CBD Lite Administration Guide Version 2.12.1

First Published: 2026-03-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CHAPTER 1

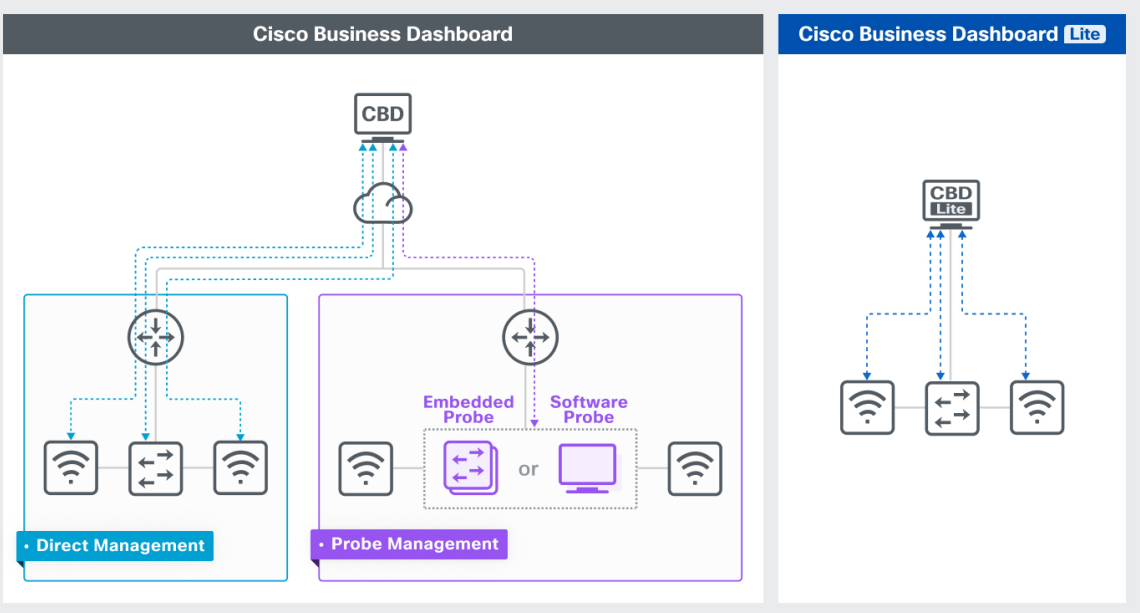
CBD Lite Overview

This chapter contains the following sections:

About Cisco Business Dashboard Lite

Cisco Business Dashboard Lite provides tools that help you monitor and manage the devices in your Cisco Business network. It automatically discovers your network and allows you to configure and monitor all supported devices such as switches and wireless access points. It also notifies you about the availability of firmware updates, and about any devices that are no longer under warranty or covered by a support contract.

Cisco Business Dashboard Lite is a simplified version of Cisco Business Dashboard. It retains the core features of the original product while reducing complexity and resource usage. This makes it suitable for users who need basic functionality without the additional overhead of the full product.



Feature Comparison Table

Feature	Cisco Business Dashboard Lite	Cisco Business Dashboard
Deployment options	Native Microsoft Windows installation	Virtualized environments (e.g., VMWare, VirtualBox, Hyper-V, AWS, Microsoft Azure) or to be installed directly on Ubuntu Linux.
Deployment location requirements	Same network as managed devices	Any convenient location, even when it's hosted in the cloud and the managed devices are behind Network Address Translation (NAT)
Device onboarding requirements	No configuration changes necessary for management	Requires changes to device configurations, enabling the Cisco Business Dashboard (CBD) agent, and establishing an active connection to CBD for management.
OS requirements	Microsoft Windows	Ubuntu Linux
Minimum system requirements	Any CPU/RAM specifications required by Windows, 5 GB Disk	2 vCPU, 4 GB RAM, 60 GB Disk
Supported devices	Refer to the Cisco Business Dashboard Lite – Device Support List for details	Refer to the Cisco Business Dashboard – Device Support List for details.
Maximum supported devices	100	15,000
Network discovery and inventory report	Yes	Yes
Device configuration and operation	Yes	Yes
Customizable monitoring dashboard	Yes	Yes
Device lifecycle report	Yes	Yes
Automatic firmware update notifications & One-click apply	Yes	Yes
Be alerted automatically to important events such as network devices going offline	Popup	Popup, email, open helpdesk ticket, send to collaboration space
Manage networks across multiple sites	No	Yes
Remote access to sites and devices without VPNs	No	Yes
Cisco Network Plug and Play (PnP)	No	Yes

Feature	Cisco Business Dashboard Lite	Cisco Business Dashboard
Role based access	Yes	Yes
Muti-tenant support/organizations	No	Yes
Device groups	No	Yes
API support for third-party integration	No	Yes
Integrates with popular Professional Service Automation (PSA) tools	No	Yes

New Release Information and Updates

This section provides information on key new features and changes in Cisco Business Dashboard Lite.

Table 1: New Features and Changed Behavior in Cisco Business Dashboard Lite, Release 2.12.1

Feature	Description
Localization Enhancements	Previously untranslated pages have been corrected.
Switch Trunk Port VLAN Configuration Enhancements	Adds support for allowing all VLANs, 1-4094, on switch trunk ports. Also adds configurable VLAN update behavior for network configuration profiles, allowing users to choose whether profile VLANs are applied to all switch trunk ports, only trunk ports connected to network devices, or no switch trunk ports. Trunk ports already configured to allow all VLANs are not affected by these update modes.
LLDP Enablement Prompt for Cisco IOS Device Discovery	Adds a discovery notice chip in the topology view when LLDP is needed to discover Cisco IOS devices.
User Profile Completion Reminder	Adds a non-blocking reminder when the current user profile is incomplete. The Dashboard shows a visual hint on the user avatar, prompting the user to update the required profile information. The reminder disappears after the profile is completed.

Table 2: New Features and Changed Behavior in Cisco Business Dashboard, Release 2.12.0

Feature	Description
Cross Launch SSH Console for Switch CLI Access	Users can now open the switch's SSH console directly in their browser to access the selected device's command line interface.
CLI Command Runner	Execute diagnostic CLI commands simultaneously across multiple devices. Results can be exported to text files for offline analysis and review..

Feature	Description
Global Device Configuration Backups View	A centralized view to monitor backup status, verify the last backup timestamps, and identify unprotected devices. Features include bulk configuration downloads and customizable auto-cleanup policies.
Device Integrity Tool	This tool evaluates the integrity of Cisco devices by verifying critical software and hardware components that incorporate Cisco Trustworthy Technologies. These built-in security capabilities help detect counterfeit components, identify unauthorized software modifications, and ensure that Cisco products are operating as intended.
Wireless LANs Network Configuration Profile	The Wireless LANs network configuration profile allows you to manage the wireless networks in your environment.
Topology Enhancements	Adds a topology shortcut icon in the device basic info panel and detail page to open the topology view with the hostname pre-filled in the topology search and introduces a Remove Stale Data button to clear stale topology data such as offline devices and links from the topology view.

Table 3: New Features and Changed Behavior in Cisco Business Dashboard, Release 2.11.1

Feature	Description
Localization Enhancements	Previously untranslated pages have been corrected.
Inventory Export to CSV	Export all devices matching the current filters to a CSV file.
Performance Enhancements	Cisco Business Dashboard Lite can now support up to 100 network devices.

Table 4: New Features and Changed Behavior in Cisco Business Dashboard Lite, Release 2.11.0

Feature	Description
Topology View Enhancement	Adds support for selecting layout (Vertical Tree, Horizontal Tree, Star), link line style (Curve or Straight), and link line thickness (Consistent or Link Speed Based).
VLAN-Matched Device IP Selection for Display	Adds an IP Interfaces tab to the device detail page and a Management VLAN setting to Administration > Discovery page. For devices with multiple IP addresses, the IP address of the VLAN interface matching the configured management VLAN will be displayed in Inventory and Topology views.
Manual Start for Scheduled Jobs	Adds a "Start Immediately" button to the Schedule Profiles table, allowing users to manually initiate scheduled jobs.
AI Assistant	Introduced an AI Assistant to answer document-related questions for SMB products.

Feature	Description
Authentication Network Configuration Profile	Adds support for an authentication profile that contains settings for the local user database on devices and specifies authentication servers (RADIUS servers) for network access authentication.

Table 5: New Features and Changed Behavior in Cisco Business Dashboard Lite, Release 2.10.1

Feature	Description
Localization Enhancements	Previously untranslated pages have been corrected.
Network Configuration Reapplication	A device-level reapplication feature has also been introduced to reapply selected network configuration profiles to individual devices.

Table 6: New Features and Changed Behavior in Cisco Business Dashboard Lite, Release 2.10.0

Feature	Description
Switch Power Savings Widget	A new widget "Switch Power Savings" has been added to the dashboard, providing detailed power saving statistics for Green Ethernet and PoE. This update also includes a revised layout for the dashboard page.
Wireless Client Report	The dashboard now includes a Wireless Client Report, which provides detailed information about the wireless clients on the network.
Schedule Profile	A Schedule Profile allows users to define and manage jobs that are scheduled to occur at a future date. This feature supports both one-time tasks and recurring tasks, providing flexibility in scheduling operations.

Table 7: New Features and Changed Behavior in Cisco Business Dashboard Lite, Release 2.9.1

Feature	Description
Localization	The web user interface now supports the following languages: • English • Simplified Chinese • French • German • Japanese • Spanish • Portuguese

Feature	Description
Automatic Launch	Added an option to automatically launch CBD Lite upon Windows login.

Table 8: New Features and Changed Behavior in Cisco Business Dashboard Lite , Release 2.9.0

Feature	Description
Topology Map	Network topology now can be discovered and visually displayed.
Network Actions	Network actions allow you to perform tasks on all supported devices within the network. For example, you can back up all network device configurations with a single click.
Support for Cisco Business Access Points	Fully support has been added for the Cisco Business Access Points.
Historical View of Device CPU Usage	A new widget displaying historic device CPU usage data has been added in the detailed device information panel within the Dashboard tab.
UX/UI Improvement	Device icons across the platform have been refreshed for a more modern look. The Inventory view has been improved to include a download icon next to the device firmware version number, indicating when a new firmware update is available.
Add Time Window to Monitoring Profile	Applies exclusively to CPU usage monitoring. Alerts or warnings will be generated only if CPU usage data consistently exceeds the threshold within a specified time window.
Product Improvement	A new feature allows Cisco Business Dashboard to send information about hardware and software usage in the network in further developing the Cisco product portfolio. The "Product Improvement" option in privacy settings can be used to turn this feature on or off.

Audience

This guide is primarily intended for network administrators who are responsible for Cisco Business Dashboard Lite software installation and management.

Related Documents

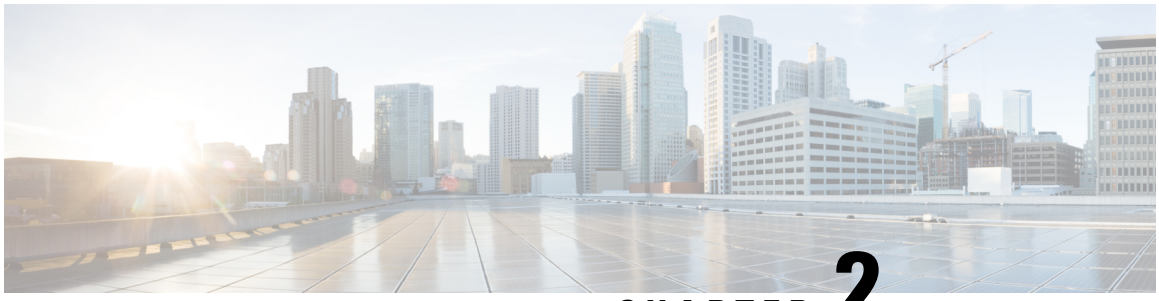
The documentation for Cisco Business Dashboard Lite is comprised of a number of separate guides. These include:

- **Quick Start Guide** —This guide provides details on performing the initial setup for Cisco Business Dashboard Lite using the most commonly selected options. Check out the Cisco Business Dashboard Lite Quick Start Guide.
- **Installation Guides**

  The following table lists all the installation guides for the Dashboard Lite software that can be deployed on different platforms. Refer the path provided in the location column for details:

Supported Platforms	Location
Microsoft Windows	Cisco Business Dashboard Lite Installation Guide for Microsoft Windows.

- **Administration Guide** —This is a reference guide that provides details about all the features and options provided by the software and how they may be configured and used. Check out the Cisco Business Dashboard Lite Administration Guide.
- **Device Support List**—This list provides details of the devices supported by Cisco Business Dashboard Lite. Check out the Cisco Business Dashboard Lite - Device Support List.



CHAPTER 2

Using CBD Lite

This chapter contains the following sections:

Using the Cisco Business Dashboard Lite GUI

This chapter provides an overview of the Cisco Business Dashboard Lite GUI including descriptions of the navigation pane links.

1. The **Header** pane

   The header toolbar contains the following options:

   - A menu button to display the navigation pane
   - Header text
   - A series of icons for functions such as language selection, notifications, task activity, feedback, context sensitive help, and version information.

2. The **Work** pane is this is the area where the feature interface is displayed.

   When you click an option in the **Navigation** pane, its corresponding window opens in this area.

3. The **Navigation** pane provides access to the Cisco Business Dashboard features. The navigation pane is displayed when the **Menu** icon is clicked, and slides away once a selection is made.

Navigation Pane Options

The **Navigation** pane provides options to access the major Cisco Business Dashboard features.

Icon	Description
	The **Favorites** allows you to bookmark your favorite sections in the Cisco Business Dashboard for easy access.

Icon	Description
	The **Dashboard** allows you to monitor the performance of your network over time. The dashboard allows you to monitor traffic levels, connected device counts, and other details about the network.
	The **Network** icon displays the network topology view that allows you to track the physical layout of the network.
	The **Inventory** tool provides a list of all devices in the network, allows you to view detailed information about the devices, and to perform actions such as update firmware, backup configurations, and reboot.
	The **Provision** option provides access to **Port Management** and **Network Configuration**, and allows you to manage the ports and make configuration changes.
	The **Assurance** page provides access to **Monitoring** which allows you to monitor and manage your network.
	The **Reports** option will display a number of reports that provide life-cycle information about your network devices, including end of life bulletins, warranty information and service contract details.
	The **Administration** pages allow you to maintain the Cisco Business Dashboard.
	The **System** pages are used to administer the Cisco Business Dashboard application.

Header Toolbar Options

The **Header** toolbar provides access to other system functions and displays system notifications.

Icon	Description
	The currently logged in user is displayed at the top of the navigation bar along with **My Profile**, **Language** , and **Logout** option. Click **My Profile** to display the user's profile page. If the current user's profile is incomplete, a profile completion reminder appears on the user icon. The reminder disappears after the profile is completed.
	The **Menu button** is located on the top left of the header—Click this button to display the navigation pane.
	The **Notification Center** icon displays the number and severity of outstanding notifications in Cisco Business Dashboard. Click this icon to display the Notification Center panel which provides you the option to filter the notification events that are displayed.

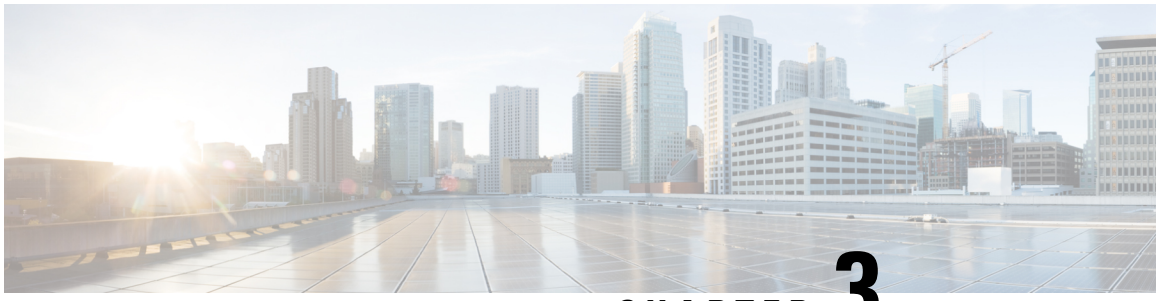
Icon	Description
	The **Job Center** icon shows the status of currently executing jobs and the history of past jobs. Jobs include any actions performed by Cisco Business Dashboard including both user-initiated jobs and system jobs. Click this icon to display jobs that are pending, in progress, and completed.
	Click the **Support Center** icon to access the help information, virtual assistant, feedback and **About Cisco Business Dashboard**. Click the **About Cisco Business Dashboard** icon to see information about this version, including the current version. If a new version is available, a green icon with an arrow will be displayed on the **Support Center** icon and the **About** icon, and a link to apply the update will be available in the pop-up of **About**.
	Click the AI Assistant to use the AI Assistant. The AI Assistant in CBD acts as your go-to resource for quick, accurate answers to your questions about Cisco Business products.

Upgrading Cisco Business Dashboard Lite

From time to time, Cisco releases new versions and updates for Cisco Business Dashboard Lite and posts them to the Software Center on cisco.com. Cisco Business Dashboard Lite periodically checks the Software Center for updates and if one is found, displays a badge on the  icon in the header panel of the UI. You can click to have the Dashboard download and apply the update.

To set up Dashboard to download and apply the update:

1. Click **About Cisco Business Dashboard Lite** to open the pop-up. If any updates are available for the Dashboard will be listed here.
2. If an update is available for the Dashboard, click the download icon. Alternatively you can download the Cisco Business Dashboard Lite installer file by navigating to https://cisco.com/go/cbd-sw and selecting the Download Software option from the product selection panel at the bottom right.
3. Copy the installer file to the Dashboard file system.
4. Execute the installer.



CHAPTER 3

Dashboard

This chapter contains the following sections:

About the Monitoring Dashboard

The **Dashboard** page in the Cisco Business Dashboard Lite lets you view the performance of the network in real time. It shows all the devices and provides the data in a graphical format.

This dashboard is a customizable arrangement of widgets that you can select. Following are the widgets included by default in the dashboard:

Widget	Description
Inventory Summary	Displays a breakdown of the devices discovered in the network.
Device Health	Displays the overall health of the devices in the network.
Traffic	Displays a graph of the traffic flowing through the selected interface.
Switch Port Utilization	Displays the percentage of switch ports in-use vs. total number of switch ports.
Switch PoE Utilization	Displays a graphic representation of the PoE utilization status.
Switch Power Savings	Displays detailed power saving statistics for Green Ethernet and PoE.
Wireless Clients by Device	Displays the number of devices associated with the selected wireless access point.

Controls on each of the widgets allows the data shown to be customized.

In the graphical widgets, click on the labels in the legend on the graph to toggle the display of each set of data. This allows you to further refine the data being shown and can help with troubleshooting a specific device on your network, or even the network itself.

Adding a Widget

This feature allows you to add one or more widgets to the existing default ones displayed in the dashboard to monitor tasks specific to a device or network you wish to view.

Procedure

Step 1 Click the Dashboard Edit icon to open the edit window. + icon beside each widget name.

Step 2 To add a widget, click the + icon beside each widget name.

Step 3 Drag the new widget to the desired location in the dashboard and resize if necessary.

Modifying a Widget

You can modify any widget on your dashboard with the following steps:

Procedure

Step 1 Click the **Config Widget** icon on the top right of the widget to modify parameters such as sample interval or thresholds.

Step 2 Use the drop-down lists within the new widget to select the specific data you wish to display.

Step 3 To change the title of the Widget click the Edit Mode icon.

Important
You must be in **Edit Mode** in the Dashboard to change the title of a widget.

Deleting a Widget

Procedure

Step 1 Click the Dashboard Edit icon and select **Edit Mode**.

Step 2 Click the **remove widget** icon at the top right of the widget to be removed. Rearrange the remaining widgets as desired.

Modifying the Dashboard Layout

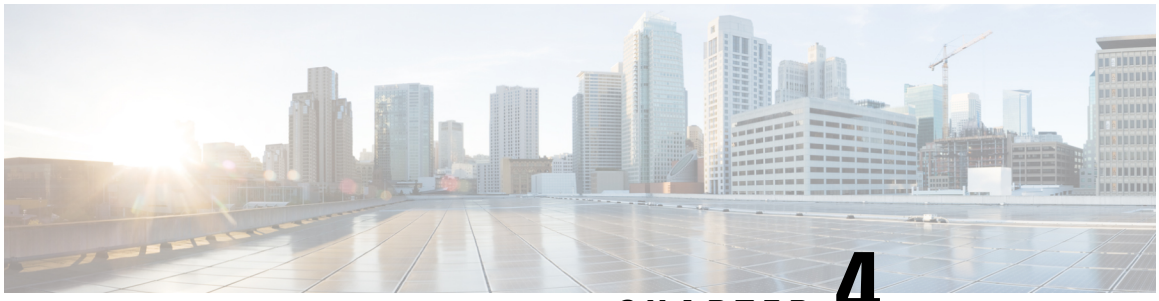
The **Dashboard** layout can be customized using the following steps:

Procedure

Step 1 Click the Dashboard Edit icon and select **Edit Mode**.

Step 2 Click in the header of a widget and drag to move the widget in the **Dashboard**. Other widgets will adjust dynamically to make room. Click and drag on the edge or corner of a widget to re-size. As you rearrange the layout, the dashboard will automatically re-size to fit in the available width.

Step 3 Click the Dashboard Edit icon again and select **View Mode** to preserve the changes.



CHAPTER 4

Network

This chapter contains the following sections:

Overview of the Topology Map and Tools

About the Topology Map

Cisco Business Dashboard Lite looks for discovered devices for network connectivity details and then builds a graphical representation or topology from the information it gathered. The data collected includes:

- CDP & LLDP neighbor information
- Multicast DNS and DNS Service Discovery (aka Bonjour)

Note When LLDP is needed to complete Cisco IOS device discovery, Dashboard may display a discovery notice in the topology view. Follow the prompt to enable LLDP.

This information determines how the network is constructed. When the network contains network infrastructure devices that are not manageable for any reason, Cisco Business Dashboard Lite will attempt to understand the topology based on the information that can be collected.

Click on devices or links in the topology to display the **Basic Info** panel for that device or link. This panel provides more detailed information about the device or link, and allows you to carry out different actions on a device.

Overlays and **Filters** are displayed on top of the Topology Map, allowing you to limit the devices displayed in the topology by device type or by tag. It also allows you to enhance the topology to show additional information such as the traffic load on links or how a particular VLAN is configured in the network.

Accessing the Topology Map

To access the **Topology Map** open the **Network** panel from the **Navigation** pane.

The **Topology** is displayed in the work pane.

Topology Controls

The Topology controls are located to the left of the **Topology Map**.

Icon	Description
	**Zoom in** - Adjusts the **Topology** window's view. Click the ✚ (plus) icon on the menu bar to increase the size of the network in the viewing area.
	**Zoom out** - Adjusts the **Topology** window's view. Click the ━ (minus) icon to reduce the size of the network in the viewing area.
	Click **Re-layout Topology** to redraw the topology using the automatic layout algorithm. If a device is selected in the topology when the button is clicked, then that device will be designated as the root of the topology tree when the layout is calculated. To select a device, click on the device icon and an orange circle will be shown around the device.
	Click **Fit stage** to zoom until the entire network fills the viewing area.
	Click **Enter full screen mode** to fill the screen with the Cisco Business Dashboard user interface.
	Click **Export Topology** to export the current topology view as an image in PNG format. The image will be saved to the default download location for the browser.
	Click **Topology Settings** to adjust labels displayed for topology icons and to select layout (Vertical Tree, Horizontal Tree, Star), link line style (Curve or Straight), and link line thickness (Consistent or Link Speed Based).
	Remove stale devices/links such as offline devices from the topology.

Topology Icons

The following icons appear in the **Topology** window:

Icon	Description
	**Access Point**
	**Access Point - Primary**

Icon	Description
	**Access Point - Mesh Extender**
	**Cloud** - This represents a network or part of a network that is not managed by Cisco Business Dashboard.
	**Links** - Links are connection lines between devices. Click a link to display the target and the source device names and other basic details such as speed and so on.
	**Router**
	**Switch**
	**Switch Stack**

Overlays & Filters

It is at the top of the Topology screen, next to the **Search** box.

Item	Description
Select Overlay	This feature enhances the **Topology** map with additional information based on the view selection. It can be one of the following: • The **Link Utilization View** identifies current network performance by monitoring the amount of traffic. This traffic is displayed using the color coded links in the **Topology** map. The color coding changes based on the percentage utilization of the link. Green represents links that are only moderately loaded, while orange and red represent links that are approaching capacity limits. Controls are provided to allow you to adjust the thresholds for different colors. • The **VLAN View** displays where a VLAN is enabled in the network. This can be used to identify a partitioned VLAN or other misconfiguration. When you select **VLAN View** in the Overlay drop-down, a second drop-down box appears below this field where you can select the VLAN ID to be displayed. • The **POE View** highlights links in the topology map which indicates devices that are currently being powered from a POE-enabled switch.

Item	Description
Select Tag	Specify a **Device Tag** in the text box below the **Select Tag** to filter the topology to show devices matching the specified tag. Device tags are assigned in the **Detailed Info** panel.
Show only: • **Routers** • **Switches** • **Wireless** • **Unmanaged Networks** • **Hosts** • **Others**	Check the check box against the devices in the list that you want to view in the **Topology** map. This feature helps you filter the devices you want to view in the map and removes the ones that are unchecked in the device list.

Network Actions

Use the **Network Actions** drop-down list to select actions that can be performed on all devices in the network that support that action. For example, you can backup all network device configurations with a single click. Network actions may optionally be scheduled to take place at a later time. Available network actions which can be performed on all network devices are as follows:

- Backup Network Config
- Upgrade All Devices Firmware
- Save Network Running Config
- Delet Offline Devices

Viewing Basic Device Information

Click on a network device such as a switch or a router, or a link connecting two devices, to view basic information about the device including outstanding notifications, and actions that may be performed.

The **Basic Info** panel also provides access to more detailed information for a device, and allows you to directly access the administration interface of the device.

The table in the following section provides the type of device details that are displayed. To view the basic device information follow the steps below.

Procedure

Step 1 In the Topology map, click on a network device such as a switch or a router to view the details.

Step 2 In the **Basic Info** panel, the device details are displayed under the **Overview** tab. Each of these items are described in the following table.

Information Panel	
Model	Model name of the device.
Description	Device or product description.
Firmware Version	The firmware version of the device.
PID VID	Product ID and the Version ID.
MAC Address	The *Media Access Control (MAC)* address is a standardized data link layer address that is required for certain network interface types. These addresses are specific and unique to each device and are not used by other devices in the network.
Serial Number	The device serial number.
Status	The online / offline status of the device.
Domain	The domain name of the device.
Vendor	The manufacturer of the device.

Notification Panel	**Notifications Panel Header**—The notifications panel header shows summary counts of the outstanding notifications for the device. **Notifications Panel Body**—The body of the notifications panel lists the outstanding notifications for the device. Check the check box against a notification to acknowledge it and remove it from the list of notifications. You may use notification filtering to display acknowledged notifications if needed.
Events Panel	The Events Panel shows a list of all notifications and other events that have occurred over the past 24 hours for this device. To view and filter a complete list of all events for all devices, visit the Event Log.
POE Panel	The POE Panel is displayed on POE enabled switches and provides a summary of the power usage across each of the ports in the device.
Stack Information Panel	The Stack Information panel is displayed for switch stacks, and shows the hardware details for each member of the stack, including model information, serial number and MAC address
Connected Device Panel	Host, AP, IP Phone and IP Camera devices include the **Connected Device** panel. This panel shows how the device is attached to the network, listing the upstream network device and, where applicable, port that the device is connected to.

In addition to the **Overview** tab, the **Basic Info** panel also has an **Actions** tab that allows you to perform various operational tasks on the device.

Viewing Detailed Device Information

Procedure

Step 1 On the **Topology** or **Inventory** page, click on a network device such as a switch or a router for which you want to view detailed information.

Step 2 In the **Basic Info** panel, click **Details** at the upper right corner.

Step 3 In the **Detailed Info** panel, you will find a detailed list of device information on the left, and additional functions under the following tabs:

- **Dashboard**—Displays a series of dashboard widgets specific to the device
- **Port Management**—Allows you to manage the configuration of the switch ports

  Note
  This information is available only for devices with switch ports.

- **Wireless LANs**—Allows you to view the Wireless LANs and manage the radio configuration on the device.

  Each radio may be enabled or disabled, and the channel and transmit power controlled from this tab.

  Note
  This information is available only for wireless devices.

- **Notifications**— Provides a list of active notifications for this device.
- **Event Log**—Provides a list of past actions and notifications for this device
- **Config Backups**—Allows you to view a list of backup configuration of the devices and perform actions such as restore, save or delete configuration

  Note
  This information is available only for devices that support the Backup Configuration operation

- **Pending Config**—Compares the desired configuration based on the configuration profiles defined with the current configuration on the device and highlights any differences.

  Note
  This panel is only displayed for devices supported for configuration operations.

- IP Interfaces - Allows you to view all IP interfaces and associated IP addresses.

  Note
  This information is available only for Cisco Catalyst 1200/1300 series switches, Cisco Business 220/250/350 series switches, and Cisco 250/350/550 series switches.

Each of these are described in the following steps:

Step 4 A detailed list of information about the device is displayed on the left. This list contains the following information:

Item Name	Description
Hostname	Click **Edit** next to the device name to modify the device hostname. Click **Save** to save the changes.
Model	Model name of the device.
MAC Address	The *Media Access Control (MAC)* address is a standardized data link layer address that is required for certain network interface types. These addresses are specific and unique to each device and are not used by other devices in the network.
Status	Displays the current status of the device. For example, online or offline.
Actions	The **Actions** drop-down and **Open Device GUI** icon allow you to act on the device from the **Detailed Info** panel.
IP	The IP Addresses of the device.
Domain	The domain name of the device.
PID VID	Product ID and the Version ID.
Serial Number	The serial number of the device.
Vendor	The manufacturer of the device.
Description	Device or product description.
TAGs	In the TAGs field, enter any alphanumeric characters and then press **Enter** to create new tags for this device. To delete an existing tag, click on the ✖ in the tag. Click **Save** to save the changes. Tags may be used to help identify devices with common characteristics. You may use tags elsewhere in Cisco Business Dashboard Probe to restrict views of the network to displaying a subset of devices.
Discovery Method	Displays the protocols and devices by which this device was discovered.
Pending Config	Displays the status of the device configuration and whether there are any differences between the current config for the device and the expected config.

Step 5 Click **Dashboard** to display a set of widgets showing the current state of the device.

Step 6 Use the form to make changes, then click **Save** to apply the changes.

Step 7 Click **Port Management** to view and manage the configuration of the switch ports on the device. A visual representation of the device is displayed, similar to that shown in the **Port Management** page.

This window specifies the port details of the device in a visual representation. The model and serial number of the device are displayed above the image and a tabular view of the ports is displayed underneath.

Step 8 Click **WLAN** to manage the radio settings and view the Wireless LANs configured on this device.

Step 9 Click **Event Log** to see a list of historical notifications and other events that are recorded for this device. You can use filters to limit the entries that are displayed.

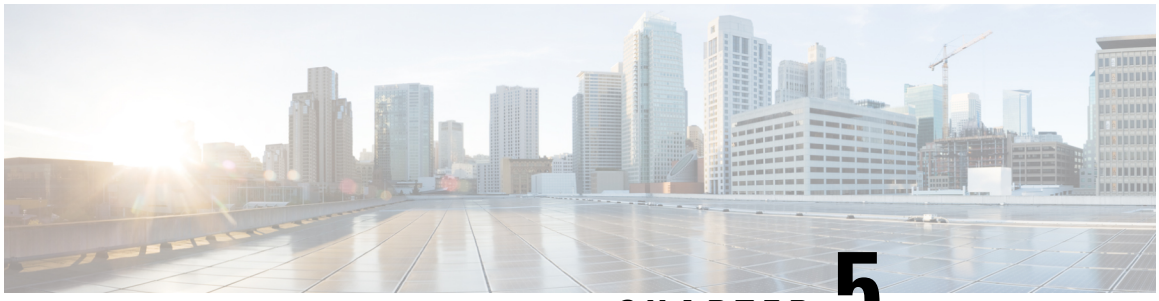
Step 10 Click **Config Backups** to view and manage configuration backups for this device. On this tab, you will see a table listing each backup stored on the Probe, with the following details:

Table 9: Config Backups

Item	Description
Timestamp	The date and time the configuration backup was taken.
Comment	The notes entered by the user at the time the backup was performed.
Backed up by	The user who performed the configuration.
Actions	Choose one of the following backup actions: • **Restore configuration to device**—Restores the selected backup to the device • **Save configuration to PC**—Saves the backup as a zip file to your local drive on your PC • **Delete configuration**—Removes the backup • **View configuration**—Helps view the contents of the configuration backup in the browser

You may also trigger a config backup from the tab by clicking **Backup Configuration**.

Step 11 Click **Pending Config** to view a side-by-side comparison between the current device config and the expected configuration based on the configuration profiles applied to the device. Configurations are represented in a device-independent format and any differences are highlighted. You may use the buttons at the top of the page to apply any outstanding changes, accept the current device configuration, or re-read the current device configuration. You may click the Reapply Network Configuration button to reapply selected network configuration profiles to this device.



CHAPTER 5

Inventory

This chapter contains the following sections:

Viewing Device Inventory

Access the Inventory page to view, monitor and support all of the device inventory in your network. The **Inventory** page displays a complete list of the devices and their details in a tabular view. Additionally, it also provides action buttons to perform configuration tasks and apply the latest firmware updates for supported devices. The following table provides details of the information displayed:

Table 10: Inventory Details

Item	Description
Hostname	Displays the name of the device.
Type	The type of device such as a switch, router or wireless access point (WAP).
Tags	Lists any tags associated with the device.
IP	The Internet Protocol (IP) addresses of the device.
MAC	The Media Access Control (MAC) address is a standardized data link layer address that is required for certain network interface types. These addresses are specific and unique to each device and are not used by other devices in the network.
Serial Number	The serial number for the device.
Version	The current firmware version of the device.
Vendor	The vendor that manufactured the device.
Model	Model name of the device.
Notification	A count of the outstanding notifications for the device

The following additional controls are available on the **Inventory** page:

- **Select columns** button—Use this button located at the top left of the table to choose which columns to display.
- **Filter Box**—You may use the **Filter box** to limit the display by typing device names, device types, serial numbers and so on. By default, the inventory is filtered to display only network devices.
- Export to CSV File button - Click this icon to export all devices matching the current filters to a CSV file.
- **Refresh** button—Click this button to update the table to show the latest available information.
- **Action** button —Allow you to perform actions on one or more selected devices. Action buttons are only displayed when one or more devices supporting actions are selected. For more details on these actions, see next topic.

Performing Device Actions

You can perform actions such as firmware update, configuration backup & restore and reboot easily on devices in the network. To perform these actions, do the following:

Procedure

Step 1 On the **Inventory** page, click on a network device such as a switch or a router.

Step 2 In the **Basic Info** panel, select the **Actions** tab. Depending on the device capabilities one or more of the following actions are displayed:

Update firmware to latest	Allows you to apply the latest firmware update to the device. Cisco Business Dashboard Lite will download the update from Cisco and then upload it to the device. The device will reboot at the completion of the update.
Upgrade From Local	Allows you to upload a firmware upgrade file from your local drive. Cisco Business Dashboard Lite will upload the file to the device, and the device will reboot at the completion of the update.
Backup Configuration	Allows you to save a copy of the current device configuration on the Dashboard. **a.** Click **Backup Configuration**. **b.** In the **Backup Configuration** window, optionally, you may add a note in the text box for the backup you wish to perform. **Note** This note is displayed whenever the backup is listed in the GUI. **c.** Click **Save Backup** to complete this action or **Cancel** if you no longer wish to proceed. A backup configuration job is created and may be viewed in the **Task Center**.

Restore Configuration	Allows you to restore a previously backed up configuration to the device. Click **Restore Configuration**. The following backup configuration options are provided: • **Backups for *device name***—Lists all available backups to configure for a specific device • **Backup for other device**—Lists all available backups to configure other devices of the same type or same Product ID • **Backup for other compatible device**—Lists all available backups to configure other devices in the series that are compatible with the selected device To perform the backup configuration, do the following: **a.** In the **Restore Configuration** window, select the backup you wish to restore to the device. Use the scroll bar to view all the available backups and click the corresponding radio button. This enables the **Restore Configuration** button. Alternatively, you may choose to upload a configuration file. To do so, drag and drop the configuration file onto the target area, or click on the target area to select a file from the file system. **b.** Click **Restore Configuration** to complete this action. A restore configuration job is created and may be viewed in the **Task Center**.
Reboot	Restarts the device. When you click this button, you will be prompted to click again to confirm.
Save Running Configuration	For devices that support separate running and startup configurations, this action copies the current running configuration to the startup configuration. This ensures any configuration changes that are retained when the device next reboots.
Run CLI Command	Open the CLI Command Runner tool with the selected devices automatically pre-populated.
Delete	Remove an offline device from the Topology and Inventory.

Step 3 Device actions may optionally be scheduled to take place at a later time. To schedule a device action, click **Schedule** and fill out the form to create a new **Schedule Profile**.

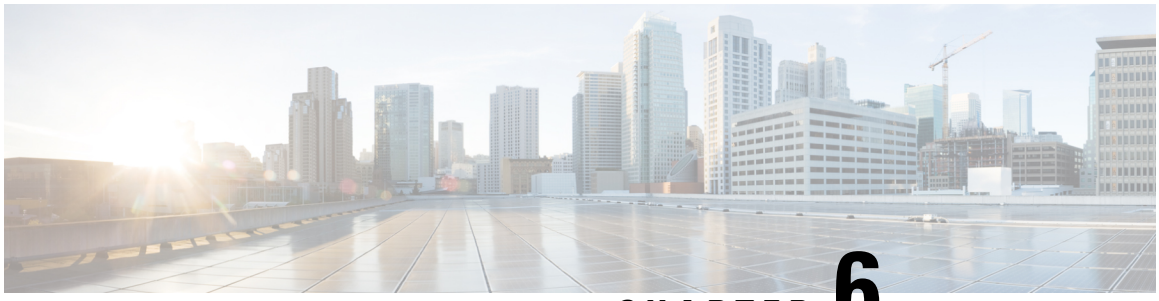
Accessing the Device CLI

In some circumstances, you may need to access the command line interface of a network device directly. To access the command line interface, do the following:

1. On the **Topology** or **Inventory** page, click on a network device such as a switch which you want to access the command line interface (CLI).

2. In the Basic Info panel, click **Open Device CLI** icon at the upper right corner. A new window will open in your browser showing the device command line interface.
3. SSH server must be enabled for CBD Lite to access the CLI. If it's not enabled, an option may be provided to initiate a jobthat enables it automatically. Please wait a few minutes for the job to complete successfully, then try again by clickingthe Open Device CLI icon.
4. If a device has saved credentials, CBD Lite will automatically log in SSH using those credentials. Otherwise, users will needto manually enter their username and password.

Note When you access the command line interface by clicking Open Device CLI icon, your browser will connect to the device through the Dashboard.



CHAPTER 6

Provision

This chapter contains the following sections:

Port Management

Port Management provides a front panel view of each device that includes switch ports that can be configured by Cisco Business Dashboard. This page allows you to view the status of the ports including traffic counters, and make changes to the port configuration. This page also lets you view and configure the Smartports role for ports on devices that support Smartports. You can use the search box to limit the devices displayed. Type in all or part of a device name, product ID, or serial number to find the desired device.

A list view of the same information is also provided to show all the switch ports in a tabular format. The front panel view in **Port Management** presents two different views of the device:

The **Physical** view allows you to see the status and change the configuration of the port at the physical layer. You can view or change settings for speed, duplex, Energy Efficient Ethernet (EEE), Power over Ethernet (PoE), and VLANs. Each port is shown with a green LED indicating link and a yellow LED indicating that power is being supplied to the attached device.

The **Smartports** view allows you to see the current Smartports role for each port, and to change the role.

Note A **Smartport** is an interface to which a built-in (or user-defined) template can be applied. These templates are designed to provide a means of quickly configuring the device to support the communication requirements and utilize the features of various types of network devices.

To view the status of a port, click on the port in either the front panel view or list view. The Basic Info panel for the port appears, showing a series of panels as follows:

General	This panel shows the physical layer status of the port and allows you to enable the port or shut it down
Ethernet	Use this panel to control speed and duplex settings
VLAN	This panel shows the VLANs currently configured on the port. Click the **Select VLAN** or **Create VLAN** buttons to modify this configuration

POE	This panel is only displayed for POE-enabled ports, and allows you to configure the POE settings for the port. You can also power-cycle an attached POE device by clicking the Toggle Power button
Green Ethernet	This panel allows you to manage the Energy Efficient Ethernet (EEE) configuration for the port
Port Authentication	This panel allows you to enable 802.1x port authentication on this port. Authentication will be performed against the authentication server(s) specified in the Authentication profile.
Smartports	This panel shows the Smartports roles available for this port. Click on a role to apply that configuration to the port. The currently configured role is highlighted.

To make changes to the port settings, click the **edit** icon in the top right of the pane containing that setting. Once the changes have been made, click the **Save** icon.

Network Configuration

The **Network Configuration** pages allow you to define various configuration parameters that typically apply to all devices in the network. These parameters include configuration such as time settings, domain name services, administrator authentication, and Virtual LANs.

Time Management

The **Time Management** page allows you to configure timezones, daylight saving, and NTP servers for the network. The following sections provide instructions on modifying the Time Settings configuration profile.

Modifying a Time Management Configuration Profile

1. Navigate to **Provision > Network Configuration** > **Time Management**.
2. Click the toggle button to enable the profile.
3. In the **Time Setting** section, select an appropriate timezone from the drop-down list.
4. Optionally enable **Daylight Saving** by checking the check box, and then specify the parameters for daylight saving in the fields provided. You may choose to specify fixed dates or a recurring pattern. You may also specify the offset to be used.
5. Optionally enable the Network Time Protocol (NTP) in the **Use NTP** section for clock synchronization by checking the check box. In the boxes provided specify at least one NTP server address.
6. Click **Update**.

DNS Resolvers

The **DNS Resolvers** page allows you to configure the domain name and domain name servers for the network. The following sections provide instructions on creating, modifying and deleting the DNS resolvers configuration profile.

Modifying a DNS Resolver Configuration Profile

1. Navigate to **Provision > Network Configuration** > **DNS Resolvers**.
2. Click the toggle button to enable the profile.
3. Specify the domain name for the network.
4. Specify at least one DNS server address.
5. Click **Save**.

Authentication

The **Authentication** page allows you to configure administrative user access to network devices and set authentication servers (RADIUS servers) to use when authenticating network access. The following sections provide instructions on modifying the authentication configuration profile.

1. Navigate to **Provision > Network Configuration > Authentication**.
2. Click the toggle button to enable the profile.
3. Optionally, specify one or more username and password combinations for local user authentication. Additional users may be added by clicking the ✚ (plus) icon.
4. Optionally specify one or more RADIUS servers to use for authentication.
5. Click **Update**.

Virtual LANs

The **Virtual LANs** page allows you to divide your switch network into multiple virtual networks or VLANs. You can find the existing VLANs in the network that were not configured by Cisco Business Dashboard Lite also displayed on this page in a separate table. The following sections provide instructions on modifying Virtual LAN configuration profile.

Create a Virtual LAN

1. Navigate to **Provision > Network Configuration** > **Virtual LANs**.
2. Click the toggle button to enable the profile.
3. You can choose how the profile applies VLANs to switch trunk ports. Select one of the following update modes:
   - **Apply VLANs to all switch trunk ports**: Adds the VLANs to the allowed VLAN list of every switch trunk port.
   - **Apply VLANs only to switch trunk ports connected to network devices**: Adds the VLANs to the allowed VLAN list only for switch trunk ports connected to network devices. This option relies on topology detection, which may be unavailable for newly discovered devices or when LLDP/CDP is disabled.
   - **Do not apply VLANs to switch trunk ports**: Does not add the VLANs to the allowed VLAN list of any switch trunk port.

If a trunk port is already configured to allow all VLANs, the selected VLAN update mode does not affect that port.

4. Click the ✚(plus) icon to add a new VLAN.
5. Specify a descriptive name for the VLAN, and the VLAN ID to be used. The VLAN ID should be a number in the range 1-4094.
6. You may create multiple VLANs. If you want to create additional VLANs, click **+ (plus) icon** and go back to step 4.
7. Click **Update**. The new VLAN will be created on all VLAN-capable devices.

If the VLAN ID of the newly created VLAN matches an existing VLAN already present on devices, that VLAN will be adopted by Cisco Business Dashboard Lite and removed from the discovered Virtual LANs table.

Modify a VLAN

1. Click the edit button.
2. Make the required changes to the VLAN settings and click **Update**.

Remove a VLAN

1. Click the edit button.
2. Click the X icon next to the VLAN to be removed.

Remove a VLAN not created by Cisco Business Dashboard Lite

In the table of discovered VLANs, click the **delete** icon next to the VLAN or VLANs to be removed.

Note VLAN 1 may not be deleted.

Wireless LANS

The Wireless LANs page allows you to manage the wireless networks in your environment. You can find the existing Wireless LANs in the network that were not configured by Cisco Business Dashboard Lite also displayed in a separate table. The following sections provide you instructions on modifying Wireless LAN configuration profile.

Create a Wireless LAN

To create a wireless LAN, complete the following steps.

Procedure

Step 1 Navigate to **Provision > Network Configuration > Wireless LANs**

Step 2 Click the toggle button to enable the profile

Step 3 Click the ✚(plus) icon to add a new Wireless LAN.

Step 4 Specify an SSID name for the Wireless LAN, and the VLAN ID that it should be associated with. The VLAN ID should be a number in the range 1-4094.

Step 5 Select the type of security required.

Step 6 If you select an **Enterprise** security type, then make sure to enable the authentication profile containing the preferred RADIUS server(s) to use.

Step 7 Optionally, click to expand the Advanced Settings to change the **Broadcast**, **Application Visibility**, **Local Profiling** and **Radio** settings to match your requirements.

Step 8 Click **Save** to continue or **Cancel** to discard your changes.

Step 9 You can create multiple Wireless LANs. If you want to create additional Wireless LANs, Click the ✚ (plus) icon and go back to step 4.

Step 10 Click **Update**. The new WLANs will be created on all devices with wireless access point capabilities.

If the newly created Wireless LAN matches an existing Wireless LAN already present on devices, that Wireless LAN will be adopted by Cisco Business Dashboard Lite and removed from the discovered Wireless LANs table.

Step 11 To modify a Wireless LAN, click **Edit,** make the required changes and then click **Update.**

Step 12 To remove a Wireless LAN, click **Edit**, then click **Delete** and then click **Update**.

Step 13 To remove a Wireless LAN that was not created by Cisco Business Dashboard Lie, in the table of discovered Wirless LANs, click the radio button for the Wireless LAN to be removed and then click **Delete.**

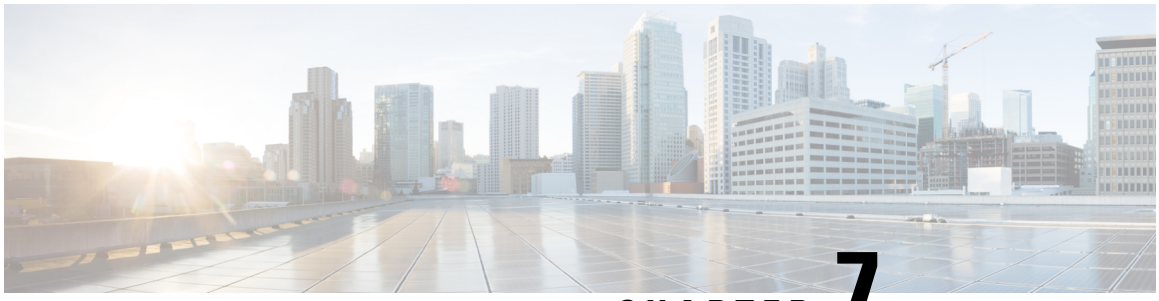
Reapply Network Configurations

In certain situations, such as when the device is offline or lacks the correct credentials, changes made to a network configuration profile may not be applied to the devices. To fix this, the network configuration profile may be reapplied to all devices using the following steps:

1. Navigate to the network configuration page.
2. Click **Reapply Configuration**.

Alternatively, you can go to the device detail page to perform the reapplication. Cisco Business Dashboard Lite supports reapplication at two levels.

- **Profile level**: Applies the current network configuration profile to all devices.
- **Device level**: Applies selected network configuration profiles to an individual device.



CHAPTER 7

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 11: 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.

Event	Level	Description	Clears Automatically?
Reachability/Device Offline	Alert	A device is no longer detectable on the network	Yes, when the device is rediscovered.
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 12: 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 38 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.

Configuration Backups

The Configuration Backups page provides a centralized view of configuration backups for all managed devices. Use this page to quickly identify which devices have available backups, verify the latest backup timestamps, and find devices that currently do not have backup protection.From the global view, you can initiate manual

backup operations, download configuration files for selected devices or all devices, and manage automatic retention policies for cleanup of older backup files.

View Configuration Backup Status

1. Navigate to **Assurance > Configuration Backups**.
2. Optionally, use the filter box to filter the devices that are displayed.
3. Review the table. The table displays device details together with the total number of available backups, the last backup time, the last backup comment, and the user who most recently backed up the device.

Back Up Device Configurations

1. Navigate to **Assurance > Configuration Backups**.
2. Select one or more devices in the **Configuration Backups** table.
3. Click the backup action in the toolbar to back up the selected devices. To back up a single device, you can also use the backup action in the **Action** column for that device.

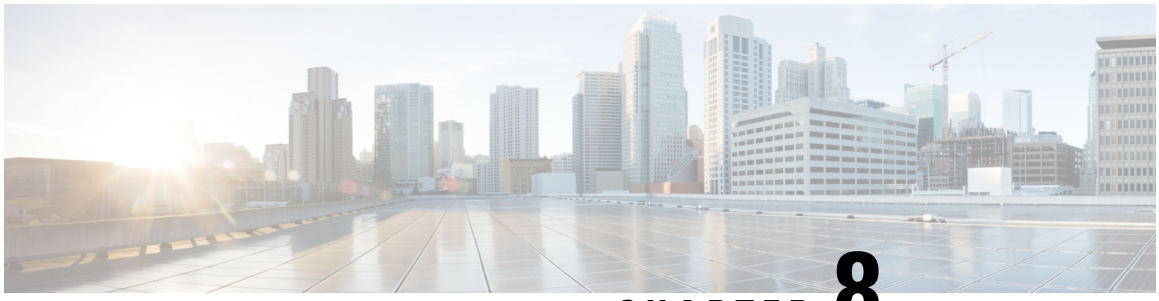
Download Backup Files

1. Navigate to **Assurance > Configuration Backups**.
2. To download most recent backups for selected devices, select one or more devices and click the **Save configuration to PC** action in the toolbar.
3. To download most recent backups for all devices, click the **Save configuration to PC** action in the toolbar directly without selecting any devices.
4. To download most recent backup for a single device, click the **Save configuration to PC** action in the toolbar or in the **Action** column.

Manage Auto Cleanup Policies

1. Navigate to **Assurance > Configuration Backups** and select the **Auto Cleanup Policy** tab.
2. To change the system default policy, select **Enable Auto Cleanup** if required, specify the cleanup parameters - including how old backups must be before deletion and the minimum number of recent backups to keep, and click **Save**.
3. Click the **Run Cleanup Now** to perform a manual cleanup, which allows you to immediately remove backup files using the configured cleanup parameters without waiting for the scheduled auto cleanup

Note An event log entry is generated for each cleanup action that deletes backup files.



CHAPTER 8

Tools

This chapter contains the following sections:

CLI Command Runner

The **CLI Command Runner** tool allows you to execute diagnostic CLI commands on supported devices and immediately view the output. You may run one or more commands across any number of selected devised from a single workflow.

Note CLI Command Runner is intended for **EXEC** mode diagnostic commands, such as show commands. Use **CLI Template** for configuration-related tasks.

Run Diagnostic CLI Commands

Complete these steps to run the diagnostic CLI command runner.

Procedure

Step 1 Navigate to **Tools** > **CLI Command Runner**.

Step 2 Select the target type: **Devices, or All Devices.**

Step 3 If the target type is Devices, in **Select Devices** field, type to search and select the devices on which the ommands should run.

Step 4 In **Select/Enter Commands** field, choose commands from the default command list or enter commands manually. The current user most recent executed 20 commands are listed at the top of the command list.

Step 5 Optionally, select **Auto Enable SSH Server on Device** to automatically enable the SSH server on supported devices before command execution.

Step 6 Click **Run Command(s)**.

Note

Commands are executed on the device through an SSH connection. Cisco Business Dashboard can automatically enable the SSH server on supported devices if it is currently disabled. If automatic enablement is not supported for a device, you must manually enable the SSH server on that device before proceeding.

Review and Export CLI Output

Follow these steps to review and export the CLI output.

Procedure

Step 1 Navigate to **Tools > CLI Command Runner**.

Step 2 Click the **Last Run** link beside the page title.

Step 3 Review the results of the most recent execution and export the output if required

View the Last Execution Results

Follow these steps to review and export the CLI output.

Procedure

Step 1 Navigate to **Tools > CLI Command Runner**.

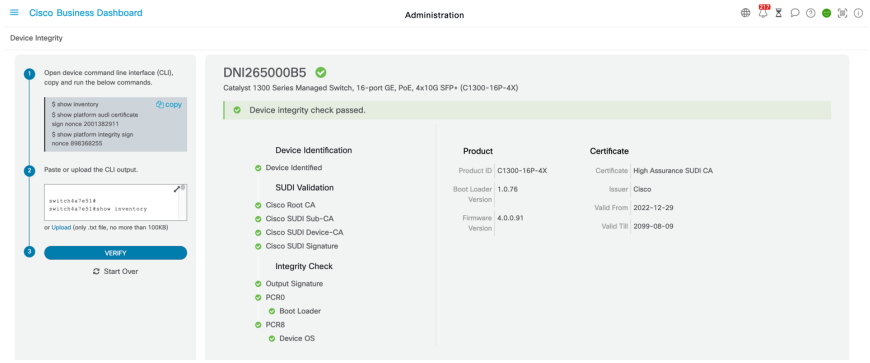
Step 2 Click the **Last Run** link beside the page title.

Step 3 Review the results of the most recent execution and export the output if required

Device Integrity

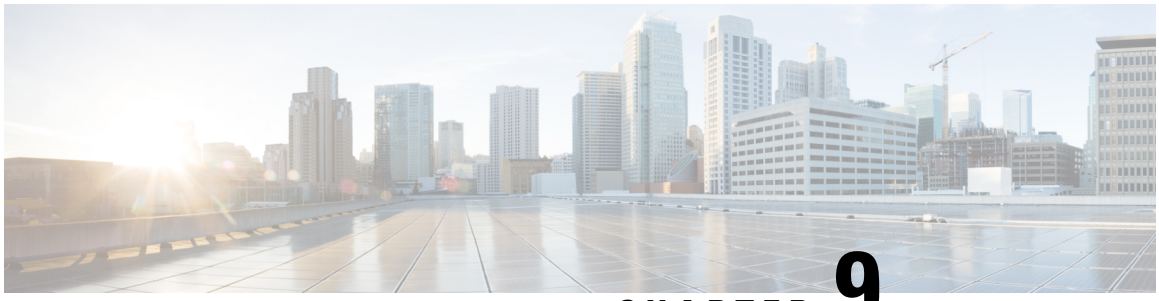
This service analyzes the integrity of your Cisco product by verifying key components of Cisco's software and hardware that include Cisco's Trustworthy Technologies. These security technologies are designed into Cisco Networking devices to protect against counterfeit and software modification and verify that Cisco

products are operating as intended.



To verify device integrity, follow these steps:

1. Copy the CLI commands.
2. Open the device command line interface (CLI), paste and run the CLI commands.
3. On the CBD GUI, paste the CLI outputs or save the CLI outputs into a file, then upload.
4. Click **Verify.**



CHAPTER 9

Reports

This chapter contains the following sections:

Lifecycle

The **Lifecycle** Report provides a high level view of the status of the network devices, taking into account both software and hardware lifecycle status. The following table describes the information provided in this report.

Field	Description
Hostname	The hostname of the device.
Device Type	The type of device.
Model	The model number of the device.
Week of Manufacture	The date of manufacture for the device, displayed as week number and year.
Firmware Update Available	Displays the latest firmware version available for the device, or states that the device firmware is currently up to date.
Firmware Version	Displays the current firmware version running on the device.
End of Life Status	Specifies if an End of Life bulletin has been published for the device and the date of the next key milestone in the End of Life process.
Maintenance Status	Specifies if the device is currently under warranty or covered by a support contract.

The row in the table for a device that may require attention is color-coded to indicate the urgency. For example, a device with a published End of Life bulletin will be colored orange if the End of Support milestone has not been reached, and red if the device is no longer supported by Cisco.

The Search box located at the top of the report can be used to filter the results. Enter text in the Search box to limit the number of entries that are displayed with the matching text.

The column selection icon at the top left of the report can be used to customize the information displayed. Click on the icon and then use the check boxes that appear to select the columns you wish to include in the report.

End of Life

The **End of Life Report** lists any devices that have an **End of Life** bulletin published, along with key dates in the End of Life process, and the recommended replacement platform. The following table describes the information provided:

Table 13: End of Life Report

Field	Description
Product ID	The product ID or part number of the device.
Name	The hostname of the device.
Device Type	The type of device.
Current Status	The stage at which the End of Life process of the product is at.
Date of Announcement	The date the End of Life bulletin was published.
Last Date of Sale	The date after which the product will no longer be sold by Cisco.
Last Date of Software Releases	The date after which no more software versions will be released for the product.
Last Date for New Service Contract	The last date for taking out a new support contract on the device.
Last Date for Service Renewal	The last date for renewing an existing support contract on the device.
Last Date of Support	The date after which Cisco will no longer provide support for the product.
Recommended Replacement	The recommended replacement product.
Product Bulletin	The product bulletin number and a link to the bulletin on the Cisco website.

Each row of the table is color-coded to indicate the stage of the End of Life process the device is at. For example, a device that has past the Last Date of Sale but not yet reached the Last Date of Support will be colored orange, and a device that is past the Last Date of Support is colored red.

Maintenance

The **Maintenance** Report lists all network devices which includes the warranty and support contract status information for each of them. The following table describes the information provided in this report.

Field	Description
Hostname	The hostname of the device.
Device Type	The type of device.
Model	Model number of the device.
Serial Number	The serial number for the device.
Status	The current support status of the device.
Coverage End Date	The date at which the current support contract will expire.
Warranty End Date	The date at which the warranty for the device will expire.

Each row of the table is color-coded to indicate the support status for the device. For example, a device that is approaching the expiry date of the warranty or support contract will be colored orange, while a device that is out of warranty and does not have a current support contract will be colored red.

The Search box located at the top of the report can be used to filter the results. Enter text in the Search box to limit the number of entries that are displayed with the matching text.

The column selection icon at the top left of the report can be used to customize the information displayed. Click on the icon and then use the check boxes that appear to select the columns you wish to include in the report.

Viewing the Wireless Client Report

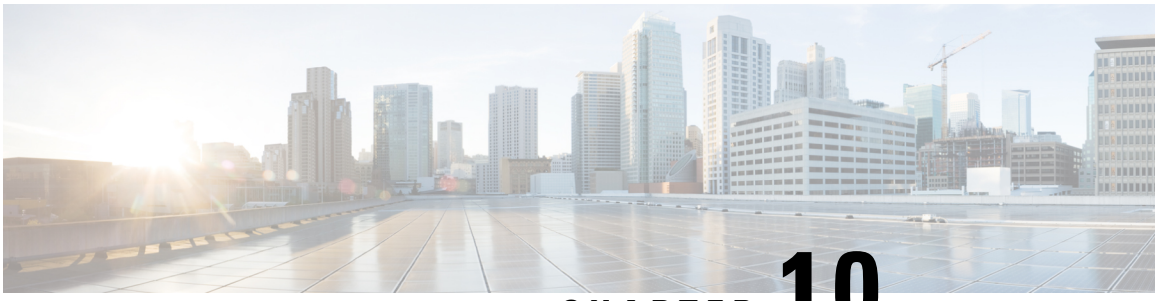
The **Wireless Client Report** shows details about the wireless clients on the network. Reports may be generated for time ranges from daily to yearly using the controls at the top of the page. Each data sets includes graphs that shows a breakdown over time for the selected row.

The following tables describe the information provided in each report.

Table 14:

Column	Description
MAC	The MAC address of the client.
Hostname	The hostname of the client, where available.
Username	The username entered by the client in the guest portal. Only available for wireless guest.
SSID	The SSID the client was last associated with.

Column	Description
802.11 Type	The 802.11 variant used by the client.
Usage	The total volume of data sent and received by the client.
First Seen	The time at which the client was first detected.
Last Seen	The time at which the client was last seen.
Time Online	The total time that the client was online.
% Online Time	The percentage of time the client was online in the total time the client was known to the network.



CHAPTER 10

Administration

This chapter contains the following sections:

Discovery

The Cisco Business Dashboard Lite builds an initial list of devices in the network from listening to mDNS (aka Bonjour, please check your device setting to make sure Bonjour is enabled on the Management VLAN) advertisements. The Cisco Business Dashboard Lite then connects to each device using a supported protocol and gathers additional information such as CDP & LLDP adjacency tables. This information is used to identify additional devices in the network, and the process repeats until all devices have been discovered.

Cisco Business Dashboard Lite may not always be able to discover network devices in other VLANs or subnets using only the automated discovery processes. When this occurs, it can be beneficial to have the dashboard explicitly search the IP address ranges associated with those VLANs or subnets. To search an IP address range, do the following:

1. Navigate to **Administration > Discovery**.
2. Specify the IP address ranges to search.
3. Click **Save**.

Based on the input, the Dashboard Lite will search the specified address ranges for devices with an active web server and attempt to connect to the device HTTPS port (443) using the credentials provided. If the dashboard is successful in accessing the device, it will be added to the inventory and will be managed in the same way as any other device in the network.

By default, the Dashboard may display any discovered IP address for devices with multiple IP addresses. If you specify a Management VLAN, the IP address of the VLAN interface that matches the configured Management VLAN will be shown in the Inventory and Topology views. The Management VLAN setting only affects which IP address is displayed; the Dashboard may use any discovered, reachable IP address to access the device.

Device Credentials

For Cisco Business Dashboard Lite to fully discover and manage the network, it needs credentials to authenticate with the network devices. When a device is first discovered, the **Cisco Business Dashboard Lite** will attempt to authenticate with the device using the default username: `cisco`, password: `cisco`. If this attempt fails, a notification will be generated and valid credentials must be supplied by the user. To supply valid credentials, follow the steps below.

1. Navigate to **Administration** > **Device Credentials**. The first table on this page lists all the devices that have been discovered that require credentials.
2. Enter valid credentials into the **Username/Password** fields. You may click the ✚(plus) icon next to the corresponding field to enter up to three **Cisco Business Dashboard Lite** credentials. Ensure that passwords are entered using plain text.
3. Click **Apply**. The **Cisco Business Dashboard Lite** will test each credential against each device that requires that type of credential. If the credential is valid, it will be stored for later use with that device.
4. Repeat steps 2 to 3 as necessary until every device has valid credentials stored.

To enter a single credential for a specific device, follow the steps below.

1. Click the **Edit** icon shown against the device in the discovered devices table. A popup will appear prompting you to enter a credential that corresponds to the Credential Type selected.
2. Enter a username and password credential in the fields provided.
3. Click **Apply**. To close the window without applying, click the ✖ on the top right corner of the pop-up.

Underneath the **Add New Credential** section is a table showing the identity for each device for which has a valid credential stored and the time that credential was last used. To display the stored credential for a device, you may click the **Show Password** icon next to the device. To hide the credentials again, click the **Hide Password** icon. You may also show and hide credentials for all devices using the button at the top of the table. You may also delete credentials that are no longer required. To delete stored credentials, follow the steps below.

1. Navigate to **Administration** > **Device Credentials**.
2. In the **Saved Credentials** table, select the check box against one or more sets of credentials to be deleted. You may also select the checkbox at the top of the table to select all credentials.
3. Click **Delete Selected Credentials**.

To delete a credential for a single device, you may also click the **Delete** icon next to the device.

Users

The **User Management** page allows you to control how users are granted access to Cisco Business Dashboard Lite, change settings that affect how those users interact with the Dashboard.

Cisco Business Dashboard Lite has settings to control the dashboard features that are available using the Dashboard Access drop-down list. The options available for these settings include:

- **Administrator**—An Administrator has full access to Dashboard features including the ability to maintain the system.
- **Operator**—An Operator has similar power to an Organization Administrator, but cannot manage users.
- **Read only**—A Read only user can only view network information, they cannot make any changes.

Cisco Business Dashboard Lite allows users to be authenticated against the local user database.

When the Cisco Business Dashboard Lite is first installed, a default **Administrator** is created in the local user database with the username and password both set to `cisco`.

Note User settings can be managed by **Administrators** only.

Add a New User to the Local User Database

1. Navigate to **Administration**>**Users** and select the **Users** tab.
2. Click the ✚ (plus) icon to create a new user.
3. In the fields provided, enter a username, display name, email address and password, and specify the Dashboard Access settings. You may also provide contact details for the user.
4. Click **Save**.

Modify a User

1. Navigate to **Administration**>**Users** and select the **Users** tab.
2. Select the radio button next to the user that needs to be changed and click the **Edit** icon.
3. Make the modifications as required.
4. Click **Save**.

Delete a User

1. Navigate to **Administration**>**Users** and select the **Users** tab.
2. Select the radio button next to the user that needs to be deleted and click **delete** at the top of the table.

Change password complexity

To enable or change password complexity requirements, follow these steps.

1. Navigate to **Administration**>**Users** and select the **User Settings** tab.
2. Select the **Local** tab under **Authentication Source**, modify the **User Password Complexity** settings as required and click **Save**.

Restore Access when All Administrative Access has been Lost

If administrative access to the Cisco Business Dashboard Lite application is lost, follow these steps to recover the same access.

1. Log on the server of the Dashboard Lite, open the Dashboard Lite Server Application.
2. Click the **Tools** > **Recover Password** menu.

After that, the local user authentication is enabled, and the default Administrator with username **cisco** and password **cisco** is restored.

Change session timeouts

To change idle and absolute timeouts for user sessions, follow these steps.

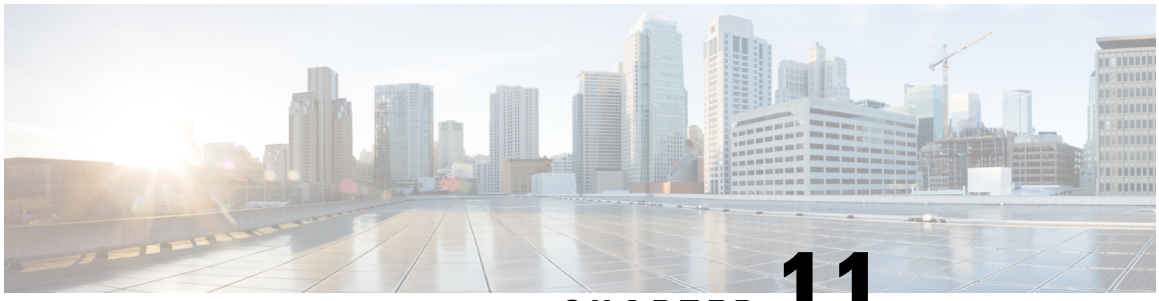
1. Navigate to **Administration**>**Users** and select the **User Settings** tab.
2. Modify the **User Session** parameters as required and click **Save**. Hover over the help icons to see allowable ranges for these parameters.

Login Attempts

Cisco Business Dashboard Lite keeps a log of every attempt made to log in and out of the system, both successful and unsuccessful. To view the log, navigate to **Administration**>**Login Attempts**. The table displays the following information:

Field	Description
Username	The username associated with the event.
Display Name	The display name for the user.
IP	The IP address of the device from which the user logged in.
Type	The type of event including: • LOGIN • LOGOUT
Status	Indicates if the attempt succeeded or failed.
Timestamp	The date and time the event took place.

You may use the search box above the table to show only entries that match a particular user or IP address.



CHAPTER 11

System

This chapter contains the following sections:

Privacy Settings

Some of the features of Cisco Business Dashboard Lite require the use of online services hosted by Cisco and result in the sharing of certain information with Cisco. These services include:

- **Lifecycle Reporting**—This feature includes the generation of the **Lifecycle Report**, **End of Life Report and Maintenance Report** in Cisco Business Dashboard Lite. Lifecycle Reporting is enabled by default.
- **Product Improvement**—This feature allows Cisco Business Dashboard Lite to send information about hardware and software usage in the network for the purpose of further developing the Cisco product portfolio. Product Improvement is enabled by default.
- **Software Updates**— Notification of the availability of software updates for network devices, and the ability to have those updates automatically applied. Software Updates are enabled by default.

All of these features are subject to the Cisco Privacy Policy and you may enable or disable them at any time. The **Privacy Settings** page is displayed during the initial setup of the Dashboard, allowing you to disable any of the default enabled features prior to any network data being collected. More detail for each of these features and the information shared may be found below.

Lifecycle Reporting

Cisco Business Dashboard Lite provides information on the lifecycle state of each of the Cisco devices in the network. In order to do this, the Dashboard must provide Cisco with the product ID, serial number and hardware and software versions for each Cisco device. The IP address of the Dashboard may also be recorded. No personal or sensitive information will be intentionally collected during this process.

To disable the generation of lifecycle reports, follow the steps below.

1. Navigate to **System**>**Privacy Settings**.
2. Un-check the check boxes for the reports you wish to disable.
3. Click **Save**.

Product Improvement

By enabling this feature, Cisco Business Dashboard Lite periodically sends hardware and software product usage information to Cisco. The IP address of the Dashboard may also be recorded. No personal or sensitive information will be intentionally collected during this process.

To see an example of what information is sent, follow the steps below.

1. Navigate to **System** > **Privacy Settings**.
2. Click the **View a Sample** link next to the **Send product improvement data to Cisco** checkbox. An example of an upload with sample data will be displayed.

To disable the generation of product improvement data, do the following:

1. Navigate to **System** > **Privacy Settings**.
2. Uncheck the **Send product improvement data to Cisco** checkbox.
3. Click **Save**.

Software Updates

Use of this feature requires Cisco Business Dashboard Lite to send the product ID and hardware and software version information for each device to Cisco. Your local IP address may also be recorded. No personal or sensitive information will be intentionally collected during this process.

To disable the use of automatic software updates, do the following:

1. Navigate to **System**>**Privacy Settings**.
2. Un-check the check boxes for both device firmware checks and Cisco Business Dashboard Lite application checks.
3. Click **Save**.

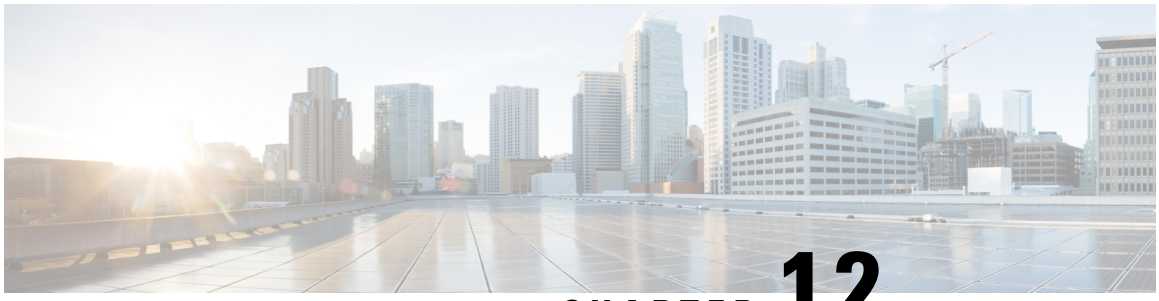
Log Settings

The Log Settings page allows you to control the amount of detail included in log files. The default logging level is Info, but you can reduce the number of messages logged by selecting Warn or Error, or view more detail by selecting Debug.

To change the log levels for the Dashboard, follow the steps below.

1. Navigate to **System > Log Settings**.
2. Use the radio buttons to select the desired logging level.
3. Click **Save**.

The log files for the Dashboard can be found in the directory %LOCALAPPDATA%\CiscoBusiness\DashboardLite/logs on the local file-system. You may click Download Log File to download an archive of the contents of this directory. It may take several minutes to collect all the data.



CHAPTER 12

Job Management

This chapter contains the following sections:

About Jobs and Job Center

Any tasks or actions carried out by Cisco Business Dashboard Lite are referred to as Jobs and are tracked in the Job Center. Jobs include both user-initiated jobs and jobs initiated automatically by the system

The Job Center lists all jobs that are currently executing or have occurred in the past on the Jobs tab, including details such as the type of job, affected devices, and the current status or whether the job completed successfully.

In addition to showing currently executing and historical jobs, the Job Center has a second tab for **Schedule Profiles**. A Schedule Profile represents a job that is yet to occur because it has been scheduled for a later date. Schedule Profiles include tasks that will run only once, as well as tasks that have been defined to run periodically.

Viewing and Filtering Jobs

To view currently active jobs and historical jobs, follow the steps below.

Procedure

Step 1 In the Home window, click the Job Center icon on the top right corner of the global tool bar. The number badge on the icon specifies the total number of currently executing jobs. Currently active and historical jobs are listed on the Jobs tab in the Job Center. Information such as the Job Type, who it was created by and when, and status information are all displayed. You may click on the Job Type parameter for a specific job to display more detailed information

Step 2 The Filter box limits the jobs displayed in the table. By default, all jobs will be listed. To change an existing filter, double-click on that filter to change the setting. To add a new filter, click on the Filter by attributes label and select a filter from the drop-down list.

Managing Schedule Profiles

The **Schedule Profiles** tab does not just allow you to view the profiles that have been defined. You can also create new profiles and edit or delete existing profiles. You can also search for all the jobs that have been created by a profile.

To create a new schedule profile, follow the steps below.

1. In the **Home** window, click the **Job Center** icon on the top right corner of the global tool bar. Select **Schedule Profiles**.
2. Click the ✚ (plus) icon at the top left of the table.
3. In the **Job Detail** section of the displayed form, select a job type, and target devices or all devices. Note that selected job types may not be applied to all devices. Available job types are as follows:
   - Reboot device
   - Backup configuration for device
   - Restore configuration for device
   - Upgrade device firmware
   - Save device running configuration
   - Upgrade device firmware to the latest
4. In the **Schedule** section of the form, select a recurrence and specify a start time for the job. For recurring jobs, also specify when the job should end.
5. Depending on the job type selected, additional information may be required. If so, additional fields will be displayed underneath the Schedule section of the form. Complete these fields as required.
6. When you are satisfied with the configuration, click **Save**. To exit without creating a profile, click **Cancel**.

To edit an existing schedule profile, follow these steps below.

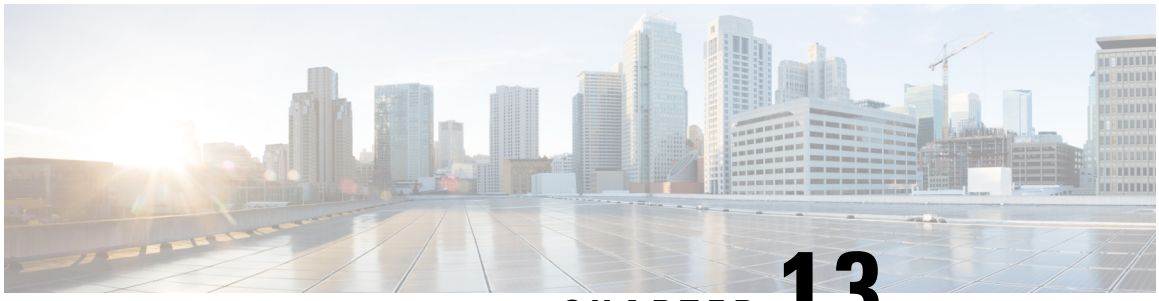
1. In the **Home** window, click the **Job Center** icon on the top right corner of the global tool bar. Select the **Schedule Profiles** tab.
2. Identify the profile you need to edit. You can use the filters to help you identify the right profile.
3. Look in the **Actions** column at the far right of table. Click the **edit** icon.
4. Update the profile using the form that is provided. Note that you cannot change the job type of a profile.
5. When you are satisfied with your changes, click **Save**. To discard any changes, click **Cancel**.

To remove an existing schedule profile, follow the steps below.

1. In the **Home** window, click the **Job Center** icon on the top right corner of the global tool bar. Select the **Schedule Profiles** tab.
2. Identify the profile you want to remove. You can use the filters to help you identify the right profile.
3. Click the **delete** icon in the **Actions** column to remove the profile.

To see all the jobs associated with a schedule profile, follow the steps below.

1. In the **Home** window, click the **Job Center** icon on the top right corner of the global tool bar. Select the **Schedule Profiles** tab.
2. Identify the profile you want to search for associated jobs. You can use the filters to help you identify the right profile.
3. Click the **View Jobs** icon in the **Actions** column. The view switches to the **Jobs** tab with the displayed filtered to show only jobs that are associated with this profile.



CHAPTER 13

AI Assistant

This chapter contains the following sections:

Overview

The Cisco AI Assistant is designed to optimize network management: reference documentation when needed, provide network insights, expediting troubleshooting, and empowering IT productivity. By leveraging AI-powered intelligence, recommendations, and insights, the AI Assistant helps streamline routine network operations, freeing up valuable time for more strategic work and innovation.

The Cisco AI Assistant is focused on enhancing three critical areas of network management:

- **Documentation Reference** - Answering questions about Cisco Business Dashboard and Cisco small business network devices, including Catalyst 1200/1300 series Switch, Cisco Business 250/350 Series Switch and Cisco Business 100/200 Series Access Points, and more.
- **Network Insight** - Gaining deeper visibility into network health and user experience with instant intelligence and summarized network data.
- **Troubleshooting** – Identifying anomalies and resolving network issues quickly to minimize downtime and help prevent major outages.

Prerequisites

Customers need to ensure they have met the following prerequisites to use the AI Assistant:

1. Both your browser and Cisco Business Dashboard Lite server must have internet access. Otherwise, the AI Assistant icon won’t appear.
2. You must have a Cisco Account, Google Account, or Apple Account to use the AI Assistant. Please refer to https://www.cisco.com/c/en/us/about/account.html for how to register a Cisco.com account.

Onboarding First-Time User

After opening the AI Assistant for the first time, a carousel window opens and you are introduced to the AI Assistant. You are presented with information on how the AI Assistant protects the privacy of your data, and a few tips on how to best use it.

In the carousel window, Click **Next** to the learn how the AI Assistant works with your data. We recommend that you read through this to understand how the AI Assistant treats your data and strives for transparency.

Clicking **Launch AI Assistant** opens the AI Assistant in a floating conversation window; You can select a response from one of our suggestion tiles or type in a question in the text box.

Cisco AI Assistant Components

The Cisco AI Assistant is engineered with user-friendly components.

- **Text Input Box -** At the bottom of the window, you have a text input box that allows you to type and engage with the AI Assistant.
- **New Thread -** Click the **edit** icon to start a new conversation with the AI Assistant
- **Chat History -** Expand the menu tray on the left side of the screen to see your chat history.
- **Feedback -** The AI Assistant has an option to provide feedback for its responses. Click thumbs up to show appreciation or thumbs down to let the assistant know that it can do better.
- **Logged-in User** - Display the Cisco.com account user’s name and provide logout option.
- **Change View -** Click on the view icon on the top right to open the AI Assistant in one of the 3 views: floating window, docked view or full screen view.

Guidelines for Crafting Prompts

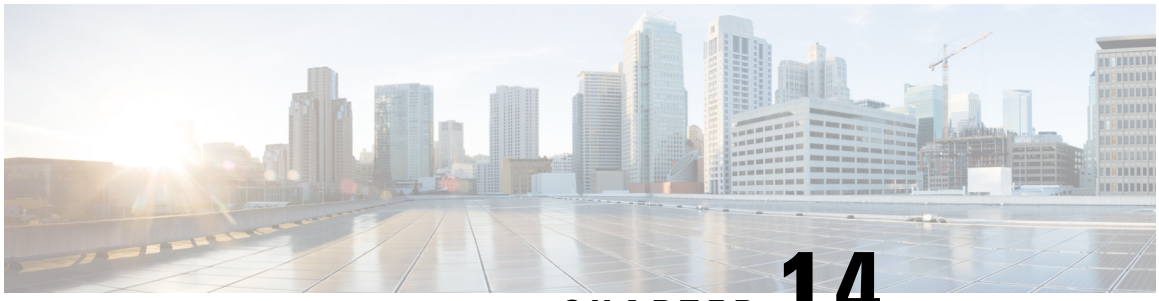
A prompt is a text input that you provide to the Cisco AI Assistant to initiate a conversation or request information. Essentially, it's the question you pose to the AI Assistant. The way you format and construct your prompt plays a crucial role in determining the response obtained from the AI Assistant.

Key Components of a Prompt

- **Clarity**: Be clear and specific about what you're asking for.
- **Context**: Provide necessary background information.
- **Purpose**: State what you want to achieve with your prompt.

  By providing precise input and context, you will significantly increase the chances of receiving a relevant answer from the AI Assistant.
- **Be Specific and provide context:** Draft your prompt with relevant information, use the correct device models, device names, etc. that could help the AI Assistant understand your request better.
- **Use Proper Syntax:** While the AI Assistant can understand colloquial language, clear and grammatically correct sentences can improve response accuracy.

- **Clarify the Desired Output:** If you have a preference for the response format (e.g., a list, a detailed explanation, tables), mention it.
- **Correction and Feedback:** If the response doesn't meet your expectations, you can provide feedback or ask for clarification within your next interaction.
- **Direct Naming Requests:** Use the phrase "give me only the names" to instruct the AI Assistant to provide solely names in its response. For example, if a user wants to know the names of devices without additional details, they can use the phrase 'give me only the names of devices' to instruct the AI Assistant to provide solely the names in its response.
- **Sequential Questioning:** For multiple inquiries, pose them as separate, follow-up questions to enhance clarity and context, rather than combining them into a single complex .
- **Explicit Multi-Attribute Queries:** Clearly state "Both" or "all of the following" when seeking multiple attributes; otherwise, the AI Assistant might select an attribute at random to respond to.



CHAPTER 14

FAQs

This chapter contains the following sections:

General FAQs

What languages are supported by the Cisco Business Dashboard Lite?

Cisco Business Dashboard Lite is translated into the following languages:

- Chinese
- English
- French
- German
- Japanese
- Portuguese
- Spanish

Discovery FAQs

What protocols does Cisco Business Dashboard Lite use to manage my devices?

Cisco Business Dashboard Lite uses a variety of protocols to discover and manage the network. Exactly which protocols are using for a particular device will vary between device types.

The protocols used include:

- Multicast DNS and DNS Service Discovery (aka *Bonjour*, see *RFCs 6762 & 6763*)
- Cisco Discovery Protocol (CDP)

- Link Layer Discovery Protocol (see *IEEE specification 802.1AB*)
- RESTCONF (See *https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/)*
- Proprietary web services APIs

How does Cisco Business Dashboard Lite discover my network?

The Cisco Business Dashboard Lite builds an initial list of devices in the network from listening to mDNS advertisements. The Cisco Business Dashboard Lite then connects to each device using a supported protocol and gathers additional information such as CDP & LLDP adjacency tables. This information is used to identify additional devices in the network, and the process repeats until all devices have been discovered.

Does Cisco Business Dashboard Lite do network scans?

The Cisco Business Dashboard Lite does not actively scan the broader network. You may explicitly search the IP address ranges for manageable devices. If this is done, then the dashboard will attempt to connect to webserver HTTPS ports on each IP address in the specified ranges to determine if a device is manageable.

Configuration FAQs

What happens when a new device is discovered? Will its configuration be changed?

If network configuration profiles have been enabled, then that configuration will be applied to newly discovered devices.

What happens when I disable a network configuration profile?

Configuration for the device will not change.

Security Consideration FAQs

What port ranges and protocols are required by Cisco Business Dashboard Lite?

The following table lists the protocols and ports used by Cisco Business Dashboard Lite:

Table 15: Cisco Business Dashboard Lite - Protocols and Ports

Port	Direction	Protocol	Usage
TCP 4443	Inbound	HTTPS	Secure web access to the Dashboard.
TCP 443	Outbound	HTTPS	Management of devices with secure web services enabled. Access Cisco web services for information such as software updates, support status, and end of life notices.
UDP 5353	Inbound/Outbound	mDNS	Multicast DNS service advertisements from the local network. Used for device discovery.

Port	Direction	Protocol	Usage
TCP 22	Outbound	SSH	CLI access to the device.
UDP 53	Outbound	DNS	Domain name resolution.

What Cisco servers does Cisco Business Dashboard Lite communicate with and why?

The following table lists the Cisco servers that Cisco Business Dashboard Lite communicates with, and the purpose of that conversation:

Table 16: Cisco Business Dashboard Lite - Cisco Servers

Hostname	Purpose
apix.cisco.com	Used to retrieve software update information and product lifecycle information. This server is only used if software updates or lifecycle reporting are enabled in **System > Privacy Settings**.
dl.cisco.com download-ssc.cisco.com softwarecloud.cisco.com	Used to download software update files from Cisco. These servers are only used if software updates are enabled in **System > Privacy Settings** and you execute an upgrade operation for a network device or for Cisco Business Dashboard Lite.
cloudsso.cisco.com id.cisco.com	Used to authenticate Cisco Business Dashboard Lite prior to communicating with apix.cisco.com. This server is only used if software updates or lifecycle reporting are enabled in **System > Privacy Settings**.
smb-ai.cbd-aws.com	Used by AI Assistant
*.firebaseio.com	Used to collect product improvement data. This server is only used if product improvement is enabled in **System > Privacy Settings.**

What processes are required by Cisco Business Dashboard Lite?

The following table lists the processes used by Cisco Business Dashboard Lite:

Table 17: Cisco Business Dashboard Lite - Processes

Process	Additional Details
Dashboard Essential Processes	
“<Install Directory>/jdk/bin/javaw.exe” … -jar “<Install Directory>/lib/launcher.jar”	The main Cisco Business Dashboard Lite server application
“<Install Directory>/jdk/bin/java.exe” … -jar “<Install Directory>/lib/cbdlite.jar”	Web Server

Process	Additional Details
Dashboard Essential Processes	
"<Install Directory>/mongodb/bin/mongod.exe" ……	Database services

Does Cisco Business Dashboard Lite have 'backdoor' access to my devices?

No. When Cisco Business Dashboard Lite discovers a supported device, it will attempt to access the device using credentials provided in **Administration** > **Device Credentials** page.

How secure are the credentials stored in Cisco Business Dashboard Lite?

Credentials for accessing Cisco Business Dashboard Lite are irreversibly hashed using the SHA512 algorithm. Credentials for devices are reversibly encrypted using the AES-128 algorithm.

How do I recover a lost password for the web UI?

If you have lost the password for all the admin accounts in the web UI, you can recover the password by logging on the server of the Dashboard Lite, open the Dashboard Lite Server Application, and click the **Tools > Recover Password** menu. This tool resets the password for the cisco account to the default of cisco, or, if the cisco account has been removed, it will recreate the account with the default password.