APPENDIX A

Troubleshooting AUS

These topics will help you troubleshoot AUS:

Why Is the Device Not 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 inventory. The method for adding devices using Security Manager is explained in Updating Configuration Files, page 1-8.

After deploying a configuration as described in that topic, check the Security Manager deployment results to ensure deployment was successful. Also, check AUS event reports to ensure the device successfully contacted AUS and retrieved the configuration.

If deployment was successful and the device successfully downloaded the configuration, it should appear in the AUS device list.

Why Has the Device Not Contacted 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 firewall software version. (You must use a minimum of release 6.3.) All versions of ASA are supported.

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

- Wait for the polling period to end.
- If the device has not contacted AUS after the polling period ends, verify that the device can connect to AUS by logging into the device and pinging the AUS server from the device console.
- 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 **Auto Update Server > Reports > Events** in AUS. 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 Auto Update URL to verify that it matches the URL in the system information report (**Auto Update Server > Reports > System Info**). Log into the device, enter enable mode, and enter show auto-update to view the AUS settings configured on the device.

  If the URL does not match the URL shown in the system information report, set the new AUS URL by entering the following.

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

- 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 5-4) or from the device console (if debug is enabled on the console).

To enable debug on the device console, log into the device, enter enable mode, and configure the following commands:

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

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. These credentials come from Security Manager for devices that it adds (the HTTP username and password and the enable password).
- A user changed, through the command line, the set of credentials that the device was using to connect to AUS. Now the credentials no longer match 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.
- Log into the device and use the command line to change the username and password. Enter:

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

Why Is the Device Not Current After I Request an Auto Update?

If you requested that a device immediately contact AUS for an auto update (see Requesting an Immediate Auto Update, page 2-6), 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 Update Now command does not work on such devices; you must wait until the polling period ends for the device to obtain the update.
- Ensure that the device identity configured in the Security Manager inventory matches the device ID configured on the device. Ensure that the correct HTTP username and password, and enable password, are correct.
- View the event report to check whether any command was generated incorrectly for any of the policy settings.

Why Does AUS Give Errors When I Try to Add an Image File?

If you are trying to add a PDM, ASDM, ASA, or PIX 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 file.
- The image file that you are adding is not correct, or it is corrupted.
- The file name does not fit the expected file naming pattern.

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.
- Make sure that you do not change the file name when you download the file from Cisco.com.
- Verify that the image file is not corrupted. Check the MD5 checksum of the image file. To view the checksum value, select **Auto Update Server > Files** and click the name of the image file in the Name column. A popup window appears with information about the file, including the checksum value. For more information, see the Viewing the File Summary Page, page 3-1.

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

Why Cannot I Add a Configuration File?

You can add only ASDM, PDM, ASA, and PIX software image files. To add configuration files, you must use Security Manager to configure the device and to deploy the configuration to AUS. For an explanation of the process, see Updating Configuration Files, page 1-8.

I Assigned an Image File To a Device—Why Is It Not Current?

If you assigned an image file to a device but the device does not contain this file, 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 Immediate Auto Update, page 2-6).
- Check the event report (select **Auto Update Server > Reports > Events)** 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 report, which indicates 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.

  If the device has not contacted AUS to report that it is running an image file, see Why Has the Device Not Contacted AUS?, page A-2.

Why Cannot I Assign Two Image Files of the Same Type To A Device?

A device can run only one ASA software image, PIX 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 or ASA Software Image To It?

After you assign a new ASA or PIX 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 **Auto Update Server > Reports > Events**) for errors. If there are errors, assign a new image file.

Why Are Some Buttons Grayed-Out?

If buttons are grayed out on certain AUS screens, you do not have the correct privileges to perform those commands. See Appendix B, "User Roles and Permissions."

Why Cannot 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.

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 4-3. After unassigning the configuration file, correct and redeploy it using Security Manager.

How Can I Check the Connection between AUS and a PIX or 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 2-3.

At the defined interval, the device contacts AUS. Verify that the device contacted AUS by reviewing the event report. See Viewing the Event Report, page 5-4.

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 3-3.

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

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.

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

Table A-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 does not follow the expected naming pattern.	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.

Table A-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
CALLHOME-FILE_NOT_FOUND	The selected file could not be found. You already deleted this file from the database.	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.
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 AUS.	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 Immediate Auto Update, page 2-6).
CALLHOME-SECURITY-NOT_ AUTHENITCATED	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.
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. See Adding a Device Directly to AUS, page 2-3.
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. See Adding a Device Directly to AUS, page 2-3.

Table A-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
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.
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.
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-INVALID_UPLOAD_ FILE	The filename is invalid.	Enter a valid filename to upload.
CALLHOME-UI_CANNOT_MODIFY_ CONFIG_MAPPING	The assignments for the configuration file cannot be modified.	Use Security Manager to modify the configuration file.

Table A-1 AUS Error Messages (continued)

Message	Probable Cause	Possible Solution
CALLHOME-UI_INVALID_ IPADDRESS	The IP address is invalid. You entered an invalid IP address.	Enter a valid IP address.
CALLHOME-UI_MULTICAST_ ADDRESS	The multicast address is not within the RFC multicast range (224.0.0.0-239.255.255.255). An invalid multicast address was entered.	Enter a valid multicast IP address.
CALLHOME-UI_NO_DEVICE_EXIST	The device no longer exists. You might have already deleted the device.	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.	Enter the start time using the HH:MM format.
CALLHOME-BOUNDS-INVALID_ EMPTY_END_UPDATE_WINDOW_ TIME	The duration for the auto update schedule is left blank. You did not enter the duration time for the auto window.	Enter the duration 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.	Select the day 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.	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.	Ensure that the update schedule type is configured properly.
CALLHOME-UPDATE_WINDOW_ NOT_CONFIGURED	The auto update schedule cannot be deleted. You did not configure an update schedule.	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.	Delete the existing update schedule.