



Setting Up the Network

This chapter contains the following sections:

- [Setting Up the Network for Cisco Business Dashboard, on page 1](#)
- [Setting Up Network Plug and Play, on page 4](#)
- [Configuring the Network, on page 6](#)

Setting Up the Network for Cisco Business Dashboard

Setting Up Device Credentials

For Cisco Business Dashboard to be able to manage the network devices, you must provide suitable credentials to allow access to each device.

When the Probe discovers a device, it will initially attempt to access the device using the default credentials with the username: `cisco`, password: `cisco` and the SNMP community set to: `public`. However, if the device is not using default credentials, then correct credentials must be supplied as detailed in the following steps:

1. Navigate to **Administration > Device Credentials**. The first table on this page lists all the devices that have been discovered that require credentials, while the second table lists all the discovered devices for which working credentials are known.
2. Enter a username and password combination and/or SNMP credentials in the respective fields at the top of the page. If more sets of credentials are required, then click the +(plus) icon. This allows up to three sets of each type of credential to be entered.
3. Click **Apply**. The Probes will test each credential against each device for which a credential is required. Working credentials are saved for each device.

The Probes will discover each network and generate a topology map and inventory for the network after being provided with the working credentials.

Learn About Your Network

Cisco Business Dashboard provides a high-level view of your network as either a map or a list of networks. To see the high-level view of all networks, perform the following steps:

1. Make sure you have associated your Probes with the Cisco Business Dashboard as described in the previous chapter.

2. Click **Network** in the Dashboard navigation. Click the button to display either the **Map View** or the **List View**.
3. In **Map View**, you may click and drag the map to reposition it, and use the plus and minus buttons to zoom in and out. Each network with a Cisco Business Dashboard Probe installed will be displayed as an icon on the map. Each icon contains a number showing the number of outstanding notifications for that network, and the color of the icon shows the highest severity level outstanding. Click on an icon to see more details about that site. If multiple icons are too close to be easily distinguished, they will be replaced with a cluster marker showing the number of Network icons in that cluster. Click on the cluster marker to zoom in on the sites in that cluster.

In **List View**, you can click the icon at the top left corner of the table to select the columns to be displayed, and you can click on the column headings to sort the table.
4. Use the Search box to find a specific network or to find the network that contains a particular device. You may enter the name, address or IP address of a network in the Search box, or the name, IP address, MAC address or serial number of a device.
5. When you click on a network, the **Basic Info** panel appears showing you more information about that network. This information includes the network name and address, and a list of outstanding notifications for the network.
6. You may click **More** in the **Basic Info** panel to open up the **Network Detail** a detailed information about that network, including the network topology diagram and floor-plans. It also allows you to modify settings for this network and view all the devices discovered in this network.

You may also use the **Inventory** to see detailed information about all the devices in your network. The **Inventory** page provides a list of all discovered devices in a tabular view. You can filter the list to restrict the devices displayed, and click on individual devices to see more information about that device.

Discover the Network by Scanning IP Addresses (Optional - Direct Managed Networks Only)

For direct managed networks, Cisco Business Dashboard may not always be able to discover network devices in other VLANs or subnets using only the automated discovery processes. When this occurs, it can be beneficial to have the dashboard explicitly search the IP address ranges associated with those VLANs or subnets. To search an IP address range, do the following:

1. Log on to the dashboard administration interface and open the Job Center by clicking on the hourglass icon in the top right corner of the screen.
2. Select the **Schedule Profiles** tab and click the plus (+) icon to create a new schedule profile.
3. Set the Job Type to **Search IPv4 Range for Devices**.
4. Select the appropriate organization and chose the network to search.
5. Set the schedule for the job. Optionally set it to recur periodically if you want to search the network regularly.
6. Specify the credentials to use when discovering devices and specify the IP address ranges to search.
7. Click **Save**.

Based on the schedule, the dashboard will search the specified address ranges for devices with an active web server and attempt to connect to the device using the credentials provided. If the dashboard is successful in

accessing the device, it will be added to the inventory and will be managed in the same way as any other device in the network.

Customizing the Topology Map (Optional)

Once working credentials are provided, the **Probes** or direct managed devices will discover each network and generate a **Topology** map. You may adjust the map as necessary.

1. Navigate to **Network** and select the network of interest. Click **More** to display the topology.
2. You may drag individual device icons to improve the layout. Any changes you make to the layout are permanent. Cisco Business Dashboard will not make further changes to the location of the icons. If you wish to re-enable automatic placement of icons, then click **Relayout Topology**.
3. Click **Overlays** to open the **Overlays and Filters** panel and use the check boxes to limit the device types that are displayed in the topology diagram.

Uploading Floor Plans (Optional)

You may upload floor plans for each network and place your network devices in order to document the location of your equipment. The following steps guide you through this process:

1. When viewing the topology diagram for a network, click **Floor Plan**.
2. Enter a name for the building and the floor, and then either drag an image file into the drop zone or click inside the widget to select an image file on your PC. Image formats supported include .png, .gif, .jpg
3. Click **Save** to save the changes.
4. To place a device on the floor plan, click **Add Devices** and type the device name or IP address into the search box at the bottom of the screen. Matching devices will be displayed, where grayed out devices have already been placed on a floor plan.
5. Click and drag a device to add it to the floor plan in the correct location.

Customizing the Monitoring Dashboard

You may customize the monitoring dashboard to suit your requirements using the following steps:

1. Select **Dashboard** from the navigation at the left of the screen. The default dashboard will be displayed.
2. To relocate individual widgets within the dashboard, click on the gear icon at the top right of the dashboard and select the **Edit Mode** option. Click and hold to drag each widget to the desired location. To resize a widget, click and hold on the edge or corner of the widget to resize.
3. To add a new widget to the dashboard, click the gear icon at the top right of the dashboard and select to add a widget. Select the desired widget from the list. To remove a widget from the dashboard, click **remove widget ✕** icon in the top right corner of the widget when in edit mode.
4. Once the dashboard is laid out correctly, click the gear icon at the top right of the dashboard and select **View Mode** to lock the changes in place.
5. To change the behavior of a widget, click **edit widget configuration** icon in the top right of the widget. Use the drop down lists to select the specific device, interface or network the widget should monitor.

Customizing Notification Display

You may customize the behavior of notifications using the following steps:

1. Navigate to **Administration > Organizations** and select the organization where you want to customize notification behavior.
2. Click **Notification**
3. Unchecked the **Inherit from Notification Defaults** checkbox. Use the check boxes to control which notifications generate a pop-up alert in the user interface, and those that generate an email notification. If you use email notifications, you must ensure that the email settings are correctly configured. Click **Save**.

You may also customize the **Notification Defaults** by navigating to **Administration > Notification Defaults**.

Setting Up Network Plug and Play

Cisco Business Dashboard provides a Cisco Network Plug and Play service that allows you to centrally manage firmware and configuration files for selected Cisco devices. For more information about Network Plug and Play, refer to the [PnP Solution Guide](#).

To set up Network Plug and Play, perform the following tasks.

Upload Firmware

1. Navigate to **Network Plug and Play > Images**.
2. Click the **+**(plus) icon.
3. Choose an organization and then drag a firmware file 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.
4. Click **Upload**.

You may designate an image as the default image for one or more device types. To designate an image as a default image, do the following:

1. Select the checkbox for the image in the **Images** table and click **edit**.
2. 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.
3. Click **save**.

Upload Configurations (Optional)

1. Navigate to **Network Plug and Play > Configurations**.
2. Click the **+**(plus) icon.
3. Choose an organization and then drag a configuration file from your PC and drop it on the target area of the **Upload File** window. Alternatively, you can click on the target area and select a configuration file to upload.

4. Click **Upload**.

Instead of uploading configurations, you may make use of the included configuration templates supplied with the Dashboard application. You can click on the name of a configuration file to view the contents if you wish.

Setting up Discovery

In order for network devices to use **Network Plug and Play**, they first need to discover the **Network Plug and Play** server. There are three mechanisms that may be used to provide this information to the devices:

1. **DHCP**: The network device can learn the address of the Network Plug and Play server using DHCP option 43. For more detail on the option format, refer to section, *About Network Plug and Play*, in the [Cisco Business Dashboard Administration Guide](#).
2. **DNS**: If the network device does not learn the server address through DHCP, it will attempt to lookup a well-known hostname, `pnpserver`, in the local domain—For example, `pnpserver.example.com`. You may configure your DNS infrastructure to ensure that this name resolves to the address of the Cisco Business Dashboard.
3. **Plug and Play Connect**: Cisco provides a redirection service, **Plug and Play Connect**, that the device will query if it is not able to find the address of the server any other way. To set up the redirection service for your network, please refer to the section *Network Plug and Play* in the [Cisco Business Dashboard Administration Guide](#).

Registering Devices

To register devices in preparation for installation, do the following:

1. Navigate to **Network Plug and Play > Enabled Devices**.
2. Click the **+** (plus) icon to add devices manually.



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 **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. Enter the name, product ID (PID) and serial number of the device to be registered and select an organization, network, device group and device type from the drop-down lists.
4. You may select either or both of a firmware image and configuration file to use for this device. If you choose Default image as the image, the device will use the image designated as the default for that device type at the time the device connects to the server.
5. Click **Save**.

Auto Claiming Devices

A device that connects to the server and is not present in the inventory is considered to be an unclaimed device. Unclaimed devices may be automatically claimed and provisioned by the server by creating an Auto Claim rule for that product ID. To create an Auto-Claim rule, do the following:

1. Navigate to **Network Plug and Play > Auto Claim Devices**.

2. Click the **+** (plus) icon.
3. Enter the product ID (PID) to automatically claim and select an organization, network, device group and device type from the drop-down lists.
4. You may select either or both of a firmware image and configuration file to use for this product ID. If you choose Default image as the image, auto claimed devices will use the image designated as the default for that device type at the time the device connects to the server.
5. Click **Save**.

Configuring the Network

If you are installing a new network, you may want to take this opportunity to perform the initial configuration of the network. Even in an existing network, you can choose to make configuration changes at this time.

Updating Firmware for devices (Optional)

The Dashboard will notify you if there are firmware updates available for the devices in your network, and an **Update Firmware** icon will be displayed against the device in several areas of the user interface.

To update firmware for a single device, follow the steps below:

1. Click on the device in the **Topology Map** to display the **Basic Info** panel.
2. Open the **Action** panel and click on the **Upgrade firmware to latest** button. The Dashboard will download the necessary firmware from Cisco and apply the update to the device. The device will reboot as part of this process.

Alternatively, firmware can be upgraded from your PC by clicking the **Upgrade From Local** option and specifying the firmware image to be uploaded.

3. You can view the progress of the upgrade by clicking on the **Task Status** icon in the top right of the user interface.

You can also upgrade individual devices from the **Inventory** view. For details, refer to section, *Viewing Device Inventory*, in the [Cisco Business Dashboard Administration Guide](#).

Updating Firmware for a Network

If you wish to upgrade an entire network to the latest available firmware, follow the steps below:

1. Open the **Network Detail** view for the network you wish to update.
2. Click **Network Actions** at the top of the page and select the **Upgrade Firmware** option. The Dashboard will download the necessary firmware files from Cisco for each device that has an available update, and will apply the update to each device in turn. Each device will reboot as part of this process.
3. You can view the progress of the upgrade by clicking on the **Task Status** icon in the top right of the user interface.

Configuring Device Groups

The Dashboard uses the concept of device groups to allow you to apply configuration to multiple devices at the same time and to ensure that configuration settings match across the network. To allocate devices to a device group, follow the steps below:

1. Navigate to **Administration > Device Groups**.
2. Click the **+** (plus) icon to add a new group.
3. Specify an organization, a name and description for the device group. Click **Save**.
4. To add devices to the device group, click the **+** (plus) icon in the **Devices** table. Use the search box to find devices to add to the group. Select one or more devices to join the group. Each device can only be a member of one group. If a selected device was previously a member of a different group, it will be removed from that group. If you wish to remove a device from the group, click the **Delete** icon next to the device, and the device will be moved to the **Default** device group. Device groups can contain a mixture of different device types.

Creating Configuration Profiles

The Dashboard allows you to easily apply common configuration to multiple network devices. You can use the **Network Configuration Wizard** to create configuration profiles for each section of the configuration, or you can create profiles individually. To use the **Network Configuration Wizard**, follow the steps below:

1. Navigate to **Network Configuration > Wizard**.
2. Enter a profile name for the configuration profiles to be created, choose an organization and select one or more device groups to which the configuration will be applied.
3. Click **Next**.
4. Specify the time settings for this group. A **Time Management** profile contains settings for the timezone, daylight savings, and NTP. If you do not wish to create a **Time Management** profile for this group, click **Skip**, otherwise click **Next**.
5. Specify the **DNS settings** for this group. A **DNS Resolvers** profile contains settings for the domain name, and the DNS servers to use. If you do not wish to create a DNS Resolvers profile for this group, click **Skip**, otherwise click **Next**.
6. Specify the user authentication settings for this group. An **Authentication profile** contains settings for the local user database for the devices. If you do not wish to create an **Authentication profile** for this group, click **Skip**, otherwise click **Next**.
7. Specify the Virtual LANs to be created for this group. A VLAN profile contains the details for one or more VLANs. If you do not wish to create a VLAN profile, click **Skip**. To add multiple VLANs, click **Add Another** after completing each VLAN. Click **Next**.
8. Specify the Wireless LANs to be created for this group. A Wireless LAN profile contains the details for one or more SSIDs. If you do not wish to create a Wireless LAN profile, click **Skip**. To add multiple SSIDs, click **Add Another** after completing each SSID. Click **Next**.
9. Review the configuration settings you have made. If you wish to make changes, use **Edit** or **Back** to return to the appropriate screen. Once you are satisfied, click **Finish** to create the profiles and apply to the devices in the selected device groups.

10. You can view the progress of the configuration by clicking on the **Task Status** icon in the top right of the user interface.

Backing Up Device Configurations

The Dashboard allows you to back up the configurations of your network devices. To back up the configuration for a single device, follow the steps below:

1. Click on the device in the **Topology Map** to display the **Basic Info** panel.
2. Open the **Action** panel and click **Backup Configuration** button. Optionally, you can add a note describing this backup in the window that appears. The **Dashboard** will copy the configuration of the device.
3. You can view the progress of the backup by clicking on the **Task Status** icon in the top right of the user interface.

You can also backup individual devices by clicking **Backup Configuration** in the **Inventory** view.

If you wish to back up the configurations for the entire network, follow the steps below:

1. Open the **Network Detail** view for the network you wish to back up.
2. Click **Actions** button at the top of the page and select the **Backup Configurations** option. Optionally, add a note describing this backup in the window that appears. The Dashboard will copy the configuration of each device.
3. You can view the progress of the backup by clicking on the **Task Status** icon in the top right of the user interface.