



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

Product Manual
Crestron Electronics, Inc.

Original Instructions

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

Regulatory Model: M202029001, M202029002

Crestron product development software is licensed to Crestron dealers and Crestron Service Providers (CSPs) under a limited nonexclusive, nontransferable Software Development Tools License Agreement. Crestron product operating system software is licensed to Crestron dealers, CSPs, and end-users under a separate End-User License Agreement. Both of these Agreements can be found on the Crestron website at www.crestron.com/legal/software_license_agreement.

The product warranty can be found at www.crestron.com/warranty.

The specific patents that cover Crestron products are listed at www.crestron.com/legal/patents.

Certain Crestron products contain open source software. For specific information, visit www.crestron.com/opensource.

Crestron, the Crestron logo, and XiO Cloud are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Bluetooth is either a trademark or registered trademark of Bluetooth SIG, Inc. in the United States and/or other countries. Active Directory and Microsoft Teams are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Wi-Fi is either a trademark or registered trademark of Wi-Fi Alliance in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.

©2021 Crestron Electronics, Inc.

Contents

Introduction	1
Audience	1
Web Interface Configuration	2
Connect to the Device	3
Action	6
Restore	7
Reboot	7
Upload Firmware	7
Manage Certificates	8
Save Changes	9
Revert	9
Download Logs	10
Status	11
Settings	12
System Setup	12
Phone Lock	13
Display	13
Time/Date	13
Network	14
Connections	16
Auto Update	16
XiO Cloud	17
Remote Syslog	17
Security	19
Access Control	19
Current Users	19
Users	20
Groups	21
802.1x Configuration	22
Certificate Authentication	22
Password Authentication	24
Log Out from the Web Interface	25
Crestron XiO Cloud Service	26
Claim a Single Device	26
Claim Multiple Devices	28

Introduction

The Crestron Flex UC-P8 and UC-P10 series desk phones are designed for use with the Microsoft Teams® communications platform. They provide superior voice calling, simple operation, hands-free conferencing, and a consistent user experience with the Microsoft Teams touch screen UI.

The information provided in this product manual is applicable for the following variants:

- [UC-P8-T](#)
- [UC-P8-T-I](#)
- [UC-P8-T-HS](#)
- [UC-P8-T-HS-I](#)
- [UC-P8-T-C](#)
- [UC-P8-T-C-I](#)
- [UC-P8-T-C-HS](#)
- [UC-P8-T-C-HS-I](#)
- [UC-P10-T](#)
- [UC-P10-T-I](#)
- [UC-P10-T-HS](#)
- [UC-P10-T-HS-I](#)
- [UC-P10-T-C](#)
- [UC-P10-T-C-I](#)
- [UC-P10-T-C-HS](#)
- [UC-P10-T-C-HS-I](#)

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, 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.

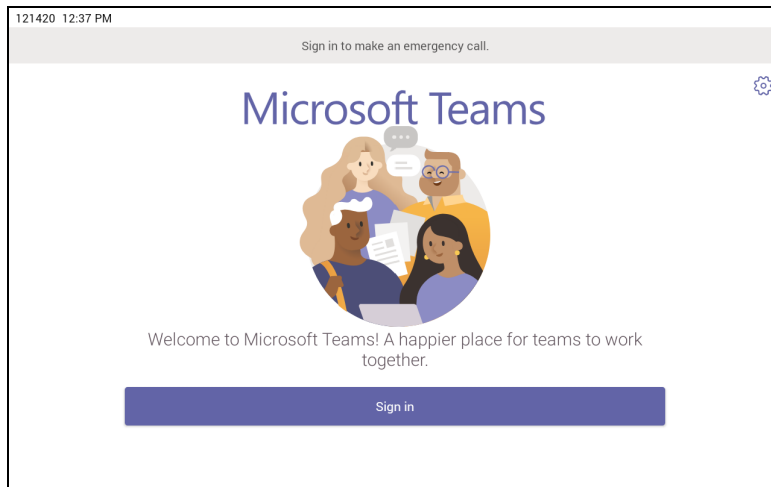
NOTE: Unless otherwise indicated in this guide, the web interface is the same for all desk phones models.

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

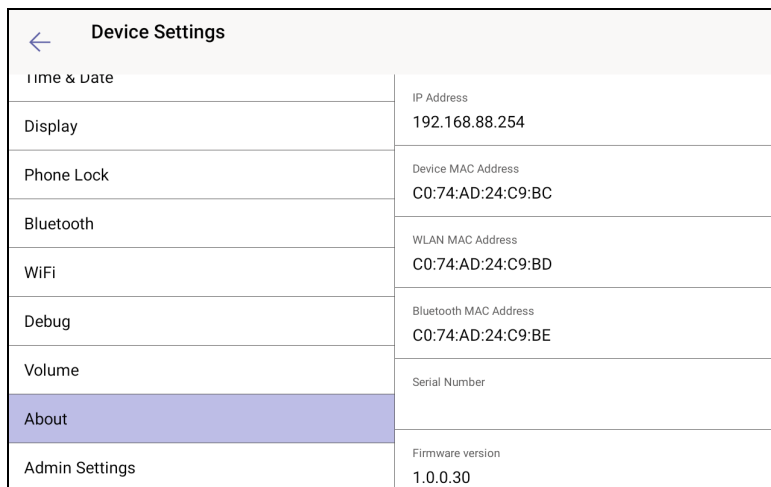
Connect to the Device

To connect to the device:

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



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

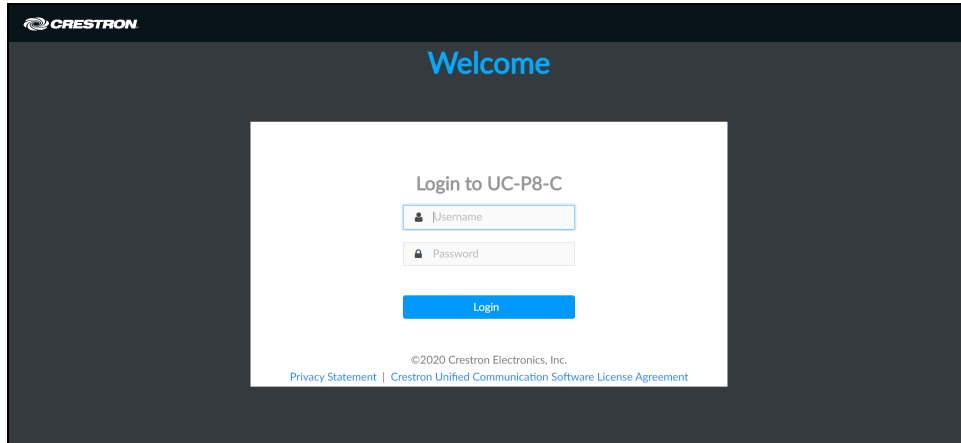


Device Settings	
Time & Date	IP Address
Display	192.168.88.254
Phone Lock	Device MAC Address
Bluetooth	C0:74:AD:24:C9:BC
WiFi	WLAN MAC Address
Debug	C0:74:AD:24:C9:BD
Volume	Bluetooth MAC Address
About	C0:74:AD:24:C9:BE
Admin Settings	Serial Number
	Firmware version
	1.0.0.30

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

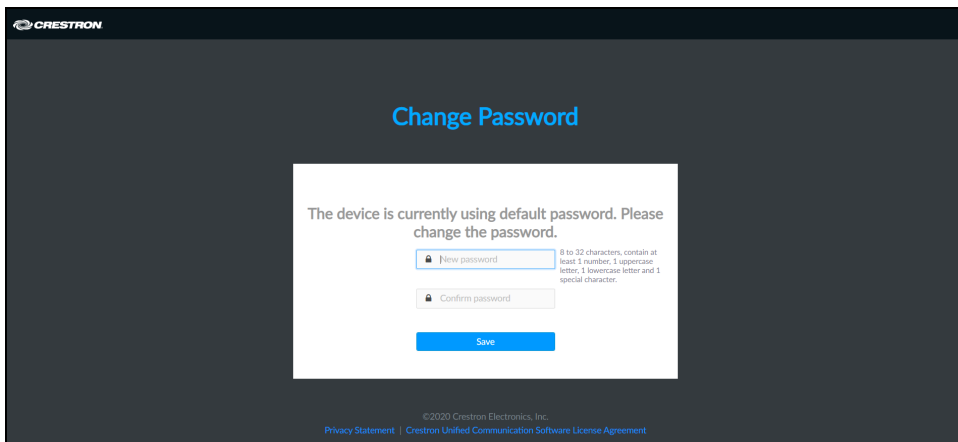
- c. Note the IP address and tap  to close the About screen.

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

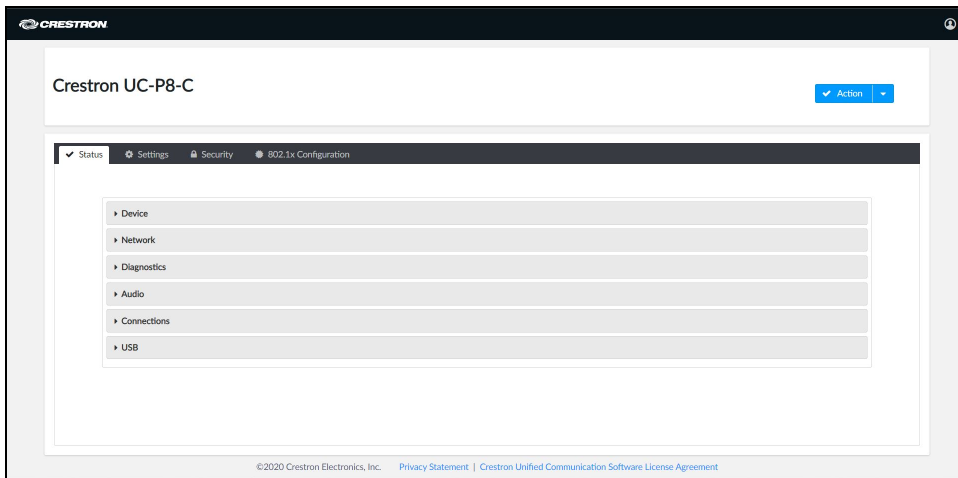


NOTE: Before prompting you to login, the web browser may display a security warning message about the security certificate. It is safe to ignore this warning as long as the user verifies that the browser's address bar indicates the correct IP address or host name of the device.

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.



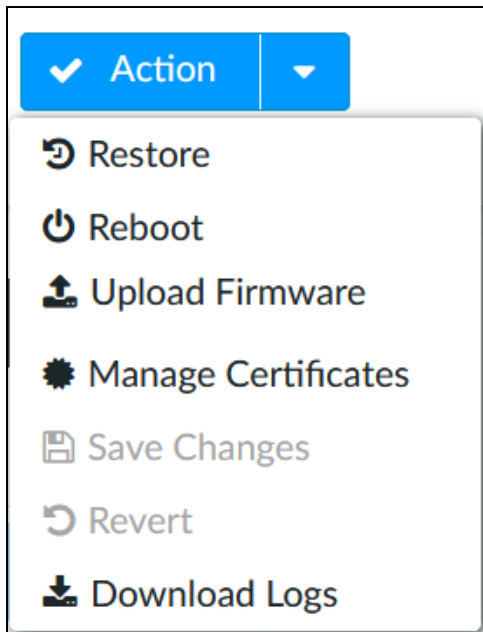
The configuration interface displays the **Action** drop-down menu and the following tabs:

- **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.

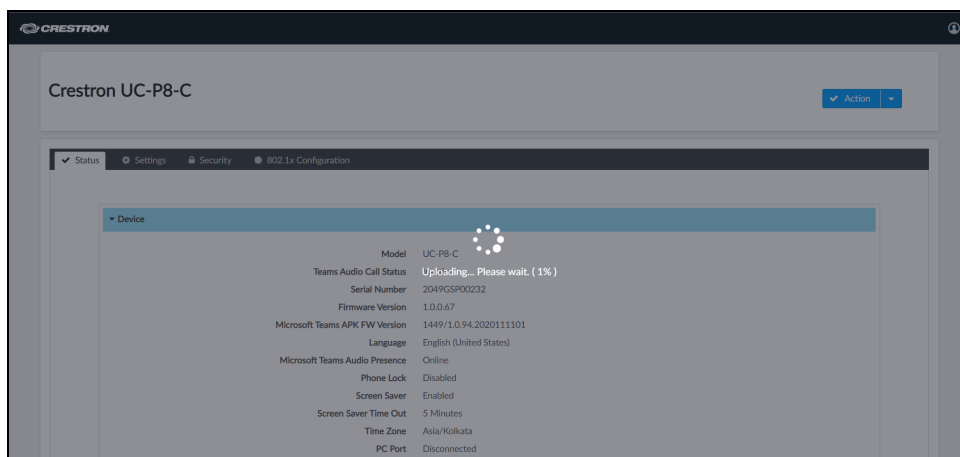
After selecting **Reboot**, a dialog box is displayed asking whether the device should be rebooted. Select **OK** to reboot the device or **Cancel** to cancel the reboot.

Upload Firmware

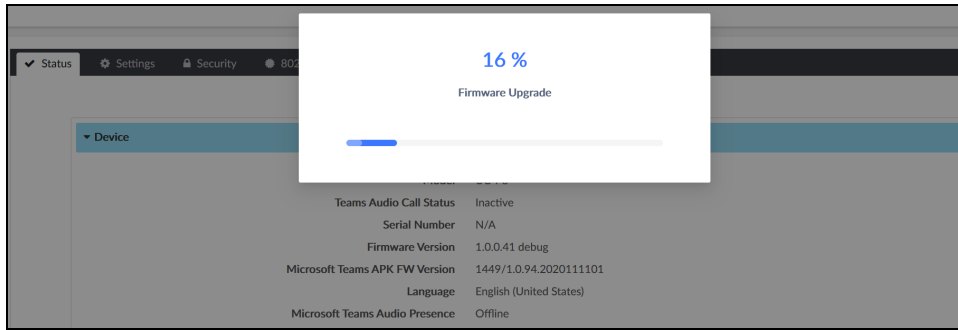
To upgrade the device firmware manually using the web configuration interface:

NOTE: For time-based auto update of the firmware or apk, refer to the [Auto Update \(on page 16\)](#) .

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.



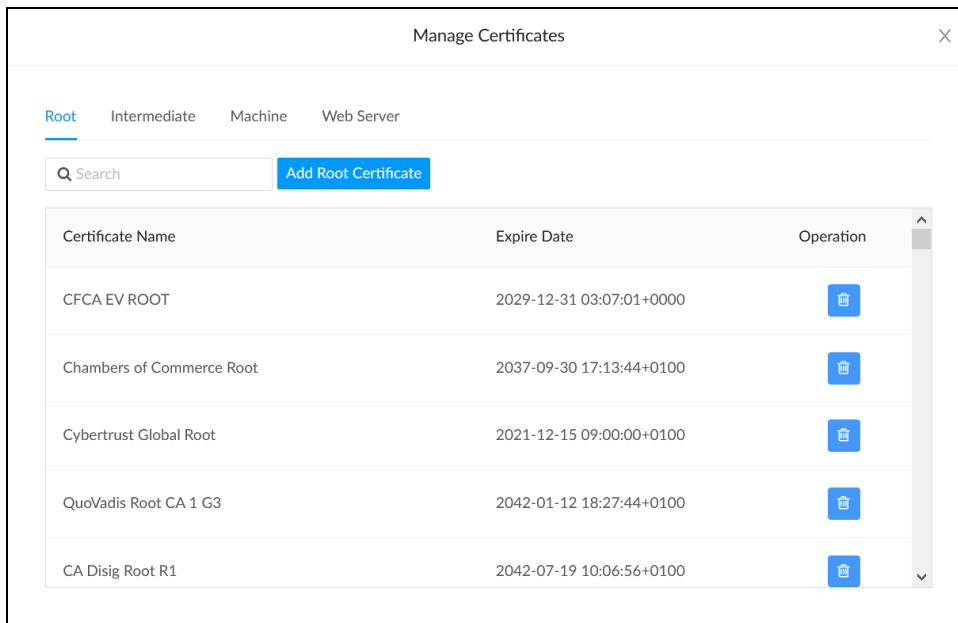
The firmware upgrade process starts once the firmware file is uploaded.



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

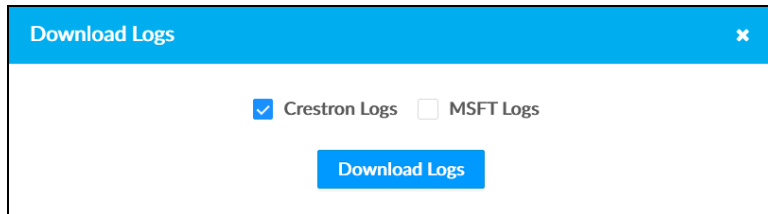
Click **Revert** to revert the device back to the last saved configuration settings.

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



Download Logs

Crestron Logs MSFT Logs

Download Logs

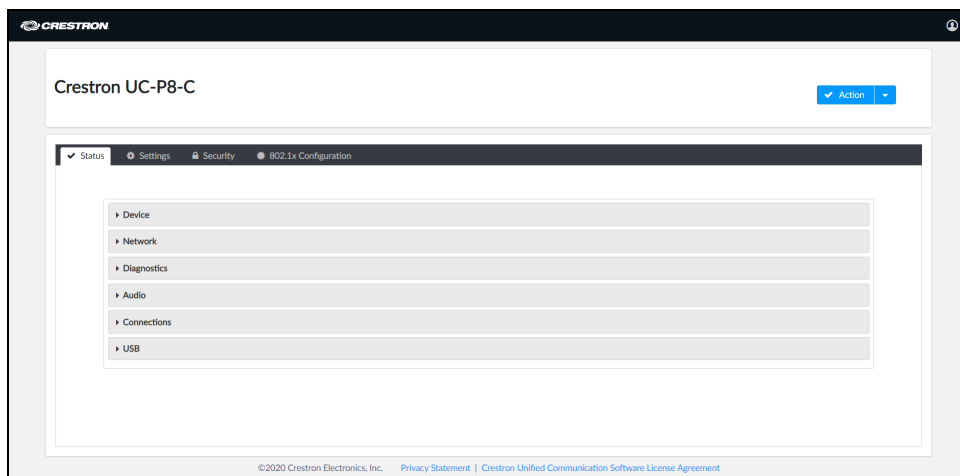
Status

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.

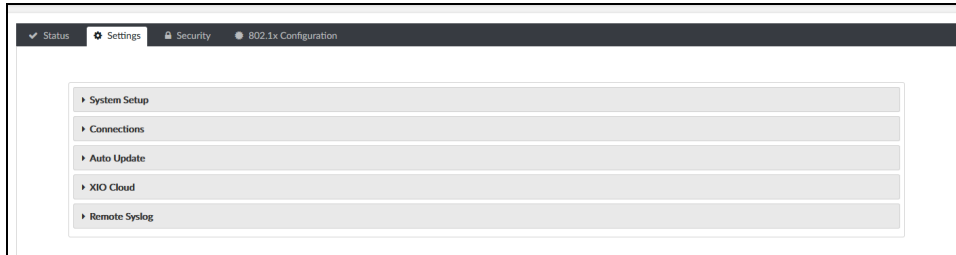
NOTE: The device must be connected to a Wi-Fi® network before running the diagnostic process.

- 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

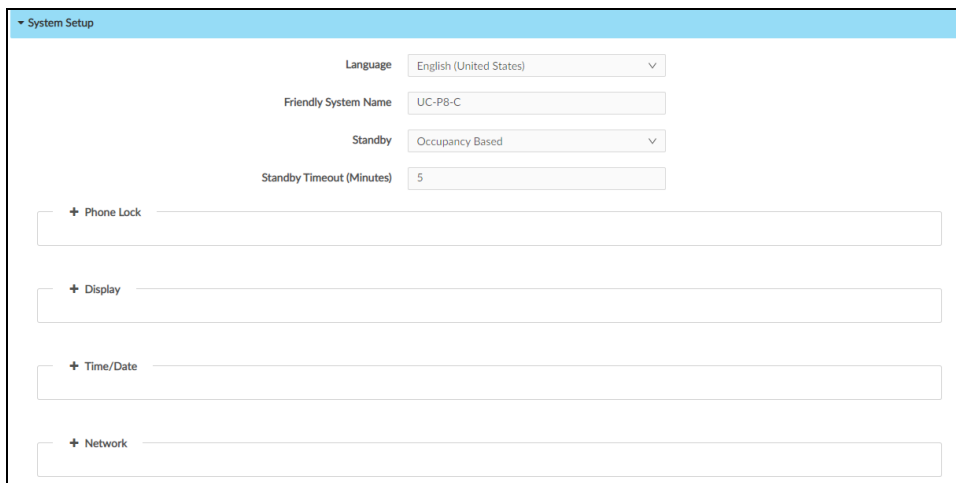
Click the **Settings** tab to display selections for configuring various device settings.



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. Default is UC-P8-C.

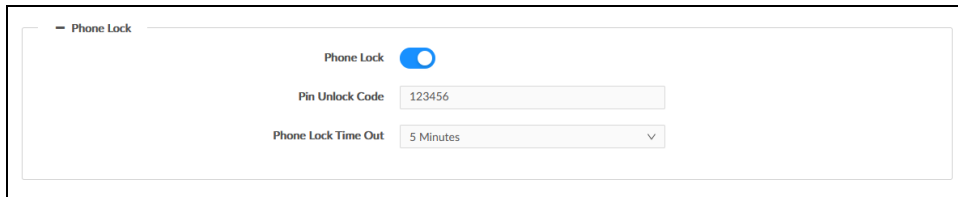
Set the **StandBy** mode to **Always On** or **Occupancy Based**.

- If **Always On** is selected, the device will not go into sleep mode.
- If **Occupancy Based** is selected, specify **Standby Timeout (Minutes)** after which the device will go into sleep mode. The default value is 5 minutes. The range is 5 to 120 minutes.

NOTE: Sleep mode will show a black screen only. No screensaver will be displayed.

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

Phone Lock



Phone Lock settings interface showing the Phone Lock toggle (turned on), Pin Unlock Code (123456), and Phone Lock Time Out (5 Minutes).

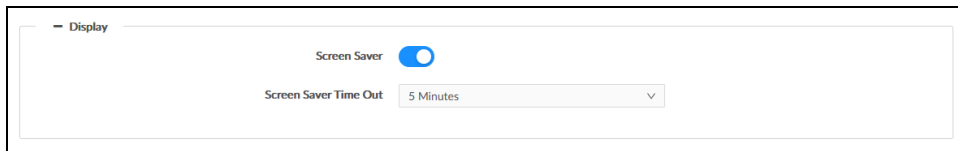
Phone Lock: Select to activate or deactivate the phone lock option.

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



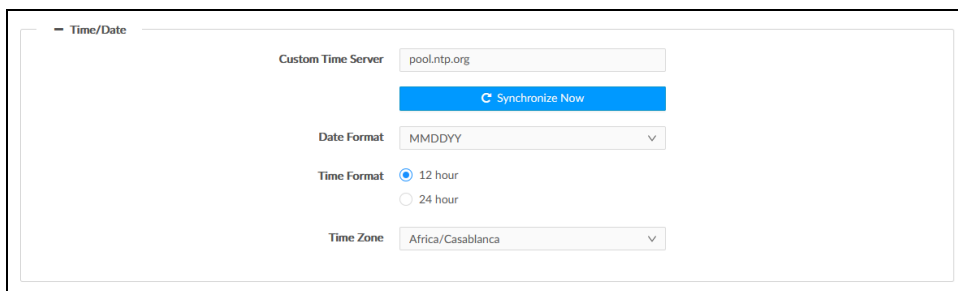
Display settings interface showing the Screen Saver toggle (turned on) and Screen Saver Time Out (5 Minutes).

Screen Saver: Select to activate or deactivate the screen saver option.

If enabled, set the corresponding parameter:

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.

Time/Date



Time/Date settings interface showing Custom Time Server (pool.ntp.org), Synchronize Now button, Date Format (MMDDYY), Time Format (12 hour selected), and Time Zone (Africa/Casablanca).

Specify **Custom Time Server** to use for time synchronization. Default is "pool.ntp.org."

Trigger the synchronization process, click **Synchronize Now**.

Select the **Date Format** to be used on the device. The available options are:

- MMDDYY (Default)
- DDMMYY
- YYYYDDMM

Set **Time Format** to 12 hour (default) or 24 hour.

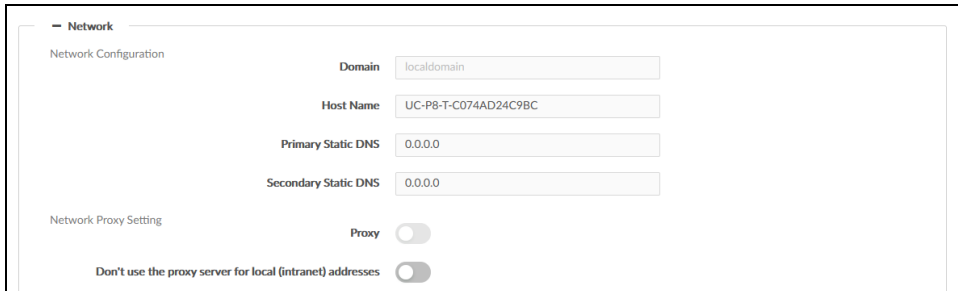
Select the local time zone from the **Time Zone** drop-down to display the correct time on the device.

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.

To configure the network settings:

1. Enter a host name in the **Host Name** field and a domain name (optional) in the **Domain** field.

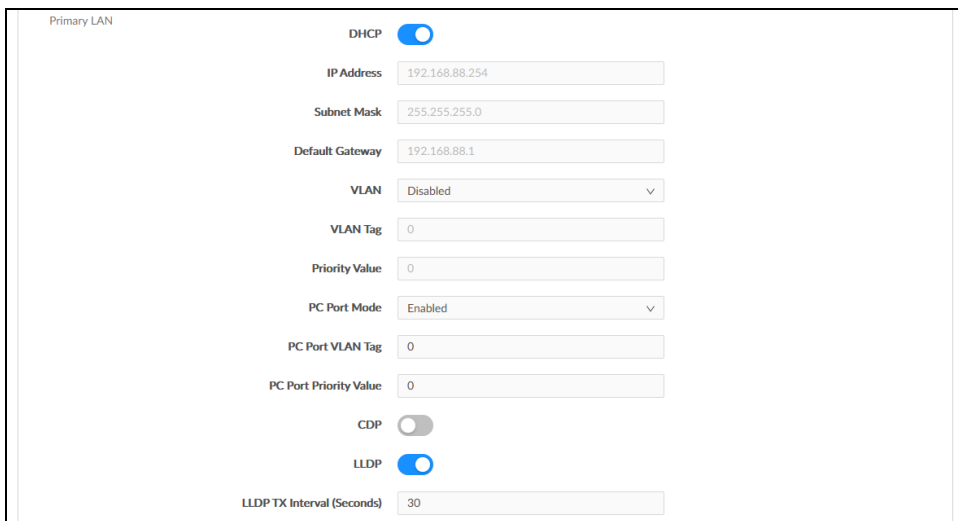


The screenshot displays the 'Network' configuration interface. It is divided into two sections: 'Network Configuration' and 'Network Proxy Setting'. Under 'Network Configuration', there are four input fields: 'Domain' (containing 'localdomain'), 'Host Name' (containing 'UC-P8-T-C074AD24C9BC'), 'Primary Static DNS' (containing '0.0.0.0'), and 'Secondary Static DNS' (containing '0.0.0.0'). Under 'Network Proxy Setting', there are two toggle switches: 'Proxy' (which is currently turned off) and 'Don't use the proxy server for local (intranet) addresses' (which is currently turned on).

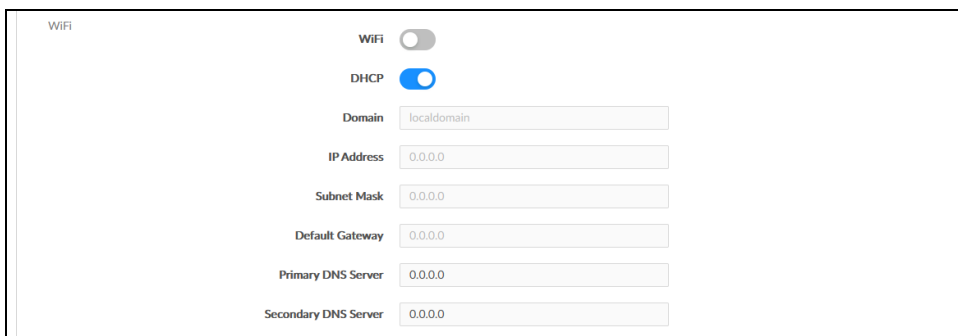
2. The device has two network adapters, **Primary LAN** and **WiFi**. Each network adapter can be set to have its IP address, subnet mask, default gateway, and DNS servers set manually, or obtain the settings from a DHCP server. Choose one of the following options for each network adapter.

- 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.



The screenshot shows the configuration page for the Primary LAN interface. The DHCP toggle is turned on. The IP Address is 192.168.88.254, Subnet Mask is 255.255.255.0, and Default Gateway is 192.168.88.1. The VLAN is set to Disabled, and the VLAN Tag is 0. The Priority Value is 0. The PC Port Mode is set to Enabled, and the PC Port VLAN Tag is 0. The PC Port Priority Value is 0. The CDP toggle is turned off, and the LLDP toggle is turned on. The LLDP TX Interval (Seconds) is set to 30.

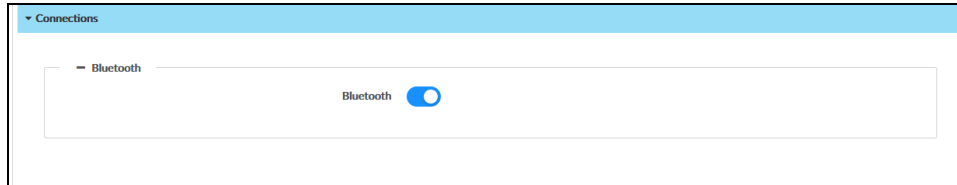


The screenshot shows the configuration page for the WiFi interface. The WiFi toggle is turned off, and the DHCP toggle is turned on. The Domain is localdomain. The IP Address, Subnet Mask, Default Gateway, Primary DNS Server, and Secondary DNS Server are all set to 0.0.0.0.

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

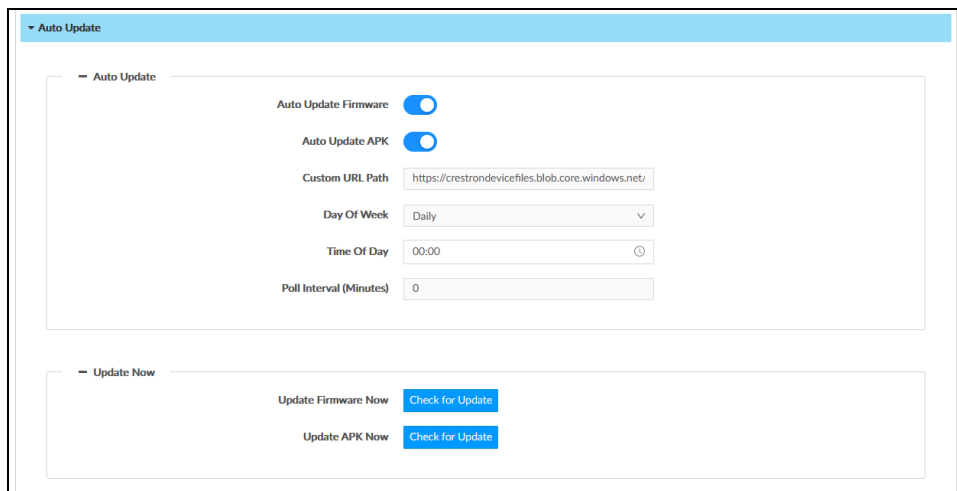
Connections

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.



To configure **Auto Update**:

1. Enable **Auto Update Firmware**.
2. Enable **Auto Update APK**.
3. Set **Custom 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. 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 the **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.

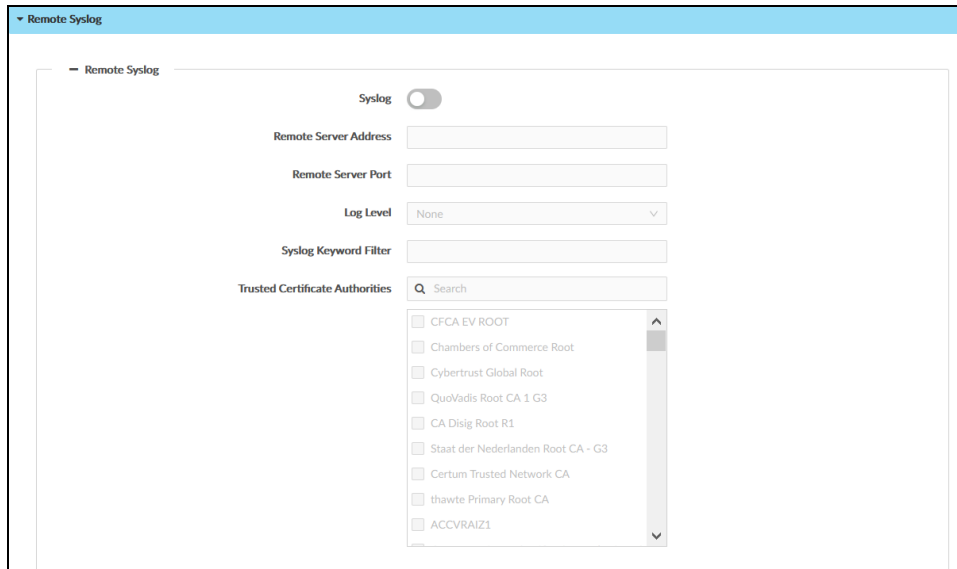
XiO Cloud

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:

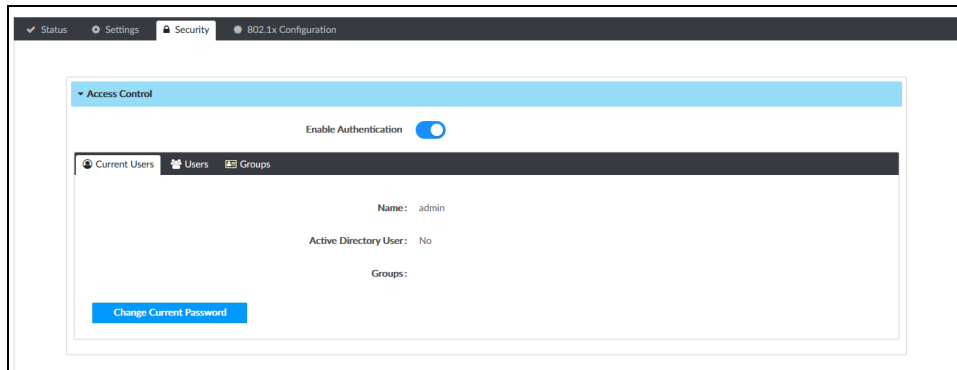
1. Switch **Syslog** to Enabled.
2. Enter the IP address or Fully Qualified Domain Name (FQDN) in the **Remote Server Address**.
3. Enter the port number in the **Remote Server Port**. The range is 0 to 65535.
4. Select **Log Level** for Syslog. The default setting is **None**. There are four levels 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.



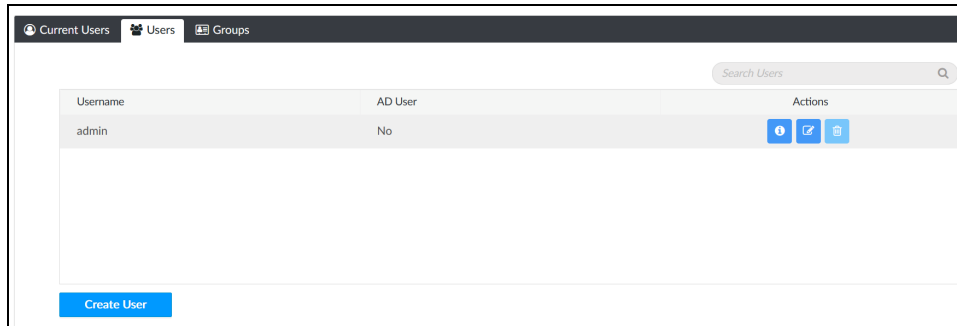
Current Users




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

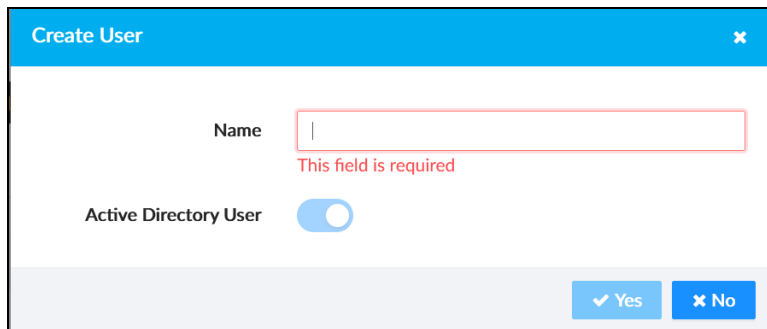
Select the **Users** tab to manage authorized users. A list of authorized users is displayed.



- 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.

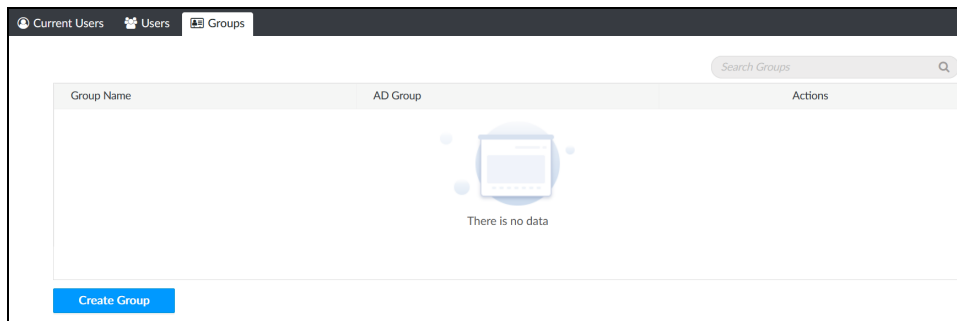
- Click **Create User** to add a user. The Create User dialog box is displayed.



A screenshot of the 'Create User' dialog box. The dialog has a blue header with the title 'Create User' and a close button. Below the header, there is a 'Name' label followed by an empty text input field. Below the input field, the text 'This field is required' is displayed in red. Below the name field, there is an 'Active Directory User' label followed by a toggle switch that is currently turned on. At the bottom right of the dialog, there are two buttons: 'Yes' and 'No'.

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.

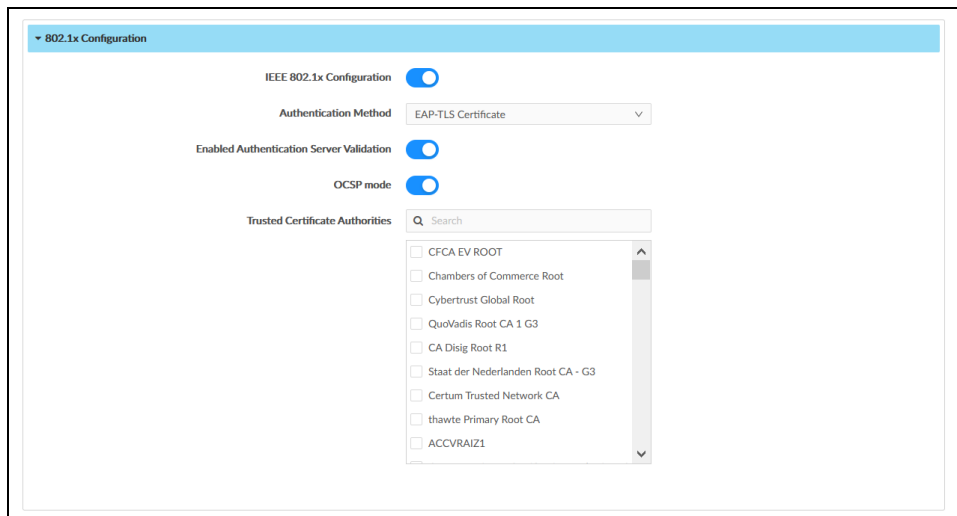
A dialog box titled 'Create Group' with a close button (x) in the top right corner. It contains a 'Name' field with a red border and a red error message 'This field is required' below it. Below the name field is a toggle switch for 'Active Directory Group', which is currently turned on. At the bottom right, there are two buttons: 'Yes' with a checkmark icon and 'No' with an 'x' icon.

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.

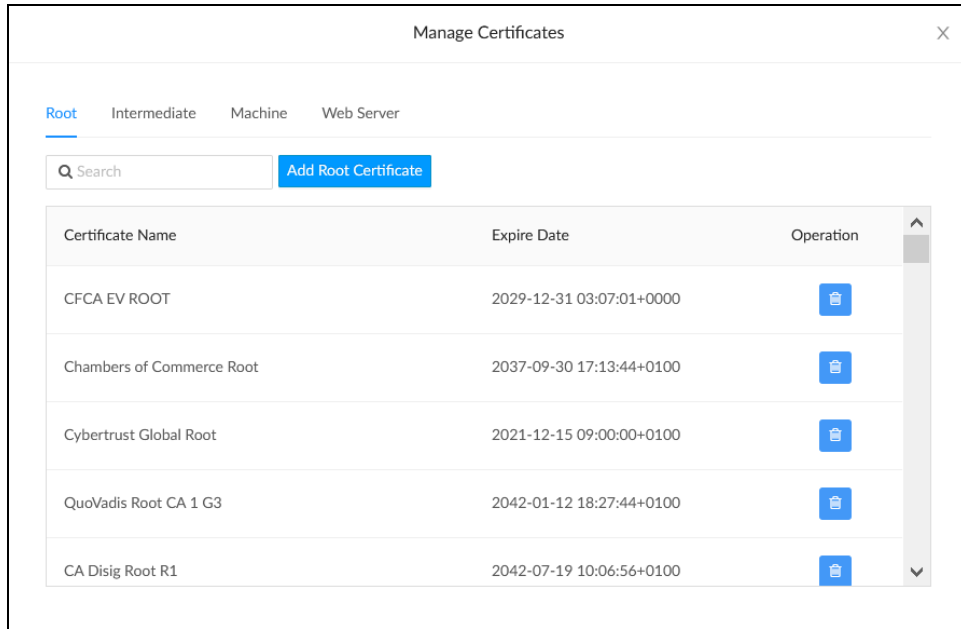


Enable **IEEE 802.1x Configuration** and select the desired method of authentication.

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.

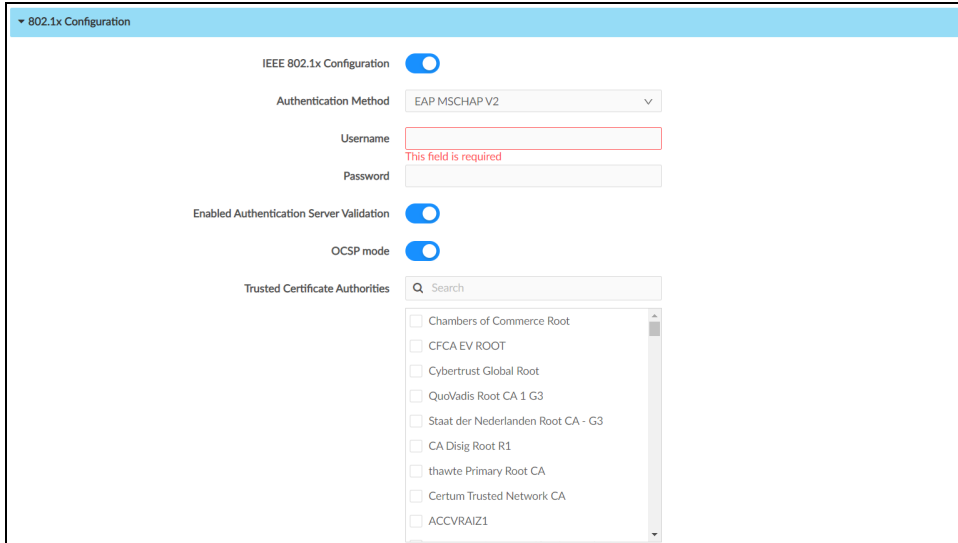
5. To load a custom certificate, click **Manage Certificates** and follow this procedure:
 - a. Select the **Root** tab to manage certificates for 802.1x authentication.



- 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

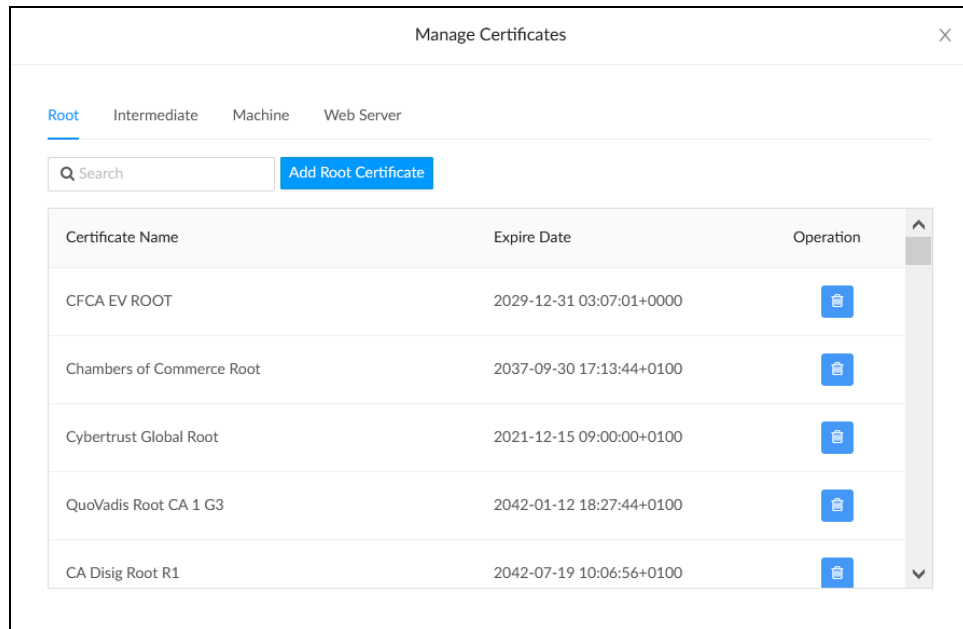
1. In the **Authentication Method** field, select **EAP-MSCHAP V2-password**.
2. Enter the username and password.




The screenshot displays the '802.1x Configuration' interface. At the top, there is a blue header with a dropdown arrow and the text '802.1x Configuration'. Below this, the 'IEEE 802.1x Configuration' section has a toggle switch that is turned on. The 'Authentication Method' is set to 'EAP-MSCHAP V2' in a dropdown menu. The 'Username' and 'Password' fields are empty, with a red error message 'This field is required' appearing below the Username field. The 'Enabled Authentication Server Validation' toggle is also turned on. The 'OCSP mode' toggle is turned on. The 'Trusted Certificate Authorities' section features a search box with a magnifying glass icon and a list of authorities, each with an unchecked checkbox. The list includes: Chambers of Commerce Root, CFCA EV ROOT, Cybertrust Global Root, QuoVadis Root CA 1 G3, Staat der Nederlanden Root CA - G3, CA Disig Root R1, thawte Primary Root CA, Certum Trusted Network CA, and ACCVRAIZ1.

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 settings.

Log Out from the Web Interface

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

Crestron XiO Cloud Service

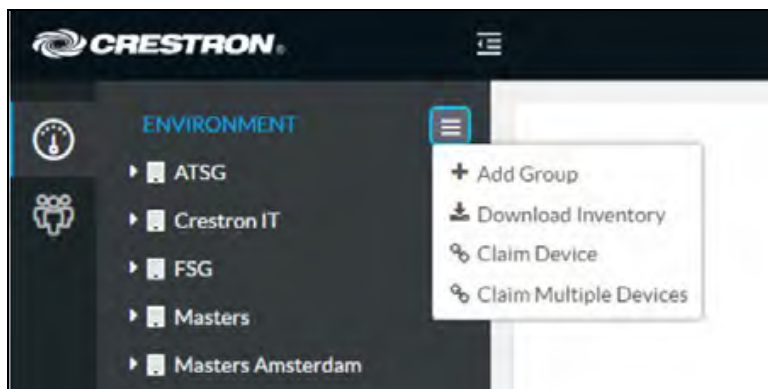
The XiO Cloud service allows all supported Crestron devices across an enterprise to be managed and configured from one central, secure location in the cloud. The XiO Cloud service may be used to view the status of a device, to configure various device and network settings, to manage licenses, and to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

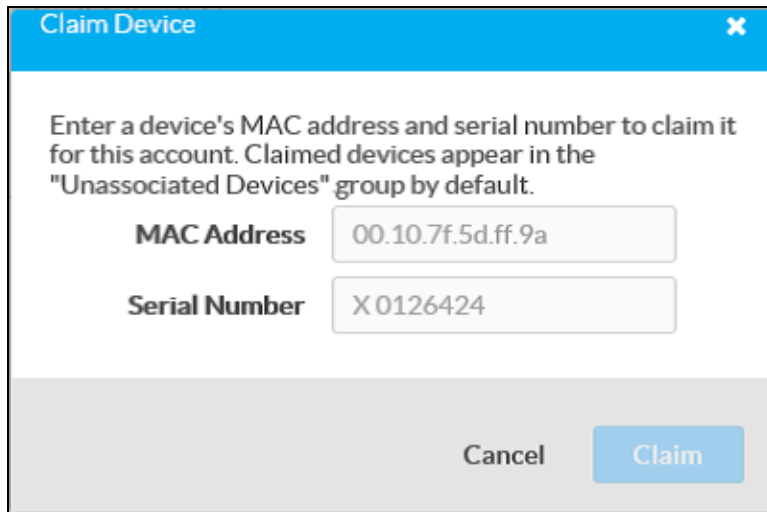
For information on creating environments, managing devices, and managing users with the XiO Cloud service, refer to the XiO Cloud User Guide [XiO Cloud User Guide \(Doc. 8214\)](#).

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.



Claim Device

Enter a device's MAC address and serial number to claim it for this account. Claimed devices appear in the "Unassociated Devices" group by default.

MAC Address 00.10.7f.5d.ff.9a

Serial Number X 0126424

Cancel Claim

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

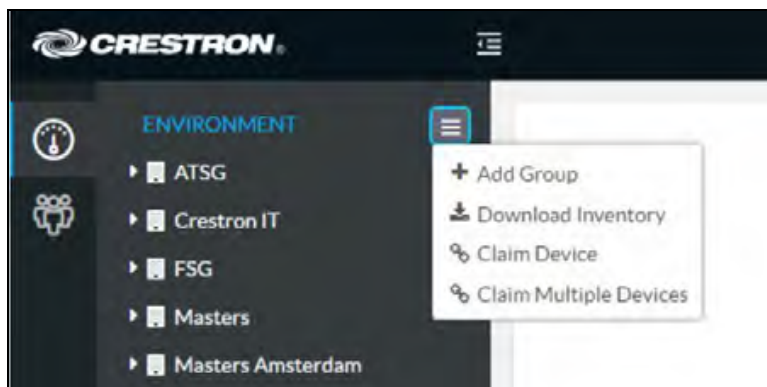
C0.74.ad.11.22.35,20YC074ad112235

C0.74.ad.11.22.36,20YC074ad112236

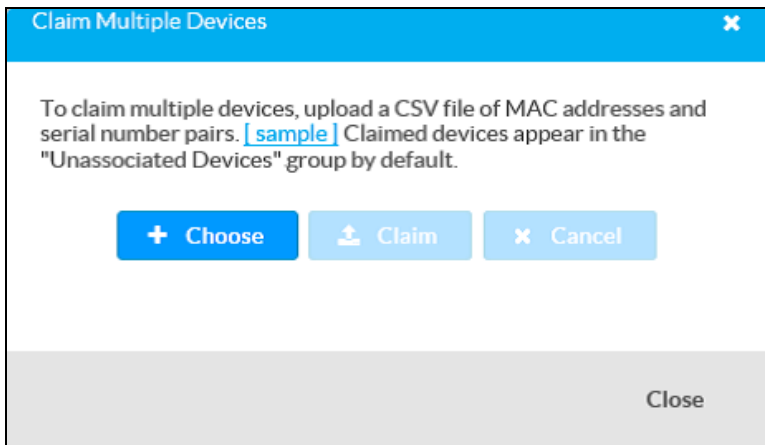
C0.74.ad.11.22.37,20YC074ad112237

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).

This page is intentionally left blank.

