



CHAPTER 3

Security Manager and Cisco Secure ACS

This chapter describes how to troubleshoot common problems that could occur because of the way Security Manager and Cisco Secure ACS interact. It contains the following topics:

- [Using Multiple Versions of Security Manager with Same ACS, page 3-1](#)
- [Authentication Fails When in ACS Mode, page 3-2](#)
- [System Administrator Granted Read-Only Access, page 3-2](#)
- [ACS Changes Not Appearing in Security Manager, page 3-3](#)
- [Devices Configured in ACS Not Appearing in Security Manager, page 3-3](#)
- [Working in Security Manager after Cisco Secure ACS Becomes Unreachable, page 3-3](#)
- [Restoring Access to Cisco Secure ACS, page 3-4](#)
- [Authentication Problems with Multihomed Devices, page 3-4](#)
- [Authentication Problems with Devices Behind a NAT Boundary, page 3-4](#)
- [Updating Device Credentials via Cisco Secure ACS](#)

Using Multiple Versions of Security Manager with Same ACS

You cannot use the same Cisco Secure ACS with two different versions of Security Manager. For example, if you have integrated Security Manager 3.0.1 with a Cisco Secure ACS and another part of your organization plans to use Security Manager 3.2 *without* upgrading the existing installation, you must integrate Security Manager 3.2 with a different ACS than the one used for Security Manager 3.0.1.

If you upgrade an existing Security Manager installation, you can continue to use the same Cisco Secure ACS. The permission settings will be updated as required.

Authentication Fails When in ACS Mode

If authentication keeps failing when you log in to Security Manager or CiscoWorks Common Services, even though you used Common Services to configure Cisco Secure ACS as the AAA server for authentication, do the following:

- Ensure that there is connectivity between the ACS servers and the server running Common Services and Security Manager.
- Ensure that the user credentials (username and password) you are using are defined in ACS and are assigned to the appropriate user group.
- Ensure that the Common Services server is defined as a AAA client on the Network Configuration page of ACS. Verify that the shared secret keys defined in Common Services (AAA Mode Setup page) and ACS (Network Configuration) match.
- Ensure that the IP address of each ACS server is correctly defined on the AAA Mode Setup page in Common Services.
- Ensure that the correct account is defined on the Administration Control page of ACS.
- Go to the AAA Mode Setup page in Common Services and verify that Common Services and Security Manager (as well as any other installed applications, such as AUS) are registered with Cisco Secure ACS.
- Go to Administration Control > Access Setup in ACS and ensure that the ACS is configured for HTTPS communication.
- If you receive “key mismatch” errors in the ACS log, check whether the Security Manager server is defined as a member of a network device group (NDG). If it is, be aware that if you defined a key for the NDG, that key takes precedence over the keys defined for the individual devices in the NDG, including the Security Manager server. Ensure that the key defined for the NDG matches the secret key of the Security Manager server.

System Administrator Granted Read-Only Access

Problem You have read-only access to all policy pages of Security Manager even after logging in as a System Administrator with full permissions.

Solution Do the following in Cisco Secure ACS:

- (When using network device groups (NDGs)) Click **Group Setup** on the Cisco Secure ACS navigation bar, then verify that the System Administrator user role is associated with all necessary correct NDGs for *both* CiscoWorks and Cisco Security Manager, especially the NDG containing the Common Services/Security Manager server.
- Click **Network Configuration** on the navigation bar, then:
 - Verify that the Common Services/Security Manager server is not assigned to the Not Assigned (default) group.
 - Verify that the Common Services/Security Manager server is configured to use TACACS+ not RADIUS. TACACS+ is the only security protocol supported between the two servers.



Note You can configure the network devices (routers, switches, firewalls, and so on) managed by Security Manager for either TACACS+ or RADIUS.

ACS Changes Not Appearing in Security Manager

When you are using Security Manager with Cisco Secure ACS 4.x, information from ACS is cached when you log into Security Manager or CiscoWorks Common Services on the Security Manager server. If you make changes in the Cisco Secure ACS Network Configuration and Group Setup while logged into Security Manager, the changes might not appear immediately or be immediately effective in Security Manager. You must log out of Security Manager and Common Services and close their windows, then log in again, to refresh the information from ACS.

If you need to make changes in ACS, it is best practice to first log out of and close Security Manager windows, make your changes, and then log back into the product.

**Note**

Although Cisco Secure ACS 3.3 is not supported, if you are using that version of ACS, you must open Windows Services and restart the Cisco Security Manager Daemon Manager service to get the ACS changes to appear in Security Manager.

Devices Configured in ACS Not Appearing in Security Manager

Problem The devices that you configured on the Cisco Secure ACS are not appearing in Security Manager.

Solution The device display names defined in Security Manager *must* match the names you configure in ACS when you add the devices as AAA clients. This is particularly important when you use domain names. If you intend to append a domain name to the device name in Security Manager, the AAA client hostname in ACS must be `<device_name>.<domain_name>`, for example, `pixfirewall.cisco.com`.

Working in Security Manager after Cisco Secure ACS Becomes Unreachable

Security Manager sessions are affected if the Cisco Secure ACS cannot be reached. Therefore, you should consider creating a fault-tolerant infrastructure that utilizes multiple Cisco Secure ACS servers. Having multiple servers helps to ensure your ability to continue work in Security Manager even if connectivity is lost to one of the ACS servers.

If your setup includes only a single Cisco Secure ACS and you wish to continue working in Security Manager in the event the ACS becomes unreachable, you can switch to performing local AAA authentication on the Security Manager server. To change the AAA mode, do the following:

-
- Step 1** Log in to Common Services using the *admin* CiscoWorks local account.
 - Step 2** Select **Server > Security > AAA Mode Setup**, then change the AAA mode back to Non-ACS/CiscoWorks Local. This enables you to perform authentication and authorization using the local Common Services database and its built-in roles. Bear in mind that you must create local users in the AAA database to make use of local authentication.
 - Step 3** Click **Change**.
-

Restoring Access to Cisco Secure ACS

If you cannot access Security Manager because the Cisco Secure ACS is down, do the following:

- Open up Windows Services on the ACS server and check whether the CSTacacs and CSRADIUS services are up and running. Restart these services, if required.
- Perform the following procedure in CiscoWorks Common Services:

-
- Step 1** Log in to Common Services as the Admin user.
- Step 2** Open a DOS window and run `NMSROOT\bin\perl ResetLoginModule.pl`.
- Step 3** Exit Common Services, then log in a second time as the Admin user.
- Step 4** Go to **Server > Security > AAA Mode Setup**, then change the AAA mode to Non-ACS > CW Local mode.
- Step 5** Open Windows Services and restart the Cisco Security Manager Daemon Manager service.
-

Authentication Problems with Multihomed Devices

Problem You cannot configure a multihomed device (a device with multiple network interface cards (NICs)) that was added to the Cisco Secure ACS, even though your user role includes Modify Device permissions.

Solution When you define a multihomed device as a AAA client of the Cisco Secure ACS, make sure to define the IP address of each NIC. Press **Enter** between each entry. For more information, see *Adding Devices as AAA Clients Without NDGs* in the *User Guide for Cisco Security Manager* for your release (at http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html). In addition, you must modify the gatekeeper.cfg file on the Security Manager server after completing the installation process. For more information, see the *Installation Guide for Cisco Security Manager* for your release at http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html.

Authentication Problems with Devices Behind a NAT Boundary

Problem You cannot configure a device with a pre-NAT or post-NAT IP address that was added to the Cisco Secure ACS, even though your user role includes Modify Device permissions.

Solution When a device is behind a NAT boundary, make sure to define all IP addresses, including pre-NAT and post-NAT, for the device in the AAA client configuration settings in Cisco Secure ACS. For more information on how to add AAA client settings to ACS, see *User Guide for Cisco Secure Access Control Server*.

Updating Device Credentials via Cisco Secure ACS

Problem You update the credentials of your managed devices on a regular basis and want your Cisco Secure ACS to automatically update Security Manager with these new credentials.

Solution Perform the following procedure in CiscoWorks Common Services:

-
- Step 1** Log in to Common Services as the Admin user.
- Step 2** Click the **Device and Credentials** tab, then click **Device Management**.
- Step 3** On the Device Management page, click **Bulk Import**.
- Step 4** In the Import Devices popup window, do the following:
- a. In the Select a Layer field, click **Remote NMS**.
 - b. From the NMS Type list, select **ACS**.
 - c. Enter the details of your Cisco Secure ACS, including the hostname, username, password, and port.
 - d. In the Conflict Resolution Option field, select **Use Data from Import Source**.
 - e. Set the schedule for performing the bulk import. For example, to update Security Manager with new device credentials once a month, select **Monthly** as the Run Type, then define a start date and time.
 - f. Click **Import**.
-

