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 1: 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 2: 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 3: 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 4: 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 5: 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.