RMC4

4-Series™ Control System

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: RMC4

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, .AV Framework, 3-Series, 4-Series, Cresnet, Crestron Fusion, Crestron Toolbox, infiNET EX, VT Pro-e, and XiO Cloud are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Apple, HomeKit, iPad, and iPhone are either trademarks or registered trademarks of Apple, Inc. in the United States and/or other countries. Android is either a trademark or a registered trademark of Google Inc. in the United States and/or other countries. Active Directory, Azure, and Microsoft are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Python is either a trademark or a registered trademark of Python Software Foundation in the United States and/or other countries. UL is either a trademark or a registered trademark of Underwriters Laboratories, Inc. in the United States and/or other countries. Wi-Fi is either a trademark or a 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.

©2022 Crestron Electronics, Inc.

Contents

Overview 1
Features 2
4-Series Control Engine 2
Modular Programming Architecture 3
Onboard Control Ports 3
Crestron Fusion Room Monitoring and Scheduling 3
XiO Cloud Provisioning and Management 3
.AV Framework Software 4
Enhanced Enterprise-Grade Security 4
SNMP V3 Support 4
BACnet Support 4
Apple HomeKit Integration 4
PoE Network Powered 4
Integrator Friendly Enclosure 5
Physical Description 6
Specifications 8
Product Specifications 8
Dimension Drawings 11
Installation 12
Mount the Control System 12
Surface Mounting 12
DIN Rail Mounting 13
Connect the Control System 14
Configure the Control System 16
Configuration via IP Address 16
Configuration via XiO Cloud 16
Create an Admin Account 17
Set the Time Zone 17
Pair with Apple HomeKit 18
Configure .AV Framework Software 18
Configuration 19
Actions Menu 20
Save Changes 20
Revert 20
Reboot 21
Restore 21
Update Firmware 21
Download Logs 21

Manage Certificates 22
Status 22
Device 22
Network 23
Program 24
AV Framework 25
Settings 25
System Setup 26
Programs 32
Projects 36
Services 38
Cloud Settings 39
Auto Update 40
AV Framework 42
Security 43
Current User 44
Users 45
Groups 49
802.1x Configuration 52

Programming 55

Resources 56

Crestron Support and Training 56
Programmer and Developer Resources 56
Product Certificates 56
Related Documentation 56

Overview

The RMC4 is a secure, high-performance, cost-effective control processor with a powerful 4-Series™ control engine. The RMC4 is designed to integrate and automate technology within any modern networked home, commercial building, or government facility.

This section provides the following information:

- Features (on page 2)
- Physical Description (on page 6)

Features

Key features include:

- Compact 4-Series™ control system with 1 GB SDRAM and 8 GB flash memory
- Embedded 4-Series multicore CPU processor
- iPhone®, iPad®, and Android™ device control app support
- XPanel computer and web based control
- Modular programming architecture (optional)
- Onboard IR/serial, COM, digital input, relay, Cresnet® network, and Ethernet control ports
- USB OTG (On-the-Go) port
- Support for Crestron Fusion® software and XiO Cloud® service
- Native .AV Framework™ software program
- Enterprise-class network security and authentication
- SNMP V3 remote IT management support
- Native BACnet network/IP support
- Installer setup via software, web browser, or cloud
- IPv6 ready
- Integrates with Apple® HomeKit® technology
- Compact, stackable IFE micro form factor
- Surface or DIN rail mountable
- Available rack mount and pole mount options

4-Series Control Engine

4-Series™ control systems come equipped with an upgraded multicore CPU, delivering a sizable speed and performance increase compared to all Crestron 3-Series® control processors. The improved performance allows 4-Series control systems to handle the increasing demands of an advanced automated system. Crestron 4-Series delivers a dynamic and secure control system platform capable of managing a room full of disparate technologies.

Reliable networking and IP control afford seamless integration with other systems and devices, with add-on control capability using Crestron touch screens, wireless remotes, and mobile device apps. Remote management is also offered through Crestron Fusion® software and the XiO Cloud® service.

Modular Programming Architecture

The RMC4 is designed to run a single program out of the box. The optional modular programming architecture (MPA) add-on allows the RMC4 to run up to ten programs simultaneously.[1] Programmers can develop and run independent, device-specific programs, enabling each program to be optimized for a specific function and allowing for changes to be made to one program without affecting the whole system.

Onboard Control Ports

Through a full complement of onboard control ports, the RMC4 can be integrated with a wide variety of audio, video, lighting, motorized shades, thermostats, door locks, sensors, security systems, and other equipment.

- Ethernet provides an interface for connecting to the building network and controlling Crestron AV switchers, audio processors, power controllers, and other IP controllable equipment.
- Cresnet® network connectivity provides support for Crestron lighting dimmers, motorized shades, sensors, thermostats, keypads, and more.[2]
- Onboard RS-232, IR, relay, and digital input control ports enable direct integration with all types of third-party equipment.

Expanded connectivity can be provided to the RMC4 via Crestron control port expansion modules, Ethernet to Cresnet bridges, wired Ethernet I/O extenders, or Wi-Fi® network I/O extenders (all sold separately).

Crestron Fusion Room Monitoring and Scheduling

Crestron Fusion provides an integrated platform for creating smart buildings that save energy and enhance worker productivity. As part of a complete managed network in a corporate enterprise, college campus, convention center, or any other facility, the RMC4 works with Crestron Fusion to enable remote scheduling, monitoring, and control of rooms and technology from a central help desk or mobile app. It also enables organizations to reduce energy consumption by tracking real-time usage and automating control of AV, lighting, shades, and HVAC. For more information about Crestron Fusion, visit www.crestron.com/fusion.

XiO Cloud Provisioning and Management

4-Series control systems leverage the power and flexibility of XiO Cloud services, enabling users to remotely provision, monitor, and manage Crestron devices across an enterprise network. XiO Cloud can be used to configure and load programs to the control system before it is received, making the control system fully functional as soon as it is connected to the network. XiO Cloud is built on the Microsoft® Azure® software platform and utilizes Microsoft's industry leading Azure IoT Hub technology. XiO Cloud enables installers and IT managers to deploy and manage thousands of devices in the time it previously took to manage just one. Unlike other virtual machine based cloud solutions, Azure services provide unlimited scalability to suit the ever growing needs of an enterprise. For more information, visit www.crestron.com/xiocloud.

.AV Framework Software

The RMC4 provides native support for the .AV Framework™ software program. .AV Framework software is a web-based management solution that is used to deploy scalable Crestron® enterprise room solutions without requiring any programming. For more information on the capabilities supported by .AV Framework, visit www.crestron.com/avframework.

Enhanced Enterprise-Grade Security

The RMC4 is an enterprise-class control processor that can be deployed across hundreds of spaces and set up using a web browser, Crestron Toolbox™ software, or XiO Cloud. It employs standard network security protocols, including 802.1X network access control, Active Directory® service authentication, SSH, TLS, and HTTPS to ensure reliability and compliance with your organization's IT policies.

The RMC4 is configured to meet Crestron's enhanced security standards right out of the box. The RMC4 ships with authentication enabled and requires that an administrator account be created before access is granted to device configuration and control interfaces.

SNMP V3 Support

Built-in SNMP V3 support enables integration with third-party IT management software, allowing network administrators to manage and control Crestron systems on the network in an IT-friendly format.

BACnet Support

Native support for the BACnet communication protocol provides a direct interface to third-party building management systems over Ethernet, simplifying integration with HVAC, security, and other systems. Using BACnet, each system runs independently but communicates together on one platform.[1]

Apple HomeKit Integration

The RMC4 supports integration with an Apple® HomeKit® technology system. Once the RMC4 is paired with a HomeKit system via SIMPL programming, a Crestron TSR-310 can be used to control supported Apple devices. A pairing QR code is affixed to the RMC4 that makes it easy to pair the control system directly to the Apple Home app.[2]

PoE Network Powered

Using PoE technology, the RMC4 gets its operating power directly through the LAN wiring, eliminating the need for a local power supply or dedicated power wiring. A PoE injector (PWE-4803RU) simply connects in line with the LAN cable at a convenient location. Crestron PoE switches (CEN-SW-POE-5 or CEN-SWPOE-16) may also be used to provide a total networking solution with built-in PoE. All PoE injectors and switches are sold separately.

Integrator Friendly Enclosure

The RMC4 features the Crestron IFE form factor, a compact Integrator Friendly Enclosure design that fits almost anywhere and enables a variety of installation options. Its shape allows the RMC4 and other IFE compliant devices to be stacked together. Using the included mounting bracket, it can be fastened to a flat surface or snapped onto a standard DIN rail. Rack mount and pole mount kits are also available (sold separately).

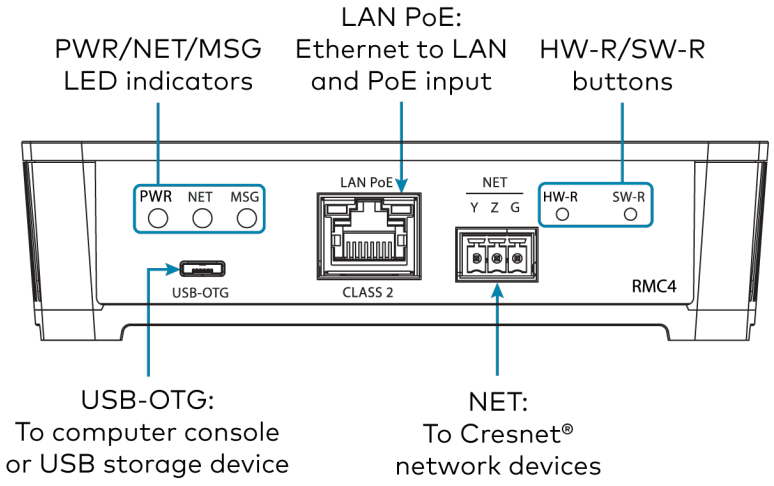
Notes:

1. Enabling Modular Programming Architecture (MPA) on the RMC4 requires the purchase of one SW-RMC3-10PROG license. The license enables support for running up to 10 simultaneous programs on a single RMC4. The license is not required if only one program is run on the RMC4. To obtain a license for the RMC4, complete the "Request for SW-RMC3-10PROG License" form. For questions, contact license@crestron.com.
2. The NET (Cresnet) port on the RMC4 is a 3-pin connector which provides connectivity (and not power) for Cresnet data only. The Cresnet power conductor does not terminate to the RMC4. An external Cresnet power supply is required to provide power for Cresnet devices.
3. A BACnet and IP license is required. A free license is available to support up to 50 BACnet objects on a single 4-Series control system. Enabling support for more than 50 BACnet objects requires the purchase of one SW-3SERIES-BACNET-50+ license. The RMC4 supports a maximum of 500 BACnet objects when dedicated for BACnet use only. Actual capabilities are contingent upon the overall program size and complexity. To obtain the license, visit www.crestron.com/bacnetlicense.
4. This feature is only available when using the TSR-310. Other Crestron touch screens, handheld remotes, and keypads are not supported. For these interfaces, traditional IR or CEC control must be used to control supported Apple devices.

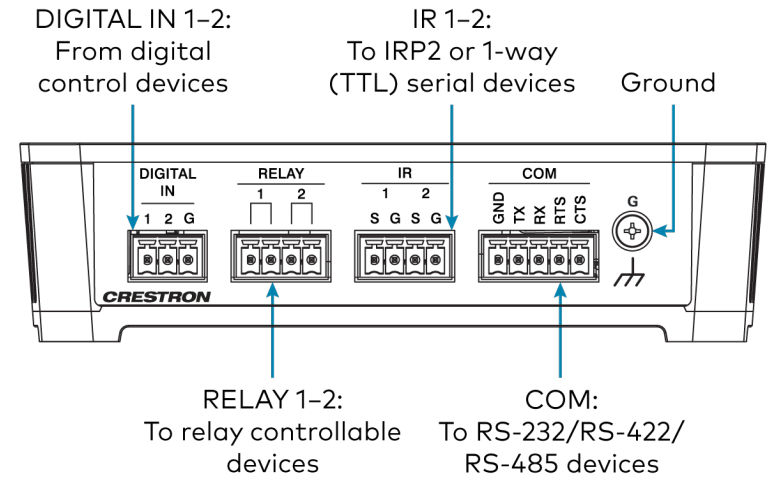
Physical Description

The RMC4 provides the following connectors and indicators.

RMC4 Front Panel



RMC4 Rear Panel



Connectors

USB-OTG	(1) USB Type Micro-AB female; USB OTG port for computer console and USB mass storage devices
LAN PoE	(1) 8-pin RJ-45 connector, female; 100BASE-T Ethernet port; PoE (Power over Ethernet) PD (Powered Device) port
NET	(1) 3-pin 3.5 mm detachable terminal block; Cresnet master port; Provides data only (no power)

DIGITAL IN 1–2	(1) 3-pin 3.5 mm detachable terminal block; Comprises (2) digital inputs (referenced to GND); Voltage Range: Rated for 0–24VDC; Input Impedance: 2.2k Ω pulled up to 5V; Logic Threshold: >2.0V low/0 and <1.1V high/1
RELAY 1–2	(1) 4-pin 3.5 mm detachable terminal block; Comprises (2) normally open, isolated relays; Rated 1A, 30VAC/VDC; MOV arc suppression across contacts
IR 1–2	(1) 4-pin 3.5 mm detachable terminal block; Comprises (2) IR output ports; IR output up to 1.2 MHz; 1-way serial TTL/RS-232 (0–5V) up to 115.2k baud; IRP2 IR emitters sold separately
COM	(1) 5-pin 3.5 mm detachable terminal block; Bidirectional RS-232/422/485 port; Up to 115.2k baud; Hardware and software handshaking support
G	(1) 6-32 screw; Chassis ground lug

Controls and Indicators

PWR	(1) Bicolor green/amber LED, indicates operating power is present; Amber indicates that the device is booting and is not yet ready to operate; Green indicates that the device is ready to operate
NET	(1) Amber LED, indicates communication with Cresnet devices
MSG	(1) Red LED, indicates control processor has generated an error message
HW-R	(1) Recessed push button, initiates hardware reset
SW-R	(1) Recessed push button, initiates software reset
LAN PoE	(1) Green and (1) Amber LEDs; Green LED indicates Ethernet link status and connection speed; Amber LED indicates Ethernet activity

Specifications

Product specifications for the RMC4 are provided below.

Product Specifications

Control Engine

Crestron® 4-Series™; real-time, preemptive multi-threaded/multitasking kernel; Transaction-Safe Extended FAT file system; supports up to 10 simultaneously running programs (license required[1]), native .AV Framework™ software program

Communications

Ethernet	100 Mbps, auto-switching, auto-negotiating, auto-discovery, full/half duplex, industry-standard TCP/IP stack, UDP/IP, CIP, DHCP, SSL, TLS, SSH, SFTP (SSH File Transfer Protocol), FIPS 140-2 compliant encryption, IEEE 802.1X, SNMP, BACnet and IP[3], IPv4 or IPv6, Active Directory® service authentication, HTTPS web server, HTTPS web browser setup and XiO Cloud® client, SMTP email client
Cresnet® Network	Cresnet master mode
USB	Supports computer console and USB mass storage class devices via the front panel USB OTG (On-the-Go) device port
RS-232/422/485	For 2-way device control and monitoring, supports RS-232, RS-422, or RS-485 up to 115.2k baud with hardware and software handshaking
IR/Serial	Supports 1-way device control via infrared up to 1.2 MHz or serial TTL/RS-232 (0–5V) up to 115.2k baud

Memory

SDRAM	1 GB
Flash	8 GB
External Storage	Supports USB storage devices up to 1 TB

Connectors

USB-OTG	(1) USB Type Micro-AB female; USB OTG port for computer console and USB mass storage devices
LAN PoE	(1) 8-pin RJ-45 connector, female; 100BASE-T Ethernet port; PoE (Power over Ethernet) PD (Powered Device) port
NET	(1) 3-pin 3.5 mm detachable terminal block; Cresnet master port; Provides data only (no power)[2]

DIGITAL IN 1–2	(1) 3-pin 3.5 mm detachable terminal block; Comprises (2) digital inputs (referenced to GND); Voltage Range: Rated for 0–24VDC; Input Impedance: 2.2k Ω pulled up to 5V; Logic Threshold: >2.0V low/0 and <1.1V high/1
RELAY 1–2	(1) 4-pin 3.5 mm detachable terminal block; Comprises (2) normally open, isolated relays; Rated 1A, 30VAC/VDC; MOV arc suppression across contacts
IR 1–2	(1) 4-pin 3.5 mm detachable terminal block; Comprises (2) IR output ports; IR output up to 1.2 MHz; 1-way serial TTL/RS-232 (0–5V) up to 115.2k baud; IRP2 IR emitters sold separately
COM	(1) 5-pin 3.5 mm detachable terminal block; Bidirectional RS-232/422/485 port; Up to 115.2k baud; Hardware and software handshaking support
G	(1) 6-32 screw; Chassis ground lug

Controls and Indicators

PWR	(1) Bicolor green/amber LED, indicates operating power is present; Amber indicates that the device is booting and is not yet ready to operate; Green indicates that the device is ready to operate
NET	(1) Amber LED, indicates communication with Cresnet devices
MSG	(1) Red LED, indicates control processor has generated an error message
HW-R	(1) Recessed push button, initiates hardware reset
SW-R	(1) Recessed push button, initiates software reset
LAN PoE	(1) Green and (1) Amber LEDs; Green LED indicates Ethernet link status and connection speed; Amber LED indicates Ethernet activity

Power

Power over Ethernet	IEEE 802.3at Type 1 (802.3af compatible) Class 0 (12.95 W) PoE Powered Device
Power Consumption	6.5 W

> **NOTE:** The RMC4 does not use or supply any Cresnet power.

Environmental

Temperature	32 to 104°F (0 to 40°C)
Humidity	10% to 90% RH (noncondensing)
Heat Dissipation	22 BTU/hr

Construction

Enclosure	IFE micro form factor, black and blue plastic
Mounting	Freestanding, stackable, surface mount, or 35 mm DIN EN 60715 rail mount; Occupies 8 DIN module spaces (144 mm); Surface/DIN rail mounting bracket included, optional rack mount and pole kits sold separately

Dimensions

Height	1.35 in. (34 mm); 1.77 in. (45 mm) with bracket
Width	5.04 in. (128 mm); 5.36 in. (136 mm) with bracket
Depth	2.86 in. (73 mm); 3.33 in. (85 mm) with bracket

Weight

6.4 oz (180 g)

Compliance

Regulatory Model: RMC4;
UL® Listed for US & Canada, CE, IC, FCC Part 15 Class B digital device

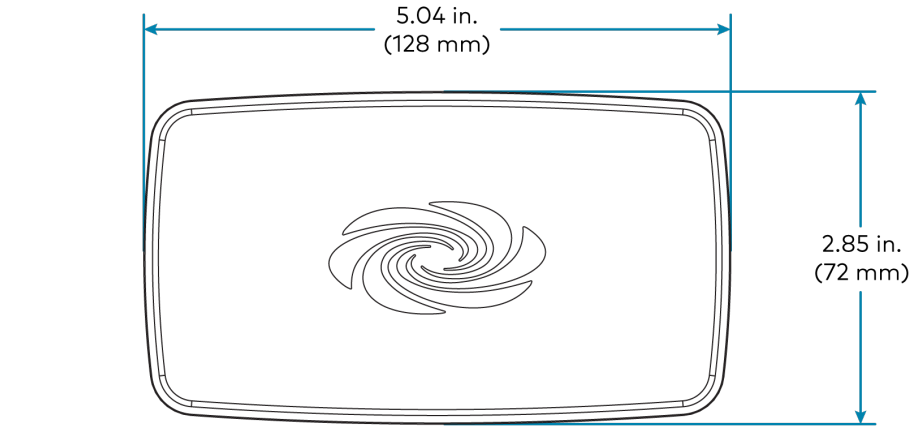
Notes:

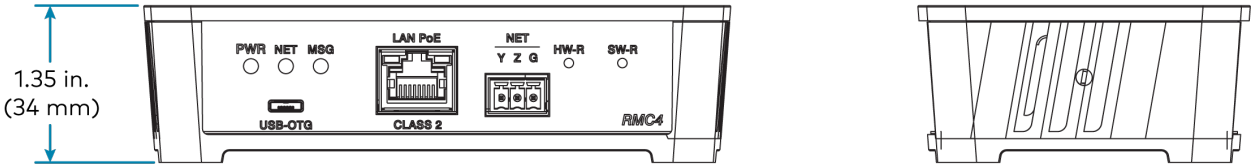
1. Enabling Modular Programming Architecture (MPA) on the RMC4 requires the purchase of one SW-RMC3-10PROG license. The license enables support for running up to 10 simultaneous programs on a single RMC4. The license is not required if only one program is run on the RMC4. To obtain a license for the RMC4, complete the "Request for SW-RMC3-10PROG License" form. For questions, contact license@crestron.com.
2. The NET (Cresnet) port on the RMC4 is a 3-pin connector which provides connectivity (and not power) for Cresnet data only. The Cresnet power conductor does not terminate to the RMC4. An external Cresnet power supply is required to provide power for Cresnet devices.
3. A BACnet and IP license is required. A free license is available to support up to 50 BACnet objects on a single 4-Series control system. Enabling support for more than 50 BACnet objects requires the purchase of one SW-3SERIES-BACNET-50+ license. The RMC4 supports a maximum of 500 BACnet objects when dedicated for BACnet use only. Actual capabilities are contingent upon the overall program size and complexity. To obtain the license, visit www.crestron.com/bacnetlicense.

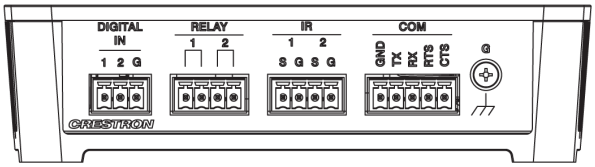
4. This feature is only available when using the TSR-310. Other Crestron touch screens, handheld remotes, and keypads are not supported. For these interfaces, traditional IR or CEC control must be used to control supported Apple devices.

Dimension Drawings

Add dimension drawings.







Installation

Use the following procedures to install the RMC4 control system.

Mount the Control System

The RMC4 can be mounted onto a flat surface or a standard DIN rail using the included mounting bracket.

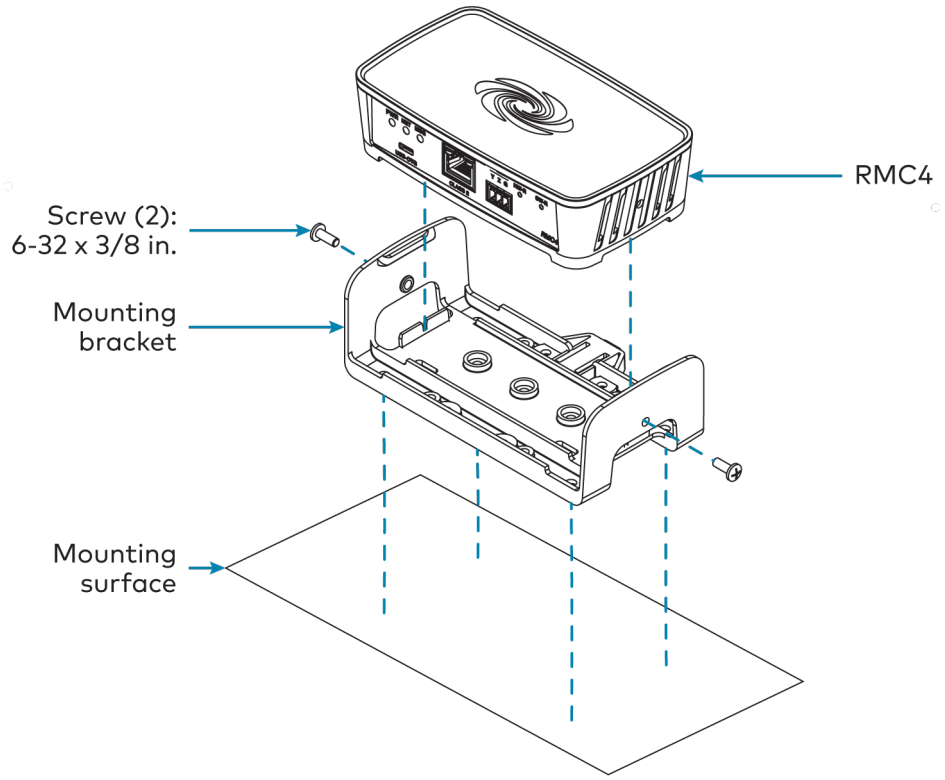
> **CAUTION:** To prevent overheating, do not operate the RMC4 in an area that exceeds the environmental temperature range (32 to 104°F or 0 to 40°C) for this device.

Optional rack mount and pole mount kits (not included) are also available for use with the RMC4. For more information, refer to the RMK-IFE-1U Installation Guide and the PLMK-IFE-101 Installation Guide.

Surface Mounting

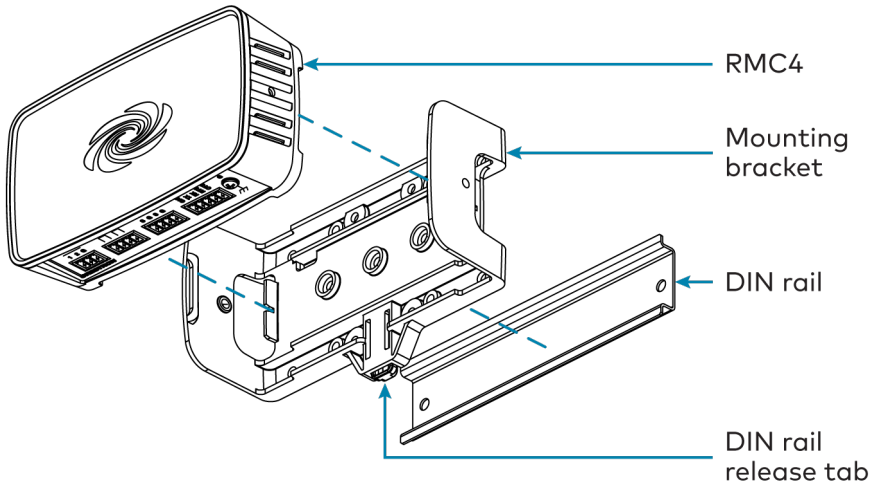
1. Detach the RMC4 from the mounting bracket by pulling the left and right flanges of the bracket outward to release the tabs that hold the RMC4 in place.
2. Attach the mounting bracket to the surface by using four appropriate mounting screws (not included) through the four mounting holes on the bottom of the bracket.
3. Align the slots on the bottom of the RMC4 with the tabs on the mounting bracket.
4. Press the RMC4 into the bracket until it snaps into place.

5. (Optional) Secure the RMC4 to the bracket using the two included 6-32 x 3/8 in. screws as shown in the following illustration.



DIN Rail Mounting

1. Detach the RMC4 from the mounting bracket by pulling the left and right flanges of the bracket outward to release the tabs that hold the RMC4 in place.
2. Pull the DIN rail release tab downward using a flat-head screwdriver.
3. Position the DIN rail mounting tabs (located on the rear of the bracket) over the top edge of the DIN rail.
4. Push the DIN rail release tab upward to lock the mounting bracket onto the rail.
5. Align the slots on the bottom of the RMC4 with the tabs on the mounting bracket.
6. Press the RMC4 into the bracket until it snaps into place.

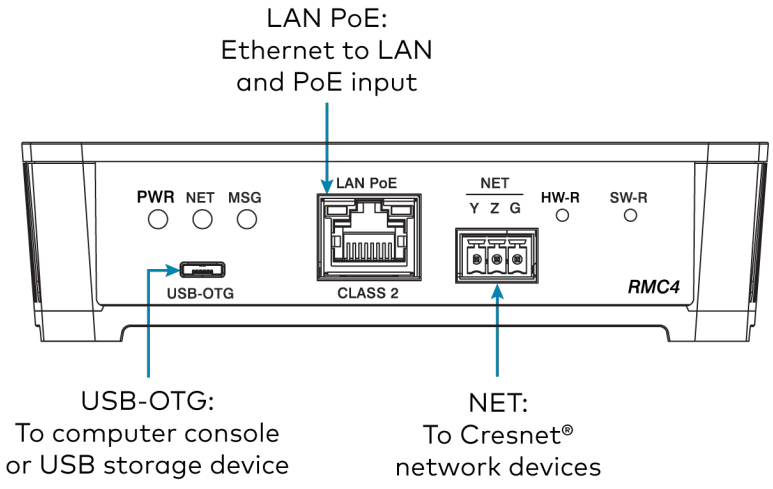


NOTE: Do not use the included screws to secure the bracket to the bottom of the RMC4 when mounting into a DIN rail, as it will then not be possible to remove the RMC4 from the DIN rail.

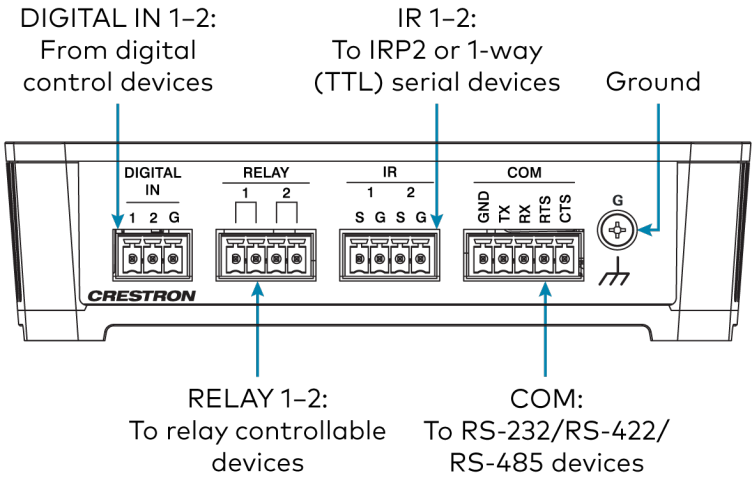
Connect the Control System

Make all device connections as shown in the following illustrations.

Front Panel Connections



Rear Panel Connections



Observe the following when connecting the RMC4:

- Power is provided to the RMC4 by a single Ethernet cable. A Crestron PoE (Power over Ethernet) power supply, such as the PWE-4803RU, or a PoE-capable network switch is recommended (both not included).
- Connect the chassis ground lug to a known earth ground circuit (for example, building steel) to ensure that the RMC4 is grounded properly.
- Apply power after all connections have been made.

COM 1 Connections

Port	RS-232	RS-422[1]	RS-485
G	GND	GND	GND[2]
TX	TX (from RMC4)	TX- (from RMC4)	TX-/RX-
RX	RX (to RMC4)	RX+ (from RMC4)	Not used
RTS	RTS (from RMC4)	TX+ (from RMC4)	TX+/RX+
CTS	CTS (to RMC4)	RX- (to RMC4)	Not used

1. RS-422 transmit and receive are balanced signals that require two lines plus a ground in each direction. RXD+ and TXD+ should idle high (going low at start of data transmission). RXD- and TXD- should idle low (going high at start of data transmission). If necessary, RXD+/RXD- and TXD+/TXD- may be swapped to maintain correct signal levels.
2. A ground terminal connection is recommended but not required.

Configure the Control System

The control system may be configured using the provided web configuration interface. The interface can be accessed using the control system IP address or the XiO Cloud® service.

Configuration via IP Address

To access the web configuration interface using the control system IP address:

> **NOTE:** The control system ships with DHCP enabled. A DHCP server is required to access the web configuration interface via the control system IP address.

1. Connect the control system to the network.
2. Use the Device Discovery tool in Crestron Toolbox™ software to discover the control system and its IP address on the network.
3. Enter the control system IP address into a web browser.

Configuration via XiO Cloud

The XiO Cloud® service allows supported devices across an enterprise to be managed and configured from one central and secure location in the cloud. Supported Crestron® devices are configured to connect to the service out of the box.

Use of the service requires a registered XiO Cloud account. To register for an XiO Cloud account, refer to www.crestron.com/Support/Tools/Licensing-Registration/XiO-Cloud-Registration-Room-Licenses.

> **NOTE:** The device may be disconnected from the XiO Cloud service by navigating to the **Cloud Services** tab in Crestron Toolbox™ software (**Functions** > **Device Info** > **Cloud Services**). For details, refer to the Crestron Toolbox help file.

To connect the device to the XiO Cloud service:

1. Record the MAC address and serial number that are labeled on the shipping box or the device. The MAC address and serial number are required to add the device to the XiO Cloud service.

   > **NOTE:** If the device has multiple MAC addresses, use the MAC address that is providing the primary connection back to the network. For most devices, the Ethernet MAC address should be used. However, if your device is connecting to the network over a different protocol (such as Wi-Fi® communications), use the MAC address for that protocol instead.

2. Log in to your XiO Cloud account at portal.crestron.io.
3. Claim the device to the XiO Cloud service as described in the XiO Cloud User Guide.

Select the device from the cloud interface to view its status and settings. The device may now also be managed and assigned to a group or room. For more information, refer to the XiO Cloud User Guide.

> **NOTE:** For XiO Cloud accounts with room-based licenses, the device must be added to a licensed room before its status and settings can be viewed.

Create an Admin Account

The first time the web configuration interface is accessed, a page is displayed asking the user to create an admin account. A similar message is displayed when connecting to the control system in Crestron Toolbox software if an admin account has not already been created.

To create an admin account:

1. Enter a username and password for the admin account in the appropriate text fields.

   > **CAUTION:** Do not lose the username and password for the admin account, as the control system must be reset to factory settings to regain access.

2. Click **OK** to create the admin account. The web configuration interface refreshes to show the standard login page.
3. Reenter the credentials created in step 1 and click **Sign In**.

   > **NOTE:** The username and password must also be entered when connecting from Crestron Toolbox or XPanel.

Set the Time Zone

The time zone must be set on the control system to ensure that the correct time settings are pushed to controlled devices.

To set the time zone:

1. Access the web configuration interface using either the device IP address or the Crestron XiO Cloud service.
2. Navigate to **Settings** > **System Setup**.
3. Select the time zone where the control system is used from the **Time Zone** drop-down menu.
4. Click **Save Changes** on the top right of the screen.

Pair with Apple HomeKit

The control system can be paired with Apple® HomeKit® technology to enable communication between the control system and Apple HomeKit devices and accessories.

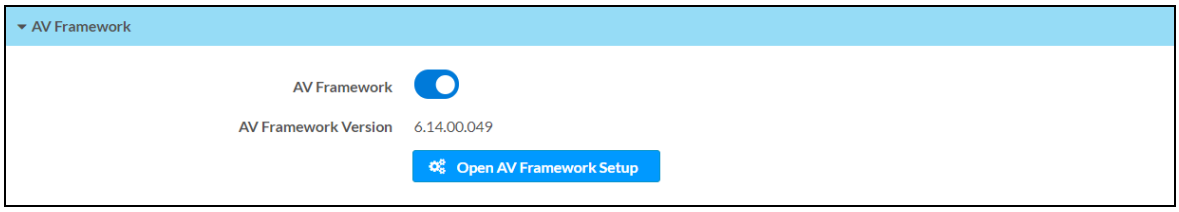
For pairing instructions and to locate the unique QR code required for pairing, refer to the RMC4 Product Information document (Doc. 8541) that shipped with the control system.

Configure .AV Framework Software

The control system provides native support for the .AV Framework™ software program. .AV Framework software is a web-based management solution that is used to deploy scalable Crestron® enterprise room solutions without requiring any programming. For more information on the capabilities supported by .AV Framework, visit www.crestron.com/avframework.

To turn on the .AV Framework software program for the control system:

1. Open the web configuration interface as described in Configure the Control System (on page 16).
2. Navigate to **Settings** > **AV Framework**.



3. Turn on the **AV Framework** toggle.
4. Save the configuration. The control system will reboot with the native .AV Framework software program turned on.

After the control system reboots, click **Open AV Framework Setup** to launch the .AV Framework web configuration utility. For more information on configuring .AV Framework for the control system, refer to the .AV Framework Software for 4-Series Control Systems Operations Guide.

Configuration

Prior to configuration, ensure the device is running the latest firmware. To update the firmware, refer to Update Firmware (on page 21)**.**

The control system may be monitored and configured using the included web configuration interface. The configuration interface is accessible from a web browser if the control system IP address is known.

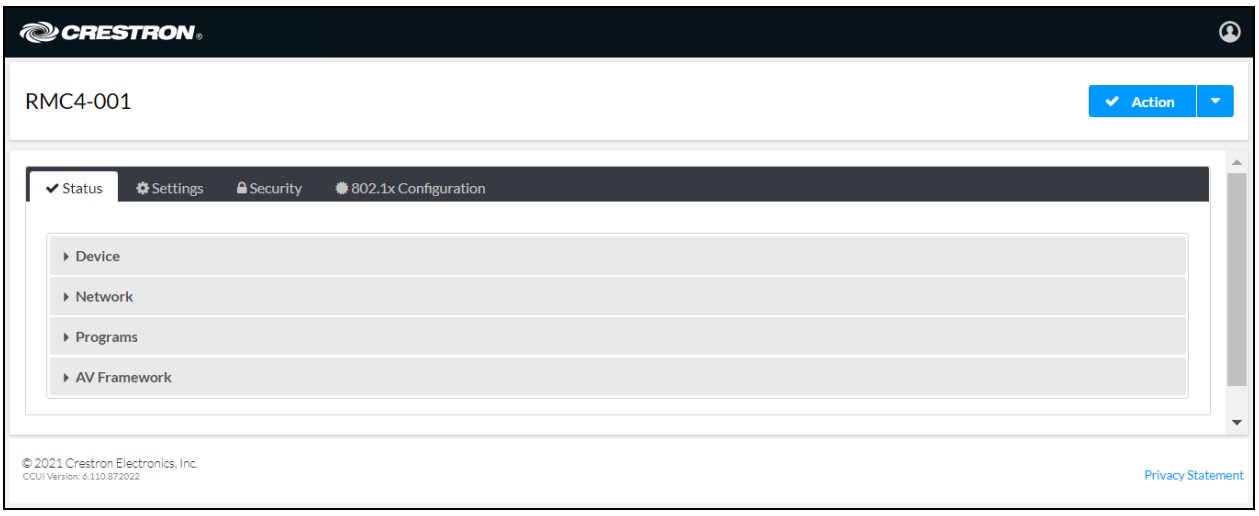
The web configuration interface is also accessible through the XiO Cloud® service. For more information, refer to Connect to XiO Cloud Service.

To access the configuration interface:

1. Use the Device Discovery tool in Crestron Toolbox™ software to discover the control system and its IP address on the network.
2. Open a web browser.
3. Enter the control system IP address into the browser URL field. A login page is displayed.
4. Enter the administrator username and password in the appropriate text fields and select **Sign In**. The configuration interface is displayed.

> **NOTE:** For more information on creating an administrator account, refer to Installation (on page 12). For more information on managing user accounts on the control system, refer to Security (on page 43).

Web Configuration Interface



The configuration interface provides the following tabs:

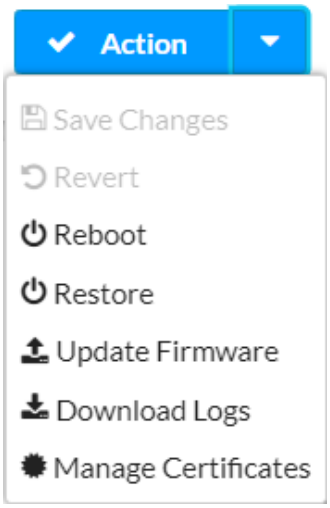
- **Status**: Used to monitor control system status
- **Settings**: Used to configure control system settings
- **Security**: Used to configure authentication and other security settings
- **802.1x Configuration**: Used to configure IEEE 802.1x network authentication for control system security

The **Status** tab is the default tab that is displayed, as shown in the preceding image.

Actions Menu

The configuration interface provides an **Actions** drop-down menu on the top right of the page. The **Actions** menu may be accessed at any time.

Actions Menu



Once any changes have been made to the control system configuration, the **Actions** button changes to a **Save Changes** button. Select **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 **Yes** to reboot the device or **No** to cancel the reboot.

The **Actions** menu provides the following selections.

Save Changes

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

Revert

Select **Revert** to revert the control system back to the last saved configuration settings.

Reboot

Select **Reboot** to reboot the control system.

After **Reboot** is selected, a dialog box is displayed asking whether the control system should be rebooted. Select **Yes** to reboot the device or **No** to cancel the reboot.

Restore

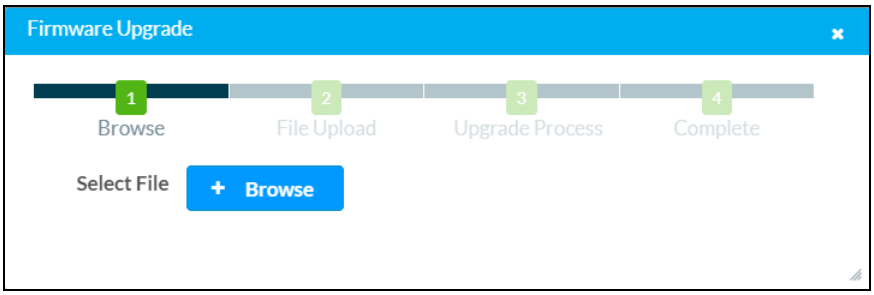
Select **Restore** to restore the control system configuration settings to their default values.

After **Restore** is selected a dialog box is displayed asking whether the device settings should be restored. Select **Yes** to restore the settings or **No** to cancel the restore.

Update Firmware

Select **Update Firmware** to upgrade the control system firmware manually with a downloaded PUF (package update file). The **Firmware Upgrade** dialog box opens.

Firmware Upgrade Dialog Box



To upload a firmware PUF through the web configuration interface:

> **NOTE:** Visit the appropriate device product page or www.crestron.com/Support/Resource-Library to download the latest firmware PUF.

1. Select **Browse**, and then navigate to the firmware PUF on the host computer.
2. Select the firmware PUF, and then select **Open**.
3. Select **Load** to load the PUF to the control system. The upload progress is shown in the dialog box.
4. Once the control system has completed the firmware upgrade, select **OK**.

Select the **x** button to close the **Firmware Upgrade** dialog box at any time during the upgrade process. Selecting the **x** button before the PUF is uploaded cancels the upgrade.

Download Logs

Select **Download Logs** to download the control system message logs for diagnostic purposes. The message files download as a compressed .tgz file. Once the compressed file is downloaded, extract the message log files to view them.

Manage Certificates

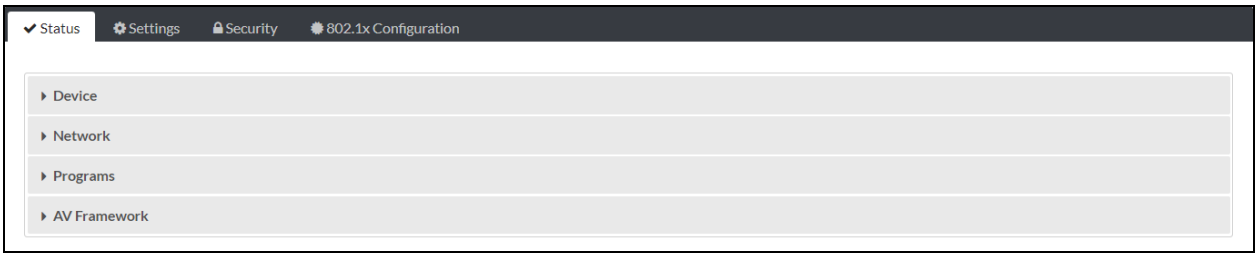
Select **Manage Certificates** to manage any certificates that are installed on the control system. For more information on certificate management, refer to 802.1x Configuration (on page 52).

Status

Select the **Status** tab on the top left of the configuration interface to display selections for viewing the status of device, network, and USB, and .AV Framework™ software settings.

Select on a selection name to expand the selection. If the selection is expanded, select the selection name again to collapse the section.

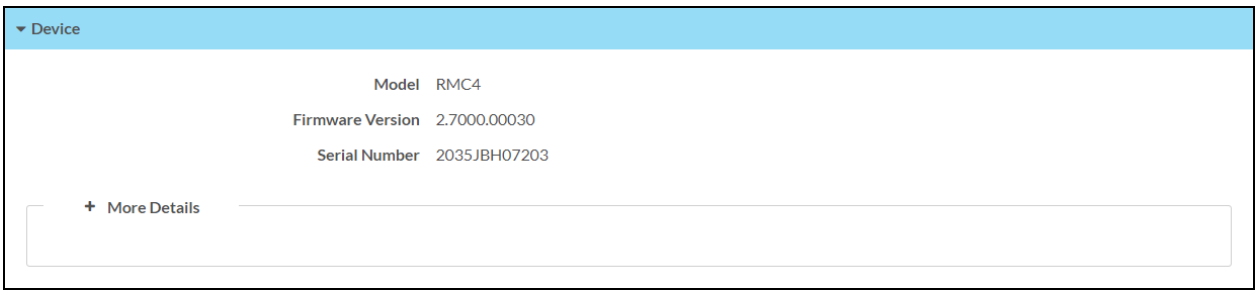
Status Tab Selections



Device

Select **Device** to view general device information.

Status Tab - Device



The following **Device** information is displayed:

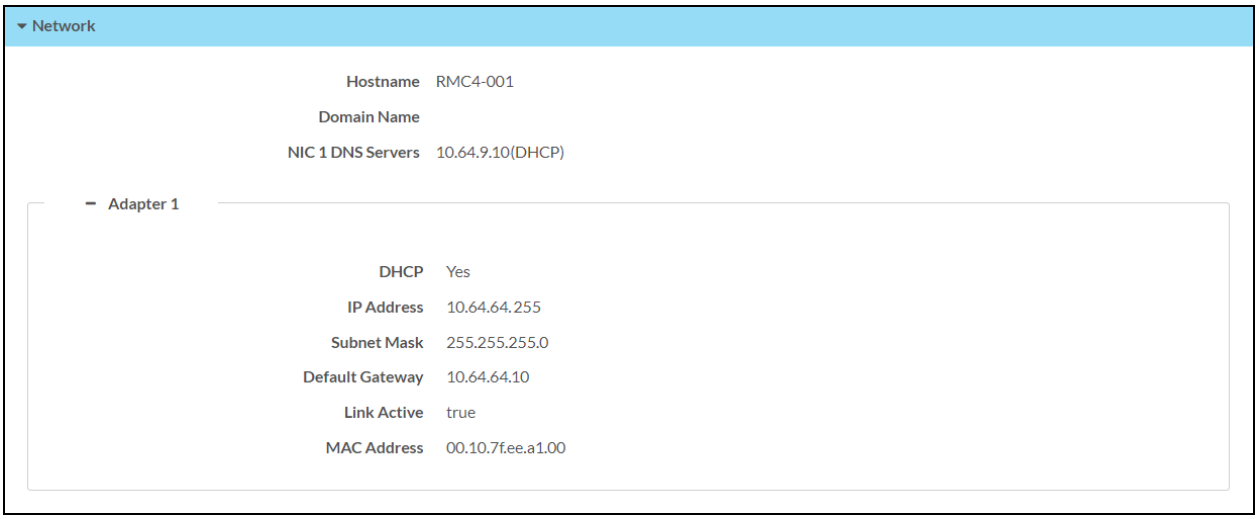
- **Model**: The control system model name
- **Serial Number**: The control system serial number
- **Firmware Version**: The firmware version loaded onto the control system

Select **+ More details** at the bottom of the **Device** tab to display an expanded section that shows more control system information. If **+ More Details** is selected, select **- Less Details** to collapse the section.

Network

Select **Network** to view the status of the network settings for the control system.

Status Tab - Network



The following **Network** information is displayed:

- **Hostname**: The control system hostname
- **Domain Name**: The control system domain name
- **NIC 1 DNS Servers**: The DNS (domain name server) addresses used to resolve the control system domain to an IP address

Select the **+** (plus) icon next to **Adapter 1** to display the following Ethernet settings:

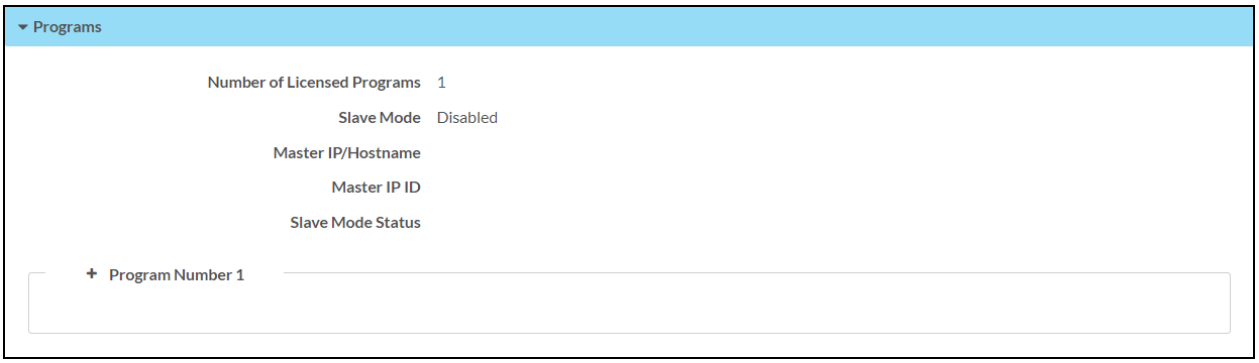
- **DHCP**: Reports whether the IP address is dynamic (**Yes**) or static (**No**)
- **IP Address**: The control system IP address, shown only if an Ethernet connection is active
- **Subnet Mask**: The control system subnet mask address, shown only if an Ethernet connection is active
- **Default Gateway**: The gateway router address, shown only if an Ethernet connection is active

- **Link Active**: Reports the status of the Ethernet connection (A **true** message indicates that the Ethernet connection is active, while a **false** message indicates that the Ethernet connection is inactive.)
- **MAC Address**: The unique MAC (media access control) address for the Ethernet adapter

Program

Select **Program** to view the status of the program and slave mode settings for the control system.

Status Tab - Program



The following **Program** information is displayed:

- **Number of Licensed Programs**: The number of licensed programs supported by the control system

  > **NOTE:** The RMC4 is designed to run a single program out of the box. The optional modular programming architecture (MPA) add-on allows the RMC4 to run up to ten programs simultaneously via a SW-RMC3-10PROG license.

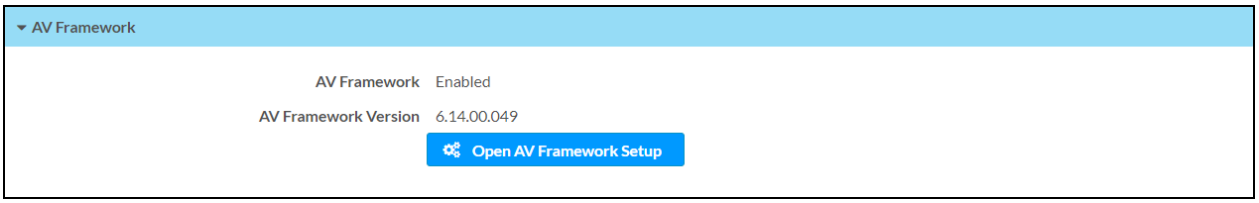
- **Slave Mode**: Reports whether the control system is running in subordinate mode (**Enabled**) or not (**Disabled**)
- **Master IP/Hostname**: The IP address or hostname of the primary control system, shown only if subordinate mode is turned on
- **Master IP ID**: The IP ID of the primary control system connection, shown only if subordinate mode is turned on
- **Slave Mode Status**: Indicates the connection status to a primary control system while in subordinate mode, shown only if subordinate mode is turned on

If one or more programs have been loaded to the control system, expandable subsections are shown that correspond with the program slot. Expand the subsection for a given program slot to display details about the loaded program.

AV Framework

Select **AV Framework** to view the status of the native .AV Framework software program running on the control system

Status Tab - AV Framework



The following **AV Framework** information is displayed:

- **AV Framework**: Reports whether the native .AV Framework software program has been turned on (**Enabled**) or not (**Disabled**)
- **AV Framework Version**: Reports the version of the native .AV Framework software program running on the control system, shown only if the native .AV Framework software program is turned on

If the native .AV Framework software program is turned on, an **Open AV Framework Setup** button is provided to launch the .AV Framework web configuration utility. For more information on configuring .AV Framework for the control system, refer to the .AV Framework Software for 4-Series Control Systems Operations Guide.

Settings

Select the **Settings** tab on the top left of the configuration interface to display selections for configuring various control system settings.

Settings Selections

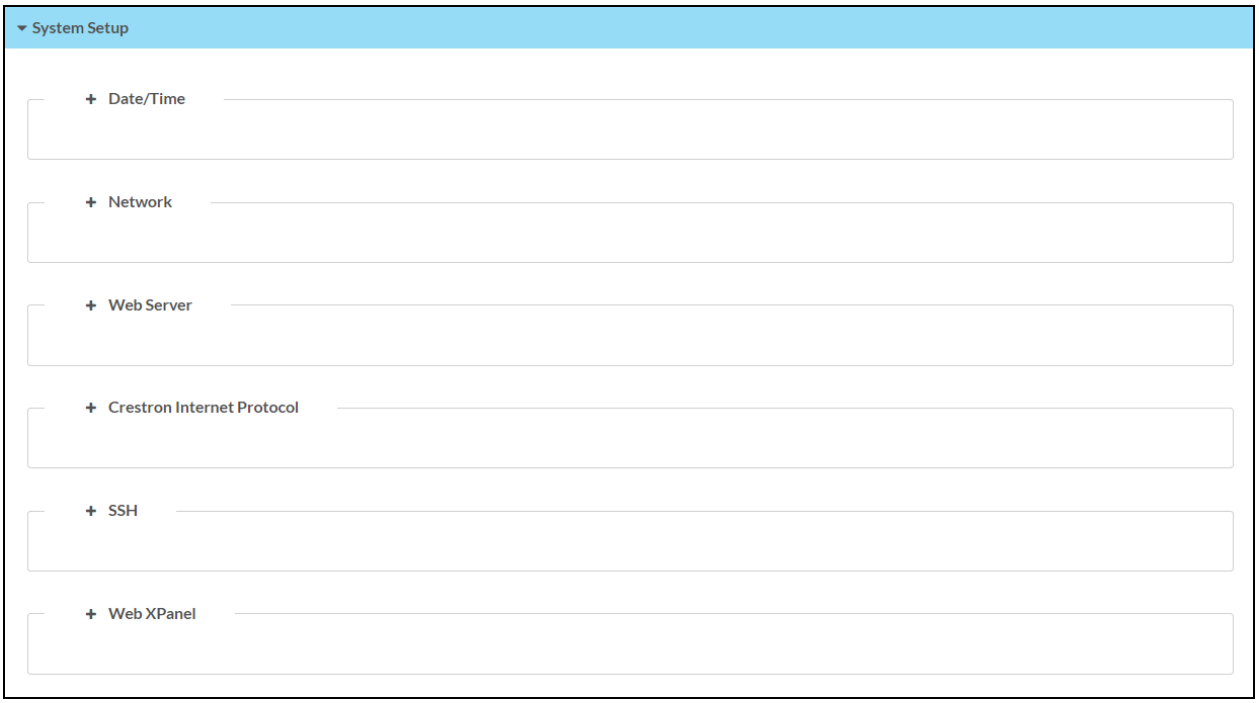
Each selection is described in the sections that follow.

NOTE: If an invalid value is entered for a setting, the web interface will not allow changes to be saved until a valid value is entered. Red text is displayed next a setting to indicate an invalid value.

System Setup

Select **System Settings** to configure general network and control system settings.

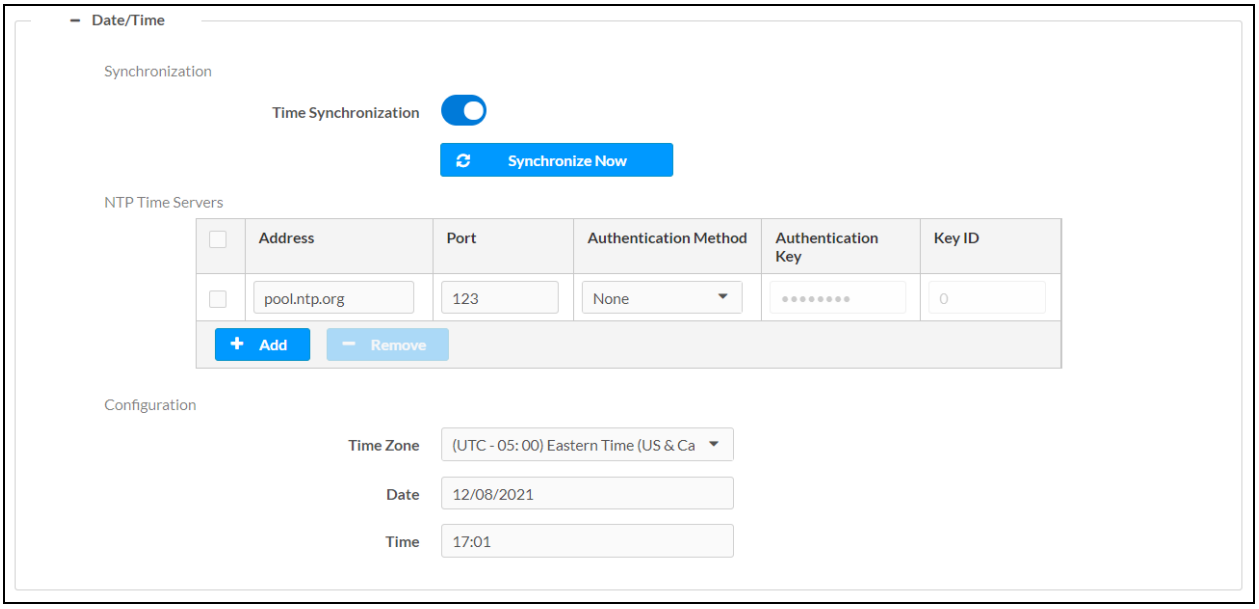
Settings Tab - System Setup



Time/Date

Select the **+** (plus) icon next to **Time/Date** to display the following time and date settings.

Settings Tab - System Setup (Time/Date)



- **Time Synchronization**: Turn on the toggle to use time synchronization via NTP (Network Time Protocol).
- **Synchronize Now**: With **Time Synchronization** turned on, select **Synchronize Now** to synchronize the control system with the NTP server(s) entered in the **NTP Time Servers** table.

- **NTP Time Servers**: With **Time Synchronization** turned on, use the provided table to enter information regarding the NTP server(s) used to synchronize the date and time for the control system.
    - Select **Add** to add a new NTP server entry into the table.
    - Enter the following information for each entry:
        - Enter the NTP server address into the **Address** text field.
        - Enter the NTP server port into the **Port** text field.
        - Use the **Authentication Method** drop-down menu to select the authentication method used to access the NTP server (if one exists).
        - If an authentication method is selected, enter the key used to authenticate against the NTP server into the **Authentication Key** text field.
        - If an authentication method is selected, enter the ID for the key used to authenticate against the NTP server into the **Key ID** text field.
    - To remove an entry, fill the checkbox to the left of the table entry, and then select **Delete**.

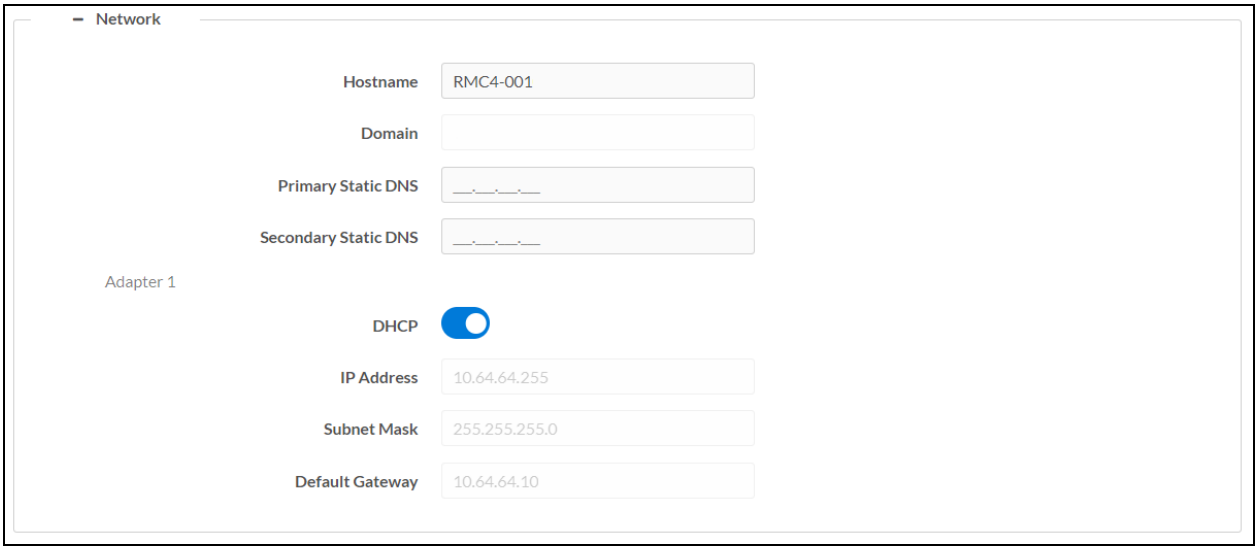
    > **NOTE:** NTP servers are configured into a particular slot. The server configured for the first table row will be the primary server used for time synchronization. The servers configured into additional table rows will be used as secondary servers.

- **Time Zone**: Select a time zone for the control system using the drop-down menu.
- **Date**: Select the date for the control system using the pop-up calendar that is displayed.
- **Time**: Select the time for the control system (in 24-hour format) using the pop-up menu that is displayed.

Network

Select the **+** (plus) icon next to **Network** to display the following network settings.

Settings Tab - System Setup (Network)



- **Hostname**: Enter the control system hostname.
- **Domain**: Enter the fully qualified domain name on the network.
- **Primary Static DNS**: Enter the primary DNS address.
- **Secondary Static DNS**: Enter the secondary DNS address.
- **DHCP**: Turn on the toggle to use DHCP for the Ethernet connection.

  > **NOTE:** If DHCP is turned on, IP does not function until a reply has been received from the server. The control system broadcasts requests for an IP address periodically.

- **IP Address**: If **DHCP** is turned off, enter the control system IP address on the network.
- **Subnet Mask**: If **DHCP** is turned off, enter the control system subnet mask address on the network.
- **Default Gateway**: If **DHCP** is turned off, enter the gateway router address on the network.

Web Server

Select the **+** (plus) icon next to **Web Server** to display the following control system web server settings.

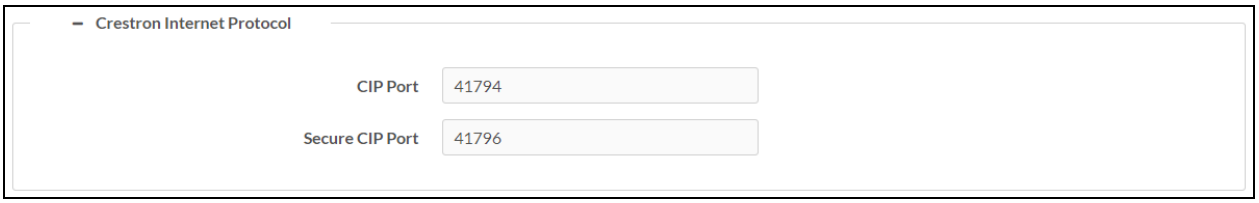
Settings Tab - System Setup (Web Server)

- Turn on the **Web Server Enabled** toggle to turn on the web server for the control system. The control system web server allows for users to upload web pages and mobility projects to a control system.
- If **Web Server Enabled** is turned on, enter an HTTP port to use for the web server in the **HTTP Port** text field. Port 80 is used by default.
- If **Web Server Enabled** is turned on, enter an HTTPS port to use for the web server in the **HTTPS Port** text field. Port 443 is used by default.

Crestron Internet Protocol

Select the **+** (plus) icon next to **Crestron Internet Protocol** to display the following Crestron Internet Protocol (CIP) port settings.

Settings Tab - System Setup (Crestron Internet Protocol)



- Enter the Crestron Internet Protocol port used by the control system in the **CIP Port** text field. Port 41794 is used by default.
- Enter the Secure Crestron Internet Protocol port used by the control system in the **SCIP Port** text field. Port 41796 is used by default.

SSH

Select the **+** (plus) icon next to **SSH** to display the following SSH (Secure Shell) settings.

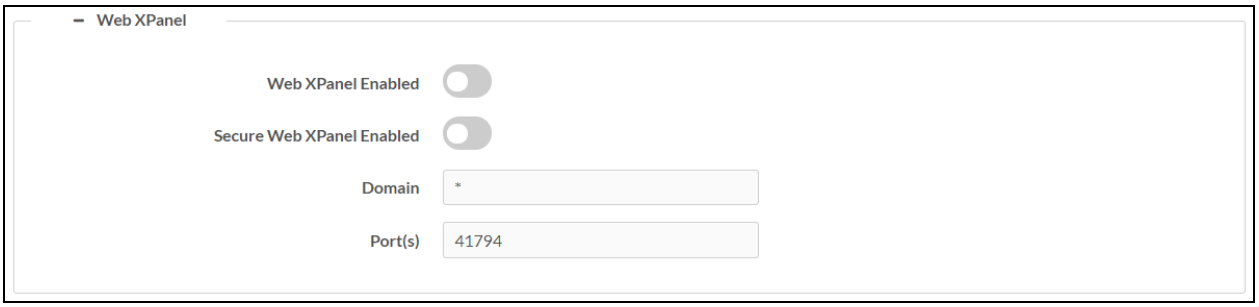
Settings Tab - System Setup (SSH)

- Turn on the **SSH Enabled** toggle to turn on SSH for the control system.
- If **SSH Enabled** is turned on, enter a port to use for the SSH protocol in the **SSH Port** text field. Port 22 is used by default.

Web XPanel

Select the **+** (plus) icon next to **Web XPanel** to display the following control system Web XPanel settings.

Settings Tab - System Setup (Web XPanel)



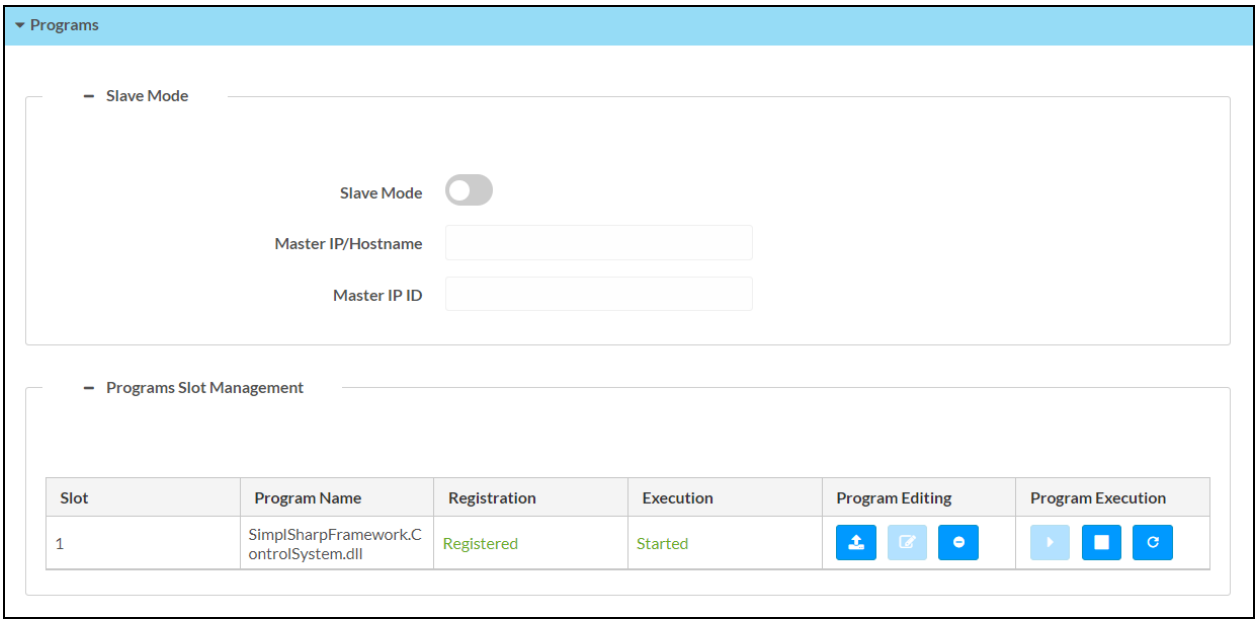
- Turn on the **Web XPanel Enabled** toggle to turn on the Web XPanel functionality for the control system.
- Turn on the **Secure Web XPanel Enabled** toggle to turn on a secure Web XPanel connection for the control system. If this toggle is turned on, the Web XPanel can only connect to the control system over encrypted TLS/SSL.
- Enter a domain name for the Web XPanel in the **Domain** text field.
- Enter one or more ports for the Web XPanel in the **Port(s)** text field. Port 41794 is used by default.

> **NOTE:** Enter "*" to open all ports for the Web XPanel. A range of ports can also be specified.

Programs

Select **Programs** to manage control system programs and to configure subordinate mode settings for the control system.

Settings Tab - Programs



Slave Mode

> **NOTE:** For more information on using subordinate mode for a 4-Series control system, refer to the "Master-Slave Mode" topic in the 4-Series Control Systems Reference Guide.

Select the **+** (plus) icon next to **Slave Mode** to display the following subordinate mode settings.

- Turn the **Slave Mode** toggle on to run the control system in subordinate mode. If this toggle is turned on, the control system will follow a program running on the primary control system and will make its ports available to that control system.
- If **Slave Mode** is turned on, enter the IP address or hostname of the primary control system in the **Master IP/Hostname** text field.
- If **Slave Mode** is turned on, enter the IP ID for the connection to the primary control system in the **IP ID** text field.

Program Slot Management

> **NOTE:** For more information on managing programs on a 4-Series control system, refer to the "Program Management" topic in the 4-Series Control Systems Reference Guide.

Select the **+** (plus) icon next to **Program Slot Management** to display the following program management settings.

Each program slot is represented in a table that provides the following information and controls:

- **Slot**: The program slot number (1-10)

  > **NOTE:** The RMC4 is designed to run a single program out of the box. The optional modular programming architecture (MPA) add-on allows the RMC4 to run up to ten programs simultaneously via a SW-RMC3-10PROG license.

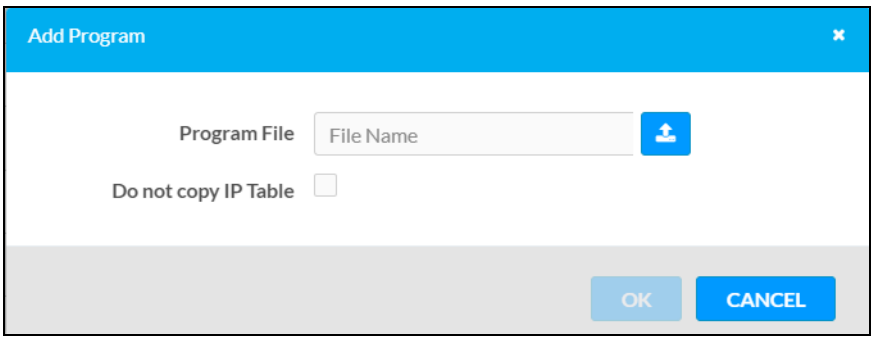
- **Program Name**: The name for the control system program
- **Registration**: The registration status of the program
- **Execution**: The execution status of the program
- **Program Editing**: Provides the following program editing controls:
  - Select the **Upload Program** button to load a new program to the control system. Instructions for loading a new program to the control system are provided below.
  - Select the **Edit Program** button to edit information about the program (if available).
  - If the program is unregistered, select the **Register Program** button to register the program with the control system.
  - If the program is registered, select the **Unregister Program** button to unregister the program from the control system.
- **Program Execution**: Provides the following program execution controls:
  - If the program is stopped, select the **Start Program** button to start the program.
  - If the program is running, select the **Stop Program** button to stop the program.
  - Select the **Restart Program** button to restart the program.

Load a New Program

To load a new program to the control system:

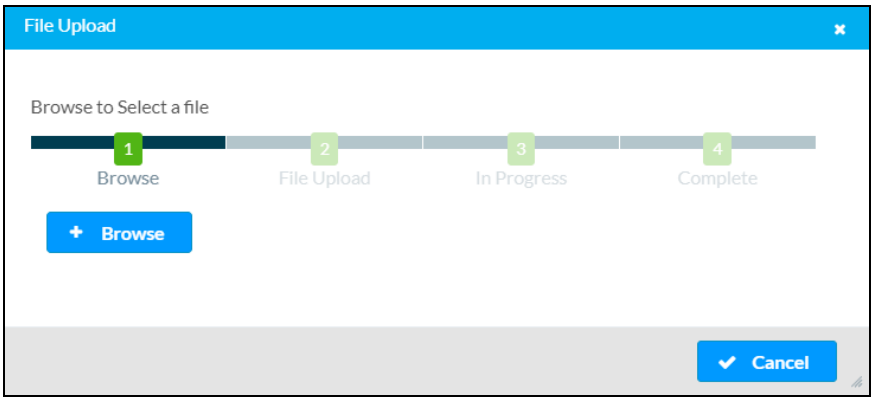
1. Select the **Upload Program** button in an available program slot. The **Add Program** dialog box is displayed.

   Add Program Dialog Box



2. If desired, fill the **Do not copy IP Table** check box to prevent the program IP table from being copied to the control system following the upload.
3. Select the **Program File** button. The **File Upload** dialog box is displayed.

   File Upload Dialog Box



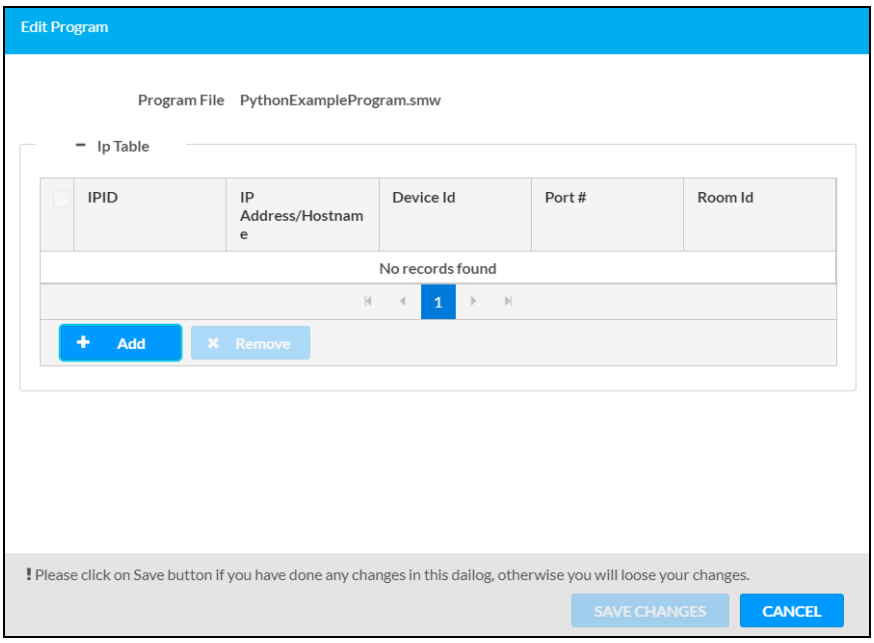
4. Select **Browse**, and then navigate to the program file (LPZ or CPZ) on the host computer.
5. Select the program file, and then select **Open**.
6. Select **Load** to load the program file to the control system. The upload progress is shown in the dialog box.
7. Once the control system has completed the program upload, select **OK**. The program will appear in the **Program Slot Management** table and will automatically try to register and start itself on the control system.

Edit a Program

To edit the IP table for a control system program (if permitted by the program):

1. Select the **Edit Program** button in the desired program slot. The **Edit Program** dialog box is displayed.

   Edit Program Dialog Box



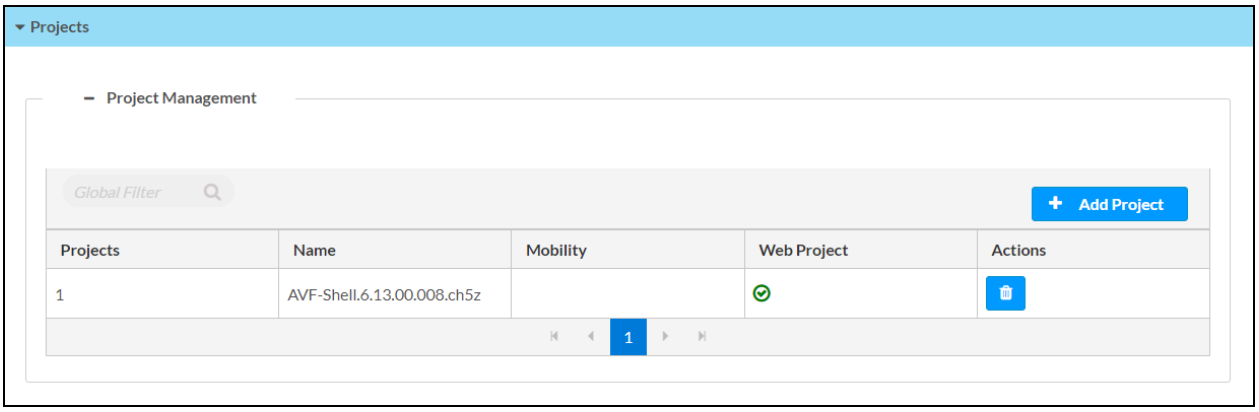
> **NOTE:** If IP table entries have already been defined in the program, these entries will populate the table in the **Edit Program** dialog box unless the **Do not copy IP Table** check box was filled when loading the program to the control system.

2. Select **Add** to add a new IP table entry for the program (if necessary).
3. Enter or update the following information in each column for the IP table entry:
   - **IPID**: Enter an IP ID that will be used for communication between a device and the control system.
   - **IP Address/Hostname**: Enter the IP address or hostname for the device that will connect to the control system over IP.
   - **Device Id**: Enter a unique ID for the connecting device. By default, this value is the same as the provided IP ID.
   - **Port #**: Enter the port used for communication between device and control system.
   - **Room Id**: Enter the Crestron Virtual Control (VC-4) room ID that is associated with the IP table entry. This setting is applicable only for VC-4 connections.
4. Select **Save Changes** to save any changes to the IP table.

Projects

Select **Projects** to manage web and mobility projects for the control system.

Settings Tab - Programs



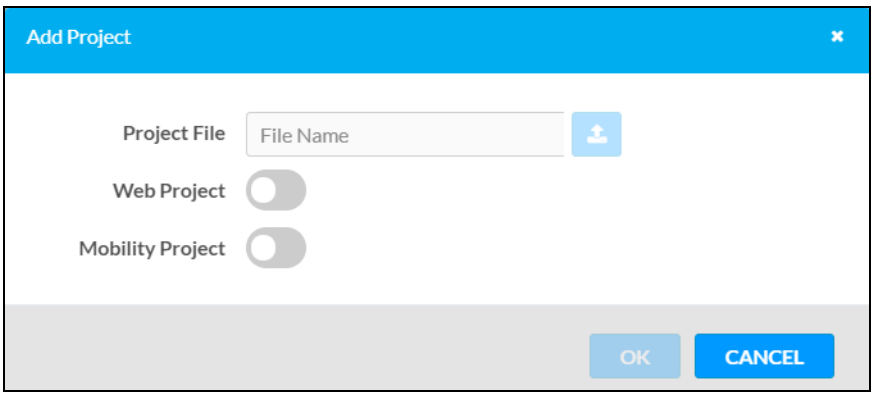
Each loaded project is represented in a table that provides the following information and controls:

- **Projects**: The project number on the control system
- **Name**: The name for the web or mobility project
- **Mobility**: Displays a green check icon if the project is a mobility project
- **Web Project**: Displays a green check icon if the project is a web project
- **Actions**: Select the trash can button to delete the project from the control system

To load a new web or mobility project to the control system:

1. Select the **Add Project** button. The **Add Project** dialog box is displayed.

   Add Project Dialog Box

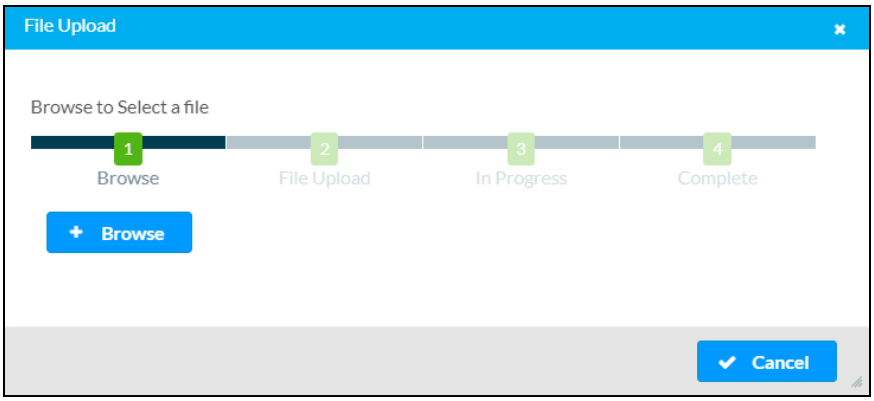
   

2. Turn on the **Web Project** or **Mobility Project** toggles to define whether the loaded project is a web or a mobility project.

   > **NOTE:** If the project is both a web and a mobility project, both toggles can be selected.

3. Select the **Project File** button. The **File Upload** dialog box is displayed.

   File Upload Dialog Box

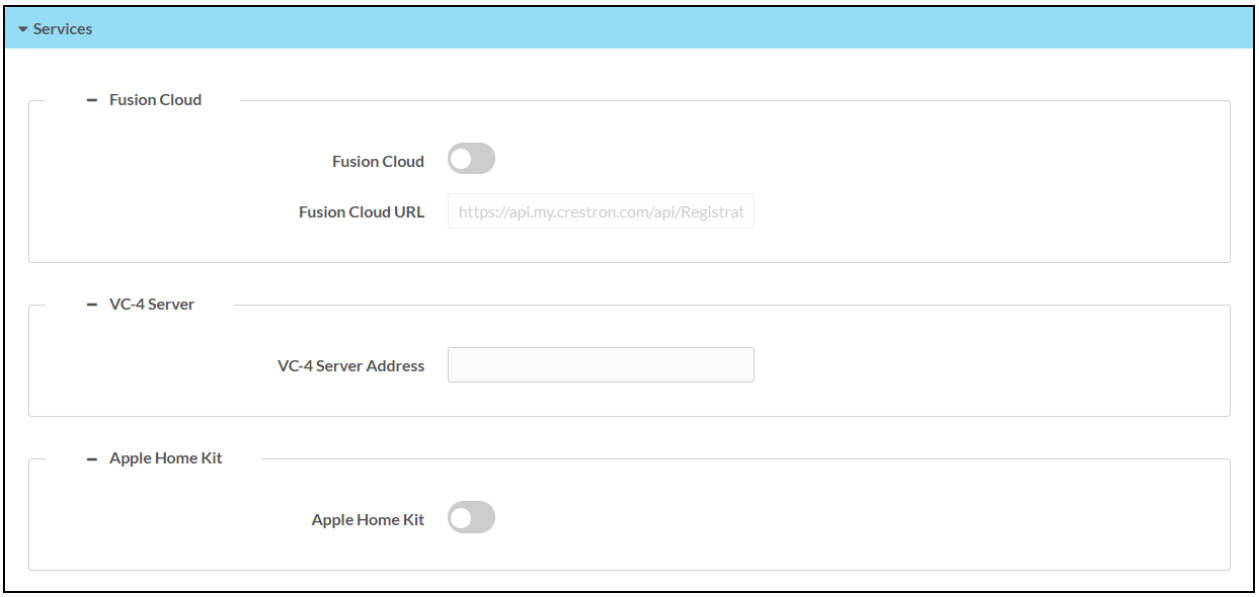


4. Select **Browse**, and then navigate to the project file on the host computer.
5. Select the project file, and then select **Open**.
6. Select **Load** to load the project file to the control system. The upload progress is shown in the dialog box.
7. Once the control system has completed the project upload, select **OK**. The program will appear in the **Project Management** table.

Services

Select **Services** to manage various external services that integrate with the control system.

Settings Tab - Services



Crestron Fusion Cloud

> **NOTE:** If connecting to a Crestron Fusion software on-premises server, connections are made using either traditional (outbound) or inbound communications. For more information, refer to the Crestron Fusion 10 On-Premises Software Getting Started Guide.

- Turn on the **Crestron Fusion Cloud** toggle to allow a connection to a Crestron Fusion Cloud server.
- If **Crestron Fusion Cloud** is turned on, enter the address used to connect the control system to the desired Crestron Fusion Cloud server in the **Crestron Fusion Cloud URL** text field.

VC-4 Server

> **NOTE:** For more information on connecting the control system to Crestron Virtual Control (VC-4), refer to the help file in the Crestron Virtual Control web configuration interface. To access the help file, select the question mark button ? on the top left of the page.

Enter a VC-4 server address into the **VC-4 Server Address** text field to establish a connection between the control system and a VC-4 server.

Apple HomeKit

> **NOTE:** For more information on pairing the device with an Apple® HomeKit® system, refer to support.apple.com/en-us/HT204893.

Turn on the **Apple Home Kit** toggle to turn on the HomeKit feature on the control system.

Cloud Settings

Select **Cloud Settings** to turn a connection between the control system and an XiO Cloud® service account on or off.

Settings Tab - Cloud Settings

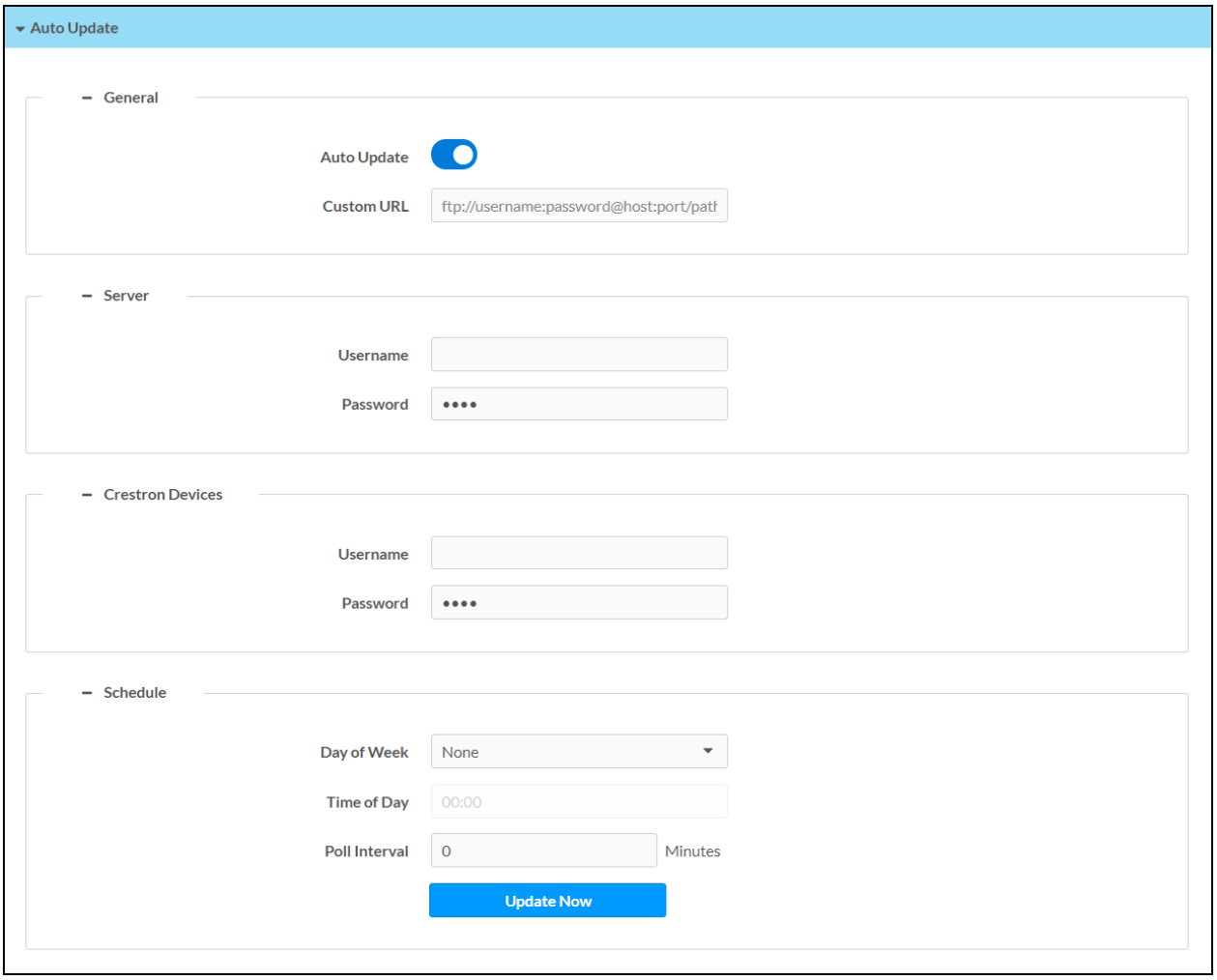
Turn on the **Cloud Configuration Service Connection** to allow a connection between control system and an XiO Cloud account. This setting is turned on by default.

For more information on connecting to the XiO Cloud service, refer to Connect to XiO Cloud Service.

Auto Update

Select **Auto Update** to configure automatic firmware updates for the control system and connected devices.

Settings Tab - Auto Update



NOTE: For more information on configuring automatic updates for the control system, refer to the "Auto Update Mechanism" topic in the 4-Series Control Systems Reference Guide.

General

- Turn on the **Auto Update** toggle to use automatic updates for the control system and connected devices.
- If **Auto Update** is turned on, enter a custom update server FTP address in the **Custom URL** text field.

Server

The following settings can be configured for the auto update server if **Auto Update** is turned on:

- Enter a username for accessing the auto update server in the **Username** text field.
- Enter a password for accessing the auto update server in the **Password** text field.

Crestron Devices

The following settings can be configured for updating connected Crestron devices if **Auto Update** is turned on:

- Enter a username for pushing automatic updates to controlled Crestron devices in the **Username** text field.
- Enter a password for pushing automatic updates to controlled Crestron devices in the **Password** text field.

Schedule

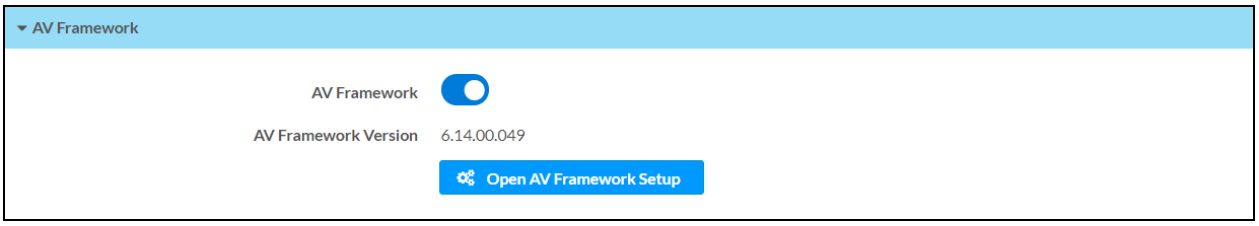
The following settings can be configured for scheduling automatic updates if **Auto Update** is turned on:

- Use the **Day of Week** drop-down menu to select a day of the week to check for and perform automatic updates.
    - Select **Daily** to check for new updates every day.
    - Select **None** to only check for new updates manually.
- If a value is provided for **Day of Week** other than "None," enter a time of day (in 24-hour format) when the control system will check updates on the scheduled day.
- If "None" is selected for **Day of Week**, enter the polling interval (in hours) for when the control system will poll the server for updates.
- Select **Update Now** to check the update server for new firmware and to update the control system immediately if new firmware is available.

AV Framework

Select **AV Framework** to configure the native .AV Framework software program running on the control system.

Settings Tab - AV Framework



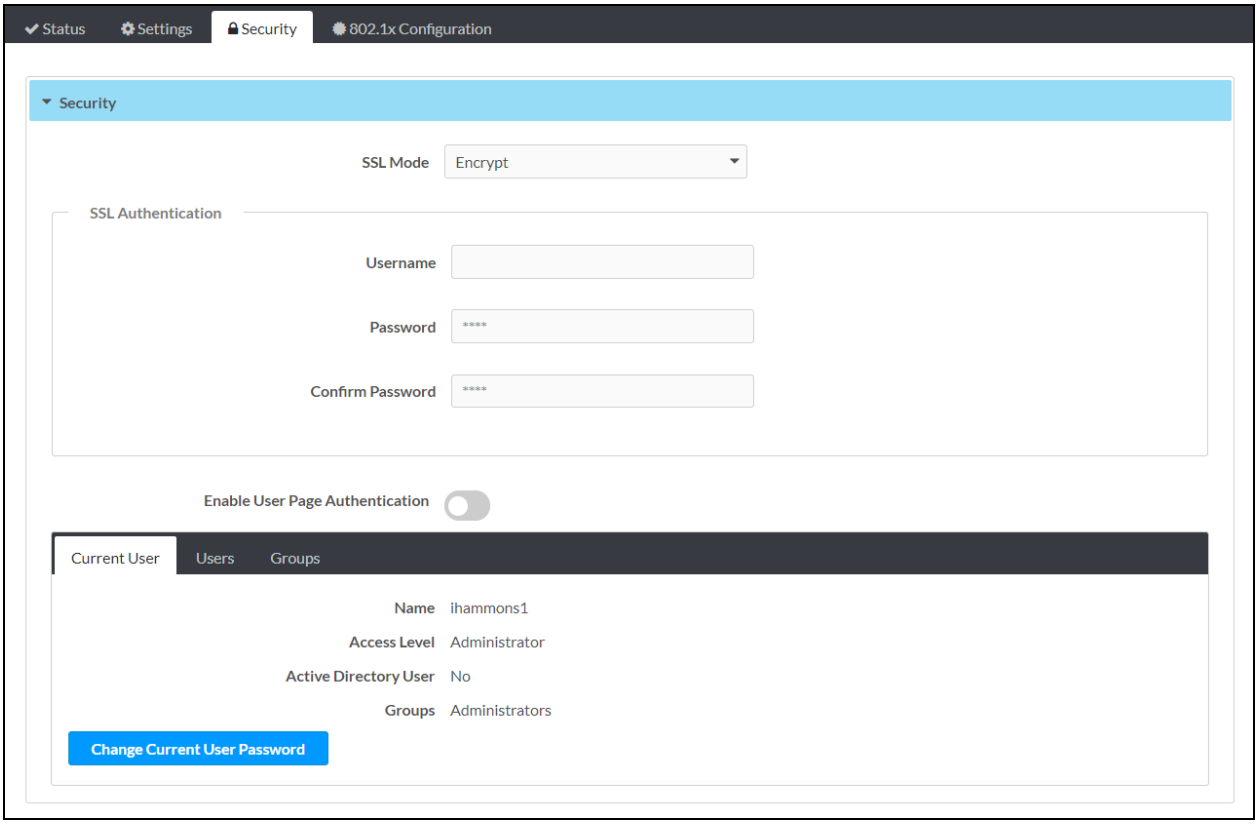
NOTE: If an older version of the .AV Framework program is detected in the Program 01 slot (6.13 and prior), the program is loaded to the Program 00 slot, but it is not turned on within the control system. The older .AV Framework program must be removed manually before the newer version can be turned on. For more information, refer to the .AV Framework Software for 4-Series Control Systems Operations Guide.

- Turn on the **AV Framework** toggle to turn on the native .AV Framework software program on the control system.
- If **AV Framework** is turned on, the version of the native .AV Framework software program is reported next to **AV Framework Version**.
- If **AV Framework** is turned on, select **Open AV Framework Setup** to launch the .AV Framework web configuration utility. For more information on configuring .AV Framework for the control system, refer to the .AV Framework Software for 4-Series Control Systems Operations Guide.

Security

Select the **Security** tab on the top left of the configuration interface to display selections for configuring security and authentication settings for the control system.

Security Tab Selections



Expand the **Security** accordion to configure the following settings:

> **NOTE:** For more information about configuring authentication settings on a 4-Series control system, refer to the "Authentication" topic in the 4-Series Control Systems Reference Guide.

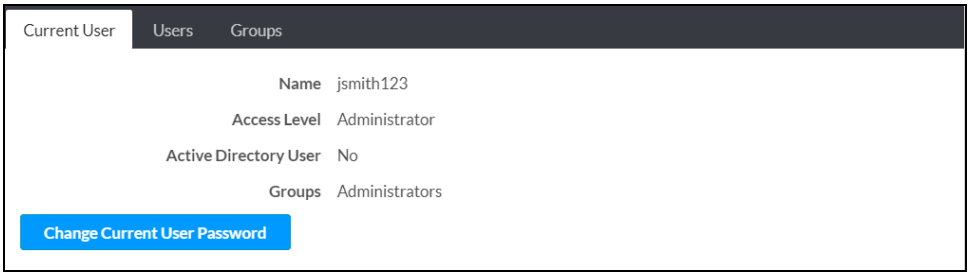
- **SSL Mode**: Select an SSL (Secure Sockets Layer) mode to use for establishing a secure connection to the control system:
  - **Encrypt and Validation**: The control system will require a username and password to validate an encrypted SSL connection. Enter a username and password in the appropriate fields that are displayed.
  - **Encrypt**: The control system will use an encrypted SSL connection.
- **Enable User Page Authentication**: Turn on the toggle to use user page authentication for web pages and mobility projects. If this toggle is turned on, a user will be prompted for login credentials as they load the project.

Control system users and groups can be viewed and modified within the table provided at the bottom of the accordion. Use the following settings to add, delete, and edit control system users and groups.

Current User

Select the **Current User** tab to view and edit information for the current control system user.

Current User Tab



The following settings are displayed for the current user:

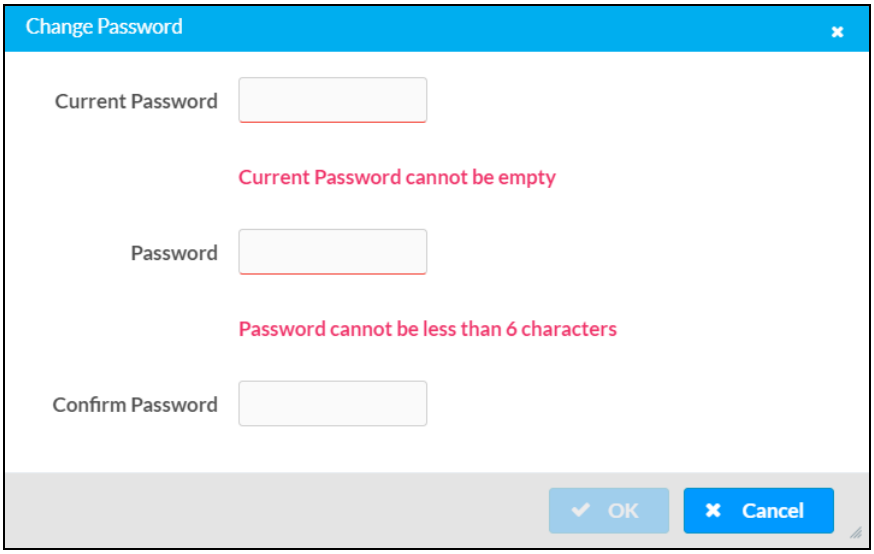
- **Name**: The chosen username
- **Access Level**: The access level granted to the user (**Administrator**, **Programmer**, **Operator**, **User**, or **Connect**)
- **Active Directory User**: Reports whether the current user is (**Yes**) or is not (**No**) authenticated through Active Directory® software

  > **NOTE:** A user must be added to an Active Directory group before the user may be selected as an active directory user. For more information, refer to Groups (on page 49).

- **Groups**: Any groups of which the current user is a member

Select **Change Current User Password** to change the password for the current user. The **Change Password** dialog box is displayed.

Change Password Dialog Box



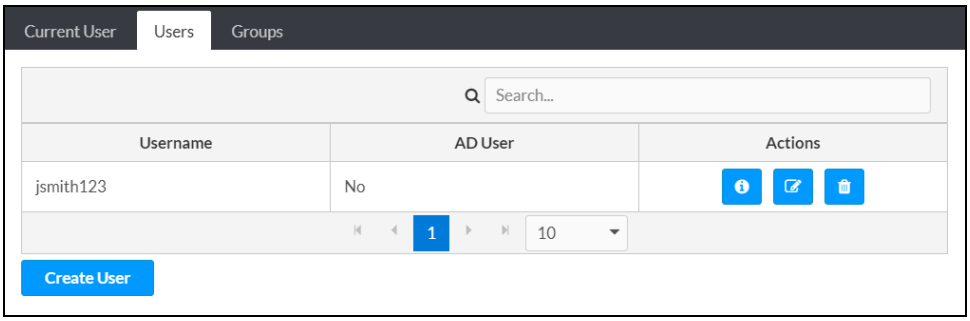
Enter the existing password in the **Current Password** field. Then, enter a new password in the **Password** field, and reenter the password in the **Confirm Password** field.

Select **OK** to save the new password, or select **Cancel** to cancel the change.

Users

Select the **Users** tab to view and edit information for the control system users.

Users Tab



Enter text into the **Search Users** field to find and display users that match the search term(s).

Control system users are listed in table format. The following information is displayed for each control system user:

- **Username**: The chosen username
- **AD User**: Reports whether the user is (**Yes**) or is not (**No**) authenticated through Active Directory

> **NOTE:** A user must be added to an Active Directory group before the user may be selected as an active directory user. For more information, refer to Groups (on page 49).

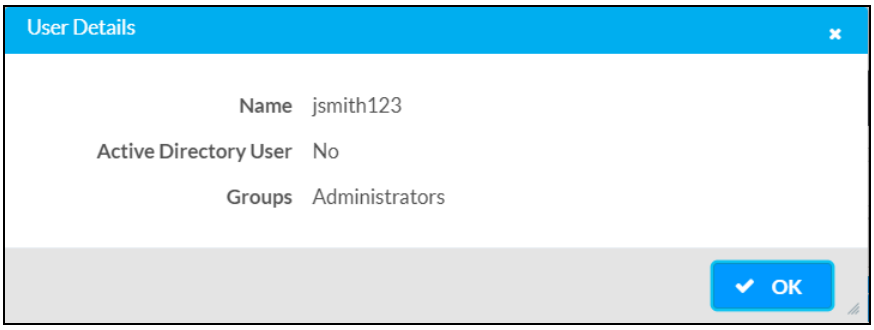
If the control system users span multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page. Additionally, the number of users displayed on each page may be set to 5, 10, or 20 users.

An **Actions** column is also provided for each user that allows various actions to be performed. The following selections may be selected from the **Actions** column.

User Details

Select the information button in the **Actions** column to view information for the selected user. The **User Details** pop-up dialog box is displayed.

User Details Dialog Box



The following settings are displayed for the current user:

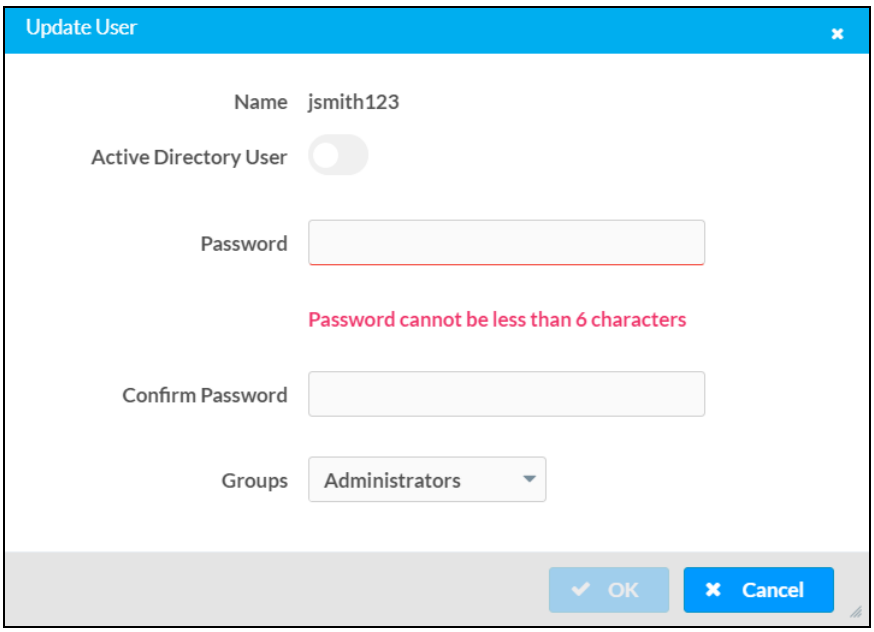
- **Name**: The chosen username
- **Active Directory User**: Reports whether the user is (**Yes**) or is not (**No**) authenticated through Active Directory
- **Groups**: Lists any groups that contain the user

Select **OK** to return to the **Authentication Management** > **Users** page.

Update User

Select the editing button in the **Actions** column to edit settings for the selected user. The **Update User** dialog box is displayed.

Update User Dialog Box



The following **Update User** settings may be viewed or configured:

- **Name**: The chosen username
- **Active Directory User**: Turn on the toggle to use authentication via Active Directory for the selected user.
- **Password**: Enter a new password for the selected user.
- **Confirm Password**: Reenter the password provided in the **Password** field.
- **Groups**: Add the user to one or more groups. For more information, refer to Groups (on page 49).

> **NOTE:** A user must be added to an Active Directory group to be selected as an Active Directory user.

Select **OK** to save any changes and to return to the **Users** selections. Select **Cancel** to cancel any changes.

Delete User

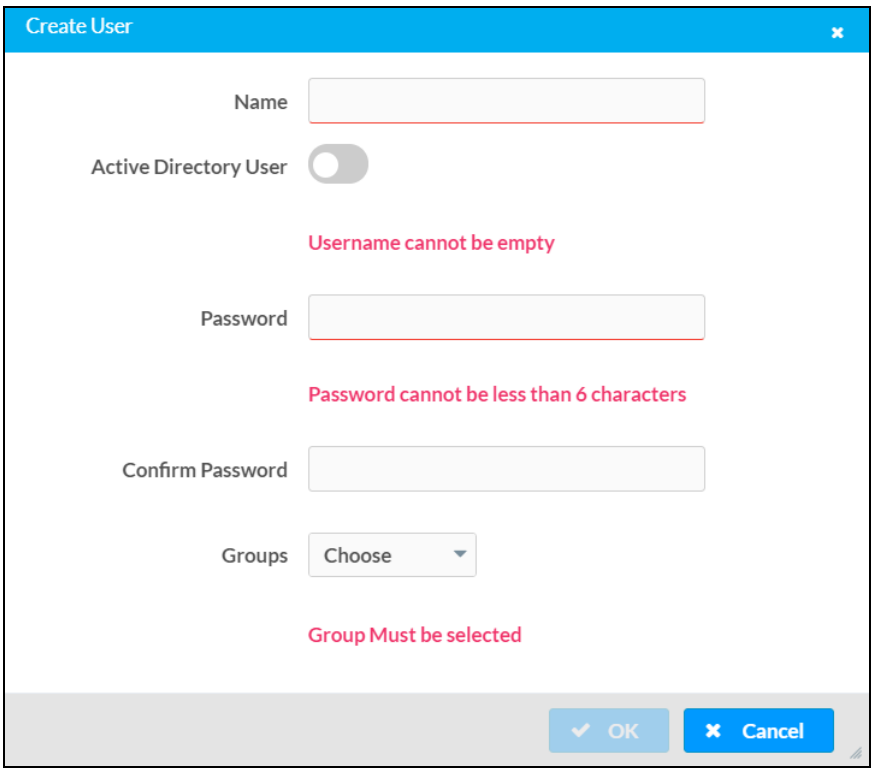
Select the trashcan icon in the **Actions** column to delete the user.

A pop-up dialog box is displayed asking whether the user should be deleted. Select **Yes** to delete the user or **No** to cancel.

Create User

Select **Create User** at the bottom of the page to create a new control system user. The **Create User** dialog box is displayed.

Create User Dialog Box



Use the following settings to create a new user:

- **Name**: Enter a username.
- **Active Directory User**: Turn on the toggle to use authentication via Active Directory for the user.
- **Password**: Enter a password for the user.
- **Confirm Password**: Reenter the password provided in the **Password** field.
- **Groups**: Add the user to one or more groups. For more information, refer to Groups (on the facing page).

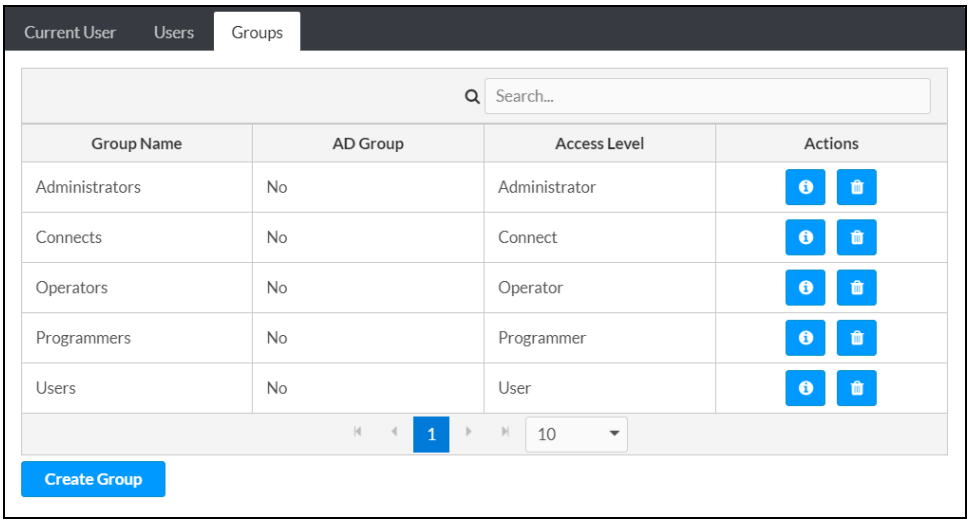
> **NOTE:** A user must be added to an Active Directory group to be selected as an Active Directory user.

Select **OK** to save any changes and to return to the **Users** selections. Select **Cancel** to cancel creating a new user.

Groups

Select the **Groups** tab to view and edit settings for control system groups. Control system groups are used to group users by access level and Active Directory authentication settings.

Groups Tab



Enter text in the **Search Groups** field to find and display groups that match the search term(s).

Control system groups are listed in table format. The following information is displayed for each control system group:

- **Group Name**: The chosen group name
- **AD Group**: Reports whether the group is (**Yes**) or is not (**No**) authenticated through Active Directory

  > **NOTE:** Active Directory provides an extra layer of authentication for control system groups and users. Active directory group and user names are stored in the control system console along with a unique SID (security identifier). When an Active Directory user attempts to authenticate against the console, the console first checks the user credentials. If the Active Directory authentication is successful, Active Directory queries the console for the user or group's SID. The user is granted access to the control system only if at least one SID match is found.

- **Access Level**: The access level for the selected group (**Administrator**, **Programmer**, **Operator**, **User**, or **Connect**)

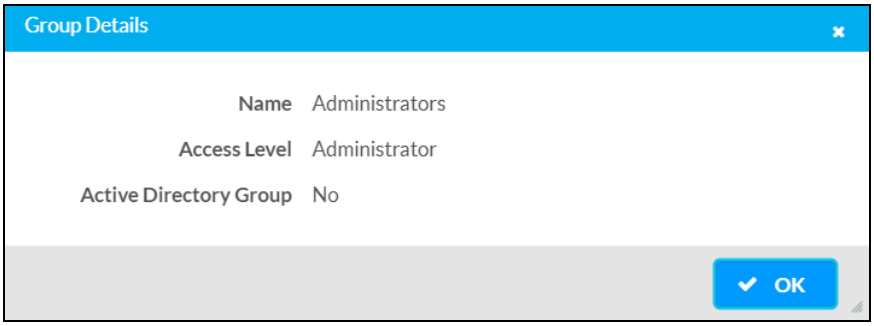
If the control system groups span multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page. Additionally, the number of groups displayed on each page may be set to 5, 10, or 20 users.

An **Actions** column is also provided for each group that allows various actions to be performed. The following selections may be selected from the **Actions** column.

Group Details

Select the information button in the **Actions** column to view information for the selected group. The **Group Details** dialog box is displayed.

Group Details Dialog Box



The following settings are displayed for the current group:

- **Name**: The chosen group name

  > **NOTE:** If authenticating with Active Directory, do not enter the domain name for the Active Directory group in the **Name** field. If this information is being entered via console commands, omit `domain\local` from the command (for example, `adddomaing -n:crestron -L:A` instead of `adddomaing -n:domain.local\crestron -L:A`).

- **Access Level**: The access level of the group and its users
- **Active Directory User**: Reports whether the group is (**Yes**) or is not (**No**) authenticated through Active Directory

Select **OK** to return to the **Groups** selections.

Delete Group

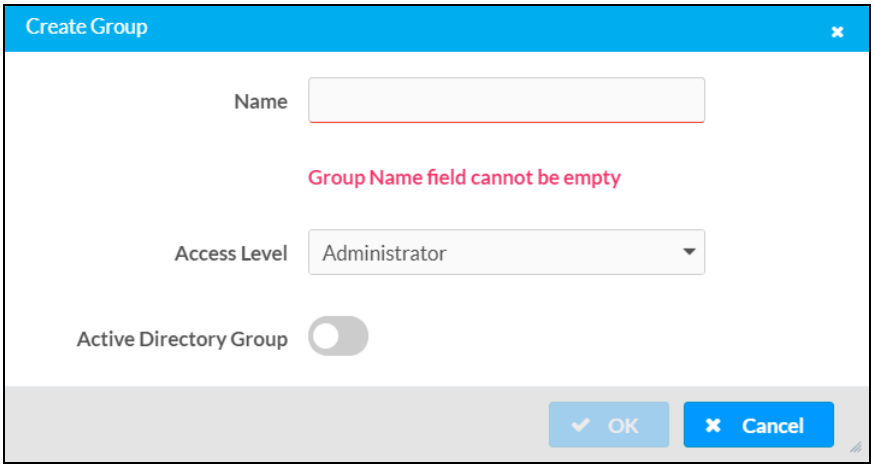
Select the trashcan icon in the **Actions** column to delete the group.

A pop-up dialog box is displayed asking whether the group should be deleted. Select **Yes** to delete the group or **No** to cancel.

Create Group

Select **Create Group** at the bottom of the page to create a new control system group. The **Create Group** dialog box is displayed.

Create Group Dialog Box



Use the following settings to create a new group:

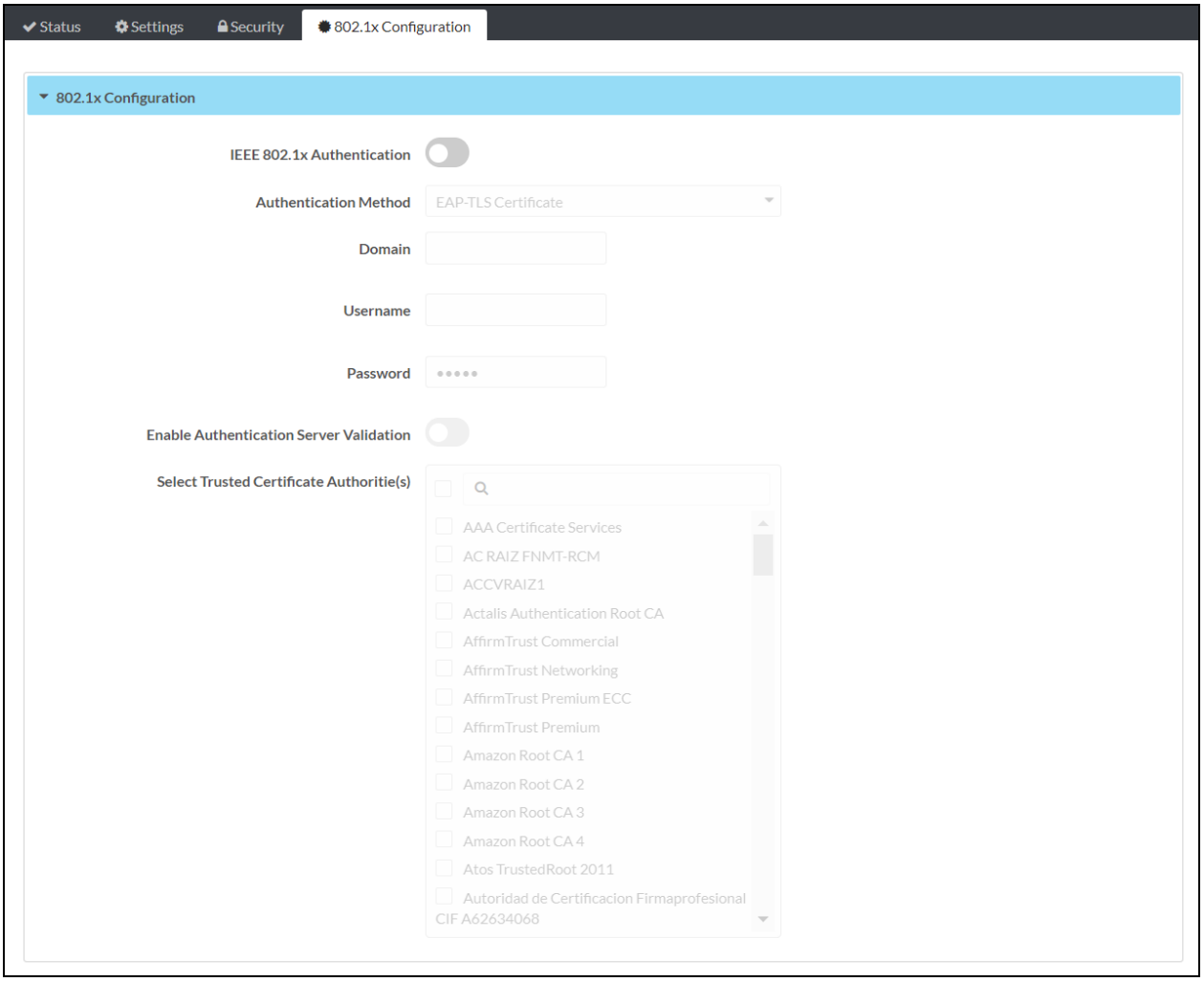
- **Name**: Enter a group name.
- **Access Level**: Select an access level for the group and its users from the drop-down menu.
- **Active Directory Group**: Turn on the toggle to use authentication via Active Directory for the group.

Select **OK** to save any changes and to return to the **Groups** selections. Select **Cancel** to cancel creating a new group.

802.1x Configuration

Select the **802.1x Configuration** tab on the top left of the configuration interface to display selections for configuring IEEE 802.1X network authentication for control system security.

802.1x Configuration Tab Selections



Expand the **802.1x Configuration** accordion to configure the following settings:

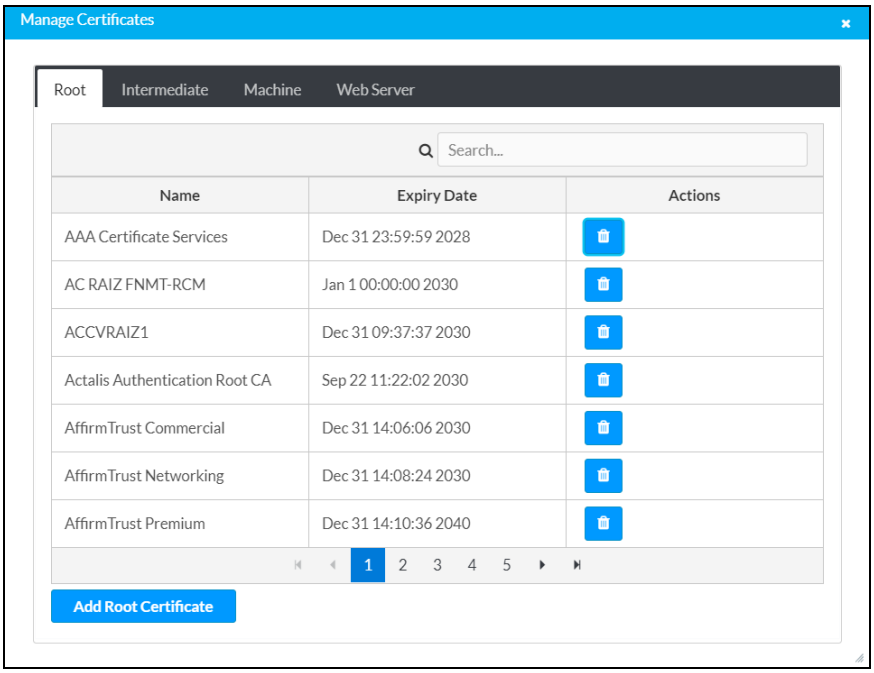
> **NOTE:** For more information about configuring 802.1X network authentication on a 4-Series control system, refer to the "802.1X" topic in the 4-Series Control Systems Reference Guide.

- **IEEE 802.1x Authentication**: Turn on the toggle to use 802.1X authentication for the control system.

- **Authentication Method**: Select an 802.1 authentication method (**EAP-TLS Certificate** or **EAP MSCHAP V2- password**) from the drop-down menu.
    - **Domain**: If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a domain name that is required for authentication.
    - **Username**: If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a username that is required for authentication.
    - **Password**: If **EAP MSCHAP V2- password** is selected for **Authentication Method**, enter a password that is required for authentication.
- **Enable Authentication Server Validation**: Turn on the toggle to use server validation for increased security.
- **Select Trusted Certificate Authorities**: Select trusted CAs (Certificate Authorities) from the provided CAs to be used for server validation:
    - 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.
    - Select the check box to the left of the search field at the top of the CA menu to select all CAs as trusted CAs.

Select **Manage Certificates** from the **Action** menu to add or remove CAs from the list. The **Manage Certificates** dialog box is displayed with the **Root** tab selected.

Manage Certificates Dialog Box - Root Tab



Select the tabs near the top of the page to switch between the different types of CAs (**Root**, **Intermediate**, **Machine**, or **Web Server**). The same settings are provided for each type of CA.

Type a search term into the **Search...** text field to search for and display CAs that match the search term.

The following information is provided for each type of CA:

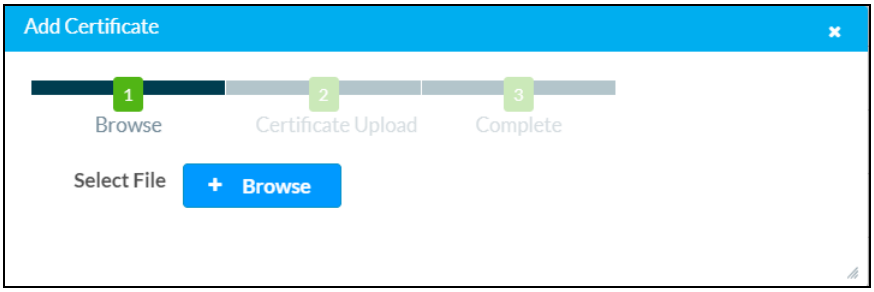
- **Name**: The CA name
- **Expiry Date**: The date and time that the CA is set to expire

If the CAs span multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page.

Select the trashcan button in the **Actions** column for a CA to delete it. A pop-up dialog box is displayed asking if the CA should be deleted. Select **Yes** to delete the certificate or **No** to cancel.

Select **Add [Type] Certificate** to add a CA of one of the four available types (**Root**, **Intermediate**, **Machine**, or **Web Server**) to the list of CAs. The **Add Certificate** pop-up dialog box is displayed.

Add Certificate Dialog Box



To add a new certificate:

1. Select **Browse**.
2. Navigate to the CA file on the host computer.
3. Select the CA file, and then select **Open**.
4. Select **Load** to load the CA file to the control system. The upload progress is shown in the dialog box.
5. Once the control system has completed the upload, select **OK**.

Select the **x** button to close the **Add Certificate** dialog box at any time during the upload process. Selecting the **x** button before the CA file is uploaded to the control system cancels the upload.

Select the **x** button to close the **Manage Certificates** dialog box and to return to the **802.1x Authentication** page.

Programming

4-Series control systems support an open development environment that enables programmers to use standard tools to create C# programs. Programmers can also use Crestron tools such as SIMPL, SIMPL# Pro, and VT Pro-e® software to create control system programs and projects.

- For more information on programming for a 4-series control system using C#, refer to online help answer ID 1000637.
- For more information on programming for a 4-series control system using the Python® programming language, refer to the Python Programming Language on 4-Series Control Systems Developer Microsite.

Resources

The following resources are provided for the RMC4.

NOTE: You may need to provide your Crestron.com web account credentials when prompted to access some of the following resources.

Crestron Support and Training

- Crestron True Blue Support
- Crestron Resource Library
- Crestron Online Help (OLH)
- Crestron Training Institute (CTI) Portal

Programmer and Developer Resources

- help.crestron.com: Provides help files for Crestron programming tools such as SIMPL, SIMPL#, and Crestron Toolbox™ software
- developer.crestron.com: Provides developer documentation for Crestron APIs, SDKs, and other development tools

Product Certificates

To search for product certificates, refer to support.crestron.com/app/certificates.

Related Documentation

- 4-Series Control Systems Reference Guide
- 4-Series Control Systems Security Reference Guide
- .AV Framework Software for 4-Series Control Systems Reference Guide
- Crestron Fusion® Software Help File
- Crestron Programming Design Guide
- XiO Cloud User Guide

This page is intentionally left blank.

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

Product Manual — Doc. 9227A

01/31/22
Specifications subject to
change without notice.