Assurance

This chapter contains the following sections:

Monitoring

Cisco Business Dashboard Lite allows for real-time monitoring of the network, networking events and collects historical data for reporting purposes. This helps network administrators maintain a robust understanding of the network's health and performance, and allows them to act quickly should issues arise.

Notification Center

Cisco Business Dashboard Lite generates notifications when different events occur in the network. A notification may generate 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 CBD Lite.

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.

Event	Level	Description	Clears Automatically?
Credential Required/User ID	Warning	The Dashboard is unable to access the device due to an authentication error.	Yes, when the Dashboard 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.
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.
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.

Viewing and Filtering Current Device Notifications

To view currently active notifications for a single device or all devices, do the following:

Procedure

Step 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:

- Information (green circle icon)

- Warning (orange triangle icon)
- Alert (red inverted triangle icon)

Step 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 may acknowledge all notifications in the display by checking the **ACK All** checkbox
- Filter the displayed notifications—Instructions for this action is provided in the following step

Step 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 dropdown list. The following filters are available:

Table 2: Available Filters

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. It can be one of the following: • Info • Warning • Alert You may include higher severity levels by selecting the **Higher** checkbox.
Include Ack	Include notifications that have been acknowledged.
Device	Displays notifications for the specified device(s). Start typing in the filter and matching devices will be listed in a dropdown. Click to select the desired device. You may include multiple devices in the filter.

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

To control how you receive notifications, change the notification settings.

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, on page 4 for more information on viewing and filtering historical events.

Event Log

Open the Event Log screen to search for events that happen across your network. This screen provides an interface where you can search and sort through the events generated across the network. Up to 500,000 of these events are stored for a maximum of 90 days. You can use the filter controls provided to limit the events displayed based on any combination of the following parameters:

Add a **Time** to specify the start and end times for the period of interest. Only events occurring in this period will be displayed.

Add a **Severity** filter to select the level of events to display. You can also check the *Higher* checkbox to include events with a higher severity level.

Add the **Type** filter to select one or more event types to display. The types are arranged in a tree structure, and selecting a type will automatically include all event types underneath the selected type in the tree.

Use the **Device** filter to display events by one or more devices. As you type, matching devices will be displayed. You can also specify devices by name, IP address, or MAC address.

Events that match the filter conditions will be displayed in a table. You can also sort the information in the table using the column headings.

Monitoring Profile

Monitoring Profiles control the data that is collected from devices and the notifications that are generated.

Active notifications are also visible in the **Notification Center** and are displayed in the device information views. Changes in notifications are also recorded in the **Event Log**.

Reporting monitors collect the data used for the wireless reports and traffic graphs in the monitoring dashboard.

Modify a Monitoring Profile

To modify a monitoring profile, follow the steps below.

1. Navigate to **Assurance > Monitoring > Monitoring Profiles**.
2. Make changes to the notification and reporting monitors as required. You can restore the monitor settings to the defaults by clicking the **Reset to defaults** button.