



APPENDIX **B**

Troubleshooting AUS

These topics will help you troubleshoot AUS:

- [Why isn't the device showing up in the Device Summary?](#)
- [Why hasn't the device contacted the AUS?](#)
- [AUS gives authentication errors—what should I do?](#)
- [Why isn't the device current after I request an auto update?](#)
- [Why can't I access the AUS from my browser after several hours?](#)
- [Why can't I add a file that is not a ASA image, PIX security appliance image, ASDM image file or PDM image file through the AUS GUI?](#)
- [I assigned an image file to a device—why isn't it current?](#)
- [Why can't I assign two image files of the same type to a device?](#)
- [Why does the device reboot after I assign a new PIX security appliance image or ASA software image to it?](#)
- [Why does the device keep downloading the same file?](#)
- [Why aren't reports from more than 7 days ago displayed?](#)
- [Why can't I access the AUS from my browser after several hours?](#)
- [Why are buttons are grayed-out on certain screens?](#)
- [Why can't I start AUS after I reboot my machine?](#)
- [If I uninstall Security Manager, how do I remove devices from AUS?](#)
- [How can I stop a device from trying to download a faulty or incorrect configuration file?](#)

Why isn't the device showing up in the Device Summary?

- [How can I check the connection between AUS and a PIX security appliance or an ASA device?](#)
- [What can I do if configuration errors are reported?](#)
- [How do I ensure that my IOS device is subscribing to the correct CNS subjects?](#)
- [What can I do if devices do not show up in the CNS Devices Report?](#)
- [Understanding Error Messages](#)

Why isn't the device showing up in the Device Summary?

If the device is not shown in the Device Summary, it was not added correctly to the Security Manager.

To correct the problem:

-
- Step 1** Use Security Manager to add the device to AUS. For more information, see [Adding Devices of Auto Update Type to the Security Manager Inventory, page A-4](#).
 - Step 2** To verify that the device was added to AUS, select **Device > Device Summary**.
 - Step 3** To make sure that the device was deployed to AUS, check Security Manager for deployment errors.
-

Why hasn't the device contacted the AUS?

If the device has never contacted AUS, it could be because:

- The device is not configured with the correct AUS URL.
- The device does not have network connectivity.
- The credentials for the device in AUS are incorrect.
- The device is configured correctly but has not yet polled AUS.

- You are not using the correct PIX security appliance software version.

For the device to contact AUS, do one or more of the following:

- Wait for the polling period to end.



Note The default polling period is 12 hours. You can use Security Manager to change the polling period. See the Security Manager documentation or online help for more information.

- If the device has not contacted AUS after the polling period ends, verify that the device can connect to AUS by pinging it from the device console. To do this, from the device console, enter:

```
ping outside <AUSIPAddress>
```

- Verify that the device is configured to operate in its deployed environment. If it is deployed for DHCP, ensure that a DHCP server is present to give the device a network address. If the device is deployed with a static IP address, verify that the IP address is correct.
- Check the Event Report to see if there are any authentication errors for the device by selecting Report > Event Report. If there are authentication errors, the Event Type column displays CONNECT_FAILURE and the description column gives a message that the device has an authentication error.
- Check the AutoUpdate URL to verify that it matches the URL in the System Info report (Report > System Info Report) by performing the following steps:

- a. Connect to the device console.

- b. Enter Enable mode. Enter:

```
en
```

- c. Enter the enable password that you previously set.

- d. Enter:

```
show auto-update
```

You will see all AUS settings, including the AUS URL.

- If the URL does not match the URL shown in the System Info report, set the new AUS URL by entering the following.

```
conf t
auto-update server
```

AUS gives authentication errors—what should I do?

```
https://username:password@AUSserverAddress:port/autoupdate/
AutoUpdateServlet
```

- Make sure that you are using PIX security appliance software version 6.2 or later (earlier PIX security appliance software versions will not work with AUS). See *Supported Devices and Software Versions for Auto Update Server 3.0* for more information.
- Check the AUS logs to see if there are any errors.

AUS gives authentication errors—what should I do?

Authentication errors can occur when the device tries to contact AUS. Authentication errors are visible in the Event Report (see [Viewing the Event Report, page 6-3](#)) or from the device console (if debug is enabled on the console).

To enable debug on the console:

Step 1 Enter Enable mode by entering:

```
en
```

Step 2 Enter your enable password.

Step 3 Enter the following:

```
conf t
logging on
logging console debug
```

The device displays all error messages; you can use the information to debug the device.

Authentication errors can result from using incorrect credentials:

- When you added the device to AUS, you entered a set of credentials that allowed the device to contact the server. The username/password credentials are incorrect.
- A user changed, through the command line, the set of credentials that the device was using to connect to AUS. Now, the set of credentials no longer matches the server credentials.

To resolve the problem, do one or more of the following:

- Wait until the device contacts AUS and reports the new configuration file.
- Access the device to resolve authentication problems. See the appropriate device documentation.
- Use the command line from Security Manager to change your username and password. Enter:

```
en
conf t
auto-update server
https://username:password@AUSServerAddress:port/autoupdate/
AutoUpdateServlet
```

Why isn't the device current after I request an auto update?

If you requested that a device immediately contact AUS (see [Requesting an Auto Update, page 3-12](#)), but the device is not current, the cause could be one of the following:

- The request has not yet gone through the queue. If you requested that multiple devices immediately contact AUS, it might take a period of time for the request to go through, as AUS processes requests one at a time.
- The device is not accessible.
- The CLI commands generated by Security Manager for the configured policy definitions are incorrect.

To resolve the problem, do one or more of the following:

- Wait a few moments for the request to go through the queue.
- Verify that the device is not behind a firewall or NAT boundary. The Request Auto Update command does not work on such devices; you must wait until the polling period ends before the device is current.
- Ensure that the device identity configured in the Security Manager inventory matches the device ID configured on the device.
- View the Event report to check whether any command was generated incorrectly for any of the policy settings.

Why does the AUS give errors when I try to add a PDM, ASDM, ASA or PIX security appliance software image file?

If you are trying to add a PDM, ASDM, ASA, or PIX security appliance software image file to AUS and are receiving error messages, the problem might be one of the following:

- You are not selecting the correct image type to assign to the device.
- The image file that you are adding is not correct, or it is corrupted.

You can resolve the problem by doing one or more of the following:

- Make sure that you select the correct image type when adding the file.
- Verify that the image file is not corrupted. Check the MD5 checksum of the image file. To view the checksum value, select **Images > Software Images**. Click the name of the image file in the Image Name column. A popup window appears, providing you with information about the image file, including the checksum value. For more information, see the [Viewing the File Summary Page, page 4-1](#).

Compare this checksum value with the value you received when the image was downloaded. If they are different, the image file is corrupted.

Why can't I add a file that is not a ASA image, PIX security appliance image, ASDM image file or PDM image file through the AUS GUI?

The AUS GUI supports only ASDM and PDM image files, and ASA and PIX security appliance images; therefore, you cannot use it to add any other types of files.

If you are trying to add configuration files, use Security Manager. See the Security Manager documentation for more information.

I assigned an image file to a device—why isn't it current?

If you assigned an image file to a device but the device does not contain this information, the problem could be because:

- The device must contact AUS to report that it is running an image file. Depending on the polling period of the device, you might need to wait several hours for an update.
- The device is having problems contacting AUS.
- The image file is bad.

To resolve the problem, do one or both of the following:

- Check the AUS timestamp to verify the last time the device contacted AUS. If the polling period has not ended, then the device has not contacted AUS to report the latest information. If you do not want to wait for the polling period to end, you can request that the device contact AUS immediately (see [Requesting an Auto Update, page 3-12](#)).
- Check the Event Report (select **Report > Event Report**) to look for errors. If a bad image file is assigned to the device, you will see the `DEVICE_CONFIG_ERROR` event type in the Event report. This event type denotes that an error occurred while downloading the image file. Assign a new image file to the device or remove the assignment to revert to the previously configured image file on the device.

**Note**

If the device has not contacted AUS to report that it is running an image file, see [Why hasn't the device contacted the AUS?, page B-2](#).

Why can't I assign two image files of the same type to a device?

A device can run only one ASA software image, PIX security appliance software image, ASDM file, or PDM file at a time, so you can assign only one file of each type to a device.

Why does the device reboot after I assign a new PIX security appliance image or ASA software image to it?

After you assign a new PIX security appliance software image or ASA software image to a device, a reboot is required. The reboot is automatic.

Why does the device keep downloading the same file?

If a device continuously downloads a file, the device is having problems running the image.

Check the Event Report (select **Report > Event Report**) for errors. If there are errors, assign a new image file.

Why aren't reports from more than 7 days ago displayed?

AUS reports show data only from the past 7 days; they do not show data from any time earlier.

Why can't I access the AUS from my browser after several hours?

Your AUS session automatically times out after 2 hours of idle time. To access AUS, log in to AUS again.

Why are buttons are grayed-out on certain screens?

If buttons are grayed out on certain AUS screens, you might not have the correct privileges to perform certain commands. See [Appendix C, “User Roles and Permissions.”](#)

Why can't I start AUS after I reboot my machine?

It takes AUS a few minutes to restart after you reboot your machine. Do one of the following:

- Wait a few minutes before starting AUS.
- Check the AUS error logs to ensure that all processes are running properly.

If I uninstall Security Manager, how do I remove devices from AUS?

You can delete devices using AUS. For details, see [Deleting Devices, page 3-11](#).

How can I stop a device from trying to download a faulty or incorrect configuration file?

You can unassign the configuration file. For details, see [Assigning and Unassigning Files to a Single Device, page 5-4](#). After unassigning the configuration file, correct and redeploy it using Security Manager.

How can I check the connection between AUS and a PIX security appliance or an ASA device?

If you have not installed Security Manager yet, or you simply want to check the connection between AUS and a device, you can add the device to AUS manually. For details, see [Adding a Device Directly to AUS, page 3-5](#).

At the defined interval, the device will contact AUS. Verify that the device contacted AUS by reviewing the Event report. See [Viewing the Event Report, page 6-3](#).

After verifying that the connection between AUS and the device is correct, delete the device from AUS.

What can I do if configuration errors are reported?

If the Event Failure Summary report shows configuration errors, view the suspected configuration file to find the problem. See [Viewing Configuration Files, page 4-4](#).

Use the line number in the configuration error to locate the fault in the configuration file.

Why is the display format difficult to read in Netscape?

AUS is configured to use optimum font settings for readable and usable displays. Changing these font settings results in displays that might be difficult to read. We recommend that you do not override the default font settings. Use only the default font settings for AUS.

How do I ensure that my IOS device is subscribing to the correct CNS subjects?

To verify the list of subjects subscribed, enter the **show cns event subjects** command from the device CLI. If successful, the device displays the following list of subjects:

- cisco.cns.config.load
- cisco.cns.inventory.get
- cisco.cns.exec.cmd

Make sure that cisco.cns.exec.cmd is listed. Otherwise, enter **cns exec 80** to configure the device to register for the required event subjects, where 80 is the default port number. For more information, see [Bootstrapping CNS Devices, page D-5](#).

What can I do if devices do not show up in the CNS Devices Report?

-
- Step 1** Make sure that the CNSEventGateway process is running:
- a. From the CiscoWorks desktop, select **Server Configuration > Administration > Process Management > Process Status**.
 - b. If the state is Program started - No mgt msgs received or Program Running, go to [Step 4](#).
- Step 2** If the CNSEventGateway process did not start, verify that the ESS (Event Services) process is running:
- a. From the CiscoWorks desktop, select **Server Configuration > Administration > Process Management > Process Status**.
 - b. If the state is Program started - No mgt msgs received or Program Running, go to [Step 4](#).
- Step 3** If neither of these processes is running, restart both processes:
- a. From the CiscoWorks desktop, select **Server Configuration > Administration > Process Management > Start Process**.

b. Verify that the CNSEventGateway and ESS processes are displayed.

c. Click **Finish**.

Step 4 If the CNSEventGateway is running and you are able to launch AUS, but the device still does not show up in the CNS Devices report, verify that the device is properly configured and that it is connected to the CNS Event Gateway:

a. Log in to the device console.

b. Enter **show cns event connections**.

The display shows the status of the event agent connection, such as whether it is connecting to the gateway, connected, or active. It also displays the gateway used by the event agent and its IP address and port number.

c. If device still does not show up in the CNS Devices report, try to clear the CNS event by entering the following commands in the order given:

- **config terminal**
 - **no cns event ip**
 - **cns event ip**
-

Understanding Error Messages

You can check the following logs for information about errors:

- *NMSROOT\MDC\log\operation\autoupdate.log*—AUS log that contains all messages from the AUS application.
- *NMSROOT\MDC\tomcat\logs\stdout.log*—Tomcat output log that contains messages from any application running under tomcatServletEngine.
- *NMSROOT\MDC\tomcat\logs\stderr.log*—Tomcat standard error log that contains a java stack trace when the java code breaks.
- *NMSROOT\MDC\log\operation\CNSEventGateway-*portnumber*.log*—Log that contains information about the communication between the CNS Event gateway running on AUS and any device. One entry is logged per device. The *portnumber* value in the *CNSEventGateway-*portnumber*.log* denotes the port that the device uses to contact the event gateway. The default port is 11011.



Note *NMSROOT* is the directory in which AUS is installed.

Table B-1 displays common error messages, their probable causes, and possible solutions.

Table B-1 *AUS Error Messages*

Message	Probable Cause	Possible Solution
CALLHOME-DB-ADD_FILE_FAILURE	An error occurred when the file was being added to AUS. A database communications problem occurred.	Try to add the file to AUS again. If that does not work, restart AUS.
CALLHOME-FILE-INVALID_FILE_NAME	The filename is incorrect. The name of the file is either too long or too short, or the file is named “.” or “..”.	Enter the correct filename.
CALLHOME-FILE-INVALID_FILE_CONTENTS	You added a file that is either corrupt or is not the correct file type.	Replace the file or try to add a different file.
CALLHOME-FILE_NOT_FOUND	The selected file could not be found. You already deleted this file from the database.	Please refresh the screen by clicking the Files tab.
CALLHOME-FILE-BAD_FILE_NAME	There was a problem when AUS tried to access the file. Either the file does not exist or it cannot be read.	Verify that the file exists and that it is not corrupt.

Table B-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
CALLHOME-FILE-INVALID_IMAGE	You cannot add the file to AUS; either the file is corrupted or you are trying to add a file type that is different from the file type specified in the GUI.	Download a new version of the image file and add the file to AUS.
CALLHOME-DEVICE-NOT_CALLED_HOME_YET	The device did not contact AUS; AUS does not know the IP address of the device.	Wait until the device contacts the AUS and requests an auto update (see Requesting an Auto Update, page 3-12).
CALLHOME-SECURITY-NOT_AUTHENTICATED	AUS cannot authenticate your username/password credentials. Either your credentials are incorrect or your session timed out.	Reenter your username and password and log in to AUS.
CALLHOME-COMMON-AUDIT_FAILED	AUS cannot write to either the ACS or the Core audit log. A communication error occurred.	Restart AUS. If the problem persists, contact Cisco technical support.
CALLHOME-DEVICE_NOT_FOUND	AUS cannot find the selected device. The device was already deleted from the database.	Refresh the screen by clicking the Devices tab.
CALLHOME-FILE-CANNOT_DELETE_FILE	You cannot delete the file. The file is in use.	Try to delete the file again. If you cannot delete the file, restart AUS.

Table B-1 **AUS Error Messages (continued)**

Message	Probable Cause	Possible Solution
CALLHOME-DEVICE-BAD_ CALLHOME_IMMEDIATE_ RESPONSE	An error occurred during auto update. Enable or AAA credentials are incorrect, or the device does not allow HTTP access.	Ensure that the device allows HTTP access for AUS; ensure that the AUS AAA and enable credentials are correct.
CALLHOME-FILE-MOVE_ERROR	The temporary file used when you added the file cannot be deleted. The filename you specified contains invalid or illegal characters, or the file already exists in the storage area.	Check the storage directory to verify that the file is not already there. Try the task again; if the problem persists, restart AUS and try to add the configuration file again. Check the log file for errors.
CALLHOME-DEVICE-CH_ IMMEDIATE_NO_CREDENTIALS	AUS cannot perform an auto update. AUS does not know what credentials to use to communicate with the device because no enable password or AAA credentials were entered for the device.	Modify the device entry with the correct credentials and try the task again.
CALLHOME-INVALID_UPLOAD_ FILE	The file is invalid.	Enter a valid filename.
CALLHOME-DB-NO_CONNECTION	AUS cannot connect to the database. The database server is stopped.	Restart AUS and try the task again.

Table B-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
CALLHOME-DB-BAD_PASSWORD_STATE	An error occurred while the database password was being changed. The AUS db.prop file does not contain the correct username and password for the database, or you entered the password incorrectly.	Verify that the AUS db.prop file contains the correct username and password for the database and enter your username and password again.
CALLHOME-DB-COMMIT_ERROR	AUS is unable to write data to the database.	Restart AUS and try the task again.
CALLHOME-DB-POOL_ERROR	AUS is unable to connect to the database.	Restart AUS and try the task again.
CALLHOME-DB-DISK_FULL	You ran out of disk space.	Remove unneeded information from your hard drive or add a new hard drive.
CALLHOME-DB-ADD_DEVICE_FAILURE	There is a problem adding the device to the system. A database communications problem occurred.	Try to add the device again. If you still cannot add the device to AUS, restart AUS.
CALLHOME-DB-ADD_FILE_FAILURE	There is a problem adding the file to the system. A database communications problem occurred.	Try to add the file again. If you still cannot add the file to AUS, restart AUS.
CALLHOME-DB-DUPLICATE_VALUE	You are trying to add a file that already exists in AUS.	Use the existing entry, or delete the existing entry and retry the task.

Table B-1 **AUS Error Messages (continued)**

Message	Probable Cause	Possible Solution
CALLHOME-DB-DEVICE_NOT_FOUND	AUS cannot find the requested device. A device that was added to AUS tried to contact AUS.	Verify that you entered the correct device ID and try the task again.
CALLHOME-DEVICE-INVALID_AUTHORIZATION	The device passed invalid authorization information. Check the device username and password.	Update the device username and password.
CALLHOME-FILE-CHECKSUM_MISMATCH	The checksum of the file has changed since the file was added to the database. Either another user changed the file or your system is compromised.	Make sure your machine is secure. Then delete the image file and add a new copy of the file to AUS.
CALLHOME-DEVICE_CNS_NO_RESPONSE	AUS cannot contact the device. The device is not connected to the CNS Event Gateway.	Please ensure that the device is properly configured to connect to the CNS Event Gateway.
CALLHOME-DEVICE_CNS_SHOW_ERROR	An error occurred during the running of the show command. You entered an invalid command.	Please enter a valid command.

Table B-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
CALLHOME-DEVICE_CNS_NO_DYNAMIC_INT	<p>Either the device does not have a DHCP interface or the DHCP interface has one of the following errors: no assigned address, protocol down, or interface down.</p> <p>You did not configure the DHCP interface properly on the device.</p>	Please configure a dynamic IP address on one of the interfaces.
CALLHOME-DEVICE_CNS_EMPTY_IDLIST	<p>The device list that was passed is empty.</p> <p>Incorrect XML was passed.</p>	Please try the task again.
CALLHOME-INVALID_UPLOAD_FILE	The filename is invalid.	Please enter a valid filename to upload.
CALLHOME-UI_CANNOT_MODIFY_CONFIG_MAPPING	The assignments for the configuration file cannot be modified.	Please use Security Manager to modify the configuration file.
CALLHOME-UI_INVALID_IPADDRESS	<p>The IP address is invalid.</p> <p>You entered an invalid IP address.</p>	Please enter a valid IP address.
CALLHOME-UI_MULTICAST_ADDRESS	<p>The multicast address is not within the RFC multicast range (224.0.0.0-239.255.255.255).</p> <p>An invalid multicast address was entered.</p>	Please enter a valid multicast IP address.

Table B-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
CALLHOME-UI_NO_DEVICE_EXIST	The device no longer exists. You might have already deleted the device.	Please refresh the screen by clicking the Devices tab.
CALLHOME-BOUNDS-INVALID_EMPTY_START_UPDATE_WINDOW_TIME	The start time for auto update schedule was left blank. You did not enter the time for auto update to start.	Please enter the start time using the HH:MM format.
CALLHOME-BOUNDS-INVALID_EMPTY_END_UPDATE_WINDOW_TIME	The end time for auto update schedule is left blank. You did not enter the time for auto update to end.	Please enter the end time using the HH:MM format.
CALLHOME-BOUNDS-INVALID_EMPTY_UPDATE_WINDOW_DAY_INFO	The day of the week on which you want a weekly auto update to occur was left blank. You did not select the days of the week for auto updates to occur.	Please schedule the days of the week on which weekly update must occur.
CALLHOME-COMMON-MISSING_UPDATE_WINDOW	The update schedule type is missing. A null or invalid device ID object was passed.	Please ensure that the device ID is passed properly.
CALLHOME-BOUNDS-INVALID_UPDATE_WINDOW_TYPE	The configured update schedule type is invalid. You configured an invalid update schedule type.	Please ensure that the update schedule type is configured properly.

Table B-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
CALLHOME-UPDATE_WINDOW_NOT_CONFIGURED	The auto update schedule cannot be deleted. You did not configure an update schedule.	Please schedule a configuration update first before you try to delete it.
CALLHOME-UPDATE_WINDOW_UNSUCCESSFUL	The update schedule configuration was unsuccessful. You already configured an update schedule type for the device.	Please delete the existing update schedule configuration.