Viewing Reports

Reports provide you with useful information about AUS; for example, you can view reports that show how busy AUS is, show whether any errors have occurred, or display information about devices that have contacted AUS.

These topics help you understand AUS reports:

Viewing the System Information Report

Select **Auto Update Server > Reports > System Info** to display the system information report (Table 5-1).

The report shows general information about AUS, how busy the server is, and statistics related to activity in the past 24 hours.

Table 5-1 System Info Report

Row	Description
General System Information	
Auto Update Server URL	The URL that devices use to connect to AUS. When you add the AUS to Security Manager, use this information to identify the URN.
No. of Devices Managed	The number of devices in the AUS database.
No. of Devices That Never Contacted AUS	The number of devices in the AUS database that have never contacted AUS.
Percentage of Devices Up-to-date	The percentage of devices that successfully contacted AUS and downloaded new images or configuration files.
Percentage of Devices Not Up-to-date	The percentage of devices that have not yet contacted or that failed to contact AUS and download new images or configuration files.
No. of Files	The number of files in the AUS database.

Table 5-1 System Info Report (continued)

Row	Description
No. of Assignments	The number of image to device assignments and device to image assignments.
Statistics For Last 24 Hours	
The values for the following statistics are all based on the previous 24-hour period.	
No. of Successful Auto Updates	The number of times that devices contacted AUS and successfully retrieved an auto update.
No. of Failed Auto Updates	The number of times that devices contacted AUS but failed to retrieve an auto update.
Percentage of Devices that Contacted AUS	The percentage of devices that successfully contacted AUS and downloaded new image or configuration files.
Device That Contacted AUS Most	The device that contacted AUS the most number of times.
Most Downloaded File	The file that devices downloaded most often from AUS.
No. of Unique Files Downloaded	The number of unique files that devices downloaded from AUS.
No. of Successful File Downloads	The number of file downloads that were completed successfully.
No. of Failed File Downloads	The number of times an error occurred while a device was performing an auto update.
No. of Bytes Downloaded	The number of bytes that were downloaded.
No. of New Assignments	The number of new image-to-device and device-to-image assignments.

Related Topics

- Viewing the Event Report, page 5-4
- Viewing the Event Failure Summary Report, page 5-4
- Viewing the Event Success Summary Report, page 5-5
- Viewing the No Contact Since Report, page 5-6

Understanding AUS Event Types

When you view any of the event reports, each entry in the report includes an event type. This type describes in general what happened during the event. The description column provides more specific detail.

You can filter the report table by these events. The Event Failures and Event Successes reports provide information only on the failure or success types, whereas you can view all types in the Events report.

See the following topics for information on viewing event reports:

- Viewing the Event Report, page 5-4
- Viewing the Event Failure Summary Report, page 5-4
- Viewing the Event Success Summary Report, page 5-5

The following table describes all event types.

Table 5-2 Event Type Descriptions

Event Type	Description
CONNECT_SUCCESS	The device contacted AUS successfully and reported its inventory details.
CONNECT_FAILURE	A problem occurred during an auto update attempt. Possible causes are: • An error while parsing XML. • Invalid credentials. • The device has not been added to AUS. • Connectivity problems. • The database was down while trying to add a record.
DEVICE_CONFIG_ERROR	Errors reported to the server from the device or errors that occurred while the device was loading the configuration file assigned to it. You should use these errors for debugging configuration problems. When an error occurs while the configuration file is being downloaded to the device, the running configuration reverts to the startup configuration.
GENERAL_DEVICE_ERROR	A non-configuration file error reported to AUS from the device. Possible causes are: • Problems connecting to the Auto Update servlet. • Problems with the downloaded image (invalid checksum). To configure the security appliance to use a specific software image or ASDM image if you have more than one installed, or have installed them in external Flash memory, see Configuring the Software Image and ASDM Image to Boot, page C-2.
DOWNLOAD_SUCCESS	The file was successfully sent to the remote device without error. This does not mean that the device is running the image successfully; this message could be followed by either DEVICE_CONFIG_ERROR or GENERAL_DEVICE_ERROR.
DOWNLOAD_FAILURE	An error occurred while an image or configuration file was being downloaded. Possible causes are: • Invalid credentials. • Communication problems. • Database problem.
AUS_IMMEDIATE_SUCCESS	AUS successfully contacted and updated the device when you selected **Update Now** to perform an immediate auto update.
AUS_IMMEDIATE_FAILURE	An error occurred while the device was being updated during an immediate auto update. Possible causes are: • The server does not have direct connectivity to the device (for example, it is behind a NAT boundary). For information on configuring AUS to work with NAT, see Deploying AUS Behind a NAT Boundary, page 1-2. • The enable or TACACS+ username and password that the device uses to authenticate AUS are incorrect. For more information about these credentials, see Adding a Device Directly to AUS, page 2-3. • An internal error occurred.
SYSTEM_ERROR	An internal error occurred.

Viewing the Event Report

Select **Auto Update Server > Reports > Events** to display the event report. This report shows all events, whether successful or unsuccessful.

The report shows information about devices that have contacted AUS. It includes information such as the event type, the result of the event, the date and time of the event, and a detailed description to help you fix any problems that occurred. For a description of possible event types, see Understanding AUS Event Types, page 5-2.

The report also shows information about notifications sent from devices to AUS. For example, if an ASA device downloads a configuration file and discovers errors, it sends an alert to AUS, which the report displays. Entries are added each time a device contacts AUS or a file is downloaded.

Beginning from version 4.8, Security Manager displays the updated version information of a device that has been upgraded using AUS. The event report in AUS shows if the version update for a device in Security Manager has succeeded or failed.

You can manipulate the report in the following ways:

- The report shows events only for a single day. Select the day in the **Date** field (from the past 7 days only) to view events from that day.
- Click a column name to sort the table by column information. When you sort by the Device ID column, the table is sorted first by device ID, then by timestamp.
- You can filter the table and search the table for a specific device ID using the fields above the table.

Related Topics

- Viewing the System Information Report, page 5-1
- Viewing the Event Failure Summary Report, page 5-4
- Viewing the Event Success Summary Report, page 5-5
- Viewing the No Contact Since Report, page 5-6

Viewing the Event Failure Summary Report

Select **Auto Update Server > Reports > Event Failures** to display the event failure summary report.

The report lists the devices that encountered an event failure. The information for the device includes the number of times the device encountered each type of failure (no entry in a column indicates no failures of that type). To analyze the report:

- Select the day in the **Date** field (from the past 7 days only) to view events from that day.
- Click the device ID to open a detailed report that shows all of the events for that device on that day.
- Click the number in one of the failure columns to display the detailed report pre-filtered to show failures of that type. Following are the failure types; for a description, see Understanding AUS Event Types, page 5-2.
  - **Auto Update**—The number of CONNECT_FAILURE events (failures of the device to connect to AUS).
  - **Download**—The number of DOWNLOAD_FAILURE events (failures downloading a file to the device).

  - **Request Update**—The number of AUS_IMMEDIATE_FAILURE events (failures performing an immediate auto update).
  - **Configuration**—The number of DEVICE_CONFIG_ERROR events (errors in the downloaded configuration).
  - **General**—The number of GENERAL_DEVICE_ERROR events.
  - **System**—The number of SYSTEM_ERROR events (AUS system errors).
- Click a column name to sort the table by column information. When you sort by the Device ID column, the table is sorted first by device ID, then by timestamp.
- You can filter the table and search the table for a specific device ID using the fields above the table.

Related Topics

- Viewing the Event Report, page 5-4
- Viewing the Event Success Summary Report, page 5-5
- Viewing the No Contact Since Report, page 5-6

Viewing the Event Success Summary Report

Select **Auto Update Server > Reports > Event Success** to display the event success summary report.

The report lists the devices that successfully completed an action. The information for the device includes the number of times the device succeeded at each type of event (no entry in a column indicates no successes of that type). To analyze the report:

- Select the day in the **Date** field (from the past 7 days only) to view events from that day.
- Click the device ID to open a detailed report that shows all of the events for that device on that day.
- Click the number in one of the success columns to display the detailed report pre-filtered to show successes of that type. Following are the success types; for a description, see Understanding AUS Event Types, page 5-2.
  - **Auto Update**—The number of CONNECT_SUCCESS events (where the device succeeded in connecting to AUS).
  - **Download**—The number of DOWNLOAD_SUCCESS events (successful file downloads to the device).
  - **Request Update**—The number of AUS_IMMEDIATE_SUCCESS events (performing an immediate auto update successfully).
- Click a column name to sort the table by column information. When you sort by the Device ID column, the table is sorted first by device ID, then by timestamp.
- You can filter the table and search the table for a specific device ID using the fields above the table.

Related Topics

- Viewing the Event Report, page 5-4
- Viewing the Event Failure Summary Report, page 5-4
- Viewing the No Contact Since Report, page 5-6

Viewing the No Contact Since Report

Select **Auto Update Server > Reports > No Contact Since** to display the no contact since report.

The report lists the devices that have not contacted AUS since the date specified and shows the date and time of the last successful contact. To analyze the report:

- If desired, specify a different date from which you want to view contact information in the **Select Date** field and click **Go**.
- Click the device ID to open a detailed report that shows all of the events for that device. You can view events over the previous 7 days. For more information about the types of events you can view in the detail report, see Understanding AUS Event Types, page 5-2.
- Click a column name to sort the table by column information.
- You can search the table for a specific device ID using the fields above the table.

Related Topics

- Viewing the System Information Report, page 5-1
- Viewing the Event Report, page 5-4
- Viewing the Event Failure Summary Report, page 5-4
- Viewing the Event Success Summary Report, page 5-5