Administration

This chapter contains the following sections:

Discovery

The Cisco Business Dashboard Lite builds an initial list of devices in the network from listening to mDNS (aka Bonjour, please check your device setting to make sure Bonjour is enabled on the Management VLAN) advertisements. The Cisco Business Dashboard Lite then connects to each device using a supported protocol and gathers additional information such as CDP & LLDP adjacency tables. This information is used to identify additional devices in the network, and the process repeats until all devices have been discovered.

Cisco Business Dashboard Lite 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. Navigate to **Administration** > **Discovery**.
2. Specify the IP address ranges to search.
3. Click **Save**.

Based on the input, the Dashboard Lite will search the specified address ranges for devices with an active web server and attempt to connect to the device HTTPS port (443) 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.

By default, the Dashboard may display any discovered IP address for devices with multiple IP addresses. If you specify a Management VLAN, the IP address of the VLAN interface that matches the configured Management VLAN will be shown in the Inventory and Topology views. The Management VLAN setting only affects which IP address is displayed; the Dashboard may use any discovered, reachable IP address to access the device.

Device Credentials

For Cisco Business Dashboard Lite to fully discover and manage the network, it needs credentials to authenticate with the network devices. When a device is first discovered, the **Cisco Business Dashboard Lite** will attempt to authenticate with the device using the default username: `cisco`, password: `cisco`. If this attempt fails, a notification will be generated and valid credentials must be supplied by the user. To supply valid credentials, follow the steps below.

1. Navigate to **Administration** > **Device Credentials**. The first table on this page lists all the devices that have been discovered that require credentials.
2. Enter valid credentials into the **Username/Password** fields. You may click the ✚(plus) icon next to the corresponding field to enter up to three **Cisco Business Dashboard Lite** credentials. Ensure that passwords are entered using plain text.
3. Click **Apply**. The **Cisco Business Dashboard Lite** will test each credential against each device that requires that type of credential. If the credential is valid, it will be stored for later use with that device.
4. Repeat steps 2 to 3 as necessary until every device has valid credentials stored.

To enter a single credential for a specific device, follow the steps below.

1. Click the **Edit** icon shown against the device in the discovered devices table. A popup will appear prompting you to enter a credential that corresponds to the Credential Type selected.
2. Enter a username and password credential in the fields provided.
3. Click **Apply**. To close the window without applying, click the ✖ on the top right corner of the pop-up.

Underneath the **Add New Credential** section is a table showing the identity for each device for which has a valid credential stored and the time that credential was last used. To display the stored credential for a device, you may click the **Show Password** icon next to the device. To hide the credentials again, click the **Hide Password** icon. You may also show and hide credentials for all devices using the button at the top of the table. You may also delete credentials that are no longer required. To delete stored credentials, follow the steps below.

1. Navigate to **Administration** > **Device Credentials**.
2. In the **Saved Credentials** table, select the check box against one or more sets of credentials to be deleted. You may also select the checkbox at the top of the table to select all credentials.
3. Click **Delete Selected Credentials**.

To delete a credential for a single device, you may also click the **Delete** icon next to the device.

Users

The **User Management** page allows you to control how users are granted access to Cisco Business Dashboard Lite, change settings that affect how those users interact with the Dashboard.

Cisco Business Dashboard Lite has settings to control the dashboard features that are available using the Dashboard Access drop-down list. The options available for these settings include:

- **Administrator**—An Administrator has full access to Dashboard features including the ability to maintain the system.
- **Operator**—An Operator has similar power to an Organization Administrator, but cannot manage users.
- **Read only**—A Read only user can only view network information, they cannot make any changes.

Cisco Business Dashboard Lite allows users to be authenticated against the local user database.

When the Cisco Business Dashboard Lite is first installed, a default **Administrator** is created in the local user database with the username and password both set to `cisco`.

Note User settings can be managed by **Administrators** only.

Add a New User to the Local User Database

1. Navigate to **Administration**>**Users** and select the **Users** tab.
2. Click the ✚ (plus) icon to create a new user.
3. In the fields provided, enter a username, display name, email address and password, and specify the Dashboard Access settings. You may also provide contact details for the user.
4. Click **Save**.

Modify a User

1. Navigate to **Administration**>**Users** and select the **Users** tab.
2. Select the radio button next to the user that needs to be changed and click the **Edit** icon.
3. Make the modifications as required.
4. Click **Save**.

Delete a User

1. Navigate to **Administration**>**Users** and select the **Users** tab.
2. Select the radio button next to the user that needs to be deleted and click **delete** at the top of the table.

Change password complexity

To enable or change password complexity requirements, follow these steps.

1. Navigate to **Administration**>**Users** and select the **User Settings** tab.
2. Select the **Local** tab under **Authentication Source**, modify the **User Password Complexity** settings as required and click **Save**.

Restore Access when All Administrative Access has been Lost

If administrative access to the Cisco Business Dashboard Lite application is lost, follow these steps to recover the same access.

1. Log on the server of the Dashboard Lite, open the Dashboard Lite Server Application.
2. Click the **Tools > Recover Password** menu.

After that, the local user authentication is enabled, and the default Administrator with username **cisco** and password **cisco** is restored.

Change session timeouts

To change idle and absolute timeouts for user sessions, follow these steps.

1. Navigate to **Administration**>**Users** and select the **User Settings** tab.
2. Modify the **User Session** parameters as required and click **Save**. Hover over the help icons to see allowable ranges for these parameters.

Login Attempts

Cisco Business Dashboard Lite keeps a log of every attempt made to log in and out of the system, both successful and unsuccessful. To view the log, navigate to **Administration**>**Login Attempts**. The table displays the following information:

Field	Description
Username	The username associated with the event.
Display Name	The display name for the user.
IP	The IP address of the device from which the user logged in.
Type	The type of event including: • LOGIN • LOGOUT
Status	Indicates if the attempt succeeded or failed.
Timestamp	The date and time the event took place.

You may use the search box above the table to show only entries that match a particular user or IP address.