Crestron Flex Phones

Security Reference Guide

Crestron Electronics, Inc.

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

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 online at www.crestron.com/legal/patents.

Certain Crestron products contain open source software. For specific information, please 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.

Revision History

Rev	Date	Notes	Author(s)
A	July 29, 2022	Initial version	IH

Please send comments and change recommendations to:

SecurityDocs@crestron.com

Contents

Overview

This document describes the steps needed to harden a Crestron® installation with Crestron Flex Phones and assumes a basic understanding of security functions and protocols. This guide provides information about the system configuration used for Crestron Flex Phones firmware release 1.0.4.22 or later.

> **NOTE:** The term "device" is used in this document to refer to all applicable Crestron Flex Phone models unless specified otherwise.

The information in this guide pertains to the following device models:

Model	Description
UC-P8-T	Crestron Flex 8 in. Audio Desk Phone for Microsoft Teams® Software
UC-P8-T-I	Crestron Flex 8 in. Audio Desk Phone for Microsoft Teams® Software, International
UC-P8-T-HS	Crestron Flex 8 in. Audio Desk Phone with Handset for Microsoft Teams® Software
UC-P8-T-HS-I	Crestron Flex 8 in. Audio Desk Phone with Handset for Microsoft Teams® Software, International
UC-P8-T-C	Crestron Flex 8 in. Video Desk Phone for Microsoft Teams® Software
UC-P8-T-C-I	Crestron Flex 8 in. Video Desk Phone for Microsoft Teams® Software, International
UC-P8-T-C-HS	Crestron Flex 8 in. Video Desk Phone with Handset for Microsoft Teams® Software
UC-P8-T-C-HS-I	Crestron Flex 8 in. Video Desk Phone with Handset for Microsoft Teams® Software, International
UC-P10-T	Crestron Flex 10 in. Audio Desk Phone for Microsoft Teams® Software
UC-P10-T-I	Crestron Flex 10 in. Audio Desk Phone for Microsoft Teams® Software, International
UC-P10-T-HS	Crestron Flex 10 in. Audio Desk Phone with Handset for Microsoft Teams® Software
UC-P10-T-HS-I	Crestron Flex 10 in. Audio Desk Phone with Handset for Microsoft Teams® Software, International
UC-P10-T-C	Crestron Flex 10 in. Video Desk Phone for Microsoft Teams® Software
UC-P10-T-C-I	Crestron Flex 10 in. Video Desk Phone for Microsoft Teams® Software, International

Model	Description
UC-P10-T-C-HS	Crestron Flex 10 in. Video Desk Phone with Handset for Microsoft Teams® Software
UC-P10-T-C-HS-I	Crestron Flex 10 in. Video Desk Phone with Handset for Microsoft Teams® Software, International

Ports and Protocols

The following ports and protocols may be used by the device depending on the system design and configuration.

Crestron Control Devices

Function	Destination Port	From (Sender)	To (Listener)	Notes
Crestron-CIP	41794/TCP	Device	Control System	Crestron Internet Protocol
Crestron-SCIP	41796/TCP	Device	Control System	Secure Crestron Internet Protocol
HTTPS	49200/TCP	Remote Device	Device	Web API for Crestron HTML5 User Interfaces

Common Ports

Function	Destination Port	From (Sender)	To (Listener)	Notes
NTP	123/UDP	Device	NTP Server	Network Time Protocol (NTP)
SSH	22/TCP	Admin Workstation	Device	Used for configuration and console.
LDAP	389/TCP	Device	Admin Server	
LDAPS	636/TCP	Device	Admin Server	
HTTPS	443/TCP	Admin or End User Workstation	Device	Secure web configuration
HTTPS	443/TCP	Device	XiO Cloud® Service	For XiO Cloud services only and not required for device functionality. A persistent connection is made via AMQP over WebSockets. HTTPS services such as routing lookups and file transfers may be used.

Function	Destination Port	From (Sender)	To (Listener)	Notes
HTTPS	443/TCP	Device	Microsoft Portal	For Microsoft portal services only and not required for device functionality. HTTPS services such as routing lookups and file transfers may be used.
HTTPS	443/TCP	Device	Firmware Server	Firmware upgrade path
HTTPS	443/TCP	Device	APK Server	APK upgrade path
DHCP	67/UDP	Device	DHCP Server	DHCP addressing
DHCP	68/UDP	DHCP Server	Device	DHCP addressing
HTTP	80/TCP	End User Workstation	Device	Web configuration
WPAD	80/TCP	Device	WPAD File Server	Gets the PAC file from the server.
Remote Syslog	Configurable	Device	Remote Syslog Server	Uses TLS
HTTP Proxy	Configurable	Device	Proxy Server	
HTTPS Proxy	Configurable	Device	Proxy Server	
Kerberos	88/TCP	Device	KDC (Key Distribution Center)	
DNS	3/TCP/UDP	Device	DNS server	

Prerequisites

In order to perform a secure configuration, the following prerequisites must be met.

Operating Environment

Crestron assumes the following about the operating environment of its systems:

- The system is not capable of Multi-Factor Authentication (MFA). If your organization's policy requires MFA, you cannot use the system.
- Physical security is commensurate with the value of the system and the data it contains and is assumed to be provided by the environment.
- Administrators are trusted to follow and provide all administrator guidance.

Firmware Version

Crestron Flex Phones must be running firmware version 1.0.4.22 or later.

Device Access

The administrator can access and configure the device by using a web browser. Additionally, some aspects of configuration can be performed via the XiO Cloud® service. This document describes device configuration using the web browser.

The device also provides local setup pages for commonly used configuration settings. The local setup pages can be accessed from the touch screen display by tapping the gear icon on the home page and then selecting **Device Settings**.

Default Configuration Settings

In order to configure the device, it must first be placed in its factory default state. A device can be returned to this state as follows:

1. Disconnect the Ethernet cable from the LAN port that supplies the device power over PoE (Power over Ethernet).
2. Reconnect the Ethernet cable to the LAN port. The device starts to boot.
3. When the LED light bar below the touch screen display starts to flash green, press and hold the **Volume Up** and **Microphone Mute** buttons simultaneously for at least 10 seconds. A page is displayed asking whether a factory restore should be performed.

4. Use the **Volume Up** or **Volume Down** buttons to select **Yes**, and then press the **Microphone Mute** button to confirm the selection.
5. Wait 5 to 10 minutes for the self-recovery process to complete.
6. Proceed with the network configuration.

Microsoft Teams Secure Deployment

The device runs the Microsoft Teams® software app. For more information on how to securely deploy Microsoft Teams across an enterprise, refer to docs.microsoft.com/en-us/MicrosoftTeams/security-compliance-overview.

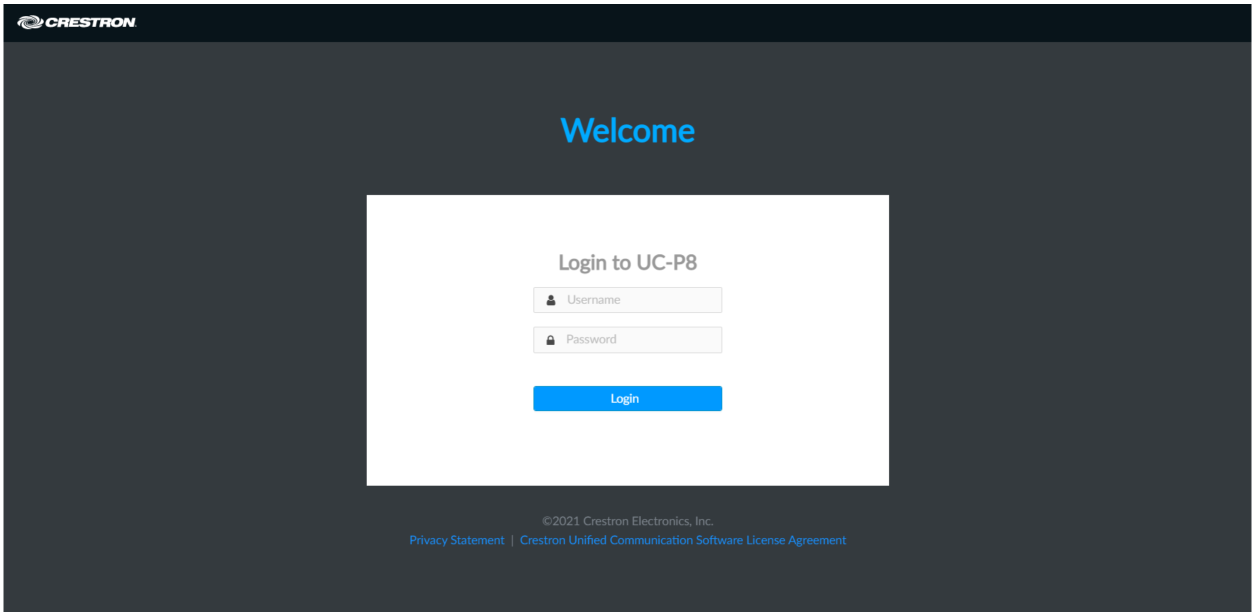
Required Configuration

The following sections describe the configuration changes required for the device for a secure deployment.

Create an Admin Account Password

The first time the web configuration interface is accessed, a **Welcome** page is displayed prompting the user to log in with admin credentials.

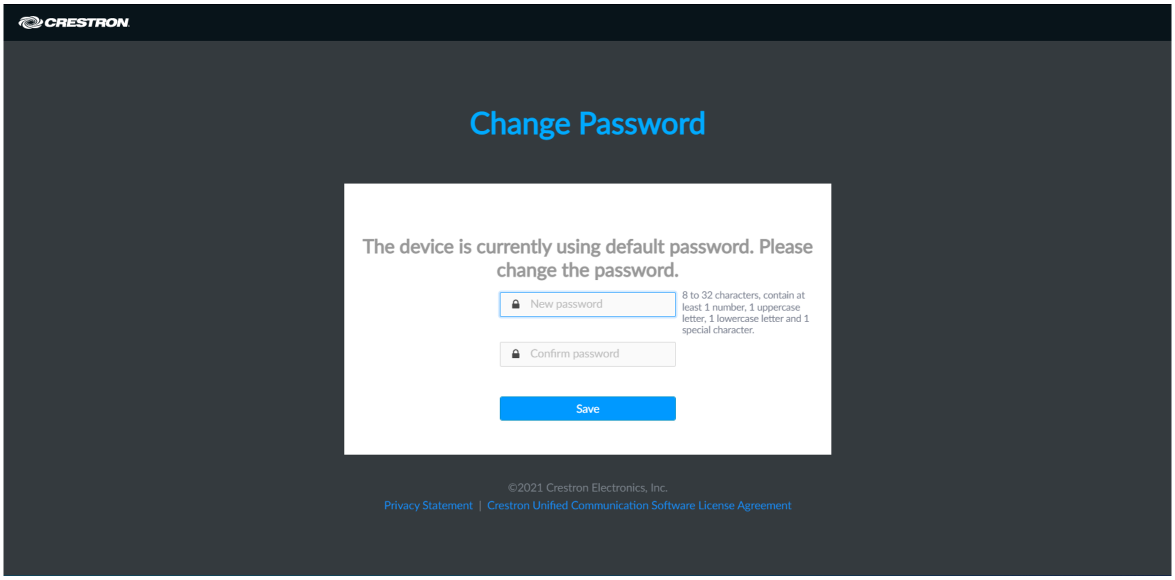
Welcome Page



CRESTRON
Welcome
Login to UC-P8
Username
Password
Login
©2021 Crestron Electronics, Inc.
Privacy Statement | Crestron Unified Communication Software License Agreement

1. Enter the default admin account username (**admin**) and password (**admin**) in the appropriate text fields.
2. Select **Login**. A **Change Password** page is displayed prompting the user to change the admin account password.

Change Password Page



Change Password

The device is currently using default password. Please change the password.

New password
Confirm password
Save

8 to 32 characters, contain at least 1 number, 1 uppercase letter, 1 lowercase letter and 1 special character.

©2021 Crestron Electronics, Inc.

Privacy Statement | Crestron Unified Communication Software License Agreement

3. Enter and confirm a new password that meets the validation rules shown (8-32 characters, contains at least 1 number, 1 uppercase letter, 1 lowercase letter, and 1 special character).
4. Select **Save** to return to the **Welcome** page.
5. Enter the admin account username and new password created in step 3.
6. Select **Login**. Upon successful login, the web configuration user interface is displayed.

Configure the Network

The following sections provide information about the tasks necessary to configure the network.

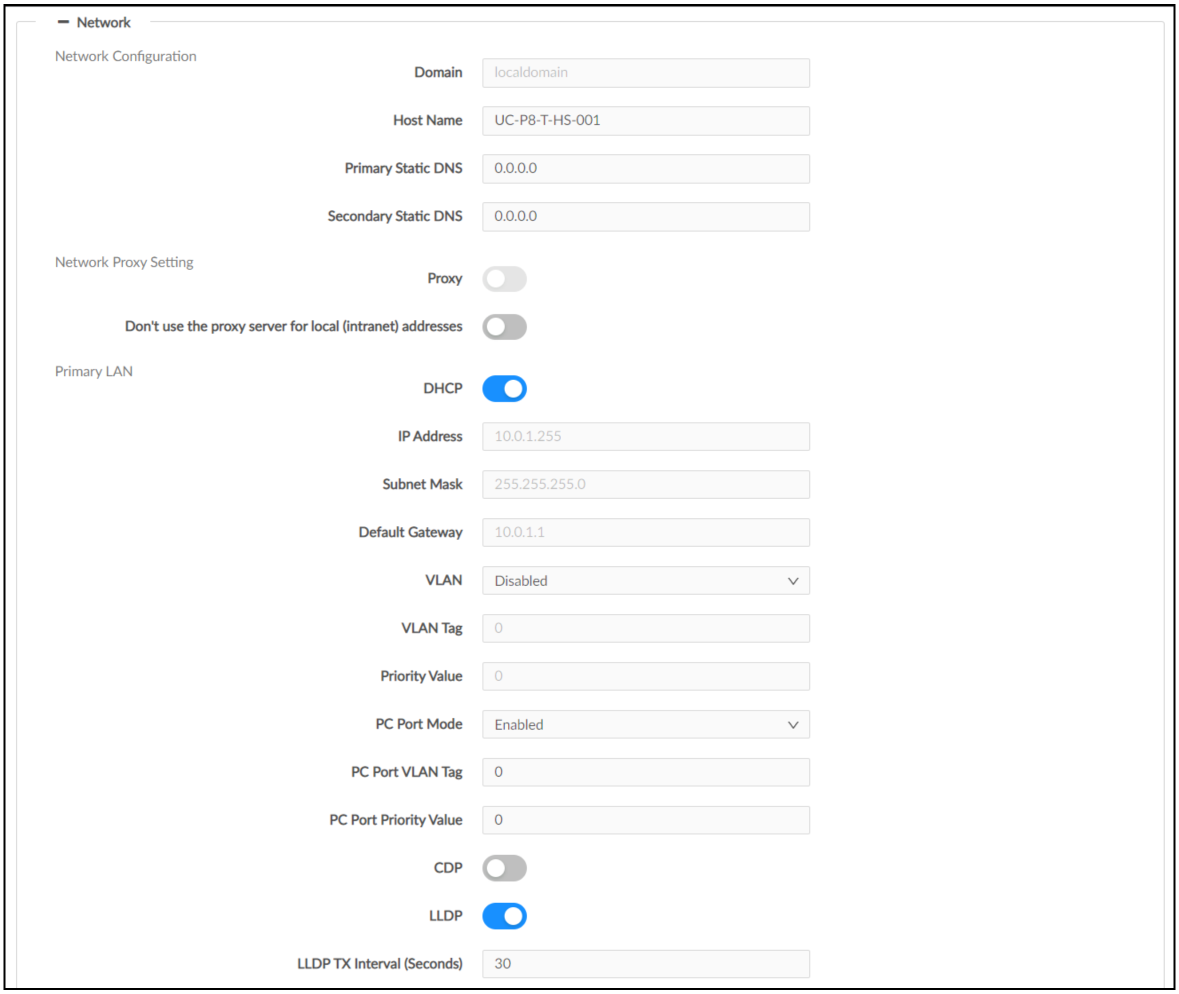
Wired Network Configuration

To configure the device to communicate on the LAN over Ethernet, the following changes must be made. If DHCP is available on the local network, then no additional configuration changes are necessary. If DHCP is not available or if the administrator wishes to manually set the network configuration, then the IP address, subnet mask, default gateway, and DNS server settings must be set.

To configure the wired network settings for the device:

1. Select the **Settings** tab.
2. Expand the **System Setup** accordion.
3. Click the **+** (plus) icon next to **Network** to display time and date settings for the device.

Settings - Network (Wired Network Settings)



− Network

Network Configuration

Domain	localdomain
Host Name	UC-P8-T-HS-001
Primary Static DNS	0.0.0.0
Secondary Static DNS	0.0.0.0

Network Proxy Setting

Proxy	○
Don't use the proxy server for local (intranet) addresses	○

Primary LAN

DHCP	●
IP Address	10.0.1.255
Subnet Mask	255.255.255.0
Default Gateway	10.0.1.1
VLAN	Disabled
VLAN Tag	0
Priority Value	0
PC Port Mode	Enabled
PC Port VLAN Tag	0
PC Port Priority Value	0
CDP	○
LLDP	●
LLDP TX Interval (Seconds)	30

4. Enter the following information for the wired network configuration.
   - **Network Configuration**
     - **Primary Static DNS**: Enter a primary DNS server address to use for DNS name lookups.
     - **Secondary Static DNS**: Enter a secondary DNS server address to use for DNS name lookups.

- **Primary LAN**
  - **DHCP**: Turn off the toggle to turn off DHCP. Turning off DHCP allows the wired network to be configured manually.
  - **IP Address**: If DHCP is turned off, enter the desired device IP address on the network.
  - **Subnet Mask**: If DHCP is turned off, enter the desired device subnet mask address on the network.
  - **Default Gateway**: If DHCP is turned off, enter the desired gateway router address on the network.

5. Configure any other wired network settings as needed (such as **VLAN**, **PC Port Mode**, **CDP**, **LLDP**, and so forth) for your deployment.
6. Select **Save Changes** from the **Action** menu.

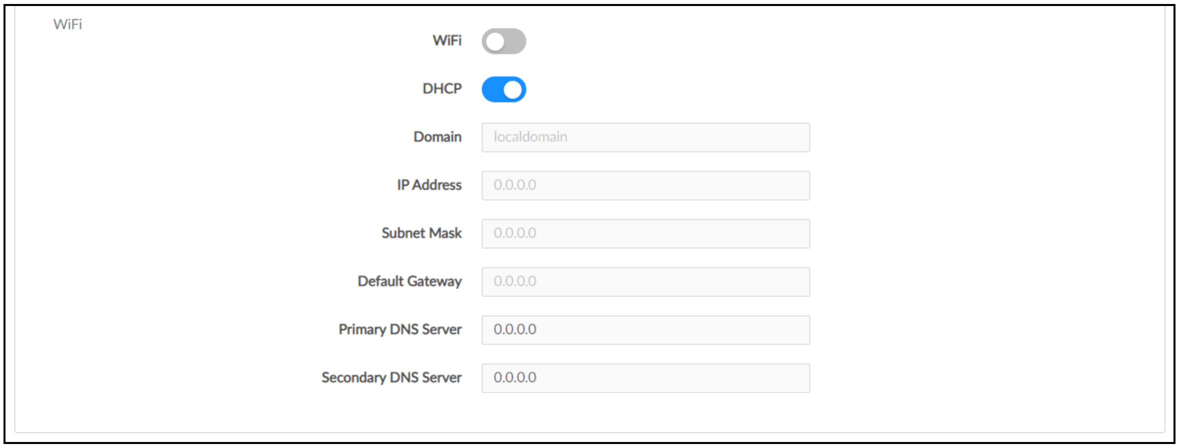
Wi-Fi Network Configuration

To configure the device to communicate to the LAN over Wi-Fi™ communications, the following changes must be made. If DHCP is available on the local network, then no additional configuration changes are necessary. If DHCP is not available or if the administrator wishes to manually set the network configuration, then the domain, IP address, subnet mask, default gateway, and DNS server settings must be set.

To configure the Wi-Fi network settings for the device:

1. Select the **Settings** tab.
2. Expand the **System Setup** accordion.
3. Click the **+** (plus) icon next to **Network** to display time and date settings for the device.

   Settings - Network (Wi-Fi Network Settings)



WiFi

WiFi: off

DHCP: on

Domain: localdomain

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

4. Turn on the **Wi-Fi** toggle to turn on the Wi-Fi adapter.

5. Enter the following information for the Wi-Fi network configuration.
   - **DHCP**: Turn off the toggle to turn off DHCP. Turning off DHCP allows the Wi-Fi network to be configured manually.
   - **Domain**: If DHCP is turned off, enter the fully qualified Wi-Fi domain name on the network.
   - **IP Address**: If DHCP is turned off, enter the desired device IP address on the network.
   - **Subnet Mask**: If DHCP is turned off, enter the desired device subnet mask address on the network.
   - **Default Gateway**: If DHCP is turned off, enter the desired gateway router address on the network.
   - **Primary DNS Server**: Enter a primary DNS server address to use for DNS name lookups.
   - **Secondary DNS Server**: Enter a secondary DNS server address to use for DNS name lookups.
6. Select **Save Changes** from the **Action** menu.

802.1X Authentication

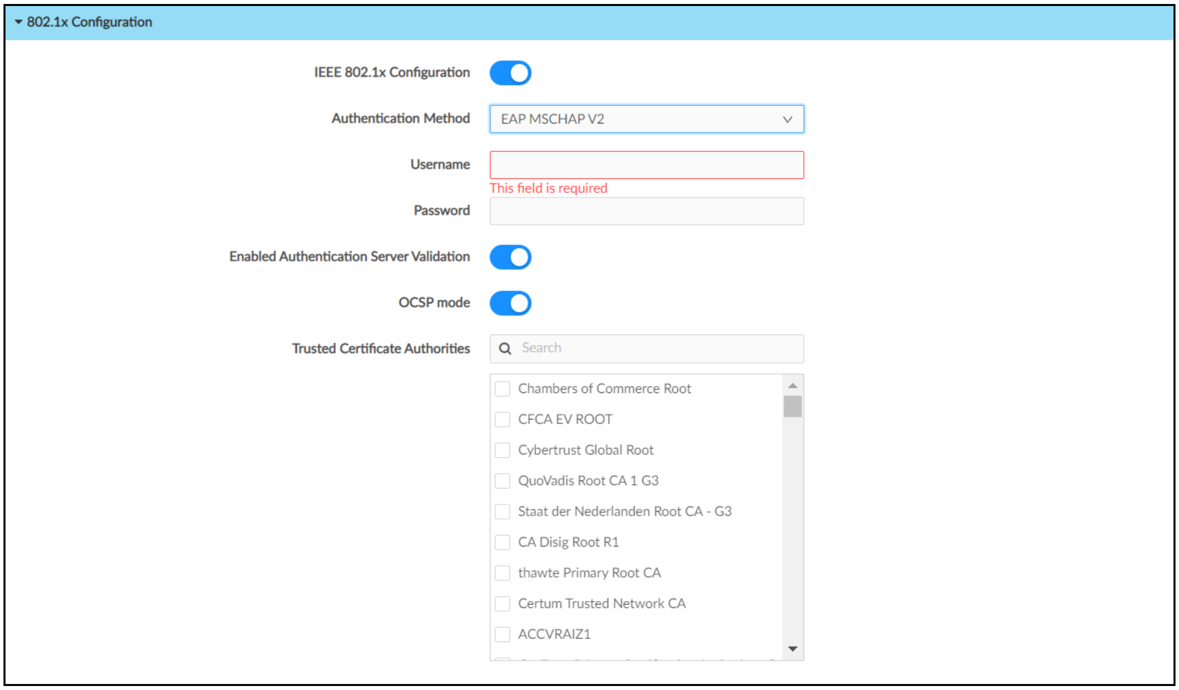
802.1X is an IEEE network standard designed to enhance the security of both wireless and wired Ethernet networks. This device supports 802.1X on its primary wired Ethernet interface only. If the network requires 802.1X, the device must be configured for 802.1X before being put on the network.

Configure 802.1X Settings

To configure 802.1X settings for the device:

1. Select the **802.1x Configuration** tab to display settings for configuring 802.1X authentication.

802.1x Configuration



▾ 802.1x Configuration

IEEE 802.1x Configuration

Authentication Method: EAP MSCHAP V2

Username:

This field is required

Password:

Enabled Authentication Server Validation

OCSP mode

Trusted Certificate Authorities: Search

- □ 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
- □ ACCVRAIZ1

2. Turn on the **IEEE 802.1x Configuration** toggle to turn on 802.1X authentication.
3. Select the desired 802.1X authentication method from the **Authentication Method** drop-down menu:
   - Select **EAP-TLS Certificate** to authenticate using a client certificate.
   - Select **EAP MSCHAP V2** to authenticate using a username and password.
4. If **EAP MSCHAP V2** is selected for **Authentication Method**, enter the username and password required for the client authentication.
5. Turn on the **Enabled Authentication Server Validation** toggle to turn on server validation. If turned on, the 802.1X supplicant will validate the authentication server's certificate.
6. If **Enabled Authentication Server Validation** is turned on and if your server supports OCSP (Online Certificate Status Protocol), turn on the **OCSP mode** toggle to require a valid OCSP stapling response for all not-trusted certificates in the server certificate chain.
7. Select trusted CAs (Certificate Authorities) from the **Trusted Certificate Authorities** selections to be used for server validation.

   > **NOTE:** For more information on configuring trusted certificate authorities, refer to Configure Trusted Certificate Authorities on page 13.

   - Select the check box to the left of a CA to select it as a trusted CA.
   - Enter a search term into the text field at the top of the CA menu to search for and display CAs that match the search term.
8. Select **Save Changes** from the **Action** menu.

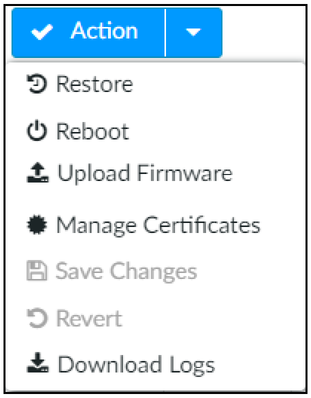
Configure Trusted Certificate Authorities

Trusted Certificate Authorities (CAs) can be added or deleted from the device for use with 802.1X and remote Syslog server validation.

To configure Trusted Certificate Authorities on the device:

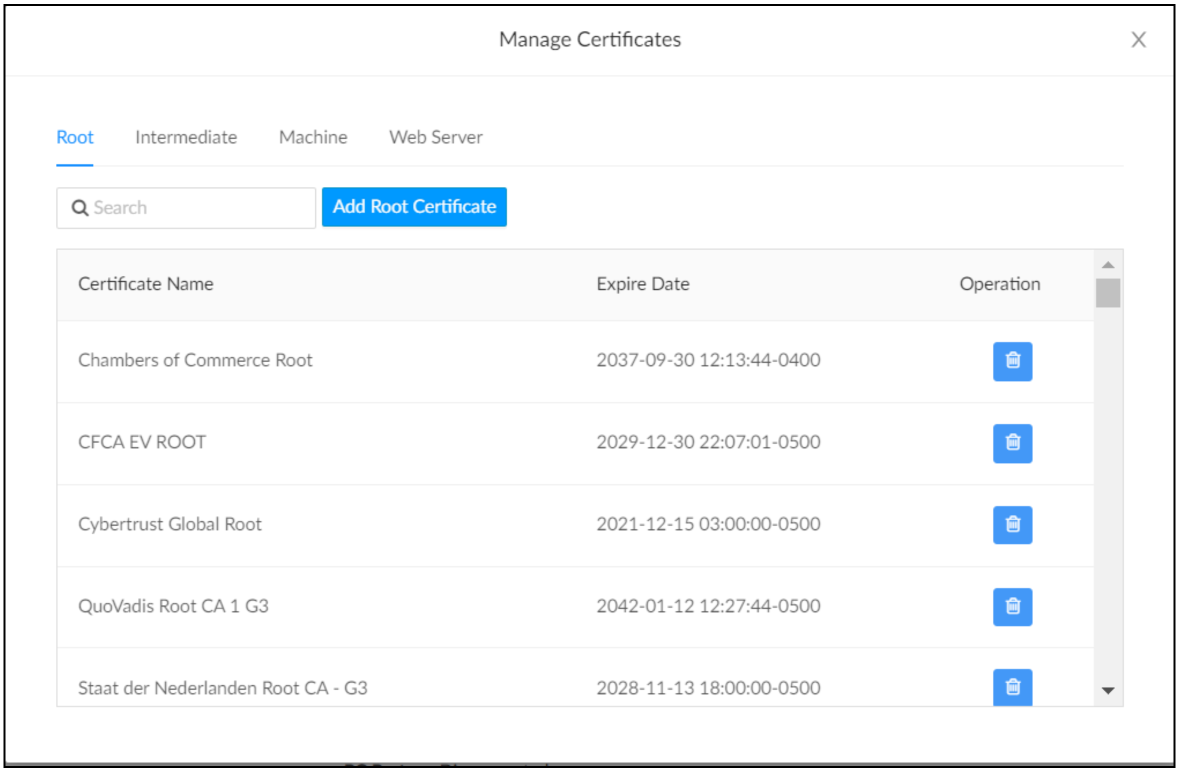
1. Select **Manage Certificates** from the **Actions** menu.

   Actions Menu

   The **Manage Certificates** dialog box is displayed.

   Manage Certificates Dialog Box

Certificate Name	Expire Date	Operation
Chambers of Commerce Root	2037-09-30 12:13:44-0400	🗑
CFCA EV ROOT	2029-12-30 22:07:01-0500	🗑
Cybertrust Global Root	2021-12-15 03:00:00-0500	🗑
QuoVadis Root CA 1 G3	2042-01-12 12:27:44-0500	🗑
Staat der Nederlanden Root CA - G3	2028-11-13 18:00:00-0500	🗑

2. To add a new certificate:
    a. Select the tabs at the top of the dialog box to select the desired CA type that will be added (**Root**, **Intermediate**, **Machine**, or **Web Server**). The same settings are provided for each CA type.
    b. Select **Add [CA Type] Certificate**, where [CA Type] is the selected CA type.
    c. Navigate to the CA file on the host computer.
    d. Select the CA file, and then select **Open**. A success message is displayed if the upload is successful, and the certificate will be added to the table for its respective CA type.
3. To delete a certificate, select the trash can button 🗑 to the right of the certificate's table row, and then select **OK** when prompted to confirm the deletion.

Set the Time and Date

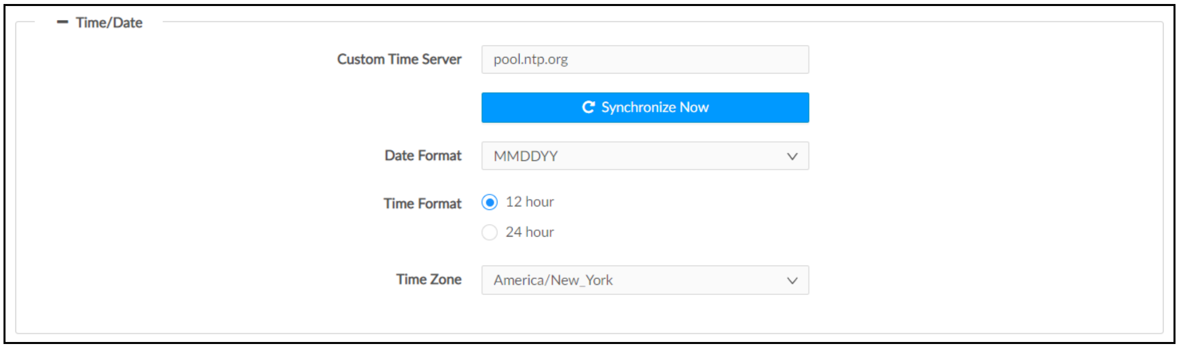
All devices use NTP to synchronize their clock. By default, the device is configured to receive time data from pool.ntp.org. A custom NTP server can be used instead.

> **NOTE:** The device does not support using secure NTP servers at this time.

To customize the time and date settings on the device:

1. Select the **Settings** tab.
2. Expand the **System Setup** accordion.
3. Click the **+** (plus) icon next to **Time/Date** to display time and date settings for the device.

Settings - Remote Syslog



− Time/Date

Custom Time Server: pool.ntp.org

Date Format: MMDDYY

Time Format: ● 12 hour ○ 24 hour

Time Zone: America/New_York

4. Enter the following information for the time and date configuration:
    - **Custom Time Server**: Enter the IP address or Fully Qualified Domain Name (FQDN) of the custom NTP server.
    - **Date Format**: Use the drop-down menu to select the format that the date will display on the device.

- **Time Format**: Select the time format that the time will display on the device (**12 hour** or **24 hour**).
- **Time Zone**: Use the drop-down menu to select the correct time zone for the device.

5. Select **Save Changes** from the **Action** menu.

Configure the Remote Syslog

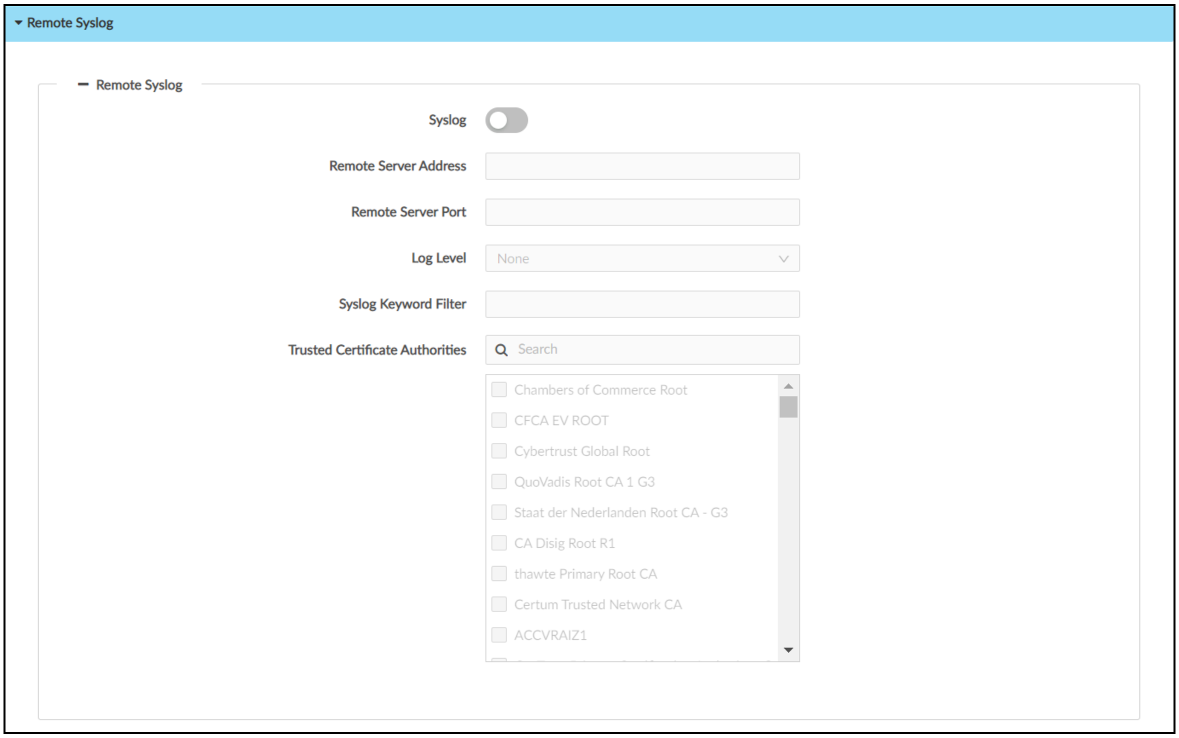
Devices do not send audit logs to a remote Syslog server by default. A connection to a remote Syslog server must be turned on and configured manually.

To turn on sending audit logs to a remote Syslog server:

> **NOTE:** The remote server host must have a system log server with 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 offload them over time. If TLS is turned on, a TLS-enabled server with the appropriate certificates is required.

1. Select the **Settings** tab.
2. Expand the **Remote Syslog** accordion to display settings for the remote Syslog.

Settings - Remote Syslog



▾ Remote Syslog

− Remote Syslog

Syslog: ○ (off)

Remote Server Address:

Remote Server Port:

Log Level: None

Syslog Keyword Filter:

Trusted Certificate Authorities: Search

□ 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
□ ACCVRAIZ1

3. Turn on the **Syslog** toggle.

4. Enter the following information for the remote Syslog configuration:
    - **Remote Server Address**: Enter the IP address or Fully Qualified Domain Name (FQDN) of the remote Syslog server.
    - **Remote Server Port**: Enter the web port of the remote Syslog server.
    - **Log Level**: Select one of the following log levels to determine which messages are logged to the remote Syslog. All messages of that log level or above will be logged.

        > **NOTE:** For examples of common events that can trigger messages for specific logging levels, refer to the UC-P8 and UC-P10 Series Desk Phones Product Manual.

        - **DEBUG**: Logs all "debug" messages and above to the Syslog.
        - **INFO**: Logs all "info" messages and above to the Syslog.
        - **WARNING**: Logs all "warning" messages and above to the Syslog.
        - **ERROR**: Logs all "error" messages and above to the Syslog.
    - **Syslog Keyword Filter**: (Optional) Enter keywords to filter the Syslog entries by those keywords. Multiple keywords should be entered as a comma-delimited list without any spaces (for example, "SIP,registration,codec").
    - **Trusted Certificate Authorities**: If TLS is turned on, select trusted CAs (Certificate Authorities) from the provided CAs to be used for server validation.

        > **NOTE:** For more information on configuring trusted certificate authorities, refer to Configure Trusted Certificate Authorities on page 13.

        - Select the check box to the left of a CA to select it as a trusted CA.
        - Enter a search term into the text field at the top of the CA menu to search for and display CAs that match the search term.
5. Select **Save Changes** from the **Action** menu.

Optional Configuration

The following sections provide information about optional device configuration settings.

Add Users and Groups

It is likely that additional users will need to be given access to the device. Refer to User and Group Management on page 20 for instructions.

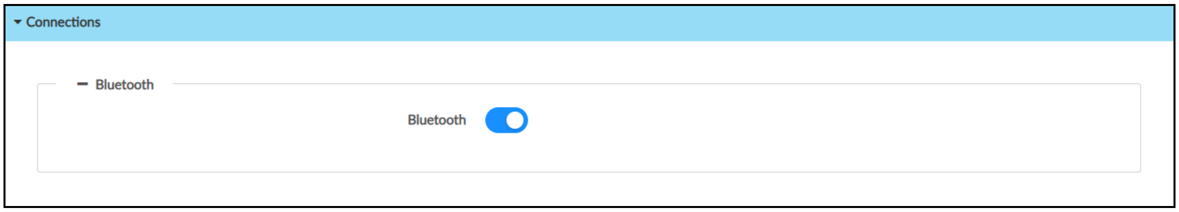
Configure Bluetooth Communications

Bluetooth™ communications are turned on by default to allow connections to supported peripheral devices. If your environment or policies do not permit Bluetooth communications, this setting can be turned off.

To turn off Bluetooth communications:

1. Select the **Settings** tab.
2. Expand the **Connections** accordion to display settings for the Bluetooth connection.

   Settings - Connections



3. Turn off the **Bluetooth** toggle.
4. Select **Save Changes** from the **Action** menu

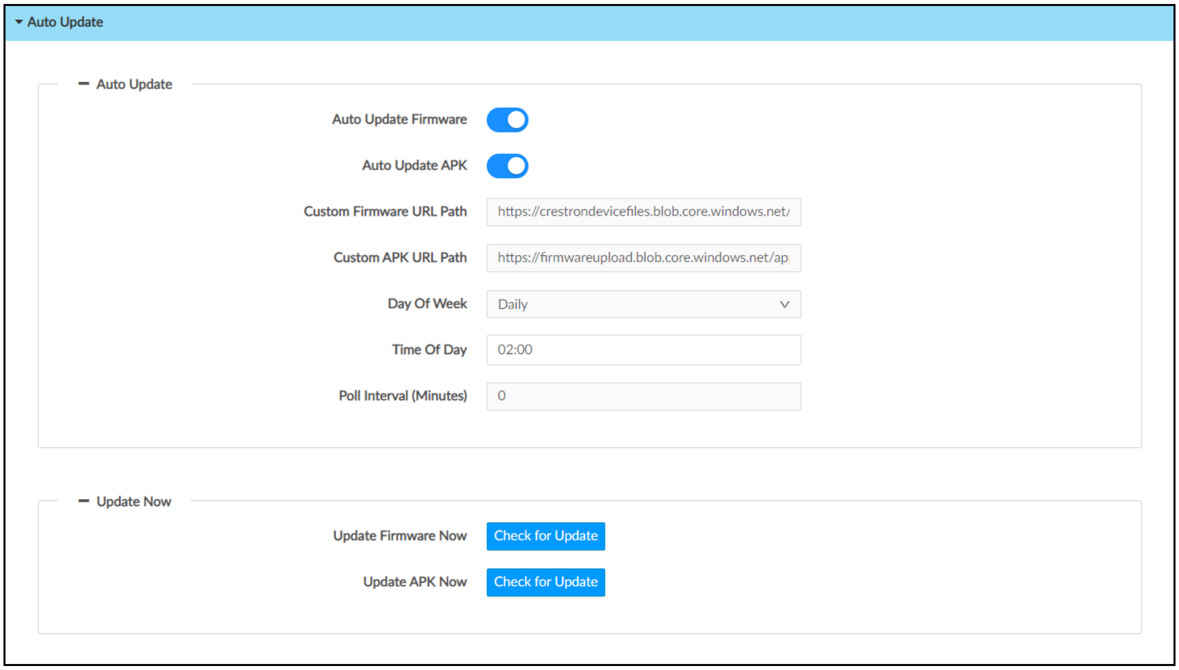
Configure Automatic Updates

The device is configured to perform automatic updates by default. When automatic updates are turned on, the device will connect to the provided update server and check for updates when scheduled (either at a set day and time or polling interval). If the device detects that an update to the firmware or Microsoft Teams APK is available, the update will be downloaded and installed automatically. If your environment or policies do not permit automatic updates, this setting can be turned off.

To turn off automatic updates:

1. Select the **Settings** tab.
2. Expand the **Auto Update** accordion to display settings for automatic updates.

   Settings - Auto Update



▾ Auto Update

− Auto Update

Auto Update Firmware ●

Auto Update APK ●

Custom Firmware URL Path: https://crestrondevicefiles.blob.core.windows.net/

Custom APK URL Path: https://firmwareupload.blob.core.windows.net/ap

Day Of Week: Daily

Time Of Day: 02:00

Poll Interval (Minutes): 0

− Update Now

Update Firmware Now: Check for Update

Update APK Now: Check for Update

3. Turn off the **Auto Update Firmware** toggle.
4. Turn off the **Auto Update APK** toggle.
5. Select **Save Changes** from the **Action** menu.

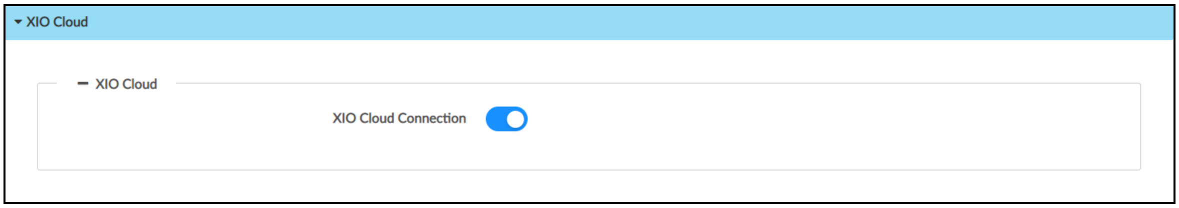
Configure a Connection to XiO Cloud

The device is connected to the XiO Cloud® service by default, which allows the device to be discovered by and claimed into the XiO Cloud service. If your environment or policies do not permit communications with external services, this settings can be turned off.

To turn off a connection to XiO Cloud:

1. Select the **Settings** tab.
2. Expand the **XiO Cloud** accordion to display settings for the XiO Cloud connection.

   Settings - XiO Cloud



▾ XIO Cloud

− XIO Cloud

XIO Cloud Connection ●

3. Turn off the **XiO Cloud Connection** toggle.
4. Select **Save Changes** from the **Action** menu.

Management Functions

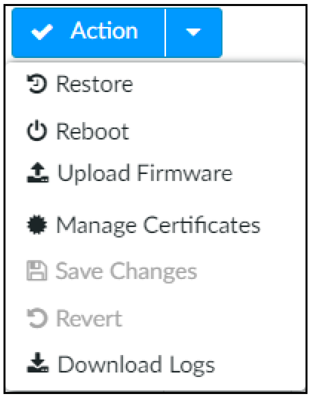
The following sections provide information about device management functions.

Firmware Update

To perform a manual firmware update:

1. Select **Upload Firmware** from the **Actions** menu.

   Actions Menu

2. Navigate to the firmware BIN file on the host computer.
3. Select the firmware BIN file, and then select **Open**. If the firmware BIN file is uploaded successfully, a message window is displayed with the status of the firmware update.
4. Upon successful firmware update, a dialog box is displayed indicating that the update was successful. Select **OK**, then log back into the web configuration interface.

User and Group Management

Users and groups can be added to the device after an administrator account has been created. User and group management is handled through the Active Directory (LDAP) service. All users and groups must be created in Active Directory before they can be added to the device.

> **NOTE:** The device does not support any local access levels outside of the local admin account. User and group access levels are created and managed through Active Directory.

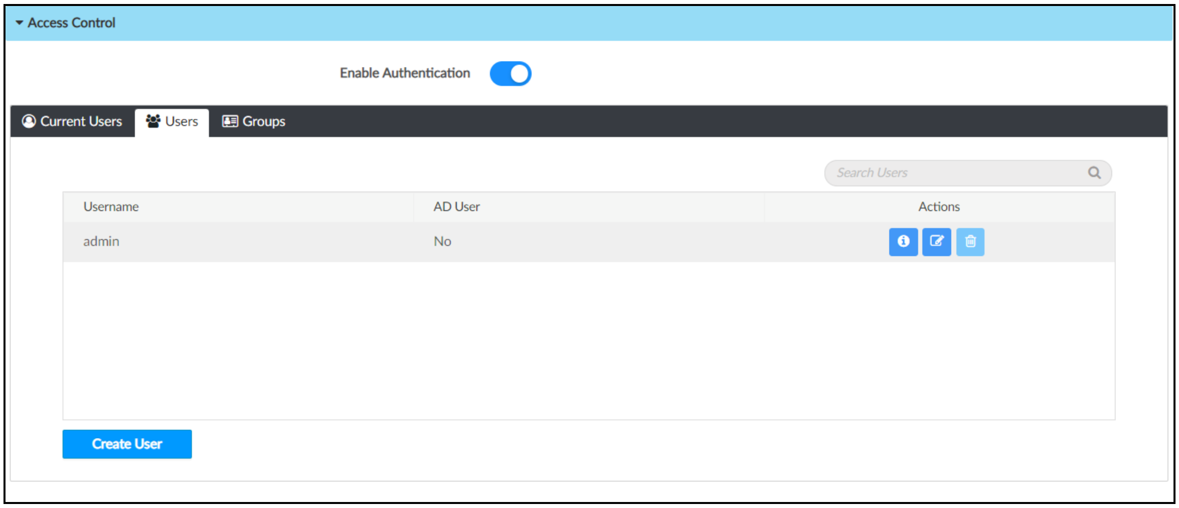
The following sections describe how to manage users and groups on the device.

Add a User

To add an Active Directory user to the device:

1. Select the **Security** tab.
2. Expand the **Access Control** accordion.
3. Select the **Users** tab to display settings for configuring users on the device.

   Security - Access Control (Users Tab)

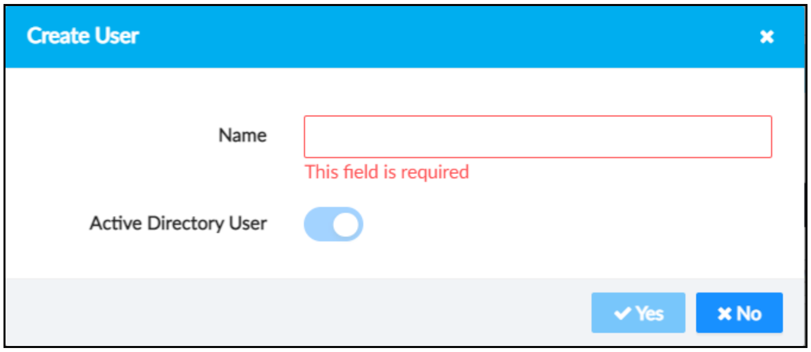


Enable Authentication: on

Username	AD User	Actions
admin	No	

4. Select **Create User**. The **Create User** dialog box is displayed.

   Create User Dialog Box



Name:

This field is required

Active Directory User: on

5. Enter the user name in the **Name** text field. The user name must match exactly the user name in Active Directory.
6. Select **Yes** to create the new user. The user is added to the **Users** table on the **Security** page.

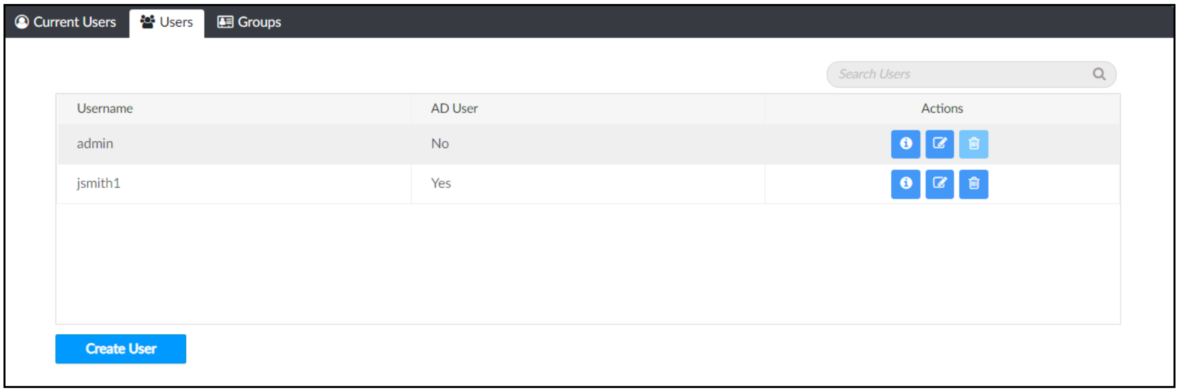
Delete a User

To delete an Active Directory user from the device:

> **NOTE:** The local admin user cannot be deleted from the device.

1. Select the **Security** tab.
2. Expand the **Access Control** accordion.
3. Select the **Users** tab to display settings for configuring users on the device.

   Users Tab



Username	AD User	Actions
admin	No	ℹ ✎ 🗑
jsmith1	Yes	ℹ ✎ 🗑

4. Select the trash can button 🗑 to the right of the user's table row. A dialog box is displayed confirming the deletion.
5. Select **Yes** to delete the user.

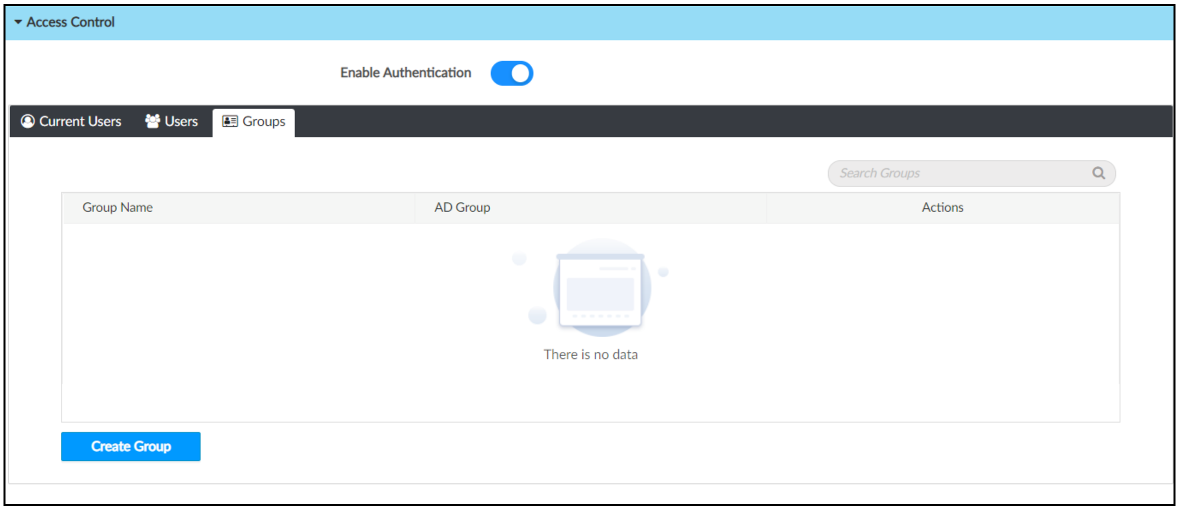
The user is removed from the device but not from the Active Directory service.

Add a Group

To add an Active Directory group to the device:

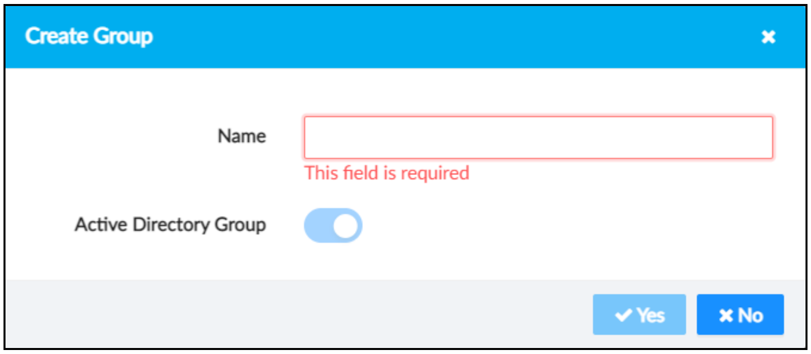
1. Select the **Security** tab.
2. Expand the **Access Control** accordion.
3. Select the **Groups** tab to display settings for configuring groups on the device.

Security - Access Control (Groups Tab)



4. Select **Create Group**. The **Create Group** dialog box is displayed.

   Create Group Dialog Box



5. Enter the domain and group name in the **Name** text field. The domain and group name must match exactly the domain and group in Active Directory (such as "CRESTRON.COM\ldapusers").
6. Select **Yes** to create the new group. The user is added to the **Groups** table on the **Security** page.

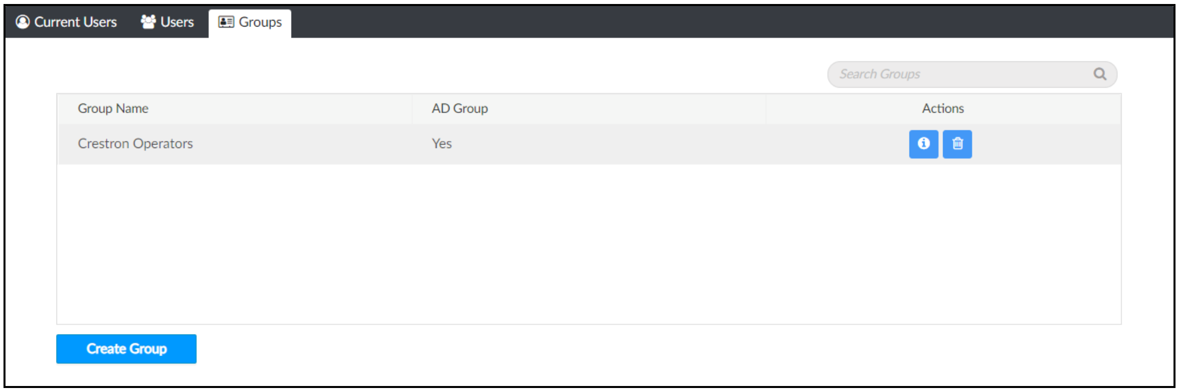
All users of the Active Directory group inherit the access level set for the group within Active Directory.

Delete a Group

To delete an Active Directory group from the device:

1. Select the **Security** tab.
2. Expand the **Access Control** accordion.
3. Select the **Groups** tab to display settings for configuring groups on the device.

Groups Tab



Group Name	AD Group	Actions
Crestron Operators	Yes	ℹ 🗑

4. Select the trash can button 🗑 to the right of the group's table row. A dialog box is displayed confirming the deletion.
5. Select **Yes** to delete the group.

The group is removed from the device but not from the Active Directory service.

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

Security Reference Guide — Doc. 9313A
07/29/22
Specifications subject to
change without notice.