Notifications

This chapter contains the following sections:

About Notifications

Cisco Business Dashboard generates notifications when different events occur in the network including Connectwise or Webex teams integration notifications. A notification may generate an email or a pop-up alert that appears in the lower right corner of the browser, and all notifications are logged for later review.

Notifications can also be acknowledged when they are no longer of interest. Those notifications will be hidden from the **Notification Center** by default.

Supported Notifications

The following table lists the notifications supported by Cisco Business Dashboard

Table 1: Supported Notifications

Event	Level	Description	Clears Automatically?
Device Notifications for Access Points, Routers, IP Phones and Switches			
Reachability/Device Discovered	Information	A new device is detected on the network.	Yes, 5 minutes after the device is discovered.
Reachability/Device Unreachable	Warning	A device is known through a discovery protocol, but is not reachable using IP.	Yes, when the device is reachable through IP again.
Reachability/Device Offline	Alert	A device is no longer detectable on the network	Yes, when the device is rediscovered.
Credential Required/SNMP	Warning	The Probe is unable to access the device due to an authentication error.	Yes, when the Probe authenticates.
Credential Required/User ID	Warning	The Probe is unable to access the device due to an authentication error.	Yes, when the Probe authenticates.
Credential Required/Password Expired	Warning	The password has expired for the admin user on the device.	Yes, when the password on the device has been reset.
Configuration Mismatch	Alert	The current device configuration does not match the configuration specified in Cisco Business Dashboard configuration profiles and device settings.	Yes, when the configuration mismatch is resolved.
Device Service/SNMP	Warning	SNMP is disabled on the device.	Yes, when SNMP is enabled.
Device Service/Web service	Warning	The web service is disabled on the device.	Yes, when web service API is enabled
Health	Warning/Alert	The device health level changes to warning or alert.	Yes, when the device health returns to normal.
Cisco Support Notifications			
Firmware	Information	A later version of firmware is available on cisco.com	Yes, when the device is updated to the latest version.
End of Life	Warning/Alert	An End of Life bulletin is found for the device or an End of Life milestone has been reached.	No
Maintenance Expiry	Warning/Alert	The device is out of warranty and/or does not have a currently active maintenance contract.	Yes, if a new maintenance contract is taken out.

Event	Level	Description	Clears Automatically?
Device Health Notifications			
CPU	Warning/Alert	Device CPU usage exceeds maximum thresholds.	Yes, when the CPU usage returns to a normal level.
Uptime	Warning/Alert	Device uptime is below minimum thresholds.	Yes, when the device uptime exceeds minimum levels.
Connected Clients	Warning/Alert	The number of connected clients exceeds maximum thresholds.	Yes, when the number of connected clients returns to an acceptable level.

Viewing and Filtering Current Device Notifications

To view currently active notifications for a single device or all devices, follow the steps below.

1. In the **Home** window, click **Notification Center** icon on the top right corner of the global tool bar. The number badge on the icon specifies the total number of unacknowledged notifications outstanding, and the color of the badge indicates the highest severity level currently outstanding.

   Any notifications currently outstanding are listed below the icons in the **Notification Center**. The number on the severity icon provides a total of the number of notifications in each of the following categories:

Icon	Description
	Information (green circle icon)
	Warning (orange triangle icon)
	Alert (red inverted triangle icon)

2. In the **Notification Center**, you can perform the following actions:

   • Acknowledge a notification—Check the check box against the notification to acknowledge it. You can acknowledge all notifications in the display by checking the **ACK All** checkbox.

   • Filter the displayed notifications—See step 3 for instructions.

3. The Filter box limits the notifications displayed in the table. By default, notifications of all types and all severity levels will be displayed. To change an existing filter, double click on that filter to change the setting. To add a new filter, click on the Add Filter label and select a filter from the drop-down list. The table below lists all the filters that are available.

Filter	Description
Notification Type	The type of notification to be displayed. For example, to display notifications for devices that are offline, choose **Device Offline** from the drop-down list.
Severity	The severity level of the notifications to be displayed including: • Info • Warning • Alert You can include higher severity levels by selecting the **Higher** checkbox.
Include Ack	Include notifications that have been acknowledged.
Network	Displays notifications for the specified network(s). Start typing in the filter and matching networks will be listed in a drop-down. Click to select the desired network. You can include multiple networks in the filter.
Device	Displays notifications for the specified device(s). Start typing in the filter and matching devices will be listed in a drop-down. Click to select the desired device. You can include multiple devices in the filter.
Show Discovery	Controls whether to include notifications for devices that have been blocked by discovery filtering.

Note Notifications for individual devices can be seen in the **Basic Info** and the **Detailed Info** panels for the device.

To control how you receive notifications, change the notification settings at the organization or system level. For more information, see Organizations or Managing Notification Defaults.

Viewing and Filtering Historical Device Notifications

The occurrence or change in state of any notification is recorded as an event on the Dashboard, and may be viewed through the Event Log. A subset of the event log can be viewed through the following panels:

The **Basic Info** panel or the **Device Detail** panel displays individual devices.

The **Basic Info** Panel shows only the last 24 hours worth of events.

The **Device Detail** panel shows all historical data for the device that is available.

Note The **Device Detail** panel can be filtered to help isolate those events you are interested in. See Event Log for more information on viewing and filtering historical events.