Crestron Flex UC-P8 and UC-P10 Series Desk Phones and Displays for Microsoft Teams® Software

Product Manual

Crestron Electronics, Inc.

The original language version of this document is U.S. English.
All other languages are a translation of the original document.

Regulatory Model: M202029001, M202029002

Contents

Overview

The Crestron Flex UC-P8 and UC-P10 series desk phones and displays are designed for use with the Microsoft Teams® communications platform.

The information provided in this product manual is applicable to the following desk phones and displays variants:

Crestron Flex Desk Phones for Microsoft Teams

The Crestron Flex desk phones listed below provide superior voice calling, simple operation, hands-free conferencing, and a consistent user experience with the Microsoft Teams touch screen UI.

- UC-P8-T-HS
- UC-P8-T-HS-I
- UC-P8-T-C-HS
- UC-P8-T-C-HS-I
- UC-P10-T-HS
- UC-P10-T-HS-I
- UC-P10-T-C-HS
- UC-P10-T-C-HS-I
- UC-P8-T (Discontinued)
- UC-P8-T-I (Discontinued)
- UC-P8-T-C (Discontinued)
- UC-P8-T-C-I (Discontinued)
- UC-P10-T (Discontinued)
- UC-P10-T-I (Discontinued)
- UC-P10-T-C (Discontinued)
- UC-P10-T-C-I (Discontinued)

> **NOTE:** The UC-P10-T-C-HS, UC-P10-T-C-HS-I, UC-P8-T-C-HS, and UC-P8-T-C-HS-I Microsoft Teams desk phones can be upgraded to Teams display. To upgrade the Microsoft Teams desk phone to Microsoft Teams display, refer to Microsoft Teams Display Upgrade on page 32.

Crestron Flex Displays for Microsoft Teams Display

The Crestron Flex displays listed below provide a native Microsoft Teams display experience. In addition to Microsoft Teams supported features, Microsoft Teams display offers unique features such as:

- **Dedicated displays for Teams** allow users to access all core Microsoft Teams features.
- **Ambient personalizable display** allows users to see important activities and notifications without context-switching on their primary work device.
- **Leave a note on lock screen** allows users to check audio, video, and text notes left by guests.

To learn more, see Microsoft Teams displays.

- UC-P8-TD
- UC-P8-TD-I
- UC-P10-TD
- UC-P10-TD-I

> NOTES:
>
> - The included handset and capacitive Microsoft Teams button are not supported by Microsoft Teams display software.
> - Remote Control via XIO Cloud is not supported by Microsoft Teams display software.

Audience

This manual provides instructions and other technical resources to the installer for setting up Crestron Flex UC-P8 and UC-P10 series desk phones and displays, from here on in referred to as device, for Microsoft Teams. For more information on installing any of these devices, visit www.crestron.com/flex.

Web Interface Configuration

The web interface of the device allows you to view status information and configure network and device settings. This interface is also accessible using the XiO Cloud® service.

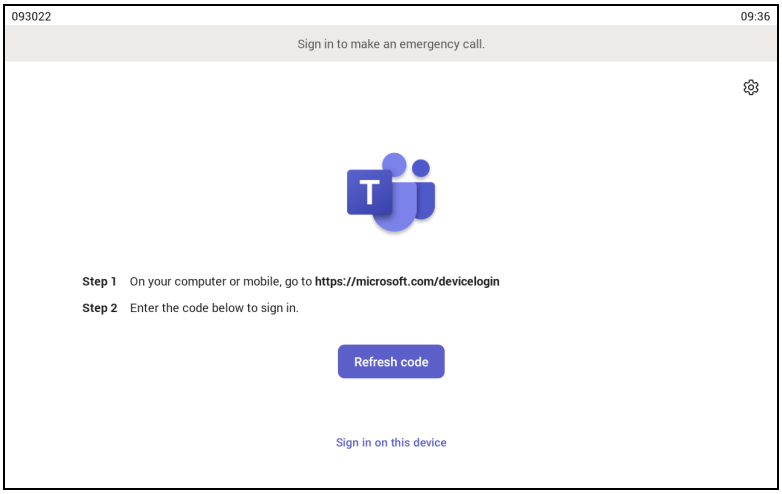
> **NOTE:** Unless otherwise indicated in this guide, the web interface is the same for all desk phones and displays.

Configuration requires a computer with a web browser. The device and computer must be connected to a commonly accessible network.

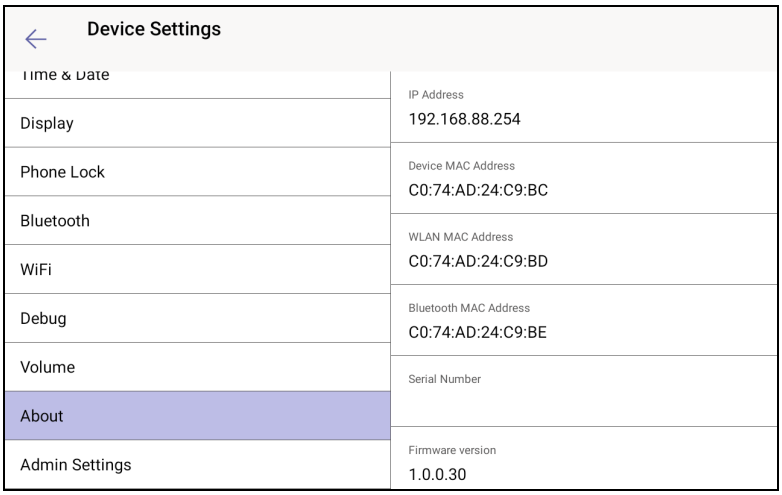
Connect to the Device

To connect to the device:

1. On the device:
   a. Tap ⚙ to access **Device Settings**.



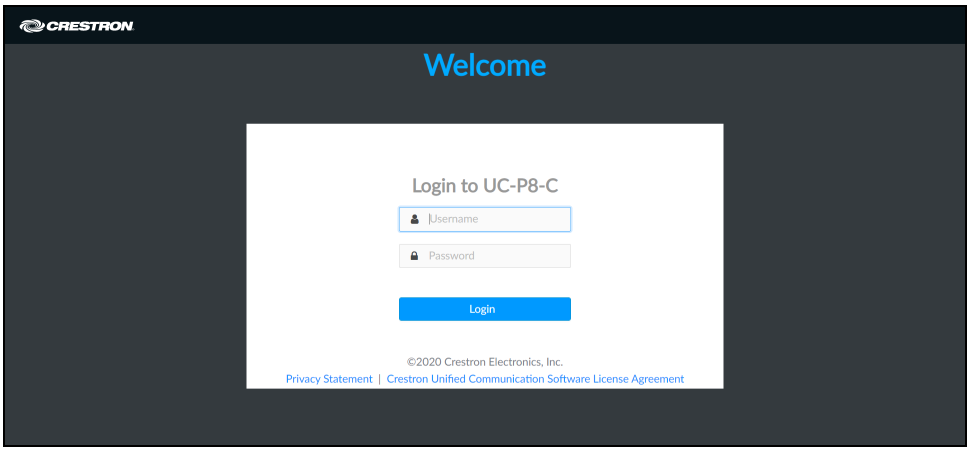
   b. Select **About** from the list that appears.



   The About page displays the IP address, Device MAC, Firmware version and other system information.

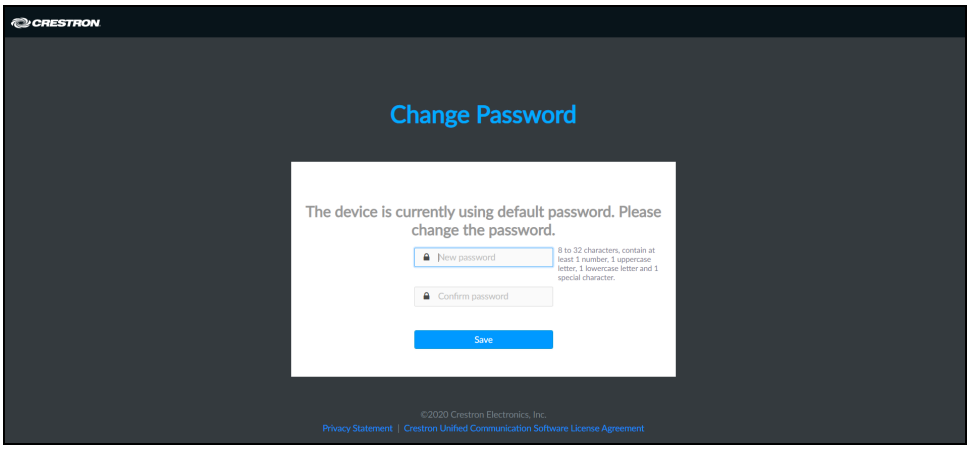
   c. Note the IP address and tap ← to close the About screen.

2. On the computer:
    a. Open a web browser.
    b. Enter the IP address into the browser URL field. The Welcome screen appears.

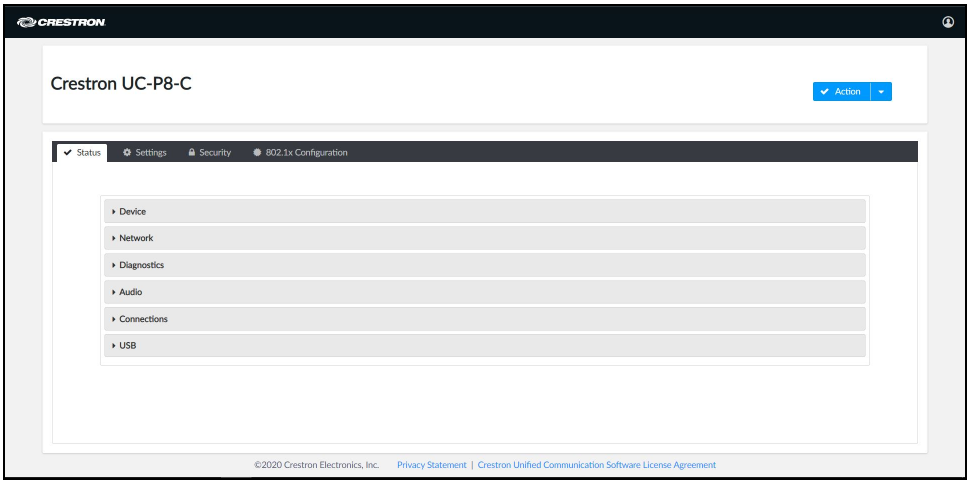


> **NOTE:** Before prompting you to login, the web browser may display a security warning message about the security certificate. It is safe to ignore this warning as long as the user verifies that the browser's address bar indicates the correct IP address or host name of the device.

3. Enter the default username (admin) and password (admin), and click **Login** to continue. The first time the web configuration interface is accessed, a dialog box is displayed asking the user to change the default password. Create a new password and click **Save** to continue.



The configuration interface is displayed.



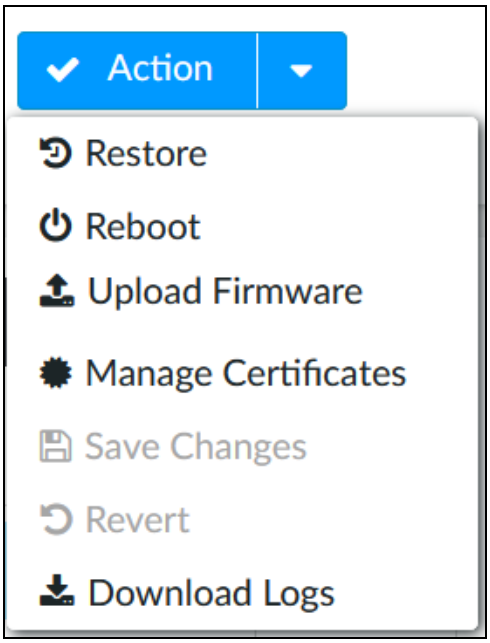
The configuration interface displays the **Action** drop-down menu and the following tabs:

- **Status**: Used to monitor device status
- **Settings**: Used to configure device settings
- **Security**: Used to enable authentication and other security settings
- **802.1x Configuration**: Used to configure IEEE 802.1x network authentication for the device security

Action

The **Action** drop-down menu is displayed at the top right side of the interface and provides quick access to common device functionalities, such as:

- Restore
- Reboot
- Upload Firmware
- Manage Certificates
- Save Changes
- Revert
- Download Logs



Once any changes have been made to the device configuration, the **Action** button changes to a **Save Changes** button. Click **Save Changes** to save changes to the configuration settings.

If a reboot is required after changes have been saved, a dialog box is displayed asking whether the reboot should be performed. Select **OK** to reboot the device or **Cancel** to cancel the reboot.

The Action menu provides the following selections.

Restore

Click **Restore** to restore the device configuration settings to their default values.

> **NOTE:** The device retains the **Language** and **WiFi** settings even after restore.

After selecting **Restore**, a dialog box is displayed asking whether the device settings should be restored. Select **OK** to restore the settings or **Cancel** to cancel the restore.

Reboot

Click **Reboot** to reboot the device.

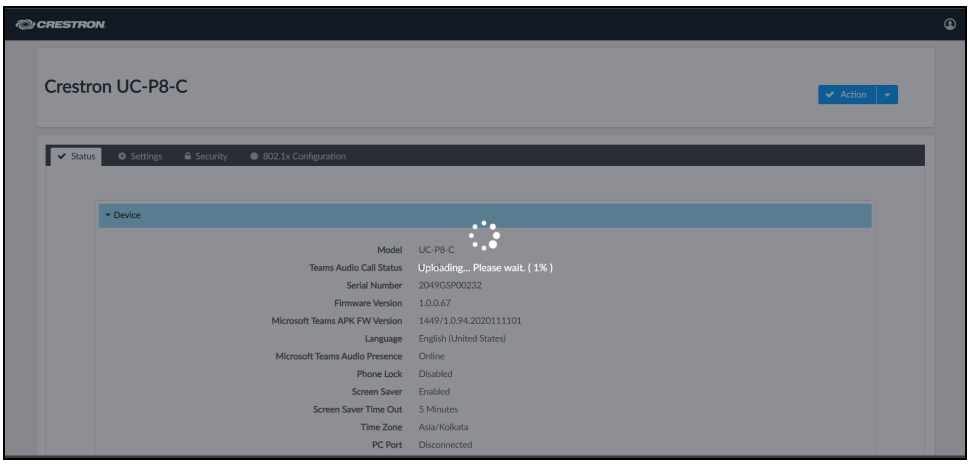
After selecting **Reboot**, a dialog box is displayed asking whether the device should be rebooted. Select **OK** to reboot the device or **Cancel** to cancel the reboot.

Upload Firmware

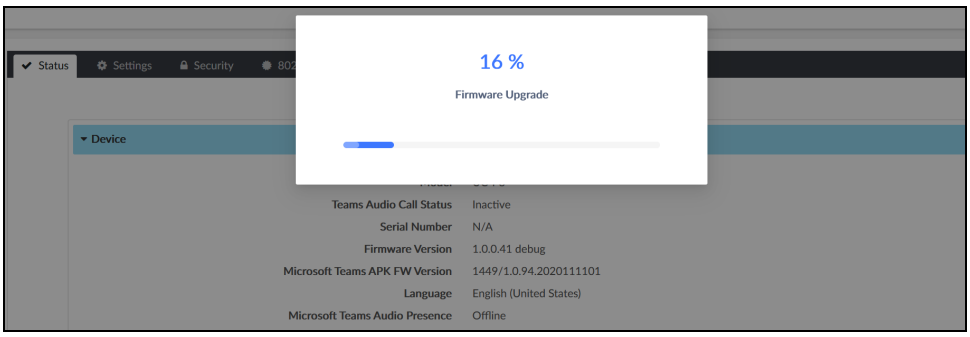
To upgrade the device firmware manually using the web configuration interface:

> **NOTE:** For time-based auto update of the firmware or apk, refer to the Auto Update on page 21 .

1. Visit www.crestron.com/firmware and download the latest firmware file.
2. Click **Upload Firmware**.
3. On the dialog box, browse and select the firmware file to upload.



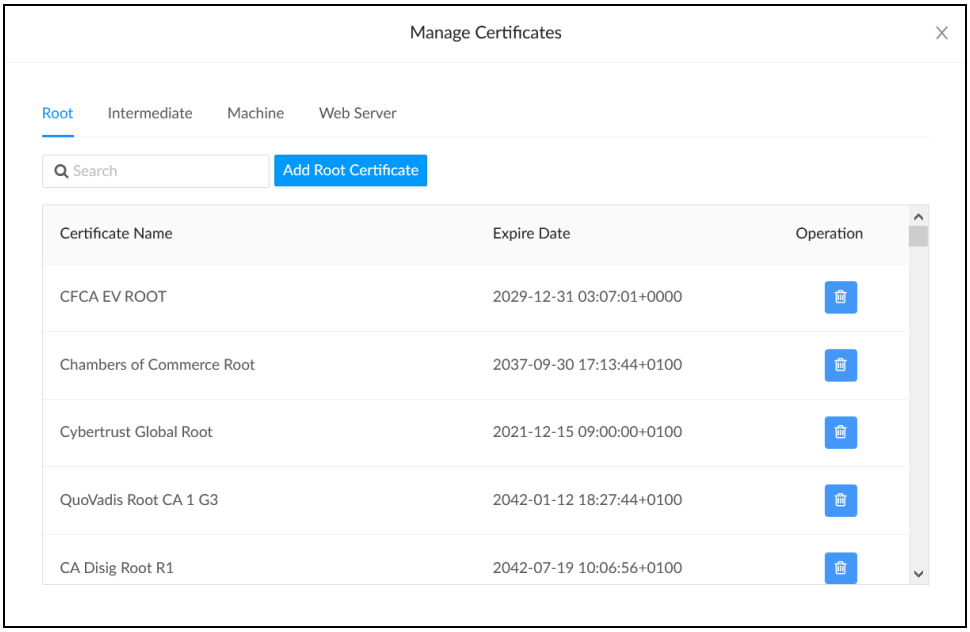
The firmware upgrade process starts once the firmware file is uploaded.



NOTE: Do not turn off the device or stop the upgrade process until the device is upgraded. After the upgrade, the device will reboot.

Manage Certificates

Click **Manage Certificates** in the **Action** drop-down menu to add, remove and manage certificates used in 802.1x and other protected networks. The following certificate tabs are displayed:



- **Root**: The Root certificate is used by the device to validate the network's authentication server. The device has a variety of Root certificates, self-signed by trusted CAs (Certificate Authorities), and preloaded into the device. Root certificates must be self-signed.
    1. Select the **Root** tab.
    2. Click **Add Root Certificate**.
    3. Select the certificate file from the dialog box that is displayed and click **Open**.
- **Intermediate**: The Intermediate store holds non self-signed certificates that are used to validate the authentication server. These certificates will be provided by the network administrator if the network does not use self-signed Root certificates.
    1. Select the **Intermediate** tab.
    2. Click **Add Intermediate Certificate**.
    3. Select the certificate file from the dialog box that is displayed and click **Open**.
- **Machine**: The machine certificate is an encrypted PFX file that is used by the authentication server to validate the identity of the device. The machine certificate will be provided by the network administrator, along with the certificate password. For 802.1x, only one machine certificate can reside on the device.
    1. Select the **Machine** tab.
    2. Click **Add Machine Certificate**.
    3. Select the certificate file from the dialog box that is displayed and click **Open**.
- **Web Server**: The Web Server certificate is a digital file that contains information about the identity of the web server.
    1. Select the **Web Server** tab.
    2. Click **Add Web Server Certificate**.
    3. Select the certificate file from the dialog box that is displayed and click **Open**.

Save Changes

Click **Save Changes** to save any changes made to the configuration settings.

Revert

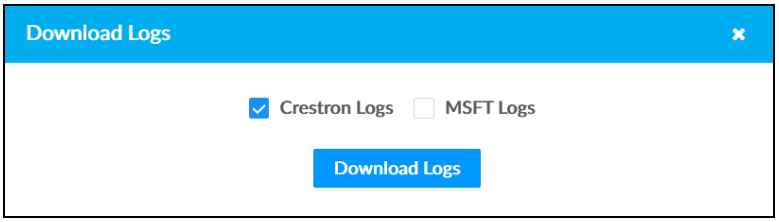
Click **Revert** to revert the device back to the last saved configuration settings.

Download Logs

Click **Download Logs** to download the device message logs for diagnostic purposes. The message files are downloaded in a compressed .tgz file. Once the compressed file is downloaded, extract the message log files to view them.

Select the logs to download:

- Crestron Logs - Logs related to the device
- MSFT Logs - Logs related to Microsoft Teams software



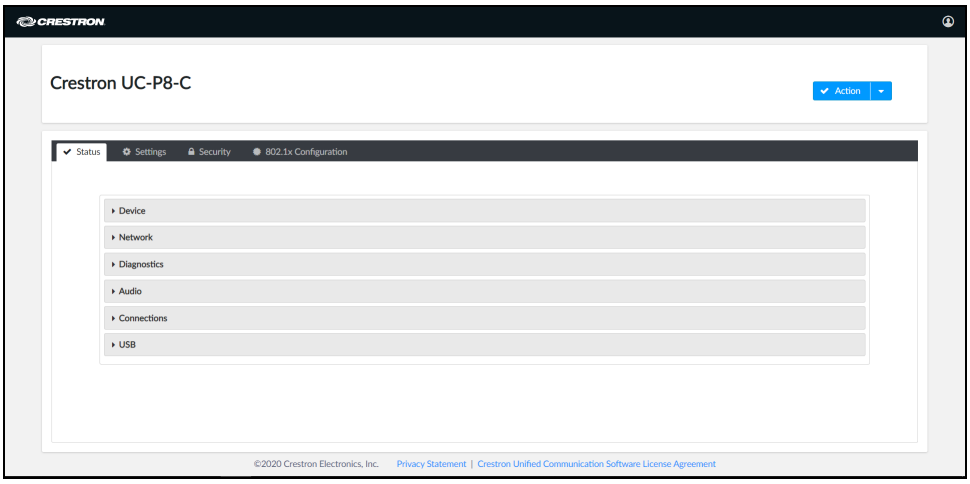
Status

The Status tab is the default tab that displays after login. The Status screen displays information about the device and its other operating parameters.

- Click **Device** to view the device information. Click **+ Show More Details** to view more details. Click **- Show Less** to view fewer details.
- Click **Network** to view network information.
- Click **Diagnostics** to view diagnostics information. Click **RUN** to start the Wi-Fi diagnostics process.

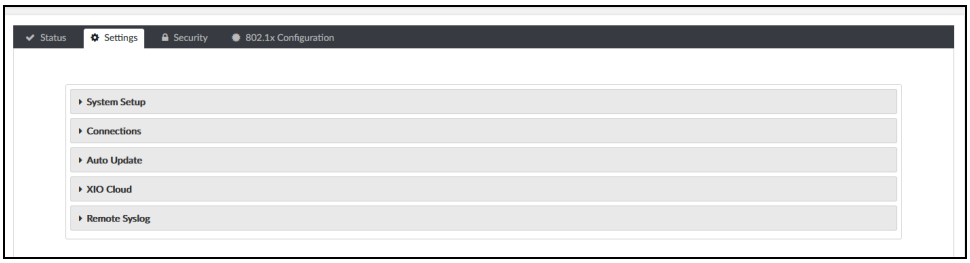
  > **NOTE:** The device must be connected to a Wi-Fi® network before running the diagnostic process.

- Click **Audio** to view audio information including **Mic Mute Status** and **Phone Status**.
- Click **Connections** to view the Bluetooth® connection status.
- Click **USB** to view the USB accessory status.



Settings

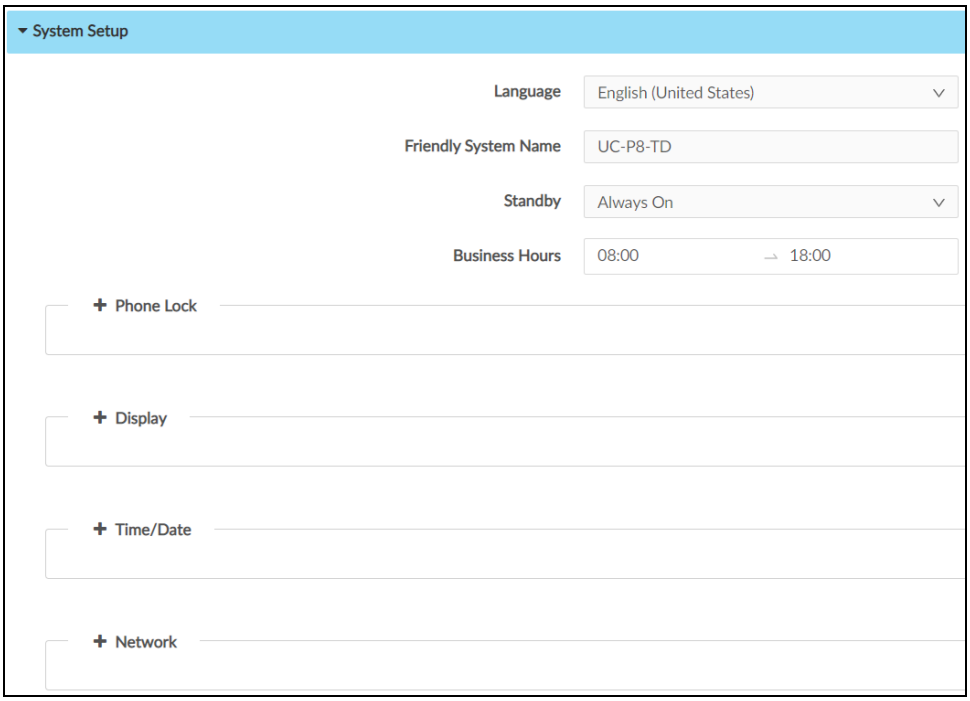
Click the **Settings** tab to display selections for configuring various device settings.



Each selection is described in the following sections.

System Setup

Click **System Setup** to configure general network and device settings.



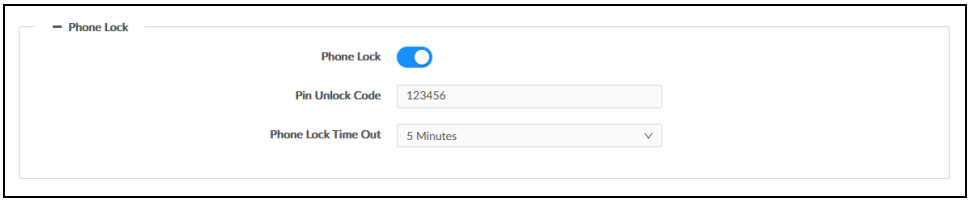
- Select the **Language** from the drop-down. The selected language will be used on the device screen.
- Set **Friendly System Name** to differentiate between different devices. The device model name appears by default.

- Set the **Standby** mode to **Always On** or **Occupancy Based**.
    - If **Always On** is selected, enter the **Business Hours**. The device will not go into sleep mode during the specified business hours.
    - If **Occupancy Based** is selected, enter the **Standby Timeout (Minutes)**, after which the device will go into sleep mode. The default value is 5 minutes. The range is 5-120 minutes.

> **NOTE:** Standby mode will show a black screen only. No screen saver will be displayed.

Touch the screen to wake up the device from Standby mode. The device supports motion detection to automatically wake up.

Phone Lock



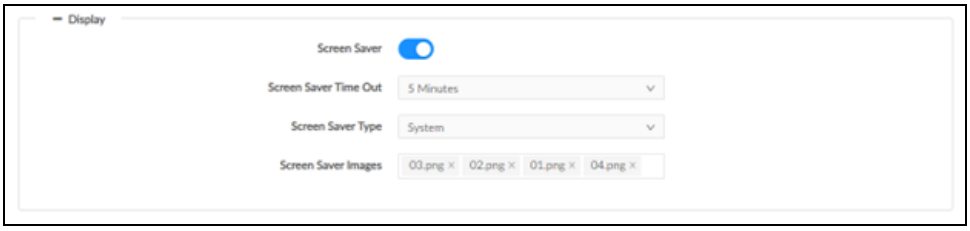
Phone Lock: Move the slider to the right to enable the phone lock.

If enabled, set the corresponding parameters:

Pin Unlock Code: Enter a 6 digit PIN code to unlock the phone.

Phone Lock Time Out: Select the inactivity duration after which the phone automatically locks the screen. The default value is 5 minutes. The range is 30 seconds to 120 minutes.

Display



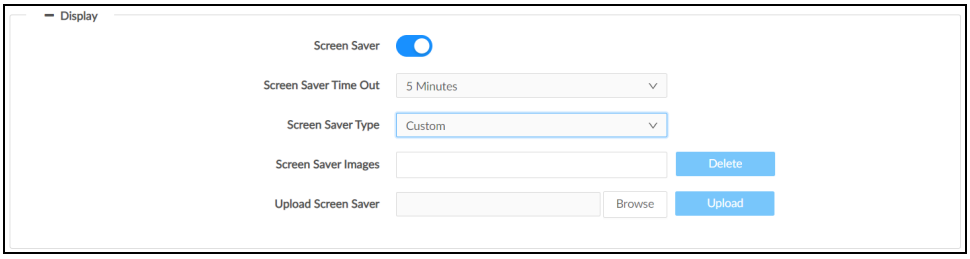
Screen Saver: Move the slider to the right to enable the screen saver.

If enabled, set the corresponding parameters:

Screen Saver Time Out: Select the inactivity duration after which the screen saver will be displayed on the screen. The default value is 5 minutes. The range is 30 seconds to 120 minutes.

Screen Saver Type: Select **System** or **Custom** from the drop-down menu.

- **System**: Displays the default screen saver images in the **Screen Saver Images** field.
- **Custom**: Allows the user to upload desired images as a screen saver.



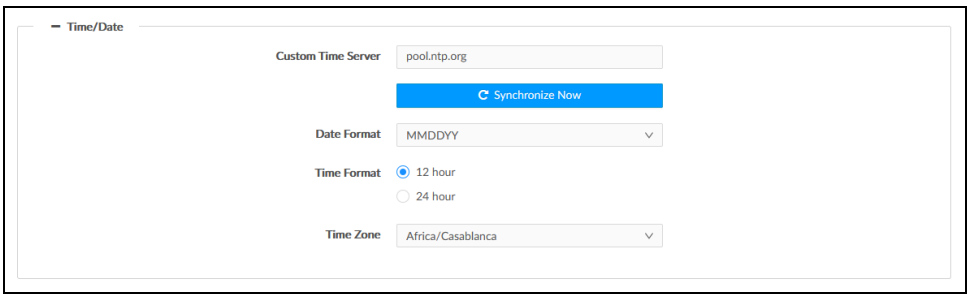
To upload a custom screen saver:

1. Click **Browse**, and then navigate to the desired image file on the computer.
2. Select the desired image file and then select **Open**.
3. Click **Upload**.
   A pop-up message appears confirming a successful upload.

   > **NOTE:** A maximum of seven images, up to 5 MB each can be uploaded.

4. Click in the **Screen Saver Images** field to view the uploaded image(s).
   A list of all the uploaded images displays.
   a. Select the desired image from the list.
      The selected image will be saved as a screen saver.
   b. Optionally, click **Delete** to delete the selected image(s).

Time/Date

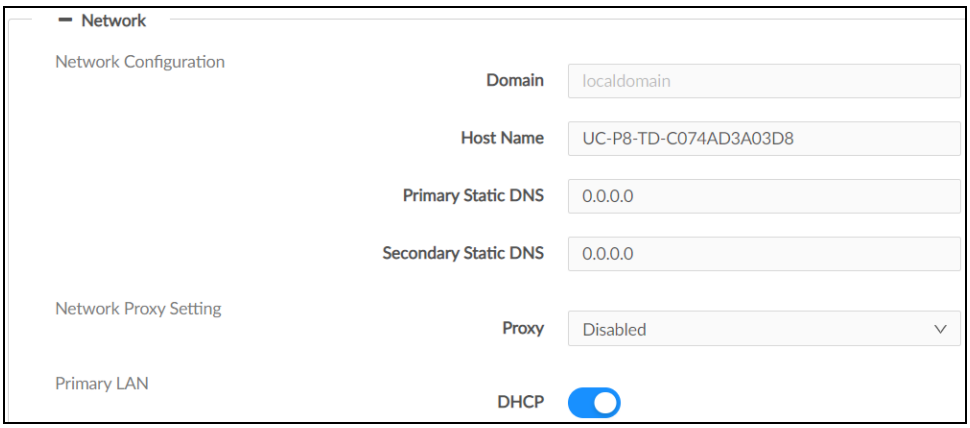


- Enter the URL of the **Custom Time Server** to use for time synchronization. Default is "pool.ntp.org."
- Click **Synchronize Now** to trigger the synchronization process.
- Select the **Date Format** to be used on the device. The available options are:
  - MMDDYY (Default)
  - DDMMYY
  - YYYYDD

- Set **Time Format** to 12 hour (default) or 24 hour.
- Select the local time zone from the **Time Zone** drop-down.

Network

Click **Network** to configure the device for operating in a network environment. The screen displays controls for configuring the network and Wi-Fi settings.

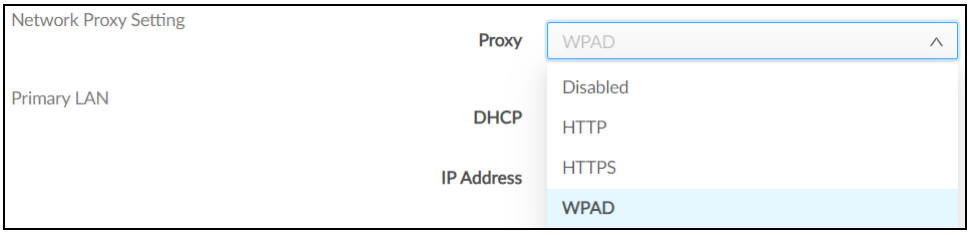


Network Configuration

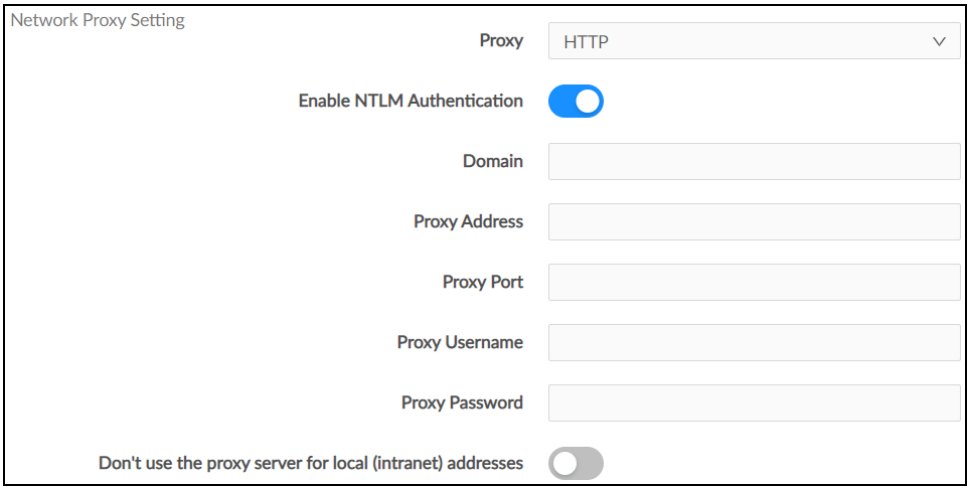
- **Domain**: The domain name is autopopulated if the DHCP is enabled. To edit the domain name, set the DHCP slider to disabled.
- **Host Name**: Enter the device host name.
- **Primary Static DNS**: Enter the primary DNS address.
- **Secondary Static DNS**: Enter the secondary DNS address.

Network Proxy Setting

- **Proxy**: Select one of the proxy setting options, **Disabled**, **HTTP**, **HTTPS**, or **WPAD** from the drop-down menu.

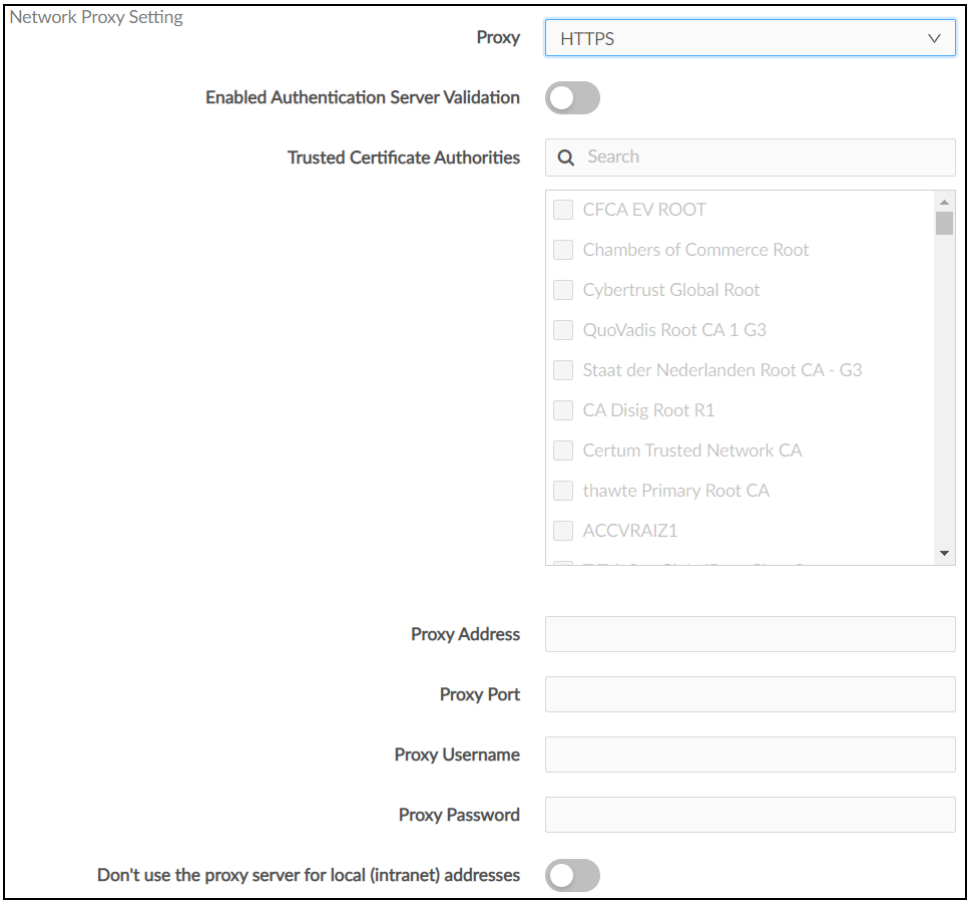


  - **Disabled**: Selecting the **Disabled** option disables the proxy.
  - **HTTP**: Selecting the HTTP option displays multiple fields.



    - **Enable NTLM Authentication**: Move the slider to the right to enable authentication and to the left to disable it.
    - **Domain**: Type the domain name of the network in the **Domain** field. The **Domain** option appears only when **Enable NTLM Authentication** is enabled.
    - **Proxy Address**: Enter the IP address of the HTTP proxy server.
    - **Proxy Port**: Enter the port number of the HTTP proxy server.
    - **Proxy Username**: Enter the username required for the HTTP proxy server.
    - **Proxy Password**: Enter the password required for the HTTP proxy server.
    - **Don't use the proxy server for local (intranet) addresses**: Move the slider to the right if you do not wish to use the proxy server for local (intranet) addresses, otherwise, move it to the left.

- **HTTPS**: Selecting the HTTPS option displays multiple fields.



  - **Enabled Authentication Server Validation** and **Trusted Certificate Authorities**: Enabling the **Enable Authentication Server Validation** option will enable the **Trusted Certificate Authorities** list box which contains signed Trusted Certificate Authorities (CAs) preloaded into the device.

    Select the check box next to each CA whose certificate can be used for server validation, as specified by the network administrator.

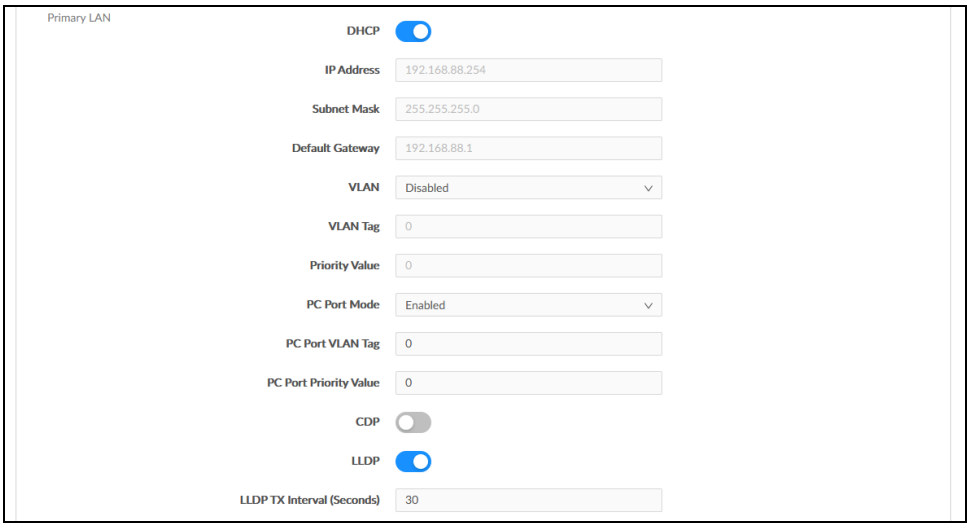
    If the network does not use any of the listed certificates, the network administrator must provide a certificate, which must be uploaded manually via the **Manage Certificates** functionality.
  - **Proxy Address**: Enter the IP address of the HTTPS proxy server.
  - **Proxy Port**: Enter the port number of the HTTPS proxy server.
  - **Proxy Username**: Enter the username required for the HTTPS proxy server.
  - **Proxy Password**: Enter the password required for the HTTPS proxy server.
  - **Don't use the proxy server for local (intranet) addresses**: Move the slider to the right if you do not wish to use the proxy server for local (intranet) addresses, otherwise, move it to the left.
- **WPAD**: Select the WPAD option to use WPAD proxy settings.

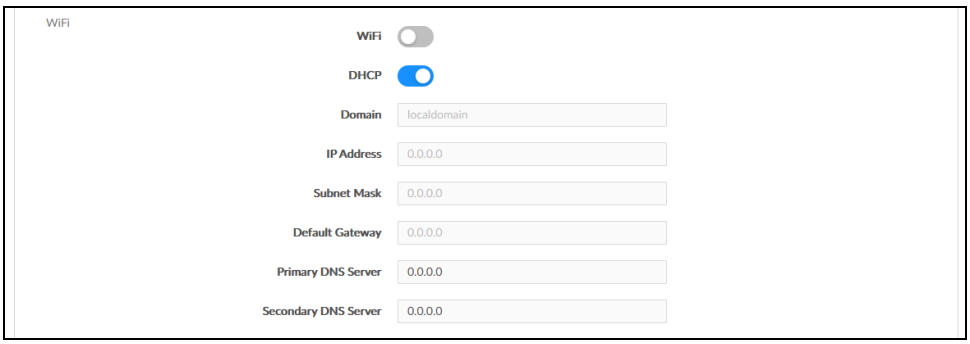
Primary LAN and **WiFi**

The device has two network adapters, **Primary LAN** and **WiFi**. Each network adapter can be set to have its IP address, subnet mask, default gateway, and DNS servers set manually, or obtain the settings from a DHCP server. Choose one of the following options for each network adapter.

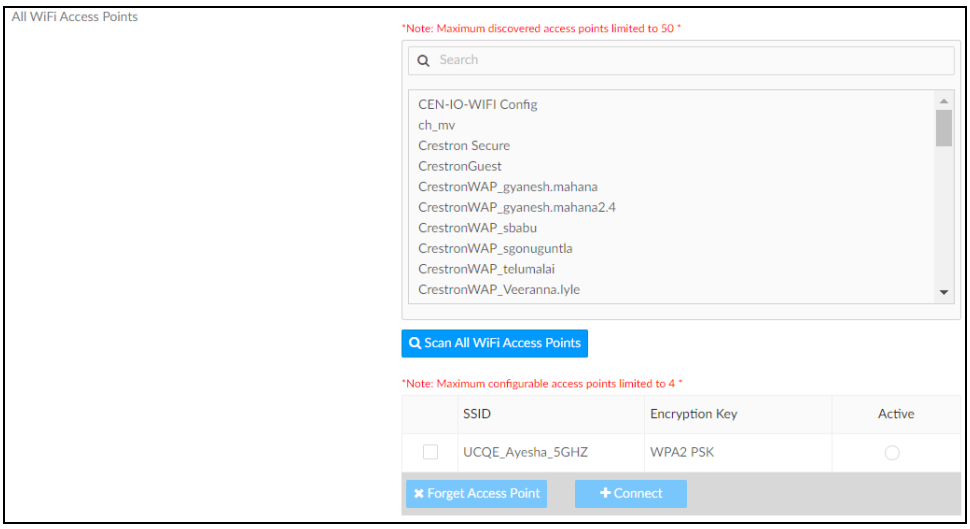
- Set **DHCP** to enabled to use a DHCP server to provide the IP address, subnet mask, and default gateway.
- Set **DHCP** to disabled to manually enter the Ethernet parameters. When set to Off, the IP address, subnet mask, default gateway, and DNS servers must be manually entered.

> **NOTE:** The **Primary DNS Server** and **Secondary DNS Server** parameters can only be set manually, regardless if the **DHCP** is enabled or disabled.



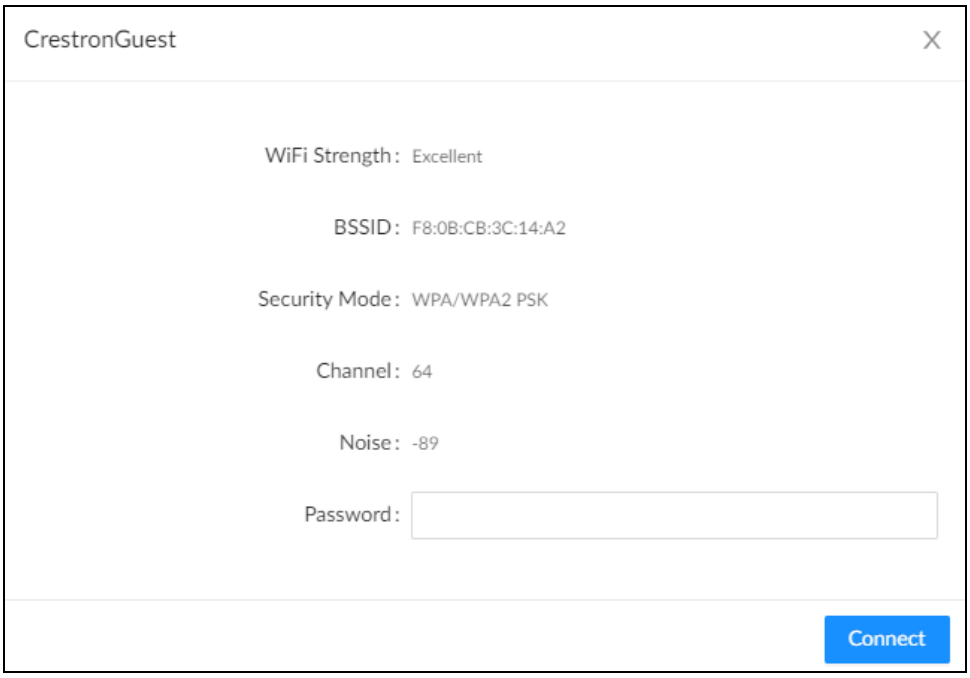


All WiFi Access Points : Displays all the available WiFi access points.



Scan all WiFi Access Points: Scans the network for any open WiFi access points. Select the desired access point from the list that appears or type in the search bar to search for a specific WiFi access point name.

Selecting a password protected WiFi access point displays a pop-up widow to enter the password. Enter the password used to connect to the WiFi access point.



Each added Wi-Fi access point is displayed in a table that contains the following information.

- **SSID**: Displays the SSID (name) of the WiFi access point.
- **Encryption Key**: Displays the security/encryption type used by the WiFi access point.
- **Active Access Point**: Indicates whether a connection to the WiFi access point is active.

Click **Save Changes** or **Revert** to return to the previous setting.

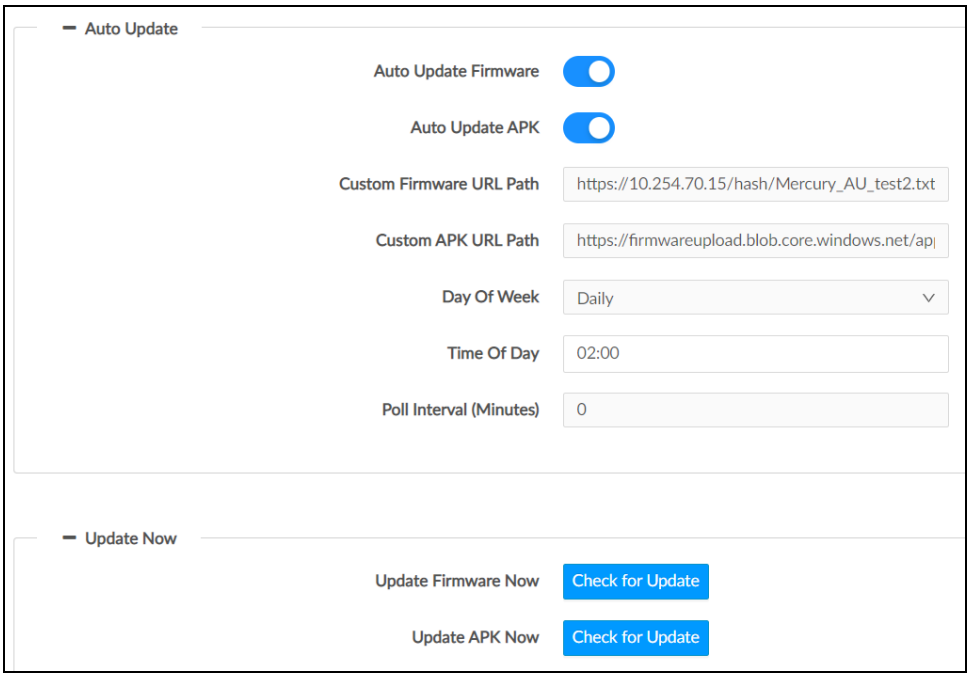
Connections

Click **Connections** to configure Bluetooth connectivity. By default, **Bluetooth** is set to enabled. To disable it, set **Bluetooth** to disabled.

Auto Update

Click **Auto Update** to configure time-based auto-update of firmware/apk or immediate update.

> **NOTE:** Disable auto-update if upgrading the device from Microsoft portal.



To configure **Auto Update**:

1. Enable **Auto Update Firmware**.
2. Enable **Auto Update APK**.

3. Set **Custom Firmware URL Path**. Keep the default path to use the Crestron firmware server or specify your firmware server path.

   > **NOTE:** Do not change the default URL unless advised by a Crestron Tech Support Specialist.

4. Set **Custom APK URL Path**. Keep the default path to use the Crestron APK server or specify your APK server path.

   > **NOTE:** Do not change the default URL unless advised by a Crestron Tech Support Specialist.

5. The Auto Update interval to update the firmware can be set in one of the ways:
   a. Specify **Day Of Week** and **Time Of Day**

      or,

   b. Specify the duration in **Poll Interval (Minutes)**. The range is 1 minute to 65535 minutes. The default value 0 sets **Poll Interval (Minutes)** to disabled.

   > **NOTE:** Enabling **Poll Interval (Minutes)** overrides the **Day Of Week** and **Time Of Day** configuration.

The device will connect to the firmware server provided in the **Custom URL Path** at the scheduled time.

Click **Check for Update** beside **Update Firmware Now** and/or **Update APK Now** to trigger the upgrade process immediately.

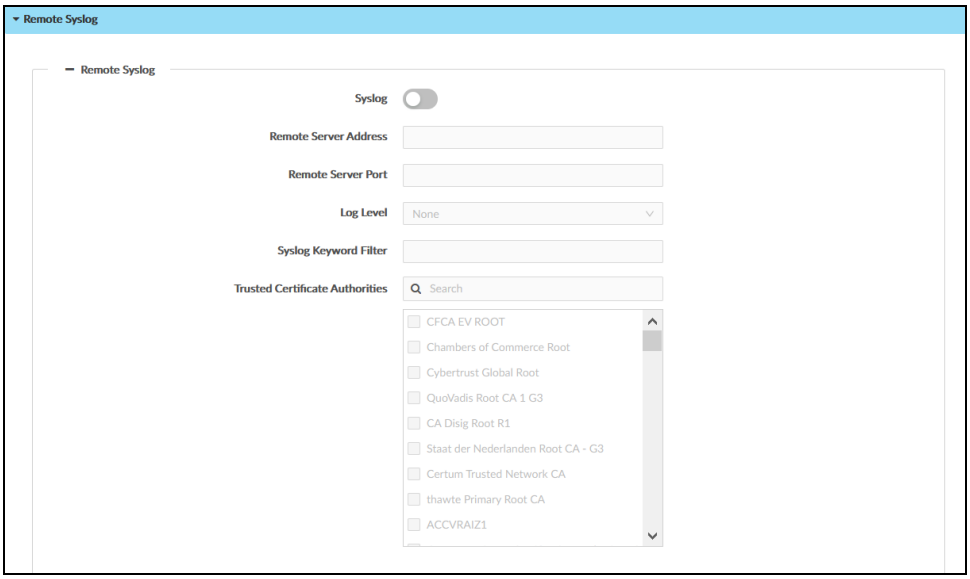
XiO Cloud

By default, the **Cloud Configuration Service Connection** is set to enabled. To disable the connection, set **Cloud Configuration Service Connection** to disabled.

Remote Syslog

Control system messages can be captured and stored on a remote server using the remote system logging function.

NOTE: The remote server host must have a system log server with the applicable security certificates and sufficient disk space to store the active system log. The host must also be configured to archive older system logs and to off-load them over time. If TLS is enabled, a TLS-enabled server with the appropriate certificates is required.



To configure remote system logging:

1. Switch **Syslog** to enabled.
2. Enter the IP address or Fully Qualified Domain Name (FQDN) in the **Remote Server Address**.
3. Enter the port number in the **Remote Server Port**. The range is 0 to 65535.
4. Select **Log Level** for Syslog. The default setting is **None**. There are four levels to select from the drop-down list: **DEBUG**, **INFO**, **WARNING**, and **ERROR**. Syslog messages are sent based on the following events:
    - Product model/version on boot up (INFO level)
    - NAT related info (INFO level)
    - Sent or received SIP message (DEBUG level)
    - SIP message summary (INFO level)
    - Inbound and outbound calls (INFO level)
    - Registration status change (INFO level)
    - Negotiated codec (INFO level)
    - Ethernet link up (INFO level)
    - SLIC chip exception (WARNING and ERROR levels)
    - Memory exception (ERROR level)

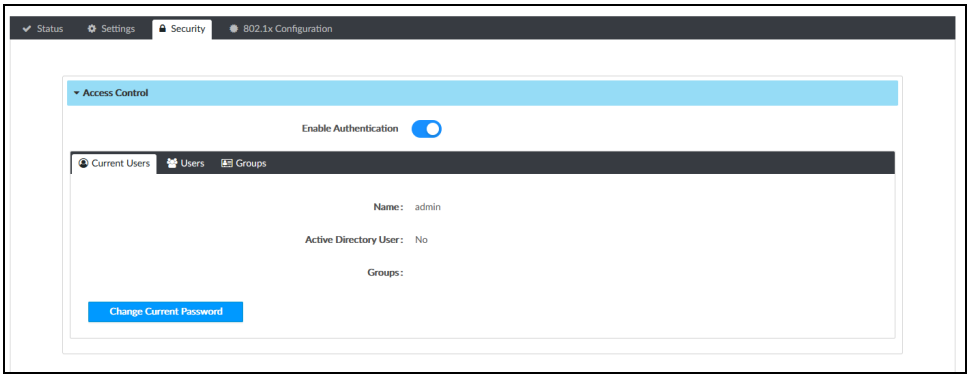
5. (Optional) Enter Syslog Keyword Filtering: Syslog will be filtered based on keywords provided. If you enter multiple keywords, it should be separated by a "comma." Please note that spaces are not allowed.

Security

Click the **Security** tab to configure security for users and groups and to allow different levels of access to the functions of the device.

Access Control

This section allows setting a password for the current user managing authorized users and user groups. By default, **Enable Authentication** is enabled.



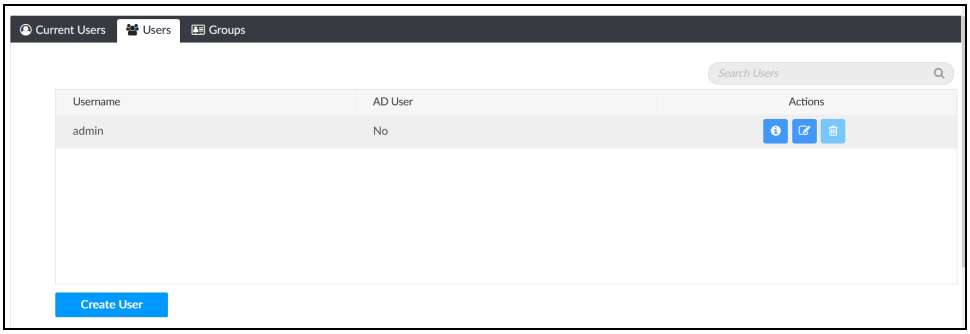
Current Users

Select the **Current Users** tab to set the current user's password.

1. Click **Change Current User Password** to change the current user's password. Enter the new password in the Password field.
2. Confirm the new password in the Confirm Password field.
3. Click **Yes** to set the new password or click **No** to cancel.

Users

Select the **Users** tab to manage authorized users. A list of authorized users is displayed.



- Click  to view details about a user.
- Click  to update a user's information.
- Click  to delete the user from the list of authorized users.

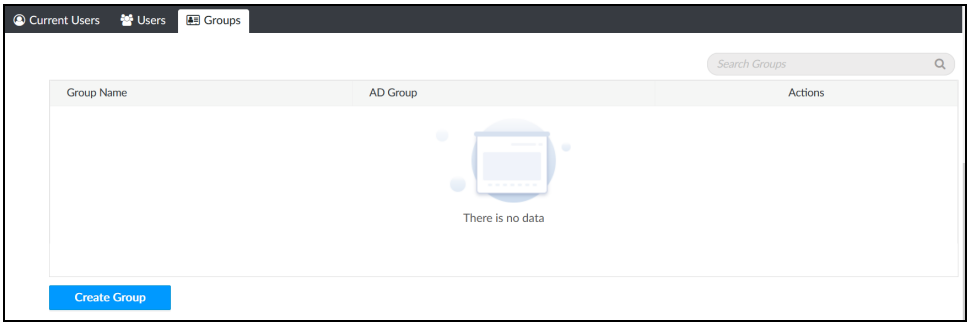
> **NOTE:** The Admin user cannot be deleted.

- Click **Create User** to add a user. The Create User dialog box is displayed.

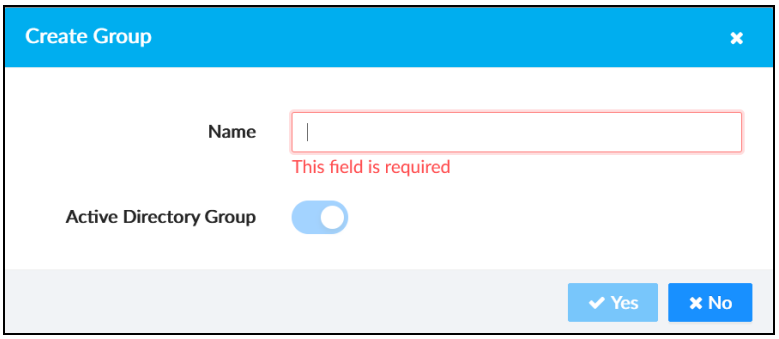
1. Enter the username in the Name field.
2. Set **Active Directory User** to enabled if the user is a member of the Active Directory® credential management group.
3. Click **Yes** to save the user or click **No** to cancel.

Groups

Select the **Groups** tab to configure user groups. A list of user groups is displayed.



- Click to view details about a group.
- Click to delete the group from the list of groups.
- Click **Create Group** to add a group to the list of user groups. The Create Group dialog box is displayed.

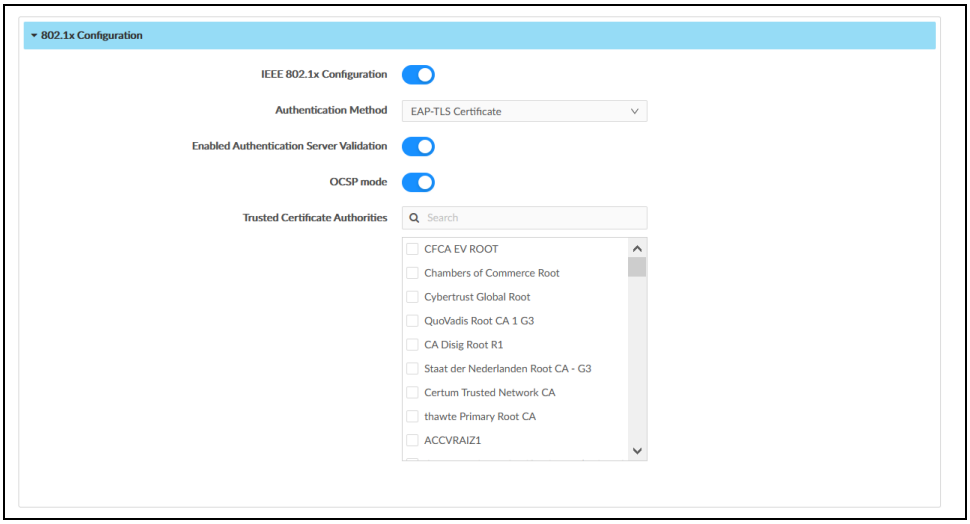


1. Enter the group name in the **Name** field.
2. Set **Active Directory Group** to enabled if the group is part of the Active Directory credential management group.
3. Click **Yes** to save the user or click **No** to cancel.

802.1x Configuration

The 802.1X standard is an IEEE network standard designed to enhance the security of wireless and Ethernet LANs. The standard relies on the exchange of messages between the device and the network's host, or authentication server.

The device has built-in support for the 802.1X standard to allow communication with the authentication server and access to protected corporate networks.

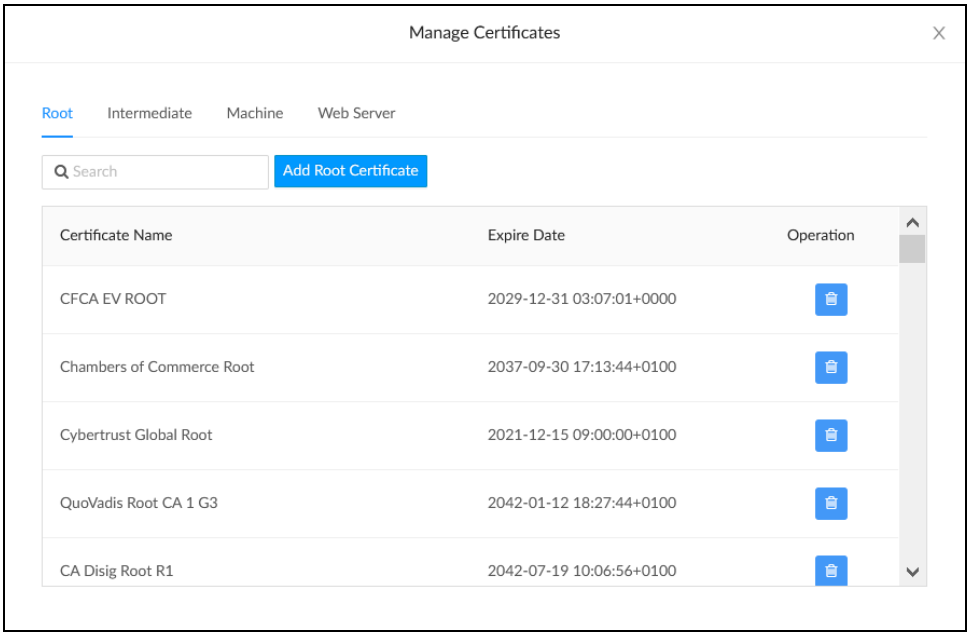


Enable **IEEE 802.1x Configuration** and select the desired method of authentication.

Certificate Authentication

1. In the **Authentication Method** field, select **EAP-TLS Certificate**.
2. If authentication server validation is not used, set **Enabled Authentication Server Validation** to disabled and continue to step 3. Otherwise, set **Enabled Authentication Server Validation** to enabled.
3. Set **OCSP mode** to enabled if the Certification Revocation List (CRL) is not required to determine the current status of a digital certificate. Set **OCSP mode** to disabled if CRL is required.
4. Select the trusted certificate authorities.
    a. To select the authority from the list, click the check box beside the desired authority.
    b. To search for a specific authority, start typing the name of the authority in the search box and check the box beside the desired authority.

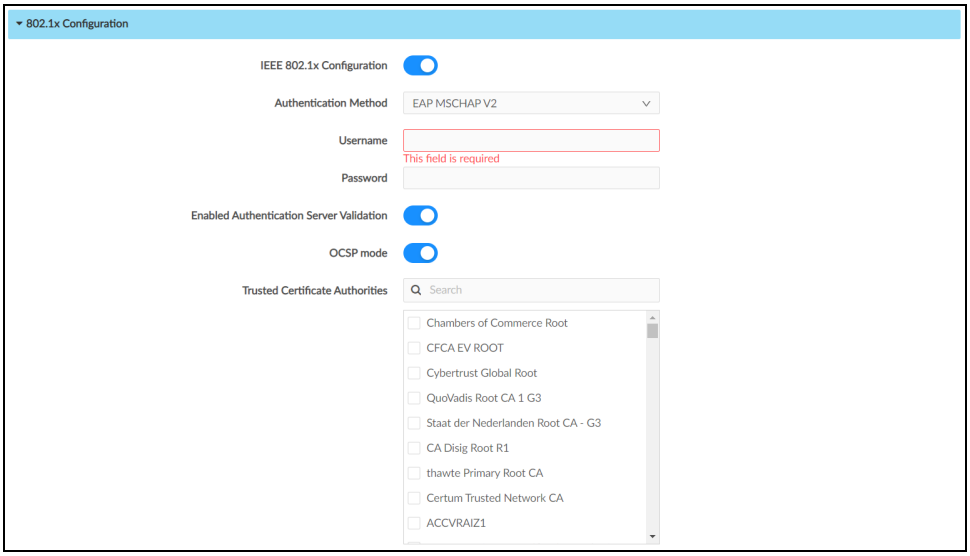
5. To load a custom certificate, click **Manage Certificates** and follow this procedure:
    a. Select the **Root** tab to manage certificates for 802.1x authentication.



    b. Click **Add Root Certificate**.
    The Add Certificate dialog box is displayed.
    c. Select the certificate file and click **Open** to add it to the list of certificates.
    d. Click to delete a certificate from the list of certificates.
6. Click **Save Changes** to save the desired changes or click **Revert** to return to the previous setting.

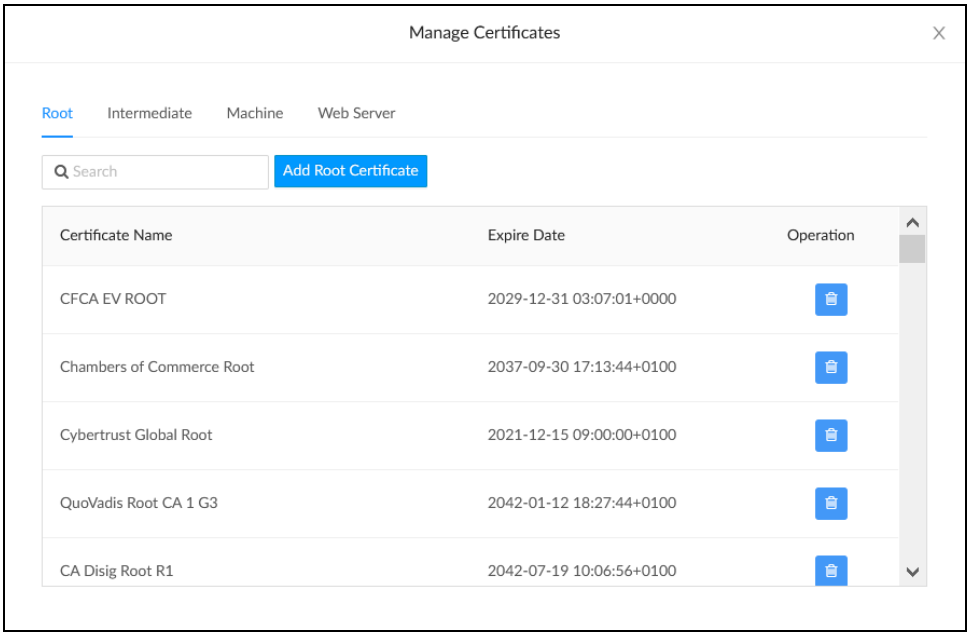
Password Authentication

1. In the **Authentication Method** field, select **EAP-MSCHAP V2-password**.
2. Enter the username and password.



3. If authentication server validation is not used, set **Enabled Authentication Server Validation** to disabled and continue to step 3. Otherwise, set **Enabled Authentication Server Validation** to enabled.
4. Set **OCSP mode** to enabled if the Certification Revocation List (CRL) is not required to determine the current status of a digital certificate. Set **OCSP mode** to disabled if CRL is required.
5. Select the trusted certificate authorities.
    a. To select the authority from the list, click the check box beside the desired authority.
    b. To search for a specific authority, start typing the name of the authority in the search box and check the box beside the desired authority.

6. To load a custom certificate, click **Manage Certificates** in the **Action** drop-down menu and follow this procedure:
    a. Click the **Root** tab to manage certificates for 802.1x authentication.



    b. Click **Add Root Certificate**.
    The Add Certificate dialog box is displayed.
    c. Select the certificate file and click **Open** to add it to the list of certificates.
    d. Click to delete a certificate from the list of certificates.
7. Click **Save Changes** to save the changes, or **Revert** to return to the previous setting.s

Log Out from the Web Interface

To log out from the web configuration and return to the welcome screen, click > **Logout**.

Microsoft Teams Display Upgrade

The Microsoft Teams desk phones eligible for the Microsoft Teams® display upgrade are:

- UC-P8-T-C-HS
- UC-P8-T-C-HS-I
- UC-P10-T-C-HS
- UC-P10-T-C-HS-I

NOTES:

- The desk phone cannot be reverted to a Microsoft Teams phone once upgraded to Microsoft Teams display.
- Remote Control via XIO Cloud is not supported by Microsoft Teams display software.
- The handset is not supported by Microsoft Teams display software. Therefore, remove the handset after upgrading the desk phone to Microsoft Teams display.
- The capacitive Microsoft Teams button is not supported by Microsoft Teams display software.

To upgrade the Microsoft Teams desk phone to Microsoft Teams display:

Prerequisites:

Ensure the desk phone is running the latest Teams firmware before upgrading it to the latest Teams display firmware.

NOTES: If the desk phone is not running the latest Teams firmware:

1. Download the latest firmware from the Resource Library.
2. Upload the firmware to the desk phone. For details, refer to Upload Firmware on page 8.

To perform the Microsoft Teams Display upgrade:

1. Download the latest Microsoft Teams display firmware from the Resource Library.
2. Upgrade the Microsoft Teams phone to the latest Microsoft Teams display firmware. For details, refer to Upload Firmware on page 8.
3. Once the Microsoft Teams display firmware is upgraded, restore the device. For details, refer to Restore on page 8.

Crestron XiO Cloud Service

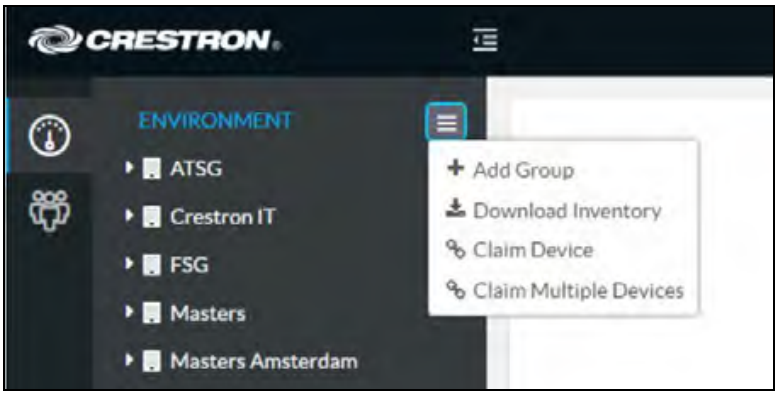
The XiO Cloud service allows all supported Crestron devices across an enterprise to be managed and configured from one central, secure location in the cloud. The XiO Cloud service may be used to view the status of a device, to configure various device and network settings, to manage licenses, and to update device firmware.

Devices must be claimed by the XiO Cloud service before they may be managed by the service. Devices may be claimed individually or as a group.

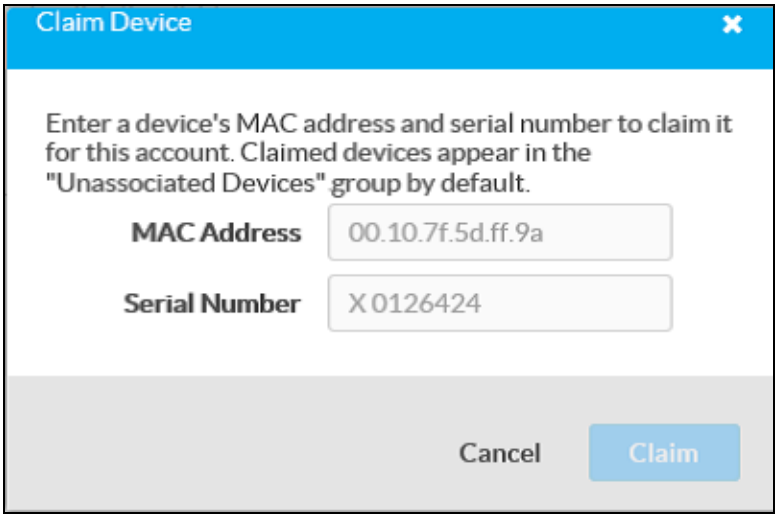
For information on creating environments, managing devices, and managing users with the XiO Cloud service, refer to the XiO Cloud User Guide XiO Cloud User Guide (Doc. 8214).

Claim a Single Device

1. Record the MAC address and serial number that are labeled on the shipping box or on the sticker attached to the device. The MAC address and serial number are required to add the device to the Crestron XiO Cloud environment.
2. Open a web browser, and log in to the Crestron XiO Cloud service at https://portal.crestron.io.
3. Click the **ENVIRONMENT** menu button ( ) to display the Environment menu.



4. Select **Claim Device** from the drop-down menu. The Claim Device dialog box is displayed.



5. Enter the MAC address and serial number recorded in step 1 in the **MAC Address** and **Serial Number fields**, respectively.
6. Click **Claim**. A message indicating a successful claiming displays.

> **NOTE:** If an error message displays stating the device does not exist, connect the device to a network that has access to the Internet, wait 15 minutes, and try again after 15 minutes.

7. Click **X** to close the dialog box. The host name of the claimed device appears in the device tree under the group Unassociated Devices.

The device can now be managed or assigned to a group. For more information on creating environments, managing devices, and managing users with the Crestron XiO Cloud service, refer to the Crestron XiO Cloud Service User Guide Guide at www.crestron.com/manuals.

Claim Multiple Devices

1. Record all of the MAC addresses and respective serial numbers in a comma delimited, CSV file, and then save it to a location that is accessible to the computer used to access the Crestron XiO Cloud service. The CSV file should be formatted as shown below:

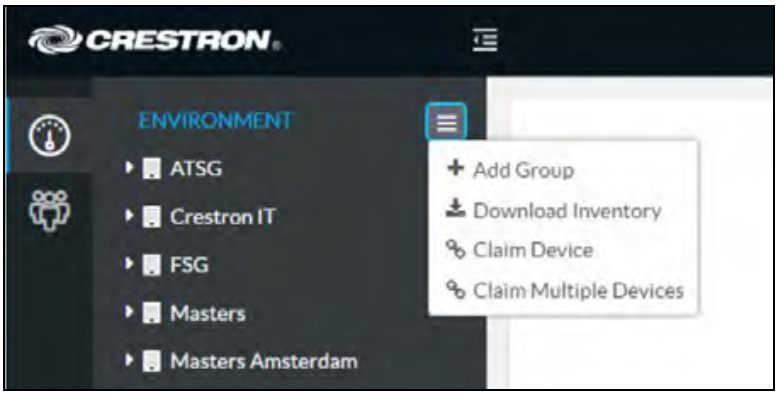
   CSV File Format

   ```
   MAC Address,Serial Number
   C0.74.ad.11.22.33,20YC074ad112233
   C0.74.ad.11.22.34,20YC074ad112234
   C0.74.ad.11.22.35,20YC074ad112235
   C0.74.ad.11.22.36,20YC074ad112236
   C0.74.ad.11.22.37,20YC074ad112237
   ```

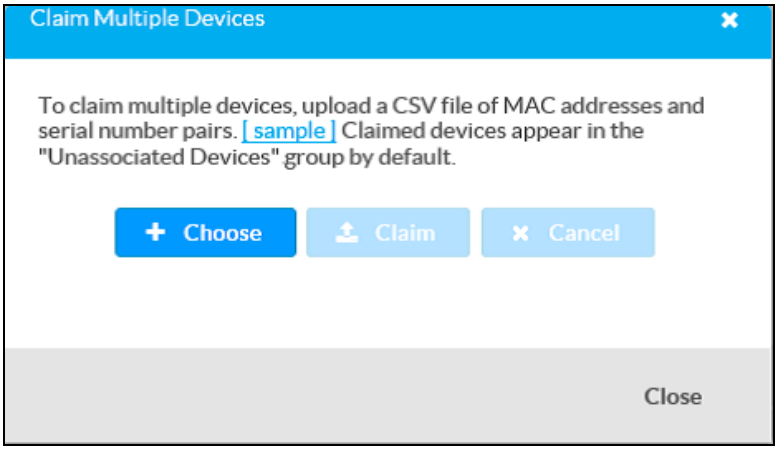
   NOTES:

   - MAC addresses and serial numbers are labeled on the shipping box or on a sticker attached to the device.
   - Use the MAC address labelled as MAC Address.

2. Open a web browser, and log in to the Crestron XiO Cloud service at https://portal.crestron.io.
3. Click the **ENVIRONMENT** menu button ( ) to display the Environment menu.



4. Select **Claim Multiple Devices** from the drop-down menu. The Claim Multiple Devices dialog box is displayed.



5. Click **Choose** and select the CSV file created in step 1.
6. Click **Claim** to claim all of the devices listed in the file. A message indicating the claim status of each device is displayed.

   > **NOTE:** If an error message displays stating the device does not exist, connect the device to a network that has access to the internet, wait 15 minutes, and then try again.

7. Click **X Cancel** to close the dialog box. The host names of the claimed devices appear in the device tree under the group Unassociated Devices.

The devices can now be managed or assigned to a group. For information on creating environments, managing devices, and managing users with the Crestron XiO Cloud service, refer to the Crestron XiO Cloud Service User Guide (Doc. 8214).

Convert Phone to Display

The following Microsoft Teams phones are eligible for Microsoft Teams displays conversion.

- UC-P8-T-C-HS
- UC-P8-T-C-HS-I
- UC-P10-T-C-HS
- UC-P10-T-C-HS-I

> **NOTES:**
>
> - The desk phone needs to be claimed in the XiO cloud service before conversion.
> - The conversion option is not available at the group level in the XiO cloud service.
> - Remote Control via XIO Cloud is not supported by Microsoft Teams display software.

- The desk phone cannot be reverted to a Microsoft Teams phone once upgraded to Microsoft Teams display.
- The handset is not supported by Microsoft Teams display software. Therefore, remove the handset after upgrading the desk phone to Microsoft Teams display.
- The capacitive Microsoft Teams button is not supported by Microsoft Teams display software.

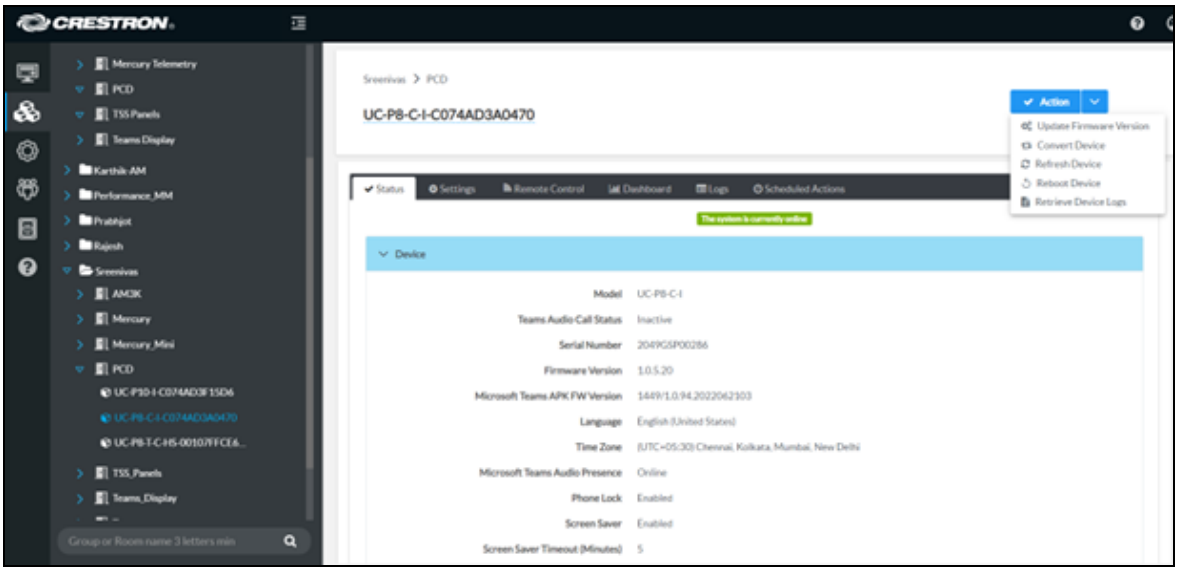
Prerequisites:

Ensure the desk phone is running the latest Teams firmware before upgrading it to the latest Teams display firmware.

NOTES: If the desk phone is not running the latest Teams firmware:

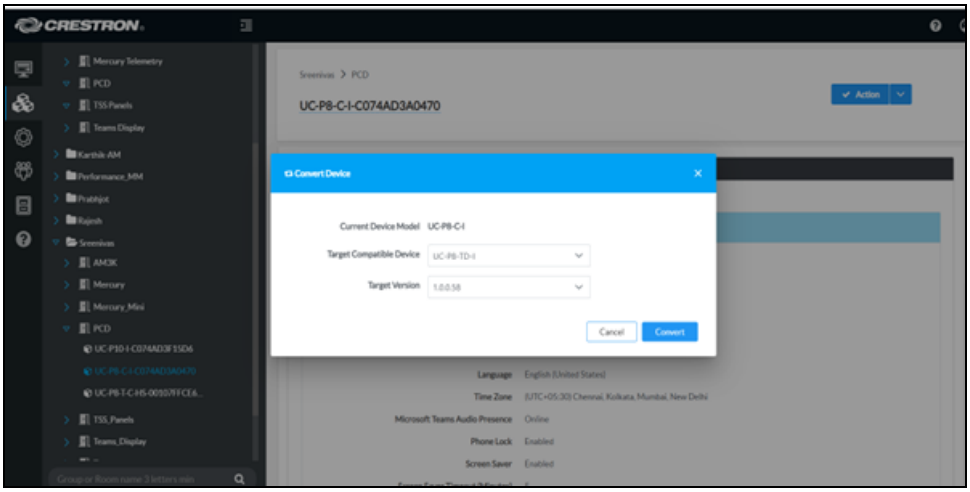
1. Download the latest firmware from the Resource Library.
2. Upload the firmware to the desk phone. For details, refer to Upload Firmware on page 8.

1. Navigate to the **Action** menu at the device level on XiO cloud service, and then select **Convert Device**.



The **Convert Device** pop-up window appears.

2. Click **Convert** to initiate the phone conversion process. Click **Cancel** to return to the previous window.



3. Click **Convert Device** on the **Confirm Device Conversion** pop-up window. The device will convert to the Microsoft Teams display. Otherwise, click **Cancel** to return to the previous window.
4. Once the Microsoft Teams display firmware is upgraded, restore the device. For details, refer to Restore on page 8.

This page is intentionally left blank.

Crestron Electronics, Inc.
15 Volvo Drive, Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7656
www.crestron.com

Product Manual — Doc. 8997B
10/11/22
Specifications subject to
change without notice.