Cisco Business Dashboard Frequently Asked Questions

Objective

This article contains the answers to frequently asked questions in setting up, configuring, and troubleshooting Cisco Business Dashboard Network Management.

> ⓘ Note:
> **Licensing Update:** Effective with Cisco Business Dashboard version 2.11.1, paid licenses are no longer required to manage more than 25 network devices. This update simplifies your deployment by removing the need for license procurement for core management features, regardless of your network size.
> There are **NO** changes regarding support for CBD.

Introduction

Cisco Business Dashboard Network Management is software that allows you to easily manage your whole network including your Cisco devices through your web browser. It automatically discovers, monitors, and configures all supported Cisco devices in your network. This software also sends you notifications about firmware updates and information about the devices in your network that are no longer supported by warranty.

Frequently Asked Questions

Table of Contents

General

1. **What languages are supported by the Cisco Business Dashboard Network Management?**

Discovery

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

3. **How does Cisco Business Dashboard discover my network?**

4. **Does Cisco Business Dashboard do network scans?**

Configuration

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

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

Security Considerations

7. **What port ranges and protocols are required by the Cisco Business Dashboard Network Manager?**

8. **What port ranges and protocols are required by Cisco Business Dashboard Network Probe?**

9. **How secure is the communication between Cisco Business Dashboard and Cisco Business Dashboard Probe?**

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

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

12. **How do I recover a lost password for the Web User Interface (UI)?**

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

Remote Access

14. **When I connect to the Web UI of a device from Cisco Business Dashboard Network Management, is the session secure?**

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

16. **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?**

Software Update

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

18. **How do I update Java on the Dashboard?**

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

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

General

1. What languages are supported by the Cisco Business Dashboard Network Management?

Cisco Business Dashboard Network Management is translated into the following languages:

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

Discovery

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

Cisco Business Dashboard uses a variety of protocols to discover and manage the network. The exact protocol being used for a particular device varies depending on the device type. These protocols include:

- Multicast Domain Name System (mDNS) and DNS Service Discovery — This protocol is also known as Bonjour. It locates devices such as printers, other computers, and the services that those devices offer on a local network. To learn more about mDNS, click **here**. For more information on DNS Service Discovery, click **here**.
- Cisco Discovery Protocol (CDP) — A Cisco proprietary protocol used to share information about other directly connected Cisco equipment, such as the operating system version and IP address.
- Link Layer Discovery Protocol (LLDP) — A vendor neutral protocol used to share information about other directly connected equipment, such as the operating system version and IP address.
- Simple Network Management Protocol (SNMP) — A network management protocol used for collecting information and configuring network devices such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.
- RESTCONF — An Internet Engineering Task Force (IETF) draft that describes how to map a Yet Another Next Generation (YANG) data modeling language specification to a RESTful interface. To know more, click **here**.

3. How does Cisco Business Dashboard discover my network?

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 and LLDP adjacency tables, Media Access Control (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.

4. Does Cisco Business Dashboard do network scans?

Cisco Business Dashboard 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.

Configuration

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

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 also be applied to newly discovered devices.

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

Any Virtual Local Area Network (VLAN) or Wireless Local Area Network (WLAN) configuration associated with profiles that are currently applied to the original device group and are not applied to the new device group will be removed, and VLAN or WLAN configuration associated with profiles that are applied to the new group and 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

7. What port ranges and protocols are required by the Cisco Business Dashboard Network Manager?

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

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 Dashboard. Communication between Probe and Dashboard.
TCP 50000 - 51000	Inbound	HTTPS	Remote access to devices.
TCP 53	Outbound	DNS	Domain name resolution.
UDP 123	Outbound	NTP	Time synchronization.
TCP443	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 local network advertising the Manager

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

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

Port	Direction	Protocol	Usage
TCP 22	Inbound	SSH	Command-line access to Probe. SSH is disabled by de on the Cisco virtual machine image.
TCP 80	Inbound	HTTP	Web access to Probe. Redirects to secure web server (443)
TCP 443	Inbound	HTTPS	Secure web access to Probe.
UDP 5353	Inbound	mDNS	Multicast DNS service advertisements from the 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 enab
UDP 161	Outbound	SNMP	Management of network devices
TCP 443	Outbound	HTTPS Multiplexed TCP	Management of devices with secure web services enab Access Cisco web services for information such as softw 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 netw advertising the Probe.

9. How secure is the communication between Cisco Business Dashboard Network Manager and Cisco Business Dashboard Probe?

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.

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

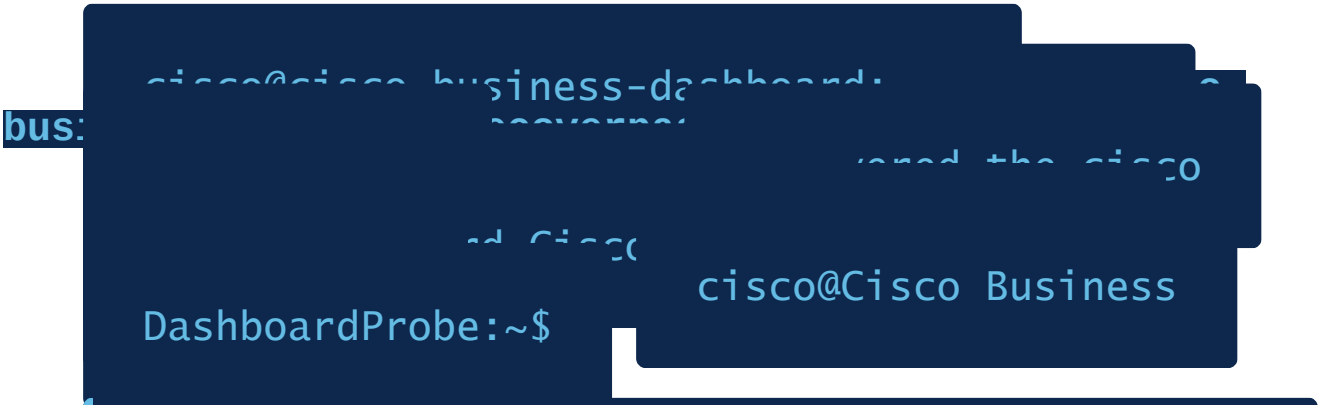
No. When Cisco Business Dashboard discovers a supported Cisco device, it will attempt to access the device using the factory default credentials for that device with the default username and password: *cisco*, or the default SNMP community: *public*. If the device configuration has been changed from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

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

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.

12. How do I recover a lost password for the Web User Interface (UI)?

If you have lost the password for all the admin accounts in the Web UI, you can reset the password by logging on the console of the Probe and running the **cbdprobe recoverpassword** tool, or logging on the console of the Probe 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. The following is an example of the commands to be provided in order to reset the password using this tool.



ⓘ Note:

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

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

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.

Remote Access

14. When I connect to the Web UI of a device from Cisco Business Dashboard Network Management, is the session secure?

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.

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

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 log out of the session.

16. 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**?

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

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

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 asthe 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.

18. How do I update Java on the Dashboard?

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.

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

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.

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

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.