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.