Cisco Business Dashboard and Probe Administration Guide, Version 2.8.0

First Published: 2022-11-14

Last Modified: 2023-09-07

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

Cisco Business Dashboard Overview

This chapter contains the following sections:

About Cisco Business Dashboard

Cisco Business Dashboard 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, routers, 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.

You can view the application by clicking Request a Demo

Cisco Business Dashboard is a distributed application which is comprised of two separate components or applications as described below:

The Dashboard

Cisco Business Dashboard also referred to as *the Dashboard*, is installed at a convenient location in the network. From the Dashboard user interface, you can get a high-level view of the status of all the sites in your network, or concentrate on a single site or device to see information specific to that site or device.

The Probe

Cisco Business Dashboard Probe also referred to as *the Probe* is installed at each site in the network and associated with the Dashboard. The probe performs network discovery and communicates directly with each managed device on behalf of the Dashboard.

Note Certain network devices support being directly associated with the Dashboard and managed without a probe being present. When network devices are being managed directly in this way, all management functions are available for the device, but the network discovery process may not be as comprehensive as when a probe is present.

Device Management Mode

Direct Managed

Certain devices can support direct association with the Dashboard and managed without a probe being present in the network.

In a direct managed network, you will need to connect the first device to the Cisco Business Dashboard manually. Then, this device reports information such as CDP, LLDP, and mDNS (aka Bonjour) to Dashboard. This information is used to identify additional devices in the network, Dashboard then connects these devices to itself automatically hence those devices become manageable, and the process repeats until all devices have been discovered. Depending on the size of your network, this process may take tens of minutes. You may optionally have the dashboard explicitly search the IP address ranges to discover network devices, which can be in other VLANs or subnets.

Direct managed network is recommended if all your devices support direct management.

Probe Managed

Probe is installed at each site in the network and associated with the Dashboard. The Probe performs network discovery and communicates directly with each managed device on behalf of the Dashboard.

A software Probe is a probe running in a virtual machine or on a Linux host. A software Probe can generally manage up to 50 network devices. Certain devices include the Probe application embedded in the device firmware. An embedded Probe can manage up to 15 network devices.

In one network you should only enable one Probe.

Audience

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

New Release Information and Updates

This section provides information on key new features and changes in Cisco Business Dashboard release 2.8.0 as of April 2024. For a full list of changes in this release, please consult the Release Notes. For details of the system requirements for Cisco Business Dashboard, please consult the Installation Guides.

Table 1: New features and changed behavior in Cisco Business Dashboard, Release 2.8.0

Feature	Description
Localization - Online Help	The web user interface supports the following languages: • Portuguese
Locate Device Action	A new action has been added to help locate the device by flashing its LED.
UX/UI Improvement	The device basic information panel, network basic information panel and port basic information panel have been updated with new UX/UI design.

Related Documents

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

- **Administration Guide (this document)**—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.
- **Device Support List**—This list provides details of the devices supported by Cisco Business Dashboard and the features available for each device type. For a list of all the devices supported by Cisco Business Dashboard, refer to the Cisco Business Dashboard - Device Support List.
- **Quick Start Guide**—This guide provides details on performing the initial setup for Cisco Business Dashboard using the most commonly selected options. For an overview of the basic tasks required for managing a network, refer the Cisco Business Dashboard Quick Start Guide .
- **Release Notes**— These are documents listing all the new features and fixes with each new Firmware Release. You will find them at Cisco Business Dashboard Release Notes.
- **Installation Guides**

  The following table lists all the installation guides of Cisco Business Dashboard software that can be deployed on different platforms.

  Refer to these guides for the System Requirements for Cisco Business Dashboard and Cisco Business Dashboard Probe.

Supported Platforms	Location
Amazon Web Services	Cisco Business Dashboard Installation Guide for Amazon Web Services(AWS)
Micorsoft Azure	Cisco Business Dashboard Installation Guide for Microsoft Azure
Oracle VirtualBox	Cisco Business Dashboard & Probe Installation Guide for Oracle VirtualBox
Microsoft Hyper-V	Cisco Business Dashboard Installation Guide for Microsoft Hyper-V
VMWare vSphere, Workstation and Fusion	Cisco Business Dashboard & Probe Installation Guide for VMWare

Supported Platforms	Location
Ubuntu Linux (Dashboard and Probe) and Raspbian Linux (Probe only)	Cisco Business Dashboard & Probe Installation Guide for Linux

Terminology

Term	Description
Hyper-V	A virtualization platform provided by Microsoft Corporation.
Open Virtualization Format (OVF)	A TAR archive containing one or more virtual machines in OVF format. It is a platform-independent method of packaging and distributing Virtual Machines (VMs).
Open Virtual Appliance or Application (OVA) file	Package that contains the following files used to describe a virtual machine and saved in a single archive using **.TAR** packaging: • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Raspberry Pi	A very low cost, single board computer developed by the Raspberry Pi Foundation. For more information, see *https://www.raspberrypi.org/*.
Raspberry Pi OS	Formally known as Raspbian, the Raspberry Pi OS is a Debian-based linux distribution optimized for the Raspberry Pi. For more information, see *https://www.raspberrypi.org/software/*.
VirtualBox	A virtualization platform provided by Oracle Corporation.
Virtual Hard Disk (VHD)	Virtual hard disk is a disk image file format for storing the complete contents of a hard drive.
Virtual Machine (VM)	A virtual computing environment in which a guest operating system and associated application software can run. Multiple VMs can operate on the same host system concurrently.
• VMWare ESXi • VMWare Fusion • vSphere Server • VMWare Workstation	A virtualization platform provided by VMWare Inc.

Term	Description
vSphere Client	User interface that enables users to connect remotely to vCenter Server or ESXi from any Windows PC. You can use the primary interface for vSphere Client to create, manage, and monitor VMs, their resources, and the hosts. It also provides console access to VMs.
Hypervisor	Also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.
Amazon Web Services (AWS)	An on-demand cloud computing platform.
Micosoft Azure Active Directory	A cloud-based identity and access management service that provides single sign-on and multi-factor authentication to help protect users from 99.9 percent of cybersecurity attacks.

CHAPTER 2

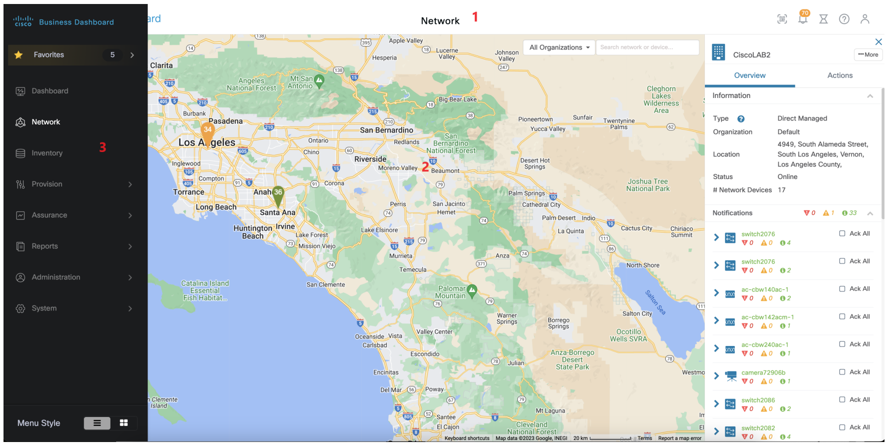
Using Cisco Business Dashboard and Probe

The section contains the following topics:

Using the Cisco Business Dashboard GUI

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

Home window



Type: Direct Managed
Organization: Default
Location: 4949, South Alameda Street, South Los Angeles, Vernon, Los Angeles County,
Status: Online
Network Devices: 17

Notifications: 0 1 33

- switch2076 0 0 4
- switch2076 0 0 2
- ac-cbw140ac-1 0 0 2
- ac-cbw142acm-1 0 0 1
- ac-cbw240ac-1 0 0 1
- camera72906b 0 0 1
- switch2086 0 0 2
- switch2082 0 0 4

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.
%	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 an overview of all of the locations in the network as either a map or a list. It also contains different views of each network and the devices discovered. The views include the network topology and a floor-plan 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, Network Configuration** and **Network Plug and Play**, 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. And **Device Integrity** which analyzes the integrity of your devices.
📄	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.

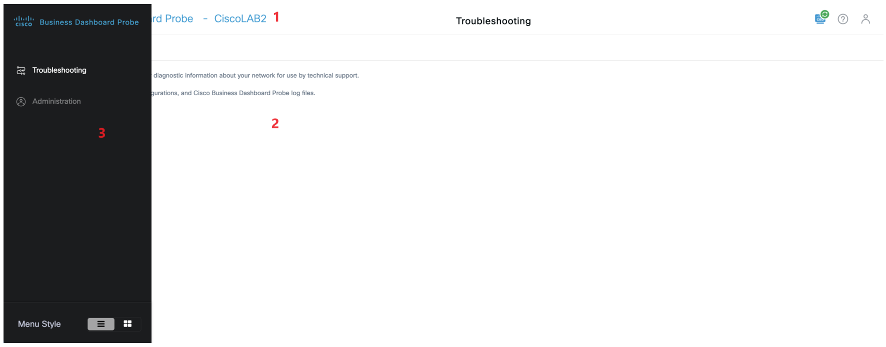
Header Toolbar Options

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 a **Language** and **Logout** option. Click on the username to display the user's profile page.
≡	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.
⌛	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, as well as any jobs that have been scheduled for a later date.
? ?	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**.

Using the Cisco Business Dashboard Probe GUI

When you log into the Cisco Business Dashboard Probe, the **Home** page appears.



diagnostic information about your network for use by technical support.

gurations, and Cisco Business Dashboard Probe log files.

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, feedback, context sensitive help, and version information.

The currently logged in user is displayed at the bottom of the navigation pane.

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 Probe 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 Probe features.

Icon	Name	Description
⇄	**Troubleshooting**	Click this to see the page that contains diagnostic tools that can help you identify problems with your network may be found under the **Troubleshooting** section.
⬡	**Administration**	The Administration page allows you to maintain the Cisco Business Dashboard Probe network application.

Header Bar Options

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

Icon	Option	Description
☰	**Menu button**	Located on the top left of the header—Click this button to display the navigation pane.
☁	**Dashboard Status**	This shows the status of the connection between Cisco Business Dashboard and the Probe. Click on this icon to open the Dashboard GUI.
? ?	**Support Center**	Click the **Support Center** icon to access the help information, virtual assistant, feedback and **About Cisco Business Dashboard Probe**. Click the **About Cisco Business Dashboard Probe** 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**.
👤	**Currently Logged In User**	The currently logged in user is displayed at the top of the navigation bar along with a **Language** and **Logout** option.

Upgrading Cisco Business Dashboard and Probe

From time to time, Cisco releases new versions and updates for Cisco Business Dashboard & Probe and posts them to the Software Center on cisco.com. Cisco Business Dashboard 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, or you can choose to download the update yourself and manually apply it.

To set up Dashboard to download and apply the update:

1. Click **About Cisco Business Dashboard** to open the pop-up. If any updates are available for the Dashboard or any associated Probes, they will be listed here.
2. If an update is available for the Dashboard, select the radio button next to that update and click **Upgrade**.

   The Dashboard will download and apply the update, and you may view the progress at any time on the **About Cisco Business Dashboard** pop-up. Once the update is complete, the Dashboard application will restart.

To apply a Dashboard update manually:

1. Download the Cisco Business Dashboard Linux 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.
2. Copy the installer file to the Dashboard file system.
3. Execute the installer using the Sudo command `sh <filename of installer>`. For example `sh cisco-business-dashboard-2.2-ubuntu-xenial-amd64.sh`. If necessary, enter your password at the sudo prompt. The Dashboard application will restart during this process.

You may also apply updates to all the Probes in the network from the Dashboard. You can update all Probes in parallel, or you can update Probes individually.

To update all Probes in parallel from the Dashboard:

1. Click **About Cisco Business Dashboard** to open the pop-up.

   If updates are available for the Dashboard or any of the associated Probes, they will be listed here.

   Note If an update is available for the Dashboard, perform that update before upgrading the probes.

   If you try to update the probes first, you will receive an error message.

2. Select the radio button next to the Probe update, and click **Upgrade**.
3. You may view the progress of the update in the user interface of the Probe.

To update an individual Probe from the Dashboard:

1. If an update is available for the Dashboard, perform that update before upgrading any probes.

   If you try to update a probe before updating the Dashboard, you will receive an error message.

2. Select **Network** in the navigation.
3. Select the network to be updated in either the **Map View** or the **List View**.
4. In the **Basic Info** panel for the network, select the **Actions** tab.
5. Click **Upgrade**.

   You may view the progress of the update in the job center.

Note When using an embedded probe running on a network device, you should consult the documentation for that device to perform an update. Some devices do not support the updating of the Probe application independently of the device firmware.

Note When Cisco Business Dashboard running in Amazon Web Services (AWS) or Microsoft Azure is being upgraded from release 2.4.1(or below) to release 2.5.0(or above), the AWS/Azure security policies should be manually updated to allow incoming UDP traffic to port 1812.

Upgrading Cisco Business Dashboard or Probe Operating System

Cisco Business Dashboard & Probe versions up to and including version 2.7.x run on the Ubuntu Linux distribution version 20.04 (Focal Fossa).

Future versions of Cisco Business Dashboard will be supported with Ubuntu 22.04 (Jammy Jellyfish) only. As a result, upgrading an existing Cisco Business Dashboard or Probe installation beyond the 2.7.x will require an updated operating system.

Due to the extensive changes between Ubuntu 20.04 and 22.04, separate installers are provided for different operating system versions of Cisco Business Dashboard & Probe. It is not possible to perform an in-place upgrade of the operating system on an existing dashboard or probe installation. The following sections address the recommended approaches for updating the operating system for the dashboard and probe.

Upgrading the Cisco Business Dashboard Operating System

To upgrade an existing Cisco Business Dashboard to a new version of the operating system, use the following process:

1. Make a backup of the existing Cisco Business Dashboard application.
   a. Log on to the dashboard GUI and from the Navigation pane open **System** > **Backup**.
   b. Enter a password to protect the backup in the fields on the screen, and click the **Backup & Download** button.
2. Create a new instance of Cisco Business Dashboard running on the updated operating system.

- If the existing dashboard is running in virtual machine or in a cloud provider such as Amazon Web Services, you should shut down the existing instance, and then create a new instance using the prebuilt Cisco Business Dashboard images.
- If the existing dashboard is installed directly on an Ubuntu Linux installation running on a server, then you should re-image the server with the updated Ubuntu version, and then install Cisco Business Dashboard.

For more information on installing Cisco Business Dashboard, refer the installation guides found at *https://cisco.com/go/cbd-docs*.

3. Log on to the new instance of Cisco Business Dashboard and restore the backup you created in step 1.
   - Navigate to **System** > **Restore**.
   - Enter the password used to protect the backup in the field provided.
   - Click the **Upload & Restore** button to upload the backup file.

4. Once the restore process has completed and you have confirmed that the new instance is running correctly, delete the old instance.

   For more information on the backup and restore process, see Backing Up and Restoring the Dashboard Configuration, on page 99 later in this guide.

Note A Cisco Business Dashboard backup file can be restored to a system running the same version as the system you just backed up, or up to one newer minor release. For example, a backup taken from a system running version 2.2.0 may be restored to a system running 2.3.1, but not to a system running 2.4.0.

Note When Cisco Business Dashboard is upgraded from release 2.4.1(or below) to release 2.5.0(or above) while running in Amazon Web Services (AWS) or Microsoft Azure, the security policies should be updated to allow incoming UDP traffic to port 1812.

Upgrading the Cisco Business Dashboard Probe Operating System

The Cisco Business Dashboard Probe stores very little configuration data and no long-term statistics. As a result, when upgrading the operating system hosting a probe, Cisco recommends that you remove the existing probe instance and install a new probe instance running on the new operating system. The new probe is then associated with Cisco Business Dashboard, and the existing network record selected during the association process.

For more information on installing the Cisco Business Dashboard Probe software, refer the installation guides located at Cisco Business Dashboard Installation Documents. For more information on associating a probe with Cisco Business Dashboard, refer to the Quick Start Guide located at Cisco Business Quick Start Guide.

Note When using an embedded probe or direct device management, there is no requirement to upgrade the probe or agent separately from the device operating system. The probe/agent is included in the device firmware and is updated automatically when upgrading the device.

CHAPTER 3

Dashboard

This chapter contains the following sections:

About the Dashboard

The **Dashboard** page in the Cisco Business Dashboard 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.
Wireless Clients by SSID	Displays the number of devices associated with the selected wireless network.
Wireless Clients by Device	Displays the number of devices associated with the selected wireless access point.
Wireless Top Ten	Displays the top ten wireless networks, access points, or clients based on traffic or client count.
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.

Controls on each of the widgets allows the data shown to be customized. The organization drop-down at the top right of the Dashboard may be used to restrict the information displayed to a specific organization.

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.

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:

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

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:

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

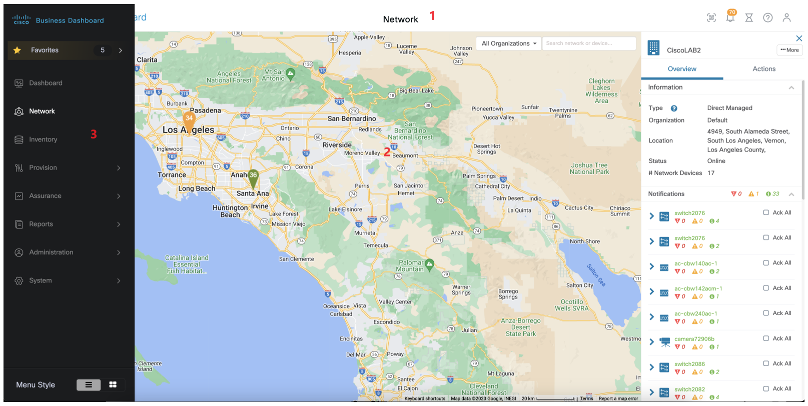
The section contains the following topics:

- About Network, on page 19
- About Network Details Panel, on page 21
- Overview of the Topology Map and Tools, on page 22
- Viewing Basic Device Information, on page 26
- Performing Device Actions, on page 27
- Accessing the Device Administration Interface, on page 29
- Viewing Detailed Device Information, on page 29
- Using Floor Plans, on page 32

About Network

Access the Network page to see an overview of the location and all the devices in your network. You can also note other networks and devices nearby. You can select the network and then see more details about that network and devices and how they are all working.

The **Network** page provides an overview of the network as either a geographic map showing the location and status of each site in the network, or as a list of all sites.



Type	Direct Managed
Organization	Default
Location	4949, South Alameda Street, South Los Angeles, Vernon, Los Angeles County,
Status	Online
# Network Devices	17

Notifications: 0, 1, 33

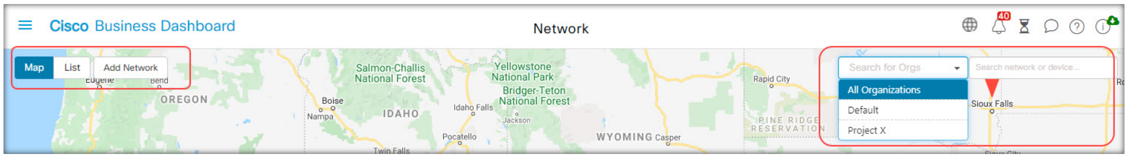
Device			
switch2076	0	0	4
switch2076	0	0	2
ac-cbw140ac-1	0	0	2
ac-cbw142acm-1	0	0	1
ac-cbw240ac-1	0	0	1
camera72906b	0	0	1
switch2086	0	0	2
switch2082	0	0	4

In the **Map View**, the number displayed on each network icon indicates the number of outstanding notifications that exist for that site, and the color of the icon indicates the highest severity level outstanding.

Note When two or more network icons are positioned too closely on the map to be easily distinguished, they will be replaced with a single cluster icon. Click on the cluster icon to automatically zoom the map to a level where the networks in that cluster can be separated.

The **Network Map** offers the following controls:

You can also click and drag anywhere in the map area to move the map in the **Work** pane.



Control Name	Control Action
Map/List selection	Use this control to chose to view networks on a map or in a table.
Add Network button	Use this button to create a new network record prior to deployment.
Organization drop-down	Select an individual organization from the drop-down list to limit the networks displayed.
Search box	Enter all or part of the name, address or IP address of a network to locate that network on the map. Alternatively, you can enter all or part of the name, IP address, serial number or MAC address of a device to identify the network where the device is located. As you type, a list of matches is displayed. • Hover over a match and the corresponding network will be highlighted. • Select a match and the corresponding network will be selected and centered in the view.
Zoom controls	Use these controls to zoom in and out of the map. Click the (**+**) plus sign to zoom in and the (**−**) minus sign to zoom out.
Fit-to-view button	This button automatically zooms out the map so that all the network markers can be displayed.

In the **List View**, the same information can be seen in the last column of the table. To see more information about a network, click on the network icon or on the table row for that site.

In the **List View**, the following controls are available:

Control Name	Control Action
Map/List selection	Use this control to chose to view networks on a map or in a table.
Column Select icon	This icon allows you to select the columns to be displayed. You can click on the column headings to sort the table.
Add Network	Click the (**+**) plus sign to add a new network prior to deploying a probe for that network.

Control Name	Control Action
Refresh	Click the refresh button to update the table and display the most current information.
Organization drop-down	Select an individual organization from the drop-down list to limit the networks that are displayed.
Search box	Enter all or part of the name, address or IP address of a network to list only matching networks in the table.

Click on a network icon or row to bring up the **Basic Info** panel for that network. The **Basic Info** panel contains the following information:

- The name of the network.
- The organization the network belongs to.
- The physical address of the network.
- The Probe IP address for the network and the IP subnet(s) discovered at the network.
- The software version of the Probe.
- The connection status.
- The number of managed devices in this network.
- A list of all current, unacknowledged notifications for this network.
- A list of events that occurred for this network in the previous 24 hours.

You can also carry out the following actions for a network from the **Basic Info** panel:

- Click **Details** to view a detailed information about the network including the network topology and floor plans.
- See the section "About Network Detail" below for more information on the **Network Detail** panel.
- Click on the **Actions** tab to display additional actions available for the network.
  - Click **Remove** to delete this network and all associated data from the dashboard.
  - Click **Upgrade** to update the Probe software at this network.
  - Click **Show Tech** to generate a Network Show Tech archive for this network.
  - Other 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.

About Network Details Panel

The **Network Detail** panel allows you to view and update information specific to that network. This information includes:

- Key network parameters including the network name, type, description, organization and default device group.

- The location of the network.
- Logging configuration for the Probe in this network. See Managing Probe Log Settings, on page 126.
- Controls that allow you to restrict the devices discovered and managed by Cisco Business Dashboard based on IP address, device type and whether the device is manufactured by Cisco. If any device types are selected, then non-network device types are implicitly excluded from discovery.
- Select **Topology** to display a logical topology of all the discovered devices in the network. Information about each device is displayed, and you can perform actions on selected Cisco products.
- Select **Floor Plan** to document and display the physical location of your network devices within your environment.

Overview of the Topology Map and Tools

About the Topology Map

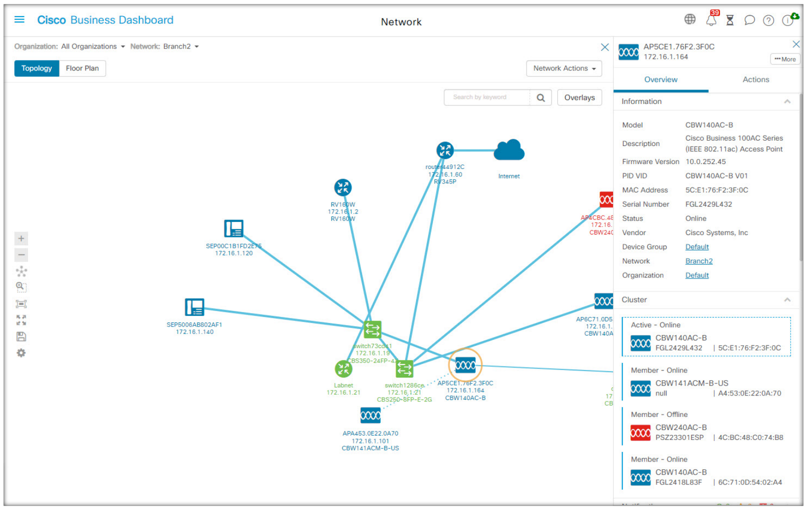
Cisco Business Dashboard looks for discovered devices for network connectivity details and then builds a graphical representation or topology from the information it gathered. The data collected includes:

- CDP & LLDP neighbor information
- MAC Address tables
- Associated Device tables from Cisco Business switches
- Routers
- Wireless Access Points

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 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.

Click **Overlays** in the **Topology Map** to display the **Overlays & Filters** panel. This panel allows 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.



AP5CE1.76F2.3F0C
172.16.1.164

Information

Model	CBW140AC-B
Description	Cisco Business 100AC Series (IEEE 802.11ac) Access Point
Firmware Version	10.0.252.45
PID VID	CBW140AC-B V01
MAC Address	5C:E1:76:F2:3F:0C
Serial Number	FGL2429L432
Status	Online
Vendor	Cisco Systems, Inc
Device Group	Default
Network	Branch2
Organization	Default

Cluster

Active - Online
CBW140AC-B
FGL2429L432 | 5C:E1:76:F2:3F:0C

Member - Online
CBW141ACM-B-US
null | A4:53:0E:22:0A:70

Member - Offline
CBW240AC-B
PSZ23301ESP | 4C:BC:48:C0:74:B8

Member - Online
CBW140AC-B
FGL2418L83F | 6C:71:0D:54:02:A4

Accessing the Topology Map

To access the **Topology Map**:

1. Open the **Network** panel from the **Navigation** pane.
2. Click the icon or table row for the network you are interested in.

The **Topology** for that network 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 re-enable automatic layout of the topology after it has been disabled by manual changes. 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 and drag **Zoom by selection** to select an area to zoom in on.

Icon	Description
⛶	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 the labels displayed for the topology icons.

Topology Icons

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

Icon	Description
∞	**Access Point**
☁	**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. The thickness of the link represents the speed of the link, with a thin line representing 100Mbps or below and a thick line representing 1Gbps or above. A dashed line represents a wireless connection.
●	**Router**
⇆	**Switch**
🖥	**Host** - A host attached to the network using a wired connection.

Icon	Description
🖥	**Wireless Host** - A host attached to the network using a wireless connection.

Overlays & Filters Panel

This panel appears on the right of the **Topology** map when **Overlays** is clicked. It is at the top-right 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. • **L2 Path Trace** shows the layer 2 path traffic between the two selected devices takes through the network. Select the device by typing the hostname, MAC address or IP address in the fields provided, or shift-click on two devices in the topology map.
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.

Item	Description
Show Discovery: • **Both** • **Blocked** • **Enabled**	Use the radio button to control whether you wish to see devices found by the dashboard that are blocked for management.

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.

Step 1 In the **Network** page, select a network and click **Details** to display the topology.

Step 2 In the Topology map, click on a network device such as a switch or a router to view the details.

Step 3 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.
CBD Agent Status	The CBD agent status for the device, only available for devices that support direct management.
Domain	The domain name of the device.
Vendor	The manufacturer of the device.
Network	The name of the network where the device is located.
Organization	The organization to which the device belongs.

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
Service Panel	Lists the network services identified on the device.
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.

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:

Step 1 On the **Topology Map** or **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 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 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.
Delete	Remove an offline device from the Topology and Inventory.
Disconnect	Force a direct managed device to disconnect from the dashboard. This action should be used with caution as direct access to the device is required to reconnect the device after it has been disconnected with this action.

Connect	Connect a disconnected direct managed device to dashboard.
Show Tech	Execute the device's Show Tech function and retrieve the resulting file through the dashboard. This action will typically only be used at the request of technical support.
Locate Device	Locate the device by flashing its LED.

Step 3 Device actions may optionally be scheduled to take place at a later time. To schedule a device action, click the **Schedule** button and fill out the form to create a new **Schedule Profile**. For more information on Scheduling Profiles see Managing Schedule Profiles, on page 121.

Accessing the Device Administration Interface

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

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 access the administration interface.

Step 2 In the **Basic Info** panel, click **Open Device GUI icon** at the upper right corner. A new window will open in your browser showing the device administration interface

Note When you access the administration interface by clicking **Open Device GUI icon**, your browser will connect to the device through the Dashboard. This means that if you are accessing the network remotely, only the Dashboard needs to be directly reachable from outside the site.

Because these connections all go through the same host - the Dashboard - cookies for one device will be presented to other devices, and may be updated by other devices if the name is the same. A common symptom of this is the browser session on the first device will be immediately logged out after connecting to a second device because the session cookie has been updated.

Viewing Detailed Device Information

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
- **PnP**—Allows you to manage the Network Plug and Play settings for 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.

- **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 where the current configuration does not match the desired configuration.

- **CBD Agent**—Managing the logging configuration for the CBD Agent on a direct managed device.

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.
CBD Agent	The CBD agent status for the device, only available for devices that support direct management.
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.

Item Name	Description
Network	The network that this device belongs to.
Organization	The organization that this device belongs to.
Device Group	Click **Edit** next to the device group to change the group the device belongs to. Click **Save** to save the changes.
Monitoring Profile	Click **Edit** next to the monitoring profile to select a monitoring profile to use for this device. Alternatively, the monitoring profile may be inherited from the device group this device belongs to. Click **Save** to save the changes.
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 Click **PnP** to view the settings to be applied to the device using Network Plug and Play.

Step 7 Use the form to make changes, then click **Save** to apply the changes.

Step 8 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 9 Click **WLAN** to manage the radio settings and view the Wireless LANs configured on this device.

Step 10 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 11 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 2: 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.

Item	Description
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 12 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.

Step 13 For direct managed devices, click **CBD Agent** to manage the log settings associated with the dashboard connection. Typically this page will only be used at the direction of a support engineer, but more information on these settings may be found in the section titled Managing Probe Log Settings. To retrieve the log files from the device, you can click the **Download Log File** button here, or access the device administration UI directly and download the files using the steps specific to that device.

Using Floor Plans

The Floor Plan view allows you to keep track of the physical locations of your network equipment. You may upload a plan for each floor in the building(s) and position each of the network devices on the plan. This helps you to easily locate devices if maintenance is required. The Floor Plan is similar in operation to the Topology Map, and devices placed on the Floor Plan may be operated in the same way as devices in the Topology Map.

Creating a New Floor Plan

1. Navigate to **Network Details Panel** and click **Floor Plan**. If an existing floor plan is displayed, click the **Home** icon at the top left of the floor plan.

2. If the building you wish to add a floor plan to has already been created, go to the next step. Otherwise, enter a name for the building that houses the floor into the **New Building** field. Click the **save** icon.

3. Drag and drop an image file containing the floor plan onto the target area for the new floor, or click on the target area to specify a file to upload. Supported image formats are `png, gif,` and `jpg`. Image files can be a maximum of 500KB in size.

4. Enter a name for the floor into the **New Floor** field. Click the **save** icon.

5. Repeat steps 2 to 4 for each building and floor with network devices.

Placing Network Devices on a Floor Plan

1. Navigate to **Network Details Panel** and click **Floor Plan**. If the floor plan you are interested in is not already displayed, then click on the floor plan.
2. Click **Add Devices**, and then use the search box at the bottom left to find the device you wish to place. You may search by hostname, device type, or IP address. As you type, matching devices will be displayed below the search box. Gray icons represent devices that have already been placed on a floor plan.
3. Click and drag a device to add it to the floor plan in the correct location. If you select a device that has already been placed on another floor plan, it will be removed and added to this one.
4. Repeat steps 2 & 3 until all devices have been added to the floor plan.

Removing a Device from the Floor Plan

1. Navigate to **Network Details Panel** and click **Floor Plan**. If the floor plan you are interested in is not already displayed, then click on the floor plan.
2. Identify the device you wish to remove and click to select it.
3. Click on the red cross that is displayed to remove the device from the floor plan.

Changing the Floor Plan

1. Navigate to **Network Details Panel** and click **Floor Plan**. If an existing floor plan is displayed, click the **Home** icon at the top left of the floor plan.
2. To change a building name, click the **edit** icon next to the name. Once the changes are complete, click the **save** icon.
3. To change a floor plan, click the **edit** icon next to the floor plan name. You may change the floor plan by dragging a new image file to the target area, or clicking on the target area to upload a new file from your PC. You may also change the name of the floor plan. Once the changes are complete, click the **save** icon.

Removing a Floor Plan

1. Navigate to **Network Details Panel** and click **Floor Plan**. If an existing floor plan is displayed, click the **Home** icon at the top left of the floor plan
2. Identify the floor plan you wish to remove, and click the **delete** icon at the top right corner of the image target area.
3. If you wish to remove an entire building containing all the floor plans, click the **delete** icon next to the building name.

CHAPTER 5

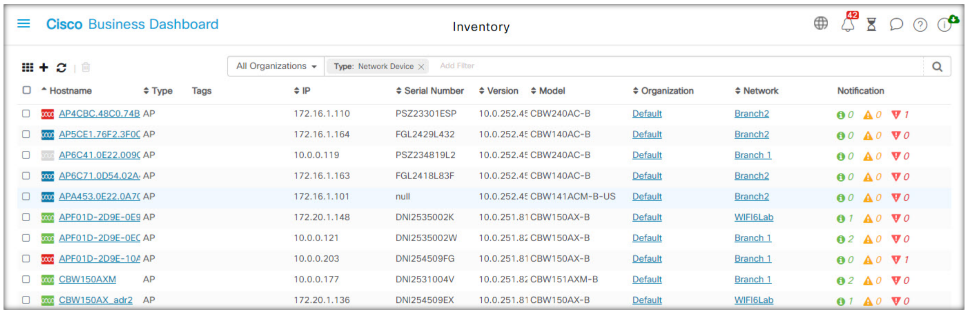
Inventory

The section contains the following topics:

- Viewing Device Inventory, on page 35

Viewing Device Inventory

Access this page to view, monitor and support all of the devices and 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:



☐	Hostname	Type	Tags	IP	Serial Number	Version	Model	Organization	Network	Notification
☐	AP4CBC.48C0.74B	AP		172.16.1.110	PSZ23301ESP	10.0.252.45	CBW240AC-B	Default	Branch2	ℹ 0 ⚠ 0 ▼ 1
☐	AP5CE1.76F2.3F0C	AP		172.16.1.164	FGL2429L432	10.0.252.45	CBW140AC-B	Default	Branch2	ℹ 0 ⚠ 0 ▼ 0
☐	AP6C41.0E22.009C	AP		10.0.0.119	PSZ234819L2	10.0.252.45	CBW240AC-B	Default	Branch 1	ℹ 0 ⚠ 0 ▼ 0
☐	AP6C71.0D54.02A	AP		172.16.1.163	FGL2418L83F	10.0.252.45	CBW140AC-B	Default	Branch2	ℹ 0 ⚠ 0 ▼ 0
☐	APA453.0E22.0A7C	AP		172.16.1.101	null	10.0.252.45	CBW141ACM-B-US	Default	Branch2	ℹ 0 ⚠ 0 ▼ 0
☐	APF01D-2D9E-0E9	AP		172.20.1.148	DNI2535002K	10.0.251.81	CBW150AX-B	Default	WIFI6Lab	ℹ 1 ⚠ 0 ▼ 0
☐	APF01D-2D9E-0EC	AP		10.0.0.121	DNI2535002W	10.0.251.82	CBW150AX-B	Default	Branch 1	ℹ 2 ⚠ 0 ▼ 0
☐	APF01D-2D9E-10A	AP		10.0.0.203	DNI254509FG	10.0.251.81	CBW150AX-B	Default	Branch 1	ℹ 0 ⚠ 0 ▼ 1
☐	CBW150AXM	AP		10.0.0.177	DNI2531004V	10.0.251.82	CBW151AXM-B	Default	Branch 1	ℹ 2 ⚠ 0 ▼ 0
☐	CBW150AX_adr2	AP		172.20.1.136	DNI254509EX	10.0.251.81	CBW150AX-B	Default	WIFI6Lab	ℹ 1 ⚠ 0 ▼ 0

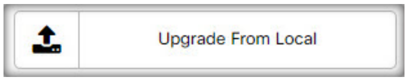
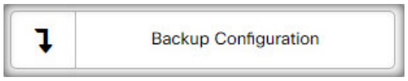
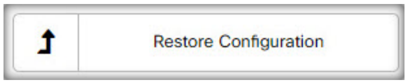
Table 3: Inventory Details

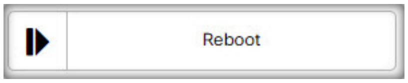
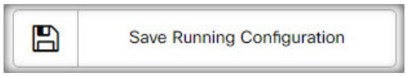
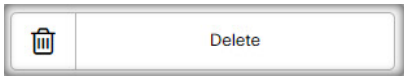
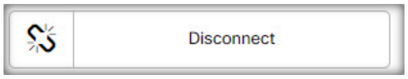
Item	Description
Hostname	Displays the name of the device.
Type	The type of device such as a switch, router or wireless access point (WAP).
Tags	Lists any tags associated with the device.
IP	The Internet Protocol (IP) addresses of the device.
MAC (hidden by default)	The Media Access Control (MAC) address 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.

Item	Description
Serial Number	The serial number for the device.
Version	The current firmware version of the device.
Vendor (hidden by default)	The vendor that manufactured the device.
Model	Model name of the device.
CBD Agent Status	The CBD agent status for the device, is only available for devices that support direct management.
Organization	The organization the device belongs to.
Network	The network to which the device belongs
Notification	A count of the outstanding notifications for the device
PnP Status (hidden by default)	The current Network Plug and Play status for the device. For more information, see the **Network Plug and Play** pages.

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
- **Add** icon—Click the (✚) plus icon to add new devices to the inventory prior to the device being discovered. When manually adding a device to the inventory you can provide basic information about the device including identity information, organization and device group, and PnP settings. Providing this information ahead of time ensures the device will be correctly managed when it is connected to the network
- **Refresh** button—Click this button to update the table to show the latest available information
- **Actions** buttons—The following action buttons allow you to perform actions on one or more selected devices

	Upgrade Firmware To Latest
	**Upgrade From Local**
	**Backup Configuration**
	**Restore Configuration**

	**Reboot**
	**Save Running Configuration**
	**Delete**
	**Disconnect**

Action buttons are only displayed when one or more devices supporting actions are selected.

Note For more details on these actions, see Performing Device Actions

CHAPTER 6

Provision

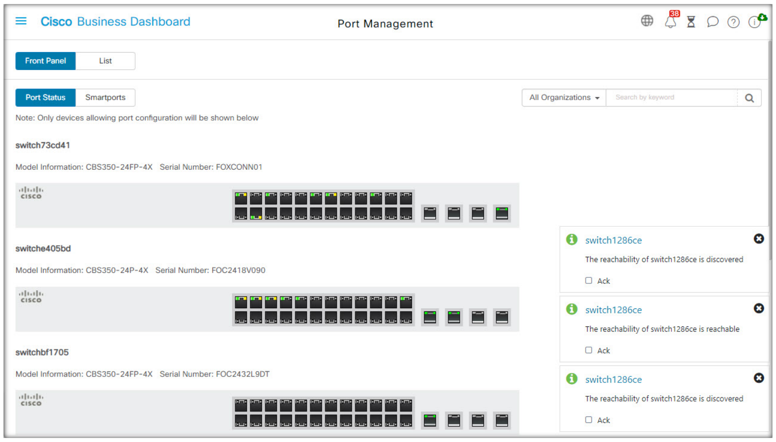
The section contains the following topics:

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.



Note: Only devices allowing port configuration will be shown below

switch73cd41

Model Information: CBS350-24FP-4X Serial Number: FOXCONN01

switche405bd

Model Information: CBS350-24P-4X Serial Number: FOC2418V090

switchbf1705

Model Information: CBS350-24FP-4X Serial Number: FOC2432L9DT

switch1286ce

The reachability of switch1286ce is discovered

☐ Ack

switch1286ce

The reachability of switch1286ce is reachable

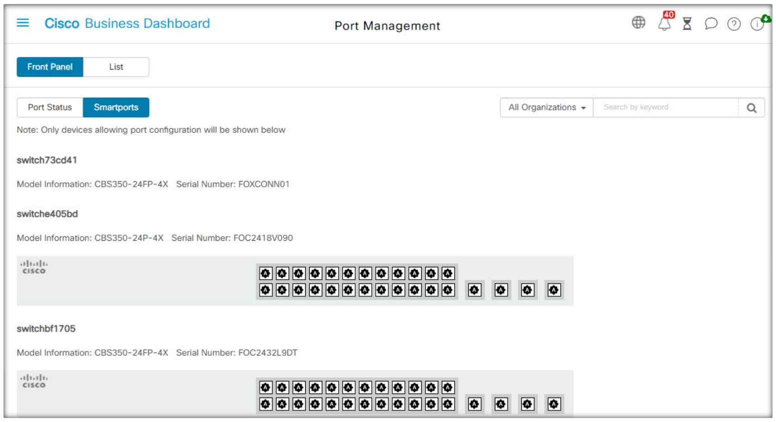
☐ Ack

switch1286ce

The reachability of switch1286ce is discovered

☐ Ack

The **Smartports** view allows you to see the current Smartports role for each port, and to change the role. Each port is overlaid with an icon indicating the current role:



Note: Only devices allowing port configuration will be shown below

switch73cd41

Model Information: CBS350-24FP-4X Serial Number: FOXCONN01

switche405bd

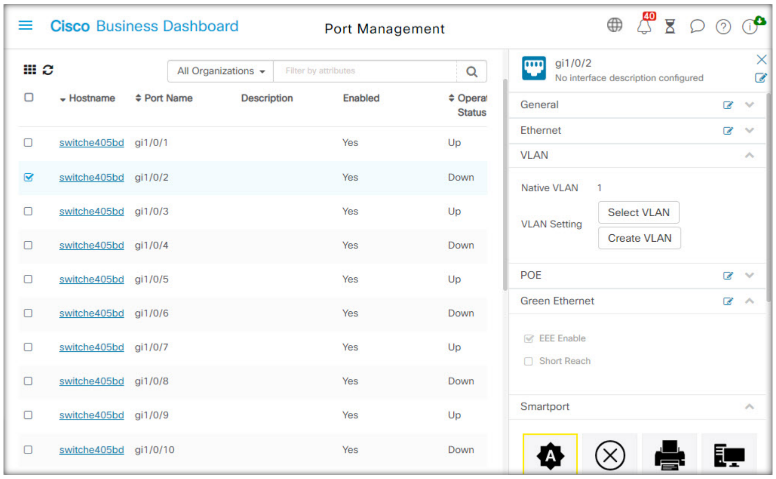
Model Information: CBS350-24P-4X Serial Number: FOC2418V090

switchbf1705

Model Information: CBS350-24FP-4X Serial Number: FOC2432L9DT

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:



☐	Hostname	Port Name	Description	Enabled	Operat Status
☐	switche405bd	gi1/0/1		Yes	Up
☑	switche405bd	gi1/0/2		Yes	Down
☐	switche405bd	gi1/0/3		Yes	Up
☐	switche405bd	gi1/0/4		Yes	Down
☐	switche405bd	gi1/0/5		Yes	Up
☐	switche405bd	gi1/0/6		Yes	Down
☐	switche405bd	gi1/0/7		Yes	Up
☐	switche405bd	gi1/0/8		Yes	Down
☐	switche405bd	gi1/0/9		Yes	Up
☐	switche405bd	gi1/0/10		Yes	Down

gi1/0/2
No interface description configured

Native VLAN 1

VLAN Setting

☑ EEE Enable

☐ Short Reach

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
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 assigned to the device. If no authentication servers are defined, Cisco Business Dashboard will be used as the default authentication server.
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
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 section contains the following topics:

About Network Configuration

The **Network Configuration** pages allow you to define various configuration parameters that typically apply to some or all devices in the network. These parameters include configuration such as time settings, domain name services, administrator authentication, and Virtual LANs and Wireless LANs. You can create configuration profiles for each of these areas separately, or you can use the wizard to create profiles for each area in a single workflow. The configuration profiles are applied to one or more device groups, and then pushed out to the devices.

Using the Wizard

Use the wizard to create configuration profiles for each of the Network Configuration elements, and assign those profiles to one or more device groups in a single workflow.

1. Navigate to **Provision > Network Configuration** > **Wizard**.
2. In the **Device Group Selection** screen, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured.
3. Click **Next**. In each of the screens that follow, select the configuration as required. For more details on these parameters, see the following sections.
4. Complete the configuration settings on each screen and click **Next**. If you do not wish to configure settings on a particular screen for this profile, click **Skip**.
5. Click **Back** to visit the previous screens or you may click the headings on the left.
6. Complete the configuration and review the settings on the final screen. Click **Finish** to apply the configuration to the selected devices.

Configuring 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 creating, modifying and deleting the Time Settings configuration profile.

Create a Time Management Configuration Profile

1. Navigate to **Provision > Network Configuration** > **Time Management**.
2. Click the ✚(plus) icon to add a new profile.
3. On the **Device Group Selection** section, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured.
4. In the **Time Setting** section, select an appropriate timezone from the drop-down list.
5. 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.
6. 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.
7. Click **Save**.

Modify a Time Management Configuration Profile

1. Select the radio button next to the profile to be changed, and click the **edit** icon.
2. Make the required changes to the profile settings and click **Update**.

Remove a Time Management Configuration Profile

1. Select the radio button next to the profile which needs to be removed.
2. Click the **delete** icon.

Configuring 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.

Create a DNS Resolver Configuration Profile

1. Navigate to **Provision > Network Configuration** > **DNS Resolvers**.
2. Click the ✚(plus) icon to add a new profile.
3. On the **Device Group Selection** section, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured.
4. Specify the domain name for the network.

5. Specify at least one DNS server address.

6. Click **Save**.

Modify a DNS Resolver Configuration Profile

1. Select the radio button next to the profile to be changed, and click the **edit** icon.

2. Make the required changes to the profile settings and click **Update**.

Remove a DNS Resolver Configuration Profile

1. Select the radio button next to the profile to be removed.

2. Click the **delete** icon.

Configuring 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 based on users. The following sections provide instructions on creating, modifying and deleting the authentication configuration profile.

Create an Authentication Configuration Profile

1. Navigate to **Provision** > **Network Configuration** > **Authentication**.

2. Click the ✚(plus) icon to add a new profile.

3. On the **Device Group Selection** section, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured.

4. Optionally, specify one or more username and password combinations for local user authentication. Additional users may be added by clicking the ✚ (plus) icon.

5. You may also choose to require the use of complex passwords.

6. Optionally specify one or more RADIUS servers to use for authentication. You can check the checkbox to enable the use of Cisco Business Dashboard for authentication.

7. Click **Save**.

Note Users requiring network access must be granted the Network Access permission. See Users, on page 84 for more information.

Note When using Cisco Business Dashboard for network access authentication, it is strongly recommended that the dashboard have a certificate signed by a public certificate authority. If this is not done, most client devices will present a certificate warning to the user, and some clients will not proceed with authentication at all.

Modify an Authentication Configuration Profile

1. Select the radio button next to the profile to be changed, and click the **edit** icon.
2. Make the required changes to the profile settings and click **Update**.

Remove an Authentication Configuration Profile

1. Select the radio button next to the profile which needs to be removed.
2. Click the **delete** icon.

Configuring 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 also displayed on this page in a separate table. The following sections provide instructions on creating, modifying and deleting Virtual LAN configuration profiles.

Create a Virtual LAN

1. Navigate to **Provision > Network Configuration** > **Virtual LANs**.
2. Click the ✚(plus) icon to add a new VLAN.
3. On the **Device Group Selection** section, enter a profile name for this configuration, choose an organization and select one or more device groups to be configured.
4. 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.
5. You may create multiple VLANs using a single profile. If you want to create additional VLANs in this profile, click **Add Another** and go back to step 4.
6. Click **Save**. The new VLAN will be created on all VLAN-capable devices in the selected groups.

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

Modify a VLAN

1. Check the radio button next to the VLAN to be changed, and click the **edit** icon.
2. Make the required changes to the VLAN settings and click **Update**.

Remove a VLAN

Check the radio button next to the VLAN to be removed, and click the **delete** icon.

Remove a VLAN not created by Cisco Business Dashboard

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.

Configuring 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 also displayed in a separate table. The following sections provide you instructions on creating, modifying and deleting Wireless LAN configuration profiles.

Create a Wireless LAN

1. Navigate to **Provision** > **Network Configuration**>**Wireless LANs**.
2. Click the ✚(plus) icon to add a new Wireless LAN profile.
3. On the **Device Group Selection** section, enter a profile name, choose an organization and select one or more device groups to be configured.
4. Click the ✚(plus) icon to add a new SSID.
5. 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 1-4095, and if it does not already exist in the network, a new VLAN will be created automatically.
6. Select the type of security required.

   If you select **Guest** as the security type, you then need to specify the type of authentication to be used with the guest portal. The options include Username/Password, Web Consent, and Email Address. More information on these options can be found in Configuring Guest Portals, on page 47.

   Note SSIDs with a security setting of Guest will only be applied to CBWxxx access points.

   If you select an **Enterprise** security type, then make sure to assign an authentication profile to the device containing the preferred RADIUS server(s) to use. If one has not been defined for this device, the Cisco Business Dashboard will be used by default.
7. Optionally, click to expand the Advanced Settings to change the **Broadcast**, **Application Visibility**, **Local Profiling** and **Radio** settings to match your requirements.
8. Click **Save** to continue or **Cancel** to discard your changes.
9. You can create multiple Wireless LANs using a single profile. If you want to create additional Wireless LANs in this profile, go back to step 4.
10. Click **Save**. The new WLAN will be created on all devices with wireless access point capabilities in the selected groups.

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

Modify a Wireless LAN

1. Check the radio button next to the Wireless LAN to be changed, and click the **edit** icon.
2. Make the required changes to the Wireless LAN settings and click **Update**.

Remove a Wireless LAN

Select the radio button next to the Wireless LANs to be removed, and then click the **delete** icon.

Note If a Virtual LAN was created automatically when creating the Wireless LAN, the Virtual LAN will not be deleted when the Wireless LAN is deleted. The Virtual LAN may be deleted on the **Virtual LANs** page.

Remove a Wireless LAN Not Created By Cisco Business Dashboard

In the table of discovered Wireless LANs, click the radio button for the Wireless LAN to be removed and then click the **delete** icon. In some cases, a WLAN may not be able to be deleted from certain devices. In these cases, it will be necessary to make changes to the device configuration directly.

Configuring Wireless Radios

The Wireless Radios page allows you to manage radio frequency (RF) optimization across the wireless networks in your environment. A Wireless Radio profile allows you to control whether the access points should automatically adjust their wireless radio settings to suit the environment, as well as enabling the detection and reporting of rogue access points and interferers.

The following sections provide you instructions on creating, modifying and deleting Wireless Radio profiles.

Create a Wireless Radio Profile

1. Navigate to **Provision > Network Configuration** > **Wireless Radios**.
2. Click the ✚(plus) icon to add a new Wireless Radio profile.
3. On the Device Group Selection section complete the following:
    - Enter a profile name for this configuration.
    - choose an organization.
    - Select one or more device groups to be configured.
4. Choose whether automatic RF Optimization should be performed by the access points in the network. If you enable RF Optimization, be sure to select appropriate values for Client Density and Traffic Type.
5. Optionally enable the detection of rogue access points.
6. Optionally enable the detection of interferers.
7. Click **Save**.

    The new Wireless Optimization settings will be applied to all wireless access points with RF optimization capabilities in the selected groups.

Modify a Wireless Radio Profile

1. Check the radio button next to the Wireless Radio Profile to be changed and click the edit icon.
2. Make the required changes to the RF optimization settings and click Update

Remove a Wireless Radio Profile

1. Select the radio button next to the Wireless Radio Profile to be removed, and then click the delete icon.

Configuring Guest Portals

The Guest Portals page allows you to centrally manage the web page presented to a guest user when connecting to a guest wireless network. Cisco Business Dashboard hosts a single guest portal for each organization, and each portal may be individually customized to represent the identity of the organization.

The guest portals support multiple methods of authenticating the user, and the same portal can present a different authentication method on different networks. The authentication methods supported are:

- Username/Password – Each guest user must be defined ahead of time in the dashboard and assigned a username and password. The username and password must then be entered into the guest portal when connecting to the wireless network.
- Web Consent – The guest user is presented with the organization’s Acceptable Use Policy and must accept the policy in order to access the network.
- Email Address – The guest user is prompted to provide an email address prior to gaining access to the network. The email address is recorded as the username for the client and may be seen in the wireless client report and the device user interface.

The appearance of each guest portal may be customized by changing all of the text fields including the font used, modifying colors, and updating the background and logo images.

To customize a guest portal, do the following:

1. Navigate to **Provision > Network Configuration > Guest Portals**.
2. Select the radio button for the guest portal to be customized and click the edit icon
3. Use the form presented to update the appearance of the captive portal. You may modify any of the text fields, upload new images to use as background and logo, and modify the colors and font used.

   The guest portal has slightly different content depending on the authentication method chosen. Select the tabs at the bottom of the page to update the fields for the different versions of the portal.

   You may view your changes before saving them by clicking the Preview button on each of the different authentication methods. To restore the portal to the default appearance, click the Reset to defaults button at the top right.
4. Click **Update** to save your changes or **Cancel** to discard them.

Network Plug and Play

The section contains the following topics:

About Network Plug and Play

Network Plug and Play is a service that works in conjunction with Network Plug and Play enabled devices to allow firmware and configuration to be managed centrally, and to allow zero-touch deployment of new network devices. Devices may be deployed directly using the Network Plug and Play protocol, or indirectly if discovered by a probe that is associated with the Dashboard.

When installed, a Network Plug and Play enabled device will identify the Network Plug and Play server through one of manual configuration, DHCP, DNS, or the Plug and Play Connect service. The following sections provide more detail on the configuration of the Network Plug and Play service in Cisco Business Dashboard.

Network Requirements

A Network Plug and Play device will automatically find the address of the Network Plug and Play server using one of the following methods below. Each method will be attempted in turn until an address is found or all methods have failed. The methods used are, in order:

- **Manual configuration**—A Network Plug and Play enabled device can be manually configured with the address of the server through the administration interface
- **DHCP**—The address of the server can be supplied to the device in the Vendor-specific Information option
- **DNS**—If the DHCP Vendor-specific Information option has not been provided, then the device will perform a DNS lookup for the server using a well-known hostname
- **Plug and Play Connect Service**—If no other method has been successful, the device will attempt to contact the Plug and Play Connect service. This service will then redirect the device to your server.

Once the device has identified the server, it will contact the server and update firmware and configuration as specified by the server.

Certificate Requirements

When establishing a connection to a Network Plug and Play server, the client checks to ensure the certificate presented by the server is valid and can be trusted. For the certificate to be acceptable and the connection to proceed, the certificate must meet the following conditions:

- The certificate must be signed by a trusted Certificate Authority (CA), or the certificate itself must be trusted by the client. A certificate downloaded from the TrustpoolBundleURL learned from DHCP, or from the Plug and Play Connect service is trusted by the client
- If the server identity is discovered using manual configuration, DHCP or Plug and Play Connect, and is an IP address, then either the **Common Name** field or the **Subject-Alt-Name** field must contain that IP address
- If the server identity is discovered using manual configuration, DHCP or Plug and Play Connect, and is a hostname, then either the **Common Name** field or the **Subject-Alt-Name** field must contain that hostname
- If the server identity is discovered using DNS discovery, then either the **Common Name** field or the **Subject-Alt-Name** field must contain the IP address corresponding to the well-known hostname pnpserver.<*local domain*>

Note Some of the older Network Plug and Play client implementations do not verify the presence of the server identity in the certificate.

Setting up Discovery using DHCP

To discover the server address using DHCP, the device will send a DHCP discover message with option 60 that contains the string “ciscopnp”. The DHCP server must send a response containing the Vendor-specific Information option (option 43). The device extracts the server address from this option and uses this address to contact the server. An example of an option 43 string containing the address of a Network Plug and Play server is “5A1N;B2;K4;I172.19.45.222;J80”.

The option 43 string has the following components, delimited by semicolons:

- 5A1N—Specifies the DHCP sub-option for Plug and Play, active operation, version 1, no debug information. It is not necessary to change this part of the string.
- B2—IP address type:
  - B1 = hostname
  - B2 = IPv4
- K4—Transport protocol to be used between the Cisco Plug and Play Agent and the server:
  - K4 = HTTP (default)
  - K5 = HTTPS
- Ixxx.xxx.xxx.xxx—IP address or hostname of the server (following a capital letter i). In this example, the IP address is 172.19.45.222.
- Jxxxx—Port number to use to connect to the server. In this example, the port number is 80. The default is port 80 for HTTP and port 443 for HTTPS.
- T*trustpoolBundleURL*—Optional parameter that specifies the external URL of the trustpool bundle if it is to be retrieved from a different location than the server. For example, to download the bundle from a TFTP server at 10.30.30.10, you would specify the parameter like this: Ttftp://10.30.30.10/ca.p7b
- If you are using trustpool security and you do not specify the T parameter, the device retrieves the trustpool bundle from the server.
- Zxxx.xxx.xxx.xxx;—IP address of the NTP server. This parameter is mandatory when using trustpool security to ensure that all devices are synchronized.

Consult the documentation for your DHCP server for details on how to configure DHCP options.

Setting up Discovery using DNS

If DHCP discovery fails to get the IP address of the server, the device falls back to a DNS lookup method. Based on the network domain name returned by the DHCP server, the device constructs a fully qualified domain name (FQDN) for the server, using the preset hostname “pnpserver”.

For example, if the DHCP server returns the domain name “example.com”, the device constructs the FQDN “pnpserver.example.com”. It then uses the local name server to resolve the IP address for this FQDN.

Setting up Discovery using Plug and Play Connect

Plug and Play Connect is a Cisco-provided service that is the last resort used by a Network Plug and Play-enabled device to discover the server. To use Plug and Play Connect for server discovery, you must first create a Controller Profile representing the PnP server, and then register each of your devices with the Plug and Play Connect Service.

Accessing the Plug and Play Connect Service

To access the Plug and Play Connect Service, do the following:

1. In your web browser, navigate to *https://software.cisco.com*
2. Click the **Log In** button at the top right of the screen. Log in with a cisco.com ID associated with your Cisco Smart Account.
3. Select the **Plug and Play Connect** link under the **Network Plug and Play** heading. The main page for the **Plug and Play Connect** service is displayed.

Creating a Controller Profile

To create a Controller Profile for the PnP server, do the following:

1. Open the Plug and Play Connect web page in your browser. If necessary, select the correct Virtual Account to use.
2. Select the Controller Profiles link, and then click the Add Profile button.
3. Select a Controller Type of PNP SERVER from the drop-down list. Then click Next.
4. Specify a name, and optionally a description for the profile.
5. Under the heading for Primary Controller, use the drop-down provided to select whether to specify the server by name or IP address. Fill in the name or addresses of the server in the fields provided.
6. Select the protocol to use when communicating with the server. It is strongly recommended that HTTPS be used to ensure the integrity of the provisioning process.
7. If the protocol selected is HTTPS, the certificate used by the server should be uploaded using the controls provided. See Managing Certificates, on page 92 for details on downloading the certificate from Cisco Business Dashboard.
8. Optionally specify a Secondary Controller.
9. Click **Next**, and review the settings before clicking **Submit**.

Registering Devices

Certain products purchased directly from Cisco may be associated with your Cisco Smart Account at the time of order, and these will automatically be added to Plug and Play Connect. However, the majority of Cisco Business Plug and Play-enabled products will need to be registered manually. To register devices with Plug and Play Connect, do the following:

1. Open the Plug and Play Connect web page in your browser. If necessary, select the correct Virtual Account to use it.

2. Select the **Devices** link, and then click **Add Devices**. You may need to be approved to manually add devices to your account. This is a one-time process, and, if it is required, you will be notified by email once approval has been granted.
3. Choose whether to add devices manually, or to add multiple devices by uploading details in CSV format. Click the link provided to download a sample CSV file. If you choose to upload a CSV file, click the **Browse** button to select the file.
4. Click **Next**.
5. If you selected to add devices manually, click **Identify Device**. Specify the Serial Number and Product ID for the device to be added. Select a Controller Profile from the drop-down. Optionally enter a description for this device.
6. Repeat step 4 until you have added all your devices, then click **Next**.
7. Review the devices you have added, and then click **Submit**.

Configuring the Network Plug and Play Service

There are several tasks that you need to perform when setting up the Network Plug and Play service for your environment. These include uploading configurations and images, adding and configuring devices to use Network Plug and Play, and managing devices that connect to the service when they have not previously been registered with the service. The following sections describe these tasks in detail.

Using the Network Plug and Play Dashboard

The **Network Plug and Play** Dashboard provides an overview of the devices currently being provisioned using Network Plug and Play.

Three charts are displayed showing the device status broken down by:

- Device group
- PnP enabled device
- Devices that are not defined in the Cisco Business Dashboard inventory (unclaimed devices)

Each chart shows the number of devices or groups in each of the states listed. You can click on the state heading on any of the charts to see a detailed list of devices or groups that fall into that category. The following table provides a breakdown of the different statuses:

Table 4: Network Plug and Play Dashboard – Status Definitions

Status	Description
Groups	
Pre-provisioned	Device groups with PnP-enabled devices in the Pending state only.
In Progress	Device groups with some PnP-enabled devices in the Pending state and some in the Provisioning or Provisioned state.
Provisioned	Device groups where all PnP-enabled devices are in the Provisioned state.

Status	Description
Error	Device groups with one or more PnP-enabled devices in the Error state.
Enabled Devices	
Pending	Devices in the inventory that have been enabled for PnP, but have not yet contacted the PnP server.
Provisioning	Devices that have contacted the PnP server and begun provisioning but have not completed the provisioning process.
Provisioned	Devices that have been successfully provisioned using PnP.
Error	Devices where the PnP provisioning process has failed.
Unclaimed Devices	
Unclaimed	Devices that have contacted the PnP server but are not defined in the inventory.
Ignored	Unclaimed devices that have been explicitly ignored by the user.

You can restrict the data displayed to a specific organization using the organization drop-down at the top right of the page. When viewing device groups, type all or part of a group name in the search box to limit the groups displayed in the table. Or you can enter a device name, product ID or serial number in the search box when viewing provisioning rules to display the current status of an individual device.

Note The chart for unclaimed devices is only displayed to **Administrators** who are viewing data for **All Organizations**.

Managing Enabled Devices

Enabled Devices are devices in the inventory that have been configured for provisioning with an image or configuration file, or were previously discovered by Cisco Business Dashboard and have attempted to connect using the Network Plug and Play protocol. An Enabled Device that has been configured with an image or configuration file will have that image and/or configuration applied to the device at the next opportunity. If the device is connected to and managed by the Dashboard, the changes will be applied immediately. Otherwise, the changes will be applied the next time the device is connected - either via a probe or direct management, or when it checks in using the Network Plug and Play protocol. An Enabled Device may also be set to apply changes during the next change window, in which case the changes will be delayed until the next change window after the device checks in.

To create a new Enabled Device, follow the steps below.

1. Navigate to **Provision > Network Plug and Play** >**Enabled Devices**.
2. Click the ✚(plus) icon to add a new enabled device to the inventory.

Note You may also click the upload icon to add devices in bulk using a csv file. Template csv files may be downloaded from the **Provision > Network Plug and Play > Configurations** page by opening the configuration template to be used for the devices and selecting **Download CSV Template** from the **Actions** dropdown.

3. Fill out the **Add New Device** form with the requested parameters, including identifying details for the device, the organization, network and device group it should belong to, then click **Next**.

4. Optionally, select a firmware image to be applied to the device. If you choose **Default** for the image, the device will use the image that is designated as the default for the product ID at the time the device connects to the server.

Note You may use the checkbox on this page to delay the provisioning of the new device until the next change window. However, this is rarely appropriate when creating a new device, as a new device is not usually an active part of the network until after provisioning is complete.

5. Optionally, select a configuration to be applied to the device, along with the version of the configuration if there is more than one version. If the configuration is a template containing placeholders, a form will be displayed prompting for the values that should be used for this device. Complete these fields as necessary. If the template makes use of parameters defined by the system, click on the checkbox to display the values that will be used.

6. Click **Next** to proceed to the **Summary** screen. Review the data entered to ensure it is correct. You can also review the final device configuration in the preview window at the bottom. When you are satisfied, click **Finish**.

To edit an existing device, follow the steps below.

1. Navigate to **Provision > Network Plug and Play**>**Enabled Devices**.
2. Check the checkbox for the device to be modified and click **Edit**. Alternatively, you can click the name of the device.
3. Click **Next** to display the **Provision Device** screen. Change the image and/or configuration file if required and make any changes to the parameter values associated with the configuration. Optionally, check the checkbox to ensure that changes will be applied during the change window.
4. Click **Next** to proceed to the **Summary** screen. Review the data entered to ensure it is correct. You can also review the final device configuration in the preview window at the bottom. When you are satisfied, click **Finish**.

Note If the image or configuration file settings are changed for a device that has already been provisioned, that device's state will reset to pending, and the device will be re-provisioned.

To remove an Enabled Device, follow the steps below.

1. Navigate to **Provision > Network Plug and Play** >**Enabled Devices**.
2. Check one or more checkboxes for the devices to be removed and click the **delete** icon.

Note If an Enabled Device is deleted when that device is otherwise known to the Dashboard and the device is online, only the image and configuration files settings for that device will be removed. The device will remain in the inventory similar to any other managed device. If a device subsequently connects to the Dashboard using PnP, a new entry will be added to the Enabled Devices table.

Unclaimed Devices

Note The **Unclaimed Devices** page is only available to Administrators.

An unclaimed device is one that has connected to the service, but there is no device record in the inventory that matches the device. To see a list of unclaimed devices, and to claim an unclaimed device so it can be managed using Network Plug and Play, follow the steps below.

1. Navigate to **Provision > Network Plug and Play** >**Unclaimed Devices** and select the **Unclaimed** tab.
2. Click the claim button for the device to be managed.
3. Fill out the Unclaimed Device form with the requested parameters, including the organization, network and device group it should belong to, then click **Next**.
4. Optionally, select a firmware image to be applied to the device. If you choose **Default** for the image, the device will use the image that is designated as the default for the product ID at the time the device connects to the server.
5. Alternatively, select a configuration to be applied to the device, along with the version of the configuration if there is more than one version. If the configuration is a template containing placeholders, a form will be displayed prompting for the values that should be used for this device. Complete these fields as necessary.

   If the template makes use of parameters defined by the system, you can check the checkbox to display the values that will be used.
6. Click **Next** to proceed to the **Summary** screen. Review the data entered to ensure it is correct. You can also review the final device configuration in the preview window at the bottom. When you are satisfied, click **Finish**.

To remove a device from the Unclaimed list without provisioning it, follow the steps below.

1. Navigate to **Provision > Network Plug and Play**>**Unclaimed Devices** and select the **Unclaimed** tab.
2. Click **Ignore** for the device you wish to remove from the list.

The devices will be moved to the **Ignored** list and no further action will be taken. To reclaim an ignored device, follow the steps below.

1. Navigate to **Provision > Network Plug and Play**>**Unclaimed Devices** and select the **Ignored** tab.
2. Click the **Unignore** button for the device to be reclaimed.

The devices will be moved to the **Unclaimed** list, and you can claim the devices as described above.

Auto Claiming Devices

Note The **Auto Claim** page is only available to Administrators.

Unclaimed devices can be automatically claimed and provisioned by the server by creating an Auto Claim rule for that product ID. To create an Auto Claim rule, follow the steps below.

1. Navigate to **Provision > Network Plug and Play**>**Auto Claim Devices**.
2. Click the ✚(plus) icon to create a new **Auto Claim** rule.
3. Fill out the Auto Claim Device form with the requested parameters, including the Product ID (PID) to be matched, and the organization, network, and device group the newly claimed device should belong to, then click **Next**.
4. Optionally, select a firmware image to be applied to the device. If you choose **Default** for the image, the device will use the image that is designated as the default for the product ID at the time the device connects to the server.
5. Alternatively, select a configuration to be applied to the device, along with the version of the configuration if there is more than one version. If the configuration is a template containing placeholders, a form will be displayed prompting for the values that should be used for this device. Complete these fields as necessary.

   If the template makes use of parameters defined by the system, you can check the checkbox to display the values that will be used.
6. Click **Next** to proceed to the **Summary** screen. Review the data entered to ensure it is correct. You can also review the final device configuration in the preview window at the bottom. When you are satisfied, click **Finish**.

New devices that are not present in the inventory will be compared against the list of Auto Claim rules. If there is a match, a new device record will be created in the inventory with the image and configuration file defined by the **Auto Claim** rule. The device will then be provisioned accordingly. If the device does not match an **Auto Claim** rule, it will be added to the Unclaimed list and no further action will be taken.

Device Firmware Images

The **Images** page allows you to upload firmware images that can then be deployed to the devices.

Firmware images can be designated as the default image for different platforms, allowing you to update the firmware across an entire family of devices very easily. Firmware images are specific to an organization and can only be used for provisioning devices associated with the same organization.

To upload a firmware image, follow the steps below.

1. Navigate to **Provision > Network Plug and Play** > **Images**.
2. Click the ✚(plus) icon.
3. Select the organization for the image from the dropdown.
4. Drag a firmware image from your PC and drop it on the target area of the **Upload File** window. Alternatively, click the target area and select a firmware image to upload.
5. Click **Upload**.

You can change the filename or designate an image as the default image for one or more device types. To modify the filename or designate an image as a default image, follow the steps below.

1. Navigate to **Provision > Network Plug and Play** >**Images**.
2. Select the radio button for the image in the **Images** table and click **edit**.
3. If desired, modify the filename of the image using the textbox provided.
4. Optionally enter a comma-separated list of product IDs into the **Default Image for Product IDs** field. Product IDs can contain the wildcard characters '?', representing a single character, and '*', representing a string of characters.
5. Click **Save**.

To remove an image, follow the steps below.

1. Navigate to **Provision > Network Plug and Play** >**Images**.
2. Select the radio button for the image to be deleted and click **delete**.

Device Configuration Files

The Configurations page allows you to upload or create configuration files that can then be deployed to the devices. Configuration files are specific to an organization and can only be used for provisioning devices associated with the same organization.

Configuration files can be simple text files, or can contain placeholders and associated metadata to allow the same configuration file to be used with multiple devices, while still allowing for unique parameters to be set on a device by device basis. For example, a single configuration template could be applied to multiple devices, but allow the hostname to be specified individually for each device.

Several configuration templates are included with the Dashboard application as system templates and are available to all organizations. These templates allow commonly changed settings to be modified, and can be used as is, or copied and used as a basis for new templates. For more information on the syntax of the configuration templates, See *Appendix A: Managing Configuration Templates*.

To create a new configuration manually, follow the steps below.

1. Navigate to **Provision > Network Plug and Play**>**Configurations**.
2. Click the ✚(plus) icon.
3. The template editor opens with a blank area for the configuration on the left, and a form on the right for managing the metadata associated with the template.

   Enter a name for the configuration in the field at the top left. Select an organization and enter a comma-separated list of product IDs that support this configuration in the fields on the right. Optionally, enter a description. Product IDs can contain the wildcard characters '?', representing a single character, and '*', representing a string of characters.
4. Create the configuration by typing or pasting text into the text area on the left. If necessary, make the appropriate changes to the metadata using the controls on the right.

   You can use the **Preview** button to see how the configuration template will appear when it is assigned to a device.
5. When you are satisfied with the configuration, click **Save**.

To upload a configuration file, follow the steps below.

1. Navigate to **Provision > Network Plug and Play** >**Configurations**.
2. Click the **Upload** icon.
3. Select the organization for the configuration from the dropdown. Specify a name for the configuration and optionally add a description.
4. Drag a configuration file from your PC and drop it on the target area of the **Upload File** window. Alternatively, click the target area and select a configuration file to upload.
5. Click **Upload**.

You can click on the filename of the uploaded configuration file to view the contents in the template editor, if you wish.

To remove a configuration, follow the steps below.

1. Navigate to **Provision > Network Plug and Play** >**Configurations**.
2. Check one or more checkboxes for the configurations to be removed and click the **delete** icon.

Managing Settings

The Network Plug and Play Settings page allows you to control the operation of the Network Plug and Play Protocol.

The **Check In Time Interval** controls how frequently a device will connect to the Network Plug and Play service after initial provisioning. To modify this parameter, follow the steps below.

1. Navigate to **Provision > Network Plug and Play**>**Settings**.
2. Enter the desired interval between connections in the field provided. The time is in minutes, and the default is 2880 minutes, or two days.
3. Click **Save**.

The **Check In Time Interval** is set for the system as a whole, but can be overridden at the organization level. If no interval is set for the organization, then the system value is used.

Configuring the Certificate

The certificate automatically generated by Cisco Business Dashboard during first startup is a self-signed certificate. In most cases, this will not be sufficient for the certificate to be accepted by the Network Plug and Play client, and it will be necessary to generate a new certificate. When generating a new self-signed certificate or certificate signing request (CSR), the Dashboard will include the contents of the **Common Name** field in the **Subject Alternative Name** field in addition to any values specified in the **Subject Alternative Name** field on the GUI.

For more information on configuring the Dashboard’s certificate, see Managing Certificates, on page 92.

Monitoring Network Plug and Play

Each device known to the Network Plug and Play service is shown on either the **Enabled Devices** page or the **Unclaimed Devices** page with a status displayed. This status can also be viewed on the **Inventory** page by enabling the display of the **PnP Status** column. The status field shows the current state of the device, and will contain one of the values as listed in the following table. By clicking on the status field, you can see more detail, including a history of the state changes for this device over time.

Table 5: Network Plug and Play - Device Status

Status	Description
Pending	Device is defined but has not made contact with the service.
Provisioning	The device has made the initial connection to the service.
Provisioning_Image	A firmware image is being applied by the device.
Provisioned _Image_Rebooting	The device is rebooting to run the new firmware.
Provisioned_Image	New firmware has been applied successfully.
Provisioning_Config	A configuration file is being applied to the device.
Provisioned_Config	The configuration file has been successfully applied to the device. Depending on the type of device, it can reboot to apply the configuration.
Error	An error has occurred. Check log files for more details.
Provisioned	The provisioning process for the device is complete.

CHAPTER 7

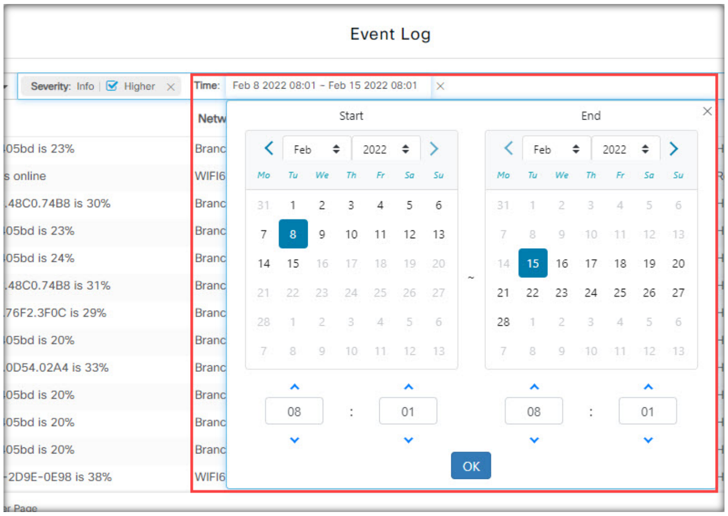
Assurance

The section contains the following topics:

About the 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.

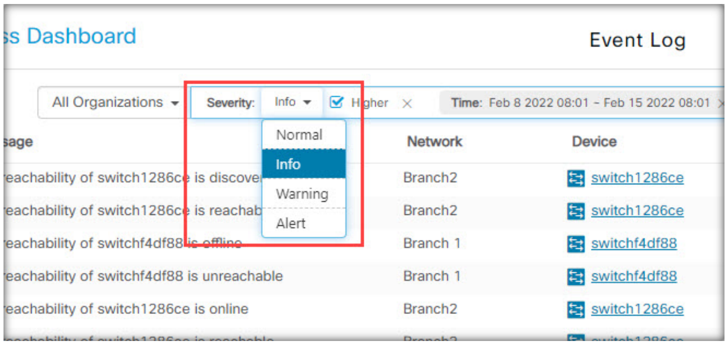


Event Log

Severity: Info | ☑ Higher

Time: Feb 8 2022 08:01 ~ Feb 15 2022 08:01

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.



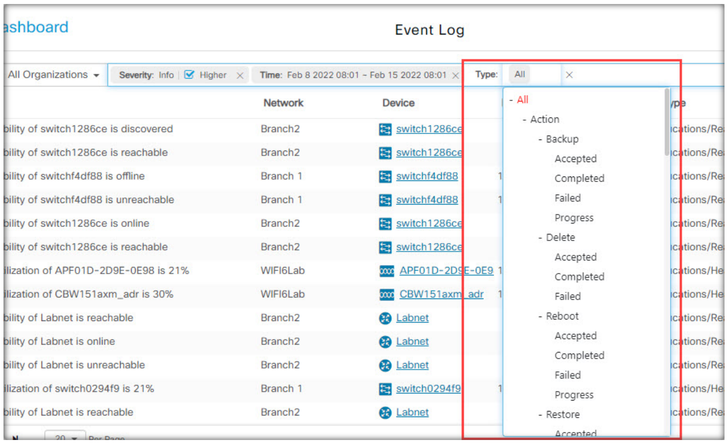
ss Dashboard

Event Log

All Organizations ▾ | Severity: Info ▾ ☑ Higher × | Time: Feb 8 2022 08:01 – Feb 15 2022 08:01 ×

sage	Network	Device
eachability of switch1286ce is discove	Branch2	switch1286ce
eachability of switch1286ce is reachab	Branch2	switch1286ce
eachability of switchf4df88 is offline	Branch 1	switchf4df88
eachability of switchf4df88 is unreachable	Branch 1	switchf4df88
eachability of switch1286ce is online	Branch2	switch1286ce

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.



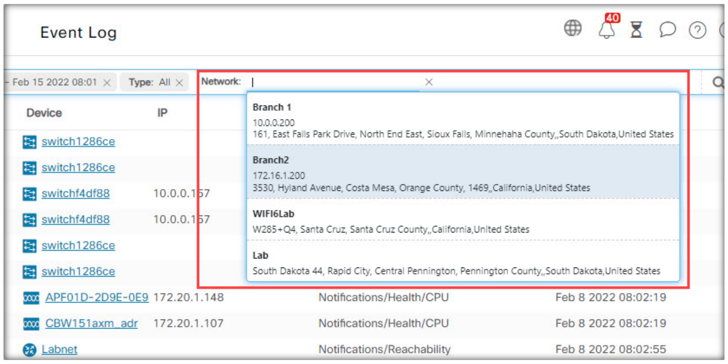
ashboard

Event Log

All Organizations ▾ | Severity: Info ☑ Higher × | Time: Feb 8 2022 08:01 – Feb 15 2022 08:01 × | Type: All ×

	Network	Device		ype
bility of switch1286ce is discovered	Branch2	switch1286ce		ications/Re
bility of switch1286ce is reachable	Branch2	switch1286ce		ications/Re
bility of switchf4df88 is offline	Branch 1	switchf4df88	1	ications/Re
bility of switchf4df88 is unreachable	Branch 1	switchf4df88	1	ications/Re
bility of switch1286ce is online	Branch2	switch1286ce		ications/Re
bility of switch1286ce is reachable	Branch2	switch1286ce		ications/Re
ilization of APF01D-2D9E-0E98 is 21%	WIFI6Lab	APF01D-2D9E-0E9	1	ications/He
ilization of CBW151axm_adr is 30%	WIFI6Lab	CBW151axm_adr	1	ications/He
bility of Labnet is reachable	Branch2	Labnet		ications/Re
bility of Labnet is online	Branch2	Labnet		ications/Re
bility of Labnet is unreachable	Branch2	Labnet		ications/Re
ilization of switch0294f9 is 21%	Branch 1	switch0294f9	1	ications/He
bility of Labnet is reachable	Branch2	Labnet		ications/Re

Use the **Network**filter to display events by one or more networks. As you type, matching sites will be displayed.



Event Log

- Feb 15 2022 08:01 × | Type: All × | Network: |

Branch 1
10.0.0.200
161, East Falls Park Drive, North End East, Sioux Falls, Minnehaha County,,South Dakota,United States

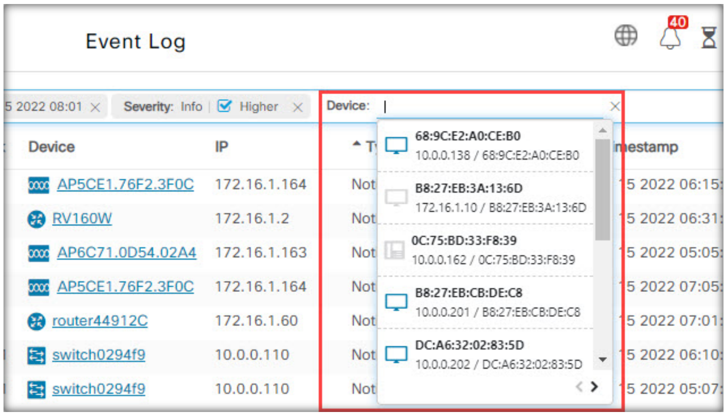
Branch2
172.16.1.200
3530, Hyland Avenue, Costa Mesa, Orange County, 1469,,California,United States

WIFI6Lab
W285+Q4, Santa Cruz, Santa Cruz County,,California,United States

Lab
South Dakota 44, Rapid City, Central Pennington, Pennington County,,South Dakota,United States

Device	IP		
switch1286ce			
switch1286ce			
switchf4df88	10.0.0.157		
switchf4df88	10.0.0.157		
switch1286ce			
switch1286ce			
APF01D-2D9E-0E9	172.20.1.148	Notifications/Health/CPU	Feb 8 2022 08:02:19
CBW151axm_adr	172.20.1.107	Notifications/Health/CPU	Feb 8 2022 08:02:19
Labnet		Notifications/Reachability	Feb 8 2022 08:02:55

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.



Event Log

5 2022 08:01 × | Severity: Info | ☑ Higher × | Device: |

Device	IP	T	…estamp
AP5CE1.76F2.3F0C	172.16.1.164	Not	5 2022 06:15:
RV160W	172.16.1.2	Not	5 2022 06:31:
AP6C71.0D54.02A4	172.16.1.163	Not	5 2022 05:05:
AP5CE1.76F2.3F0C	172.16.1.164	Not	5 2022 07:05:
router44912C	172.16.1.60	Not	5 2022 07:01:
switch0294f9	10.0.0.110	Not	5 2022 06:10:
switch0294f9	10.0.0.110	Not	5 2022 05:07:

68:9C:E2:A0:CE:B0
10.0.0.138 / 68:9C:E2:A0:CE:B0

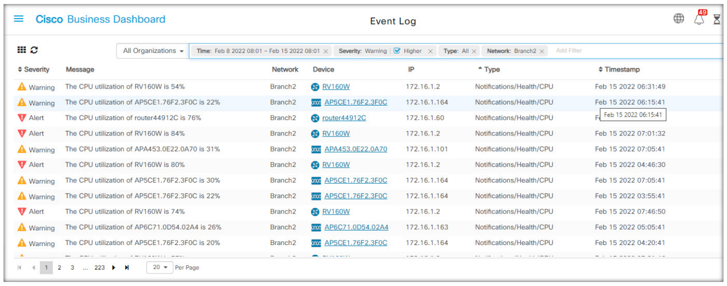
B8:27:EB:3A:13:6D
172.16.1.10 / B8:27:EB:3A:13:6D

0C:75:BD:33:F8:39
10.0.0.162 / 0C:75:BD:33:F8:39

B8:27:EB:CB:DE:C8
10.0.0.201 / B8:27:EB:CB:DE:C8

DC:A6:32:02:83:5D
10.0.0.202 / DC:A6:32:02:83:5D

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



Cisco Business Dashboard — Event Log

All Organizations | Time: Feb 8 2022 08:01 – Feb 15 2022 08:01 × | Severity: Warning | ☑ Higher × | Type: All × | Network: Branch2 × | Add Filter

Severity	Message	Network	Device	IP	Type	Timestamp
Warning	The CPU utilization of RV160W is 54%	Branch2	RV160W	172.16.1.2	Notifications/Health/CPU	Feb 15 2022 06:31:49
Warning	The CPU utilization of AP5CE1.76F2.3F0C is 22%	Branch2	AP5CE1.76F2.3F0C	172.16.1.164	Notifications/Health/CPU	Feb 15 2022 06:15:41
Alert	The CPU utilization of router44912C is 76%	Branch2	router44912C	172.16.1.60	Notifications/Health/CPU	F Feb 15 2022 06:15:41
Alert	The CPU utilization of RV160W is 84%	Branch2	RV160W	172.16.1.2	Notifications/Health/CPU	Feb 15 2022 07:01:32
Warning	The CPU utilization of APA453.0E22.0A70 is 31%	Branch2	APA453.0E22.0A70	172.16.1.101	Notifications/Health/CPU	Feb 15 2022 07:05:41
Alert	The CPU utilization of RV160W is 80%	Branch2	RV160W	172.16.1.2	Notifications/Health/CPU	Feb 15 2022 04:46:30
Warning	The CPU utilization of AP5CE1.76F2.3F0C is 30%	Branch2	AP5CE1.76F2.3F0C	172.16.1.164	Notifications/Health/CPU	Feb 15 2022 07:05:41
Warning	The CPU utilization of AP5CE1.76F2.3F0C is 22%	Branch2	AP5CE1.76F2.3F0C	172.16.1.164	Notifications/Health/CPU	Feb 15 2022 03:55:41
Alert	The CPU utilization of RV160W is 74%	Branch2	RV160W	172.16.1.2	Notifications/Health/CPU	Feb 15 2022 07:46:50
Warning	The CPU utilization of AP6C71.0D54.02A4 is 26%	Branch2	AP6C71.0D54.02A4	172.16.1.163	Notifications/Health/CPU	Feb 15 2022 05:05:41
Warning	The CPU utilization of AP5CE1.76F2.3F0C is 20%	Branch2	AP5CE1.76F2.3F0C	172.16.1.164	Notifications/Health/CPU	Feb 15 2022 04:20:41

1 2 3 ... 223 | 20 Per Page

Monitoring Defaults

Monitoring Profiles allow you to control the device monitoring that is performed in the network. Monitoring Profiles may be applied at the organization level or at the system level. Organizations that choose to inherit system level monitoring profiles will have the behavior controlled by the **Monitoring Defaults** page.

To change the **Monitoring Profiles** applied across the system, follow the steps below.

1. Navigate to **Assurance** > **Monitoring** > **Monitoring Defaults**.
2. Use the drop-downs to select the appropriate monitoring profile to be applied to devices of the corresponding type. See Managing Monitoring Profiles for more information on creating monitoring profiles.
3. Click **Save**.

See Monitoring Profiles for more information about the types of monitoring that can be performed and how to configure them. See Organizations, on page 79 for details on changing monitoring settings at the organization level.

Monitoring Profiles

Monitoring Profiles control the data that is collected from devices and the notifications that are generated. Profiles can be applied to different types of devices within an organization or across the system. For instance some devices might need different monitoring requirements depending on their location or security requirements. Within a profile, two types of monitors are supported – **Notification Monitors** and **Reporting Monitors**.

Notification Monitors cause notifications and alerts to be generated, usually due to a change in device state or a parameter crossing a threshold. Notifications have different levels of severity – informational, warning and alert – and can be delivered through the following channels:

- Pop-up notifications of the Web UI.
- Email. This requires that email settings are correctly configured. See Managing Email Settings, on page 97 for more details.
- Help desk ticket. This requires integration with an application providing help desk services. See Managing Integration Settings, on page 105 for more details.
- Collaboration message. This requires integration with a collaboration application. See Managing Integration Settings, on page 105 for more details.

Note Cisco recommends you configure the Monitoring Profiles to ensure the average rate of 60 tickets and/or collaboration messages per hour is not exceeded. When communicating with external applications, sustained rates over this could result in API congestion and loss of events.

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.

Multiple monitoring profiles can be created, and different profiles can be assigned to different device types at the system level or on a per-organization basis. For more information on assigning monitoring profiles to devices, see Organizations, on page 79 and Monitoring Defaults, on page 61.

Add a New Monitoring Profile

1. Navigate to **Assurance** > **Monitoring** > **Monitoring Profiles**.
2. Click the **+** (plus) icon to create a new profile
3. Specify a name for the profile and an organization to associate the profile to. You can also specify All Organizations here, allowing the profile to be used with any organization or as a system level default.
4. You can also provide a description for the profile and a comma-separated list of email address to receive notifications.
5. Click **Save**
6. The screen updates to display the different notification and reporting monitors. You can enable and disable individual monitors using the controls provided.
7. The notification monitors have additional settings that can be modified by clicking the **Edit** icon for the monitor. The settings will vary between monitors, but include the notification types that should be generated, the severity of the notification, and the thresholds that should trigger the notification.

Copy an Existing Monitoring Profile

To copy an existing monitoring profile, follow the steps below.

1. Navigate to **Assurance > Monitoring > Monitoring Profiles**.
2. Select the check box next to the profile to be copied and click the **Save As** icon.
3. Update the profile name, description, organization and email address(es) as required, then click **Save**.
4. 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.

Modify a Monitoring Profile

To modify an existing monitoring profile, follow the steps below.

1. Navigate to **Assurance > Monitoring > Monitoring Profiles**
2. Select the check box next to the profile to be copied and click the **Edit** icon.
3. Update the profile settings and email address(es) as required, then click **Save**.
4. 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.

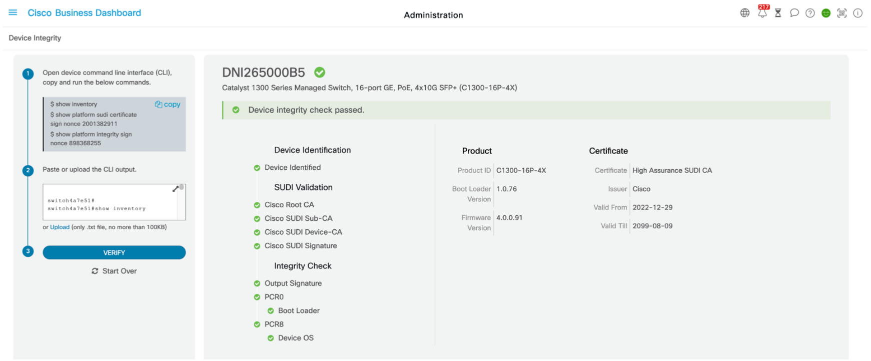
Remove a Monitoring Profile

1. Navigate to **Assurance > Monitoring > Monitoring Profiles**.
2. Select the check box next to the profile to be copied and click the **Delete** icon.

Note If the profile is in use as an organization-level monitoring profile, then the corresponding organization and device type will be updated to inherit the system-level configuration. Profiles that are in use as system-level monitoring profiles can not be removed. Remove the profile from the **Assurance > Monitoring > Monitoring Defaults** page before deleting it.

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.



1 Open device command line interface (CLI), copy and run the below commands.

```
$ show inventory
$ show platform sudi certificate
sign nonce 2001382911
$ show platform integrity sign
nonce 898368255
```

2 Paste or upload the CLI output.

```
switch4a7e51#
switch4a7e51#show inventory
```

or Upload (only .txt file, no more than 100KB)

DNI265000B5 ✓

Catalyst 1300 Series Managed Switch, 16-port GE, PoE, 4x10G SFP+ (C1300-16P-4X)

✓ Device integrity check passed.

Device Identification

- ✓ Device Identified

SUDI Validation

- ✓ Cisco Root CA
- ✓ Cisco SUDI Sub-CA
- ✓ Cisco SUDI Device-CA
- ✓ Cisco SUDI Signature

Integrity Check

- ✓ Output Signature
- ✓ PCR0
  - ✓ Boot Loader
- ✓ PCR8
  - ✓ Device OS

Product

Product ID	C1300-16P-4X
Boot Loader Version	1.0.76
Firmware Version	4.0.0.91

Certificate

Certificate	High Assurance SUDI CA
Issuer	Cisco
Valid From	2022-12-29
Valid Till	2099-08-09

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.**

Notifications

This segment contains the following sections:

About Notifications

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

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

Supported Notifications

The following table lists the notifications supported by Cisco Business Dashboard

Table 6: 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.

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

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

Viewing and Filtering Current Device Notifications

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

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 7: 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.

Filter	Description
Include Ack	Include notifications that have been acknowledged.
Network	Displays notifications for the specified network(s). Start typing in the filter and matching networks will be listed in a dropdown. Click to select the desired network. You may include multiple networks in the filter.
Device	Displays notifications for the specified device(s). Start typing in the filter and matching devices will be listed in a 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 at the organization or system level.

Viewing and Filtering Historical Device Notifications

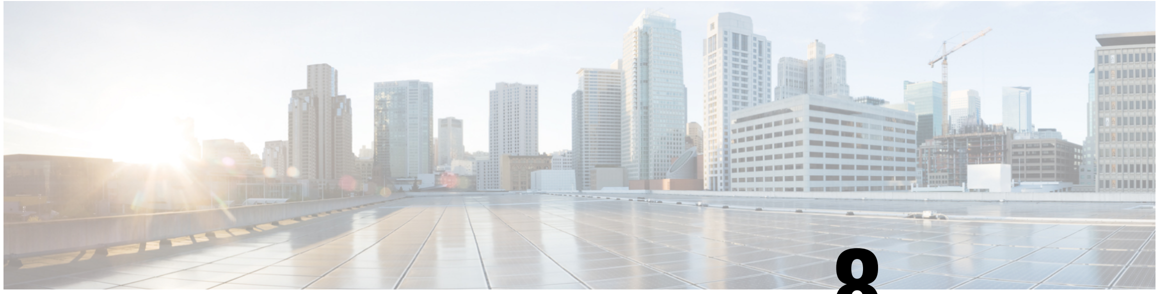
The occurrence or change in state of any notification is recorded as an event on the Dashboard, and may be viewed through the Event Log. A subset of the event log can be viewed through the following panels:

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 About the Event Log for more information on viewing and filtering historical events.



CHAPTER 8

Reports

This chapter contains the following sections:

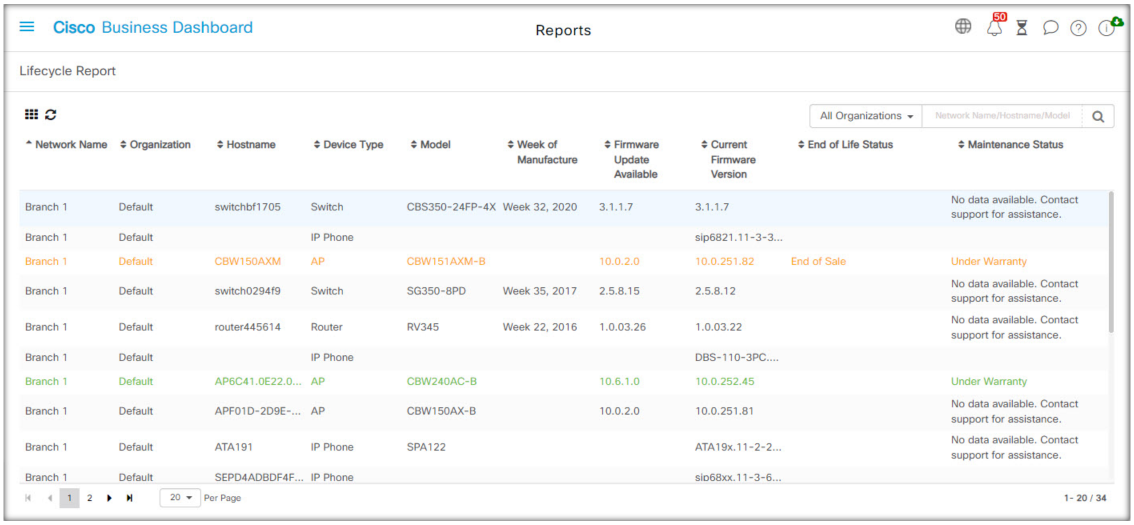
About Reports

The **Reports** option in the Cisco Business Dashboard provides a series of reports about your network. The reports provided include:

- **Lifecycle**—Provides a summary of the lifecycle status of the devices in the network.
- **End of Life**—Shows any devices that have an End of Life bulletin published.
- **Maintenance**—Lists all devices and their warranty state and whether the device has an active support contract.
- **Wireless Network**— Shows information about the wireless environment, including SSIDs, access points, and spectrum usage.
- **Wireless Client**—Displays details about wireless clients seen on the network.

Viewing the Lifecycle Report

The **Lifecycle Report** provides a high level view of the status of the network devices, taking into account both software and hardware lifecycle status.



Network Name	Organization	Hostname	Device Type	Model	Week of Manufacture	Firmware Update Available	Current Firmware Version	End of Life Status	Maintenance Status
Branch 1	Default	switchbf1705	Switch	CBS350-24FP-4X	Week 32, 2020	3.1.1.7	3.1.1.7		No data available. Contact support for assistance.
Branch 1	Default		IP Phone				sip6821.11-3-3...		
Branch 1	Default	CBW150AXM	AP	CBW151AXM-B		10.0.2.0	10.0.251.82	End of Sale	Under Warranty
Branch 1	Default	switch0294f9	Switch	SG350-8PD	Week 35, 2017	2.5.8.15	2.5.8.12		No data available. Contact support for assistance.
Branch 1	Default	router445614	Router	RV345	Week 22, 2016	1.0.03.26	1.0.03.22		No data available. Contact support for assistance.
Branch 1	Default		IP Phone				DBS-110-3PC....		
Branch 1	Default	AP6C41.0E22.0...	AP	CBW240AC-B		10.6.1.0	10.0.252.45		Under Warranty
Branch 1	Default	APF01D-2D9E-...	AP	CBW150AX-B		10.0.2.0	10.0.251.81		No data available. Contact support for assistance.
Branch 1	Default	ATA191	IP Phone	SPA122			ATA19x.11-2-2...		No data available. Contact support for assistance.
Branch 1	Default	SEPD4ADBDF4F...	IP Phone				sip68xx.11-3-6...		

The following table describes the information provided in this report.

Field	Description
Network Name	The name of the network in which the device is located.
Organization	The organization the device belongs to.
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.

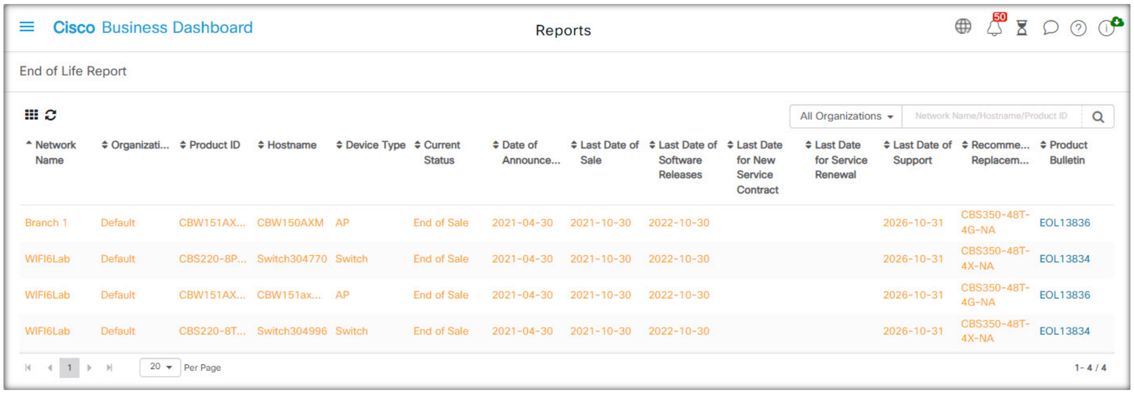
The row in the table for a device that may require attention is color-coded to indicate the urgency. For example, a device with a published End of Life bulletin will be colored orange if the End of Support milestone has not been reached, and red if the device is no longer supported by Cisco.

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. Results may be limited to a specific organization using the Organization drop-down.

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 End of Life Report

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.



Network Name	Organizati...	Product ID	Hostname	Device Type	Current Status	Date of Announce...	Last Date of Sale	Last Date of Software Releases	Last Date for New Service Contract	Last Date for Service Renewal	Last Date of Support	Recomme... Replacem...	Product Bulletin
Branch 1	Default	CBW151AX...	CBW150AXM	AP	End of Sale	2021-04-30	2021-10-30	2022-10-30			2026-10-31	CBS350-48T-4G-NA	EOL13836
WIFI6Lab	Default	CBS220-8P...	Switch304770	Switch	End of Sale	2021-04-30	2021-10-30	2022-10-30			2026-10-31	CBS350-48T-4X-NA	EOL13834
WIFI6Lab	Default	CBW151AX...	CBW151ax...	AP	End of Sale	2021-04-30	2021-10-30	2022-10-30			2026-10-31	CBS350-48T-4G-NA	EOL13836
WIFI6Lab	Default	CBS220-8T...	Switch304996	Switch	End of Sale	2021-04-30	2021-10-30	2022-10-30			2026-10-31	CBS350-48T-4X-NA	EOL13834

The following table describes the information provided:

Field	Description
Network Name	The name of the network in which the device is located.
Organization	The organization the device belongs to.
Product ID	The product ID or part number of the device.
Hostname	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.

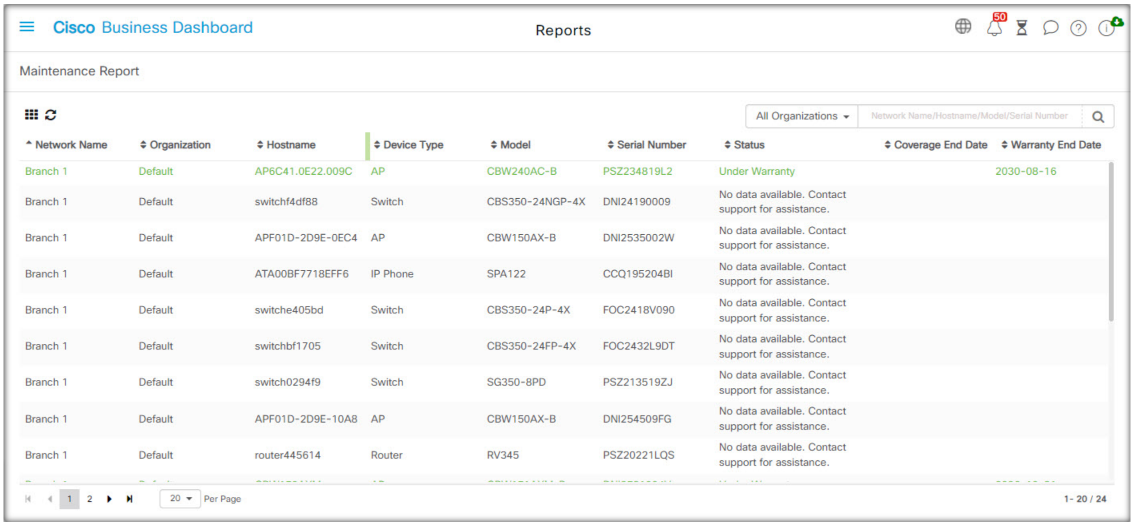
Each row of the table is color-coded to indicate the stage of the End of Life process the device is at. For example, a device that has past the Last Date of Sale but not yet reached the Last Date of Support will be colored orange, and a device that is past the Last Date of Support is colored red.

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. Results may be limited to a specific organization using the Organization drop-down.

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 Maintenance Report

The **Maintenance Report** lists all network devices which includes the warranty and support contract status information for each of them.



Network Name	Organization	Hostname	Device Type	Model	Serial Number	Status	Coverage End Date	Warranty End Date
Branch 1	Default	AP6C41.0E22.009C	AP	CBW240AC-B	PSZ234819L2	Under Warranty		2030-08-16
Branch 1	Default	switchf4df88	Switch	CBS350-24NGP-4X	DNI24190009	No data available. Contact support for assistance.		
Branch 1	Default	APF01D-2D9E-0EC4	AP	CBW150AX-B	DNI2535002W	No data available. Contact support for assistance.		
Branch 1	Default	ATA00BF7718EFF6	IP Phone	SPA122	CCQ195204BI	No data available. Contact support for assistance.		
Branch 1	Default	switche405bd	Switch	CBS350-24P-4X	FOC2418V090	No data available. Contact support for assistance.		
Branch 1	Default	switchbf1705	Switch	CBS350-24FP-4X	FOC2432L9DT	No data available. Contact support for assistance.		
Branch 1	Default	switch0294f9	Switch	SG350-8PD	PSZ213519ZJ	No data available. Contact support for assistance.		
Branch 1	Default	APF01D-2D9E-10A8	AP	CBW150AX-B	DNI254509FG	No data available. Contact support for assistance.		
Branch 1	Default	router445614	Router	RV345	PSZ20221LQS	No data available. Contact support for assistance.		

The following table describes the information provided in this report.

Field	Description
Network Name	The name of the network in which the device is located.
Organization	The organization the device belongs to.
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.

Field	Description
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. Results may be limited to a specific organization using the Organization drop-down.

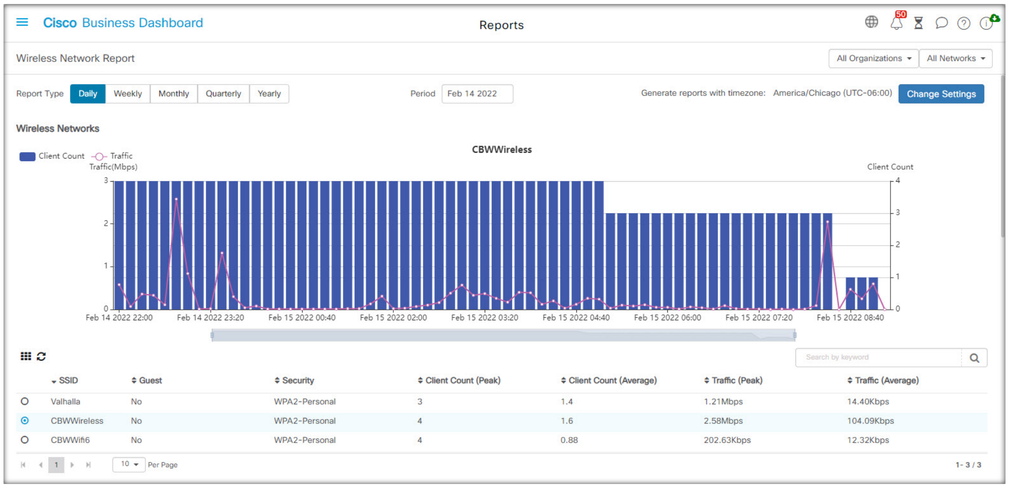
The column selection icon at the top left of the report can be used to customize the information displayed. Click on the icon and then use the check boxes that appear to select the columns you wish to include in the report.

Viewing the Wireless Network Report

The **Wireless Network Report** shows details about the wireless network broken down by SSID, wireless spectrum usage, and access point, and includes a list of rogue access points that have been detected. Reports can be generated for time ranges from daily to yearly using the controls at the top of the page.

Several of the data sets include a graph that shows a breakdown over time for the selected row. You can click on the labels in the legend on the graph to toggle the display of each set of data.

The following tables describes the information provided in the different sections of the report.



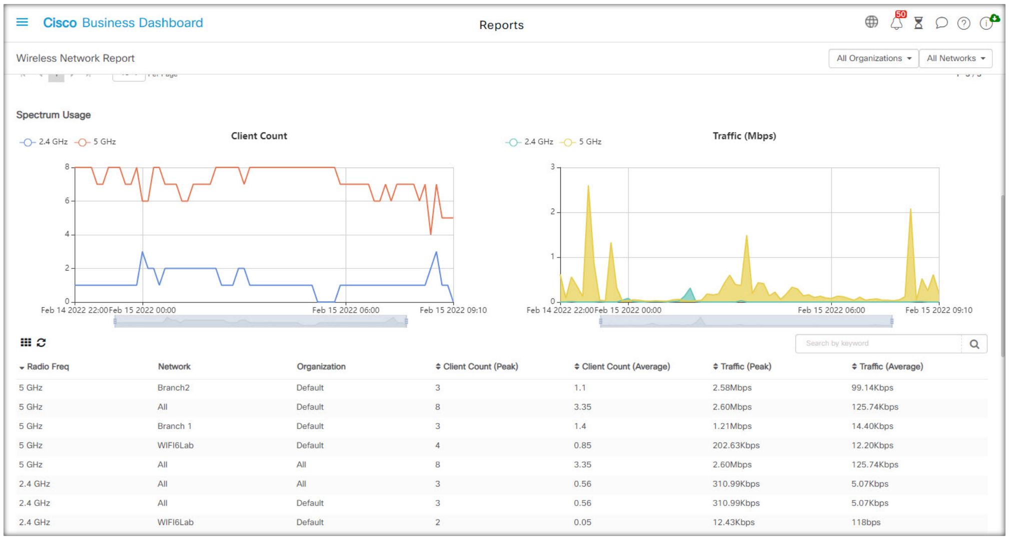
Period Feb 14 2022

Generate reports with timezone: America/Chicago (UTC-06:00)

	SSID	Guest	Security	Client Count (Peak)	Client Count (Average)	Traffic (Peak)	Traffic (Average)
○	Valhalla	No	WPA2-Personal	3	1.4	1.21Mbps	14.40Kbps
●	CBWWireless	No	WPA2-Personal	4	1.6	2.58Mbps	104.09Kbps
○	CBWWifi6	No	WPA2-Personal	4	0.88	202.63Kbps	12.32Kbps

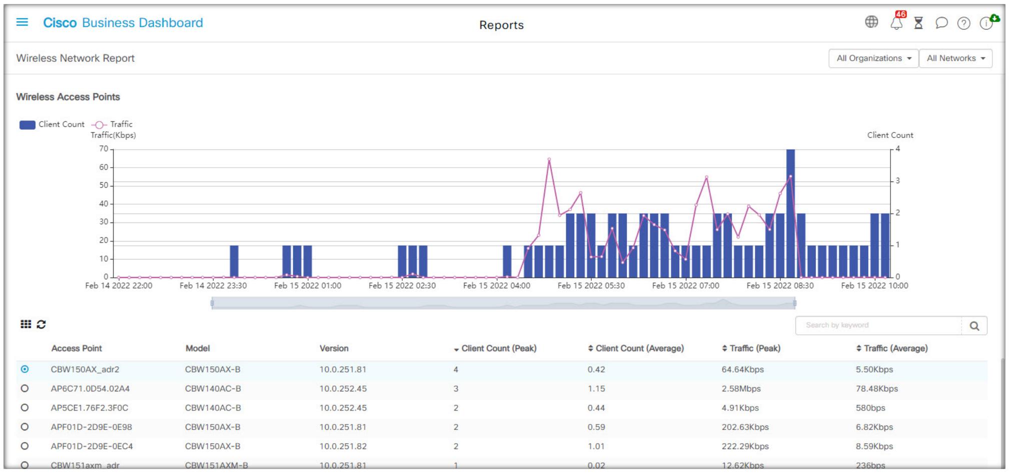
Wireless Networks Table	
SSID	The wireless network name.
Network (hidden by default)	The network where the SSID is located.
Organization (hidden by default)	The organization the SSID belongs to.
Guest	Whether the SSID is configured for guest access.

Wireless Networks Table	
Security	The security method configured for the SSID.
Client Count (Peak)	The maximum number of clients associated with the SSID during the period covered by the report.
Client Count (Average)	The average number of clients associated with the SSID during the period covered by the report.
Traffic (Peak)	The maximum aggregate traffic rate through the SSID during the period covered by the report.
Traffic (Average)	The average aggregate traffic rate through the SSID during the period covered by the report.



Radio Freq	Network	Organization	Client Count (Peak)	Client Count (Average)	Traffic (Peak)	Traffic (Average)
5 GHz	Branch2	Default	3	1.1	2.58Mbps	99.14Kbps
5 GHz	All	Default	8	3.35	2.60Mbps	125.74Kbps
5 GHz	Branch 1	Default	3	1.4	1.21Mbps	14.40Kbps
5 GHz	WIFI6Lab	Default	4	0.85	202.63Kbps	12.20Kbps
5 GHz	All	All	8	3.35	2.60Mbps	125.74Kbps
2.4 GHz	All	All	3	0.56	310.99Kbps	5.07Kbps
2.4 GHz	All	Default	3	0.56	310.99Kbps	5.07Kbps
2.4 GHz	WIFI6Lab	Default	2	0.05	12.43Kbps	118bps

Spectrum Usage Table	
Radio Freq	The radio frequency band in use – either 2.4GHz or 5GHz.
Network	The network the spectrum usage data displayed applies to.
Organization	The organization the spectrum usage data applies to.
Client Count (Peak)	The maximum number of clients using the frequency band during the period covered by the report.
Client Count (Average)	The average number of clients using the frequency band during the period covered by the report.
Traffic (Peak)	The maximum aggregate traffic rate through the frequency band during the period covered by the report.
Traffic (Average)	The average aggregate traffic rate through the frequency band during the period covered by the report.

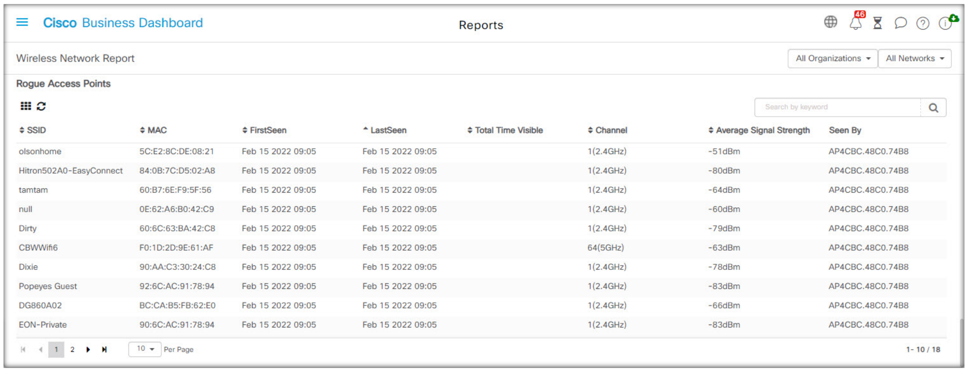


Wireless Network Report

Wireless Access Points

	Access Point	Model	Version	Client Count (Peak)	Client Count (Average)	Traffic (Peak)	Traffic (Average)
●	CBW150AX_adr2	CBW150AX-B	10.0.251.81	4	0.42	64.64Kbps	5.50Kbps
○	AP6C71.0D54.02A4	CBW140AC-B	10.0.252.45	3	1.15	2.58Mbps	78.48Kbps
○	AP5CE1.76F2.3F0C	CBW140AC-B	10.0.252.45	2	0.44	4.91Kbps	580bps
○	APF01D-2D9E-0E98	CBW150AX-B	10.0.251.81	2	0.59	202.63Kbps	6.82Kbps
○	APF01D-2D9E-0EC4	CBW150AX-B	10.0.251.82	2	1.01	222.29Kbps	8.59Kbps
○	CBW151axm_adr	CBW151AXM-B	10.0.251.81	1	0.02	12.62Kbps	236bps

Wireless Access Point Table	
Access Point	The name of the access point.
Network (hidden by default)	The network where the access point is located.
Organization (hidden by default)	The organization the access point belongs to.
Model	The model of the access point.
Version	The firmware version running on the access point.
Client Count (Peak)	The maximum number of clients associated with the access point during the period covered by the report.
Client Count (Average)	The average number of clients associated with the access point during the period covered by the report.
Traffic (Peak)	The maximum aggregate traffic rate through the access point during the period covered by the report.
Traffic (Average)	The average aggregate traffic rate through the access point during the period covered by the report.



Wireless Network Report

Rogue Access Points

SSID	MAC	FirstSeen	LastSeen	Total Time Visible	Channel	Average Signal Strength	Seen By
olsonhome	5C:E2:8C:DE:08:21	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-51dBm	AP4CBC.48C0.74B8
Hitron502A0-EasyConnect	84:0B:7C:D5:02:A8	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-80dBm	AP4CBC.48C0.74B8
tamtam	60:B7:6E:F9:5F:56	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-64dBm	AP4CBC.48C0.74B8
null	0E:62:A6:B0:42:C9	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-60dBm	AP4CBC.48C0.74B8
Dirty	60:6C:63:BA:42:C8	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-79dBm	AP4CBC.48C0.74B8
CBWWifi6	F0:1D:2D:9E:61:AF	Feb 15 2022 09:05	Feb 15 2022 09:05		64(5GHz)	-63dBm	AP4CBC.48C0.74B8
Dixie	90:AA:C3:30:24:C8	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-78dBm	AP4CBC.48C0.74B8
Popeyes Guest	92:6C:AC:91:78:94	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-83dBm	AP4CBC.48C0.74B8
DG860A02	BC:CA:B5:FB:62:E0	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-66dBm	AP4CBC.48C0.74B8
EON-Private	90:6C:AC:91:78:94	Feb 15 2022 09:05	Feb 15 2022 09:05		1(2.4GHz)	-83dBm	AP4CBC.48C0.74B8

1 2 | 10 Per Page | 1- 10 / 18

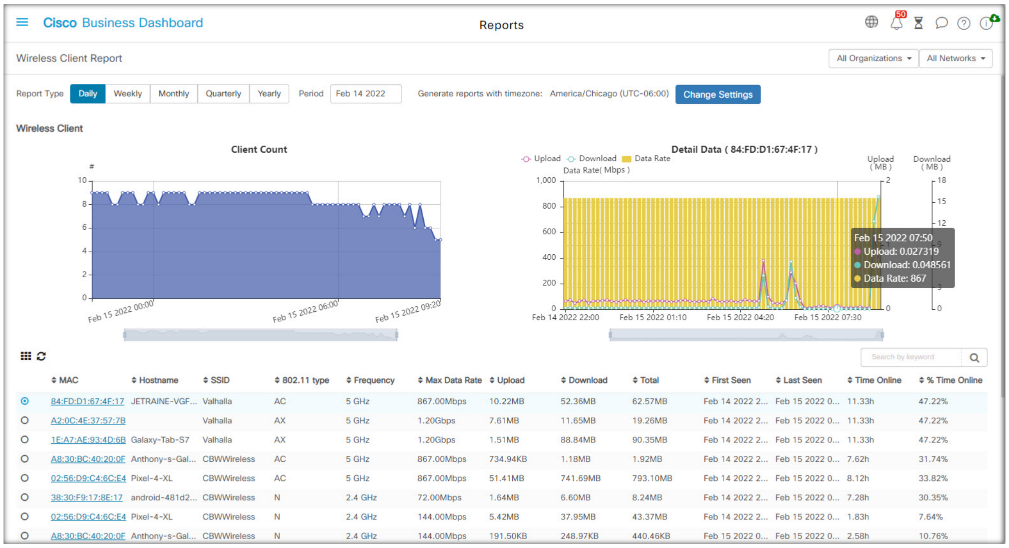
Rogue Access Points Table	
SSID	The SSID detected.
Network (hidden by default)	The network where the detecting access point is located.
Organization (hidden by default)	The organization the detecting access point belongs to.
MAC	The MAC address of the rogue access point.
First Seen	The time at which the rogue access point was first detected.
Last Seen	The time at which the rogue access point was last seen.
Total Time Visible	The total time that the rogue access point was online.
Channel	The wireless channel used by the rogue access point.
Average Signal Strength	The average signal strength of the rogue access point as seen by the detecting access point.
Seen By	The access point(s) that detected the rogue access point.

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. You may click on the labels in the legend on the graph to toggle the display of each set of data.

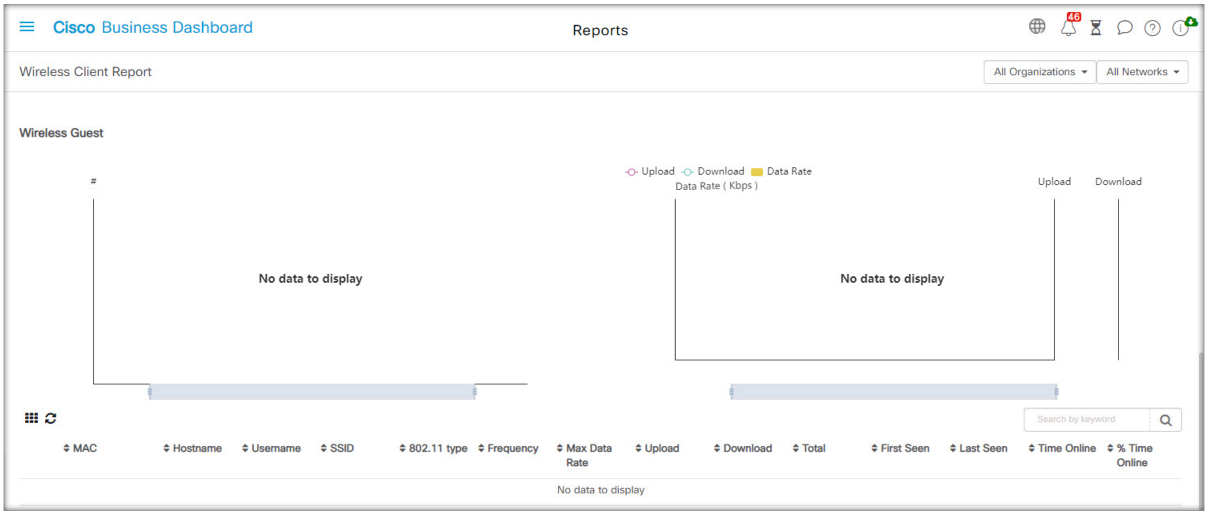
The following tables describe the information provided in each report.



Report Type: Daily Period: Feb 14 2022 Generate reports with timezone: America/Chicago (UTC-06:00)

	MAC	Hostname	SSID	802.11 type	Frequency	Max Data Rate	Upload	Download	Total	First Seen	Last Seen	Time Online	% Time Online
●	84:FD:D1:67:4F:17	JETRAINE-VGF...	Valhalla	AC	5 GHz	867.00Mbps	10.22MB	52.36MB	62.57MB	Feb 14 2022 2...	Feb 15 2022 0...	11.33h	47.22%
○	A2:0C:4E:37:57:7B		Valhalla	AX	5 GHz	1.20Gbps	7.61MB	11.65MB	19.26MB	Feb 14 2022 2...	Feb 15 2022 0...	11.33h	47.22%
○	1E:A7:AE:93:4D:6B	Galaxy-Tab-S7	Valhalla	AX	5 GHz	1.20Gbps	1.51MB	88.84MB	90.35MB	Feb 14 2022 2...	Feb 15 2022 0...	11.33h	47.22%
○	A8:30:BC:40:20:0F	Anthony-s-Gal...	CBWWireless	AC	5 GHz	867.00Mbps	734.94KB	1.18MB	1.92MB	Feb 14 2022 2...	Feb 15 2022 0...	7.62h	31.74%
○	02:56:D9:C4:6C:E4	Pixel-4-XL	CBWWireless	AC	5 GHz	867.00Mbps	51.41MB	741.69MB	793.10MB	Feb 14 2022 2...	Feb 15 2022 0...	8.12h	33.82%
○	38:30:F9:17:8E:17	android-481d2...	CBWWireless	N	2.4 GHz	72.00Mbps	1.64MB	6.60MB	8.24MB	Feb 14 2022 2...	Feb 15 2022 0...	7.28h	30.35%
○	02:56:D9:C4:6C:E4	Pixel-4-XL	CBWWireless	N	2.4 GHz	144.00Mbps	5.42MB	37.95MB	43.37MB	Feb 14 2022 2...	Feb 15 2022 0...	1.83h	7.64%
○	A8:30:BC:40:20:0F	Anthony-s-Gal...	CBWWireless	N	2.4 GHz	144.00Mbps	191.50KB	248.97KB	440.46KB	Feb 15 2022 0...	Feb 15 2022 0...	2.58h	10.76%

Wireless Clients Table	
MAC	The MAC address of the client
Hostname	The hostname of the client, where available.
Organization	The organization in which the client was last seen.
Network	The network where the client was last seen.
SSID	The SSID the client was last associated with.
802.11 Type	The 802.11 variant used by the client.
Frequency	The frequency band used by the client.
Max Data Rate	The maximum data rate used by the client.
Upload	The volume of data uploaded by the client.
Download	The volume of data downloaded by the client.
Total	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.



Wireless Client Report

Wireless Guest

MAC	Hostname	Username	SSID	802.11 type	Frequency	Max Data Rate	Upload	Download	Total	First Seen	Last Seen	Time Online	% Time Online

No data to display

Table 8: Wireless Guests Table

Wireless Guests Table	
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.
Organization	The organization in which the client was last seen.
Network	The network where the client was last seen.
SSID	The SSID the client was last associated with.
802.11 Type	The 802.11 variant used by the client.
Frequency	The frequency band used by the client.
Max Data Rate	The maximum data rate used by the client.
Upload	The volume of data uploaded by the client.
Download	The volume of data downloaded by the client.
Total	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.

Note The **First Seen** and **Last Seen** timestamps are the time reported by the access point. It is recommended that all network devices implement clock synchronization using a mechanism such as the Network Time Protocol (NTP).

CHAPTER 9

Administration

This chapter contains the following sections:

About Administration

The **Administration** option in Cisco Business Dashboard allows you to control the operation of the application at the organizational level. This option is divided into the following pages:

- **Organizations**—Create and maintain organizations in Cisco Business Dashboard.
- **Device Groups**—Allocate network devices into groups for easy management.
- **Device Credentials**—Enter credentials to be used when accessing network devices.
- **Users**— Define user access to Cisco Business Dashboard.
- **Login Attempts**—Provides a log of all user access to Cisco Business Dashboard.

Not all pages are visible to all roles. Operators cannot manage user settings.

Organizations

Organizations are used in Cisco Business Dashboard to split networks, users, and devices into groups that are typically administered separately. Each network or device belongs to an organization, and each user can manage one or more organizations. An organization might represent a customer or a department or a region – whatever is most suitable for your company – but in all cases, the use of organizations allows more granular control over who can view and manage the different parts of the network. A single organization called **Default** is created when Cisco Business Dashboard is installed.

Create a New Organization

1. Navigate to **Administration** > **Organizations**.
2. Click the ✚(plus) icon at the top of the table.
3. Specify a name for the organization and enter the required details.
4. Enter a name for a new device group that should be used as the default group for newly discovered devices. The new device group will be created along with the organization.
5. Specify a start time and duration for the organization's change window.
6. Click **Save**.
7. Repeat the steps above for each organization you wish to create.

Modify an Existing Organization

1. Navigate to **Administration**>**Organizations**.
2. Select the radio button for the organization to be modified and click the **Edit** icon
3. Make changes as required and click **Save**.

Delete an Organization

1. Navigate to **Administration** >**Organizations**.
2. Select the radio button for the organization to be modified and click the **Delete** icon.

Manage Monitoring Profiles for an Organization

Monitoring Profiles allow you to control how network device monitoring is performed across the organization. The profiles selected at the organization level will be applied across all networks in the organization.

To change the Monitoring Profiles for an organization, do the following:

1. Navigate to **Administration** >**Organizations**.
2. Click the name of the organization to be modified and select the **Monitoring Profiles** tab.
3. Use the drop-downs to select the appropriate monitoring profile to be applied to devices of the corresponding type. See Monitoring Profiles, on page 61 for more information on creating monitoring profiles.

   You can also choose to follow the behavior defined at system level by checking the Inherit from **Monitoring Defaults** check boxes for individual device types or for the entire organization.
4. Click **Save**.

Manage Users Associated with an Organization

Users with a role of **Organization Administrator** or lower must be explicitly associated with an organization to be able to view or manage devices in that organization.

To associate a user with the organization, follow the steps below.

1. Navigate to **Administration >Organizations**.

2. Click the name of the organization to be modified and select the **Users** tab.

3. Click the ✚(plus) icon. Select the user from the drop-down list.

> **Note** **Administrator** level users are implicitly associated with all organizations and will not appear in the drop-down list.

To remove a user from the organization, follow the steps below.

1. Navigate to **Administration**>**Organizations**.

2. Click the name of the organization to be modified and select the **Users** tab.

3. Click the **Delete** icon next to the user in the table.

Manage Networks Associated with an Organization

Every network in Cisco Business Dashboard belongs to a single organization. You can view a list of networks associated with an organization by selecting the **Networks** tab on the **Organization Detail** page.

Associating a network with an organization is done when the network is first created. To change the organization a network is associated with, follow the steps below.

1. Navigate to **Network** and select the network that you wish to change. Click **More** to display the **Network Detail** panel.

2. Click the **Edit** icon next to the network name.

3. Select the new organization from the drop-down list.

4. Click **OK**.

You can create new networks for an organization from this view. Click the ✚(plus) icon to create a new network and fill in appropriate values in the form that is displayed.

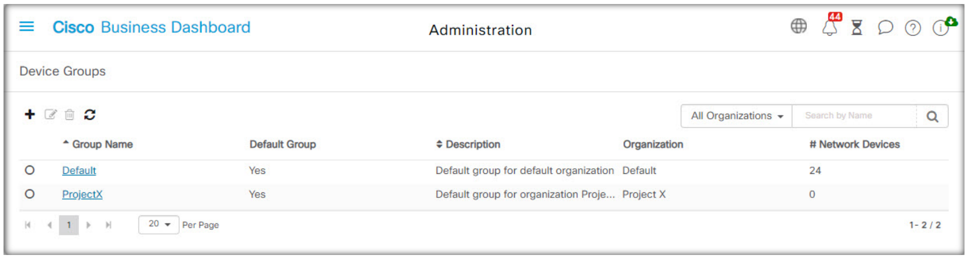
Device Groups

Cisco Business Dashboard uses device groups for performing most configuration tasks. Multiple network devices are grouped together so that they may be configured in a single action such as creating VLANS or WLANS to only a subset of devices.

Each device group can contain devices of multiple types, and when configuration is applied to a device group, that configuration is only applied to devices in the group that support that feature. For example, if a device group contains wireless access points, switches and routers, then configuration for a new wireless SSID will be only be applied to the wireless access points, and will be applied to the routers only if they are wireless routers.

Device groups may include devices from multiple networks, but all devices must belong to a single organization. A device group may be designated as the default group for an organization or network, and any newly discovered devices for that network or organization will be placed in the default device group.

Create a New Device Group



	Group Name	Default Group	Description	Organization	# Network Devices
○	Default	Yes	Default group for default organization	Default	24
○	ProjectX	Yes	Default group for organization Proje...	Project X	0

20 Per Page 1- 2 / 2

1. Navigate to **Administration**> **Device Groups**.
2. Click on the ✚(plus) sign to create a new group.
3. Enter an organization, a name and a description for the group. Click **Save**.
4. Optionally, add devices to the device group by clicking the ✚(plus) icon and using the search box to select devices to be added to the group. You may add devices individually or by network. If the selected device is already a member of a different group, it will be removed from that group. Each device may only be a member of a single group.

Modify the Device Group

1. Navigate to **Administration**> **Device Groups**.
2. Select the radio button next to the group to be changed and click the **edit** icon.
3. Change the name and description if necessary. Click **Save**.
4. Add and remove devices from the group as required. To remove a device that was previously added to the group, click the **trashcan** icon next to the device. The device will be moved to the **Default** group for the network or organization.

Note You cannot delete a device from the **Default** group. To remove a device from the **Default** group you must add it to a new group.

Delete a Device Group

1. Navigate to **Administration**> **Device Groups**.
2. Click the radio button for the device group to be removed, and then click the **delete** icon.

Note You cannot delete a **Default** group.

Reapply Network Configuration to all Devices in a Group

In some situations— such as when an entire network is offline, when a change is made to a network configuration profile — multiple devices in a device group may not have the correct configuration applied.

To fix this, the network configuration profiles may be reapplied to all devices in the group using the following steps:

1. Navigate to **Administration > Device Groups**.
2. Select the radio button next to the group to be reconfigured and click **Edit**.
3. Click the **Reapply Network Configuration** button located at the top right corner of the page

A series of jobs will be created to apply each of the network configuration profiles assigned to the device group to the devices in the group.

Device Credentials

For Cisco Business Dashboard to fully discover and manage the network, it needs credentials to authenticate with the network devices. When a device is first discovered, the Probe will attempt to authenticate with the device using the default username: `cisco`, password: `cisco`, and SNMP community: `public`. 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 any or all of the **Username/Password** fields, **SNMP Community** field, and **SNMPv3** credential fields. You may click the ✚(plus) icon next to the corresponding field to enter up to three of each type of credential. Ensure that passwords are entered using plain text.

Note For **SNMPv3** credentials, the supported authentication protocols are None, MD5, and SHA, and the supported encryption protocols are None, DES, and AES

3. Click **Apply**. The Probes 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 or an SNMP 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 the Probe 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, change settings that affect how those users interact with the Dashboard and control whether those users should also be allowed to access the network when performing user-based network authentication. This is a useful tool when you need to add new users or remove them from the network.

Cisco Business Dashboard has settings to control the dashboard features that are available using the Dashboard Access drop-down list, and whether the user can access the network when user user-based network access (the Network Access checkbox). The options available for these settings include:

- **Administrator**—An Administrator has full access to Dashboard features including the ability to maintain the system.
- **Organization Administrator**—An Organization Administrator is limited to managing one or more organizations, but cannot make changes to the system.
- **Operator**—An Operator has similar power to an Organization Administrator, but cannot manage users.
- **Readonly**—A Readonly user can only view network information, they cannot make any changes.
- **No Access**—A No Access user will not be able to use any of the dashboard features, but may log on to the dashboard to manage their user profile.
- **Network Access**—This setting controls whether the user can access the network when user-based network access is in use. If the Dashboard Access setting is set to Organization Administrator or below, then access will only be permitted for organizations in the user's organization list.

Cisco Business Dashboard allows users to be authenticated against the local user database. From release 2.2.1 onwards, users may also be authenticated against a Microsoft Azure Active Directory instance.

Note Only local users will be checked when performing authentication for user-based network access.

When the Cisco Business Dashboard 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** and **Organization 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 and Network Access settings. You may also provide contact details for the user.
4. Click **Save**.

If the user is not an **Administrator**, then you must add the user to one or more organizations. To do so, select the **Organizations** tab and click the ✚(plus) icon. Select the desired organization from the drop-down list.

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**.

To add the user to a new organization, select the **Organizations** tab and click the ✚(plus) icon. Select the desired organization from the dropdown list. To remove them from an organization, click the **Delete** icon next to the organization in the table.

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**.

Note When authenticating against an Azure Active Directory instance, password complexity is managed in Active Directory.

Enable Azure Active Directory Authentication

Cisco Business Dashboard supports user authentication using an instance of Microsoft Azure Active Directory. Active Directory users are assigned roles and organization lists based on the Active Directory groups the user is a member of.

To enable Azure Active Directory as an authentication source, follow these steps.

1. In the **Azure Active Directory**, create a new App registration for Cisco Business Dashboard, assign it delegated permissions of User.Read and Domain.Read.All from the **Microsoft Graph API** and create a **Client secret**. Take note of the Application (client) ID, the Client secret and the Directory (tenant) ID.

2. Open the Cisco Business Dashboard web GUI and navigate to **Administration**>**Users**. Select the **User Settings** tab, and then select the **Azure AD** tab under **Authentication Source**.
3. Click the **Enable** Checkbox.
4. Enter the **Client ID**, **Client Secret** and **Tenant ID** collected in step 1 into the field provided
5. Optionally, specify a comma-separated list of domains that should be allowed to access the dashboard. Click **Save**.
6. Click the ✚(plus) icon under the **User Group Mappings** header to create a new group mapping. Enter the **Object ID** for the Active Directory group into the field provided, then select a role and organization list to be applied to users in this group. Repeat this step for all the groups that need to be mapped.

   If a user matches multiple groups, then the role and organization mappings from the first match will be used.
7. Make a note of the **Redirect URL** displayed beneath the **Enable** checkbox. Return to Azure Active Directory and add the URL to the list of Redirect URIs for the App registration.

Note The host and port displayed in the redirect URL should be reachable from the web browsers of users accessing the dashboard. If the current displayed values are not be reachable, update the appropriate fields on the **Systems Variables** tab on the **System**>**Platform Settings** page.

Manage Local Authentication

Authentication against the local user database is enabled by default. To disable local authentication, follow these steps.

1. Ensure that authentication against Azure Active Directory has been set up as described above. Log on to the dashboard using an Administrator account authenticated by Active Directory.
2. Navigate to **Administration**>**Users** and select the **User Settings** tab. Under **Authentication Source**, select the **Local** tab.
3. Deselect the **Enable** checkbox and click **Save**.

To enable local authentication again, follow these steps.

1. Navigate to **Administration** > **Users** and select the **User Settings** tab. Under **Authentication Source**, select the **Local** tab.
2. Select the **Enable** checkbox and click **Save**.

Restore Access when All Administrative Access has been Lost

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

1. Log on to the host operating system using SSH or via the console.
2. Enter the command **cisco-business-dashboard recoverpassword**

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

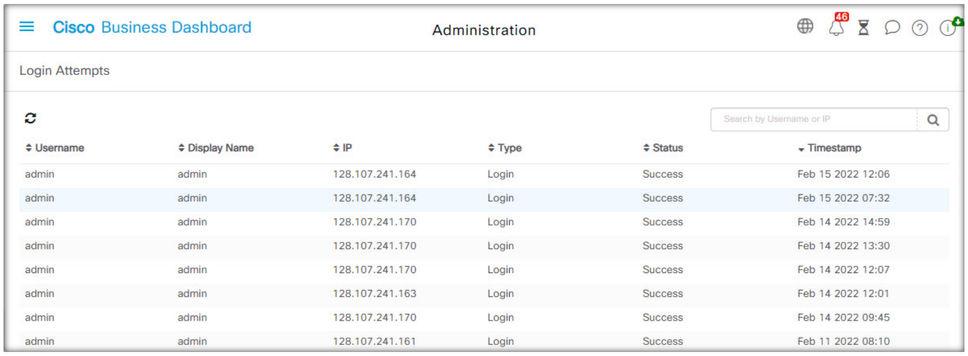
Change session timeouts

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.

Viewing Login Attempts

Cisco Business Dashboard keeps a log of every attempt made to log in and out of the system, both successful and unsuccessful.

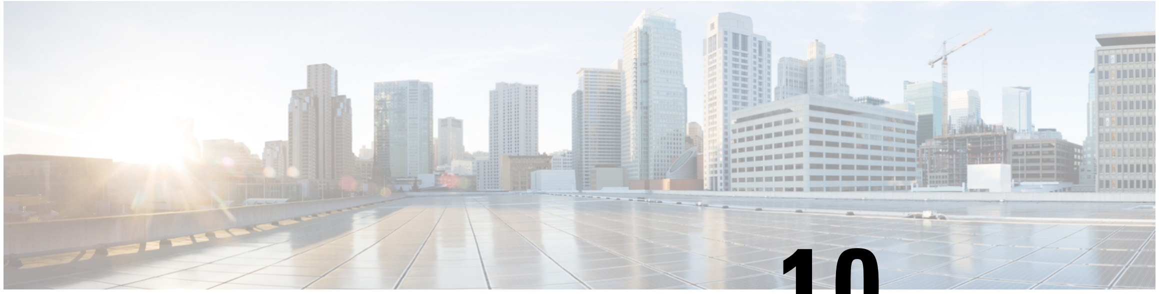


Username	Display Name	IP	Type	Status	Timestamp
admin	admin	128.107.241.164	Login	Success	Feb 15 2022 12:06
admin	admin	128.107.241.164	Login	Success	Feb 15 2022 07:32
admin	admin	128.107.241.170	Login	Success	Feb 14 2022 14:59
admin	admin	128.107.241.170	Login	Success	Feb 14 2022 13:30
admin	admin	128.107.241.170	Login	Success	Feb 14 2022 12:07
admin	admin	128.107.241.163	Login	Success	Feb 14 2022 12:01
admin	admin	128.107.241.170	Login	Success	Feb 14 2022 09:45
admin	admin	128.107.241.161	Login	Success	Feb 11 2022 08:10

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 10

System

The section contains the following topics:

About System

The System option in Cisco Business Dashboard allows you to manage the operation of the platform.

This section is divided into the following pages:

Page Name	Page Function
License	Manage software licensing for the Dashboard.
Certificate	Manage security certificates on the Dashboard.
Email Settings	Set up email and manage settings.
API Usage	Monitor the use of the Cisco Business Dashboard API.
Backup	Backup the configuration and other data for the Dashboard.
Restore	Restore the configuration and other data for the Dashboard.
Platform Settings	Manage network configuration for the Dashboard.
Privacy Settings	Control the data that can be shared with Cisco.

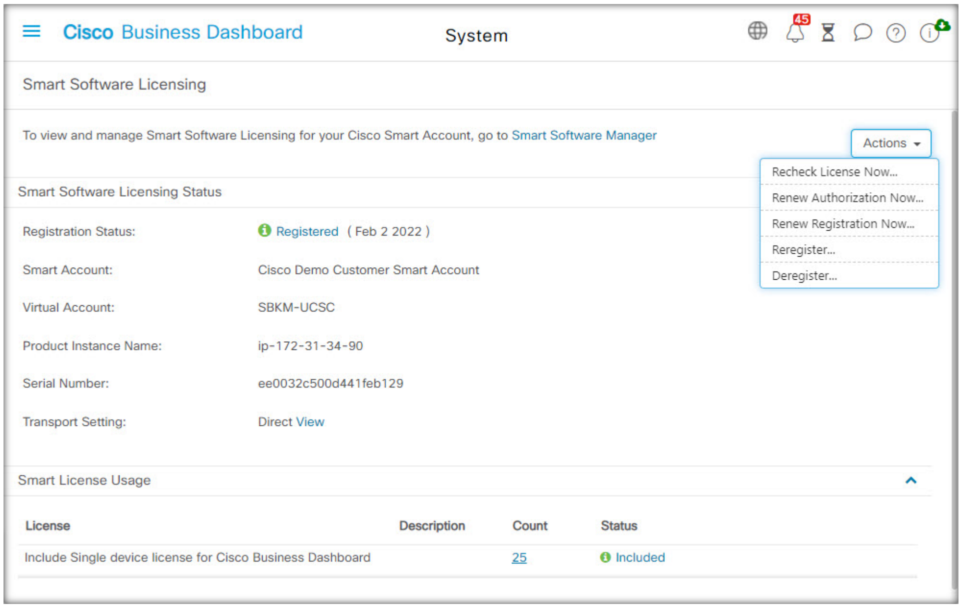
Page Name	Page Function
Log Settings	Change log settings for the Dashboard.
Local Probe	Manage a Probe hosted on the Dashboard.
Integration Settings	Manage the integration of Cisco Business Dashboard with external applications.

Note These pages are only available to **Administrators**.

Managing Licenses

Note This page is not present on the metered version of Cisco Business Dashboard for AWS.

The **License** page allows you to see the number and type of licenses required for your network, and allows you to connect the **Dashboard** to the Cisco Smart Licensing system. If you have 25 devices or less there is no need for additional licensing. There are two information panels on this page.



Smart Software Licensing

To view and manage Smart Software Licensing for your Cisco Smart Account, go to Smart Software Manager

Smart Software Licensing Status

Registration Status:	Registered (Feb 2 2022)
Smart Account:	Cisco Demo Customer Smart Account
Virtual Account:	SBKM-UCSC
Product Instance Name:	ip-172-31-34-90
Serial Number:	ee0032c500d441feb129
Transport Setting:	Direct View

Smart License Usage

License	Description	Count	Status
Include Single device license for Cisco Business Dashboard		25	Included

- **Smart Software Licensing Status**

  This panel shows the registration state of the Smart License client and information about the Smart Account in use.

- **Smart License Usage**

  This panel lists the quantities and types of license required based on the current state of the network. This information will automatically update as the network changes, and the Dashboard will update the number of licenses requested from the Smart Account. The Status field shows whether the required number of licenses have been successfully obtained.

This page also contains controls allowing you to register and deregister the Dashboard from your Smart account.

If the Dashboard is not able to obtain sufficient licenses to manage the network, it will operate in evaluation mode and a message will be displayed in the header of the Dashboard's user interface. When running in evaluation mode, you have 90 days to correct the situation. If the problem is not addressed within 90 days, some functionality of the Dashboard will be restricted until the problem is addressed, either by obtaining more licenses, or reducing the number of devices being managed.

Register the Dashboard to your Smart Account

To register the Dashboard with your Smart Account, follow the steps below:

1. Log on to your Smart Account at *https://software.cisco.com*.

   Select the **Smart Software Licensing** link located under the License section.

2. Select the **Inventory** page, and if necessary, change the selected virtual account from the default.
3. Click on the **General** tab.
4. Create a new **Product Instance Registration Token** by clicking on the **New Token…** button. Optionally add a description and change the **Expire After** time.
5. Click **Create Token**.
6. Copy the newly created token to the clipboard by selecting **Copy** from the **Actions** drop-down located at the right of the token.
7. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
8. Click the **Register** button and paste the token into the field provided.
9. Click **OK**.

The Dashboard will register with Cisco Smart Licensing and request sufficient licenses for the number of network devices being managed. If there are insufficient licenses available, a message will be displayed on the user interface, and you will have 90 days to obtain sufficient licenses before system functionality is restricted.

Remove the Dashboard from your Smart Account

To remove the Dashboard from your Smart Account and return any licenses allocated back to the pool, follow the steps below:

1. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
2. Select **Deregister…** from the drop-down list located at the top right. Click **Deregister** in the pop-up to confirm.

Immediately Check for Licenses

Cisco Business Dashboard checks daily to ensure there are still sufficient licenses available for the network, and will update immediately if the number of licenses required decreases. However, if the number of licenses required increases, or if licenses are added or removed from the pool, it may take up to a day before the Dashboard will be updated. To force the Dashboard to update its license allocation immediately, follow the steps below.

1. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
2. Select **ReCheck License Now…** from the drop-down list located at the top right. Cisco Business Dashboard will query Cisco Smart Licensing immediately to ensure that there are sufficient licenses available for the Dashboard to operate.

Renew Authorization Now

The Renew Registration Now action cause the Dashboard to refresh the certificates used to authenticate communication with Cisco Smart Licensing. Typically, this will only be required at the request of Cisco Support when rectifying an extended communications outage. To renew the registration, follow the steps below.

1. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
2. Select **Renew Authorization Now…** from the drop-down list located at the top right.

Renew Registration Now

The Renew Registration Now action causes the Dashboard to refresh the certificates used to authenticate communication with Cisco Smart Licensing. Typically, this will only be required at the request of Cisco Support when rectifying an extended communications outage. To renew the registration, follow the steps below.

1. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
2. Select **Renew Registration Now…** from the drop-down list located at the top right.

Transfer the Dashboard to a Different Account

Re-registering a Dashboard allows it to be moved from one Virtual Account to another. To move a Dashboard between accounts, follow the steps below.

1. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
2. Select **Reregister...** from the drop-down list located at the top right.
3. Enter the new registration token in the box provided. If the Dashboard is currently registered to another account, ensure the **Reregister this product instance if it is already registered** checkbox is selected, then click **OK**.

Managing Certificates

At the time of installation, Cisco Business Dashboard will generate a self-signed certificate to secure web and other communication with the server. You may choose to replace this certificate with one signed by a trusted certificate authority (CA).

There are several ways this can be done:

- Cisco Business Dashboard supports automatically issuing and renewing certificates from the Let's Encrypt certificate authority.
- You may provide a certificate signing request (CSR) to your preferred certificate authority for signing. Cisco Business Dashboard will generate the CSR for you.
- You may choose to have the certificate authority generate a certificate and the corresponding private key independently from the Dashboard. If so, you should combine the certificate chain and private key into a PKCS#12 format file prior to uploading to the dashboard.

For more details on each of these options, and instructions for viewing the current certificate and regenerating a self-signed certificate, see the sections below.

Automatically Install a Certificate from Let's Encrypt

From release 2.2.1, Cisco Business Dashboard can automatically obtain and renew a domain-validated certificate from the **Let’s Encrypt Certificate Authority** (https://letsencrypt.org) and in release 2.5.0, these certificates can be managed through the Administration page.

Important You must have a fully qualified domain name registered and a DNS record that points to the public IP address. Refer to Managing Platform Settings, on page 100 for more information.

To install a Let’s Encrypt certificate using the administration GUI, do the following:

1. Navigate to **System**> **Certificate** and select the Update Certificate tab.
2. Select the *Let’s Encrypt Certificate* radio button.
3. Check the box to enable the use of a Let’s Encrypt certificate.
4. Enter one or more fully qualified domain names into the fields provided. The names must be defined in the domain name system (DNS) and resolve to the address of the Cisco Business Dashboard server.
5. Provide an email address to be used for urgent renewal and security notices.
6. Review the Let’s Encrypt Subscriber Agreement using the link provided and then check the box to accept the agreement.
7. Optionally check the box to share the email address with the Electronic Frontier Foundation (https://www.eff.org).
8. Click the Get Certificate button.

The Dashboard will contact the Let’s Encrypt Certificate Authority and obtain a certificate using the HTTP verification method. The page will update to show the details of the certificate along with the expiry date. The certificate will be automatically renewed approximately 30 days before expiry.

If you need to update the certificate at any point, follow these steps:

1. Navigate to **System**>**Certificate** and select the **Update Certificate** tab.
2. Select the **Let’s Encrypt Certificate** radio button.
3. Use the check-boxes and the fields provided to update the name(s) to be applied to the certificate.

   Or you can update the contact details at the bottom of the screen.

4. Click the Get Certificate button.

You can also force the certificate to be regenerated before the normal renewal time by leaving the fields on the page unchanged and clicking the Force Renewal button.

To install a Let's Encrypt certificate using the command line, do the following:

1. Log on to the host operating system using SSH or via the console.
2. Execute the **cisco-business-dashboard letsencrypt** command and specify one or more fully qualified hostnames using the **-d** option. (For example, **cisco-business-dashboard letsencrypt -d dashboard.example.com -d pnpserver.example.com**.) All names listed in the command must resolve to the IP address of the dashboard server.
3. Follow the prompts to have a certificate issued and applied to the dashboard application. The certificate will be automatically renewed by the dashboard as it approaches expiry.

Note The **Let's Encrypt** service will need to connect to the dashboard web server to verify ownership of the hostname(s). To allow this, the dashboard web server must be accessible from the Internet. See Managing Platform Settings, on page 100 for details on how to restrict access to the dashboard application to only authorized IP addresses.

Generate a Certificate Signing Request (CSR)

1. Navigate to **System**>**Certificate** and select the **CSR** tab.
2. Enter appropriate values into the fields provided in the form that is displayed. These values will be used to construct the CSR, and will be contained in the signed certificate you receive from the CA.
3. Click **Create** and the CSR will be automatically downloaded to your PC. Alternatively, you can download the CSR at a later date by clicking **Download** next to the CSR label.
4. If necessary, you can modify the CSR by returning to step 2.

Upload a New Certificate

To upload a new certificate using the administration GUI, follow the steps below.

1. Navigate to **System**>**Certificate** and select the **Update Certificate** tab.
2. Select **Upload Cert** radio button. The file containing the certificate can be dropped on the target area, or you may click the target area to browse the file system. The file should be in PEM format.

   You may also upload a certificate with the associated private key in PKCS#12 format by selecting the **Upload PKCS12** option instead. The password to unlock the file should be specified in the field provided.
3. Click **Upload** to upload the file and replace the current certificate.

To upload a new certificate using the command line, do the following:

1. Copy the certificate and private key files to the Cisco Business Dashboard file system using SCP or similar. Ensure access to these files is restricted to authorized personnel only as the private key is sensitive information.

2. Log on to the operating system using the console or SSH.
3. Apply the certificate to the dashboard application using the command: **cisco-business-dashboard importcert -t pem -k <private key file> -c <certificate file>**. The certificate and private key will be loaded into the dashboard application and replace the current certificate. For more information on this command and its options, enter **cisco-business-dashboard importcert -h**.

Note Some browsers may generate certificate warnings for certificates that have been signed by a well-known certificate authority, while other browsers accept the certificate without any warning. Network Plug and Play clients may also fail to accept the certificate. This is because the certificate authority has signed the certificate with an intermediate certificate that is not included in the browser or PnP client's trusted authorities store. In these circumstances, the certificate authority provides a bundle of certificates that must be concatenated with the server certificate before uploading to the Dashboard.

During upload, the dashboard will remove any duplicates or unnecessary certificates from the chain and attempt to assemble it in the correct order. Select the Current Certificate tab after upload to confirm that the certificate chain is complete and correctly formatted.

Regenerate the Self-Signed Certificate

To regenerate the self-signed certificate, follow the steps below.

1. Navigate to **System**>**Certificate** and select the **Update Certificate** tab.
2. Click **Renew Self-Signed Cert**. Enter appropriate values into the fields provided in the form that is displayed. These values will be used to construct the certificate.
3. Click **Save**.

View the Current Certificate

To view the current certificate, follow the steps below.

1. Navigate to **System**>**Certificate** and select the **Current Certificate** tab.
2. Each certificate in the chain of trust for the dashboard is listed in the table at the top of the screen, along with its type, subject and expiry date. For a dashboard with a self-signed certificate, there will be only one entry in the table, while a dashboard using a CA-signed certificate may have several entries.
3. Click on a row of the table to display the details of the corresponding certificate in the box below.
4. You may use the icons in the Actions column to down the root certificate in the chain or copy it to the clipboard. The root certificate may be required when configuring devices to connect to the dashboard when the certificate is self-signed or signed by a private CA.

Downloading the Current Certificate Chain

To download a copy of the current certificate chain, follow the steps below.

1. Navigate to **System**>**Certificate** and select the **Current Certificate** tab.
2. Click the **Download Certificate Chain** button at the bottom of the page. The certificate chain will be downloaded in PEM format by your browser.

Automatically Install a Certificate from Let's Encrypt

From release 2.2.1, Cisco Business Dashboard can automatically obtain and renew a domain-validated certificate from the **Let's Encrypt Certificate Authority** (https://letsencrypt.org) and in release 2.5.0, these certificates can be managed through the Administration page.

Important You must have a fully qualified domain name registered and a DNS record that points to the public IP address. Refer to Managing Platform Settings, on page 100 for more information.

To install a Let's Encrypt certificate using the administration GUI, do the following:

1. Navigate to **System**> **Certificate** and select the Update Certificate tab.
2. Select the *Let's Encrypt Certificate* radio button.
3. Check the box to enable the use of a Let's Encrypt certificate.
4. Enter one or more fully qualified domain names into the fields provided. The names must be defined in the domain name system (DNS) and resolve to the address of the Cisco Business Dashboard server.
5. Provide an email address to be used for urgent renewal and security notices.
6. Review the Let's Encrypt Subscriber Agreement using the link provided and then check the box to accept the agreement.
7. Optionally check the box to share the email address with the Electronic Frontier Foundation (https://www.eff.org).
8. Click the Get Certificate button.

The Dashboard will contact the Let's Encrypt Certificate Authority and obtain a certificate using the HTTP verification method. The page will update to show the details of the certificate along with the expiry date. The certificate will be automatically renewed approximately 30 days before expiry.

If you need to update the certificate at any point, follow these steps:

1. Navigate to **System**>**Certificate** and select the **Update Certificate** tab.
2. Select the **Let's Encrypt Certificate** radio button.
3. Use the check-boxes and the fields provided to update the name(s) to be applied to the certificate.

   Or you can update the contact details at the bottom of the screen.
4. Click the Get Certificate button.

You can also force the certificate to be regenerated before the normal renewal time by leaving the fields on the page unchanged and clicking the Force Renewal button.

To install a Let's Encrypt certificate using the command line, do the following:

1. Log on to the host operating system using SSH or via the console.
2. Execute the **cisco-business-dashboard letsencrypt** command and specify one or more fully qualified hostnames using the **-d** option. (For example, **cisco-business-dashboard letsencrypt -d dashboard.example.com -d pnpserver.example.com**.) All names listed in the command must resolve to the IP address of the dashboard server.

3. Follow the prompts to have a certificate issued and applied to the dashboard application. The certificate will be automatically renewed by the dashboard as it approaches expiry.

Note The **Let's Encrypt** service will need to connect to the dashboard web server to verify ownership of the hostname(s). To allow this, the dashboard web server must be accessible from the Internet. See Managing Platform Settings, on page 100 for details on how to restrict access to the dashboard application to only authorized IP addresses.

Managing Email Settings

The **Email Settings** page allows you to control how emails will be sent by Cisco Business Dashboard.

Access this page to set the following parameters.

Field	Description
SMTP Server	The domain name or IP address of the SMTP server that will be used.
SMTP Port	The TCP port to use for sending mail.
Email Encryption	The encryption method to use which includes the following: • None • TLS • SSL
Authentication	Enable or disable email authentication.
Username	The username to present if authentication is enabled.
Password	The password to present if authentication is enabled.
From Email Address	The email address to originate messages from.

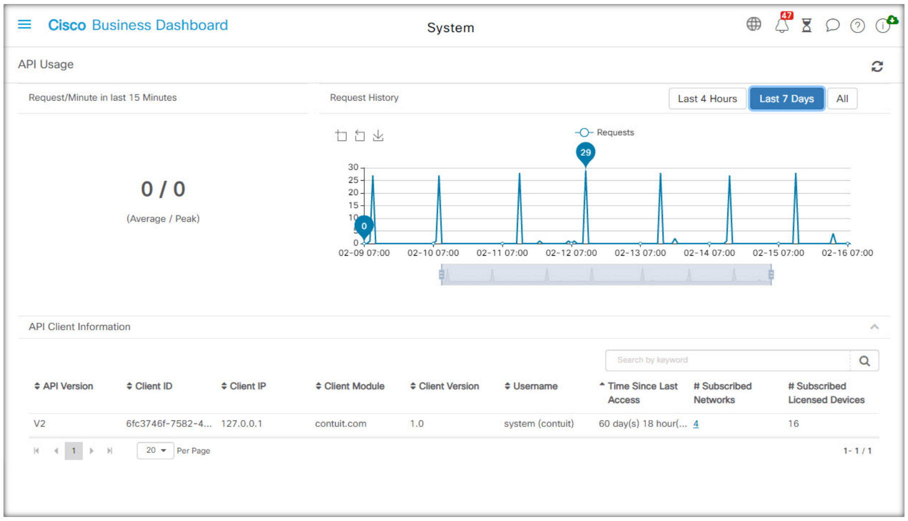
To test the configuration, click **Test Connectivity**. This will prompt for a target email address and generate a test email to the specified address.

Viewing API Usage

The API Usage page displays information about any external applications that have been integrated with the Cisco Business Dashboard. This report is divided into the following three sections:

- The **15-minute Request Monitor**—Displays the average and peak request rate over the last 15 minutes
- The **Request History** graph—Displays a graph of request activity over time. You may select time periods of the last four hours, the last seven days, or all available information. You may then use the sliders underneath the graph to narrow the focus of the graph to a particular period of interest.

- The **API Client Information** table—Lists all the clients that have used the API at least once. The following table describes the information provided in the **API Client Information** table:



API Version	Client ID	Client IP	Client Module	Client Version	Username	Time Since Last Access	# Subscribed Networks	# Subscribed Licensed Devices
V2	6fc3746f-7582-4...	127.0.0.1	contuit.com	1.0	system (contuit)	60 day(s) 18 hour(...	4	16

Field	**Description**
API Version	The version used by the client when accessing the API.
Client ID	The identifier for a particular instance of the client application.
Client IP	The IP address associated with this client. Also displays the callback URL to which the Dashboard should post event notifications when the API version is v1 and notifications have been requested.
Client Module	The type of application associated with this client.
Client Version	The version of the application associated with this client.
Username	For clients using the v1 API, this field shows the username presented by the application when authenticating to the Dashboard. For clients using the v2 API, this field shows the **Access Key ID** used by the client and the username that key is associated with.
Time Since Last Access	The time since the last activity from this client.
# Subscribed Networks	The number of networks where the application has requested event notifications. This number is a link that, when clicked, displays the Subscribed Networks table for this client. The Subscribed Networks table is described below.
# Subscribed Licensed Devices	The number of managed devices for which event notifications will be sent to this client.

To view information about the networks for which a client has requested notifications, click on the **# Subscribed Networks** link for the client in the **API Client Information** table. The**Subscribed Networks** table will be displayed for the client containing a list of the networks the client has requested notification for.

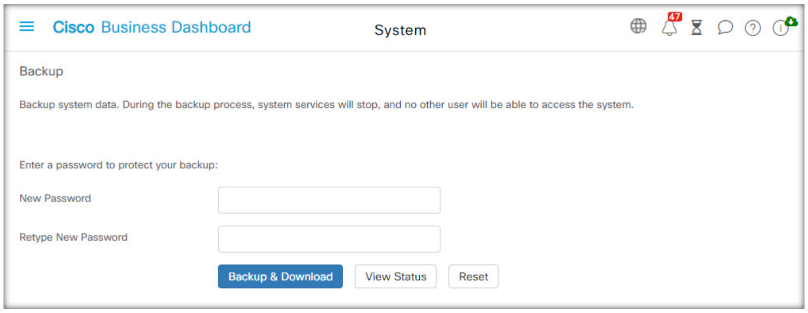
Field	Description
Network	The name of the network being monitored by the client.
# Subscribed Licensed Devices	The number of managed devices in this network for which event notifications will be sent

Backing Up and Restoring the Dashboard Configuration

The configuration and other data used by Cisco Business Dashboard can be backed up for disaster recovery purposes, or to allow the Dashboard to be easily migrated to a new host. Backups are encrypted with a password in order to protect sensitive data.

A Cisco Business Dashboard backup file may be restored to a system running the same version as the backed-up system, or up to one minor release newer. For example, a backup taken from a system running version 2.2.0 may be restored to a system running 2.3.1, but not to a system running 2.4.0.

To perform a backup, follow the steps below.



Backup

Backup system data. During the backup process, system services will stop, and no other user will be able to access the system.

Enter a password to protect your backup:

New Password

Retype New Password

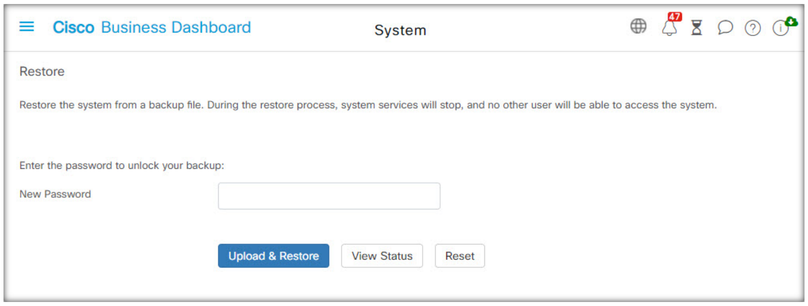
1. Navigate to **System** > **Backup**.

2. Enter a password to encrypt the backup in the **Password** and **Confirm Password** fields.

3. Click **Backup & Download**. A pop-up window will appear showing the progress of the backup. Larger systems may require some time to complete the backup, so you may dismiss the progress meter and display it again later with the **View Status** button.

When complete, the backup file will be downloaded to your PC.

To restore a configuration backup to the Dashboard, follow the steps below.



Restore

Restore the system from a backup file. During the restore process, system services will stop, and no other user will be able to access the system.

Enter the password to unlock your backup:

New Password

1. Navigate to **System** > **Restore**.

2. Enter the password that was used to encrypt the backup in the **Password** field.
3. Click **Upload & Restore** to proceed. A pop-up will appear allowing you to upload a backup file from your PC. You can drag and drop the backup file onto the target area provided, or click the target area to specify a file in your PC file system. Click **Restore** to proceed.

If the dashboard version is 2.5.0 or higher, the application will restart when the restore process completes.

Managing Platform Settings

The **Platform Settings** page allows you to modify key system settings without needing to directly access the operating system. Due to the variation in platforms supported by Cisco Business Dashboard, not all settings will be available on every platform.

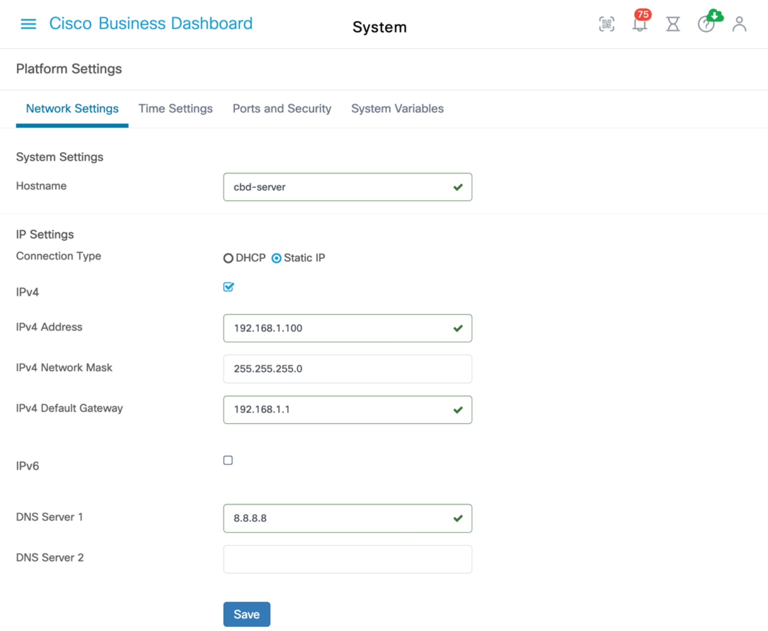
Platform settings are separated into four groups.

- Network Settings
- Time Setting
- Ports and Security
- System Variables

The following sections describe the settings available on each tab.

Changing the Hostname (Network Settings tab)

The hostname is the name used by the operating system to identify the system, and is used by Cisco Business Dashboard to identify the Dashboard when generating Bonjour advertisements.



System Settings

Hostname: cbd-server

IP Settings

Connection Type: ○ DHCP ● Static IP

IPv4: ☑

IPv4 Address: 192.168.1.100

IPv4 Network Mask: 255.255.255.0

IPv4 Default Gateway: 192.168.1.1

IPv6: □

DNS Server 1: 8.8.8.8

DNS Server 2:

To change the hostname for the Dashboard, follow the steps below.

1. Navigate to **System** > **Platform Settings**, and select the **Network Settings** tab.
2. Specify a hostname for the Dashboard in the field provided.
3. Click **Save**.

Changing Network Settings (Network Settings tab)

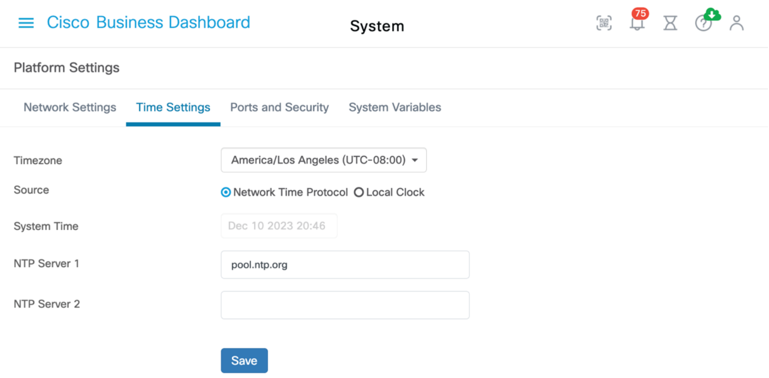
> **Note** This does not apply to Cisco Business Dashboard for AWS or Azure. To modify the network configuration, use the EC2 console in AWS for an AWS instance, and the Azure Portal for an Azure instance.

To change the network configuration for the Dashboard, follow the steps below.

1. Navigate to **System** > **Platform Settings**, and select the **Network Settings** tab.
2. Select the method for IP address assignment. The available options are DHCP (default) and Static IP. If you choose the Static IP option, then specify the address, subnet mask, default gateways and DNS servers in the appropriate fields.
3. Click **Save**

Changing Time Settings (Time Settings tab)

The **Time Settings** manage the system clock for the Dashboard. To adjust the system clock, follow the steps below.



Timezone: America/Los Angeles (UTC-08:00)
Source: ● Network Time Protocol ○ Local Clock
System Time: Dec 10 2023 20:46
NTP Server 1: pool.ntp.org
NTP Server 2:

1. Navigate to **System** > **Platform Settings**, and select the **Time Settings** tab.
2. Select the appropriate timezone for the Dashboard.
3. Select the method for time synchronization. The available options are **NTP (default)** and **Local Clock**. If the NTP option is chosen, then optionally modify the NTP servers to use for synchronization.

   If **Local Clock** is selected, the you may manually adjust the date and time using the controls provided. Alternatively, click **clock** to synchronize the time with your PC.
4. Click **Save**.

Note If the virtual machine is configured to synchronize the local clock with the host machine, any changes to the local clock done through the **Platform Settings** page will be overwritten by the hypervisor.

If the hypervisor in use is VirtualBox and the VirtualBox Guest Additions are installed in the VM, the NTP service - timesyncd - will not operate.

Changing Port Settings (Ports and Security tab)

The **Port Settings** control the TCP ports the Dashboard's user interface is hosted on. To change the default web server ports, follow the steps below.

1. Navigate to **System** > **Platform Settings**, and select the **Ports and Security** tab.
2. Change the ports used by the web server for the HTTP and HTTPS protocols.
3. Change the ports used to provide remote access to network devices through Cisco Business Dashboard.
4. Click **Save**.

Restricting Access to the Dashboard (Ports and Security tab)

You may limit the IP addresses that may access the Dashboard using the Access Control settings. You may specify different IP ranges for the Dashboard GUI, the Dashboard API, and for connections from probes and managed devices.

To limit access to the Dashboard, follow the steps below.

1. Navigate to **System** > **Platform Settings**, and select the **Web Server** tab.
2. Enter a network prefix and mask into the fields provided. If multiple prefixes are required for any section, click the **(+)**plus icon to add additional entries. Similarly, you may click the trashcan icon to remove existing entries.
3. Click **Save**.

Managing System Variables (System Variables tab)

Cisco Business Dashboard uses system variables to provide certain parameters related to the Dashboard when generating configuration templates and other tasks. Some system variables may be determined by the Dashboard automatically, but there are other variables that require user input. In particular, if the Dashboard is deployed behind a web proxy or NAT gateway, it will be necessary for the administrator to provide external addressing information for the Dashboard.

To update the external address information for the Dashboard, follow the steps below.

1. Navigate to **System** > **Platform Settings**, and select the **System Variables** tab.
2. Enter IP address and port information into the External System Settings parameters as required. If left blank, the Dashboard will use the platform address and port information for the corresponding system variable.
3. Click **Save**.

Managing Privacy

Some of the features of Cisco Business Dashboard 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. Lifecycle Reporting 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 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**.

Software Updates

Use of this feature requires Cisco Business Dashboard 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 application checks.
3. Click **Save**.

Managing Logging Settings

The **Log Settings** page allows you to control the amount of detail included in log files by the different software modules. 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 for each software module.
3. Click **Save**.

The log files for the Dashboard can be found in the directory `/var/log/ciscobusiness/dashboard/` 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.

Logging to Syslog

From release 2.2.1, Cisco Business Dashboard application logs may be sent to the host's syslog service and from there may be directed to external syslog servers.

To enable sending files to the host syslog service, follow the steps below.

1. Log on to the host operating system using SSH or via the console and edit the file `/etc/ciscobusiness/dashboard/cisco-business-dashboard-logger.conf`
2. Edit the `xxx.logger` lines to specify **file** or **syslog** or both (comma separated). The following modules are available: `redis`,`mongo` , `rabbitmq`, `nginx` and `cbd`. If `file` is specified, log messages will be directed to the default log files in the `/var/log/ciscobusiness/dashboard/` directory. If **syslog** is specified, log messages will be directed to the syslog service in the host.

Note The `mongo` module does not support multiple logging destinations. If multiple destinations are listed, the first entry takes precedence. Also, the `cbd` module will always log to the file system regardless of the presence or absence of the **file** keyword in the logger configuration.

3. Optionally, modify the `xxx.syslog.facility` lines to specify the syslog facility used for each of the modules. By default, each module logs to a separate local<*n*> facility where <*n*> ranges between 1 and 5.
4. Restart Cisco Business Dashboard using the command **cisco-business-dashboard stop** followed by **cisco-business-dashboard start**.

Once the logging configuration has been modified to direct log messages to **syslog**, the `/etc/rsyslog.conf` file should be updated to receive the logs and direct the dashboard log messages to the desired destination. For a detailed information on the configuration file, refer to https://www.rsyslog.com/doc/v8-stable/configuration/index.html.

Execute the following steps:

1. The `/etc/rsyslog.conf` file should be updated to allow log messages to be received across the loopback interface. Edit the file to include the following lines to enable this and to restrict the server to listen *only* on the loopback interface:

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514" address="::1")
input(type="imudp" port="514" address="127.0.0.1")

# provides TCP syslog reception
module(load="imtcp")
```

```
input(type="imtcp" port="514" address="::1")
input(type="imtcp" port="514" address="127.0.0.1")
```

2. Create a new file in the directory `/etc/rsyslog.d/` to contain the configuration directives specific to Cisco Business Dashboard. The file name should be of a form similar to `40-cisco-business-dashboard-syslog.conf`.
3. Edit the file created in step 2 to contain directives to send log output to the desired destinations. For example, assuming the use of the default facilities in the `cisco-business-dashboard-logger.conf` file, the following configuration would direct the warning level and above messages from the dashboard application to the syslog server with the name `logger.example.com`:

   ```
   local2.warning  @logger.example.com
   ```

4. Restart the rsyslog daemon to apply the changes using the command **sudo systemctl restart rsyslog.service**

Managing the Local Probe

Note This page is not present on Cisco Business Dashboard for AWS or Azure.

Cisco Business Dashboard Probe may be installed on the same host as Cisco Business Dashboard in order to manage devices on the network local to the Dashboard, and the Cisco virtual machine image for the Dashboard does include the Probe. If you do not wish to manage the network local to the Dashboard, you may disable the co-located Probe using the following steps:

1. Navigate to **System**>**Local Probe**.
2. Click the toggle switch to disable the local Probe.
3. Click **Save**.

To remove the Probe software entirely from the Dashboard, log on to the operating system and use the command `sudo apt-get --purge autoremove cbd-probe`. This removes the Probe software, configuration and dependencies that are not required by any other application.

Managing Integration Settings

Cisco Business Dashboard may be integrated with a variety of applications and services provided by Cisco and other vendors. When integrated with an application, data and events may be exchanged between the applications and network actions performed.

Integration is supported with the following applications and services:

- Professional Service Automation (PSA) Tools
    - Connectwise Manage
- Collaboration Tools
    - Webex

The functionality offered by each type of integration is largely common across all integrations of the same type – PSA or collaboration tool. However, some differences do exist, and you should consult the appropriate sections in Available Integrations below to see the functionality supported by each individual application. To understand the functionality supported for each class of integration, read the following sections.

Using the Professional Services Automation Tools

Three areas of functionality are available when integrating with Professional Services Automation (PSA) tools-asset management, event management and automation. Of these, event management and automation involve the user actively interacting with the functionality by creating and managing tickets. Asset management generally does not require user interaction beyond the initial setup described in the Available Integrations sections below.

Using Asset Synchronization

With asset synchronization, the inventory of network devices in Cisco Business Dashboard is automatically synchronized into the PSA as configuration records containing detailed information about the device. Accounting and billing related information is also updated as required by the PSA implementation in order to ensure that devices managed by the dashboard are correctly accounted for. For more details on what fields are updated, see the section corresponding to the PSA being used in the Available Integrations, on page 109.

The asset synchronization process happens automatically at midnight each day. In the event an immediate synchronization is needed, one can be initiated by clicking the **Sync Assets** button on the Asset Synchronization screen. This can also be done from a collaboration tool if one has been integrated with Cisco Business Dashboard.

Note The asset synchronization process typically takes several minutes, and can take much longer in larger networks.

Automating Network Actions with Automation Tickets

Automation tickets allow actions to be performed on network devices by opening specially formatted tickets.

Tickets can specify whether the action should occur immediately or during the next change window, and may optionally require an approval step prior to execution. When all the preconditions are met, Cisco Business Dashboard will execute the action specified in the ticket and the ticket is updated with the success or failure of the operation.

The creation process for automation tickets varies slightly between PSA tools. For details on creating an automation ticket for the PSA being used, consult the corresponding section of Available Integrations, on page 109.

When an automation ticket is created and is set to the **Start** state, Cisco Business Dashboard takes control of the ticket and performs the following steps:

1. CBD checks the ticket to ensure all the required information is present. If there is a problem, the internal notes are updated and the ticket is marked as **Needs Attention**.

2. If the ticket is well formed, it is checked to see if approval is required. If so, the ticket is marked as **Needs Approval** and no further action is taken until the ticket is approved.

3. The ticket is checked to see when the action should be performed. If the ticket is set to run now, the dashboard will perform the action immediately. If the action is set to run in the next change window, then a new schedule profile is created and the ticket is updated to show that a job is pending.
4. When the action is complete, the dashboard updates the notes in the ticket with the success or failure of the operation. If the action completed successfully, the ticket is closed. If the action failed, then the ticket is marked as **Needs Attention**. When the reason for the failure is addressed, the ticket can be rescheduled by changing the state back to **Start**, or closed if the action is no longer required.

Approval of automation tickets is an option that allows a degree of change control to be inserted in the automation process. By designating automation tickets to require approval, this ensures that an action is validated by a human prior to it being executed, and that validation is recorded in the ticket history.

A ticket requiring approval may be approved in one of two ways:

1. The ticket may be updated directly using the PSA interface.
2. The ticket may be approved through a collaboration tool that has been integrated with Cisco Business Dashboard. In this case, a note is added to the ticket recording the approval and the identity of the approver.

Managing Network Events with Notification Tickets

To enable the creation of tickets in response to network events, the Cisco Business Dashboard monitoring profiles must be updated to add the **Open Helpdesk Ticket** action to one or more of the notification monitors. For more information on managing monitoring profiles, see Monitoring Profiles, on page 61.

Note Cisco recommends you configure the Monitoring Profiles to ensure the average rate of 60 tickets and/or collaboration messages per hour is not exceeded on an ongoing basis. When communicating with external applications, sustained rates over this could result in API congestion and loss of events.

When a notification happens that matches a monitoring profile with **Open Helpdesk Ticket** enabled, a new ticket is opened in the notification board and associated with the configuration record for the corresponding device. The body of the ticket is updated with pertinent information about the notification.

For most notification monitors, only notification tickets may be opened. However, in the case of the firmware notification, additional options are available. When a new firmware version is discovered for a device, the ticket created can also be opened as an automation ticket which will apply the firmware update to the device during the next change window.

When configuring the firmware notification in a monitoring profile, two additional options are provided – **With Automation** and **With Approval**. If the **With Automation** checkbox is enabled, then an automation ticket will be created instead of a notification ticket. The ticket will be opened in the automation board, associated with the device configuration, and have a type set to **Upgrade Firmware to Latest**.

Finally, the subtype will be set to schedule the upgrade to occur during the next change window. If the **With Approval** checkbox is enabled, the subtype will also be set to require approval before the upgrade is scheduled.

Using the Collaboration Tools

Use of the collaboration tools with Cisco Business Dashboard falls into two main areas:

- Setting up and receiving notifications of network events.

- Interacting with Cisco Business Dashboard through the limited control interface.

The following sections describe each of these activities in more detail.

Managing Notifications of Network Events

To enable notifications to be sent to a collaboration space in response to network events, the Cisco Business Dashboard monitoring profiles must be updated to add the **Send To Collaboration Space** action to one or more notification monitors. For more information on managing monitoring profiles, see Monitoring Profiles.

Note Cisco recommends you configure the Monitoring Profiles to ensure the average rate of 60 tickets and/or collaboration messages per hour is not exceeded on an ongoing basis. When communicating with external applications, sustained rates over this could result in API congestion and loss of events.

When a notification matching a monitoring profile with **Send To Collaboration Space** enabled occurs, a message is pushed to the collaboration space. The message includes pertinent information about the notification, including notification details, and links to view the device in Cisco Business Dashboard and the associated help desk ticket if one has been created for the event.

Interacting with Cisco Business Dashboard through a Collaboration Space

When integrated with a collaboration tool, Cisco Business Dashboard provides a limited command interface using a collaboration bot that can be used to query the dashboard and take actions.

When invoking a command, the interface requires the user to mention the bot for the command to be accepted. While the interface can tolerate a certain amount of flexibility in input, it does not provide natural language processing, but is limited to a set of pre-defined commands. The table below provides a list of available commands and associated actions.

Table 9: Supported Collaboration Commands

Command	Description
Menu Help ?	Provides a list and descriptions of all the available commands.
Approvals	Provides a list of automation tickets requiring approval. This command is only available when the dashboard is integrated with a Professional Services Automation tool.
Approve <Ticket#>	Marks the specified automation ticket as approved for execution. This command is only available when the dashboard is integrated with a Professional Services Automation tool.
Assets	Initiates the asset synchronization process. This command is only available when the dashboard is integrated with a Professional Services Automation tool.

Command	Description
Firmware	Provides a list of all network devices with an available firmware update.
Upgrade <Serial#>	Schedules a firmware update for the specified device to occur during the next change window. If the dashboard is integrated with Connectwise Manage, an automation ticket requiring approval will be created for this task, or it will be scheduled directly in Cisco Business Dashboard.
Tickets	Provides a list of open tickets in the Automation and Notification boards. This command is only available when the dashboard is integrated with a Professional Services Automation tool.

Available Integrations

For details on setting up the different integrations and the information exchanged with each application, read the corresponding section below.

Connectwise Manage

Connectwise Manage is a Professional Services Automation tool (PSA) designed for use by Managed Services Providers. It includes asset management, accounting and billing, and help desk services as part of its functionality. Integrating Cisco Business Dashboard with Connectwise Manage helps you ensure that asset records are kept up to date for network devices, manage events and network actions with help desk tickets.

Supported Functionality

When integrated with Connectwise Manage, Cisco Business Dashboard offers additional functionality in three main areas: asset management, event management, and automation.

For asset management, Cisco Business Dashboard will automatically create and periodically update configuration records in Connectwise Manage for each network device managed by the dashboard. The configuration record includes information including device type and model, serial number, software information, warranty expiry date, and life-cycle information. If a device is removed from the dashboard inventory the configuration will be marked as inactive, but not deleted from Connectwise Manage.

In addition to creating configuration records, you can opt to associate network device types with specific products in Connectwise Manage and have Cisco Business Dashboard update agreements containing those products with the quantities of devices associated with that customer.

When managing network events, you can configure the Cisco Business Dashboard monitoring profiles so that the dashboard creates help desk tickets when the selected notifications occur. These notification tickets contain details of the event and are associated with the configuration record for the device that generated the notification. In the case of firmware notifications, the ticket can also be created as an automation ticket to apply the firmware update to the device during the next change window.

An automation ticket is a special ticket that results in Cisco Business Dashboard performing a network action. Automation tickets are created in a dedicated service board that the dashboard monitors and can be used to automate the following actions:

- Backup the configuration
- Upgrade to latest Firmware version
- Reboot the device
- Save the running configuration
- Delete the device

Automation tickets can be created to execute immediately, or during the next change window, and may be set to require approval before executing. The ticket will be updated with progress information during execution and the result of the action upon completion.

Prerequisites

Before you set up the Connectwise Manage integration, the following prerequisites must be met:

- If automation tickets will be used, the Connectwise Manage application must be able to establish connections to the Cisco Business Dashboard web server. In addition, Cisco Business Dashboard must have a certificate trusted by Connectwise Manage. In most cases, this means the certificate will need to be signed by a public CA. Refer to Managing Certificates, on page 92 for more details in setting up certificates for Cisco Business Dashboard.
- If the dashboard is located behind a NAT gateway or firewall, make sure the System Variables page under **System** > **Platform Settings** is populated with the host name and web server ports that the Connectwise Manage application will use to connect to the dashboard.
- A set of API Keys must be created for Cisco Business Dashboard, and must have at least the permissions listed in the table below.

Table 10: Permissions Required by the API Key

Permission	Add Level	Edit Level	Delete Level	Inquire Level
Companies				
Company Maintenance	None	None	None	All
Configurations	All	All	All	All
Finance				
Agreements	None	All	None	All
Procurement				
Product Catalog	None	None	None	All
Service Desk				
Service Tickets	All	All	All	All
System				
Table Setup	All	All	All	All

- A service board appropriate for automation tickets must be identified or created. This board has a number of setup requirements that will be applied during the integration process, and it is recommended that this board be dedicated to network operations. See the following section for more details on how this board will be set up.
- A service board appropriate for notification tickets must be identified or created. This board has no specific requirements associated with it and may be an existing, general-purpose board. The notification board may also be the same service board used for automation tickets.

Setting up the Connectwise Manage Integration

There are several steps involved in setting up the Connectwise Manage integration.

- Establish communication with the Connectwise Manage service.
- Map the Connectwise companies to Cisco Business Dashboard organizations.
- Configure the asset synchronization process.
- Select the service boards for event notification and automation.

This section describes how to perform each process of getting it all set up correctly.

Establish Communication with the Connectwise Manage Service

1. Navigate to **System**>**Integration Settings**.
2. Locate the tile representing the Connectwise Manage integration and ensure that the toggle switch is set to **Enabled**.
3. Click on the **Settings** icon to display the Connectwise Manage Settings pages, and then select the **Connection** tab.
4. Complete the fields in the form provided, and then click **Save**. See the table below for details about the requested parameters.

Table 11: Connectwise Manage Connection Parameters

Parameter	Description
API Hostname	The protocol and hostname of the Connectwise Manage service to connect to. It defaults to https://na.connectwise.net.
Company ID	The identifier for the company in Connectwise Manage. This is the same value as used when logging on to the Connectwise Manage GUI.
Public key	The public key from the API key defined in Connectwise Manage for Cisco Business Dashboard.
Private key	The private key from the API key defined in Connectwise Manage for Cisco Business Dashboard.

After clicking **Save**, Cisco Business Dashboard will test the connection, and then read the information from Connectwise Manage that is required later in the setup process. This information includes the list of companies, configuration types, products, agreement types, and service boards. If changes are made to any of this information in Connectwise Manage, click the **Refresh Connectwise Data** button on this page to re-read the data.

Map Connectwise companies to Cisco Business Dashboard organizations

After establishing the connection between Cisco Business Dashboard and Connectwise Manage, it is necessary to map organizations in Cisco Business Dashboard to companies in Connectwise Manage. Mapping companies to organizations allows network devices and events to be associated with the correct customer in Connectwise Manage. To complete the mapping, follow the steps below.

1. Navigate to **System**>**Integration Settings**.
2. Click on the **Settings** icon on the **Connectwise Manage** tile, then select the **Organization Mapping** tab.
3. Click the **Import from Connectwise** button. This will compare the list of companies with the list of organizations and create mappings when either the company name or company ID match the organization name.
4. Arbitrary mappings between companies and organizations can be made either manually or using comma-separated value (CSV) files.

To Manually Create a Mapping

1. Click the ✚ (plus) icon above the mapping table to create a new entry in the table.
2. From the drop-down lists, select the company and organization name to be mapped.

Note If the desired company name is not listed in the drop-down menu, return to the **Connect** tab and click the **Refresh Connectwise Data** button to update the list of companies.

3. Click the **Save** icon.

To Create Mappings using CSV files

1. Create a CSV file containing the desired mappings between an organization and company name.
2. Click the **Download** icon above the mapping table for a template CSV file that contains a list of the existing mappings.
3. Once the template file is updated, click the **Upload** button above the table to create the new mappings specified in the file.

To Change an Existing Mapping

1. Click the radio button next to the mapping.
2. Click the **Edit** icon.
3. Make the necessary changes.
4. Click the **Save** icon.

To Delete an Existing Mapping

1. Click the radio button next to the mapping.
2. Click the **Delete** icon.

Configure the Asset Synchronization Process

The creation of configuration records in Connectwise Manage to represent the network devices is a pre-requisite for the event management and automation functions to work. Cisco Business Dashboard will automatically create and update configuration records for each network device in organizations that are mapped to a Connectwise manage company. To set up asset synchronization, follow the steps below.

1. Navigate to **System**>**Integration Settings**.
2. Click on the Settings icon on the **Connectwise Manage** tile, then select the **Asset Synchronization** tab.
3. Click the **Create Default Configuration Types in Connectwise** button.

   This will create three configuration types – CBD Managed Router, CBD Managed Switch and CBD Managed WAP – with fields and questions appropriate for the network devices. If these configuration types already exist, they will be updated with the fields and questions.
4. Click the **Save** icon.

Every day at midnight, Cisco Business Dashboard will perform an asset synchronization for each organization that is mapped to a company. For each network device in that organization, a configuration record will be created with information about that device. If a configuration record already exists, it will be updated with any changes to the device information. The configuration record associated with a device that has been deleted from Cisco Business Dashboard will be marked as **Inactive**.

As part of the synchronization process, Cisco Business Dashboard will also do the following:

1. For each company, Cisco Business Dashboard will identify any agreements matching agreement types that you specify.
2. For each agreement Cisco Business Dashboard will identify any additions matching products that you select and associate with each device type.
3. For each of those additions, Cisco Business Dashboard will update the quantity based on the number of devices with types that have corresponding product selected.

To make this happen, do the following:

1. Navigate to **System** > **Integration Settings**.
2. Click on the **Settings** icon on the **Connectwise Manage** tile, then select the **Asset Synchronization** tab.
3. For each device type, click in the **Product** field, and select one or more products to associate with devices of this type.
4. Under the **Agreement Type** heading, select one or more agreement types to identify the agreements to be updated.
5. Click the **Save** icon.

Note If the desired product or agreement type is not listed in the drop down menus, return to the **Connect** tab and click the **Refresh Connectwise Data** button to update the lists.

Select the service boards for event notification and automation

Enable the event management and automation functionality by specifying Service Boards that should be used for each of these functions. To specify the Service Boards to use:

1. Navigate to **System** >**Integration Settings**.
2. Click on the **Settings** icon on the **Connectwise Manage** tile, and then select the **Ticket Settings** tab.
3. From the **Notification Board** drop-down menu, select the appropriate service board to use for tickets that are created in response to network events.
4. From the **Automation Board** drop-down menu, select the service board that should be monitored for automation tickets.

   Note If the desired service board is not listed in the drop down menus, return to the **Connect** tab and click the **Refresh Connectwise Data** button to update the list of service boards.

5. Click the **Save** icon.

   Cisco Business Dashboard will update the settings for the automation board in Connectwise Manage to contain the appropriate status values, types, and subtypes needed to support the automation functionality.

Additional Information for the Connectwise Manage Integration

When performing asset synchronization between Cisco Business Dashboard and Connectwise Manage, each managed device known to Cisco Business Dashboard is created as a Configuration associated with the Company that maps to the managed device's organization. The table below lists the mapping between configuration item fields and the data provided by Cisco Business Dashboard.

Table 12: Connectwise Manage Configuration Field Usage

Field	Description
Configuration Name	Set to the device host name
Configuration Details	
Type	The configuration type is set based on the device type and the mappings configured in the Asset Synchronization page.
Status	This is set to **Inactive** if the device has been deleted from the Dashboard inventory, otherwise it is set to **Active**.
Model	The model number of the device.
Serial Number	The serial number of the device.

Field	Description
Company	
Company	The company that corresponds to the organization of the device that is defined in the **Organization Mapping** page.
Notes	
Vendor Notes	Contains a note indicating the configuration was created by Cisco Business Dashboard and displays a creation time stamp.
Configuration Questions	The configuration questions contain the following information: • **The device product ID**: This field is similar to the model number but it is the identifier used when purchasing a new device. • **Software version**: This information includes the current version and the latest available version with release notes. • **Lifecycle information**: This includes details of warranty end dates and applicable end of life bulletins.
Device Details	
IP Address	The management IP address of the device.
MAC Address	The base MAC address of the device.

In Connectwise Manage, automation tickets are managed based on the ticket type, subtype, and status. To create an automation ticket in Connectwise Manage, create a new ticket with the following characteristics:

- The service board should be set to be the automation board created when setting up the integration.
- The ticket should be associated with exactly one configuration representing a network device managed by Cisco Business Dashboard.
- The type should be set to the desired action. Check the **Automation Ticket Types** table below for a list of available actions.
- The subtype should be chosen based on the desired execution time and whether approval is required. Check the **Automation Ticket Subtypes** table below for a list of available options.
- The status should be set to **Start** to begin the automation process. If additional work is required prior to automation commencing, then the status may be set to **Needs Attention** until the work is complete. Check the **Automation Ticket Status** table below for a full list of all the possible status values.

When using tickets requiring approval, neither Connectwise Manage or Cisco Business Dashboard can enforce a requirement for the approver to be a different person from the creator of the ticket. Approvers can not be restricted to a designated list of staff members. Any user who can edit the ticket or who has access to the collaboration space is able to approve a ticket. Operational processes will be necessary to implement restrictions of this kind if required.

Table 13: Automation Ticket Types

Type	Description
Backup Configuration	Take a copy of the current running configuration for the device and save it on Cisco Business Dashboard.
Delete	Remove an offline device from the Cisco Business Dashboard inventory.
Reboot	Restart the device.
Save Running Config	Save the running configuration on the device for use at startup.
Update Firmware to Latest	Upgrade the software on the device to the latest version published by Cisco.

Table 14: Automation Ticket Subtypes

Subtype	Description
Approval Required – Run During Change Window	This action requires approval and should be scheduled to occur during the next change window after the ticket has been approved.
Approval Required – Run Now	This action requires approval and should be executed immediately once the ticket has been approved.
Run During Change Window	The action should be scheduled to occur during the next change window.
Run Now	The action should be executed immediately.

Table 15: Automation Ticket Status

Status	Description
Start	Indicates to Dashboard that the ticket is ready for automation.
Needs Attention	Indicates that human intervention is required. This status may be manually set if there is work required before automation can start and will be set by the dashboard in the event the automation action failed.
In Process	The dashboard is actively processing the ticket.
Needs Approval	Indicates a valid automation ticket that requires approval to proceed. Human intervention is required to proceed.
Approved	Indicates the ticket has been approved and is ready for execution. A ticket may be approved by selecting this status in the Connectwise Manage user interface, or by an approval command in a collaboration tool that has been integrated with Cisco Business Dashboard.
Scheduled with CBD	A job has been scheduled in Cisco Business Dashboard but has not yet executed. The ticket will be updated once the job executes.
Complete (closed)	The requested action completed successfully.

Webex

Webex is a suite of collaboration tools and services that includes messaging, calling, and conferencing. Integrating Cisco Business Dashboard with Webex keeps you notified of critical network events and allows you to take action. You can use the Webex application on your desktop or mobile device.

Supported Functionality

When integrated with Webex, Cisco Business Dashboard can forward notifications to a collaboration space to inform the user of network events. You can customize the notifications through updating the monitoring profiles and then select which ones to forward.

In addition, a limited control interface is provided which allows the user to perform certain actions from the Webex interface. Supported actions include:

- View a list of open help desk tickets created by Cisco Business Dashboard.
- View a list of automation tickets requiring approval.
- Approve automation tickets.
- View a list of network devices with available firmware updates.
- Initiate a network device upgrade.

Prerequisites

Before you set up the Webex integration, you must create a Webex Bot and invite it to a collaboration space. To set up a bot, do the following:

1. Navigate to https://developer.webex.com/my-apps/new/bot and log in to your Webex account.
2. Fill out the form provided to create your bot. You need to provide a name, username, and a description for your bot. You also have the option to provide a custom icon for your bot.

Note Although Webex allows the bot name to contain white space characters, Cisco Business Dashboard requires the bot name to be a single word only with no white space.

3. Click **Add Bot** to create your bot. Take note of the bot token that is presented as you will need it when setting up the Webex integration.

Remember The bot token will only be displayed once, so it is important to record it in a safe place for future reference.

After the bot has been created, it must be invited to a collaboration space. A dedicated space be created for the purposes of interacting with Cisco Business Dashboard, but an existing space can also be used. However, any member of the space will have visibility of all events and the ability to execute all supported commands, so the space should only have users authorized to manage the network.

Consult the Webex documentation or the online help for the Webex app for details on creating spaces and inviting users.

Note: The bot should only be invited to a single collaboration space when integrated with Cisco Business Dashboard. The behavior of the bot will be unpredictable if invited to multiple spaces.

In addition to creating a bot, you should ensure that the Webex infrastructure is able to establish connections to the Cisco Business Dashboard web server. If the dashboard is located behind a NAT gateway or firewall, make sure the System Variables page under **System** > **Platform Settings** is populated with the host name and web server ports that the Webex infrastructure will use to connect to the dashboard.

Setting up the Webex Integration

To set up the Webex integration, do the following:

1. Navigate to **System**>**Integration Settings**.
2. Locate the Webex integration tile and ensure the toggle switch is set to **Enabled**.
3. Click on the **Settings** icon to display the **Webex Settings** page.
4. Copy the bot token you received when creating the bot into the field provided and click the **Save** icon.
5. Ensure that the status fields display the correct bot name and collaboration space.

Note: The bot should only be used by a single instance of Cisco Business Dashboard and not with any other applications. If multiple applications are associated with the bot, the behavior will be unpredictable.

Once Cisco Business Dashboard has been configured with the bot details, you can configure monitoring profiles to forward notifications to the collaboration space. For more details on monitoring profile configuration, see Monitoring Profiles, on page 61.

CHAPTER 11

Job Management

The section contains the following topics:

About Jobs and the Job Center

Any tasks or actions carried out by Cisco Business Dashboard 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.

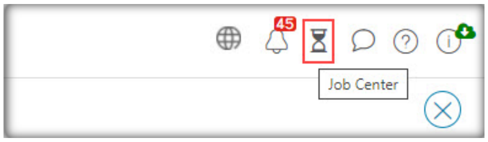
The Job Center lists all jobs that are currently executing or have occurred in the past on the **Jobs** tab, including details such as the type of job, affected devices, and the current status or whether the job completed successfully.

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.

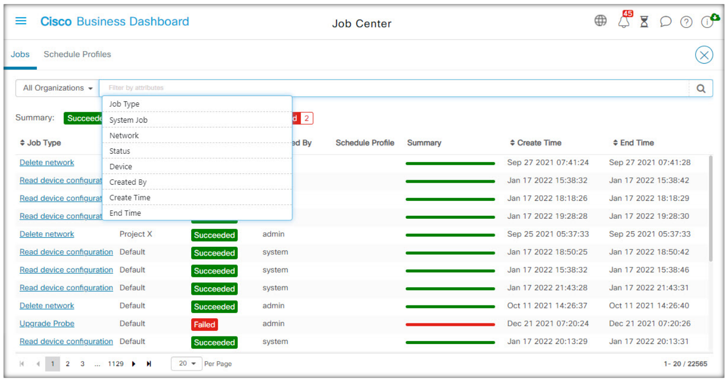
Viewing and Filtering Jobs and Schedule Profiles

To view currently active jobs, historical jobs, and schedule profiles for jobs yet to be executed, follow the steps below.

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.



Cisco Business Dashboard — Job Center

Jobs | Schedule Profiles

All Organizations ▾ | Filter by attributes

Job Type
System Job
Network
Status
Device
Created By
Create Time
End Time

Summary: Succeede… d 2

⇕ Job Type			…ed By	Schedule Profile	Summary	⇕ Create Time	⇕ End Time
Delete network					🟩	Sep 27 2021 07:41:24	Sep 27 2021 07:41:28
Read device configurat					🟩	Jan 17 2022 15:38:32	Jan 17 2022 15:38:42
Read device configurat					🟩	Jan 17 2022 18:18:26	Jan 17 2022 18:18:29
Read device configurat					🟩	Jan 17 2022 19:28:28	Jan 17 2022 19:28:30
Delete network	Project X	Succeeded	admin		🟩	Sep 25 2021 05:37:33	Sep 25 2021 05:37:33
Read device configuration	Default	Succeeded	system		🟩	Jan 17 2022 18:50:25	Jan 17 2022 18:50:42
Read device configuration	Default	Succeeded	system		🟩	Jan 17 2022 15:38:32	Jan 17 2022 15:38:46
Read device configuration	Default	Succeeded	system		🟩	Jan 17 2022 21:43:28	Jan 17 2022 21:43:31
Delete network	Default	Succeeded	admin		🟩	Oct 11 2021 14:26:37	Oct 11 2021 14:26:40
Upgrade Probe	Default	Failed	admin		🟥	Dec 21 2021 07:20:24	Dec 21 2021 07:20:26
Read device configuration	Default	Succeeded	system		🟩	Jan 17 2022 20:13:29	Jan 17 2022 20:13:31

1 2 3 ... 1129 | 20 ▾ Per Page | 1- 20 / 22565

Currently active and historical jobs are listed on the **Jobs** tab in the Job Center, while schedule profiles may be found on the Schedule Profiles tab. 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 or schedule profile to display more detailed information

Step 2 The **Filter box** limits the jobs or profiles displayed in the table. By default, all jobs and profiles 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. The following filters are available:

Table 16: Available Filters

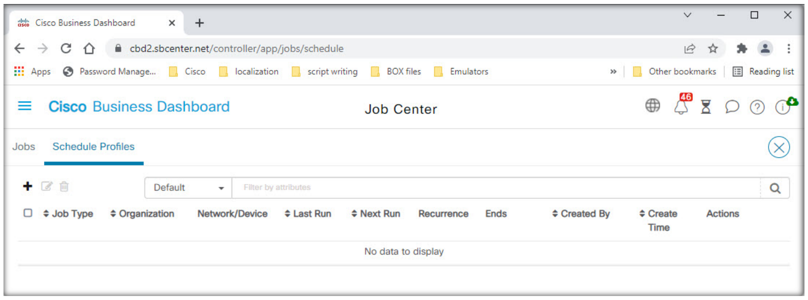
Filter	Description
Job Type	Select the type of job or profile to display from the drop-down list provided.
System Job	Use the checkbox to control whether only jobs initiated by the system are displayed, or only jobs initiated by a user. This filter is only available on the **Jobs** tab.
Status	Select a status value from the drop-down list to limit the display to only jobs in that state. This filter is only available on the **Jobs** tab.
Device	Limit the display to only jobs or profiles that affect the selected device.
Created by	Enter text in the field provided when this filter is selected. Jobs or profiles created by users matching the text entered will be displayed.
Create Time	Use the controls provided in this filter to specify a time interval. Jobs or profiles created during this interval will be displayed.
End Time	Use the controls provided in this filter to specify a time interval. Jobs that complete execution during this interval will be displayed. This filter is only available on the **Jobs** tab.
Recurrence	Select one of the supported frequencies from the drop-down list. Profiles that are set to recur with that frequency will be displayed. This filter is only available on the **Schedule Profiles** tab.
Network	Limit the display to only profiles that affect the selected network.

Filter	Description
Next Run	Use the controls provided in this filter to specify a time interval. Profiles that will next execute during this interval will be displayed. This filter is only available on the **Schedule Profiles** tab.

Managing Schedule Profiles

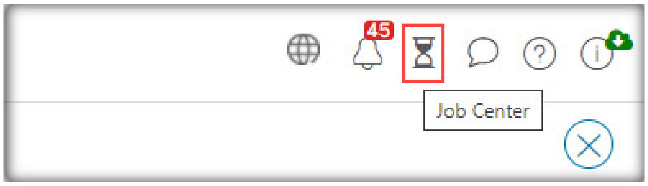
The **Schedule Profiles** tab does not just allow you to view the profiles that have been defined. You can also create new profiles and edit or delete existing profiles. You can also search for all the jobs that have been created by a profile.

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



□	⬍ Job Type	⬍ Organization	Network/Device	⬍ Last Run	⬍ Next Run	Recurrence	Ends	⬍ Created By	⬍ Create Time	Actions
					No data to display					

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, organization, and target devices or networks. Note that selected job types may not be applied to a network.

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.

   A job can also be scheduled to occur in the next change window or in each change window. The timing of the job is controlled by the change window settings applied at either the network or organization level. For more details on change windows, see Managing Change Windows, on page 122.

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 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 need to edit. You can use the filters described above 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 described above 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 described above 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.

Managing Change Windows

Change windows are periods of time that may be used to perform actions that may disrupt the network without impacting users. A change window is generally defined to occur outside working hours on a weekend or during the night but can be set to any time that suits the requirements of the organization. A change window is a recurring interval and is set by default in Cisco Business Dashboard to occur every week on Sunday between 2:00 am and 3:00 am.

Change windows are defined at the organization level but can be overwritten at the network level if required. To modify the change window for an organization, follow the steps below.

1. Navigate to **Administration**>**Organizations**.
2. Select the radio button for the organization to be modified and click the **edit** icon.
3. Click the **edit** icon next to the **Change Window Summary** parameter. A pop-up window opens allowing you to change the frequency that the change window occurs and the day and time the widow should start. By selecting the appropriate Timezone, you are able to specify the start time as a local time for the organization which reduces the potential for error. When your updates are complete, click **Save** to close the pop-up.

4. You should also set the duration of the change window. A change window may be specified in minutes or hours and must be at least 30 minutes long.

5. When you are satisfied with your changes, click **Save**. To discard any changes, click **Cancel**.

To set a change window for a particular network that is different to the change window for the organization, follow the steps below.

1. Navigate to the **Network** page.

2. Select the checkbox for the network to be modified and click **Settings** in the **Network Info** panel that appears.

3. Click the **edit** icon located at the top left next to the name of the network.

4. Under the **Change Window** heading, uncheck the **Use Organization Change Window** checkbox

5. Click the **edit** icon next to the **Change Window Summary** parameter. A pop-up window opens allowing you to change the frequency that the change window occurs and the day and time the window should start. By selecting the appropriate timezone, you are able to specify the start time as a local time for the organization which reduces the potential for error. When your updates are complete, click **Save** to close the pop-up.

6. You should also set the duration of the change window. A change window may be specified in minutes or hours and must be at least 30 minutes long.

7. When you are satisfied with your changes, click **OK**. To discard any changes, click **Cancel**.

To configure a network to use the organization change window, follow the steps below.

1. Navigate to the **Network** page.

2. Select the checkbox for the network to be modified and click the **Settings** button in the **Network Info** panel that appears.

3. Click the **edit** icon located at the top left next to the name of the network.

4. Under the **Change Window** heading, check the **Use Organization Change Window** checkbox.

5. When you are satisfied with your changes, click **OK**. To discard any changes, click **Cancel**.

CHAPTER 12

Troubleshooting

This chapter contains the following sections:

Capturing Network Diagnostic Information

The **Network Show Tech** feature allows you to easily capture diagnostic information for your network in a form which you can analyze later or send to a support engineer. A **Network Show Tech** can be generated from the Dashboard UI or directly from the Probe UI in the event you are troubleshooting problems with the Dashboard-Probe connection. To capture a **Network Show Tech**, follow the steps below.

1. Navigate to **Network** and click the check box to select the Network that you want to collect diagnostic information.

2. Select the **Actions** tab and click **Show Tech**.

   Alternatively, log on to the Probe UI and navigate to **Troubleshooting** > **Network Show Tech**.

3. Use the check boxes to control whether or not to exclude passwords and certificates from device configurations, and where the diagnostic information should be sent. The following options are available:

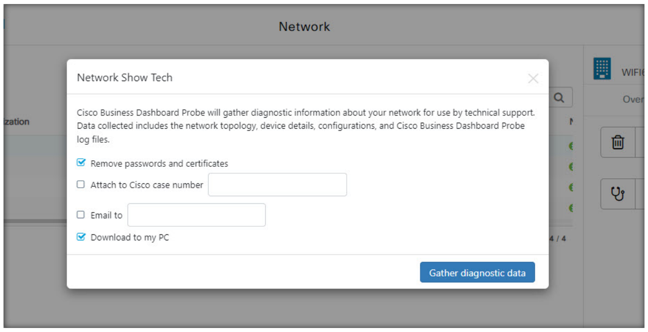
   - Attach the diagnostic information to an existing Cisco support case. To do this, enter the case number in the field provided.

   - Send the diagnostic information using email. Enter a comma-separated list of email addresses in the field provided.

   - Download the diagnostic information to your PC.

   If you are generating the **Network Show Tech** from the Probe, you do not have the options to email or attach to a support case. You must download the diagnostic information to your PC.

4. Click **Gather diagnostic data**.



Network Show Tech

Cisco Business Dashboard Probe will gather diagnostic information about your network for use by technical support. Data collected includes the network topology, device details, configurations, and Cisco Business Dashboard Probe log files.

☑ Remove passwords and certificates

□ Attach to Cisco case number

□ Email to

☑ Download to my PC

Gather diagnostic data

The diagnostic information is delivered as a zip file, and includes a basic web page to help navigate the collected data. To access the data, follow the steps below.

1. Unzip the diagnostic information file to your PC.
2. Use a web browser to open the index.html file located in the directory.

Managing Probe Log Settings

Log Settings for a Probe can be managed from the Dashboard UI or directly from the Probe UI in the event you are troubleshooting problems with the Dashboard-Probe connection. Log settings control what information the Probe will retain in its log files.

This information is important to support engineers diagnosing problems with Cisco Business Dashboard.

To change the log settings for a given network follow the steps below.

1. Open the **Network** page and click the check box next to the network that you want to change the settings.
2. Click the **Settings** button at the top of the Network overview panel.
3. Select the **Log Settings** tab.

   Alternatively, log on to the Probe UI and navigate to **Administration** > **Log Settings**.

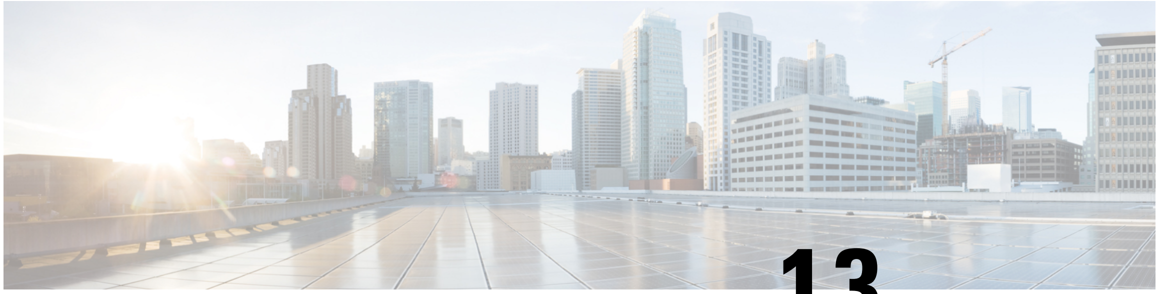
The available settings include the following parameters:

Table 17: Log Settings

Field	Description
Log Level	The level of detail that should be logged. • **Error**—Error level messages only • **Warning**—Warnings and errors • **Info**(default)—Informational messages and above • **Debug**—all messages including low level debugging messages

Field	Description
Log Module	The module(s) for which messages should be logged. • **All (default)**—All modules • **Call-home Agent**—Communication between the Probe and Dashboard • **Discovery**—Device discovery events and topology discovery • **Northbound** —Communication between the Dashboard and the Probe • **Services**—Message translation between northbound and southbound • **Southbound**—Low level communication between the Probe and devices • **System**—Core system process not covered by any other module You can select multiple modules as needed.

The Probe log files are included in the **Network Show Tech** content. For more details on **Network Show Tech** option, see Capturing Network Diagnostic Information, on page 125 section.



CHAPTER 13

Frequently Asked Questions

This chapter answers frequently asked questions about the Cisco Business Dashboard features and issues that may occur. The topics are organized into the following categories:

General FAQs

Q. What languages are supported by the Cisco Business Dashboard?

A. Cisco Business Dashboard is translated into the following languages:

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

Discovery FAQs

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

A. Cisco Business Dashboard 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*)
- Simple Network Management Protocol (SNMP)
- RESTCONF (See *https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/)*
- Proprietary web services APIs

Q. How does Cisco Business Dashboard discover my network?

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

Q. Does Cisco Business Dashboard do network scans?

A. The Cisco Business Dashboard Probe does not actively scan the broader network. The Probe will use the ARP protocol to scan the IP subnet it is directly attached to, but will not attempt to scan any other address ranges. The Probe will also test each discovered device for the presence of a webserver and SNMP server on the standard ports.

For direct managed networks, you may optionally create a schedule profile to actively scan designated IP ranges for manageable devices. If this is done, then the dashboard will attempt to connect to webserver ports on each IP address in the specified ranges to determine if a device is manageable.

Configuration FAQs

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

A. New devices will be added to the default device group. If configuration profiles have been assigned to the default device group, then that configuration will be applied to newly discovered devices.

Q. What happens when I move a device from one device group to another?

A. Any VLAN or WLAN configuration associated with profiles that are currently applied to the original device group that are not also applied to the new device group will be removed, and VLAN or WLAN configuration associated with profiles that are applied to the new group that are not applied to the original group will be added to the device. System configuration settings will be overwritten by profiles applied to the new group. If no system configuration profiles are defined for the new group, then the system configuration for the device will not change.

Security Consideration FAQs

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

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

Table 18: Cisco Business Dashboard - Protocols and Ports

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to the Dashboard. SSH is disabled by default on the Cisco virtual machine image.
TCP 80	Inbound	HTTP	Web access to the Dashboard. Redirects to secure web server (port 443).
TCP 443	Inbound	HTTPS Multiplexed TCP	Secure web access to the Dashboard Communication between Probe and Dashboard.
UDP 1812	Inbound	RADIUS	Device access to the Dashboard when authenticating user access.
TCP 50000 - 51000 (Systems deployed from the Microsoft Azure marketplace use TCP 50000 - 50049)	Inbound	HTTPS	Remote access to devices. This range may be controlled using the System > Platform Settings page.
UDP 53	Outbound	DNS	Domain name resolution.
UDP 123	Outbound	NTP	Time synchronization.
TCP 443	Outbound	HTTPS	Access Cisco web services for information such as software updates, support status, and end of life notices. Access OS and application update services.
UDP 5353	Outbound	mDNS	Multicast DNS service advertisements to the local network advertising the Dashboard.

Q. What port ranges and protocols are required by Cisco Business Dashboard Probe?

A. The following table lists the protocols and ports used by Cisco Business Dashboard Probe:

Table 19: Cisco Business Dashboard - Protocols and Ports

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to the Probe. SSH is disabled by default on the Cisco virtual machine image.
TCP 80	Inbound	HTTP	Web access to the Probe. Redirects to secure web server (port 443).

Port	Direction	Protocol	Usage
TCP 443	Inbound	HTTPS	Secure web access to the Probe.
UDP 5353	Inbound	mDNS	Multicast DNS service advertisements from the local network. Used for device discovery.
UDP 53	Outbound	DNS	Domain name resolution.
UDP 123	Outbound	NTP	Time synchronization
TCP 80	Outbound	HTTP	Management of devices without secure web services enabled.
UDP 161	Outbound	SNMP	Management of network devices.
TCP 443	Outbound	HTTPS Multiplexed TCP	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. Access OS and application update services. Communication between Probe and Dashboard.
UDP 5353	Outbound	mDNS	Multicast DNS service advertisements to the local network advertising the Probe.

Q. What Cisco servers does Cisco Business Dashboard communicate with and why?

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

Table 20: Cisco Business Dashboard - Cisco Servers

Hostname	Purpose
tools.cisco.com	Used by Smart Licensing to verify that sufficient licenses are available for the dashboard in your Smart Account. This server is only used if the dashboard instance is registered with Cisco Smart Licensing.
api.cisco.com 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.

Hostname	Purpose
dl.cisco.com download-ssc.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.
cloudsso.cisco.com id.cisco.com	Used to authenticate Cisco Business Dashboard prior to communicating with api.cisco.com. This server is only used if software updates or lifecycle reporting are enabled in **System > Privacy Settings**.
www.cisco.com	Used to retrieve updates to the root certificate authority signing certificates used to verify X509 certificates used by Cisco and third-party services to secure network communication.

Q. What processes and system services are required by Cisco Business Dashboard?

A. The following table lists the processes and system services used by Cisco servers that Cisco Business Dashboard:

Table 21: Cisco Business Dashboard - Processes and System Services

Process	Additional Details
Dashboard Essential Processes	
/usr/lib/jvm/java-x-openjdk-amd64/bin/java … -jar /usr/lib/ciscobusiness/dashboard/lib/nm-aio-application-x.x.x-SNAPSHOT.jar	The main dashboard application
/usr/lib/ciscobusiness/dashboard/bin/nginxsvc /usr/lib/ciscobusiness/dashboard/bin/nginx	Web Server
/usr/lib/ciscobusiness/dashboard/bin/mongosvc /usr/lib/ciscobusiness/dashboard/bin/mongod /usr/lib/postgresql/xx/bin/postgres postgres: xx/main:	Database services
/bin/bash /usr/lib/ciscobusiness/dashboard/bin/freeradiussvc /usr/lib/ciscobusiness/dashboard/bin/freeradius	User authentication services
/usr/lib/ciscobusiness/dashboard/bin/redissvc /usr/lib/ciscobusiness/dashboard/bin/redis-server	In-memory cache services
/usr/lib/ciscobusiness/dashboard/bin/rabbitmqsvc /usr/lib/ciscobusiness/dashboard/bin/rabbitmq-server /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd /usr/lib/erlang/erts-xx.x.x.xx/bin/epmd.smp erl_child_setup	Message broker

Process	Additional Details
Dashboard Essential Processes	
/usr/lib/ciscobusiness/dashboard/bin/bonjoursvc avahi-publish	Multicast DNS announcements
Dashboard Essential System Services	
/usr/sbin/rsyslog	Logging services
/usr/sbin/cron	Scheduling services
systemd-timesyncd	Time services
avahi-daemon	Multicast DNS listener

Q. What processes and system services are required by Cisco Business Dashboard Probe?

A. The following table lists the processes and system services used by Cisco servers that Cisco Business Dashboard Probe:

Table 22: Cisco Business Dashboard - Processes and System Services

Process	Additional Details
Probe Essential Processes	
/usr/lib/ciscobusiness/probe/bin/cbdprobe chagent	The main probe application
/usr/lib/ciscobusiness/probe/bin/fpscan	Device scanning tool
/usr/lib/ciscobusiness/probe/bin/main /usr/lib/ciscobusiness/probe/bin/publish avahi-publish	Multicast DNS announcements
nginx	Web server When collocated on a dashboard server, the probe shares the dashboard web server
Probe Essential System Services	
/usr/sbin/rsyslogd	Logging services
/usr/sbin/cron	Scheduling services
systemd-timesyncd	Time services
avahi-daemon	Multicast DNS listener

Process	Additional Details
Probe Essential Processes	
lldpd	LLDP neighbor discovery

Q. How secure is the communication between Cisco Business Dashboard and a Probe?

A. All communication between the Dashboard and the Probe is encrypted using a TLS 1.2 session authenticated with client and server certificates. The session is initiated from the Probe to the Dashboard. At the time the association between the Dashboard and Probe is first established, the user must either log on to the Dashboard via the Probe.

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

A. No. When Cisco Business Dashboard discovers a supported device, it will attempt to access the device using the factory default credentials for that device with the username and password: `cisco`, or the SNMP community:`public`. If the device configuration has been changed from the default, then it will be necessary for the user to supply correct credentials to Cisco Business Dashboard.

Q. How secure are the credentials stored in Cisco Business Dashboard?

A. Credentials for accessing Cisco Business Dashboard are irreversibly hashed using the SHA512 algorithm. Credentials for devices and other services, such as the **Cisco Active Advisor**, are reversibly encrypted using the AES-128 algorithm.

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

A. If you have lost the password for all the admin accounts in the web UI, you can recover the password by logging on the console of the Probe and running the **cbdprobe recoverpassword** tool, or logging on the console of the Dashboard and running the **cisco-business-dashboard recoverpassword** tool. 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. Following is an example of the commands to be provided in order to recover the password using this tool.

```
cisco@cisco-business-dashboard:~$ cisco-business-dashboard recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword Cisco Business Dashboard successful!
cisco@cisco-buisness-dashboard:~$
```

Note When using Cisco Business Dashboard for AWS, the password will be set to the AWS instance ID.

Q. What is the default username and password for the Virtual Machine bootloader?

A. The default credentials for the Virtual Machine bootloader are username: **root** and password: **cisco**. These may be changed by running the config_vm tool and answering yes when asked if you want to change the bootloader password.

Q. How does the dashboard authenticate network access devices?

A. The dashboard uses two levels of authentication.

- First, the source IP address of the incoming request is compared with the external IP address(es) of the networks managed by the dashboard when NAT is in use, or the internal subnets of the networks when there is no NAT in use.

- Second, a unique, randomized RADIUS secret is created for each organization and must be used by the network access device in its request.

Remote Access FAQs

Q. When I connect to a device’s administration interface from Cisco Business Dashboard, is the session secure?

A. Cisco Business Dashboard tunnels the remote access session between the device and the user. The protocol used between the Probe and the device will depend on the end device configuration, but Cisco Business Dashboard will always establish the session using a secure protocol if one is enabled (e.g. HTTPS will be preferred over HTTP). If the user is connecting to the device via the Dashboard, the session will pass through an encrypted tunnel as it passes between the Dashboard and the Probe, regardless of the protocols enabled on the device. The connection between the user's web browser and the Dashboard will always be HTTPS.

Q. Why does my remote access session with a device immediately log out when I open a remote access session to another device?

A. When you access a device via Cisco Business Dashboard, the browser sees each connection as being with the same web server (the Dashboard) and so will present cookies from each device to every other device. If multiple devices use the same cookie name, then there is the potential for one device’s cookie to be overwritten by another device. This is most often seen with session cookies, and the result is that the cookie is only valid for the most recently visited device. All other devices that use the same cookie name will see the cookie as being invalid and will logout the session.

Q. Why does my remote access session fail with an error like the following? **Access Error: Request Entity Too Large HTTP Header Field exceeds Supported Size**

A. After doing many remote access sessions with different devices, the browser will have a large number of cookies stored for the Dashboard domain. To work around this problem, use the browser controls to clear cookies for the domain and then reload the page.

Software Update FAQs

Q. How do I keep the Dashboard operating system up to date?

A. The Dashboard uses the Ubuntu Linux distribution for an operating system. The packages and kernel may be updated using the standard Ubuntu processes. For example, to perform a manual update, log on to the console as the cisco user and enter the commands `sudo apt-get update` and `sudo apt-get upgrade`. The system should not be upgraded to a new Ubuntu release, and it is recommended that no additional packages should be installed beyond those included in the virtual machine image supplied by Cisco, or those installed as part of a minimal Ubuntu install.

Q. How do I update Java on the Dashboard?

A. Cisco Business Dashboard uses the OpenJDK packages from the Ubuntu repositories. OpenJDK will automatically be updated as part of the updating the core operating system.

Q. How do I keep the Probe operating system up to date?

A. Cisco Business Dashboard uses the Ubuntu Linux distribution for an operating system. The packages and kernel may be updated using the standard Ubuntu processes. For example, to perform a manual update, log on to the console as the cisco user and enter the commands `sudo apt-get update` and `sudo apt-get upgrade`. The system should not be upgraded to a new Ubuntu release, and it is recommended that no additional packages should be installed beyond those included in the virtual machine image supplied by Cisco, or those installed as part of a minimal Ubuntu install.

Q. How do I keep the Probe operating system up to date when using a Raspberry Pi?

A. The Raspbian packages and kernel may be updated using the standard processes used for Debian-based Linux distributions. For example, to perform a manual update, log on to the console as the cisco user and enter the commands `sudo apt-get update` and `sudo apt-get upgrade`. The system should not be upgraded to a new Raspbian major release. It is recommended that no additional packages are installed beyond those installed as part of the 'Lite' version of the Raspbian distribution and those that are added by the Probe installer.

Q. I see that Cisco Business Dashboard 2.3.0 add support for Ubuntu 20.04 (Focal Fossa). If I have upgraded my system to 2.3.0, can I upgrade the operating system from Ubuntu 16.04 to Ubuntu 20.04?

A. Unfortunately the changes between the two operating system releases are too great to allow an in-place upgrade. If you have an existing system running Ubuntu 16.04, you should upgrade the dashboard to release 2.3.0, and then take a backup of the dashboard using the **System** > **Backup page**. Then either rebuild your dashboard using Ubuntu 20.04 or create a new dashboard install based on Ubuntu 20.04. You may then restore the backup from the old dashboard to the new dashboard.

Q. I see that Cisco Business Dashboard 2.7.0 adds support for Ubuntu 22.04 (Jammy Jellyfish). If I have upgraded my system to 2.7.0, can I upgrade the operating system from Ubuntu 20.04 to Ubuntu 22.04?

A. Unfortunately, the changes between the two operating system releases are too great to allow an in-place upgrade. If you have an existing system running Ubuntu 20.04, you should upgrade the dashboard to release 2.7.0, and then take a backup of the dashboard using the **System** > **Backup** page. Then either rebuild your dashboard using Ubuntu 22.04 or create a new dashboard install based on Ubuntu 22.04. You may then restore the backup from the old dashboard to the new dashboard.

APPENDIX A

Appendix A: Managing Configuration Templates

The section contains the following topics:

Managing Configuration Templates

Configuration templates can be used when there are multiple devices that have very similar configuration requirements, contain a small number of parameters that need to be different for each device. For example, a network may use identical configuration for all switches, except that each switch has a unique hostname and management IP address. Configuration templates allow you to have a single configuration file containing all the common configuration, with placeholders for the elements of the configuration that need to be unique.

There are two parts to a configuration template – the configuration itself, and the metadata that controls how the placeholders are presented in the user interface when a device record is being created. The following sections describe each of these pieces in detail.

Configuration Syntax

The configuration part of a configuration template is a text document that is very similar to a regular device configuration. When creating a configuration template, the recommended approach is to start from a configuration backup taken from a sample device that is already configured with the features and settings that the template should enable. A configuration template differs from a device configuration in that device-specific parameters – such as a hostname – are replaced with placeholders.

When you create a new device record, you are presented with a form allowing you to supply the correct values for each of the placeholders in the configuration template. These values are merged with the configuration template to generate the actual configuration that will be sent to the device.

Note The placeholder values are merged with the configuration template when the configuration is being sent to the device. This means the final device configuration may be different from that shown in the preview if any system variables change before the device connects to the Manager.

Configurations are created as Mustache templates *https://mustache.github.io/*. Mustache allows a variety of placeholders – referred to as tags in the Mustache documentation – to be used, including:

- Simple variables, where the placeholder is replaced with the value specified in the device record. A simple variable has the form **{{name}}**.
- Sections, where the placeholder encloses a block of configuration – optionally including other placeholders. The content of the section may be excluded from the final configuration, included once or repeated several times.

  The behavior of this type of placeholder is defined by the metadata in the template and the values that the user provides when creating a device record.

  A section has the form **{{#name}}…{{/name}}** where the first tag marks the beginning of the block and the second tag marks the end.
- Comments can be used to document the configuration template. A comment has the form {{**! This is a comment**}}.

Following is an example of a simple template:

```
!
hostname {{hostname}}
!
{{! Insert a list of VLANs}}
{{#vlans}}
interface vlan {{vlan-id}}
 name {{vlan-name}}
!
{{/vlans}}
```

In this example, there are several different placeholders:

- **{{hostname}}** is a simple variable. It will be replaced by the value set for the hostname in the device record.
- There is a comment placed just after the hostname configuration. The comment will not be included in the configuration sent to the device.
- **{{#vlans}}…{{/vlans}}** is a section that is used in this example to hold a list of individual VLANs. For each VLAN defined in the device record, a copy of the contents of this container will be created in the device configuration.
- **{{vlan-id}}** and **{{vlan-name}}** are both simple variables, but they are contained within the {{#vlans}} list. When the device record is created, you may specify multiple values for **{{vlan-id}}** and **{{vlan-name}}** and they will be used to generate the configuration required to create each of those VLANs.

For more details on the Mustache syntax, consult the Mustache man page at *https://mustache.github.io/mustache.5.html*.

Template Metadata

Each configuration template contains metadata that describes how each placeholder should be presented to the user when device records are being created. This metadata is generated when creating templates using the template editor.

When you create or edit a configuration template, the template editor is displayed with the configuration itself displayed on the left and a form on the right that allows you to set the metadata for each placeholder.

Each placeholder in the configuration is shown on the right, along with the following controls:

- A **Required** checkbox. This control determines whether the user must provide a value for this placeholder or not.
- A **Type** drop-down list. This allows you to select the type of placeholder, which controls how that placeholder is displayed to the user.
- A **Title**. This may be used to provide a more user-friendly name for the parameter on the GUI. If a title is not specified for a placeholder, then the placeholder itself with be displayed.
- An **Edit** icon. Certain types have more settings available to control presentation. For example, a string placeholder may be further refined to be an IP address or URL, and the input form will display an error if the text entered does have the correct format. Certain types can also be set based on system information rather than user input. See System and Dynamic Variables below for more details.
- **Move up/down** controls. These arrows allow you to change the order in which placeholders are displayed to the user. Placeholders may be grouped based on what makes the most sense to the user, rather than the order in which they appear in the configuration.

The template editor also provides a preview function which may be used to provide an example of how the placeholders form will appear to the user when creating and editing device records.

Placeholder Types

The following placeholder types are available:

- **String** – Placeholders of this type will be shown in the GUI as a simple text input box.
- **Integer** – Integers are displayed as a text input box with controls to increase or decrease the value of the number displayed. Only numbers may be entered into this field.
- **Boolean** – A Boolean placeholder is displayed in the GUI as a checkbox. If the checkbox is checked, the placeholder be set to the string value ‘true’. If the checkbox is unchecked, the value is ‘false’. A section may also be designated as a boolean, in which case the configuration contained within the section will only be included when the checkbox for the section is checked.
- **Container** – The Container type may be used to group other placeholders in the form.
- **List** – A list is a container or section of configuration that may be repeated multiple times in a generated configuration file. When form elements are generated for the placeholders inside a list, additional controls are added to add or remove elements in the list.

In addition to the simple types listed above, string variables can be further refined by clicking the **edit** icon. Options available include:

- Specifying a default value for the placeholder.
- Setting the minimum and/or maximum length for string placeholders.
- Specifying a pre-defined list of choices that may be selected (using the Enum option).
- Constraining the format of a string to be one of a hostname, URI, IPv4 address or IPv6 address. A string may also be designated as a text area if there is likely to be a significant amount of content to enter.

System and Dynamic Variables

Placeholders can not only take their values from user input, but can also take their values from parameters defined within the system. System variables are parameters that have been defined for the Manager itself – such as the Manager IP address.

By setting a placeholder to take its value from a system variable, the Manager will insert that value into the configuration without any user intervention. Some more complex deployments may require user input for the System Variables to work correctly. See Managing Platform Settings, on page 100 for more details.

Dynamic variables are similar to System variables, but the values generated dynamically are based on information such as the logged in user, or the device group the device belongs to. System and Dynamic variables are used to allow templates to be more portable between devices and systems.

Creating Configuration Templates

The recommended approach to creating config templates is to start by configuring a network device of the appropriate type with the desired settings, then take a backup of the device configuration and upload it to the Manager to use as a starting point.

Alternatively, you can create a copy of an existing template using the ‘Save As’ function. Either way, starting from an existing configuration can help reduce the time taken to create a template and also to reduce the number of revisions required to achieve the desired result.

When creating a new template, you will need to specify an organization that the template will belong to and the Product IDs (PIDs) that the template may be used with. The Product IDs may contain a ***'s** and **?'s** as wildcard characters.

Once you have your starting configuration created, you may update it using the following process:

1. Navigate to **Network Plug and Play** > **Configurations**,

2. Open your starting configuration in the template editor by selecting the configuration and clicking the **edit** icon.

   The template editor is displayed with the initial configuration file displayed on the left in a text editor window. The text editor supports many common editing functions including search, replace, and several cursor manipulation key sequences. See the table below for a list of commands.

3. Modify the configuration by inserting placeholders as described in Configuration Syntax, on page 139. Each time a new placeholder is inserted, a corresponding entry is added to the form on the right.

4. Modify the metadata associated with each placeholder using the form on the right to ensure that the placeholder is presented to the user in the most appropriate way. See Managing Configuration Templates, on page 139 above for more details on specifying metadata. You can use the Preview function to see how the form will be presented to the user when a device record is being created.

5. Repeat steps 3 and 4 until you have created placeholders for all of the configuration parameters that should vary between devices.

6. Once the template has been completed to your satisfaction, click **Save**.

Note Each time a template is saved, a new version of the template is created. Older versions of templates are retained in the Manager unless you explicitly delete them. When a template is assigned to a device, a specific version of the template is assigned – the latest version by default. As new versions are created, existing devices will continue to use the version that was assigned when they were created. A template version that is currently assigned to a device may not be deleted.

Table 23: Common Editor Commands

Function	Description	Key Bindings	
		PC	Mac
Select All	Select the whole content of the editor.	Ctrl-A	Cmd-A
Kill Line	Deletes the part of the line after the cursor. If that consists only of whitespace, the newline at the end of the line is also deleted.		Ctrl-K
Delete Line	Deletes the whole line under the cursor, including newline at the end.	Ctrl-D	Cmd-D
Undo	Undo the last change.	Ctrl-Z	Cmd-Z
Redo	Redo the last undone change.	Ctrl-Y	Shift-Cmd-Z Cmd-Y
Go Doc Start	Move the cursor to the start of the document.	Ctrl-Home	Cmd-Up Cmd-Home
Go Doc End	Move the cursor to the end of the document.	Ctrl-End	Cmd-End Cmd-Down
Go Line Start	Move the cursor to the start of the line.	Alt-Left	Ctrl-A
Go Line End	Move the cursor to the end of the line.	Alt-Right	Ctrl-E
Indent More	Indent the current line or selection.	Ctrl-]	Cmd-]
Indent Less	Outdent the current line or selection.	Ctrl-[	Cmd-[
Find		Ctrl-F	Cmd-F
Find Next		Ctrl-G	Cmd-G
Find Prev		Shift-Ctrl-G	Shift-Cmd-G
Replace		Shift-Ctrl-F	Cmd-Alt-F
Replace All		Shift-Ctrl-R	Shift-Cmd-Alt-F