CCS-UC-1-T
Crestron Mercury® Tabletop UC Audio Conference Console for Microsoft Teams™

Supplemental Guide

Crestron Electronics, Inc.

This document was written by the Technical Publications department at Crestron.

Contents

CCS-UC-1-T: Crestron Mercury Tabletop UC Audio Conference Console for Microsoft Teams

Introduction

The CCS-UC-1-T Crestron Mercury® Tabletop UC Audio Conference Console for Microsoft Teams™ provides an audio conferencing solution specifically engineered for use with the Microsoft Teams intelligent communications platform. The tabletop touch screen console features full-duplex wideband audio conferencing and speakerphone capabilities that deliver a consistent user experience in every meeting space from the familiar and intuitive Microsoft Teams UI. The Microsoft Teams UI provides simple operation, built-in calendaring, and one-touch meeting joins.

This supplemental guide discusses the requirements and configuration instructions for the CCS-UC-1-T as part of a UC-M100-T Flex M100-T Tabletop UC Audio Conference System for Microsoft Teams. For information on installing the CCS-UC-1-T, refer to the CCS-UC-1-T Quick Start Guide (Doc. 8399) at www.crestron.com/manuals.

Requirements

Administrator

This document is written for use by a facility's Information Technology (IT) administrator. The IT administrator should have the following knowledge and skills:

- General Skills
  - IP Networking
  - Basic PC Operation and Administration
- Crestron-specific skills
  - Crestron Fusion® software (if applicable)
  - Crestron XiO Cloud™ service

Operating Environment

NOTE: If the CCS-UC-1-T is powered with PoE+ (IEEE 820.3at), PoE+ switches that utilize Link Layer Discovery Protocol (LLDP) must have LLDP enabled. Please coordinate with the IT Administrator who manages network infrastructure at the customer site to make sure the PoE+ ports have LLDP enabled. For more information, refer to "Troubleshooting" on page 32.

The CCS-UC-1-T requires a Microsoft Teams account for operation.

Accessories

The CCS-UC-1-T offers a variety of accessories for a custom installation. Refer to the following websites for specifications and other information.

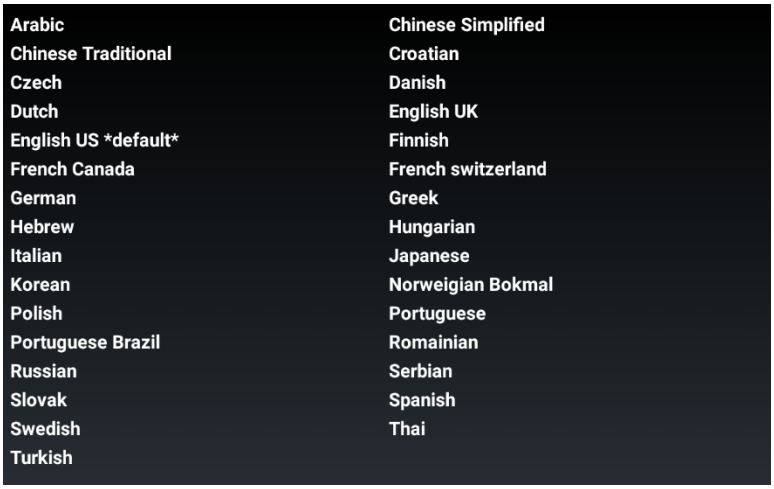
Accessories for CCS-UC-1-T

PRODUCT	PART NUMBER	WEBSITE
Microphone Pod	CCS-UCA-MIC	http://www.crestron.com/products/model/CCS-UCA-MIC
Surface Mount Kit	CCS-UCA-SMK	http://www.crestron.com/products/model/CCS-UCA-SMK

Startup & Sign In

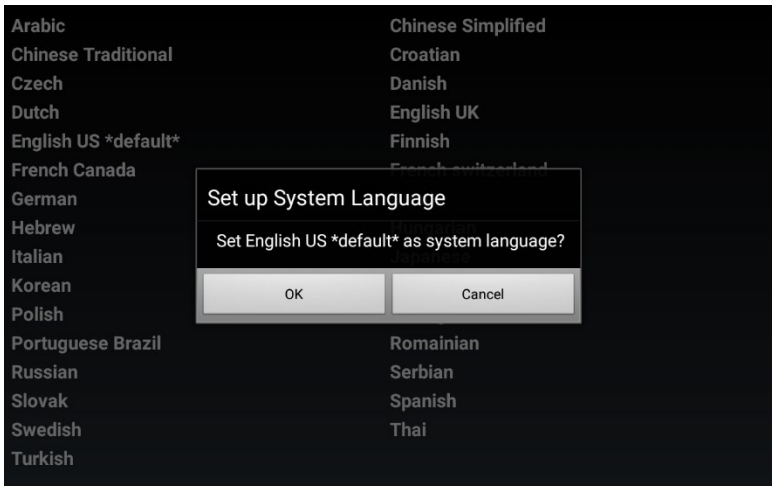
After making all connections, the device displays the language selection screen.

Select a Language



1. Tap the name of the language to use. The device will ask for confirmation.

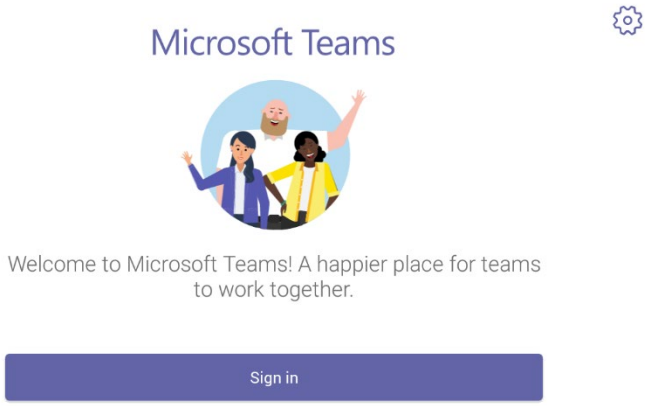
Confirm Language Selection



2. Tap **OK** to confirm the selection or **Cancel** to choose another language.

   The device will continue with configuration, and then display the Microsoft Teams start screen.

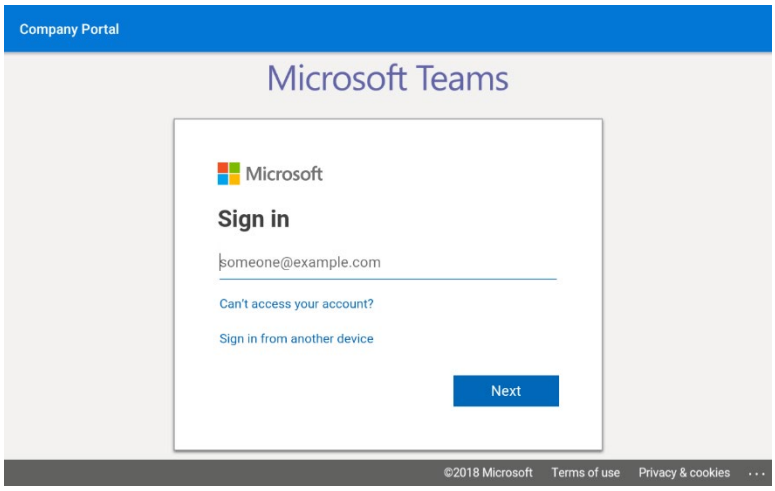
Microsoft Teams Start Screen



3. Tap **Sign in** to display the **Sign in** screen.

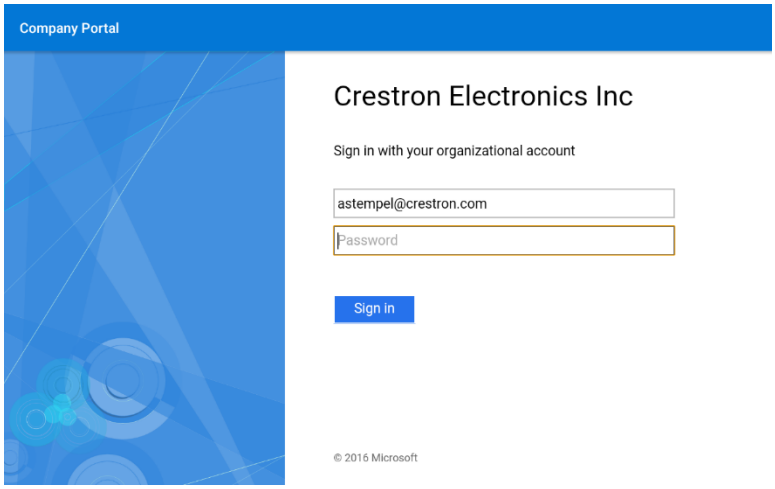
NOTE: You can also tap ⚙ on the top left to set the partner settings. For details, refer to "Partner Settings" on page 6.

Microsoft Teams Sign In Screen



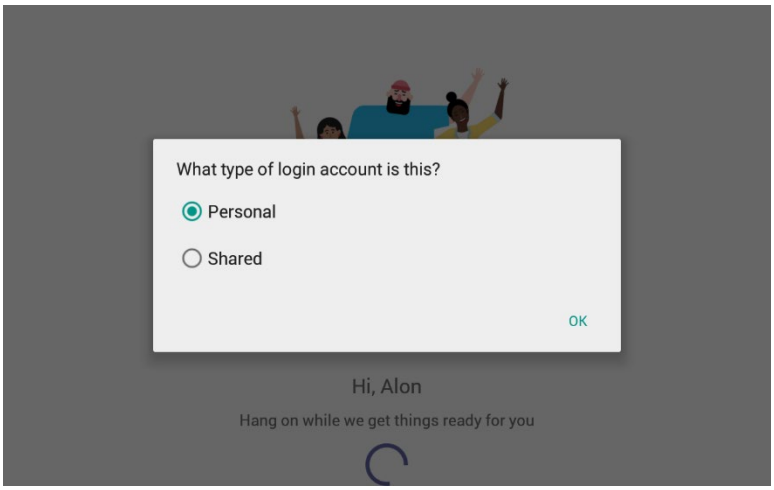
4. Enter the email address of the Microsoft Teams account, and tap **Next**. The Company Portal Sign In screen is displayed.

Company Portal Sign In Screen



5. Enter the password associated with the Microsoft Teams account, and tap **Sign in**. The device will ask you to select the type of login account.

Select Account Type



The device can be set up with a personal account or a shared account.

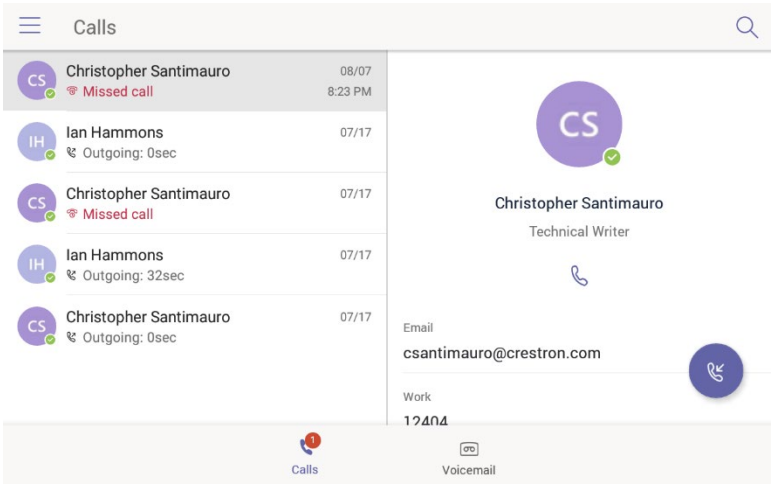
Use the **Personal** setting if the device is to be placed on a user's desk. Devices with a personal account will show call history and have access to voice mail.

Use the Shared setting if the device will be placed in a conference room. Call history information and voice mail features are not available.

Select and account type and tap **OK**.

The device will log into the Microsoft Teams service and display the home screen.

Home Screen



Configuration

The CCS-UC-1-T can be configured from the front panel (partner settings) or a computer with web browser software (device settings). If using a computer, the CCS-UC-1-T and computer must be connected to a commonly accessible network.

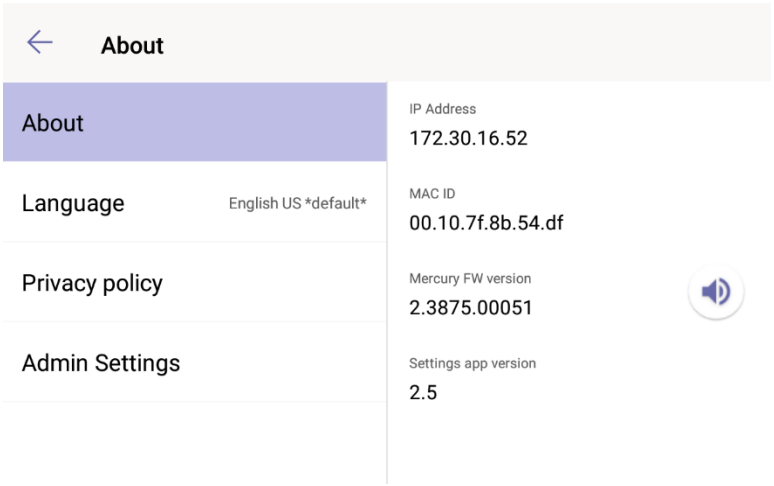
Partner Settings

You can use the device's partner settings to view information about the device, adjust the volume, set the language of the device, view the privacy policy, and configure the device.

To access the partner settings, tap ⚙ on the Microsoft Teams start screen. The IP address, MAC ID, Mercury FW version, and Settings app version are displayed.

NOTE: Partner settings can also be accessed from the main application. To access the partner settings, tap ☰, **Settings**, and then **Device Settings**.

Partner Settings



To exit the partner settings, tap ←.

Adjust Volume

To adjust the volume, press 🔊 and drag up or down to raise or lower the volume.

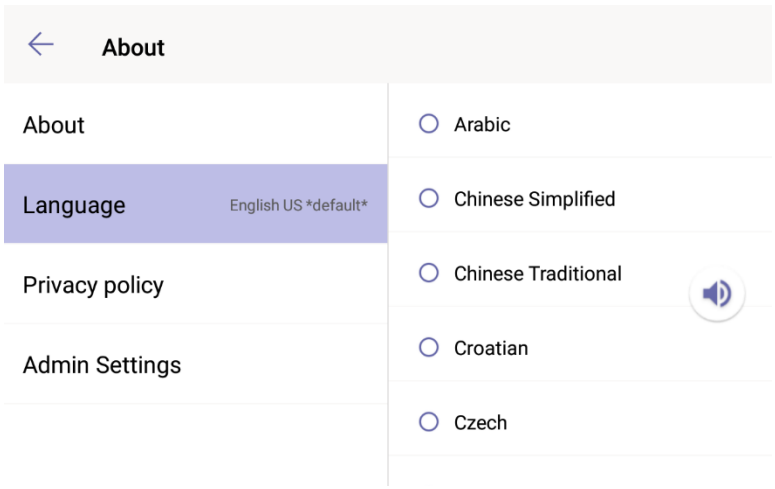
Set Language

The currently selected language is displayed in the language field.

To select a new language:

1. Tap **Language**. A list of languages will display on the right side of the screen.

Language



2. Drag a finger up or down the right side of the screen to view the list of available languages.

3. Tap a language to select it.

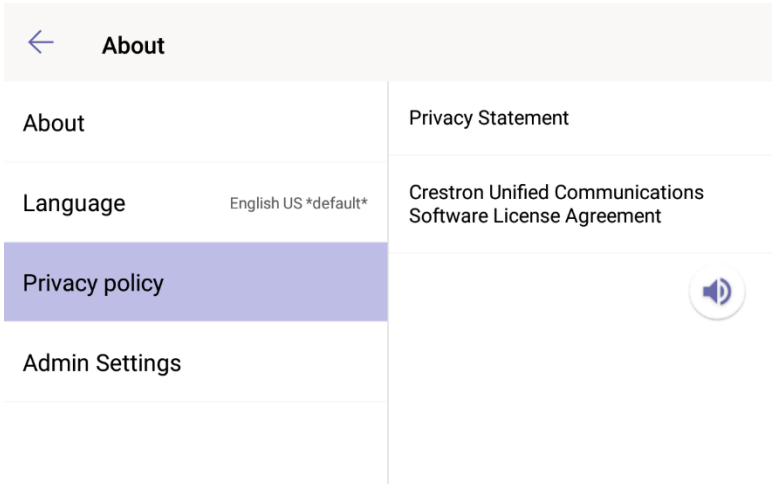
Privacy Policy

The privacy statement and the Crestron® Unified Communications software license agreement are available for viewing.

To view the view the privacy statement or the Crestron® Unified Communications software license agreement

1. Tap **Privacy Policy**.

Privacy Policy



2. Select an item to view.
   - To view the privacy statement, tap **Privacy Statement**.

– To view the software license agreement, tap **Crestron Unified Communications Software License Agreement**.

Admin Settings

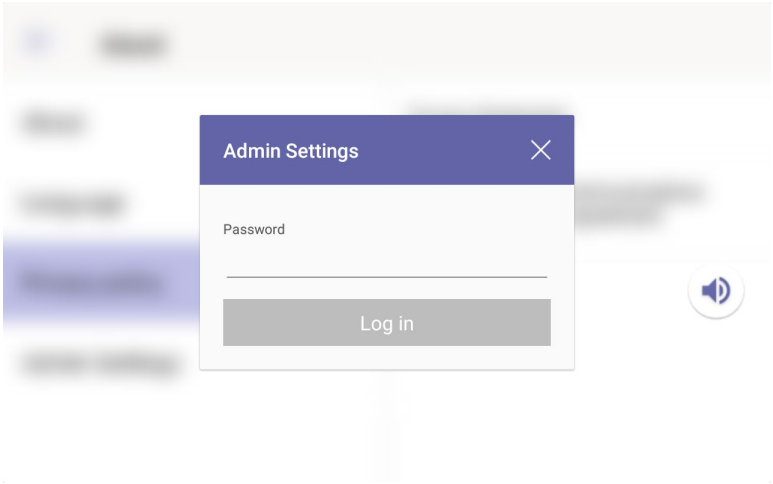
Use the Admin Settings feature to configure the display operation, time and date, network and settings. You can also change the administrator password, reboot the device, or restore the default factory settings.

NOTE: Many of these settings as well as other settings can be configured from the device's configuration web pages. For details, refer to "Device Settings" on page 12.

To access the Admin Settings feature:

1. Tap **Admin Settings**. A login screen will display.

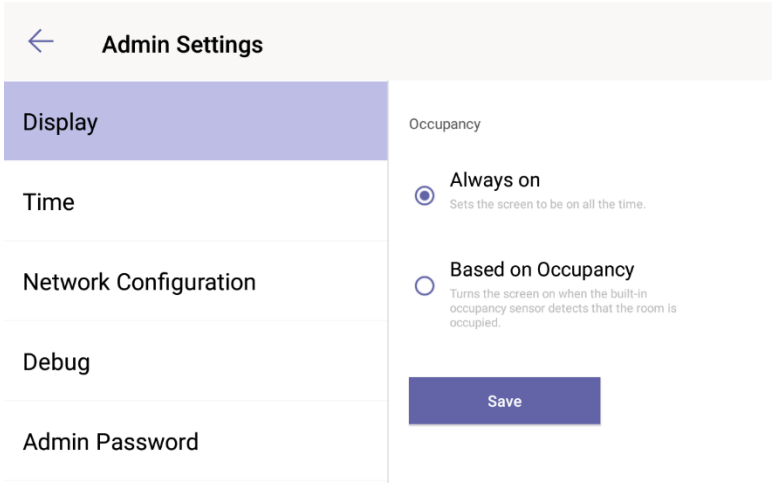
   Admin Settings Login

2. Enter the Admin Settings password (default = "**admin**") and tap **Log in**. The Admin Settings options will display.

   NOTE: After entering the Admin Settings password the first time, the device will prompt you to enter a new password. Crestron strongly recommends changing the password from the factory default.

Admin Settings Options



3. To exit the Admin settings and return to the previous screen, tap ←.

Display

The display can be set to stay on all the time or only turn on based on room occupancy. To specify how the display functions:

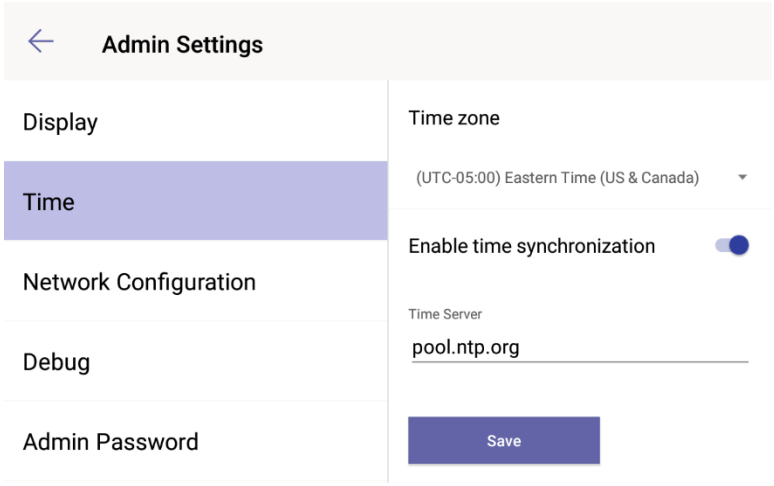
1. Tap **Display**.
2. Select an operating mode.
   - **Always on** sets the screen to be on all the time.
   - **Based on Occupancy** sets the screen to turn on when the built-in occupancy sensor detects that the room is occupied.
3. Tap **Save** to save the setting.

Time

The Time section is used to configure the built-in clock. To adjust the clock settings:

1. Tap **Time** on the left side of the screen. The settings are displayed on the right side of the screen.

Time Options



– The local time zone can be set from the front panel. To set the time zone:

  i. Tap the displayed time zone. A list of time zones is displayed.

  ii. Press and drag up or down to view the complete list of time zones.

  iii. Tap the new time zone.

– The clock can be synchronized with a time server. To enable time synchronization:

  i. Move the **Enable time synchronization** switch to the right.

  ii. In the **Time Server** field, enter the web address of the time server.

  iii. Tap **Save** to save the settings.

– The clock can be synchronized with the time server on demand. To synchronize the clock:

  i. Press and drag upward until the **Synchronize now** button is displayed.

  ii. Tap **Synchronize now**.

Network Configuration

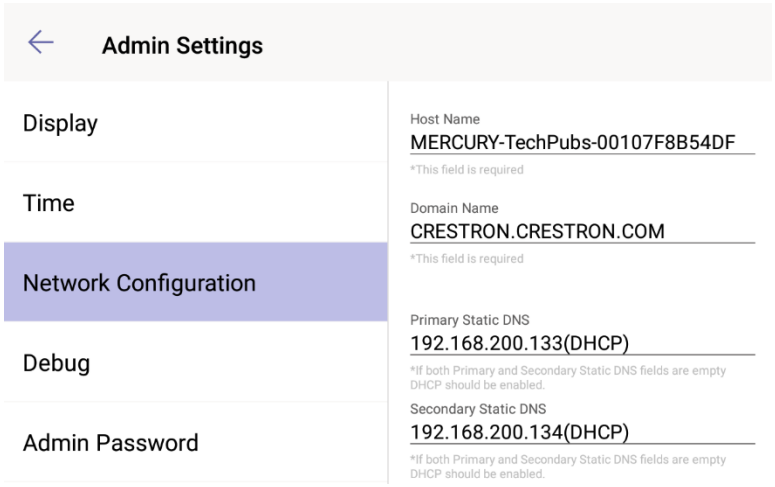
The front panel can be used to configure the network connection. The host name, domain name, primary and secondary DNS addresses, DHCP mode, IP address, subnet mask address, and default gateway address can all be set from the front panel.

NOTE: The IP address, subnet mask, and default gateway address cannot be manually set when the DHCP setting is enabled. When DHCP is enabled, the primary and secondary DNS addresses are also obtained by the DHCP server.

To configure the network connection:

1. Tap **Network Configuration** on the left side of the screen. The settings are displayed on the right side of the screen.

   Network Configuration

2. Touch and drag up or down to scroll through the available settings.

3. Tap in a field to change a setting and make any required changes. Change the DHCP setting by sliding the **DHCP** switch to the left or right.

4. Tap **Save** to save the settings.

Debug

The Debug section contains controls for rebooting the device and restoring the factory default settings. To reboot the device or restore the factory default settings, tap **Debug** on the left side of the screen and then choose one of the following options:

- Tap **Reboot Phone** to restart the device.
- Tap **Factory Defaults** to restore the factory default settings.

Admin Password

The Admin Password section allows you to change the default password ("admin") to a password of your choosing. To change the admin password:

1. Tap **Admin Password** on the left side of the screen.

2. On the right side of the screen, enter the current password in the **Current Password** field, and the new password in the **New Password** field.

3. Retype the new password the **Confirm New Password** field.

4. Tap **Change** to save the settings.

Device Settings

You can use web browser software on a computer to view web pages to configure the device.

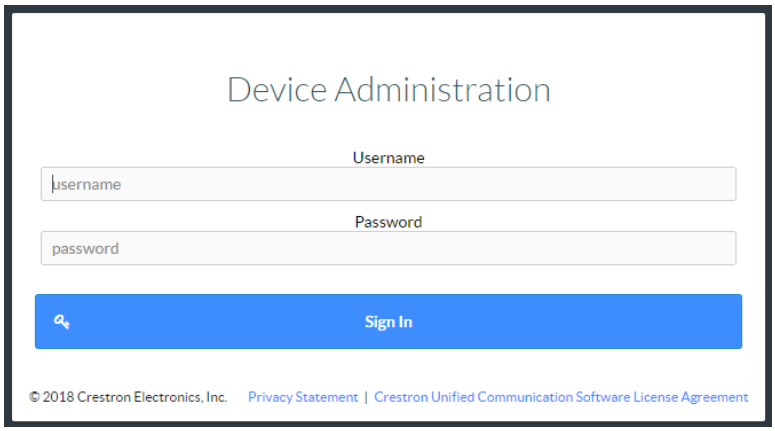
Connect to the Device

To connect to the device, follow this procedure:

1. Obtain the device's IP address from the partner settings. For details, refer to "Partner Settings" on page 6.
2. Note the IP address or host name and tap **X** to close the **System Info** screen.
3. On the computer, open a web browser and navigate to the IP address of the device. The welcome screen is displayed.

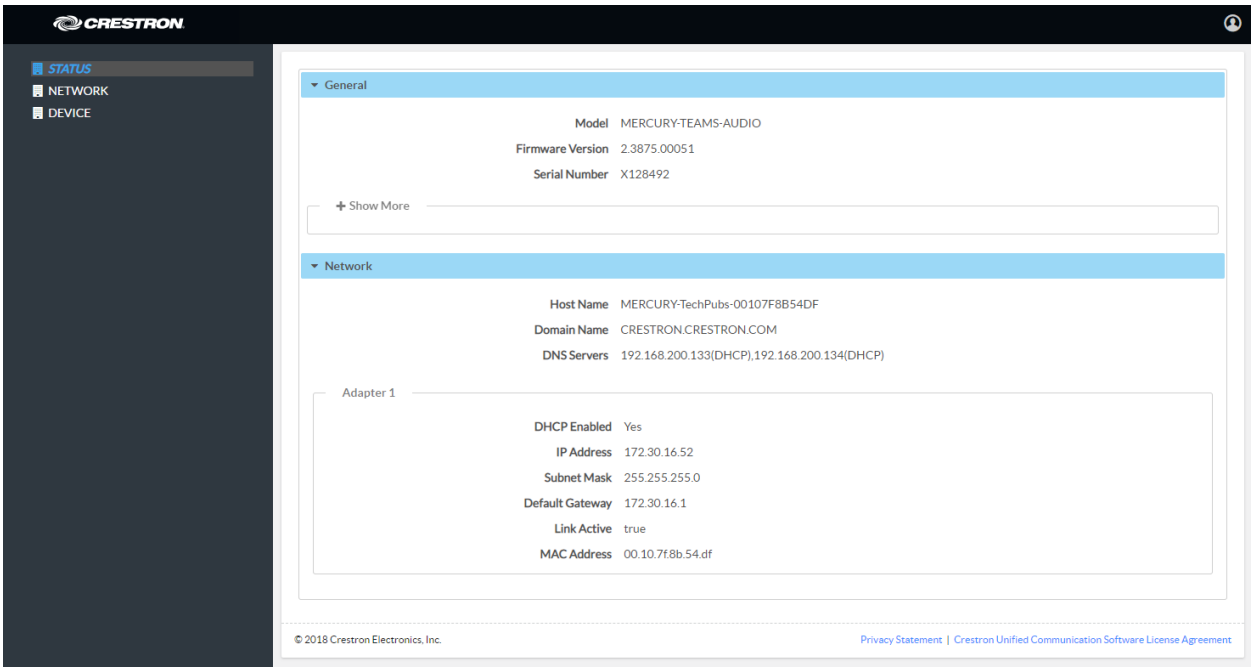
   NOTE: Prior to displaying the welcome screen, the web browser may display a security warning message about the security certificate. It is safe to ignore this warning as long as the user verifies that the browser's address bar indicates the correct IP address or host name of the device.

   Welcome Screen



4. Enter the default user name ("admin") and password ("admin").
5. Click **Sign In** to continue. The device's **Status** screen is displayed.

Status Screen



The **Status** screen displays information about the device and allows configuration of the device's operating parameters:

- **STATUS** contains general information about the device and network information. Click **Network** to view network information. Click **+ Show More Details** to view more details. Click **- Show Less** to view fewer details.
- **NETWORK** configures the device for operation in a network environment.
- **DEVICE** is used to upload firmware, reboot the device, view the system log, enable connection to Crestron XiO Cloud service, set display operation, allow automatic updates, set the date and time, authentication management, and setting the device to work with Crestron Fusion® software.

Log Out from the Device

To log out from the device and return to the welcome screen, click .

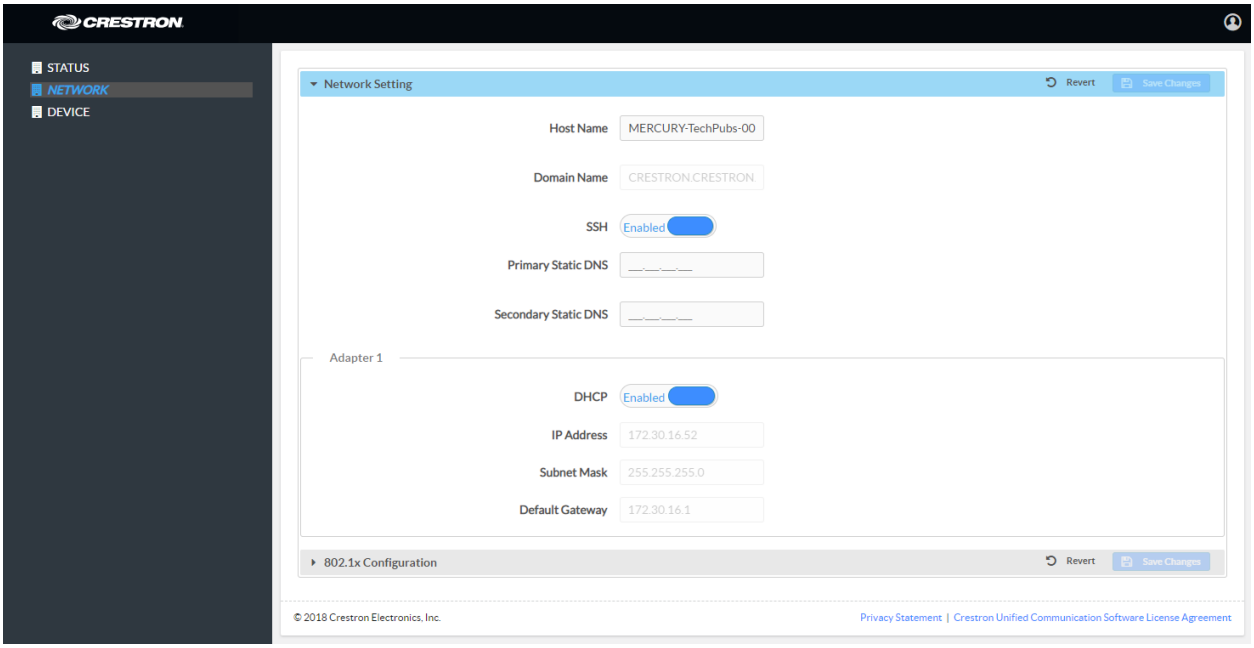
NETWORK

Click **NETWORK** to configure the device for operating in a network environment. The screen displays controls for configuring the network settings and 802.1x authentication.

Network Setting

To configure the network settings follow this procedure:

NETWORK Screen - Network Setting



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

   NOTE: Use a host name and domain name as an alternative to IP addressing when connecting client computers to the device.

2. Set **SSH** to **Enabled** to use network services securely over an unsecured network. If not needed, set **SSH** to **Disabled**.

3. If DHCP is not being used, enter IP addresses for the **Primary Static DNS** and **Secondary Static DNS** fields.

4. The 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, default gateway, and DNS server.

   – 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.

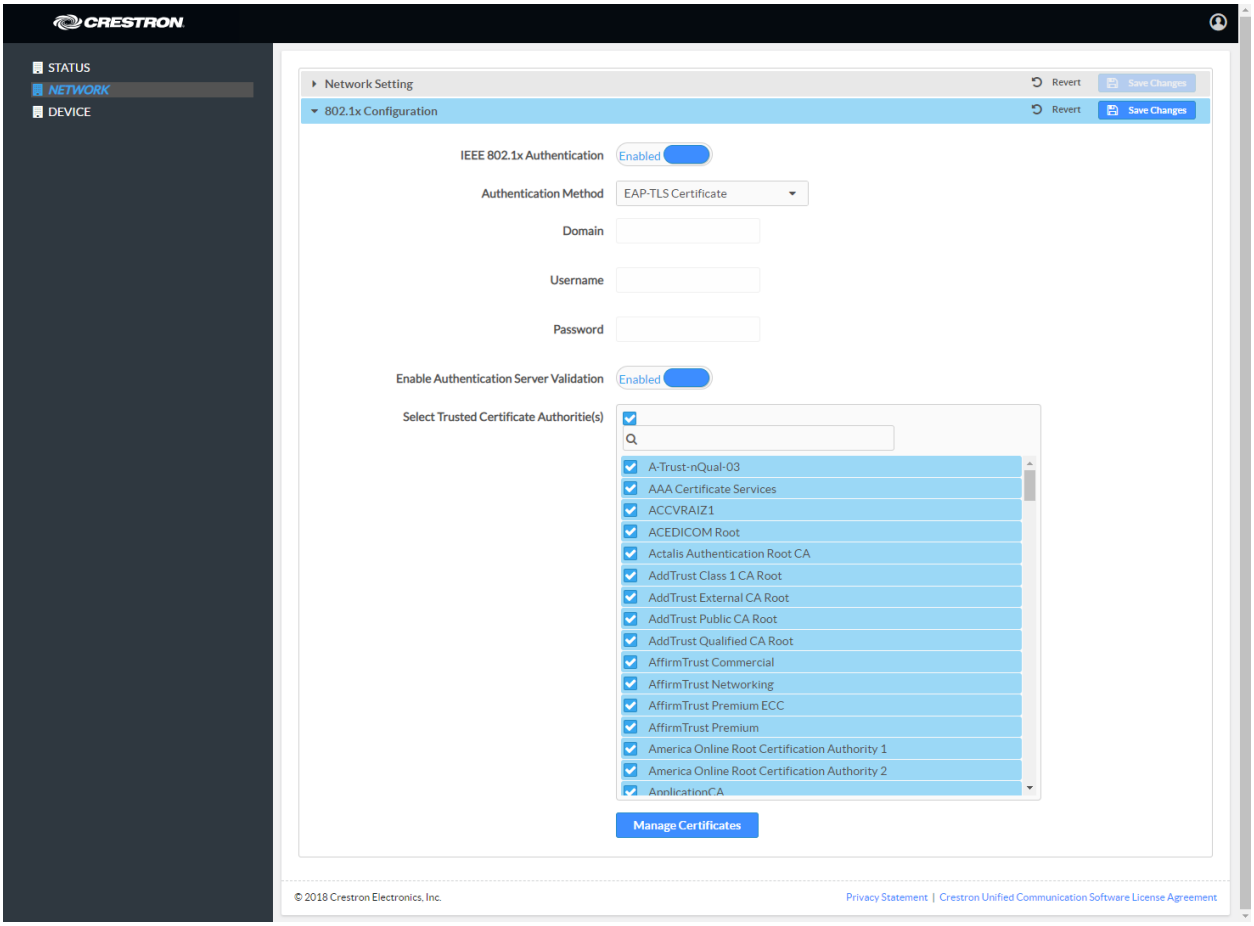
5. Click **Save Changes** when done or **Revert** to return to the previous setting.

NOTE: Any changes made to the network settings will require the device to reboot.

802.1x Configuration

Some networks require devices to use 802.1x port-based network access control for access to the network.

NETWORK Screen - 802.1x Configuration



To use 802.1x, set **IEEE 802.1x Authentication** to **Enabled** and select the desired method of authentication.

- Certificate Authentication

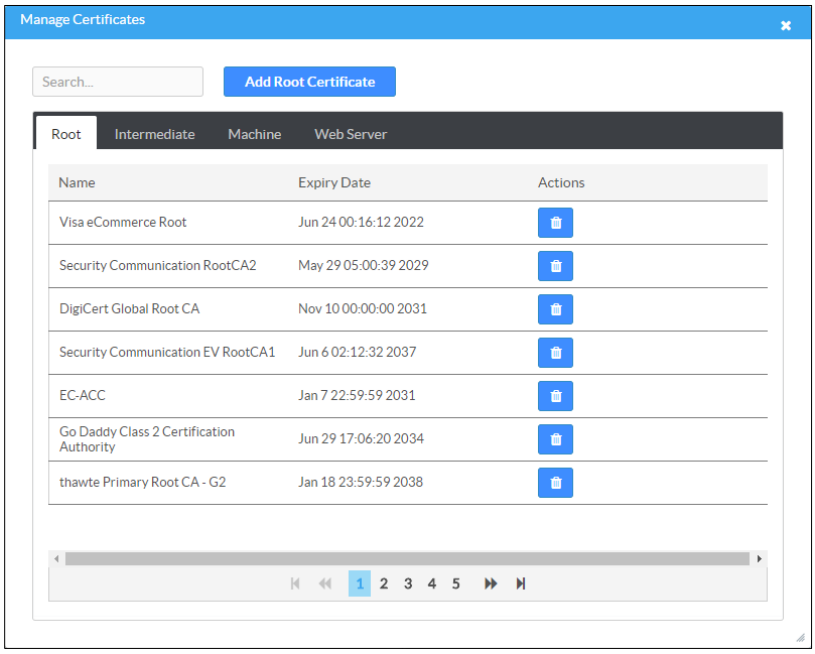
  1. In the **Authentication Method** field, select **EAP-TLS Certificate**.

  2. Enter the domain name of the authentication server.

3. Upload a machine certificate.

   a. Click **Manage Certificates** to manage certificates for 802.1x authentication. A list of certificates is displayed.

Manage Certificates Dialog Box

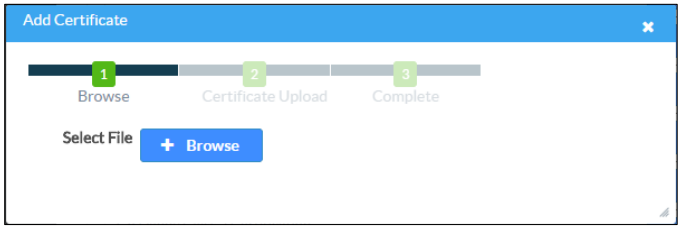


   b. Click the **Machine** tab. The current machine certificate is displayed.

   c. Click  to delete the certificate from the list of certificates.

   d. Click **Add Machine Certificate**. The Add Certificate dialog box is displayed.

Add Certificate Dialog Box



   e. Click **+ Browse**, select the certificate file, and click **Open**.

   f. When prompted, enter the password used to encrypt the file.

   g. Click **Load** to upload the certificate to the CCS-UC-1-T. A message confirming the upload is displayed.

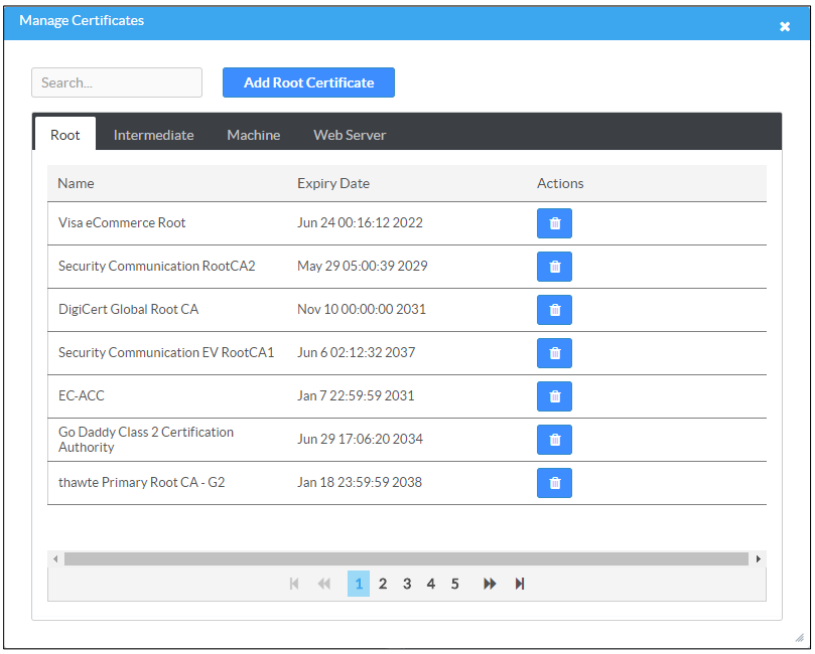
   h. Click **OK** to close the **Add Certificate** dialog box.

4. If authentication server validation is not used, set **Enable Server Validation** to **Disabled** and continue to step 6. Otherwise, set **Enable Server Validation** to **Enabled** and select the trusted certificate authorities to use.

   - To select all of the authorities, click the check box next to the search box. To unselect all of the authorities, click the check box again.
   - To search for a specific authority, start typing the name of the authority in the search box and check the box next to the desired authority.

5. Click **Manage Certificates** to manage certificates for 802.1x authentication. A list of certificates is displayed.

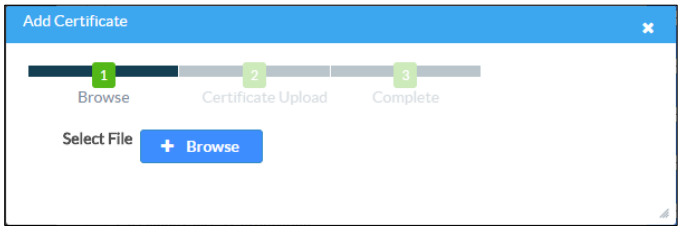
Manage Certificate Dialog Box



a. Click  to delete a certificate from the list of certificates.

b. Click **Add Root Certificate**. The Add Certificate dialog box is displayed.

Add Certificate Dialog Box



c. Click **+ Browse**, select the certificate file, and click **Open**.

d. Click **Load** to upload the certificate to the CCS-UC-1-T. A message confirming the upload is displayed.

e. Click **OK** to close the **Add Certificate** dialog box.

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

- Password Authentication

1. In the **Authentication Method** field, select **EAP-MSCHAP V2-password**.

2. Enter the domain name of the authentication server, the user name, and the password in their respective fields.

3. Set **Enable Server Validation** to **Enabled** and select the trusted certificate authorities to use.

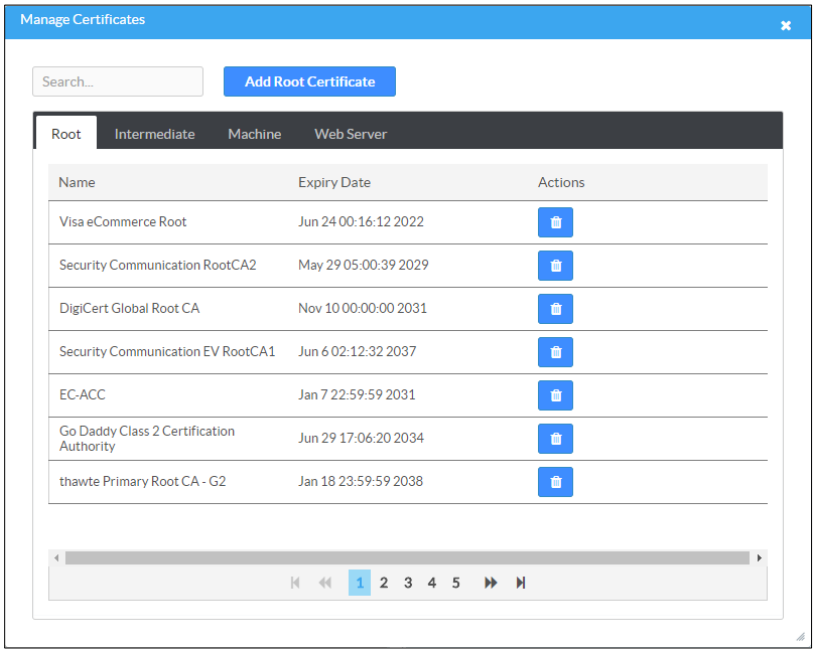
   - To select all of the authorities, click the check box next to the search box. To unselect all of the authorities, click the check box again.

   - To search for a specific authority, start typing the name of the authority in the search box and check the boxes next to the desired authorities.

4. To load a custom certificate, click **Manage Certificates** and follow this procedure:

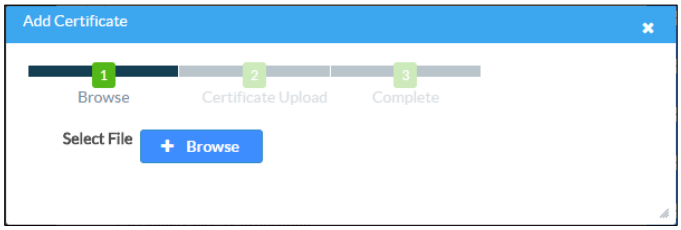
   a. Click the **Root** tab to manage certificates for 802.1x authentication.

Manage Certificates Dialog Box: Root Tab



   b. Click **Add Root Certificate**. The Add Certificate dialog box is displayed.

Add Certificate Dialog Box



c. Click **+ Browse**, select the certificate file, and click **Open**.

d. Click **Load** to upload the certificate to the CCS-UC-1-T. A message confirming the upload is displayed.

e. Click **OK** to close the **Add Certificate** dialog box.

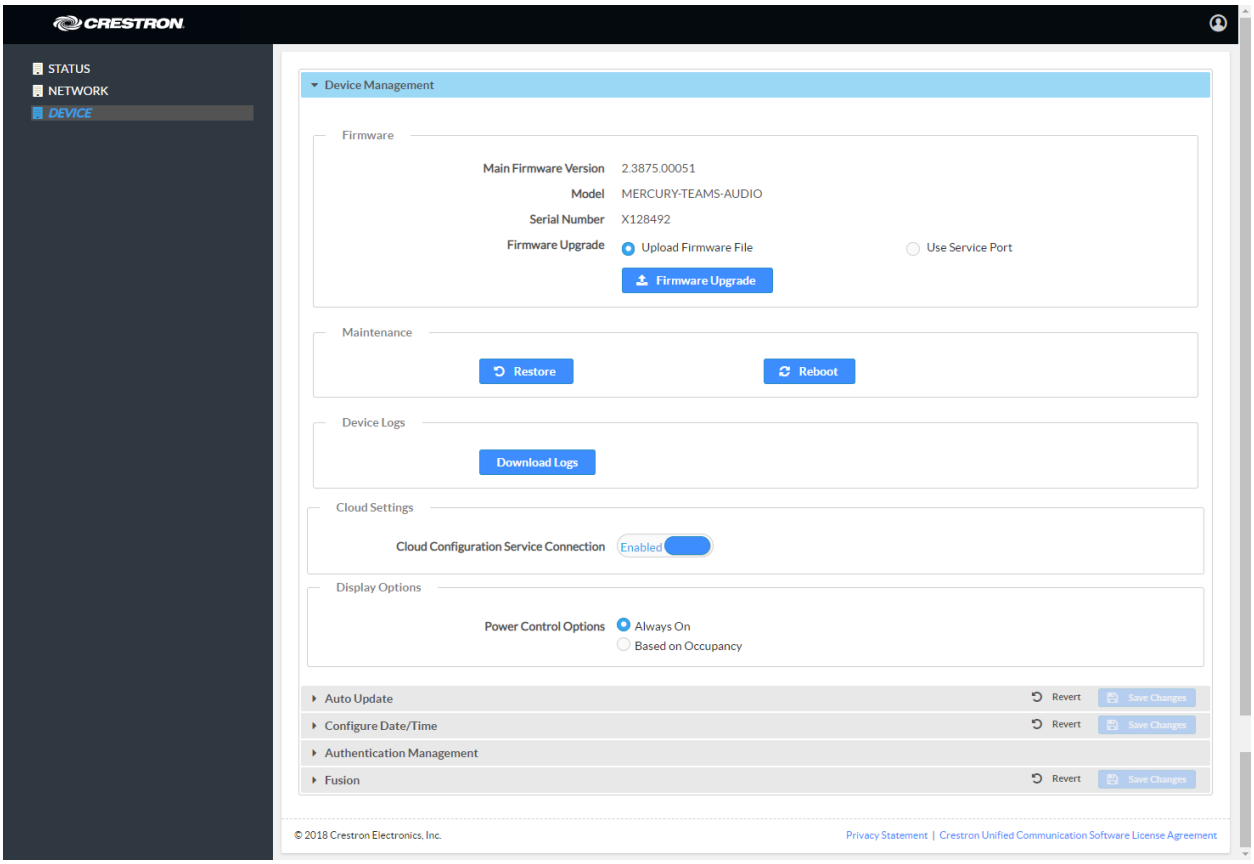
5. Click **Save Changes** when done, or **Revert** to return to the previous setting.

DEVICE

Click **DEVICE** to upload firmware, restore factory settings, download system logs, manage cloud settings, manage display settings, manage auto update settings, configure the date and time, authentication management, and configure the device for use with Crestron Fusion software.

Device Management

DEVICE Screen - Device Management



Firmware

To upload device firmware, follow this procedure:

1. Click **Firmware Upgrade**.
2. Click **+ Browse** and navigate to the location of the firmware file.
3. Select the file to use and click **Open**.
4. Click **Load** to load the firmware.

Maintenance

Click **Restore** to restore the factory settings. Click **Reboot** to reboot the device.

Device Logs

Click **Download Logs** to download the device's system logs to the PC.

Cloud Settings

By default, the **Cloud Configuration Service Connection** is set to **Enabled**. To disable the connection, set **Cloud Configuration Service Connection** to **Disabled**. For more information, refer to "Crestron XiO Cloud Service" on page 27.

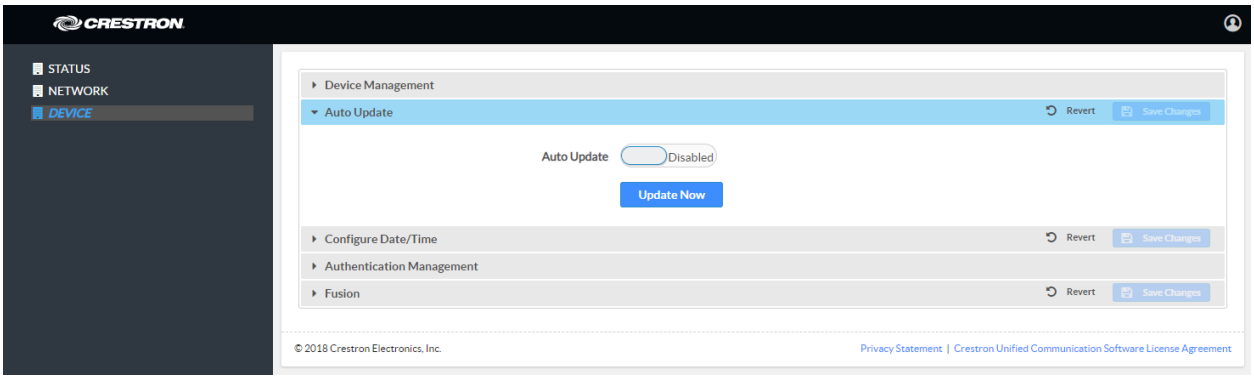
Display Options

Display Options selects when the display will be on.

- Select **Always On** to keep the display on all the time.
- Select **Based on Occupancy** to keep the display on when the built-in occupancy sensor detects that the room is occupied.

Auto Update

DEVICE Screen - Auto Update

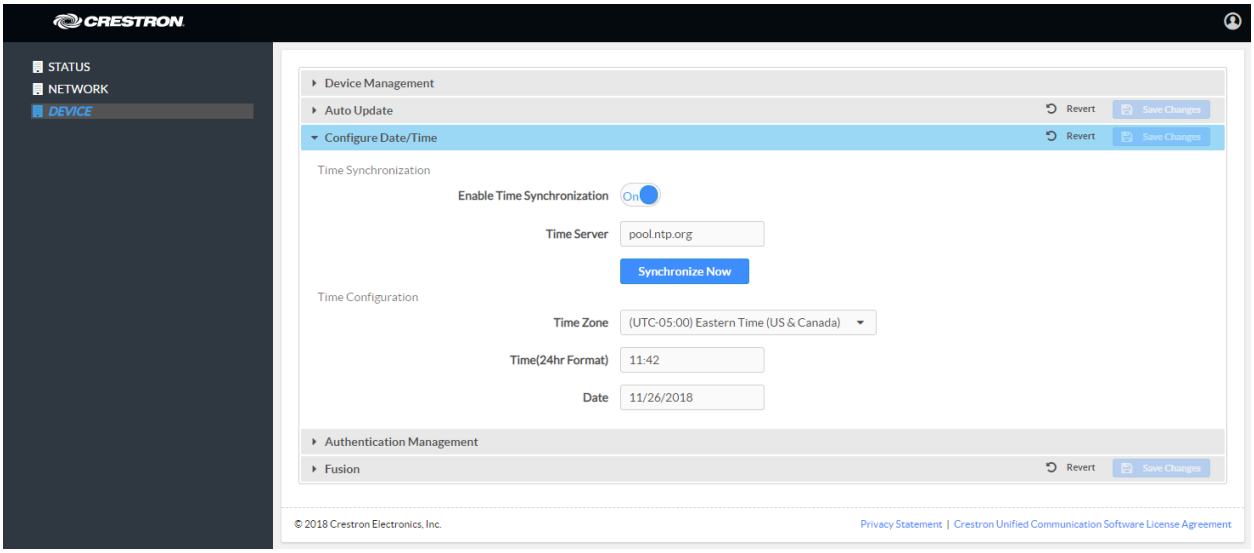


The device can automatically check for firmware updates and update as needed. To allow auto updating, set **Auto Update** to **Enabled**. To turn off auto updating, set **Auto Update** to **Disabled**.

To check for available updates, click **Update Now**.

Configure the Date and Time

DEVICE Screen - Configure Date/Time



The device's internal clock can be synchronized with a time server or set manually.

NOTE: When connected to Crestron Fusion software, the time is automatically set from Crestron Fusion. Any settings made here do not apply.

- To synchronize the clock with a time server:

  a. Set **Enable Time Synchronization** to **On**.

  b. Enter the time server's IP address or host name in the **Time Server** field.

  c. Click **Synchronize Now** to sync Crestron Mercury with the specified time server.

- Set the Time manually:

  a. Set **Enable Time Synchronization** to **Off**.

  b. Select the time zone from the **Time Zones** list.

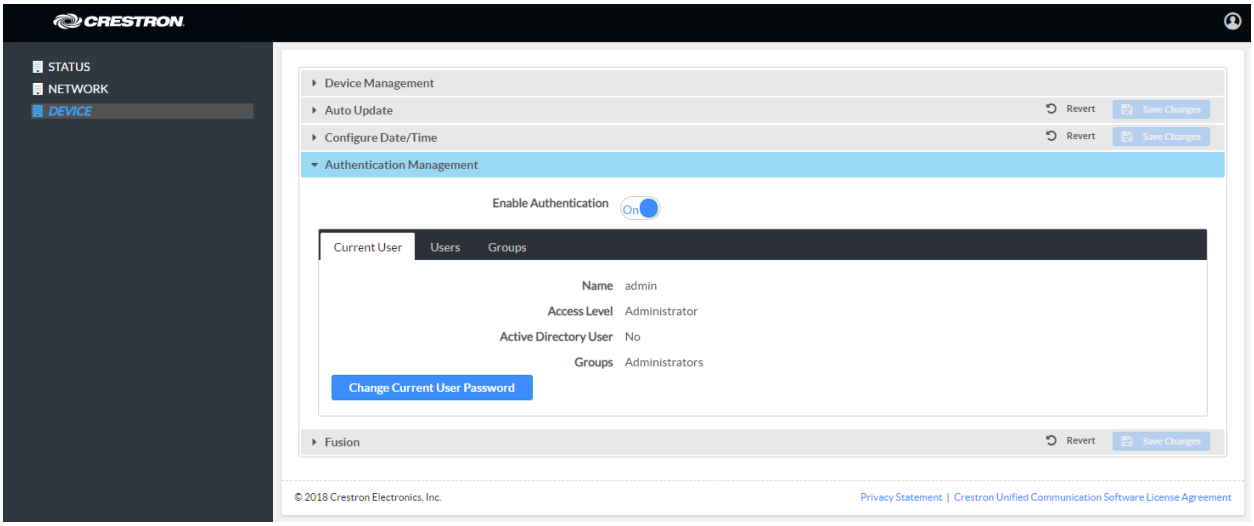
  c. Enter the time (in 24 hour format) in the **Time(24hr Format)** field.

  d. Select the date from the **Date** field.

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

Authentication Management

DEVICE Screen - Authentication Management



This section is used to set the password for the current user, and manage authorized users and user groups. By default, **Enable Authentication** is set to **On**.

- Current User

  a. Click the **Current User** tab to set the current user's password.

  b. Click **Change Current User Password** to change the current user's password.

  c. Enter the new password in the **Password** field.

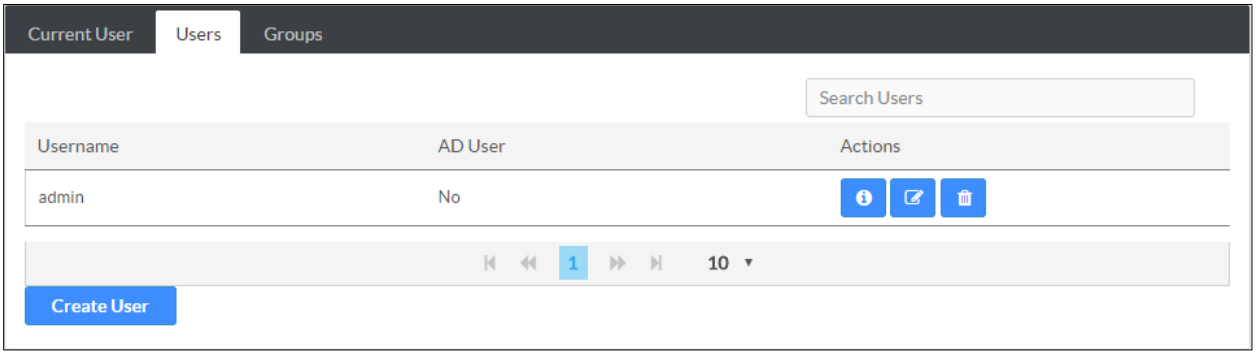
  d. Confirm the new password in the **Confirm Password** field.

  e. Click **OK** to set the new password or click **Cancel** to cancel.

- Users

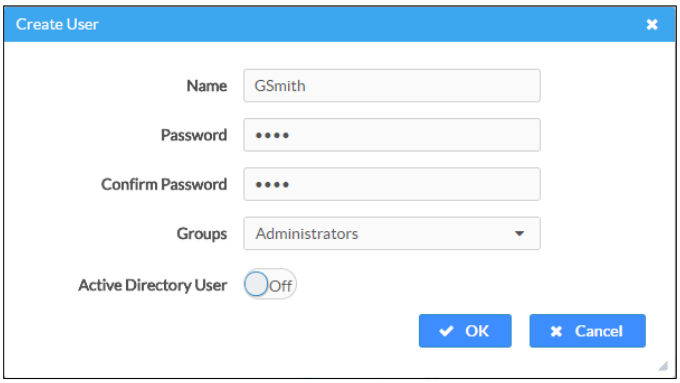
  Click the **Users** tab to manage authorized users. A list of authorized users is displayed.

DEVICE Screen - Authentication Management: Users Tab



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

Create User Dialog Box



i. Enter the user name in the **Name** field.

ii. Enter the user password in the **Password** field.

iii. Confirm the password in the **Confirm Password** field.

iv. Select the user's group memberships from the **Groups** drop-down list.

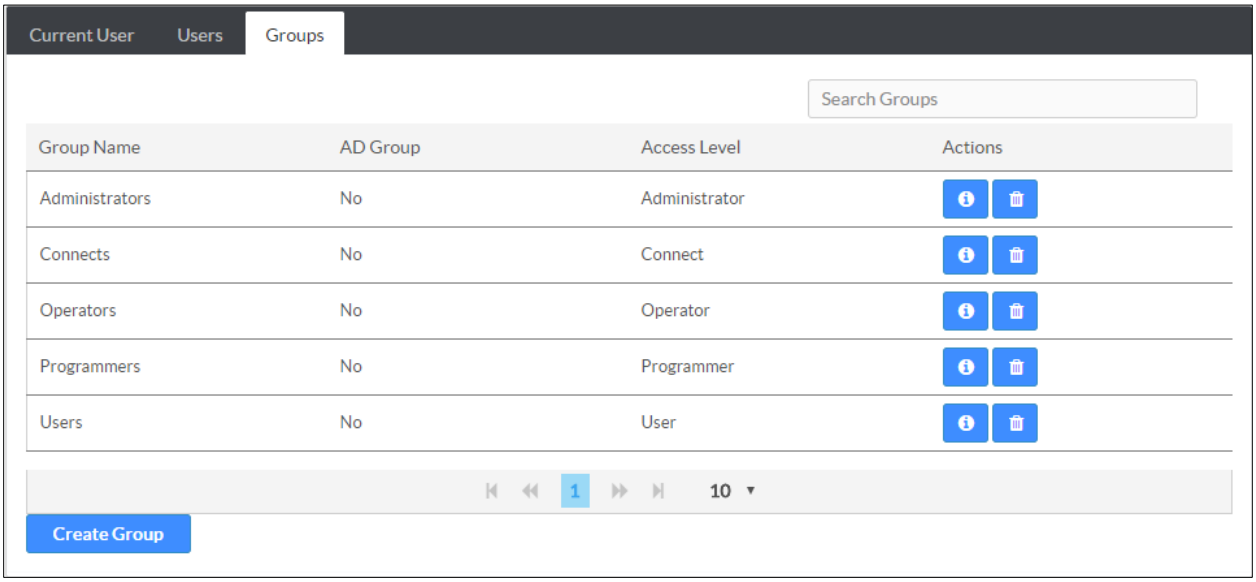
v. Select whether the user is a member of the Active Directory® credential management group with the **Active Directory Group** switch.

vi. Click **OK** to save the user or click **Cancel** to cancel.

- Groups

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

DEVICE Screen - Authentication Management: Groups Tab

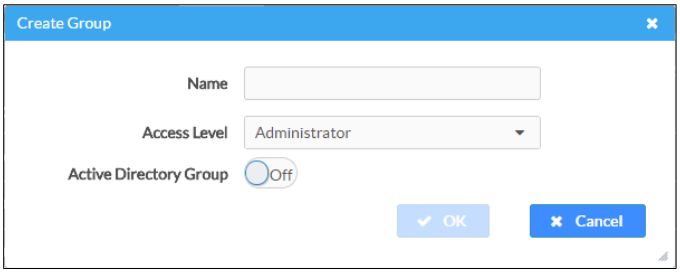


– Click  to view details about a group.

– 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.

Create Group Dialog Box



i. Enter the group name in the **Name** field.

ii. Select the group's access level from the **Access Level** drop-down list.

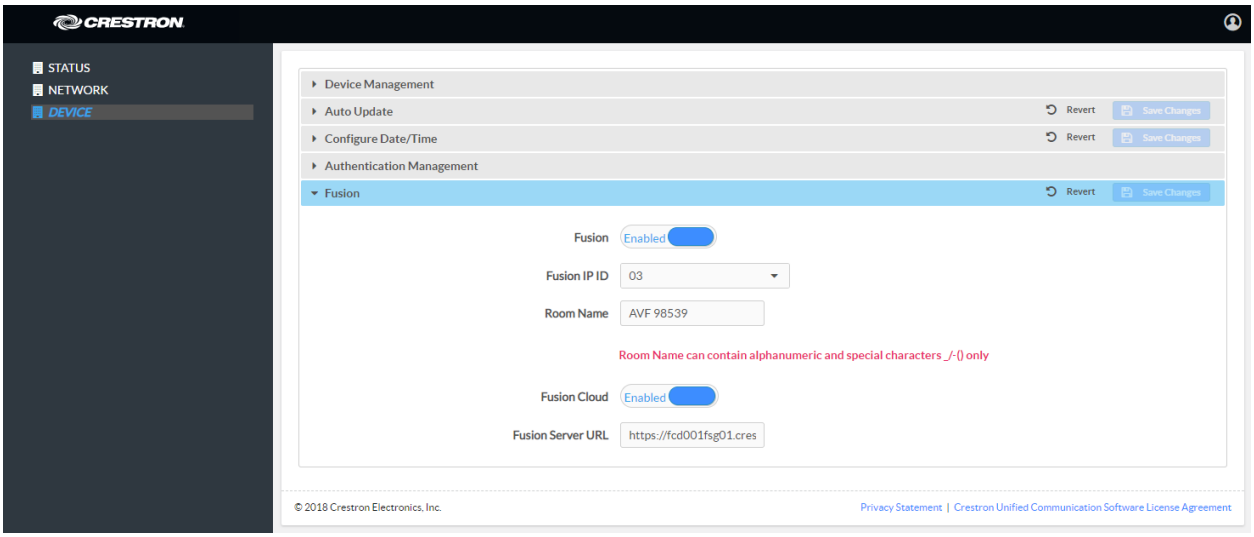
- **Administrator** grants full access to the system settings and device functions
- **Connect** grants access to the device functions
- **Operator** grants read access to the system settings and full access to the device functions
- **Programmer** grants access to program/project specific settings/ReadOnly to the rest, read/write access to the file system, no access to the setup project

- **User** grants access to the device functions

iii. Click **OK** to save the group or click **Cancel** to cancel.

Fusion

DEVICE Screen - Fusion



This section is used to configure the device to operate with Crestron Fusion software.

To configure the Crestron Fusion settings, follow this procedure:

1. To enable the device to operate with Crestron Fusion software, set **Fusion** to **Enabled**. To disable operability with Crestron Fusion software, set **Fusion** to **Disabled**.

2. In the **IPID** field, enter the IP ID number to be used by the Crestron Fusion server.

3. In the **Room Name** field, enter the name to be used by the Crestron Fusion server.

4. To allow autodiscovery by the Crestron Fusion server, set **Fusion Cloud** to **Enabled**. The **Fusion Server URL** field will be automatically populated. Otherwise, set **Fusion Cloud** to **Disabled** and manually enter the URL of the Crestron Fusion server in the **Fusion Server URL** field.

5. Click **Save Changes** to save the settings or click **Revert** to return to the previous settings.

Upon completion, the device should be brought into Crestron Fusion software as a processor. For details, refer to the Crestron Fusion help file.

Enterprise Deployment Options

Crestron has two options for deploying multiple CCS-UC-1-T devices across an enterprise. These tools can assist in deploying any number of CCS-UC-1-T devices that an organization may need to deploy.

For more information, refer to Answer ID 5719 in the Online Help on the Crestron website (www.crestron.com/onlinehelp).

Crestron XiO Cloud Service

The Crestron XiO Cloud™ service requires devices to be claimed so they can be managed by the service. To claim a single device or multiple devices, perform one of the following procedures.

Claim a Single Device

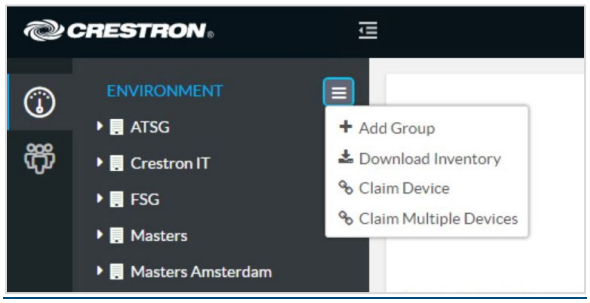
1. Record the MAC address and serial number that are labeled on the shipping box or on a sticker attached to the device. The MAC address and serial number are required to add the device to the Crestron XiO Cloud environment.

   NOTE: Use the MAC address labelled "MAC Address."

2. Open a web browser, and log in to the Crestron XiO Cloud service at https://portal.crestron.io.

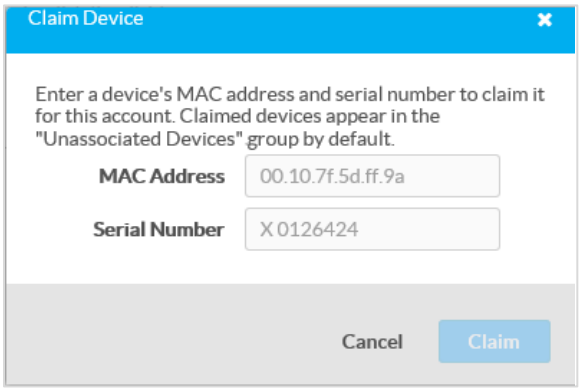
3. Click the **ENVIRONMENT** menu button ( ) to display the Environment menu.

   Environment Menu

4. Click **Claim Device**. The **Claim Device** dialog box is displayed.

Claim Device Dialog Box



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 then try again.

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 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 (Doc. 8214) 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
00.10.7e.8b.81.b6,17284712
00.10.7e.8b.8c.87,17284570
00.10.7e.96.83.93,1716JBG01207
00.10.7e.96.92.0a,1716JBG01550
00.10.7e.8b.87.c1,17284670
```

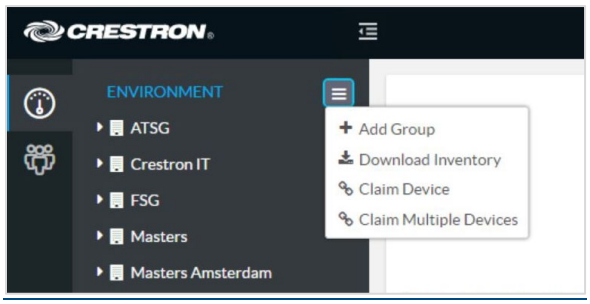
   NOTES:

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

2. Open a web browser, and log in to the Crestron XiO Cloud service at https://portal.crestron.io.

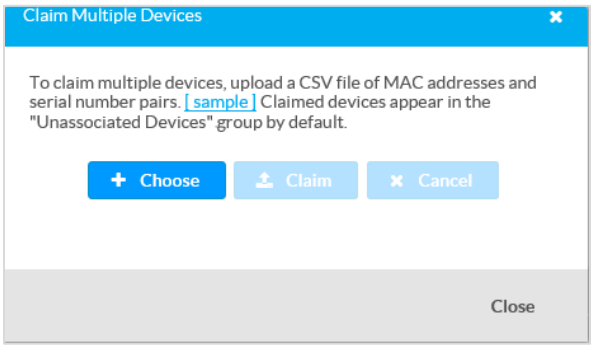
3. Click the **ENVIRONMENT** menu icon ( ) to display the Environment menu.

   Environment Menu

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

   Claim Multiple Devices Dialog Box

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** in the upper right corner 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 User Guide (Doc. 8214) at www.crestron.com/manuals.

Crestron Deployment Tool for PowerShell® Software

Crestron has developed a tool for customers without Crestron XiO Cloud service to allow deployment of multiple devices without the need to configure each device individually. With this tool, an administrator may input all the configuration settings in a single data file, and then use PowerShell® task-based command-line shell and scripting language to configure multiple devices across an enterprise.

Operation

For operational details and support on Microsoft Teams software, visit https://docs.microsoft.com/en-us/MicrosoftTeams/Microsoft-Teams#pivot=home&panel=home-all.

Troubleshooting

The following table provides troubleshooting information. If further assistance is required, contact a Crestron customer service representative.

CCS-UC-1-T Troubleshooting

TROUBLE	CAUSE	CORRECTIVE ACTION
The microphone mute LED on top of the CCS-UC-1-T is lit blue.	The CCS-UC-1-T is not receiving sufficient power for standard PoE+ (IEEE 820.3at) operation (for example, only receiving power from a standard PoE source).	Connect a PoE+ source or connect the PW-2420RU power pack (sold separately and included with the CCS-UC-1-T W/PS KIT or CCS-UC-1-T-AV W/PS KIT).
The CCS-UC-1-T displays the screen below, with the message "PoE power detected, device requires PoE+ power. Please connect a PoE+ power supply and reboot." 	The CCS-UC-1-T is not receiving sufficient power for standard PoE+ (IEEE 820.3at) operation (for example, only receiving power from a standard PoE source).	Connect a PoE+ source or connect the PW-2420RU power pack (sold separately and included with the CCS-UC-1-T W/PS KIT or CCS-UC-1-T-AV W/PS KIT).
The CCS-UC-1-T is not receiving PoE+ power from a Cisco® PoE+ switch.	The Cisco switch's Link Layer Discovery Protocol (LLDP) is disabled.	Configure the Cisco switch to enable LLDP. For example, to enable LLDP on some Cisco switches, use the following console commands: Switch# configure terminal Switch(config)# lldp run Switch(config)# end

This page is intentionally left blank.

Crestron Electronics, Inc.
15 Volvo Drive, Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7576
www.crestron.com

Supplemental Guide – DOC. 8401A
(2052763)
12.18