modify_Images	X	X	–	–	–	–	–	X
API_Modify_Assignment	X	X	–	–	–	–	X	–
GUI_Modify_Assignment	X	X	–	–	–	–	–	X
API_Modify_Admin	X	X	–	–	–	–	X	–
GUI_Modify_Admin	X	X	–	–	–	–	–	X

1. See [Table C-1](#) for descriptions.