System

The section contains the following topics:

About System

The System option in Cisco Business Dashboard allows you to manage the operation of the platform.

This section is divided into the following pages:

Page Name	Page Function
License	Manage software licensing for the Dashboard.
Certificate	Manage security certificates on the Dashboard.
Email Settings	Set up email and manage settings.
API Usage	Monitor the use of the Cisco Business Dashboard API.
Backup	Backup the configuration and other data for the Dashboard.
Restore	Restore the configuration and other data for the Dashboard.
Platform Settings	Manage network configuration for the Dashboard.
Privacy Settings	Control the data that can be shared with Cisco.

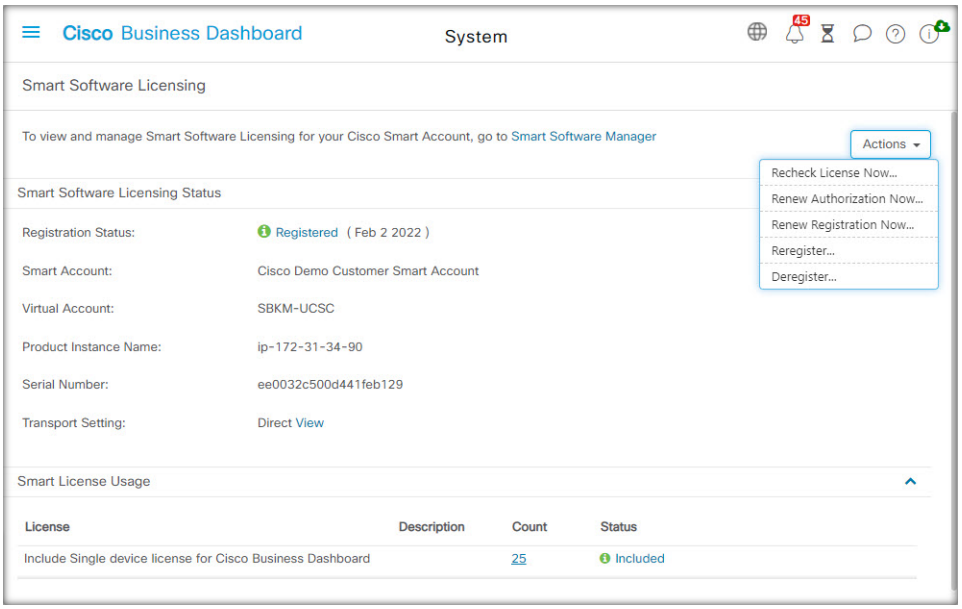
Page Name	Page Function
Log Settings	Change log settings for the Dashboard.
Local Probe	Manage a Probe hosted on the Dashboard.
Integration Settings	Manage the integration of Cisco Business Dashboard with external applications.

Note These pages are only available to **Administrators**.

Managing Licenses

Note This page is not present on the metered version of Cisco Business Dashboard for AWS.

The **License** page allows you to see the number and type of licenses required for your network, and allows you to connect the **Dashboard** to the Cisco Smart Licensing system. If you have 25 devices or less there is no need for additional licensing. There are two information panels on this page.



- **Smart Software Licensing Status**

  This panel shows the registration state of the Smart License client and information about the Smart Account in use.

- **Smart License Usage**

  This panel lists the quantities and types of license required based on the current state of the network. This information will automatically update as the network changes, and the Dashboard will update the

number of licenses requested from the Smart Account. The Status field shows whether the required number of licenses have been successfully obtained.

This page also contains controls allowing you to register and deregister the Dashboard from your Smart account.

If the Dashboard is not able to obtain sufficient licenses to manage the network, it will operate in evaluation mode and a message will be displayed in the header of the Dashboard's user interface. When running in evaluation mode, you have 90 days to correct the situation. If the problem is not addressed within 90 days, some functionality of the Dashboard will be restricted until the problem is addressed, either by obtaining more licenses, or reducing the number of devices being managed.

Register the Dashboard to your Smart Account

To register the Dashboard with your Smart Account, follow the steps below:

1. Log on to your Smart Account at *https://software.cisco.com*.

   Select the **Smart Software Licensing** link located under the License section.
2. Select the **Inventory** page, and if necessary, change the selected virtual account from the default.
3. Click on the **General** tab.
4. Create a new **Product Instance Registration Token** by clicking on the **New Token…** button. Optionally add a description and change the **Expire After** time.
5. Click **Create Token**.
6. Copy the newly created token to the clipboard by selecting **Copy** from the **Actions** drop-down located at the right of the token.
7. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
8. Click the **Register** button and paste the token into the field provided.
9. Click **OK**.

The Dashboard will register with Cisco Smart Licensing and request sufficient licenses for the number of network devices being managed. If there are insufficient licenses available, a message will be displayed on the user interface, and you will have 90 days to obtain sufficient licenses before system functionality is restricted.

Remove the Dashboard from your Smart Account

To remove the Dashboard from your Smart Account and return any licenses allocated back to the pool, follow the steps below:

1. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
2. Select **Deregister…** from the drop-down list located at the top right. Click **Deregister** in the pop-up to confirm.

Immediately Check for Licenses

Cisco Business Dashboard checks daily to ensure there are still sufficient licenses available for the network, and will update immediately if the number of licenses required decreases. However, if the number of licenses

required increases, or if licenses are added or removed from the pool, it may take up to a day before the Dashboard will be updated. To force the Dashboard to update its license allocation immediately, follow the steps below.

1. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
2. Select **ReCheck License Now…** from the drop-down list located at the top right. Cisco Business Dashboard will query Cisco Smart Licensing immediately to ensure that there are sufficient licenses available for the Dashboard to operate.

Renew Authorization Now

The Renew Registration Now action cause the Dashboard to refresh the certificates used to authenticate communication with Cisco Smart Licensing. Typically, this will only be required at the request of Cisco Support when rectifying an extended communications outage. To renew the registration, follow the steps below.

1. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
2. Select **Renew Authorization Now…** from the drop-down list located at the top right.

Renew Registration Now

The Renew Registration Now action causes the Dashboard to refresh the certificates used to authenticate communication with Cisco Smart Licensing. Typically, this will only be required at the request of Cisco Support when rectifying an extended communications outage. To renew the registration, follow the steps below.

1. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
2. Select **Renew Registration Now…** from the drop-down list located at the top right.

Transfer the Dashboard to a Different Account

Re-registering a Dashboard allows it to be moved from one Virtual Account to another. To move a Dashboard between accounts, follow the steps below.

1. Navigate to the Cisco Business Dashboard user interface and select **System** > **License**.
2. Select **Reregister...** from the drop-down list located at the top right.
3. Enter the new registration token in the box provided. If the Dashboard is currently registered to another account, ensure the **Reregister this product instance if it is already registered** checkbox is selected, then click **OK**.

Managing Certificates

At the time of installation, Cisco Business Dashboard will generate a self-signed certificate to secure web and other communication with the server. You may choose to replace this certificate with one signed by a trusted certificate authority (CA).

There are several ways this can be done:

- Cisco Business Dashboard supports automatically issuing and renewing certificates from the Let's Encrypt certificate authority.
- You may provide a certificate signing request (CSR) to your preferred certificate authority for signing. Cisco Business Dashboard will generate the CSR for you.
- You may choose to have the certificate authority generate a certificate and the corresponding private key independently from the Dashboard. If so, you should combine the certificate chain and private key into a PKCS#12 format file prior to uploading to the dashboard.

For more details on each of these options, and instructions for viewing the current certificate and regenerating a self-signed certificate, see the sections below.

Automatically Install a Certificate from Let's Encrypt

From release 2.2.1, Cisco Business Dashboard can automatically obtain and renew a domain-validated certificate from the **Let's Encrypt Certificate Authority** (https://letsencrypt.org) and in release 2.5.0, these certificates can be managed through the Administration page.

Important You must have a fully qualified domain name registered and a DNS record that points to the public IP address. Refer to Managing Platform Settings, on page 12 for more information.

To install a Let's Encrypt certificate using the administration GUI, do the following:

1. Navigate to **System**> **Certificate** and select the Update Certificate tab.
2. Select the *Let's Encrypt Certificate* radio button.
3. Check the box to enable the use of a Let's Encrypt certificate.
4. Enter one or more fully qualified domain names into the fields provided. The names must be defined in the domain name system (DNS) and resolve to the address of the Cisco Business Dashboard server.
5. Provide an email address to be used for urgent renewal and security notices.
6. Review the Let's Encrypt Subscriber Agreement using the link provided and then check the box to accept the agreement.
7. Optionally check the box to share the email address with the Electronic Frontier Foundation (https://www.eff.org).
8. Click the Get Certificate button.

The Dashboard will contact the Let's Encrypt Certificate Authority and obtain a certificate using the HTTP verification method. The page will update to show the details of the certificate along with the expiry date. The certificate will be automatically renewed approximately 30 days before expiry.

If you need to update the certificate at any point, follow these steps:

1. Navigate to **System**>**Certificate** and select the **Update Certificate** tab.
2. Select the **Let's Encrypt Certificate** radio button.
3. Use the check-boxes and the fields provided to update the name(s) to be applied to the certificate.

   Or you can update the contact details at the bottom of the screen.

4. Click the Get Certificate button.

You can also force the certificate to be regenerated before the normal renewal time by leaving the fields on the page unchanged and clicking the Force Renewal button.

To install a Let's Encrypt certificate using the command line, do the following:

1. Log on to the host operating system using SSH or via the console.
2. Execute the **cisco-business-dashboard letsencrypt** command and specify one or more fully qualified hostnames using the **-d** option. (For example, **cisco-business-dashboard letsencrypt -d dashboard.example.com -d pnpserver.example.com**.) All names listed in the command must resolve to the IP address of the dashboard server.
3. Follow the prompts to have a certificate issued and applied to the dashboard application. The certificate will be automatically renewed by the dashboard as it approaches expiry.

Note The **Let's Encrypt** service will need to connect to the dashboard web server to verify ownership of the hostname(s). To allow this, the dashboard web server must be accessible from the Internet. See Managing Platform Settings, on page 12 for details on how to restrict access to the dashboard application to only authorized IP addresses.

Generate a Certificate Signing Request (CSR)

1. Navigate to **System**>**Certificate** and select the **CSR** tab.
2. Enter appropriate values into the fields provided in the form that is displayed. These values will be used to construct the CSR, and will be contained in the signed certificate you receive from the CA.
3. Click **Create** and the CSR will be automatically downloaded to your PC. Alternatively, you can download the CSR at a later date by clicking **Download** next to the CSR label.
4. If necessary, you can modify the CSR by returning to step 2.

Upload a New Certificate

To upload a new certificate using the administration GUI, follow the steps below.

1. Navigate to **System**>**Certificate** and select the **Update Certificate** tab.
2. Select **Upload Cert** radio button. The file containing the certificate can be dropped on the target area, or you may click the target area to browse the file system. The file should be in PEM format.

   You may also upload a certificate with the associated private key in PKCS#12 format by selecting the **Upload PKCS12** option instead. The password to unlock the file should be specified in the field provided.
3. Click **Upload** to upload the file and replace the current certificate.

To upload a new certificate using the command line, do the following:

1. Copy the certificate and private key files to the Cisco Business Dashboard file system using SCP or similar. Ensure access to these files is restricted to authorized personnel only as the private key is sensitive information.

2. Log on to the operating system using the console or SSH.
3. Apply the certificate to the dashboard application using the command: **cisco-business-dashboard importcert -t pem -k <private key file> -c <certificate file>**. The certificate and private key will be loaded into the dashboard application and replace the current certificate. For more information on this command and its options, enter **cisco-business-dashboard importcert -h**.

Note Some browsers may generate certificate warnings for certificates that have been signed by a well-known certificate authority, while other browsers accept the certificate without any warning. Network Plug and Play clients may also fail to accept the certificate. This is because the certificate authority has signed the certificate with an intermediate certificate that is not included in the browser or PnP client's trusted authorities store. In these circumstances, the certificate authority provides a bundle of certificates that must be concatenated with the server certificate before uploading to the Dashboard.

During upload, the dashboard will remove any duplicates or unnecessary certificates from the chain and attempt to assemble it in the correct order. Select the Current Certificate tab after upload to confirm that the certificate chain is complete and correctly formatted.

Regenerate the Self-Signed Certificate

To regenerate the self-signed certificate, follow the steps below.

1. Navigate to **System**>**Certificate** and select the **Update Certificate** tab.
2. Click **Renew Self-Signed Cert**. Enter appropriate values into the fields provided in the form that is displayed. These values will be used to construct the certificate.
3. Click **Save**.

View the Current Certificate

To view the current certificate, follow the steps below.

1. Navigate to **System**>**Certificate** and select the **Current Certificate** tab.
2. Each certificate in the chain of trust for the dashboard is listed in the table at the top of the screen, along with its type, subject and expiry date. For a dashboard with a self-signed certificate, there will be only one entry in the table, while a dashboard using a CA-signed certificate may have several entries.
3. Click on a row of the table to display the details of the corresponding certificate in the box below.
4. You may use the icons in the Actions column to down the root certificate in the chain or copy it to the clipboard. The root certificate may be required when configuring devices to connect to the dashboard when the certificate is self-signed or signed by a private CA.

Downloading the Current Certificate Chain

To download a copy of the current certificate chain, follow the steps below.

1. Navigate to **System**>**Certificate** and select the **Current Certificate** tab.
2. Click the **Download Certificate Chain** button at the bottom of the page. The certificate chain will be downloaded in PEM format by your browser.

Automatically Install a Certificate from Let's Encrypt

From release 2.2.1, Cisco Business Dashboard can automatically obtain and renew a domain-validated certificate from the **Let's Encrypt Certificate Authority** (https://letsencrypt.org) and in release 2.5.0, these certificates can be managed through the Administration page.

Important You must have a fully qualified domain name registered and a DNS record that points to the public IP address. Refer to Managing Platform Settings, on page 12 for more information.

To install a Let's Encrypt certificate using the administration GUI, do the following:

1. Navigate to **System**> **Certificate** and select the Update Certificate tab.
2. Select the *Let's Encrypt Certificate* radio button.
3. Check the box to enable the use of a Let's Encrypt certificate.
4. Enter one or more fully qualified domain names into the fields provided. The names must be defined in the domain name system (DNS) and resolve to the address of the Cisco Business Dashboard server.
5. Provide an email address to be used for urgent renewal and security notices.
6. Review the Let's Encrypt Subscriber Agreement using the link provided and then check the box to accept the agreement.
7. Optionally check the box to share the email address with the Electronic Frontier Foundation (https://www.eff.org).
8. Click the Get Certificate button.

The Dashboard will contact the Let's Encrypt Certificate Authority and obtain a certificate using the HTTP verification method. The page will update to show the details of the certificate along with the expiry date. The certificate will be automatically renewed approximately 30 days before expiry.

If you need to update the certificate at any point, follow these steps:

1. Navigate to **System**>**Certificate** and select the **Update Certificate** tab.
2. Select the **Let's Encrypt Certificate** radio button.
3. Use the check-boxes and the fields provided to update the name(s) to be applied to the certificate.

   Or you can update the contact details at the bottom of the screen.
4. Click the Get Certificate button.

You can also force the certificate to be regenerated before the normal renewal time by leaving the fields on the page unchanged and clicking the Force Renewal button.

To install a Let's Encrypt certificate using the command line, do the following:

1. Log on to the host operating system using SSH or via the console.
2. Execute the **cisco-business-dashboard letsencrypt** command and specify one or more fully qualified hostnames using the **-d** option. (For example, **cisco-business-dashboard letsencrypt -d dashboard.example.com -d pnpserver.example.com**.) All names listed in the command must resolve to the IP address of the dashboard server.

3. Follow the prompts to have a certificate issued and applied to the dashboard application. The certificate will be automatically renewed by the dashboard as it approaches expiry.

Note The **Let's Encrypt** service will need to connect to the dashboard web server to verify ownership of the hostname(s). To allow this, the dashboard web server must be accessible from the Internet. See Managing Platform Settings, on page 12 for details on how to restrict access to the dashboard application to only authorized IP addresses.

Managing Email Settings

The **Email Settings** page allows you to control how emails will be sent by Cisco Business Dashboard.

Access this page to set the following parameters.

Field	Description
SMTP Server	The domain name or IP address of the SMTP server that will be used.
SMTP Port	The TCP port to use for sending mail.
Email Encryption	The encryption method to use which includes the following: • None • TLS • SSL
Authentication	Enable or disable email authentication.
Username	The username to present if authentication is enabled.
Password	The password to present if authentication is enabled.
From Email Address	The email address to originate messages from.

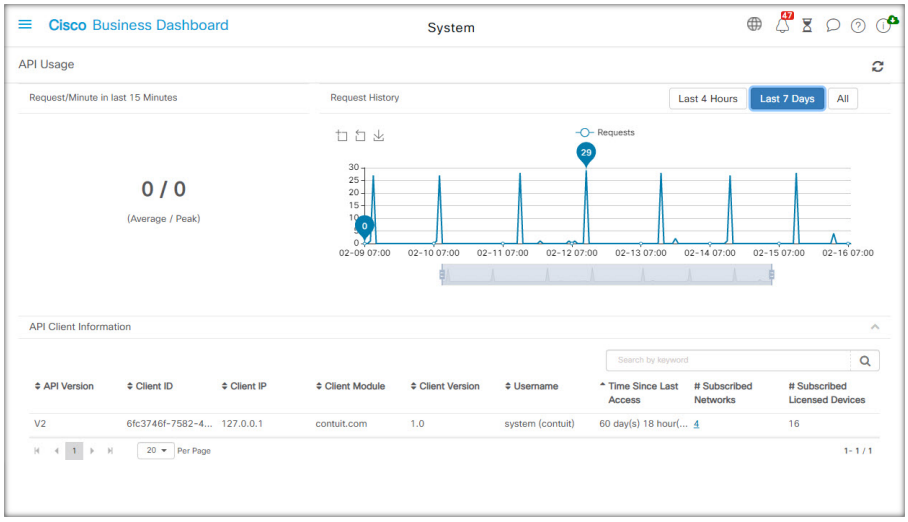
To test the configuration, click **Test Connectivity**. This will prompt for a target email address and generate a test email to the specified address.

Viewing API Usage

The API Usage page displays information about any external applications that have been integrated with the Cisco Business Dashboard. This report is divided into the following three sections:

- The **15-minute Request Monitor**—Displays the average and peak request rate over the last 15 minutes
- The **Request History** graph—Displays a graph of request activity over time. You may select time periods of the last four hours, the last seven days, or all available information. You may then use the sliders underneath the graph to narrow the focus of the graph to a particular period of interest.

- The **API Client Information** table—Lists all the clients that have used the API at least once. The following table describes the information provided in the **API Client Information** table:



Field	Description
API Version	The version used by the client when accessing the API.
Client ID	The identifier for a particular instance of the client application.
Client IP	The IP address associated with this client. Also displays the callback URL to which the Dashboard should post event notifications when the API version is v1 and notifications have been requested.
Client Module	The type of application associated with this client.
Client Version	The version of the application associated with this client.
Username	For clients using the v1 API, this field shows the username presented by the application when authenticating to the Dashboard. For clients using the v2 API, this field shows the **Access Key ID** used by the client and the username that key is associated with.
Time Since Last Access	The time since the last activity from this client.
# Subscribed Networks	The number of networks where the application has requested event notifications. This number is a link that, when clicked, displays the Subscribed Networks table for this client. The Subscribed Networks table is described below.
# Subscribed Licensed Devices	The number of managed devices for which event notifications will be sent to this client.

To view information about the networks for which a client has requested notifications, click on the **# Subscribed Networks** link for the client in the **API Client Information** table. The**Subscribed Networks** table will be displayed for the client containing a list of the networks the client has requested notification for.

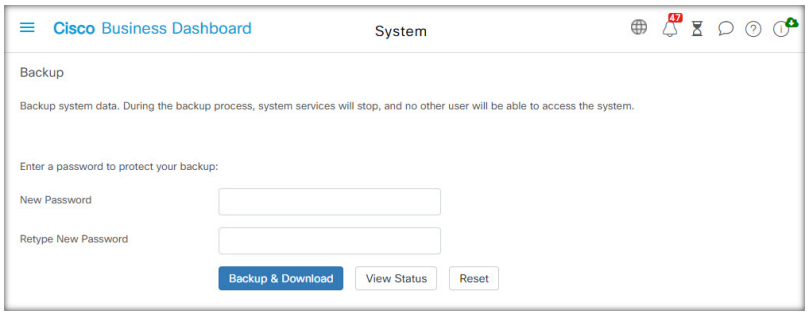
Field	Description
Network	The name of the network being monitored by the client.
# Subscribed Licensed Devices	The number of managed devices in this network for which event notifications will be sent

Backing Up and Restoring the Dashboard Configuration

The configuration and other data used by Cisco Business Dashboard can be backed up for disaster recovery purposes, or to allow the Dashboard to be easily migrated to a new host. Backups are encrypted with a password in order to protect sensitive data.

A Cisco Business Dashboard backup file may be restored to a system running the same version as the backed-up system, or up to one minor release newer. For example, a backup taken from a system running version 2.2.0 may be restored to a system running 2.3.1, but not to a system running 2.4.0.

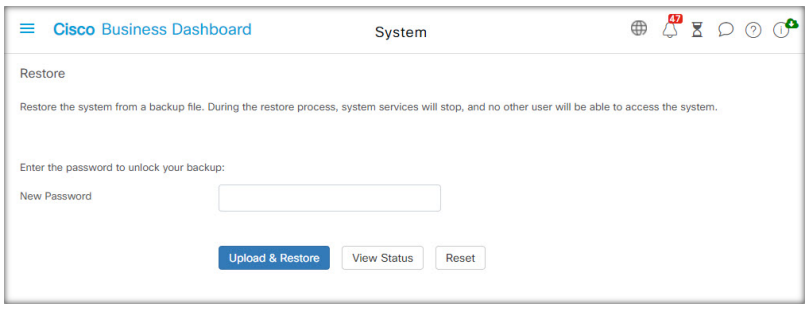
To perform a backup, follow the steps below.



1. Navigate to **System** > **Backup**.
2. Enter a password to encrypt the backup in the **Password** and **Confirm Password** fields.
3. Click **Backup & Download**. A pop-up window will appear showing the progress of the backup. Larger systems may require some time to complete the backup, so you may dismiss the progress meter and display it again later with the **View Status** button.

When complete, the backup file will be downloaded to your PC.

To restore a configuration backup to the Dashboard, follow the steps below.



1. Navigate to **System** > **Restore**.

2. Enter the password that was used to encrypt the backup in the **Password** field.
3. Click **Upload & Restore** to proceed. A pop-up will appear allowing you to upload a backup file from your PC. You can drag and drop the backup file onto the target area provided, or click the target area to specify a file in your PC file system. Click **Restore** to proceed.

If the dashboard version is 2.5.0 or higher, the application will restart when the restore process completes.

Managing Platform Settings

The **Platform Settings** page allows you to modify key system settings without needing to directly access the operating system. Due to the variation in platforms supported by Cisco Business Dashboard, not all settings will be available on every platform.

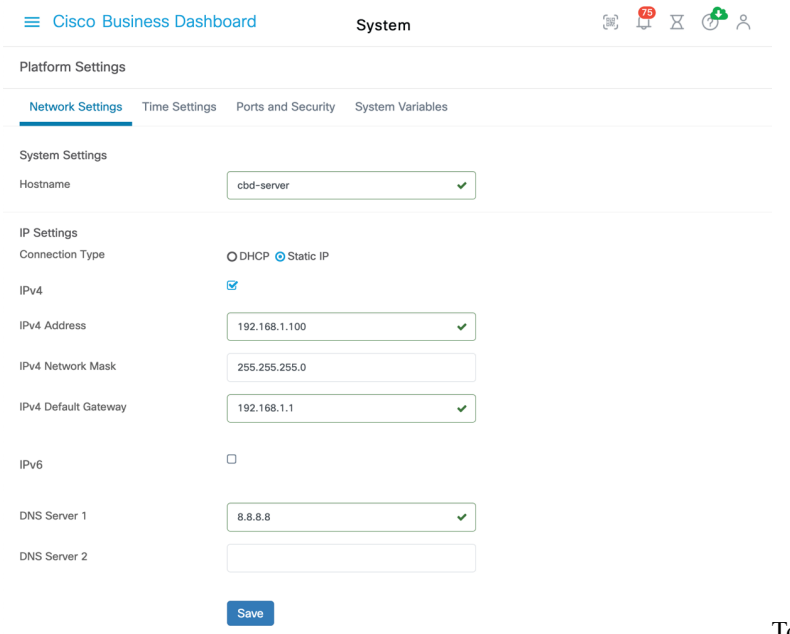
Platform settings are separated into four groups.

- Network Settings
- Time Setting
- Ports and Security
- System Variables

The following sections describe the settings available on each tab.

Changing the Hostname (Network Settings tab)

The hostname is the name used by the operating system to identify the system, and is used by Cisco Business Dashboard to identify the Dashboard when generating Bonjour advertisements.



To change the hostname for the Dashboard, follow the steps below.

1. Navigate to **System** > **Platform Settings**, and select the **Network Settings** tab.
2. Specify a hostname for the Dashboard in the field provided.
3. Click **Save**.

Changing Network Settings (Network Settings tab)

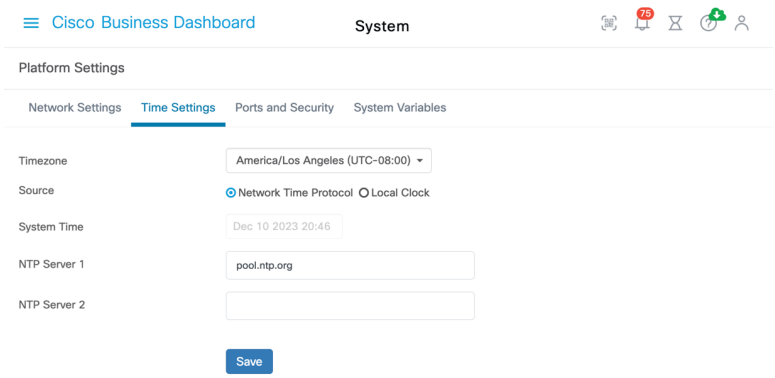
Note This does not apply to Cisco Business Dashboard for AWS or Azure. To modify the network configuration, use the EC2 console in AWS for an AWS instance, and the Azure Portal for an Azure instance.

To change the network configuration for the Dashboard, follow the steps below.

1. Navigate to **System** > **Platform Settings**, and select the **Network Settings** tab.
2. Select the method for IP address assignment. The available options are DHCP (default) and Static IP. If you choose the Static IP option, then specify the address, subnet mask, default gateways and DNS servers in the appropriate fields.
3. Click **Save**

Changing Time Settings (Time Settings tab)

The **Time Settings** manage the system clock for the Dashboard. To adjust the system clock, follow the steps below.



1. Navigate to **System** > **Platform Settings**, and select the **Time Settings** tab.
2. Select the appropriate timezone for the Dashboard.
3. Select the method for time synchronization. The available options are **NTP (default)** and **Local Clock**. If the NTP option is chosen, then optionally modify the NTP servers to use for synchronization.

   If **Local Clock** is selected, the you may manually adjust the date and time using the controls provided. Alternatively, click **clock** to synchronize the time with your PC.
4. Click **Save**.

Note If the virtual machine is configured to synchronize the local clock with the host machine, any changes to the local clock done through the **Platform Settings** page will be overwritten by the hypervisor.

If the hypervisor in use is VirtualBox and the VirtualBox Guest Additions are installed in the VM, the NTP service - timesyncd - will not operate.

Changing Port Settings (Ports and Security tab)

The **Port Settings** control the TCP ports the Dashboard's user interface is hosted on. To change the default web server ports, follow the steps below.

1. Navigate to **System** > **Platform Settings**, and select the **Ports and Security** tab.
2. Change the ports used by the web server for the HTTP and HTTPS protocols.
3. Change the ports used to provide remote access to network devices through Cisco Business Dashboard.
4. Click **Save**.

Restricting Access to the Dashboard (Ports and Security tab)

You may limit the IP addresses that may access the Dashboard using the Access Control settings. You may specify different IP ranges for the Dashboard GUI, the Dashboard API, and for connections from probes and managed devices.

To limit access to the Dashboard, follow the steps below.

1. Navigate to **System** > **Platform Settings**, and select the **Web Server** tab.
2. Enter a network prefix and mask into the fields provided. If multiple prefixes are required for any section, click the **(+)**plus icon to add additional entries. Similarly, you may click the trashcan icon to remove existing entries.
3. Click **Save**.

Managing System Variables (System Variables tab)

Cisco Business Dashboard uses system variables to provide certain parameters related to the Dashboard when generating configuration templates and other tasks. Some system variables may be determined by the Dashboard automatically, but there are other variables that require user input. In particular, if the Dashboard is deployed behind a web proxy or NAT gateway, it will be necessary for the administrator to provide external addressing information for the Dashboard.

To update the external address information for the Dashboard, follow the steps below.

1. Navigate to **System** > **Platform Settings**, and select the **System Variables** tab.
2. Enter IP address and port information into the External System Settings parameters as required. If left blank, the Dashboard will use the platform address and port information for the corresponding system variable.
3. Click **Save**.

Managing Privacy

Some of the features of Cisco Business Dashboard require the use of online services hosted by Cisco and result in the sharing of certain information with Cisco. These services include:

- **Lifecycle Reporting**—This feature includes the generation of the **Lifecycle Report**, **End of Life Report and Maintenance Report** in Cisco Business Dashboard. Lifecycle Reporting is enabled by default.
- **Software Updates**— Notification of the availability of software updates for network devices, and the ability to have those updates automatically applied. Software Updates are enabled by default.

All of these features are subject to the Cisco Privacy Policy and you may enable or disable them at any time. The **Privacy Settings** page is displayed during the initial setup of the Dashboard, allowing you to disable any of the default enabled features prior to any network data being collected. More detail for each of these features and the information shared may be found below.

Lifecycle Reporting

Cisco Business Dashboard provides information on the lifecycle state of each of the Cisco devices in the network. In order to do this, the Dashboard must provide Cisco with the product ID, serial number and hardware and software versions for each Cisco device. The IP address of the Dashboard may also be recorded. No personal or sensitive information will be intentionally collected during this process.

To disable the generation of lifecycle reports, follow the steps below.

1. Navigate to **System**>**Privacy Settings**.
2. Un-check the check boxes for the reports you wish to disable.
3. Click **Save**.

Software Updates

Use of this feature requires Cisco Business Dashboard to send the product ID and hardware and software version information for each device to Cisco. Your local IP address may also be recorded. No personal or sensitive information will be intentionally collected during this process.

To disable the use of automatic software updates, do the following:

1. Navigate to **System**>**Privacy Settings**.
2. Un-check the check boxes for both device firmware checks and Cisco Business Dashboard application checks.
3. Click **Save**.

Managing Logging Settings

The **Log Settings** page allows you to control the amount of detail included in log files by the different software modules. The default logging level is **Info**, but you can reduce the number of messages logged by selecting **Warn** or **Error**, or view more detail by selecting **Debug**.

To change the log levels for the Dashboard, follow the steps below.

1. Navigate to **System**> **Log Settings**.
2. Use the radio buttons to select the desired logging level for each software module.
3. Click **Save**.

The log files for the Dashboard can be found in the directory `/var/log/ciscobusiness/dashboard/` on the local file-system. You may click **Download Log File** to download an archive of the contents of this directory. It may take several minutes to collect all the data.

Logging to Syslog

From release 2.2.1, Cisco Business Dashboard application logs may be sent to the host's syslog service and from there may be directed to external syslog servers.

To enable sending files to the host syslog service, follow the steps below.

1. Log on to the host operating system using SSH or via the console and edit the file `/etc/ciscobusiness/dashboard/cisco-business-dashboard-logger.conf`
2. Edit the `xxx.logger` lines to specify **file** or **syslog** or both (comma separated). The following modules are available: `redis`,`mongo` , `rabbitmq`, `nginx` and `cbd`. If `file` is specified, log messages will be directed to the default log files in the `/var/log/ciscobusiness/dashboard/` directory. If **syslog** is specified, log messages will be directed to the syslog service in the host.

Note The `mongo` module does not support multiple logging destinations. If multiple destinations are listed, the first entry takes precedence. Also, the `cbd` module will always log to the file system regardless of the presence or absence of the **file** keyword in the logger configuration.

3. Optionally, modify the `xxx.syslog.facility` lines to specify the syslog facility used for each of the modules. By default, each module logs to a separate local<*n*> facility where <*n*> ranges between 1 and 5.
4. Restart Cisco Business Dashboard using the command **cisco-business-dashboard stop** followed by **cisco-business-dashboard start**.

Once the logging configuration has been modified to direct log messages to **syslog**, the `/etc/rsyslog.conf` file should be updated to receive the logs and direct the dashboard log messages to the desired destination. For a detailed information on the configuration file, refer to https://www.rsyslog.com/doc/v8-stable/configuration/index.html.

Execute the following steps:

1. The `/etc/rsyslog.conf` file should be updated to allow log messages to be received across the loopback interface. Edit the file to include the following lines to enable this and to restrict the server to listen *only* on the loopback interface:

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514" address="::1")
input(type="imudp" port="514" address="127.0.0.1")

# provides TCP syslog reception
module(load="imtcp")
```

```
input(type="imtcp" port="514" address="::1")
input(type="imtcp" port="514" address="127.0.0.1")
```

2. Create a new file in the directory `/etc/rsyslog.d/` to contain the configuration directives specific to Cisco Business Dashboard. The file name should be of a form similar to `40-cisco-business-dashboard-syslog.conf`.
3. Edit the file created in step 2 to contain directives to send log output to the desired destinations. For example, assuming the use of the default facilities in the `cisco-business-dashboard-logger.conf` file, the following configuration would direct the warning level and above messages from the dashboard application to the syslog server with the name `logger.example.com`:

   ```
   local2.warning  @logger.example.com
   ```

4. Restart the rsyslog daemon to apply the changes using the command **sudo systemctl restart rsyslog.service**

Managing the Local Probe

Note This page is not present on Cisco Business Dashboard for AWS or Azure.

Cisco Business Dashboard Probe may be installed on the same host as Cisco Business Dashboard in order to manage devices on the network local to the Dashboard, and the Cisco virtual machine image for the Dashboard does include the Probe. If you do not wish to manage the network local to the Dashboard, you may disable the co-located Probe using the following steps:

1. Navigate to **System**>**Local Probe**.
2. Click the toggle switch to disable the local Probe.
3. Click **Save**.

To remove the Probe software entirely from the Dashboard, log on to the operating system and use the command `sudo apt-get --purge autoremove cbd-probe`. This removes the Probe software, configuration and dependencies that are not required by any other application.

Managing Integration Settings

Cisco Business Dashboard may be integrated with a variety of applications and services provided by Cisco and other vendors. When integrated with an application, data and events may be exchanged between the applications and network actions performed.

Integration is supported with the following applications and services:

- Professional Service Automation (PSA) Tools
  - Connectwise Manage
- Collaboration Tools
  - Webex

The functionality offered by each type of integration is largely common across all integrations of the same type – PSA or collaboration tool. However, some differences do exist, and you should consult the appropriate sections in Available Integrations below to see the functionality supported by each individual application. To understand the functionality supported for each class of integration, read the following sections.

Using the Professional Services Automation Tools

Three areas of functionality are available when integrating with Professional Services Automation (PSA) tools-asset management, event management and automation. Of these, event management and automation involve the user actively interacting with the functionality by creating and managing tickets. Asset management generally does not require user interaction beyond the initial setup described in the Available Integrations sections below.

Using Asset Synchronization

With asset synchronization, the inventory of network devices in Cisco Business Dashboard is automatically synchronized into the PSA as configuration records containing detailed information about the device. Accounting and billing related information is also updated as required by the PSA implementation in order to ensure that devices managed by the dashboard are correctly accounted for. For more details on what fields are updated, see the section corresponding to the PSA being used in the Available Integrations, on page 21.

The asset synchronization process happens automatically at midnight each day. In the event an immediate synchronization is needed, one can be initiated by clicking the **Sync Assets** button on the Asset Synchronization screen. This can also be done from a collaboration tool if one has been integrated with Cisco Business Dashboard.

Note The asset synchronization process typically takes several minutes, and can take much longer in larger networks.

Automating Network Actions with Automation Tickets

Automation tickets allow actions to be performed on network devices by opening specially formatted tickets.

Tickets can specify whether the action should occur immediately or during the next change window, and may optionally require an approval step prior to execution. When all the preconditions are met, Cisco Business Dashboard will execute the action specified in the ticket and the ticket is updated with the success or failure of the operation.

The creation process for automation tickets varies slightly between PSA tools. For details on creating an automation ticket for the PSA being used, consult the corresponding section of Available Integrations, on page 21.

When an automation ticket is created and is set to the **Start** state, Cisco Business Dashboard takes control of the ticket and performs the following steps:

1. CBD checks the ticket to ensure all the required information is present. If there is a problem, the internal notes are updated and the ticket is marked as **Needs Attention**.
2. If the ticket is well formed, it is checked to see if approval is required. If so, the ticket is marked as **Needs Approval** and no further action is taken until the ticket is approved.

3. The ticket is checked to see when the action should be performed. If the ticket is set to run now, the dashboard will perform the action immediately. If the action is set to run in the next change window, then a new schedule profile is created and the ticket is updated to show that a job is pending.
4. When the action is complete, the dashboard updates the notes in the ticket with the success or failure of the operation. If the action completed successfully, the ticket is closed. If the action failed, then the ticket is marked as **Needs Attention**. When the reason for the failure is addressed, the ticket can be rescheduled by changing the state back to **Start**, or closed if the action is no longer required.

Approval of automation tickets is an option that allows a degree of change control to be inserted in the automation process. By designating automation tickets to require approval, this ensures that an action is validated by a human prior to it being executed, and that validation is recorded in the ticket history.

A ticket requiring approval may be approved in one of two ways:

1. The ticket may be updated directly using the PSA interface.
2. The ticket may be approved through a collaboration tool that has been integrated with Cisco Business Dashboard. In this case, a note is added to the ticket recording the approval and the identity of the approver.

Managing Network Events with Notification Tickets

To enable the creation of tickets in response to network events, the Cisco Business Dashboard monitoring profiles must be updated to add the **Open Helpdesk Ticket** action to one or more of the notification monitors. For more information on managing monitoring profiles, see Monitoring Profiles.

Note Cisco recommends you configure the Monitoring Profiles to ensure the average rate of 60 tickets and/or collaboration messages per hour is not exceeded on an ongoing basis. When communicating with external applications, sustained rates over this could result in API congestion and loss of events.

When a notification happens that matches a monitoring profile with **Open Helpdesk Ticket** enabled, a new ticket is opened in the notification board and associated with the configuration record for the corresponding device. The body of the ticket is updated with pertinent information about the notification.

For most notification monitors, only notification tickets may be opened. However, in the case of the firmware notification, additional options are available. When a new firmware version is discovered for a device, the ticket created can also be opened as an automation ticket which will apply the firmware update to the device during the next change window.

When configuring the firmware notification in a monitoring profile, two additional options are provided – **With Automation** and **With Approval**. If the **With Automation** checkbox is enabled, then an automation ticket will be created instead of a notification ticket. The ticket will be opened in the automation board, associated with the device configuration, and have a type set to **Upgrade Firmware to Latest**.

Finally, the subtype will be set to schedule the upgrade to occur during the next change window. If the **With Approval** checkbox is enabled, the subtype will also be set to require approval before the upgrade is scheduled.

Using the Collaboration Tools

Use of the collaboration tools with Cisco Business Dashboard falls into two main areas:

- Setting up and receiving notifications of network events.

- Interacting with Cisco Business Dashboard through the limited control interface.

The following sections describe each of these activities in more detail.

Managing Notifications of Network Events

To enable notifications to be sent to a collaboration space in response to network events, the Cisco Business Dashboard monitoring profiles must be updated to add the **Send To Collaboration Space** action to one or more notification monitors. For more information on managing monitoring profiles, see Monitoring Profiles.

Note Cisco recommends you configure the Monitoring Profiles to ensure the average rate of 60 tickets and/or collaboration messages per hour is not exceeded on an ongoing basis. When communicating with external applications, sustained rates over this could result in API congestion and loss of events.

When a notification matching a monitoring profile with **Send To Collaboration Space** enabled occurs, a message is pushed to the collaboration space. The message includes pertinent information about the notification, including notification details, and links to view the device in Cisco Business Dashboard and the associated help desk ticket if one has been created for the event.

Interacting with Cisco Business Dashboard through a Collaboration Space

When integrated with a collaboration tool, Cisco Business Dashboard provides a limited command interface using a collaboration bot that can be used to query the dashboard and take actions.

When invoking a command, the interface requires the user to mention the bot for the command to be accepted. While the interface can tolerate a certain amount of flexibility in input, it does not provide natural language processing, but is limited to a set of pre-defined commands. The table below provides a list of available commands and associated actions.

Table 1: Supported Collaboration Commands

Command	Description
Menu Help ?	Provides a list and descriptions of all the available commands.
Approvals	Provides a list of automation tickets requiring approval. This command is only available when the dashboard is integrated with a Professional Services Automation tool.
Approve <Ticket#>	Marks the specified automation ticket as approved for execution. This command is only available when the dashboard is integrated with a Professional Services Automation tool.
Assets	Initiates the asset synchronization process. This command is only available when the dashboard is integrated with a Professional Services Automation tool.

Command	Description
Firmware	Provides a list of all network devices with an available firmware update.
Upgrade <Serial#>	Schedules a firmware update for the specified device to occur during the next change window. If the dashboard is integrated with Connectwise Manage, an automation ticket requiring approval will be created for this task, or it will be scheduled directly in Cisco Business Dashboard.
Tickets	Provides a list of open tickets in the Automation and Notification boards. This command is only available when the dashboard is integrated with a Professional Services Automation tool.

Available Integrations

For details on setting up the different integrations and the information exchanged with each application, read the corresponding section below.

Connectwise Manage

Connectwise Manage is a Professional Services Automation tool (PSA) designed for use by Managed Services Providers. It includes asset management, accounting and billing, and help desk services as part of its functionality. Integrating Cisco Business Dashboard with Connectwise Manage helps you ensure that asset records are kept up to date for network devices, manage events and network actions with help desk tickets.

Supported Functionality

When integrated with Connectwise Manage, Cisco Business Dashboard offers additional functionality in three main areas: asset management, event management, and automation.

For asset management, Cisco Business Dashboard will automatically create and periodically update configuration records in Connectwise Manage for each network device managed by the dashboard. The configuration record includes information including device type and model, serial number, software information, warranty expiry date, and life-cycle information. If a device is removed from the dashboard inventory the configuration will be marked as inactive, but not deleted from Connectwise Manage.

In addition to creating configuration records, you can opt to associate network device types with specific products in Connectwise Manage and have Cisco Business Dashboard update agreements containing those products with the quantities of devices associated with that customer.

When managing network events, you can configure the Cisco Business Dashboard monitoring profiles so that the dashboard creates help desk tickets when the selected notifications occur. These notification tickets contain details of the event and are associated with the configuration record for the device that generated the notification. In the case of firmware notifications, the ticket can also be created as an automation ticket to apply the firmware update to the device during the next change window.

An automation ticket is a special ticket that results in Cisco Business Dashboard performing a network action. Automation tickets are created in a dedicated service board that the dashboard monitors and can be used to automate the following actions:

- Backup the configuration
- Upgrade to latest Firmware version
- Reboot the device
- Save the running configuration
- Delete the device

Automation tickets can be created to execute immediately, or during the next change window, and may be set to require approval before executing. The ticket will be updated with progress information during execution and the result of the action upon completion.

Prerequisites

Before you set up the Connectwise Manage integration, the following prerequisites must be met:

- If automation tickets will be used, the Connectwise Manage application must be able to establish connections to the Cisco Business Dashboard web server. In addition, Cisco Business Dashboard must have a certificate trusted by Connectwise Manage. In most cases, this means the certificate will need to be signed by a public CA. Refer to Managing Certificates, on page 4 for more details in setting up certificates for Cisco Business Dashboard.
- If the dashboard is located behind a NAT gateway or firewall, make sure the System Variables page under **System** > **Platform Settings** is populated with the host name and web server ports that the Connectwise Manage application will use to connect to the dashboard.
- A set of API Keys must be created for Cisco Business Dashboard, and must have at least the permissions listed in the table below.

Table 2: Permissions Required by the API Key

Permission	Add Level	Edit Level	Delete Level	Inquire Level
Companies				
Company Maintenance	None	None	None	All
Configurations	All	All	All	All
Finance				
Agreements	None	All	None	All
Procurement				
Product Catalog	None	None	None	All
Service Desk				
Service Tickets	All	All	All	All
System				
Table Setup	All	All	All	All

- A service board appropriate for automation tickets must be identified or created. This board has a number of setup requirements that will be applied during the integration process, and it is recommended that this board be dedicated to network operations. See the following section for more details on how this board will be set up.
- A service board appropriate for notification tickets must be identified or created. This board has no specific requirements associated with it and may be an existing, general-purpose board. The notification board may also be the same service board used for automation tickets.

Setting up the Connectwise Manage Integration

There are several steps involved in setting up the Connectwise Manage integration.

- Establish communication with the Connectwise Manage service.
- Map the Connectwise companies to Cisco Business Dashboard organizations.
- Configure the asset synchronization process.
- Select the service boards for event notification and automation.

This section describes how to perform each process of getting it all set up correctly.

Establish Communication with the Connectwise Manage Service

1. Navigate to **System**>**Integration Settings**.
2. Locate the tile representing the Connectwise Manage integration and ensure that the toggle switch is set to **Enabled**.
3. Click on the **Settings** icon to display the Connectwise Manage Settings pages, and then select the **Connection** tab.
4. Complete the fields in the form provided, and then click **Save**. See the table below for details about the requested parameters.

Table 3: Connectwise Manage Connection Parameters

Parameter	Description
API Hostname	The protocol and hostname of the Connectwise Manage service to connect to. It defaults to https://na.connectwise.net.
Company ID	The identifier for the company in Connectwise Manage. This is the same value as used when logging on to the Connectwise Manage GUI.
Public key	The public key from the API key defined in Connectwise Manage for Cisco Business Dashboard.
Private key	The private key from the API key defined in Connectwise Manage for Cisco Business Dashboard.

After clicking **Save**, Cisco Business Dashboard will test the connection, and then read the information from Connectwise Manage that is required later in the setup process. This information includes the list of companies, configuration types, products, agreement types, and service boards. If changes are made to any of this

information in Connectwise Manage, click the **Refresh Connectwise Data** button on this page to re-read the data.

Map Connectwise companies to Cisco Business Dashboard organizations

After establishing the connection between Cisco Business Dashboard and Connectwise Manage, it is necessary to map organizations in Cisco Business Dashboard to companies in Connectwise Manage. Mapping companies to organizations allows network devices and events to be associated with the correct customer in Connectwise Manage. To complete the mapping, follow the steps below.

1. Navigate to **System**>**Integration Settings**.
2. Click on the **Settings** icon on the **Connectwise Manage** tile, then select the **Organization Mapping** tab.
3. Click the **Import from Connectwise** button. This will compare the list of companies with the list of organizations and create mappings when either the company name or company ID match the organization name.
4. Arbitrary mappings between companies and organizations can be made either manually or using comma-separated value (CSV) files.

To Manually Create a Mapping

1. Click the ✚ (plus) icon above the mapping table to create a new entry in the table.
2. From the drop-down lists, select the company and organization name to be mapped.

Note If the desired company name is not listed in the drop-down menu, return to the **Connect** tab and click the **Refresh Connectwise Data** button to update the list of companies.

3. Click the **Save** icon.

To Create Mappings using CSV files

1. Create a CSV file containing the desired mappings between an organization and company name.
2. Click the **Download** icon above the mapping table for a template CSV file that contains a list of the existing mappings.
3. Once the template file is updated, click the **Upload** button above the table to create the new mappings specified in the file.

To Change an Existing Mapping

1. Click the radio button next to the mapping.
2. Click the **Edit** icon.
3. Make the necessary changes.
4. Click the **Save** icon.

To Delete an Existing Mapping

1. Click the radio button next to the mapping.
2. Click the **Delete** icon.

Configure the Asset Synchronization Process

The creation of configuration records in Connectwise Manage to represent the network devices is a pre-requisite for the event management and automation functions to work. Cisco Business Dashboard will automatically create and update configuration records for each network device in organizations that are mapped to a Connectwise manage company. To set up asset synchronization, follow the steps below.

1. Navigate to **System**>**Integration Settings**.
2. Click on the Settings icon on the **Connectwise Manage** tile, then select the **Asset Synchronization** tab.
3. Click the **Create Default Configuration Types in Connectwise** button.

   This will create three configuration types – CBD Managed Router, CBD Managed Switch and CBD Managed WAP – with fields and questions appropriate for the network devices. If these configuration types already exist, they will be updated with the fields and questions.
4. Click the **Save** icon.

Every day at midnight, Cisco Business Dashboard will perform an asset synchronization for each organization that is mapped to a company. For each network device in that organization, a configuration record will be created with information about that device. If a configuration record already exists, it will be updated with any changes to the device information. The configuration record associated with a device that has been deleted from Cisco Business Dashboard will be marked as **Inactive**.

As part of the synchronization process, Cisco Business Dashboard will also do the following:

1. For each company, Cisco Business Dashboard will identify any agreements matching agreement types that you specify.
2. For each agreement Cisco Business Dashboard will identify any additions matching products that you select and associate with each device type.
3. For each of those additions, Cisco Business Dashboard will update the quantity based on the number of devices with types that have corresponding product selected.

To make this happen, do the following:

1. Navigate to **System** > **Integration Settings**.
2. Click on the **Settings** icon on the **Connectwise Manage** tile, then select the **Asset Synchronization** tab.
3. For each device type, click in the **Product** field, and select one or more products to associate with devices of this type.
4. Under the **Agreement Type** heading, select one or more agreement types to identify the agreements to be updated.
5. Click the **Save** icon.

Note If the desired product or agreement type is not listed in the drop down menus, return to the **Connect** tab and click the **Refresh Connectwise Data** button to update the lists.

Select the service boards for event notification and automation

Enable the event management and automation functionality by specifying Service Boards that should be used for each of these functions. To specify the Service Boards to use:

1. Navigate to **System** >**Integration Settings**.
2. Click on the **Settings** icon on the **Connectwise Manage** tile, and then select the **Ticket Settings** tab.
3. From the **Notification Board** drop-down menu, select the appropriate service board to use for tickets that are created in response to network events.
4. From the **Automation Board** drop-down menu, select the service board that should be monitored for automation tickets.

Note If the desired service board is not listed in the drop down menus, return to the **Connect** tab and click the **Refresh Connectwise Data** button to update the list of service boards.

5. Click the **Save** icon.

   Cisco Business Dashboard will update the settings for the automation board in Connectwise Manage to contain the appropriate status values, types, and subtypes needed to support the automation functionality.

Additional Information for the Connectwise Manage Integration

When performing asset synchronization between Cisco Business Dashboard and Connectwise Manage, each managed device known to Cisco Business Dashboard is created as a Configuration associated with the Company that maps to the managed device's organization. The table below lists the mapping between configuration item fields and the data provided by Cisco Business Dashboard.

Table 4: Connectwise Manage Configuration Field Usage

Field	Description
Configuration Name	Set to the device host name
Configuration Details	
Type	The configuration type is set based on the device type and the mappings configured in the Asset Synchronization page.
Status	This is set to **Inactive** if the device has been deleted from the Dashboard inventory, otherwise it is set to **Active**.
Model	The model number of the device.
Serial Number	The serial number of the device.

Field	Description
Company	
Company	The company that corresponds to the organization of the device that is defined in the **Organization Mapping** page.
Notes	
Vendor Notes	Contains a note indicating the configuration was created by Cisco Business Dashboard and displays a creation time stamp.
Configuration Questions	The configuration questions contain the following information: • **The device product ID**: This field is similar to the model number but it is the identifier used when purchasing a new device. • **Software version**: This information includes the current version and the latest available version with release notes. • **Lifecycle information**: This includes details of warranty end dates and applicable end of life bulletins.
Device Details	
IP Address	The management IP address of the device.
MAC Address	The base MAC address of the device.

In Connectwise Manage, automation tickets are managed based on the ticket type, subtype, and status. To create an automation ticket in Connectwise Manage, create a new ticket with the following characteristics:

- The service board should be set to be the automation board created when setting up the integration.
- The ticket should be associated with exactly one configuration representing a network device managed by Cisco Business Dashboard.
- The type should be set to the desired action. Check the **Automation Ticket Types** table below for a list of available actions.
- The subtype should be chosen based on the desired execution time and whether approval is required. Check the **Automation Ticket Subtypes** table below for a list of available options.
- The status should be set to **Start** to begin the automation process. If additional work is required prior to automation commencing, then the status may be set to **Needs Attention** until the work is complete. Check the **Automation Ticket Status** table below for a full list of all the possible status values.

When using tickets requiring approval, neither Connectwise Manage or Cisco Business Dashboard can enforce a requirement for the approver to be a different person from the creator of the ticket. Approvers can not be restricted to a designated list of staff members. Any user who can edit the ticket or who has access to the collaboration space is able to approve a ticket. Operational processes will be necessary to implement restrictions of this kind if required.

Table 5: Automation Ticket Types

Type	Description
Backup Configuration	Take a copy of the current running configuration for the device and save it on Cisco Business Dashboard.
Delete	Remove an offline device from the Cisco Business Dashboard inventory.
Reboot	Restart the device.
Save Running Config	Save the running configuration on the device for use at startup.
Update Firmware to Latest	Upgrade the software on the device to the latest version published by Cisco.

Table 6: Automation Ticket Subtypes

Subtype	Description
Approval Required – Run During Change Window	This action requires approval and should be scheduled to occur during the next change window after the ticket has been approved.
Approval Required – Run Now	This action requires approval and should be executed immediately once the ticket has been approved.
Run During Change Window	The action should be scheduled to occur during the next change window.
Run Now	The action should be executed immediately.

Table 7: Automation Ticket Status

Status	Description
Start	Indicates to Dashboard that the ticket is ready for automation.
Needs Attention	Indicates that human intervention is required. This status may be manually set if there is work required before automation can start and will be set by the dashboard in the event the automation action failed.
In Process	The dashboard is actively processing the ticket.
Needs Approval	Indicates a valid automation ticket that requires approval to proceed. Human intervention is required to proceed.
Approved	Indicates the ticket has been approved and is ready for execution. A ticket may be approved by selecting this status in the Connectwise Manage user interface, or by an approval command in a collaboration tool that has been integrated with Cisco Business Dashboard.
Scheduled with CBD	A job has been scheduled in Cisco Business Dashboard but has not yet executed. The ticket will be updated once the job executes.
Complete (closed)	The requested action completed successfully.

Webex

Webex is a suite of collaboration tools and services that includes messaging, calling, and conferencing. Integrating Cisco Business Dashboard with Webex keeps you notified of critical network events and allows you to take action. You can use the Webex application on your desktop or mobile device.

Supported Functionality

When integrated with Webex, Cisco Business Dashboard can forward notifications to a collaboration space to inform the user of network events. You can customize the notifications through updating the monitoring profiles and then select which ones to forward.

In addition, a limited control interface is provided which allows the user to perform certain actions from the Webex interface. Supported actions include:

- View a list of open help desk tickets created by Cisco Business Dashboard.
- View a list of automation tickets requiring approval.
- Approve automation tickets.
- View a list of network devices with available firmware updates.
- Initiate a network device upgrade.

Prerequisites

Before you set up the Webex integration, you must create a Webex Bot and invite it to a collaboration space. To set up a bot, do the following:

1. Navigate to https://developer.webex.com/my-apps/new/bot and log in to your Webex account.
2. Fill out the form provided to create your bot. You need to provide a name, username, and a description for your bot. You also have the option to provide a custom icon for your bot.

Note Although Webex allows the bot name to contain white space characters, Cisco Business Dashboard requires the bot name to be a single word only with no white space.

3. Click **Add Bot** to create your bot. Take note of the bot token that is presented as you will need it when setting up the Webex integration.

Remember The bot token will only be displayed once, so it is important to record it in a safe place for future reference.

After the bot has been created, it must be invited to a collaboration space. A dedicated space be created for the purposes of interacting with Cisco Business Dashboard, but an existing space can also be used. However, any member of the space will have visibility of all events and the ability to execute all supported commands, so the space should only have users authorized to manage the network.

Consult the Webex documentation or the online help for the Webex app for details on creating spaces and inviting users.

Note The bot should only be invited to a single collaboration space when integrated with Cisco Business Dashboard. The behavior of the bot will be unpredictable if invited to multiple spaces.

In addition to creating a bot, you should ensure that the Webex infrastructure is able to establish connections to the Cisco Business Dashboard web server. If the dashboard is located behind a NAT gateway or firewall, make sure the System Variables page under **System** > **Platform Settings** is populated with the host name and web server ports that the Webex infrastructure will use to connect to the dashboard.

Setting up the Webex Integration

To set up the Webex integration, do the following:

1. Navigate to **System**>**Integration Settings**.
2. Locate the Webex integration tile and ensure the toggle switch is set to **Enabled**.
3. Click on the **Settings** icon to display the **Webex Settings** page.
4. Copy the bot token you received when creating the bot into the field provided and click the **Save** icon.
5. Ensure that the status fields display the correct bot name and collaboration space.

Note The bot should only be used by a single instance of Cisco Business Dashboard and not with any other applications. If multiple applications are associated with the bot, the behavior will be unpredictable.

Once Cisco Business Dashboard has been configured with the bot details, you can configure monitoring profiles to forward notifications to the collaboration space. For more details on monitoring profile configuration, see Monitoring Profiles.