



# CHAPTER 6

## 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 Info Report, page 6-1](#)
- [Viewing the Event Report, page 6-3](#)
- [Viewing the Event Failure Summary Report, page 6-8](#)
- [Viewing the Event Success Summary Report, page 6-10](#)
- [Viewing the No Contact Since Report, page 6-11](#)
- [Viewing the Detail Device Event Report, page 6-12](#)
- [Viewing the CNS Devices Report, page 6-14](#)

## Viewing the System Info Report

From the Reports tab, select the System Info Report option to display the System Info Report table ([Table 6-1](#)).

The table shows general information about AUS and also how busy the server is. The report contains information, such as how many devices have contacted AUS and how many configuration files have been downloaded within the last 24 hours.

Click a column name to sort the table by column information. You can also filter and search the table.

**Table 6-1 System Info Report**

<b>Row</b>	<b>Description</b>
<b>System Info</b>	
Auto Update Server URL	Shows the URL that devices use to connect to AUS.
No. of Devices Managed	Shows the number of devices in the AUS database.
No. of Devices That Never Contacted AUS	Shows the number of devices in the AUS database that have never contacted AUS.
Percentage of Devices Up-to-date	Shows the percentage of devices that successfully contacted AUS and downloaded new images or configuration files.
Percentage of Devices Not Up-to-date	Shows 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	Shows the number of files in the AUS database.
No. of Assignments	Shows the number of image to device assignments and device to image assignments.
<b>Statistics For Last 24 Hours</b>	
No. of Successful Auto Updates	Shows the number of times that devices successfully contacted AUS during the last 24 hours.
No. of Failed Auto Updates	Shows the number of times that devices did not contact AUS during the last 24 hours.

**Table 6-1** System Info Report (continued)

Row	Description
Percentage of Devices that Contacted AUS	Shows the percentage of devices that successfully contacted AUS and downloaded new image or configuration files during the last 24 hours.
Device That Contacted AUS Most	Shows the device that contacted AUS most often during the last 24 hours.
Most Downloaded File	Shows the file that AUS downloaded most often during the last 24 hours.
No. of Unique Files Downloaded	Shows the number of unique files that AUS downloaded during the last 24 hours.
No. of Successful File Downloads	Shows the number of file downloads that were completed successfully during last 24 hours.
No. of Failed File Downloads	Shows the number of times an error occurred while a device was performing an auto update during the last 24 hours.
No. of Bytes Downloaded	Shows the number of bytes that were downloaded during the last 24 hours.
No. of New Assignments	Shows the number of new image-to-device and device-to-image assignments during the last 24 hours.

## Viewing the Event Report

From the Reports tab, select the Event Report option to display the Event Report table ([Table 6-2](#)).

The table shows information about devices that have contacted AUS. It describes information such as the event type and result of the event. It also shows information about notifications sent from PIX security appliance and ASA devices to AUS. For example, if a PIX security appliance or an ASA device

downloads a configuration file and discovers errors, it sends an alert to AUS, which the table displays. Entries are added each time a device contacts AUS or a file is downloaded.

Click a column name to sort the table by column information. When you click the Device ID column, the table is sorted first by device ID, then by timestamp. You can also filter the table and search the table for a specified device ID.

**Table 6-2**      **Event Type Report**

Element	Description
Severity at or higher than (list)	Shows the priority level of the event. Select the severity type from the list to filter the table according to severity. The table lists events at the specified severity plus all events that occurred at a higher severity.  See <a href="#">Table 6-3</a> for severity levels and their descriptions.
Event Type list	Shows the type of event that occurred. Select the type from the list to filter the table according to event type.  See <a href="#">Table 6-4</a> for errors and their descriptions.
Device Filter field	Enables you to enter the ID of the device for which you want to search. The table is sorted first by device ID, then by timestamp.
Go button	Begins a search for information in the Device Filter field.
Date list	Shows the day on which the event occurred. You can see events that occurred during the past 7 days.  Select the date to filter the table according to the date on which the event occurred.
Device ID column	Shows the name the device uses when identifying itself to AUS, which might be different from hostname.
Event Type column	Shows the type of event that occurred. See <a href="#">Table 6-4</a> for events and their descriptions.

**Table 6-2** *Event Type Report (continued)*

<b>Element</b>	<b>Description</b>
Severity column	Shows the severity level of the event. See <a href="#">Table 6-3</a> for severity levels and their descriptions.
Timestamp column	Shows the time during which the event occurred.
Description column	Provides a brief description of the event.
Rows per page list	Specifies the number of rows per page to display.

**Table 6-3** *Severity Level Descriptions*

<b>Logging Level</b>	<b>Type</b>	<b>Description</b>
<b>0</b>	Emergency	System is unusable. Generates messages that identify system instabilities.
<b>1</b>	Alerts	Immediate action is needed. Generates messages that identify system integrity issues that require immediate administrative action.
<b>2</b>	Critical	Critical condition. Generates messages that identify critical system issues.
<b>3</b>	Errors	Error condition. Generates messages that identify system errors during operation.
<b>4</b>	Warnings	Warning condition. Generates messages that identify system warnings, for example, a device might be configured incorrectly.
<b>5</b>	Notifications	Normal but significant condition. Generates messages that identify normal operations that are typically considered significant events.

**Table 6-3** *Severity Level Descriptions (continued)*

<b>Logging Level</b>	<b>Type</b>	<b>Description</b>
<b>6</b>	Information	Informational only. Generates messages that identify system information that is typical of day-to-day activity, such as network session records.
<b>7</b>	Debugging	Generates syslog messages that assist you in debugging. Also generates logs that identify the commands issued during FTP sessions and the URLs requested during HTTP sessions. Includes all emergency, alert, critical, error, warning, notification, and information messages.
–	Disabled	No logging.

**Table 6-4** *Event Type Descriptions*

<b>Event Type</b>	<b>Description</b>
All	Displays all errors.
CONNECT_SUCCESS	Device contacted AUS successfully and reported its inventory details.
CONNECT_FAILURE	A problem occurred during an auto update attempt. Possible causes are: <ul style="list-style-type: none"> <li>• Error while parsing XML.</li> <li>• Invalid credentials.</li> <li>• Device has not been added to AUS.</li> <li>• Connectivity problems.</li> <li>• Database down while trying to add record.</li> </ul>

**Table 6-4** *Event Type Descriptions (continued)*

Event Type	Description
DEVICE_CONFIG_ERROR	<p>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 startup configuration.</p>
GENERAL_DEVICE_ERROR	<p>Non-configuration file error reported to AUS from the device. Possible causes are:</p> <ul style="list-style-type: none"> <li>• Problems connecting to the Auto Update servlet.</li> <li>• 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 <a href="#">Configuring the Software Image and ASDM Image to Boot</a>, page D-4.</li> </ul>
DOWNLOAD_SUCCESS	<p>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.</p>

**Table 6-4** *Event Type Descriptions (continued)*

Event Type	Description
DOWNLOAD_FAILURE	An error occurred while an image or configuration file was being downloaded. Possible causes are: <ul style="list-style-type: none"> <li>• Invalid credentials.</li> <li>• Communication problems.</li> <li>• Database problem.</li> </ul>
AUS_IMMEDIATE_SUCCESS	AUS successfully contacted and updated the device.
AUS_IMMEDIATE_FAILURE	An error occurred while the device was being updated. Possible causes are: <ul style="list-style-type: none"> <li>• The server does not have direct connectivity to the device (for example, it is behind a NAT boundary).</li> <li>• The enable or TACACS username and password that the device uses to authenticate AUS are incorrect.</li> <li>• An internal error occurred.</li> </ul>
SYSTEM_ERROR	An internal error occurred.

## Viewing the Event Failure Summary Report

From the Reports tab, select the Event Failure Summary Report option to display the Event Failure Summary Report table ([Table 6-5](#)).

See [Table 6-4](#) for descriptions of event types available from the Event Type list.

The table lists all or specified devices that failed a selected event. Click a column name to sort the table by column information. When you click the Device ID column, the table is sorted first by device ID, then by timestamp. You can also filter the table and search the table for a specific device ID.

**Table 6-5** *Event Failure Summary Report*

<b>Element</b>	<b>Description</b>
Event Type list	Shows the type of event that occurred. Select the type from the list to filter the table according to event type. See <a href="#">Table 6-4</a> for errors and their descriptions.
Device Filter field	Enables you to enter the ID of the device for which you want to search for within the table. The table is sorted first by device ID, then by timestamp.
Go button	Begins a search for information in the Device Filter field.
Date list	Shows the day on which the event occurred. You can see events that occurred during the past 7 days. Select the date to filter the table according to the date on which the event occurred.
Device ID column	Shows the name the device uses when identifying itself to AUS, which might differ from the hostname.  Click the device ID to display a Detail Device Event Report for the selected device. The time period corresponds to the date specified in the Date field. For more information, see <a href="#">Viewing the Detail Device Event Report, page 6-12</a> .
Auto Update column	Shows the number of CONNECT_FAILURE events. <sup>1</sup>
Download column	Shows the number of DOWNLOAD_FAILURE events. <sup>1</sup>
Request Update column	Shows the number of AUS_IMMEDIATE_FAILURE events. <sup>1</sup>
Configuration column	Shows the number of DEVICE_CONFIGURATION_ERROR events. <sup>1</sup>
General column	Shows the number of GENERAL_DEVICE_ERROR events. <sup>1</sup>

**Table 6-5** *Event Failure Summary Report (continued)*

Element	Description
System column	Shows the number of SYSTEM_ERROR events. <sup>1</sup>
Rows per page list	Specifies the number of rows per page to display.

1. Click the number to display an event report listing only this event type for the specified device. See [Table 6-4](#) for errors and their descriptions.

## Viewing the Event Success Summary Report

From the Reports tab, select the Event Success Summary Report option to display the Event Success Summary Report table ([Table 6-6](#)).

See [Table 6-4](#) for descriptions of event types available from the Event Type list.

The table lists all or specified devices that had the selected successful events. Click a column name to sort the table by column information. When you click the Device ID column, the table is sorted first by device ID, then by timestamp. You can also filter the table and search the table for a specified device ID.

**Table 6-6** *Event Success Summary Report*

Element	Description
Event Type list	Shows the type of event that occurred. Select the type from the list to filter the table according to event type. For errors and their descriptions, see <a href="#">Table 6-4</a> .
Device Filter field	Enables you to enter the ID of the device for which you want to search. The table is sorted first by device ID, then by timestamp.
Go button	Begins a search for information in the Device Filter field.
Date list	Shows the day on which the event occurred. You can see events that occurred during the past 7 days. Select the date to filter the table according to the date on which the event occurred.

**Table 6-6** *Event Success Summary Report (continued)*

Element	Description
Device ID column	Shows the name the device uses when identifying itself to AUS, which might differ from the hostname.  Click the device ID to display a Detail Device Event Report for the selected device. The time period corresponds to the date specified in the Date field. For more information, see <a href="#">Viewing the Detail Device Event Report, page 6-12</a> .
Auto Update column	Shows the number of CONNECT_SUCCESS events. <sup>1</sup>
Download column	Shows the number of DOWNLOAD_SUCCESS events. <sup>1</sup>
Request Update column	Shows the number of AUS_IMMEDIATE_SUCCESS events. <sup>1</sup>
Rows per page list	Specifies the number of rows per page to display.

1. Click the number to display an event report listing only this event type for the specified device. See [Table 6-4](#) for errors and their descriptions.

## Viewing the No Contact Since Report

From the Reports tab, select the No Contact Since Report option to display the No Contact Since Report table ([Table 6-7](#)).

The table lists all devices that have not contacted AUS since the date specified. Click a column name to sort the table by column information. When you click the Device ID column, the table is sorted first by device ID, then by last contact. You can also filter the table for a specified device ID.

**Table 6-7**      **No Contact Since Report**

Element	Description
Select date list and year field	Enables you to select the date and month from the list and enter the year to filter the table by date.
Device Filter field	Enables you to enter the ID of the device for which you want to search. The table is sorted first by device ID, then by timestamp.
Go button	Begins a search for information in the Date or Device Filter field.
Device ID column	Shows the name the device uses when identifying itself to AUS, which might differ from the hostname.  Click the device ID to display a Detail Device Event Report for the selected device. The time period corresponds to the date specified in the Date field if the date is within last 7 days. Otherwise, it shows the current day. For more information, see <a href="#">Viewing the Detail Device Event Report, page 6-12</a> .
Last Contact column	Shows the date that the device last contacted AUS.
Rows per page list	Specifies the number of rows per page to display.

## Viewing the Detail Device Event Report

You can access the Detail Device Event Report from the following three reports:

- [Event Failure Summary Report](#)
- [Event Success Summary Report](#)
- [No Contact Since Report](#)

From the Reports tab, select one of these reports. Then click the ID corresponding to the device for which you want to see detailed events ([Table 6-8](#)).

The table lists all types of events that have occurred on a specified date. Click a column name to sort the table by column information. If you click the Event Type column, the table is sorted first by the type of event, then by timestamp. You can also filter the table and search it for a specified severity or event type.

**Table 6-8** *Detail Device Event Report*

Element	Description
Severity list	Shows the severity level of the event. Select the severity level from the list to filter the table according to the severity level.  See <a href="#">Table 6-3</a> for severity levels and their descriptions.
Event Type list	Shows the type of event that occurred. Select the type from the list to filter the table according to event type.  See <a href="#">Table 6-4</a> for errors and their descriptions.
Date list and Timestamp column	Shows the day on which the event occurred. You can see events that occurred during the past 7 days.  Select the date to filter the table according to the date on which the event occurred.
Event Type list	Shows the type of event that occurred.  See <a href="#">Table 6-4</a> for errors and their descriptions.
Severity column	Shows the severity level of the event.  See <a href="#">Table 6-3</a> for severity levels and their descriptions.
Timestamp column	Shows the day on which the event occurred. You can see events that occurred during the past 7 days.
Description	Provides additional error message information about the event.  See <a href="#">Table B-1</a> for descriptions of error messages.
Rows per page list	Specifies the number of rows per page to display.

# Viewing the CNS Devices Report

From the Reports tab, select the CNS Devices Report option to display the CNS Devices Report table (Table 6-9). Use this report to verify that CNS devices are contacting AUS.



## Note

The Cisco CNS Configuration Engine is a network management application that acts as a configuration service for automating the deployment and management of network devices and services. Each Cisco CNS Configuration Engine manages a group of Cisco IOS devices (routers) and the services they deliver, storing their configurations and Cisco IOS images, then delivering them as needed. The Cisco CNS Configuration Engine automates initial configurations, configuration and image updates, dynamically generating the device-specific configuration or image on demand, and logs the results.

The table lists all CNS devices and their last contact and disconnect times. Click a column name to sort the table by column information. If you click the Device ID column, the table is sorted first by device ID, then by last contact. You can also filter the table for a specified device ID.

**Table 6-9**      **CNS Devices Report**

Element	Description
Device Filter field	Enables you to enter the ID of the device for which you want to search. The table is sorted first by device ID, then by timestamp.
Go button	Begins a search for information in the Date or Device Filter field.
Device ID column	Shows the name the device uses when identifying itself to AUS, which might differ from the hostname.

**Table 6-9** *CNS Devices Report (continued)*

Element	Description
Last Connect column	Shows the date and time that the device last connected to AUS. The <code>CONNECT_SUCCESS</code> event type in the Event report shows that the device has successfully contacted AUS. Check whether the time at which the device last contacted AUS ( <code>CONNECT_SUCCESS</code> event) is greater than the time at which the device failed to connect to AUS ( <code>CONNECT_FAILURE</code> event). If not, make sure that the communication between the device and the CNS Event gateway running on AUS is correct by entering the <b>show cns event connections</b> command on the device. For more information, see <a href="#">Bootstrapping CNS Devices, page D-5</a> .
Last Disconnect column	Shows the date and time that the device last disconnected from AUS.

