Performing Initial Setup for Direct Managed Devices

This chapter contains the following sections:

Performing Initial Setup for Direct Managed Devices

Direct managed devices are network devices that may be associated directly with a Dashboard and managed without a probe being present in the network. Only certain devices support direct management. Refer the Cisco Business Dashboard - Device Support List for a list of devices and software versions that support direct management. Direct managed devices will discover other devices in the broader network and add those devices to the Dashboard inventory.

The process for associating a direct managed device with the dashboard requires explicit configuration on both the Dashboard and the device prior to connecting. This process enables the device to be pre-configured prior to installation, or to be automatically configured using a zero-touch deployment mechanism such as Network Plug and Play.

Devices running more recent firmware versions support the use of a connection wizard to associate the device to the dashboard using a similar method to that used with a software probe.

To set up a direct managed device using the connection wizard, do the following:

1. Install the device hosting the embedded probe into the network. Connect to the administration GUI of the device and navigate to the Cisco Business Dashboard page.

2. Specify the address or hostname of the Dashboard to connect to and click the Connect to Dashboard button.

3. Your browser will be redirected to the Dashboard login screen. Login using administrator credentials for the Dashboard

4. Choose to either create a new network or to select an existing network from the drop-down provided. If you choose to create a new network, then specify a name and location for the network in the boxes provided.

   You can enter the address of the network into the appropriate fields. If you enter a partial address, a list of potential matches will be displayed, and you can select the location from the list. Alternatively, you can click on the location in the map.

5. Click Finish to be redirected back to the device GUI.

See the device documentation for more details on the location and use of the CBD agent configuration page.

To manually set up a direct managed device, follow the steps below:

1. Optionally create a new network record for the network the device will be installed in using the steps described in Performing Initial Setup for the Dashboard.
2. On the **Dashboard** UI, go to the **Inventory** and click the plus (+) icon to create a new device record. Fill in the form with appropriate details for the device that will host the probe, making certain to specify the correct product ID and serial number. This will allow the dashboard to associate the probe with the correct network.
3. On the **Dashboard** UI, go to the **My Profile** page by clicking on your username at the bottom of the navigation panel. Use this page to create a new **Access Key** using the **Generate Access Key** button. You can also use an existing access key if you prefer.

Note The access key used for associating a direct managed device with the dashboard does not need to be a long lived key. This key only needs to be valid at the time the initial association takes place. Once the device and dashboard are associated, the connection is authenticated using limited access, short-lived credentials that are unique to the device and regenerated periodically.

4. Using the device UI, navigate to the Cisco Business Dashboard configuration page and fill out the fields provided. At the minimum, you will need to supply configuration for the dashboard address and port, and access key ID and secret. If the device is running an older version of the CBD agent, you will also need to specify the organization and network names. It may also be necessary to configure the dashboard certificate. See below for more details.
5. Submit the changes. The device will connect to the dashboard and be associated with the network created in step 1.

When establishing a connection to the dashboard, the device checks to ensure the certificate presented by the dashboard 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 added to the device configuration as a trusted certificate. Refer the device administration guide for details on adding a trusted certificate.
- If the dashboard is configured as an IP address, then either the **Common Name** field or the **Subject-Alt-Name** field of the certificate must contain that IP address.
- If the dashboard is configured as a hostname, then either the **Common Name** field or the **Subject-Alt-Name** field of the certificate must contain that hostname.