View this document in HTML
crestron.com/docs/8912

Product Manual

Crestron Virtual Control Server Software

Server-Based Control System

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.

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, 3-Series, .AV Framework, AirMedia, Cresnet, Crestron Fusion, Crestron Toolbox, DM, DM Lite, DM NVX, infiNET EX, Saros, and XiO Cloud are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Kensington is either a trademark or registered trademark of Acco Brands Corporation in the United States and/or other countries. Adobe and Flash are either trademarks or registered trademarks of Adobe in the United States and/or other countries. AlmaLinux OS is either a trademark or a registered trademark of the AlmaLinux OS Foundation in the United States and/or other countries. BACnet and the BACnet logo are either trademarks or registered trademarks of American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. in the United States and/or other countries. Apache is either a trademark or a registered trademark of The Apache Software Foundation in the United States and/or other countries. Safari is either a trademark or a registered trademark of Apple, Inc. in the United States and/or other countries. Ubuntu is either a trademark or a registered trademark of Canonical Ltd in the United States and/or other countries. Rocky Linux is either a trademark or a registered trademark of Ctrl IQ, Inc. in the United States and/or other countries. Dell and OptiPlex are either trademarks or registered trademarks of Dell, Inc. in the United States and/or other countries. Chrome is either a trademark or a registered trademark of Google, Inc. in the United States and/or other countries. HDMI is either a trademark or registered trademark of HDMI Licensing LLC in the United States and/or other countries. Intel and Intel Core are either trademarks or registered trademarks of Intel Corporation in the United States and/or other countries. Linux is either a trademark or a registered trademark of Linus Torvalds in the United States and/or other countries. MariaDB is either a trademark or a registered trademark of MariaDB in the United States and/or other countries. Active Directory, Azure, Microsoft, and Microsoft Edge are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Firefox is either a trademark or a registered trademark of the Mozilla Foundation in the United States and/or other countries. Mono is either a trademark or a registered trademark of Novell 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. Red Hat and Red Hat Enterprise Linux are either trademarks or registered trademarks of Red Hat, Inc. in the United States and/or other countries. USB Type-C is either a trademark or registered trademark of USB Implementers Forum, Inc. in the United States and/or other countries. VESA and DisplayPort are either trademarks or registered trademarks of Video Electronics Standards Association in the United States and/or other countries. Wireshark is either a trademark or a registered trademark of Wireshark Foundation 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.

©2024 Crestron Electronics, Inc.

Contents

Overview 1
Features 2
VC-4 Features 3
VC-4-PC-3 Features 5
VC-4-SERVER-25 Features 8
USB-OFFLINE Features 11
SW-VC4-BN-1000 Features 12
Application Scenarios 14
Medium Classroom with Crestron Virtual Control 14
Large Hybrid Classroom with Crestron Virtual Control 15
Huddle Room with Crestron Virtual Control and Ethernet Control Module 16
Small Conference Room with Crestron Virtual Control and Ethernet Control Module 17
Large Conference Room with Crestron Virtual Control and 3-Series® Control System Retrofit 18
Large Conference Room with Crestron Virtual Control and Ethernet Control Module 19
Specifications 20
VC-4 Specifications 21
Product Specifications 21
Scalable System Requirements 22
VC-4-PC-3 Specifications 24
VC-4-SERVER-25-Specifications 27
Product Specifications 27
USB-OFFLINE Specifications 29
Installation 30
VC-4 Installation 31
Prerequisites 32
Install the Crestron Virtual Control Package 33
Migrate from Another Linux Platform 36
Upgrade or Downgrade Crestron Virtual Control 39
Uninstall the Crestron Virtual Control Package 42
VC-4-PC-3 Installation 43
Install the VC-4-PC-3 44
Upgrade or Downgrade the VC-4-PC-3 45
VC-4-SERVER-25 Installation 48
Install the VC-4-SERVER-25 49
Upgrade or Downgrade the VC-4-SERVER-25 50
Configuration 53
Initial Setup 54
VC-4 Setup 55

VC-4-PC-3 Setup 61
VC-4-SERVER-25 Setup 76
Manage Licenses 92
Manage Licenses with XiO Cloud 93
Manage Licenses Offline 95
Web Configuration 101
Actions Menu 102
Status 107
Settings 126

Secure Deployment 137

Security Overview 137
Harden the Linux Platform 138
Harden the Crestron Virtual Control Software 139
Configure Secure Device Connections 139
Load TLS Certificates 140
Configure Secure Flash Policy Files 141
Configure File Access to Crestron Files 142
Configure OCSP Client Settings 143
Configure PAM Authentication 143
Configure Cgroup Settings 146

Reference Topics 148

Turn On Local System Logging 149
Opened Server Ports 151
Troubleshoot Room Addresses 152
Connect Devices across Subnets 153
Build a Custom VC-4 Computer 154
Connecting an HTML5 XPanel with Self-Signed Certificates 155

Resources 156

Crestron Support and Training 156
Programmer and Developer Resources 156
Product Certificates 156
Related Documentation 156

Overview

The Crestron Virtual Control server-based control system provides a scalable solution for deploying programs, rooms, and devices across an enterprise. The Crestron® control system infrastructure resides entirely on a remote server, which is installed and configured using supported Linux® operating system platforms. A micro computer option (VC-4-PC-3) is also available that comes with Crestron Virtual Control preinstalled and fully configured for small to medium-sized deployments.

This section provides the following information:

- Features on page 2
- Application Scenarios on page 14

Features

Refer to the following sections for more information on the features provided by various Crestron Virtual Control solutions.

This section provides the following information:

- VC-4 Features on page 3
- VC-4-PC-3 Features on page 5
- VC-4-SERVER-25 Features on page 8
- USB-OFFLINE Features on page 11
- SW-VC4-BN-1000 Features on page 12

VC-4 Features

Crestron Virtual Control software (VC-4) offers a centralized server-based alternative to individual hardware-based control systems. Crestron Virtual Control provides a scalable virtual control solution over a network. Per-room licensing (VC-4-ROOM) makes it easy to determine the number of licenses required for an installation.

Crestron
VIRTUAL CONTROL

Key features include:

- Offers a centralized server-based alternative to individual hardware-based control systems
- Provides a scalable virtual control platform
- Streamlines deployment, maintenance, and management
- Supports XiO Cloud® cloud-based monitoring
- Supports .AV Framework™ management solution
- Supports C#, SIMPL, and SIMPL# Pro programming
- Integrates directly with IP-controllable devices over the network
- Integrates with serial, IR, CEC, and other controllable devices via decentralized control ports on DM®, DM NVX®, and other Crestron® interfaces
- Native BACnet network/IP support
- Enables server redundancy for increased reliability
- Employs enterprise-grade security to ensure maximum reliability and privacy
- Per-room licensing makes it easy to determine the number of licenses required for an installation
- Online and offline licensing options available

Overview

Crestron® Virtual Control (VC-4) is a server-based control platform for enterprise applications that can be used in place of hardware-based Crestron control systems. The platform runs programs to control multiple rooms over the network from a single, centralized location. Cloud-based monitoring is available using the XiO Cloud® service. Crestron Virtual Control also provides native support for .AV Framework™ software, which is a web-based management solution that is used to deploy scalable Crestron enterprise room solutions without requiring any programming.

> **NOTE:** When running in a virtualized environment, Crestron Virtual Control can leverage the hypervisor's fault tolerance and high-availability features. If Crestron Virtual Control is installed on a bare-metal server (such as a standalone computer), it cannot leverage these features. If these features are desired, Crestron Virtual Control software must be installed in an existing virtualized environment that supports them.

Crestron Virtual Control can be integrated with a variety of devices, including audio, video, lighting, motorized shades, thermostats, door locks, sensors, and security systems. Connected devices can be controlled directly via Ethernet, and those that require a serial, IR, or other hardware interface can be integrated via decentralized control ports on a DM NVX® encoder/decoder, DM® transmitter or receiver, CEN-CI3-1-POE interface, or the CEN-IO wired and wireless series of I/O modules. Cresnet® network devices can be integrated via a DIN-CENCN-2-POE bridge, and wireless Crestron devices can also be integrated via an infiNET EX® wireless gateway. 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.[1]

Crestron Virtual Control supports server redundancy for increased reliability. For large buildings, Crestron Virtual Control streamlines deployment and maintenance by allowing a single program to be deployed across multiple rooms. Support for C#, SIMPL, and SIMPL#Pro programming languages gives programmers design flexibility and enables programs to be shared with hardware-based control systems.[2] Crestron Virtual Control also employs enterprise-grade security to ensure maximum reliability and privacy.

Crestron Virtual Control is sold through Authorized Crestron Dealers, and requires installation on a customer-supplied server running a supported Linux® server operating system.

Room Licensing

The Crestron Virtual Control licensing model is similar to a traditional hardware purchase model: purchase a specified number of room licenses (VC-4-ROOM), and the Crestron Virtual Control installation will run the number of rooms purchased. Each room license also includes one software mobility license (SW-MOBILITY) that enables functionality for various Crestron software solutions.

The VC-4 server provides two licensing options: online licensing via the XiO Cloud® service, or offline licensing via the USB-OFFLINE dongle.

- For online licensing via the XiO Cloud service, the VC-4 server requires access to XiO Cloud to validate its licenses. An active XiO Cloud account is required, subject to the terms of the Crestron Cloudware License.[3] However, a paid XiO Cloud subscription is not required to manage licenses for the VC-4 server. An XiO Cloud account is not required to run the VC-4 server during its 90-day trial period. Use the XiO Cloud account registration form to associate VC-4-ROOM licenses with an XiO Cloud account.
- For offline licensing via the USB-OFFLINE dongle, the dongle must be connected to the VC-4 server to validate its licenses. All room licenses must be ordered and the offline licensing form must be completed prior to validating licenses via the USB-OFFLINE dongle. For more information, refer to the Crestron Virtual Control Product Manual.

Notes:

1. BACnet network/IP support is required. The VC-4 server supports up to 100 BACnet objects by default. For systems with more than 100 objects, at least one SW-VC4-BN-1000 license must be purchased. For systems with more than 1000 objects, multiple SW-VC4-BN-1000 licenses must be purchased based on the total required objects. Licenses are validated within the XiO Cloud® service or via the USB-OFFLINE dongle. The VC-4 server supports a maximum of 10000 BACnet objects when dedicated for BACnet use only. Actual capabilities are contingent upon the overall program size and complexity.
2. Crestron Virtual Control does not support programs that were created using D3 Pro software.
3. The XiO Cloud® service is licensed under Crestron's Cloudware License Agreement, available at www.crestron.com/Legal/software-products-on-premises-and-cloudware/cloudware-license-agreement.

VC-4-PC-3 Features

The VC-4-PC-3 is a Dell® micro computer that comes with Crestron Virtual Control software preinstalled and fully configured. The VC-4-PC-3 includes three room licenses with purchase and is perfect for small to medium-sized deployments.



Key features include:

- Offers server-based control system software preinstalled on a micro computer
- Ideal for small to medium-sized deployments
- Employs a powerful Dell® micro computer
- Ships with Crestron Virtual Control software (VC-4) preinstalled and fully configured
- Provides a scalable virtual control platform
- Streamlines deployment, maintenance, and management
- Supports XiO Cloud® cloud-based monitoring
- Supports .AV Framework™ management solution
- Supports C#, SIMPL, and SIMPL# Pro programming
- Integrates directly with IP-controllable devices over the network

- Integrates with serial, IR, CEC, and other controllable devices via decentralized control ports on DM®, DM NVX®, and other Crestron® interfaces
- Native BACnet network/IP support
- Employs enterprise-grade security to ensure maximum reliability and privacy
- Includes three room licenses with purchase
- Online and offline licensing options available
- Includes external power adapter

Overview

The Crestron® VC-4-PC-3 is a powerful Dell® micro computer that comes with Crestron Virtual Control software (VC-4) preinstalled and fully configured. The VC-4-PC-3 is secured and ready for operation out of the box and only needs power and an Ethernet connection to function. Most standard Crestron Virtual Control functions and features are readily available without requiring any configuration or Linux® OS knowledge. The VC-4-PC-3 includes three room licenses with purchase and is perfect for small to medium-sized deployments.[1,2]

> **NOTE:** When running in a virtualized environment, Crestron Virtual Control can leverage the hypervisor's fault tolerance and high-availability features. The VC-4-PC-3 runs as a standalone computer and, therefore, cannot leverage these features. If these features are desired, Crestron Virtual Control software must be installed in an existing virtualized environment that supports them.

Crestron Virtual Control is a control platform for enterprise applications that can be used in place of hardware-based Crestron control systems. The platform runs programs to control multiple rooms over the network from a single, centralized location. Cloud-based monitoring is available using the XiO Cloud® service. Crestron Virtual Control also provides native support for .AV Framework™ software, which is a web-based management solution that is used to deploy scalable Crestron enterprise room solutions without requiring any programming.

Crestron Virtual Control can be integrated with a variety of devices, including audio, video, lighting, motorized shades, thermostats, door locks, sensors, and security systems. Connected devices can be controlled directly via Ethernet, and those that require a serial, IR, or other hardware interface can be integrated via decentralized control ports on a DM NVX® encoder/decoder, DM® transmitter or receiver, CEN-CI3-1-POE interface, or the CEN-IO wired and wireless series of I/O modules. Cresnet® network devices can be integrated via a DIN-CENCN-2-POE bridge, and wireless Crestron devices can also be integrated via an infiNET EX® wireless gateway. 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.[3]

Crestron Virtual Control streamlines deployment and maintenance by allowing a single program to be deployed across multiple rooms. Support for C#, SIMPL, and SIMPL#Pro programming languages gives programmers design flexibility and enables programs to be shared with hardware-based control systems.[4] Crestron Virtual Control also employs enterprise-grade security to ensure maximum reliability and privacy.

Room Licensing

The VC-4-PC-3 includes three room licenses with purchase.[2] Additional rooms can be added to the VC-4-PC-3 by purchasing the desired number of room licenses (VC-4-ROOM).

The VC-4-PC-3 provides two licensing options: online licensing via the XiO Cloud® service, or offline licensing via the USB-OFFLINE dongle.

- For online licensing via the XiO Cloud service, the VC-4-PC-3 requires access to XiO Cloud to validate its licenses. An active XiO Cloud account is required, subject to the terms of the Crestron Cloudware License.[5] However, a paid XiO Cloud subscription is not required to manage licenses for the VC-4-PC-3. Use the XiO Cloud account registration form to associate VC-4-ROOM licenses with an XiO Cloud account.
- For offline licensing via the USB-OFFLINE dongle, the dongle must be connected to the VC-4-PC-3 to validate its licenses. All room licenses must be ordered and the offline licensing form must be completed prior to validating licenses via the USB-OFFLINE dongle. For more information, refer to the Crestron Virtual Control Product Manual.

Notes:

1. For optimal performance, Crestron recommends running no more than 25 rooms and/or 250 devices on the VC-4-PC-3.
2. The three included room licenses must be requested and then validated within the XiO Cloud® service or via the USB-OFFLINE dongle. No rooms will run on the VC-4-PC-3 until the room licenses are requested and applied. Any additional room licenses (VC-4-ROOM) must be purchased separately.
3. BACnet network/IP support is required. The VC-4-PC-3 supports up to 100 BACnet objects by default. For systems with more than 100 objects, at least one SW-VC4-BN-1000 license must be purchased. For systems with more than 1000 objects, multiple SW-VC4-BN-1000 licenses must be purchased based on the total required objects. Licenses are validated within the XiO Cloud service or via the USB-OFFLINE dongle. The VC-4-PC-3 supports a maximum of 10000 BACnet objects when dedicated for BACnet use only. Actual capabilities are contingent upon the overall program size and complexity.
4. Crestron Virtual Control does not support programs that were created using D3 Pro software.
5. The XiO Cloud® service is licensed under Crestron's Cloudware License Agreement, available at www.crestron.com/Legal/software-products-on-premises-and-cloudware/cloudware-license-agreement.

VC-4-SERVER-25 Features

The VC-4-SERVER-25 provides server-based control system software preinstalled on a rack server. The VC-4-SERVER-25 is ideal for medium to large-sized deployments and includes 25 room licenses with purchase.



Key features include:

- Offers server-based control system software presintalled on a rack server
- Ideal for medium to large-sized deployments
- Employs a powerful Dell® rack server
- Ships with Crestron Virtual Control software (VC-4) preinstalled and fully configured
- Provides a scalable virtual control platform
- Streamlines deployment, maintenance, and management
- Supports XiO Cloud® cloud-based monitoring
- Supports .AV Framework™ management solution
- Supports C#, SIMPL, and SIMPL# Pro programming
- Integrates directly with IP-controllable devices over the network
- Integrates with serial, IR, CEC, and other controllable devices via decentralized control ports on DM®, DM NVX®, and other Crestron® interfaces
- Native BACnet network/IP support
- Dual solid state drives (SSD) and redundant power supplies provide increased reliability
- Employs enterprise-grade security to ensure maximum reliability and privacy
- Includes 25 room licenses with purchase
- Online and offline licensing options available

Overview

The Crestron® VC-4-SERVER-25 is a powerful Dell® rack server that comes with Crestron Virtual Control software (VC-4) preinstalled and fully configured. The VC-4-SERVER-25 is secured and ready for operation out of the box and only needs power and an Ethernet connection to function. Most standard Crestron Virtual Control functions and features are readily available without requiring any configuration or Linux® OS knowledge. The VC-4-SERVER-25 also provides dual solid state drives (SSD) and redundant power supplies for increased reliability. The VC-4-SERVER-25 includes 25 room licenses with purchase and is perfect for medium to large-sized deployments.[1]

NOTE: When running in a virtualized environment, Crestron Virtual Control can leverage the hypervisor's fault tolerance and high-availability features. The VC-4-SERVER-25 runs as a standalone computer and, therefore, cannot leverage these features. If these features are desired, Crestron Virtual Control software must be installed in an existing virtualized environment that supports them.

Crestron Virtual Control is a control platform for enterprise applications that can be used in place of hardware-based Crestron control systems. The platform runs programs to control multiple rooms over the network from a single, centralized location. Cloud-based monitoring is available using the XiO Cloud® service. Crestron Virtual Control also provides native support for .AV Framework™ software, which is a web-based management solution that is used to deploy scalable Crestron enterprise room solutions without requiring any programming.

Crestron Virtual Control can be integrated with a variety of devices, including audio, video, lighting, motorized shades, thermostats, door locks, sensors, and security systems. Connected devices can be controlled directly via Ethernet, and those that require a serial, IR, or other hardware interface can be integrated via decentralized control ports on a DM NVX® encoder/decoder, DM® transmitter or receiver, CEN-CI3-1-POE interface, or the CEN-IO wired and wireless series of I/O modules. Cresnet® network devices can be integrated via a DIN-CENCN-2-POE bridge, and wireless Crestron devices can also be integrated via an infiNET EX® wireless gateway. 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.[2]

Crestron Virtual Control streamlines deployment and maintenance by allowing a single program to be deployed across multiple rooms. Support for C#, SIMPL, and SIMPL#Pro programming languages gives programmers design flexibility and enables programs to be shared with hardware-based control systems.[3] Crestron Virtual Control also employs enterprise-grade security to ensure maximum reliability and privacy.

Room Licensing

The VC-4-SERVER-25 includes 25 room licenses with purchase.[1] Additional rooms can be added to the VC-4-SERVER-25 by purchasing the desired number of room licenses (VC-4-ROOM).

The VC-4-SERVER-25 provides two licensing options: online licensing via the XiO Cloud® service, or offline licensing via the USB-OFFLINE dongle.

- For online licensing via the XiO Cloud service, the VC-4-SERVER-25 requires access to XiO Cloud to validate its licenses. An active XiO Cloud account is required, subject to the terms of the Crestron Cloudware License.[4] However, a paid XiO Cloud subscription is not required to manage licenses for the VC-4-SERVER-25. Use the XiO Cloud account registration form to associate VC-4-ROOM licenses with an XiO Cloud account.
- For offline licensing via the USB-OFFLINE dongle, the dongle must be connected to the VC-4-SERVER-25 to validate its licenses. All room licenses must be ordered and the offline licensing form must be completed prior to validating licenses via the USB-OFFLINE dongle. For more information, refer to the Crestron Virtual Control Product Manual.

Notes:

1. The 25 included room licenses must be requested and then validated within the XiO Cloud® service or via the USB-OFFLINE dongle. No rooms will run on the VC-4-SERVER-25 until the room licenses are requested and applied. Any additional room licenses (VC-4-ROOM) must be purchased separately.
2. BACnet network/IP support is required. The VC-4-SERVER-25 supports up to 100 BACnet objects by default. For systems with more than 100 objects, at least one SW-VC4-BN-1000 license must be purchased. For systems with more than 1000 objects, multiple SW-VC4-BN-1000 licenses must be purchased based on the total required objects. Licenses are validated within the XiO Cloud service or via the USB-OFFLINE dongle. The VC-4-SERVER-25 supports a maximum of 10000 BACnet objects when dedicated for BACnet use only. Actual capabilities are contingent upon the overall program size and complexity.
3. Crestron Virtual Control does not support programs that were created using D3 Pro software.
4. The XiO Cloud® service is licensed under Crestron's Cloudware License Agreement, available at www.crestron.com/Legal/software-products-on-premises-and-cloudware/cloudware-license-agreement.

USB-OFFLINE Features



Overview

The Crestron® USB-OFFLINE is a USB dongle that provides a means for validating Crestron Virtual Control (VC-4) room licenses and BACnet licenses offline without requiring an XiO Cloud® service account. The USB-OFFLINE is ideal for Crestron Virtual Control installations that require offline licensing. The USB-OFFLINE is compatible with the VC-4-PC-3 Dell® micro computer, VC-4-SERVER-25 Dell rack server, or a standalone VC-4 server.

> **NOTE:** The VC-4 software must be upgraded to version 4.0000.00057 or later prior to using the USB-OFFLINE for offline licensing.

To use offline licensing, first order your VC-4-ROOM licenses, SW-VC4-BN-1000 BACnet licenses (if needed) and USB-OFFLINE dongle. Then, configure your Crestron Virtual Control installation for offline licensing, and complete the offline licensing form to receive an offline license key. This license key must be added to your Crestron Virtual Control installation via a provided utility while the USB-OFFLINE is connected. The Crestron Virtual Control installation will then run the number of licensed rooms and/or BACnet objects as long as the USB-OFFLINE is connected. For more information, refer to the Crestron Virtual Control Product Manual.

> **NOTE:** Adding room or BACnet licenses requires resubmitting the offline licensing form to receive a new offline license key. Room licenses and BACnet licenses do not share an offline license key. For Crestron Virtual Control installations that require both license types, two unique offline license keys must be requested and applied. Crestron Virtual Control can be configured to run in either online or offline licensing mode. Existing licenses must be deleted from the Crestron Virtual Control installation before switching licensing modes.

SW-VC4-BN-1000 Features

Overview

The Crestron® SW-VC4-BN-1000 BACnet license enables support for up to 1000 BACnet objects per license on a VC-4-PC-3 Dell® micro computer, VC-4-SERVER-25 Dell rack server, or a standalone VC-4 server. The SW-VC4-BN-1000 allows for all local devices to be connected to a Building Management System (BMS) via the BACnet protocol, as well as the ability to control all BMS devices from a touch screen.

Native BACnet Network/IP Interface

BACnet network/IP support for Crestron Virtual Control provides a scalable, IP-based platform for implementing fully-integrated building management and automation. Built-in BACnet network/IP support enables seamless integration with existing building management systems, including integrated control of lighting, shades, HVAC, A/V equipment, BMS, security, voice, and data. All systems run independently and communicate with each other on the same platform.

Licensing Options

Each Crestron Virtual Control installation supports up to 100 BACnet objects by default. For systems with more than 100 objects, at least one SW-VC4-BN-1000 license must be purchased. For systems with more than 1000 objects, multiple SW-VC4-BN-1000 licenses must be purchased based on the total required objects.

The Crestron Virtual Control installation provides two BACnet licensing options: online licensing via the XiO Cloud® service, or offline licensing via the USB-OFFLINE dongle.

- For online licensing via the XiO Cloud service, the Crestron Virtual Control installation requires access to XiO Cloud to validate its licenses. An active XiO Cloud account is required, subject to the terms of the Crestron Cloudware License.[1] However, a paid XiO Cloud subscription is not required to manage licenses for the Crestron Virtual Control installation. Use the XiO Cloud account registration form to associate SW-VC4-BN-1000 licenses with an XiO Cloud account.
- For offline licensing via the USB-OFFLINE dongle, the dongle must be connected to the Crestron Virtual Control installation to validate its licenses. All BACnet licenses must be ordered and the offline licensing form must be completed prior to validating licenses via the USB-OFFLINE dongle. For more information, refer to the Crestron Virtual Control Product Manual.

Maximum BACnet Objects

Crestron Virtual Control supports a maximum of 10000 BACnet objects. Actual capabilities are contingent upon the overall program size and complexity. These limits assume the Crestron Virtual Control installation is dedicated for BACnet use only with no other significant control system functions.

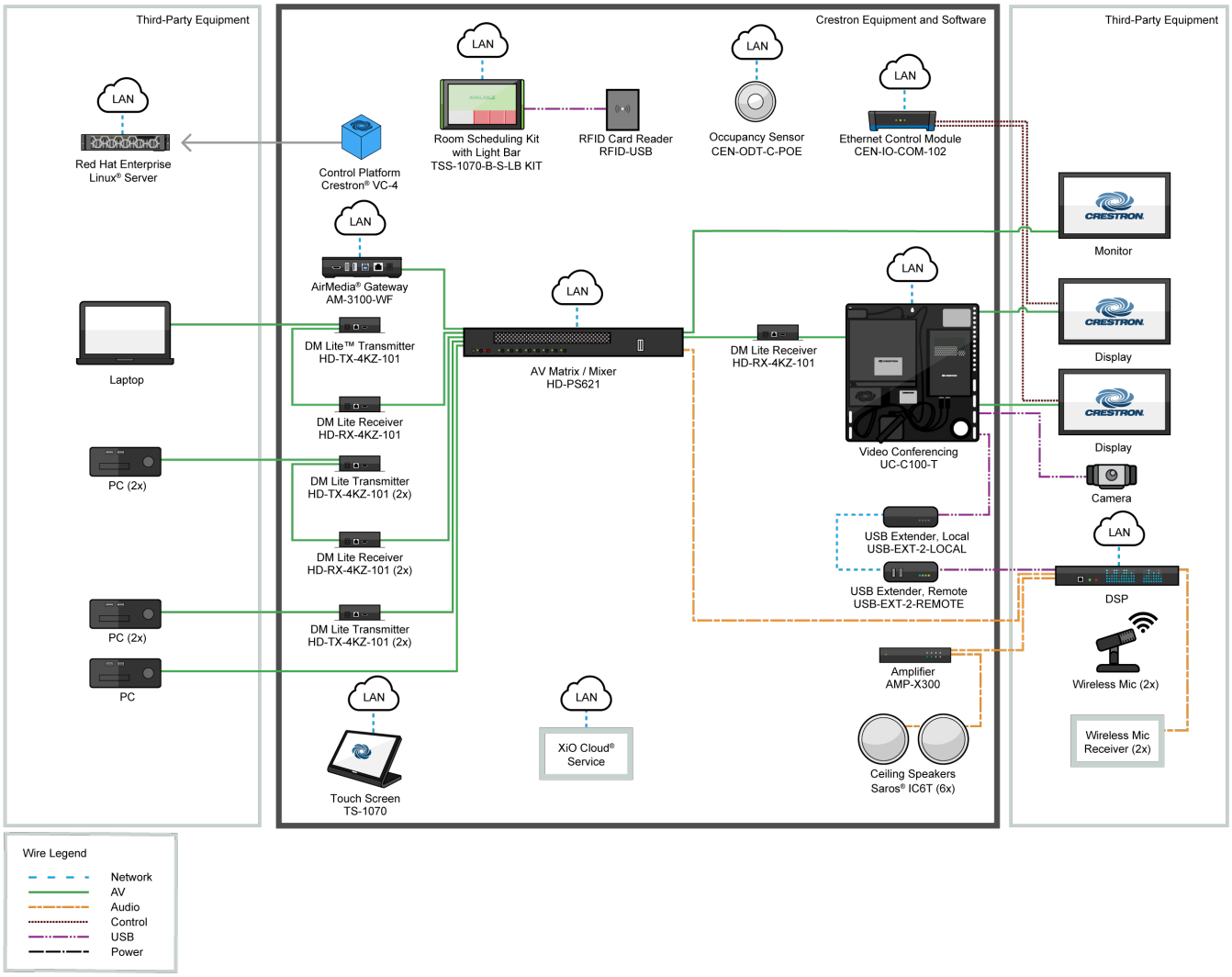
For more information, refer to the Crestron Device Library Help File.

Application Scenarios

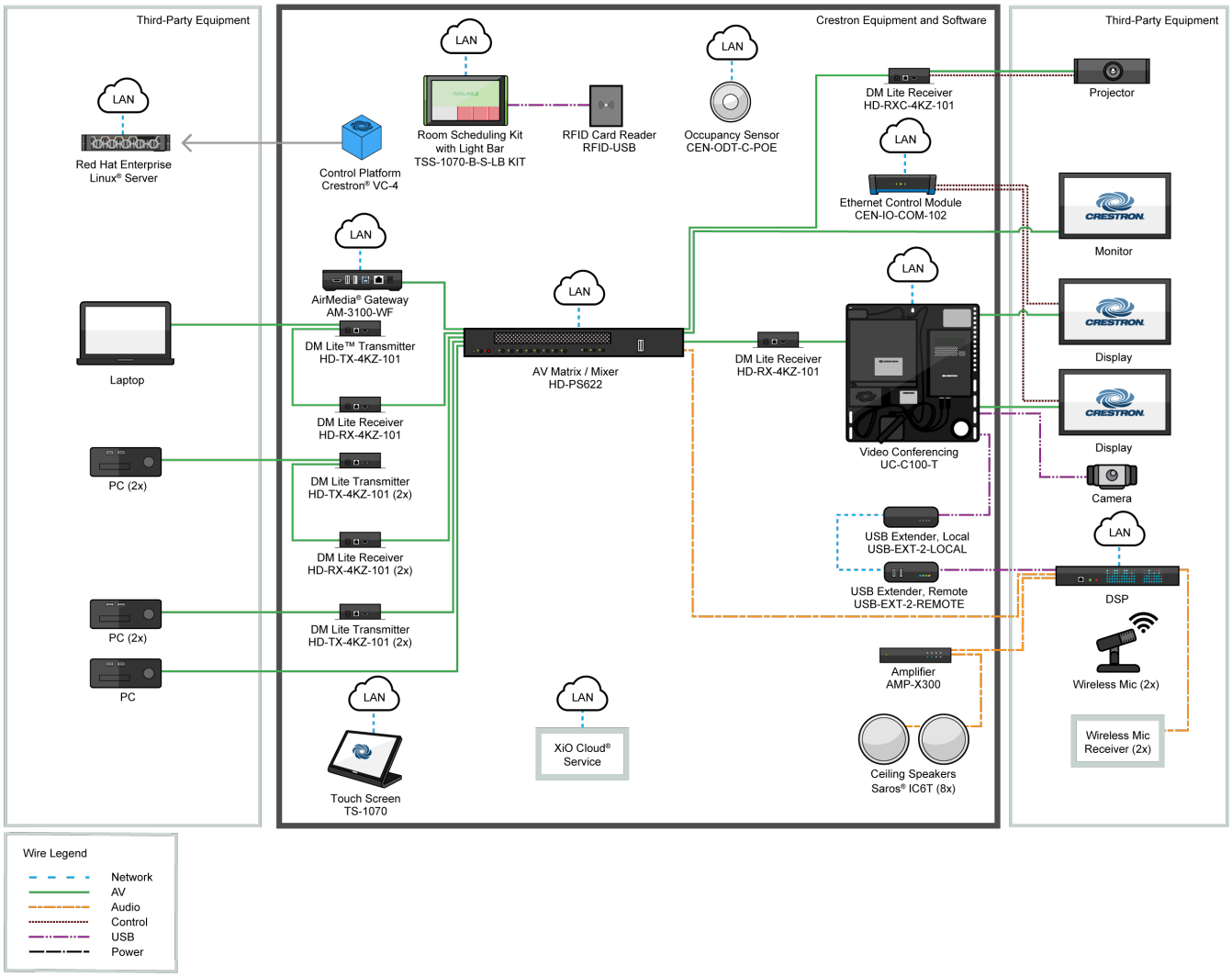
The following diagrams show various application scenarios for a Crestron Virtual Control server-based control system.

> **NOTE:** To download CAD block drawings for these application scenarios, refer to Resources on page 156.

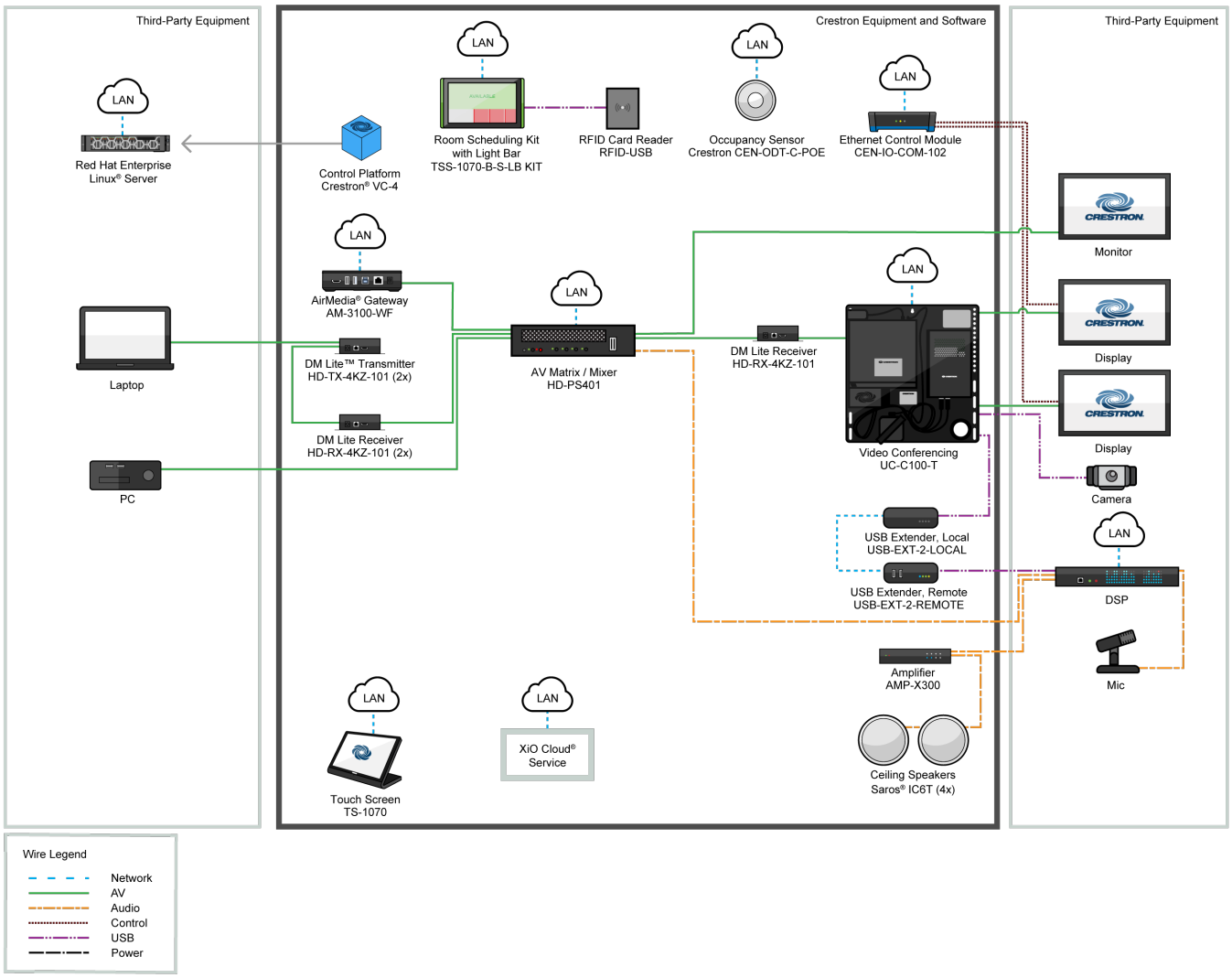
Medium Classroom with Crestron Virtual Control



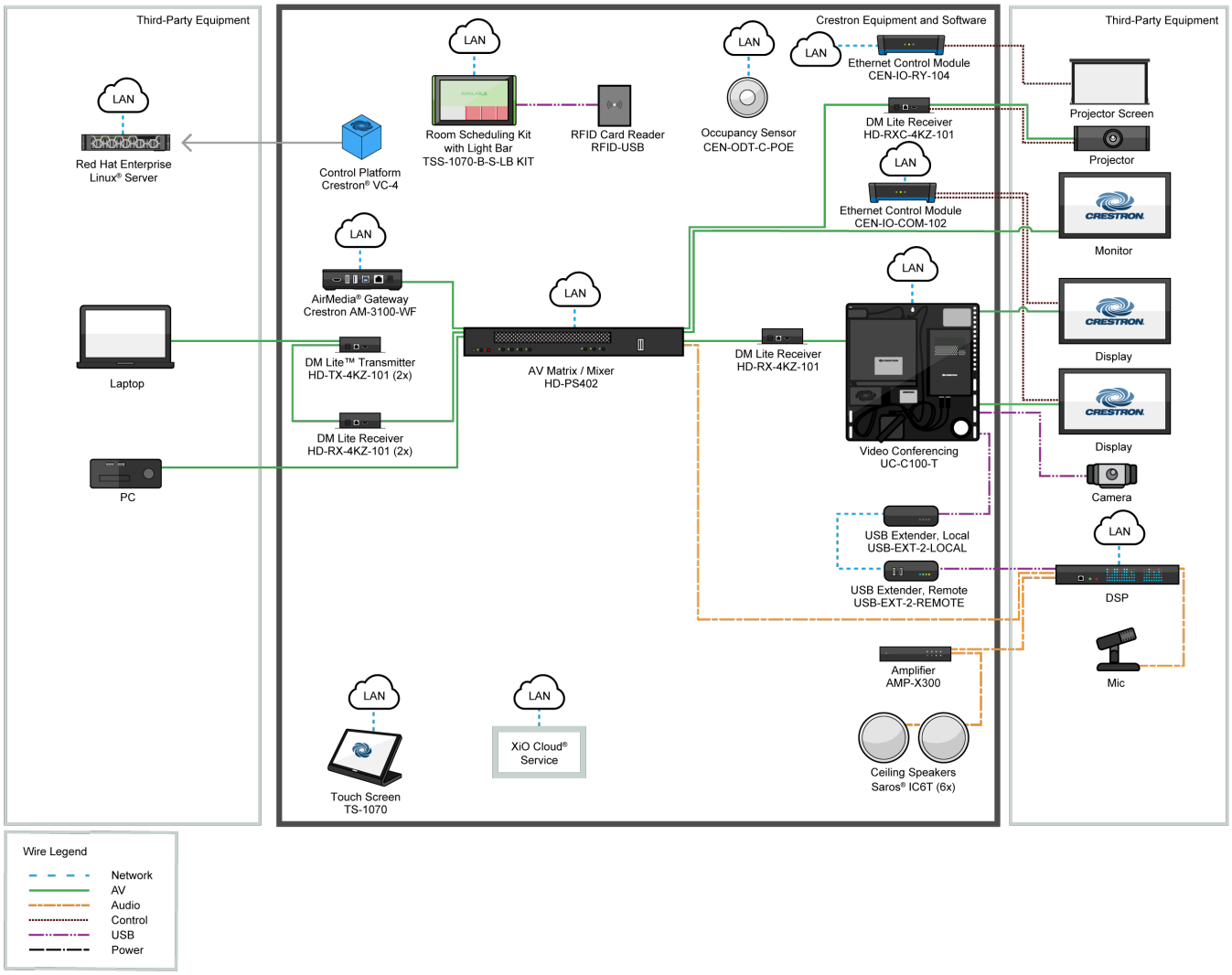
Large Hybrid Classroom with Crestron Virtual Control



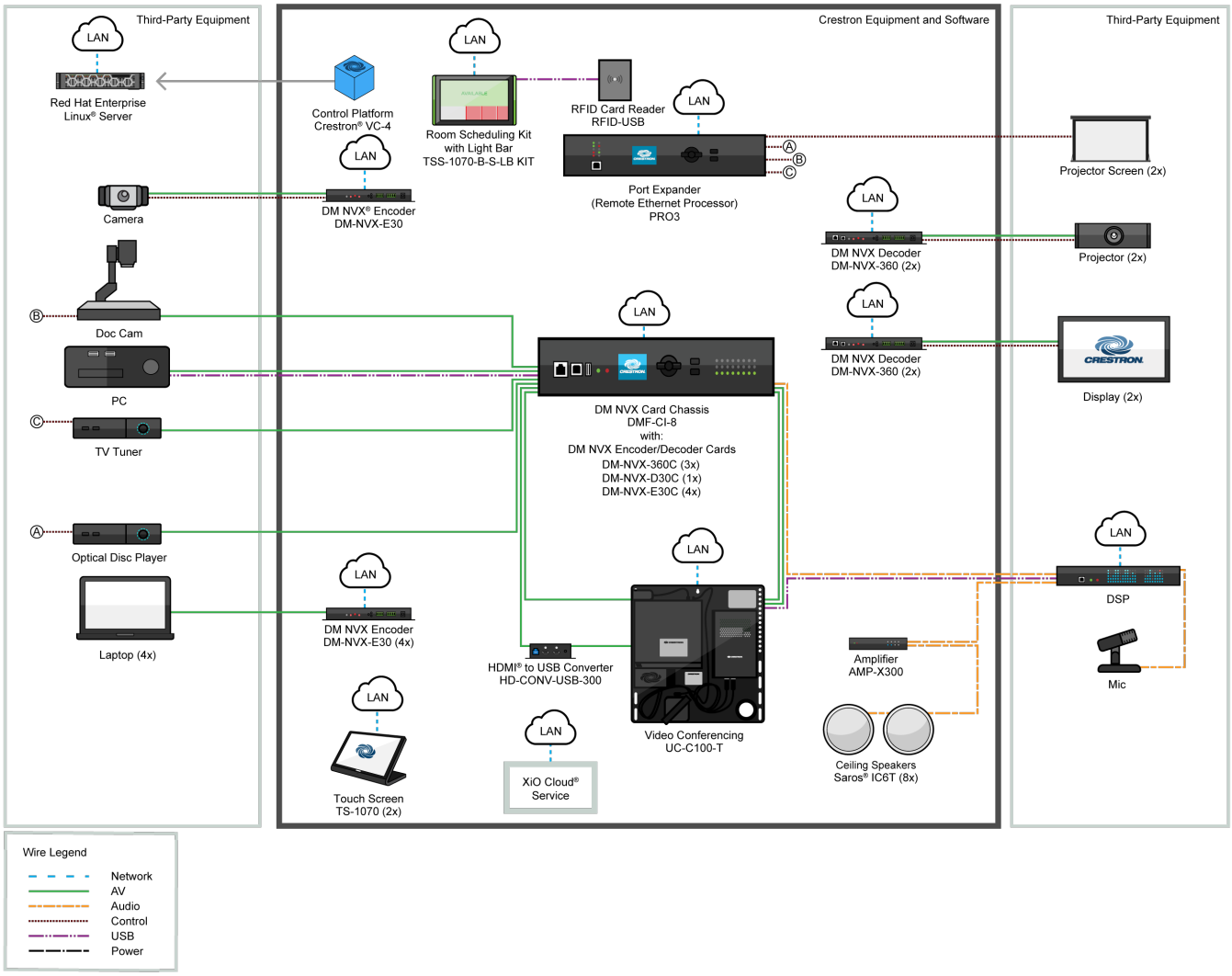
Huddle Room with Crestron Virtual Control and Ethernet Control Module



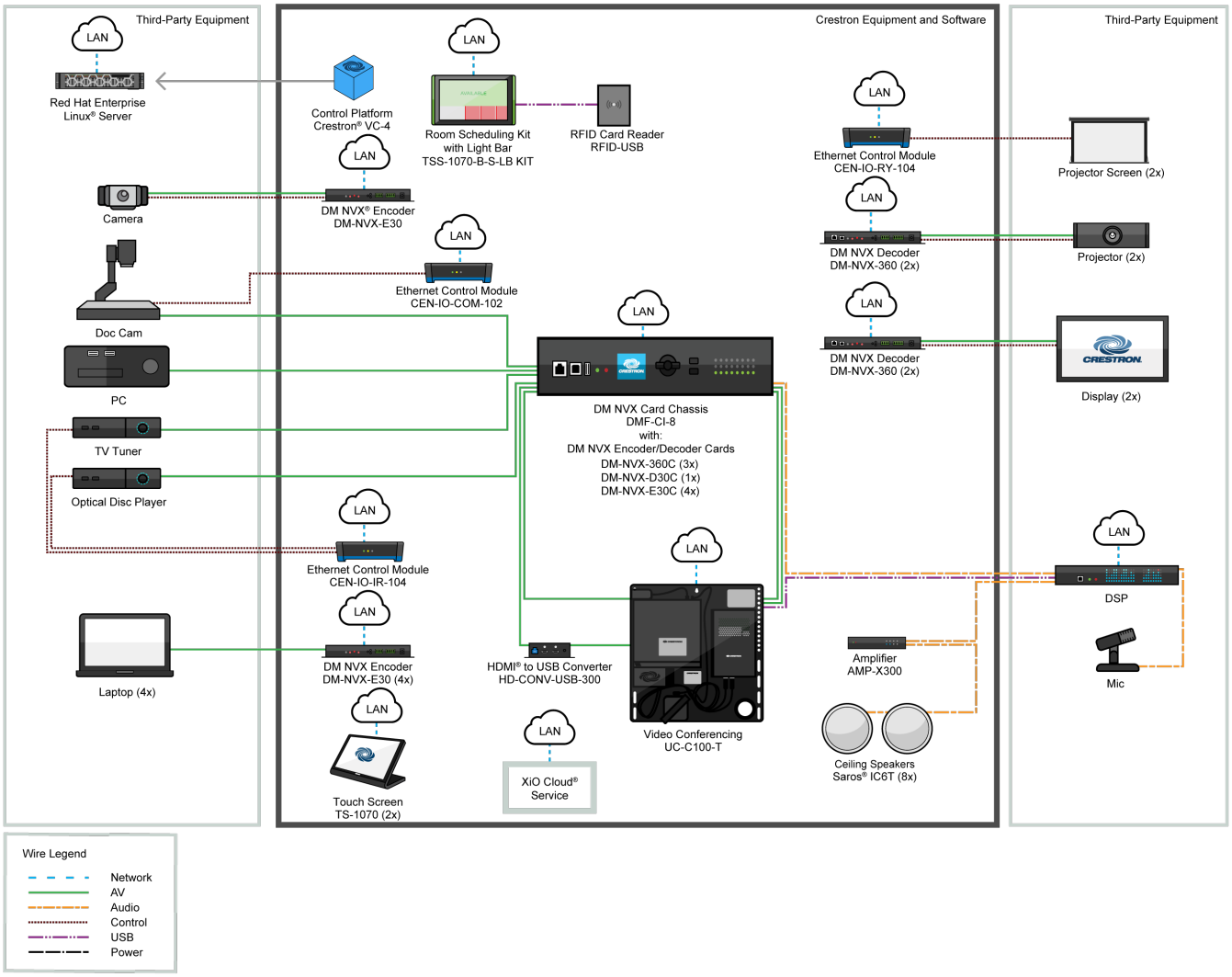
Small Conference Room with Crestron Virtual Control and Ethernet Control Module



Large Conference Room with Crestron Virtual Control and 3-Series® Control System Retrofit



Large Conference Room with Crestron Virtual Control and Ethernet Control Module



Specifications

Refer to the following sections for more information on the specifications for various Crestron Virtual Control solutions.

This section provides the following information:

- VC-4 Specifications on page 21
- VC-4-PC-3 Specifications on page 24
- VC-4-SERVER-25-Specifications on page 27
- USB-OFFLINE Specifications on page 29

VC-4 Specifications

Product specifications for VC-4 are provided below.

Product Specifications

Minimum Server Requirements

Operating System	Red Hat Enterprise Linux® 8.2 software (64-bit version) or greater; AlmaLinux OS® 8.3 software (64-bit version) or greater; Rocky Linux™ OS 8.4 software (64-bit version) or greater

> **NOTE:** Crestron Virtual Control also can be installed on a server running version 9.x of any of the operating systems above.

Network Interface	1 Gbps
Hard Drive	100 GB
Disk Space	100 GB

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

Scalable System Requirements

The number of CPU cores and the amount of RAM that is required to run the Crestron Virtual Control server varies depending on the number of rooms and the average number of devices per room that will be added to the server.

Use the tables below to determine how many CPU cores and how much RAM is required for operation based on the size of the deployment. If a row and column is grayed out, Crestron Virtual Control does not support the average devices per room for that room size at this time.

CPU Cores Required

	Average Devices Per Room																				
	5	10	20	30	40	50	60	70	80	90	100	110	120	130	140	150	160	170	180	190	200
1	2	2	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
2	2	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
5	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	8	8	8
10	4	4	4	4	4	4	4	4	4	8	8	8	8	8	8	8	8	8	8	16	16
20	4	8	8	8	8	8	8	8	8	16	16										
25	4	8	8	8	8	8	8	8	16												

	Average Devices Per Room																		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
50	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	8	8	8
100	4	4	4	4	4	4	4	4	4	8	8	8	8	8	8	8	8	8	16	16
200	4	4	4	4	8	8	8	8	8	16										
300	4	4	8	8	8	8														
400	4	4	8	8	16															
500	4	8	8	16																

RAM (GB) Required

	Average Devices Per Room																				
	5	10	20	30	40	50	60	70	80	90	100	110	120	130	140	150	160	170	180	190	200
1	2	2	2	4	4	4	4	4	4	4	4	8	8	8	8	8	8	8	8	8	8
2	2	2	4	4	4	4	8	8	8	8	8	8	8	8	8	16	16	16	16	16	16
5	2	4	4	8	8	8	16	16	16	16	16	32	32	32	32	32	32	32	32	32	32
10	4	4	8	16	16	16	32	32	32	32	32	32	64	64	64	64	64	64	64	64	64
20	4	8	16	32	32	32	64	64	64	64	64										
25	8	8	16	32	32	64	64	64	64												

	Average Devices Per Room																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
50	4	4	8	8	8	16	16	16	16	16	32	32	32	32	32	32	32	32	32	32
100	4	8	16	16	16	32	32	32	32	32	32	64	64	64	64	64	64	64	64	64
200	8	16	32	32	32	64	64	64	64	64										
300	16	32	32	64	64	64														
400	16	32	64	64	64															
500	16	32	64	64																

Notes:

1. BACnet network/IP support is required. The VC-4 server supports up to 100 BACnet objects by default. For systems with more than 100 objects, at least one SW-VC4-BN-1000 license must be purchased. For systems with more than 1000 objects, multiple SW-VC4-BN-1000 licenses must be purchased based on the total required objects. Licenses are validated within the XiO Cloud® service or via the USB-OFFLINE dongle. The VC-4 server supports a maximum of 10000 BACnet objects when dedicated for BACnet use only. Actual capabilities are contingent upon the overall program size and complexity.
2. Crestron Virtual Control does not support programs that were created using D3 Pro software.
3. The XiO Cloud® service is licensed under Crestron's Cloudware License Agreement, available at www.crestron.com/Legal/software-products-on-premises-and-cloudware/cloudware-license-agreement.

VC-4-PC-3 Specifications

Product specifications for VC-4-PC-3 are provided below.

Computer

Model	Dell® OptiPlex® 7080 Micro Desktop computer
Processor	Intel Core® i5-10500T CPU @ 2.30GHz
RAM	8 GB DDR4 2666MT/s
Storage	256 GB SSD
Graphics	Intel® UHD Graphics 630
Network	Intel I219-LM 100/1000 Mbps Ethernet
Operating System	AlmaLinux OS® 8.6 software

Communications

Ethernet	100/1000 Mbps
USB	USB 3.2 and 2.0 host ports for mouse and keyboard (used for optional configuration through command line interface)
BACnet Network/IP	Supports up to 10000 BACnet objects[3]

Buttons and Indicators

Power	(1) Push button with LED backlight; For power on/off and reset
LAN	(2) LEDs on LAN port; Indicate Ethernet link status and activity

Connectors

Audio (Front)	(1) 3.5 mm universal audio connector (not used)
Line-Out (Front)	(1) 3.5 mm line-out audio connector (not used)
USB-C (Front)	(1) USB Type-C® 3.2 (Gen 2) connector, female (not used)
SSUSB 3.2 Gen 2 (Front)	(1) USB Type-A 3.2 (Gen 2) connector, with PowerShare, female; Connects to a keyboard or mouse for optional command line configuration
Antenna	(2) Wireless antenna slots; Includes one attached wireless antenna (not used)
HDMI	(1) HDMI® connector, female; Connects to a monitor for optional command line configuration
LAN	(1) 8-pin RJ-45 connector, female; 100BASE-TX/1000BASE-T Ethernet port
SSUSB 3.2 Gen 1	(2) USB Type-A 3.2 (Gen 1) connectors, female; Provides one port with Smart Power; Connects to a keyboard or mouse for optional command line configuration

SSUSB 3.2 Gen 2	(2) USB Type-A 3.2 (Gen 2) connectors, female; Connects to a keyboard or mouse for optional command line configuration
Kensington Lock	(1) Slot for optional Kensington® lock
DisplayPort	(2) DisplayPort™ 1.4 connectors, female; Connects to a monitor for optional command line configuration
19.5VDC	(1) DC power connector; 19.5VDC power input; For included power adapter

Power

Power Adapter (Included)	Input: 100–240VAC, 50/60 Hz; Output: 130 W @ 19.5V

Environmental

Operating Temperature	50 to 95°F (10 to 35°C)
Storage Temperature	-40 to 149°F (-40 to 65°C)
Heat Dissipation	42.9 BTU/hr (short idle)

Construction

Enclosure	Metal, plastic
Mounting	Freestanding, optional VESA® mount and Kensington® lock capabilities

Dimensions

Height	1.40 in. (36 mm)
Width	7.20 in. (183 mm)
Depth	7.00 in. (178 mm)

Weight

2.87 lb (1.30 kg)

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

Notes:

1. For optimal performance, Crestron recommends running no more than 25 rooms and/or 250 devices on the VC-4-PC-3.
2. The three included room licenses must be requested and then validated within the XiO Cloud® service or via the USB-OFFLINE dongle. No rooms will run on the VC-4-PC-3 until the room licenses are requested and applied. Any additional room licenses (VC-4-ROOM) must be purchased separately.
3. BACnet network/IP support is required. The VC-4-PC-3 supports up to 100 BACnet objects by default. For systems with more than 100 objects, at least one SW-VC4-BN-1000 license must be purchased. For systems with more than 1000 objects, multiple SW-VC4-BN-1000 licenses must be purchased based on the total required objects. Licenses are validated within the XiO Cloud service or via the USB-OFFLINE dongle. The VC-4-PC-3 supports a maximum of 10000 BACnet objects when dedicated for BACnet use only. Actual capabilities are contingent upon the overall program size and complexity.
4. Crestron Virtual Control does not support programs that were created using D3 Pro software.
5. The XiO Cloud® service is licensed under Crestron's Cloudware License Agreement, available at www.crestron.com/Legal/software-products-on-premises-and-cloudware/cloudware-license-agreement.

VC-4-SERVER-25-Specifications

Product specifications for VC-4-SERVER-25 are provided below.

Product Specifications

Computer

Model	Dell® PowerEdge® R350 Rack Server
Processor	Intel® Xeon® E2378G CPU @ 2.8G0hz, 16 M Cache
RAM	128 GB DDR4, 4x32 GB UDIMM, 3200MT/s ECC
Storage	960 GB SSD, RAID 1 Configured
Network	Broadcom® 5720 100/1000 Mbps Ethernet
Operating System	AlmaLinux OS® 9.2 software

Communications

Ethernet	100/1000 Mbps
USB	USB 3.2 and 2.0 host ports for mouse and keyboard (used for optional configuration through command line interface)
BACnet Network/IP	Supports up to 10000 BACnet objects[3]

Buttons and Indicators

Power	(1) Push button with LED backlight; For power on/off and reset
LAN	(2) LEDs on LAN port; Indicate Ethernet link status and activity

Connectors

iDRAC Direct (Front)	(1) USB Micro-AB connector, female
USB 2.0 (Front)	(1) USB Type-A 2.0 connector, female; Connects to a keyboard or mouse for optional command line configuration
VGA	(1) DB-15 VGA connector, female; Connects to a monitor for optional command line configuration
LAN	(1) 8-pin RJ-45 connector, female; 100BASE-TX/1000BASE-T Ethernet port
SSUSB 3.0	(1) USB Type-A 3.0 (Gen 1) connector, female; Connects to a keyboard or mouse for optional command line configuration
USB 2.0	(1) USB Type-A 2.0 connector, female; Connects to a keyboard or mouse for optional command line configuration
IEC Connector	(1) VDC power connector; 110/220 VDC Dual Voltage power input
SFP+	(2) SFP+ ports; 1000BASE-X/10GBASE-X Ethernet ports

Power

Main Power	Input: 100–240VAC, 50/60 Hz; Output: 600 W @ 240V

Environmental

Operating Temperature	50 to 95°F (10 to 35°C)
Storage Temperature	-40 to 149°F (-40 to 65°C)
Heat Dissipation	2250 BTU/hr (maximum)

Construction

Enclosure	Metal, plastic
Mounting	1 RU 19 in. rack-mountable

Dimensions

Height	1.69 in. (43 mm)
Width	18.98 in. (482 mm)
Depth	23.58 in. (599 mm)

Weight

23.96 lb (13.14 kg)

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

USB-OFFLINE Specifications

Product specifications for USB-OFFLINE are provided below.

Environmental

Temperature	-13 to 185°F (-25 to 85°C)
Humidity	0% to 95% RH (noncondensing)

Dimensions

Height	0.31 in. (8 mm)
Width	0.63 in. (16 mm)
Depth	1.61 in. (41 mm)

Weight

0.22 oz (6.24 g)

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

Installation

Refer to the following sections for instructions on how to install various Crestron Virtual Control solutions.

This section provides the following information:

- VC-4 Installation on page 31
- VC-4-PC-3 Installation on page 43
- VC-4-SERVER-25 Installation on page 48

VC-4 Installation

Use the following procedures to install Crestron Virtual Control software (VC-4) onto a Linux platform.

These procedures assume that the Linux server platforms have already been installed and meet or exceed the specifications described in Prerequisites on page 32. The subscription manager for the Linux server platform must also be configured prior to installation.

This section provides the following information:

- Prerequisites on page 32
- Install the Crestron Virtual Control Package on page 33
- Migrate from Another Linux Platform on page 36
- Upgrade or Downgrade Crestron Virtual Control on page 39
- Uninstall the Crestron Virtual Control Package on page 42

Prerequisites

Ensure the following prerequisites are met prior to installing the Crestron Virtual Control server.

> **NOTE:** Crestron Virtual Control is software that runs on a customer-supplied Linux server. Crestron is responsible for keeping the Crestron Virtual Control software up to date and will provide security patches when necessary. Crestron is not responsible for any custom security configurations that may be required for your Crestron Virtual Control deployment.

- The IT administrator (installer) has a working knowledge of Linux platforms and commands.
- The IT administrator is responsible for the following tasks:
  - Keeping the server operating system up to date
  - Ensuring the server is compliant with current security standards.
  - Integrating the server in the corporate authentication provider (LDAP, Active Directory® service, OAuth, and others)
  - Configuring user access to the server
  - Configuring the web servers, including the rights to the path of the Crestron Virtual Control web user interface pages.
- One of the following Linux platforms is installed on a physical or virtual machine:

  > **NOTE:** Installation on a virtual machine is recommended.

  - Red Hat Enterprise Linux® Server 8.2 software (64-bit version) or greater
  - AlmaLinux OS® Server 8.3 software (64-bit version) or greater
  - Rocky Linux™ Server 8.4 software (64-bit version) or greater

  > **NOTE:** Crestron Virtual Control also can be installed on a server running version 9.x of any of the operating systems above.

- The server meets the following requirements after the Linux platform has been installed:
  - **CPU**: 4 Cores or higher
  - **RAM**: 4 GB or higher
  - **Disk space**: 100 GB or higher
- The server must be dedicated to run the Crestron Virtual Control service only.
- The server must be able to run the Apache® 2.4.37 (or later) web server, which is installed as part of the Crestron Virtual Control installation package.
- For Red Hat Enterprise Linux installations, the Red Hat® server must be registered with www.redhat.com.

Install the Crestron Virtual Control Package

To install the Crestron Virtual Control package onto the Linux platform:

> **NOTE:** The Crestron Virtual Control package generates self-signed certificates during installation, which are available at **<installation_path>/virtualcontrol/data/ssl/certs/**. These certs are used to establish secure connections with connected devices. Additionally, all certificates provided by https://curl.se/ca/cacert.pem will be installed at **/etc/ssl/certs**.

1. Download the latest Crestron Virtual Control file package from the **Software & Firmware** resource page at www.crestron.com/Support/Resource-Library.
2. Log into an account with sudo privileges on the Linux platform where the Crestron Virtual Control package will be installed.
3. Copy the package ZIP file to a location on the Linux platform.

   > **NOTE:** Do not unzip the Crestron Virtual Control package before copying it to the Linux platform. The installation script cannot be executed if the package is unzipped prior to it being copied.

4. Open a new terminal window.
5. Change directories to the location of the ZIP file, and then issue the following command to unzip the package, where `<version>` is the version number of the package file:

   ```
   sudo unzip virtualcontrol-<version>.zip
   ```

6. Change directories to the location of the unzipped package file (`vc-4`).
7. Issue the following command to start the installation. The script installs any RPM file dependencies prior to running the Crestron Virtual Control RPM file.

   ```
   sudo ./installVC4.sh
   ```

8. Enter `y` when prompted to confirm the installation.
9. When prompted, indicate whether you are migrating your Crestron Virtual Control installation from another Linux platform (enter `y`) or not (enter `n`).

   > **NOTE:** When migrating from one Linux platform to another, Crestron Virtual Control must be installed in the same path on the new platform as it was on the original platform.

   The remaining procedures describe the installation process for a new Crestron Virtual Control server instance.

NOTE: Crestron provides a migration file that is required to migrate data from an existing Crestron Virtual Control server to a different Linux platform. For example, this file can be used to migrate Crestron Virtual Control data from an Ubuntu® server platform to Red Hat. For more information on the migration file and installation, refer to Migrate from Another Linux Platform on page 36.

10. When prompted, set the directory where Crestron Virtual Control applications will be installed. Press **Enter** to use the default directory (`/opt/crestron`).

    NOTE: Crestron Virtual Control cannot be installed in the **/home** directory.

11. When prompted, set the following port numbers that are used by various Crestron Virtual Control processes:
    a. Set the Redis port number. Redis is used as a database for Crestron Virtual Control processes. Press **Enter** to use the default Redis port value.
    b. Set the CIP (Crestron Internet Protocol) port number. Press **Enter** to use the default port value (41794).
    c. Set the Secure CIP port number. Press **Enter** to use the default port value (41796).
    d. Set the secure WebSocket port number. Press **Enter** to use the default port value (49200).
    e. Set the SIMPL debugger port number. Press **Enter** to use the default port value (49300).
    f. Set the BACnet port number. Press **Enter** to use the default port value (47808).

    NOTE: If any custom ports are specified for the Crestron Virtual Control installation, the port (s) must be opened manually within the firewall on the Linux server.

12. Enter the root account password when prompted to have the Crestron Virtual Control installer check whether the MariaDB® database server is installed. The MariaDB database server is installed automatically if it is not already. If the root account password is not set, you will be prompted to create and confirm a password.

    NOTE: MariaDB is a scalable database server used by the Crestron Virtual Control server to turn data into structured information.

13. Enter a name to use for the Crestron Virtual Control database. Press **Enter** to use the default database name (`VirtualControl`).
14. Enter a username to use for the Crestron Virtual Control account. Press **Enter** to use the default username (`virtualcontrol`).
15. Enter a password for the Crestron Virtual Control account. Press **Enter** to use the default password (random string).

16. Navigate to **/etc/snmp/**, open the **snmpd.conf** file in a text editing program, and add the following two lines to the end of the file. This prevents a "Warning: Failed to connect to the agentx master agent ([NIL]) SNMP" message from displaying when running the service.

```
master agentx
agentXSocket tcp:localhost:705
```

17. Issue the following SNMPD commands to ensure the service restarts without the warning message after rebooting the Linux server:
    a. Issue `sudo systemctl restart snmpd` to restart the SNMPD service and to apply the conf file changes.
    b. Issue `sudo systemctl enable snmpd.service` to enable the SNMPD service.
    c. Issue `sudo systemctl start snmpd.service` to start the SNMPD service.
18. Restart the Red Hat server.

After restarting, the Crestron Virtual Control service starts automatically within 2 to 3 minutes. The following commands may be issued while the Crestron Virtual Control service is running:

- To check the status of the Crestron Virtual Control service while it is running, issue `sudo systemctl status virtualcontrol`.
- To restart the Crestron Virtual Control service, issue `sudo systemctl restart virtualcontrol`.

  > **NOTE:** After a restart, wait 2 to 3 minutes for the service to initialize before attempting to access the web configuration interface.

- To stop the Crestron Virtual Control service, issue `sudo systemctl stop virtualcontrol`.

Migrate from Another Linux Platform

This section provides procedures needed to migrate an existing Crestron Virtual Control installation to a different Linux platform. For example, this file can be used to migrate Crestron Virtual Control data from an Ubuntu® server platform to Red Hat Enterprise Linux® server platforms.

Generate a Data Backup

Crestron provides a migration script file that is used to take the data from an existing Crestron Virtual Control installation and to package it into a ZIP file. This ZIP file is then used to import the Crestron Virtual Control data during a fresh installation on another Linux platform.

> **NOTE:** The migration script creates a backup of all rooms, programs, and settings on the Linux server. For security reasons, x.509 keys and certificates are not backed up. This script can be run while rooms are running.

To generate a backup of existing Crestron Virtual Control data:

1. Download the latest Crestron Virtual Control installation package (**virtualcontrol-[version].zip**) from www.crestron.com/Support/Resource-Library.
2. Extract the **migration_script.sh** file from the installation package and copy it to the Linux server platform where Crestron Virtual Control is currently installed.
3. Open a new terminal window.
4. Issue the `sudo bash migration_script.sh <password>` command, where `<password>` is the password that will be used for password protection of the generated ZIP file.

Upon a successful execution of the command, a MariaDB® software backup of the Crestron Virtual Control installation is created. The path of the ZIP file is shown in the terminal.

```
Created Maria DB Backup
Migration Backup (/home/builduser/VC_Migration_Backup_10202020_173859.zip) created Successfully
```

Import the Backup to a New Installation

Once a ZIP file has been generated using the migration script file, it can be transferred to the Linux platform where the new Crestron Virtual Control installation will occur.

> **NOTE:** When migrating from one Linux platform to another, Crestron Virtual Control must be installed in the same path on the new platform as it was on the original platform.

To import the backup files during a new Crestron Virtual Control installation:

1. Copy the ZIP file generated in Generate a Data Backup on page 36 to a location on the Linux platform where Crestron Virtual Control will be installed.

2. Begin the Crestron Virtual Control installation process as described in Install the Crestron Virtual Control Package on page 33. The following prompt is displayed at the beginning of the installation:

```
Are you migrating VC4 from another build?  (Y/N) :
```

3. Type `y` and press **Enter**.
4. When prompted, enter the ZIP file name and its path (for example, `/home/builduser/VC_Migration_Backup_10202020_173859.zip`).

   If the file is found, the terminal responds with `Migration File found` and `Restoring Files from Backup` messages.

5. When prompted, enter the password used to protect the ZIP file (as created in step 3 of Generate a Data Backup on page 36.

If authentication is successful, the installation continues as described in Install the Crestron Virtual Control Package on page 33.

Reassign Room Licenses in XiO Cloud

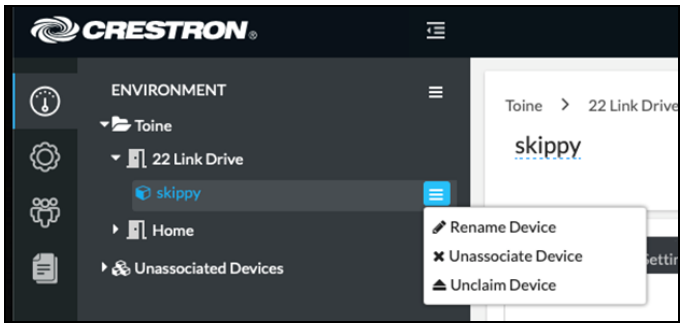
When migrating Crestron Virtual Control data from one Linux server to another, the room licenses assigned to the existing Linux server must be removed and added to the new server using the XiO Cloud® service. This is accomplished by unclaiming the existing Linux server from your XiO Cloud account.

> **NOTE:** If using the USB-OFFLINE to validate Crestron Virtual Control room licenses offline, the USB-OFFLINE can be moved between Linux servers without requiring a new offline license key. For more information on offline licensing, refer to Manage Licenses Offline on page 95.

To unclaim the existing Linux server:

1. Log into the XiO Cloud service as described in the XiO Cloud Service User Guide.
2. Navigate to the original Linux server in the **ENVIRONMENT** menu tree.
3. Position the cursor over the server in the **ENVIRONMENT** menu to reveal its context menu.
4. Select the context menu button of the server to display a drop-down menu.

   XiO Cloud - Device Drop-Down Menu



5. Select **Unclaim Device**. A confirmation dialog box is displayed.
6. Select **Yes** to unclaim the server.

Once the existing server is unclaimed, it is removed from your XiO Cloud account and all Crestron Virtual Control room licenses assigned to that server return to the account's license pool. From there, claim the new Linux server to the XiO Cloud service and assign the floating Crestron Virtual Control room licenses to the server as described in the XiO Cloud Service User Guide.

NOTE: Change the host name or IP address of the new Linux server to the host name of the existing Linux server and restart. Any connected devices will connect to the new server automatically and rooms will function normally.

Upgrade or Downgrade Crestron Virtual Control

The following procedures describe how to upgrade or downgrade Crestron Virtual Control on a Linux server.

Upgrade Crestron Virtual Control

When a new version of the Crestron Virtual Control service is available, a notification is displayed on the top of the web user interface.

Web User Interface - Update Notification



To upgrade the Crestron Virtual Control service on the Linux platform:

CAUTION: Ensure that all custom configuration files are backed up prior to upgrading the Crestron Virtual Control service, as any previous configurations will be overwritten.

1. Download the Crestron Virtual Control file package from the **Software & Firmware** resource page at www.crestron.com/Support/Resource-Library.
2. Log into an account with sudo privileges on the Linux platform where the Crestron Virtual Control package is installed.
3. Copy the package ZIP file to a location on the Linux platform.

   NOTE: Do not unzip the Crestron Virtual Control package before copying it to the Linux platform. The installation script cannot be executed if the package is unzipped prior to it being copied.

4. Open a new terminal window.
5. Change directories to the location of the ZIP file, and then issue the following command to unzip the package, where `<version>` is the version number of the package file:

   ```
   sudo unzip virtualcontrol-<version>.zip
   ```

6. Change directories to the location of the unzipped package file (`vc-4`).
7. Issue the following command to start the installation. The script installs any RPM files that are dependencies for the installation prior to running the Crestron Virtual Control RPM file.

   ```
   sudo ./installVC4.sh
   ```

8. Enter `y` when prompted to confirm the upgrade.

The upgrade may take up to 15 minutes to complete. Once the upgrade has completed, the Crestron Virtual Control service starts automatically within 2 to 3 minutes.

NOTE: Before accessing the web configuration interface following an upgrade, close and reopen any browser windows that were previously running the interface. If the browser window is not closed following an upgrade, the interface may not update to the latest version until the browser cache is cleared. For more information, refer to Initial Setup on page 54.

Upgrade with Red Hat Enterprise Linux 9.x

If the Linux® operating system must be upgraded from Red Hat Enterprise Linux® server version 8.x to 9.x, Crestron Virtual Control cannot be upgraded without performing the following procedure first. This scenario also applies to AlmaLinux OS® and Rocky Linux™ server versions 9.x.

NOTE: There are no functional or performance upgrades for Crestron Virtual Control running on Red Hat Enterprise Linux version 9.x. The Red Hat Enterprise Linux version should only be upgraded if it is deemed necessary by your IT department.

1. Log into an account with sudo privileges on the Linux platform where the Crestron Virtual Control package is installed.
2. Open a new terminal window.
3. Issue the following commands.

   ```
   sudo systemctl stop virtualcontrol
   sudo systemctl disable virtualcontrol
   ```

4. Upgrade the Red Hat Enterprise Linux OS to version 9.x on your Linux platform as described in https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/upgrading_from_rhel_8_to_rhel_9/index.

Once the upgrade is complete, perform the Crestron Virtual Control upgrade process as described in Upgrade Crestron Virtual Control on page 39.

Downgrade Crestron Virtual Control

Crestron Virtual Control can be downgraded to an earlier version if desired.

NOTES:

- If downgrading Crestron Virtual Control to version 2.7000.00047 or earlier, all SIMPL programs must be deleted from the program library and room lists. A **PrepareForDowngrade.sh** script is provided with the Crestron Virtual Control package (version 4.0000.00001 or later) that automates this task. For more information, refer to step 3 in the following procedure.
- Crestron Virtual Control cannot be downgraded to a version below 4.0002.xxxxx if the Linux platform has been upgraded to Red Hat Enterprise Linux version 9.x.

To downgrade the Crestron Virtual Control service on the Linux platform:

CAUTION: Ensure that all custom configuration files are backed up prior to downgrading the Crestron Virtual Control service, as any previous configurations will be overwritten.

1. Download the desired Crestron Virtual Control file package from the **Software & Firmware** resource page at www.crestron.com/Support/Resource-Library.
2. Log into an account with sudo privileges on the Linux platform where the Crestron Virtual Control package is installed.
3. If downgrading to version 2.7000.00047 or earlier, run the **PrepareForDowngrade.sh** script:
   a. Extract the **PrepareForDowngrade.sh** file from the installation package (version 4.0000.00001 or later) and copy it to the Linux server platform where Crestron Virtual Control is currently installed.
   b. Open a new terminal window.
   c. Issue the `sudo systemctl stop virtualcontrol` command to stop the Crestron Virtual Control service.
   d. Issue the `sudo ./PrepareForDowngrade.sh` command. The script will delete all SIMPL programs loaded to Crestron Virtual Control automatically.

      NOTE: No confirmation dialog is shown prior to running the script and deleting all SIMPL programs and their associated rooms.
4. Copy the package ZIP file to a location on the Linux platform.

   NOTE: Do not unzip the Crestron Virtual Control package before copying it to the Linux platform. The installation script cannot be executed if the package is unzipped prior to it being copied.
5. Open a new terminal window.
6. Change directories to the location of the ZIP file, and then issue the following command to unzip the package, where `<version>` is the version number of the package file:

   ```
   sudo unzip virtualcontrol-<version>.zip
   ```
7. Change directories to the location of the unzipped package file (`vc-4`).
8. Issue the following command to start the installation. The script installs any RPM files that are dependencies for the installation prior to running the Crestron Virtual Control RPM file.

   ```
   sudo ./installVC4.sh
   ```
9. Enter `y` when prompted to confirm the downgrade.

The downgrade may take up to 15 minutes to complete. Once the downgrade has completed, the Crestron Virtual Control service starts automatically within 2 to 3 minutes.

Uninstall the Crestron Virtual Control Package

To uninstall the Crestron Virtual Control package:

1. Log into an account with sudo privileges on the Linux platform where the Crestron Virtual Control package is installed.
2. Open a new terminal window.
3. Issue the following command:

   ```
   sudo rpm -e virtualcontrol
   ```

   The following options are returned.

   ```
   Select one option from below:
     (1) Uninstall
     (2) Purge
     (3) exit
   ```

4. Enter the number that corresponds with the desired uninstall method:
   a. Enter **1** to uninstall the Crestron Virtual Control package but retain the MariaDB® database.
   b. Enter **2** to uninstall the Crestron Virtual Control package and remove the MariaDB database.
   c. Enter **3** to cancel the operation.

Entering **1** or **2** will uninstall the Crestron Virtual Control package from the Linux platform. To reinstall the Crestron Virtual Control package, refer to Install the Crestron Virtual Control Package on page 33.

VC-4-PC-3 Installation

Use the following procedures to install the VC-4-PC-3.

This section provides the following information:

- Install the VC-4-PC-3 on page 44
- Upgrade or Downgrade the VC-4-PC-3 on page 45

Install the VC-4-PC-3

Use the following procedures to install to the VC-4-PC-3.

In the Box

Qty.	Description
1	VC-4-PC-3, Computer with Crestron Virtual Control Server Software
	Additional Items
1	Power Pack, 19.5VDC, 100–240VAC

Install the VC-4-PC-3

The VC-4-PC-3 must be installed in a well-ventilated area. The VC-4-PC-3 can either be placed on a flat, level surface or VESA® mounted using third-party VESA mounting solutions.

> **NOTE:** The air intake is located on the front of the device, and air is exhausted out of the rear. Ensure the device is installed in a location that permits sufficient airflow through the device.

Note the following enclosure and ventilation requirements when installing the VC-4-PC-3:

- If installing within an enclosure with doors, the doors must be of a type that allows at least 30% airflow through the enclosure (front and back).
- Leave a 4 in. (10 cm) minimum clearance on all vented sides of the VC-4-PC-3 to permit the airflow required for proper ventilation.
- Do not install the VC-4-PC-3 in an enclosure that does not provide sufficient airflow, that is dusty, or that reaches a temperature exceeding 95°F (35°C).
- Do not block the VC-4-PC-3 air vents with any objects, as this can restrict airflow and computer performance, possibly causing the VC-4-PC-3 to overheat.
- If the VC-4-PC-3 is installed in a corner, on a desk, or under a desk, leave a 2 in. (5 cm) clearance from the back of the VC-4-PC-3 to the wall to permit the airflow required for proper ventilation.

Connect the VC-4-PC-3

Make all necessary connections to the VC-4-PC-3 as described below:

> **NOTE:** Any connector on the VC-4-PC-3 that is not listed below is not used.

- **19.5VDC**: Connect to included power supply (100–240VAC, 50/60 Hz input).
- **LAN**: Connect to LAN via Ethernet cable.
- **SSUSB Type-A 3.2** (Front and Rear): Connect to mouse and keyboard for optional command line configuration.
- **HDMI** or **DisplayPort**: Connect to a monitor for optional command line configuration.

Upgrade or Downgrade the VC-4-PC-3

The following procedures describe how to upgrade or downgrade the Crestron Virtual Control service on the VC-4-PC-3.

Upgrade the VC-4-PC-3

When a new version of the Crestron Virtual Control service is available, a notification is displayed on the top of the web user interface.

Web User Interface - Update Notification



To upgrade the Crestron Virtual Control service on the VC-4-PC-3:

CAUTION: Ensure that all custom configuration files are backed up prior to upgrading the Crestron Virtual Control service, as any previous configurations will be overwritten.

1. Open a new terminal window.
2. Issue the following command to begin the download. The script downloads and extracts the latest version of the Crestron Virtual Control service into **/home/admin/vc4temp/vc4**.

   ```
   downloadVC4.sh
   ```

3. Change directories to **/home/admin/vc4temp/vc4**, and then issue the following command to start the upgrade. No user action is required once the upgrade script starts.

   ```
   sudo ./upgradeVC4-PC-3.sh
   ```

The upgrade may take up to 15 minutes to complete. Once the upgrade has completed, the Crestron Virtual Control service starts automatically within 2 to 3 minutes.

NOTE: Before accessing the web configuration interface following an upgrade, close and reopen any browser windows that were previously running the interface. If the browser window is not closed following an upgrade, the interface may not update to the latest version until the browser cache is cleared. For more information, refer to Access the Web Configuration Interface on page 73.

Downgrade the VC-4-PC-3

Crestron Virtual Control can be downgraded to an earlier version if desired.

NOTES:

- If downgrading Crestron Virtual Control to version 2.7000.00047 or earlier, all SIMPL programs must be deleted from the program library and room lists. A **PrepareForDowngrade.sh** script is provided with the VC-4-PC-3 that automates this task. For more information, refer to step 2 in the following procedure.
- Crestron Virtual Control cannot be downgraded to a version below 4.0002.xxxxx if the Linux platform has been upgraded to Red Hat Enterprise Linux version 9.x.

To downgrade the Crestron Virtual Control service on the VC-4-PC-3:

CAUTION: Ensure that all custom configuration files are backed up prior to downgrading the Crestron Virtual Control service, as any previous configurations will be overwritten.

1. Download the desired Crestron Virtual Control file package from the **Software & Firmware** resource page at www.crestron.com/Support/Resource-Library.
2. If downgrading to version 2.7000.00047 or earlier, run the **PrepareForDowngrade.sh** script:
   a. Open a new terminal window.
   b. Issue the `sudo systemctl stop virtualcontrol` command to stop the Crestron Virtual Control service.
   c. Issue the `sudo ./PrepareForDowngrade.sh` command. The script will delete all SIMPL programs loaded to Crestron Virtual Control automatically.

      NOTE: No confirmation dialog is shown prior to running the script and deleting all SIMPL programs and their associated rooms.
3. Copy the package ZIP file to **/home/admin/vc4temp** on the VC-4-PC-3.

   NOTE: Do not unzip the Crestron Virtual Control package before copying it to the Linux platform. The installation script cannot be executed if the package is unzipped prior to it being copied.
4. Open a new terminal window.
5. Change directories to **/home/admin/vc4temp**, and then issue the following command to unzip the package, where `<version>` is the version number of the package file:

   ```
   sudo unzip virtualcontrol-<version>.zip
   ```
6. Change directories to the location of the unzipped package file (`vc-4`).

7. Issue the following command to start the installation. The script installs any RPM files that are dependencies for the installation prior to running the Crestron Virtual Control RPM file.

```
sudo ./installVC4.sh
```

8. Enter `y` when prompted to confirm the downgrade.

The downgrade may take up to 15 minutes to complete. Once the downgrade has completed, the Crestron Virtual Control service starts automatically within 2 to 3 minutes.

VC-4-SERVER-25 Installation

Use the following procedures to install the VC-4-SERVER-25.

This section provides the following information:

- Install the VC-4-SERVER-25 on page 49
- Upgrade or Downgrade the VC-4-SERVER-25 on page 50

Install the VC-4-SERVER-25

Use the following procedures to install to the VC-4-PC-3.

In the Box

Qty.	Description
1	VC-4-SERVER-25, Rack Server with Crestron Virtual Control Software

Install the VC-4-SERVER-25

The VC-4-SERVER-25 must be installed in a well-ventilated area. The VC-4-SERVER-25 can either be placed on a flat, level surface or VESA® mounted using third-party VESA mounting solutions.

> **NOTE:** The air intake is located on the front of the device, and air is exhausted out of the rear. Ensure the device is installed in a location that permits sufficient airflow through the device.

Note the following enclosure and ventilation requirements when installing the VC-4-SERVER-25:

- If installing within an enclosure with doors, the doors must be of a type that allows at least 30% airflow through the enclosure (front and back).
- Leave a 4 in. (10 cm) minimum clearance on all vented sides of the VC-4-PC-3 to permit the airflow required for proper ventilation.
- Do not install the VC-4-SERVER-25 in an enclosure that does not provide sufficient airflow, that is dusty, or that reaches a temperature exceeding 95°F (35°C).
- Do not block the VC-4-SERVER-25 air vents with any objects, as this can restrict airflow and computer performance, possibly causing the VC-4-SERVER-25 to overheat.
- If the VC-4-SERVER-25 is installed in a corner, on a desk, or under a desk, leave a 2 in. (5 cm) clearance from the back of the VC-4-SERVER-25 to the wall to permit the airflow required for proper ventilation.

Connect the VC-4-SERVER-25

Make all necessary connections to the VC-4-SERVER-25 as described below:

> **NOTE:** Any connector on the VC-4-SERVER-25 that is not listed below is not used.

- **19.5VDC**: Connect to included power supply (100–240VAC, 50/60 Hz input).
- **LAN**: Connect to LAN via Ethernet cable.
- **SSUSB Type-A 3.2** (Front and Rear): Connect to mouse and keyboard for optional command line configuration.
- **HDMI** or **DisplayPort**: Connect to a monitor for optional command line configuration.

Upgrade or Downgrade the VC-4-SERVER-25

The following procedures describe how to upgrade or downgrade the Crestron Virtual Control service on the VC-4-SERVER-25.

Upgrade the VC-4-SERVER-25

When a new version of the Crestron Virtual Control service is available, a notification is displayed on the top of the web user interface.

Web User Interface - Update Notification



To upgrade the Crestron Virtual Control service on the VC-4-SERVER-25:

CAUTION: Ensure that all custom configuration files are backed up prior to upgrading the Crestron Virtual Control service, as any previous configurations will be overwritten.

1. Open a new terminal window.
2. Issue the following command to begin the download. The script downloads and extracts the latest version of the Crestron Virtual Control service into **/home/admin/vc4temp/vc4**.

   ```
   downloadVC4.sh
   ```

3. Change directories to **/home/admin/vc4temp/vc4**, and then issue the following command to start the upgrade. No user action is required once the upgrade script starts.

   ```
   sudo ./upgradeVC4-PC-3.sh
   ```

The upgrade may take up to 15 minutes to complete. Once the upgrade has completed, the Crestron Virtual Control service starts automatically within 2 to 3 minutes.

NOTE: Before accessing the web configuration interface following an upgrade, close and reopen any browser windows that were previously running the interface. If the browser window is not closed following an upgrade, the interface may not update to the latest version until the browser cache is cleared. For more information, refer to .

Downgrade the VC-4-SERVER-25

Crestron Virtual Control can be downgraded to an earlier version if desired.

NOTES:

- If downgrading Crestron Virtual Control to version 2.7000.00047 or earlier, all SIMPL programs must be deleted from the program library and room lists. A **PrepareForDowngrade.sh** script is provided with the that automates this task. For more information, refer to step in the following procedure.
- Crestron Virtual Control cannot be downgraded to a version below 4.0002.xxxxx if the Linux platform has been upgraded to Red Hat Enterprise Linux version 9.x.

To downgrade the Crestron Virtual Control service on the VC-4-SERVER-25:

CAUTION: Ensure that all custom configuration files are backed up prior to downgrading the Crestron Virtual Control service, as any previous configurations will be overwritten.

1. Download the desired Crestron Virtual Control file package from the **Software & Firmware** resource page at www.crestron.com/Support/Resource-Library.
2. If downgrading to version 2.7000.00047 or earlier, run the **PrepareForDowngrade.sh** script:
   a. Open a new terminal window.
   b. Issue the `sudo systemctl stop virtualcontrol` command to stop the Crestron Virtual Control service.
   c. Issue the `sudo ./PrepareForDowngrade.sh` command. The script will delete all SIMPL programs loaded to Crestron Virtual Control automatically.

      NOTE: No confirmation dialog is shown prior to running the script and deleting all SIMPL programs and their associated rooms.
3. Copy the package ZIP file to **/home/admin/vc4temp** on the VC-4-SERVER-25.

   NOTE: Do not unzip the Crestron Virtual Control package before copying it to the Linux platform. The installation script cannot be executed if the package is unzipped prior to it being copied.
4. Open a new terminal window.
5. Change directories to **/home/admin/vc4temp**, and then issue the following command to unzip the package, where `<version>` is the version number of the package file:

   ```
   sudo unzip virtualcontrol-<version>.zip
   ```
6. Change directories to the location of the unzipped package file (`vc-4`).

7. Issue the following command to start the installation. The script installs any RPM files that are dependencies for the installation prior to running the Crestron Virtual Control RPM file.

```
sudo ./installVC4.sh
```

8. Enter `y` when prompted to confirm the downgrade.

The downgrade may take up to 15 minutes to complete. Once the downgrade has completed, the Crestron Virtual Control service starts automatically within 2 to 3 minutes.

Configuration

Use the following procedures to configure Crestron Virtual Control on a Linux platform.

NOTE: Certain configuration tasks can also be performed via Crestron Toolbox™ software or the Crestron Virtual Control REST API.

- For more information on configuration via Crestron Toolbox, refer to the Crestron Toolbox help file.
- For more information on configuration via the REST API, refer to the REST API for Crestron Virtual Control Server-Based Control System Programming Guide.

This section provides the following information:

- Initial Setup on page 54
- Manage Licenses on page 92
- Web Configuration on page 101

Initial Setup

Refer to the following sections for instructions on performing initial setup for various Crestron Virtual Control solutions.

This section provides the following information:

- VC-4 Setup on page 55
- VC-4-PC-3 Setup on page 61

VC-4 Setup

Use the following procedures to set up the Crestron Virtual Control (VC-4) server following installation.

Access the Web Configuration Interface

The Crestron Virtual Control server may be monitored and configured using its web configuration interface. The web configuration interface provides selections for viewing and configuring rooms, programs, and connected devices.

> **NOTE:** The web configuration interface supports the following browsers:
>
> - Chrome® browser
> - Firefox® browser
> - Microsoft Edge® browser (chromium-based)
> - Safari® browser

The interface can be accessed via the control system IP address (for configuration and monitoring) or the XiO Cloud® service (for monitoring only) as described in the following sections.

IP Address

The Crestron Virtual Control web configuration interface is accessible via two different URLs: one for administrators (read/write permissions) and one for users or operators (read-only permissions).

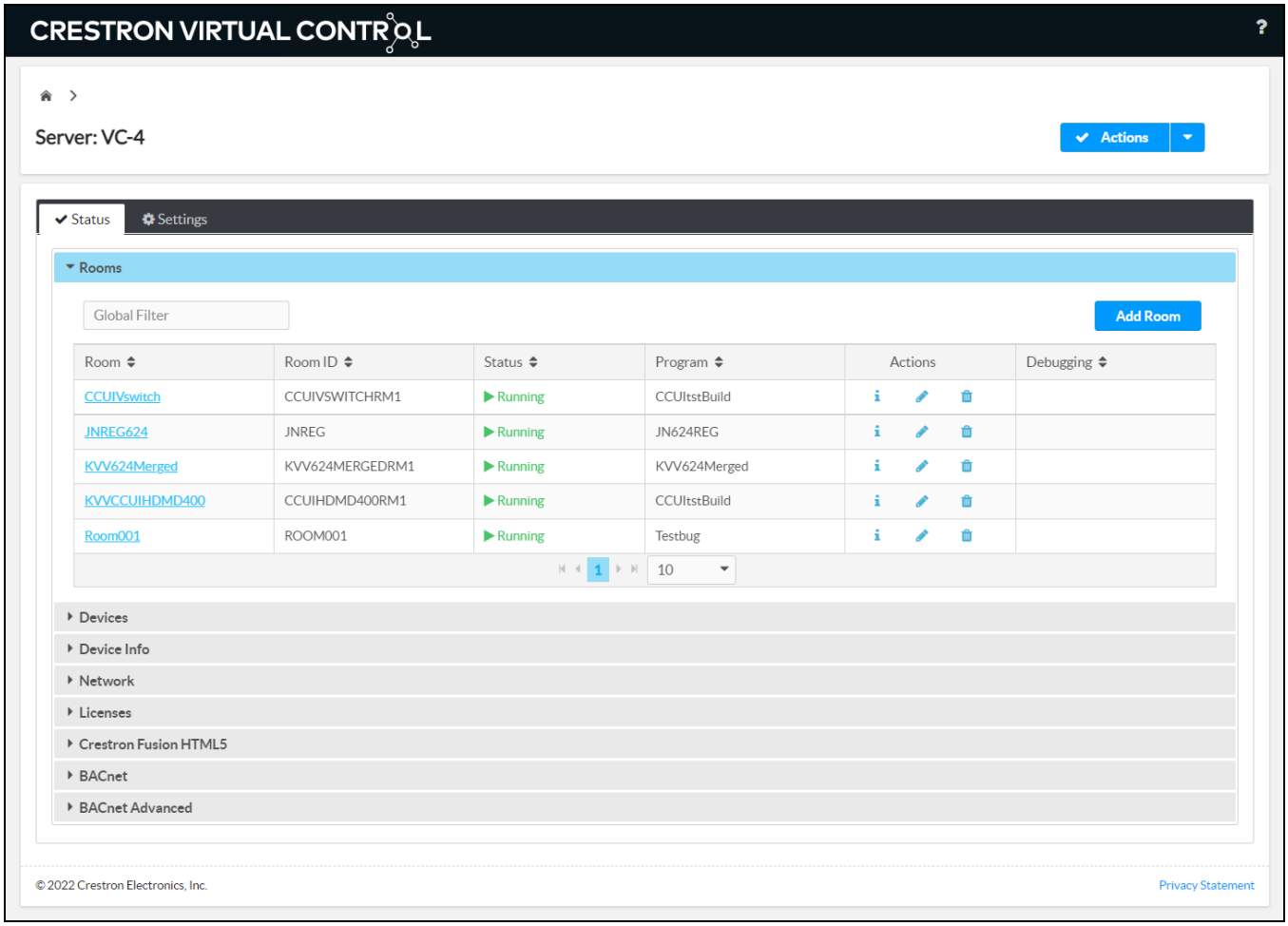
For administrator (read/write) access:

1. Enter **http://[ServerURL]/VirtualControl/config/settings/** into a supported web browser, where **[ServerURL]** is the IP address or host name of the Linux platform.
2. If PAM (Pluggable Authentication Module) has been configured for the interface, enter the required username and password in the pop-up dialog box that is displayed, and then select **Sign in**.

   > **NOTE:** For more information on configuring PAM for the web configuration interface, refer to Configure PAM Authentication on page 143.

The **Status** > **Rooms** page displays by default.

Crestron Virtual Control Web User Interface - Administrator View



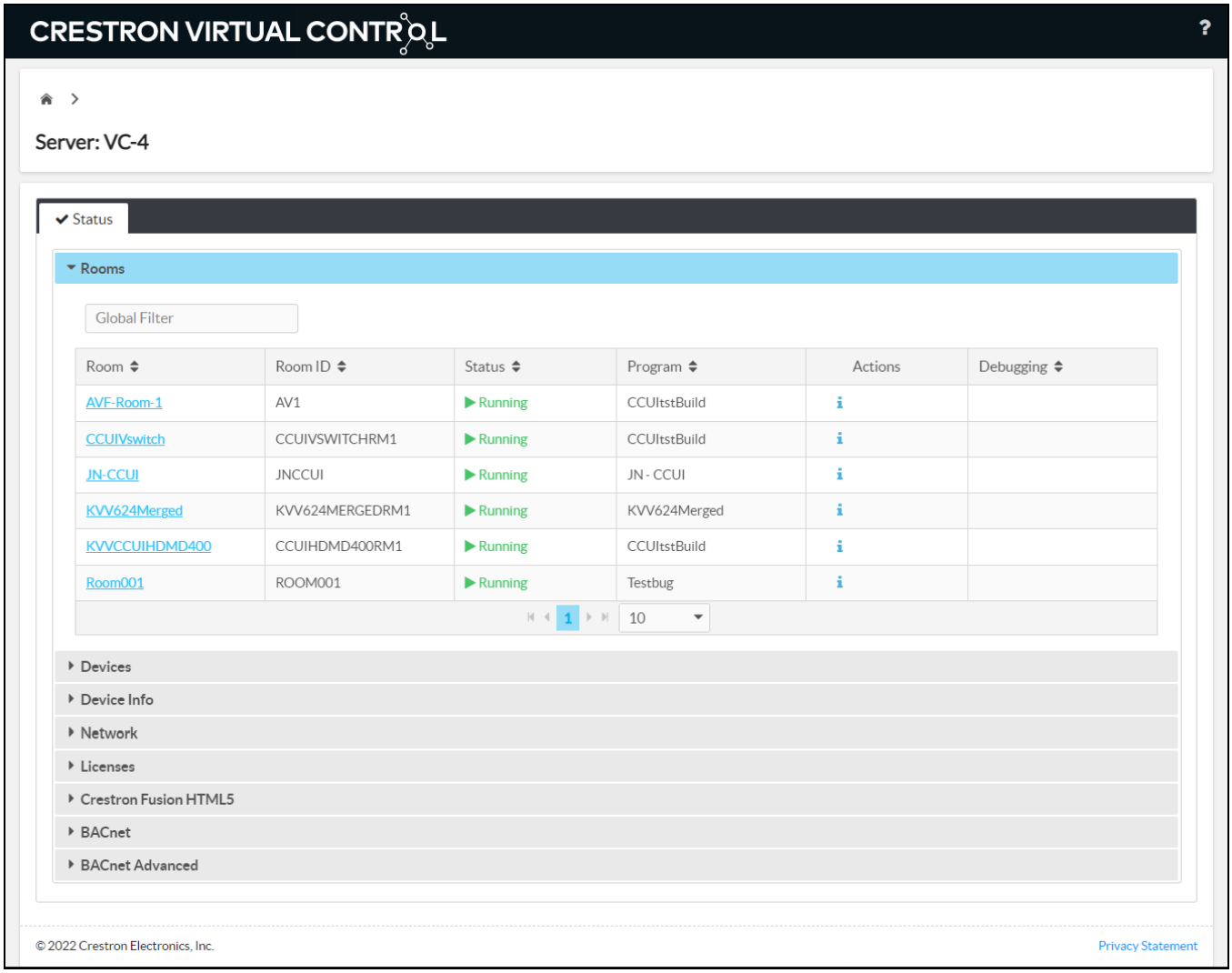
For user or operator (read-only) access:

1. Enter **http://[ServerURL]/VirtualControl/config/status/** into a supported web browser, where **[ServerURL]** is the IP address or host name of the Linux platform.
2. If PAM (Pluggable Authentication Module) has been configured for the interface, enter the required username and password in the pop-up dialog box that is displayed, and then select **Sign in**.

> **NOTE:** For more information on configuring PAM for the web configuration interface, refer to Configure PAM Authentication on page 143.

The **Status** > **Rooms** page displays by default. The **Settings** tab and the **Action** menu are not provided for read-only access. Additionally, rooms and programs may not be added or modified.

Crestron Virtual Control Web User Interface - User/Operator View



XiO Cloud Service

The XiO Cloud® service allows the Crestron Virtual Control server to be monitored from one central, secure location in the cloud.

> **NOTE:** An XiO Cloud account is required to use the service. To register for an XiO Cloud account, refer to www.crestron.com/Support/Tools/Licensing-Registration/XiO-Cloud-Registration-Room-Licenses.

To connect the control system to the XiO Cloud service:

1. Record the MAC address and serial number for the Crestron Virtual Control server. The MAC address and serial number are required to add the control system to the XiO Cloud service.

> **NOTE:** The MAC address and serial number for the Crestron Virtual Control server can be viewed by opening the **Device Info** accordion in the web configuration interface as described in Device Info on page 121.

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

Once the Crestron Virtual Control server is claimed, select it from the cloud interface to view its status. The Crestron Virtual Control server 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 Crestron Virtual Control server must be added to a licensed room before its status and settings can be viewed.

Open Ports for Remote Debugging

The Linux server firewall blocks all incoming traffic by default. In order to allow remote debugging for SIMPL#Pro programs, work with your IT administrator to open the ports used by the programs and debuggers through the firewall.

> **NOTE:** SIMPL programs are debugged directly through the web configuration interface without requiring any ports to be opened. For more information, refer to Enable Debugging on page 109

Once these ports have been determined, issue the following commands to specify the range of ports for remote debugging:

```
sudo firewall-cmd -q --zone=public --permanent --add-port=[STARTPORT-ENDPORT]/tcp

sudo firewall-cmd --reload
```

Set Custom TCP Keepalives

Custom TCP keepalives must be set to run the Crestron Virtual Control server. The default TCP keepalive timeout for a Linux system is 2 hours but should be reduced to 30 seconds to more quickly detect disconnected rooms and programs.

To set custom TCP keepalives for the Crestron Virtual Control server:

1. Navigate to **/etc/** and open the **sysctl.conf** file in a text editing program.
2. Add the following lines to the end of the file:

```
net.ipv4.tcp_keepalive_intvl=30
net.ipv4.tcp_keepalive_time=30
```

3. Save and exit the file.
4. Issue the following command to apply the changes without a restart:

```
sudo sysctl -p
```

Detect Device Disconnects

If a device connected to the Crestron Virtual Control server becomes disconnected because its Ethernet cable is disconnected and then plugged back in, the server may take up to 15 minutes to detect that the device has gone offline and to attempt to reestablish communications.

To reduce the time it takes to detect device disconnects in this scenario, reduce the TCP retry timeout for the Linux server.

1. Navigate to **/etc/** and open the **sysctl.conf** file in a text editing program.
2. Add the following line to the end of the file:

```
net.ipv4.tcp_retries2=8
```

3. Save and exit the file.
4. Issue the following command to apply the changes without a restart:

```
sudo sysctl -p
```

The server will now recognize that unplugged devices have disconnected within 2 to 3 minutes and will attempt to reestablish communications.

Increase the File Size Limit

As of Crestron Virtual Control version 2.4557.00155, the maximum file size limit has been increased from 128 MB to 512 MB. For installations running a previous version of Crestron Virtual Control, the configuration files must be updated manually to increase the file size limit even after an upgrade.

> **NOTE:** New Crestron Virtual Control installations using version 2.4557.00155 or later do not require the configuration files to be updated.

To increase the file size limit:

1. Upgrade Crestron Virtual Control to version 2.4557.00155 or later as described in Upgrade or Downgrade Crestron Virtual Control on page 39.
2. Open the **[VirtualControlHome]/conf/crestron.conf** file.
3. Locate the line `SecRequestBodyLimit 134217728` and modify it as follows:

```
SecRequestBodyLimit 536870912
```

4. Save and exit the file.

Increase System Limits for SIMPL Debugging

When debugging SIMPL programs running on the Crestron Virtual Control server, a "resource temporarily unavailable" error may occur if the SIMPL program contains a large number of joins.

To avoid this error, certain Linux system limits must be increased within the **sysctl.conf** file as follows.

> **NOTE:** This procedure is recommended only when debugging SIMPL programs running on the Crestron Virtual Control server. For more information on debugging a SIMPL program using the **SIMPL Debugger** tool in Crestron Toolbox™ software, refer to the Crestron Toolbox help file.

1. Navigate to **/etc/** and open the **sysctl.conf** file in a text editing program.
2. Add the following lines to the end of the file:

```
net.core.wmem_max=10000000
net.unix.max_dgram_qlen=4096
```

3. Save and exit the file.
4. Issue the following command to apply the changes without a restart:

```
sudo sysctl -p
```

Configure .AV Framework Software

Crestron Virtual Control 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 load and configure the .AV Framework software program on the Crestron Virtual Control server, refer to the .AV Framework Software for Crestron Virtual Control Software Operations Guide.

VC-4-PC-3 Setup

Use the following procedures to set up the VC-4-PC-3 following installation.

Discover the VC-4-PC-3 on the Network

Crestron Toolbox™ software must be used to discover the VC-4-PC-3 and its IP address on the network. The IP address is required for accessing the Cockpit graphical interface or the device web configuration interface.

> **NOTE:** The computer running Crestron Toolbox software must be on the same subnet as the VC-4-PC-3.

To discover the VC-4-PC-3 on the network:

1. Connect the VC-4-PC-3 to the Ethernet network.
2. Open Crestron Toolbox software.
3. Navigate to **Tools** > **Device Discovery Tool** to open the **Device Discovery Tool**.
4. If device discovery does not start automatically, select **Discover Devices**.

If the VC-4-PC-3 is discovered successfully, it will appear in the left-hand results column with a default hostname of "VC-4-PC-3-*xxxxxxxxxx*", where *xxxxxxxxxx* is the device MAC address.

Device Discovery Tool



Access the Cockpit Graphical Interface

The VC-4-PC-3 provides a graphical interface (Cockpit) that is used to configure settings for the installed Alma Linux OS® Linux® operating system.

CAUTION: The Cockpit graphical interface can be used to change various settings for the Linux operating system, including advanced settings that can significantly affect the performance and stability of the operating system. Crestron recommends only configuring the settings that are described in the following sections.

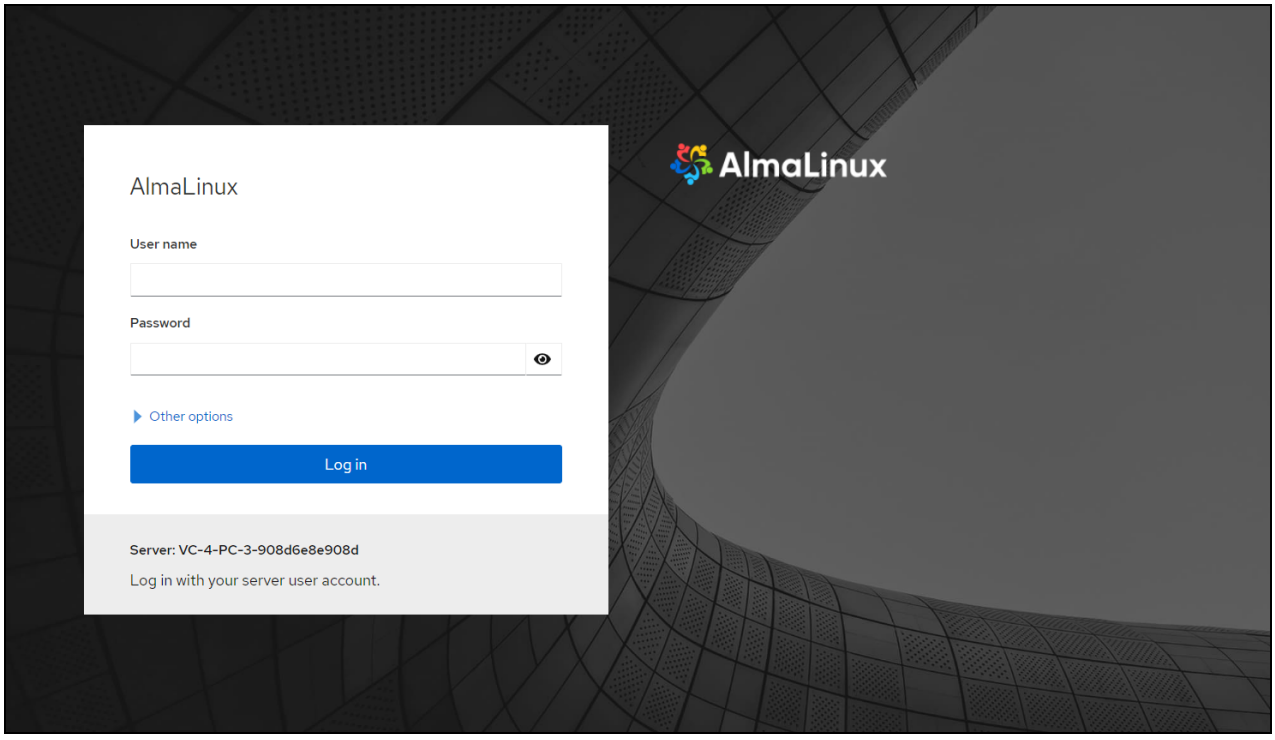
To access the Cockpit graphical interface:

1. Obtain the VC-4-PC-3 IP address as described in Discover the VC-4-PC-3 on the Network on page 61.
2. Enter **https://[ipaddress]:9090** into a web browser, where **[ipaddress]** is the VC-4-PC-3 IP address.

   NOTE: Port 9090 is required for accessing the Cockpit graphical interface. Ensure this port is not blocked and that no control system programs or other processes interfere with this port.

3. When prompted by your web browser, accept the self-signed certificate for the web server. The Alma Linux OS login page is displayed after the self-signed certificate is accepted.

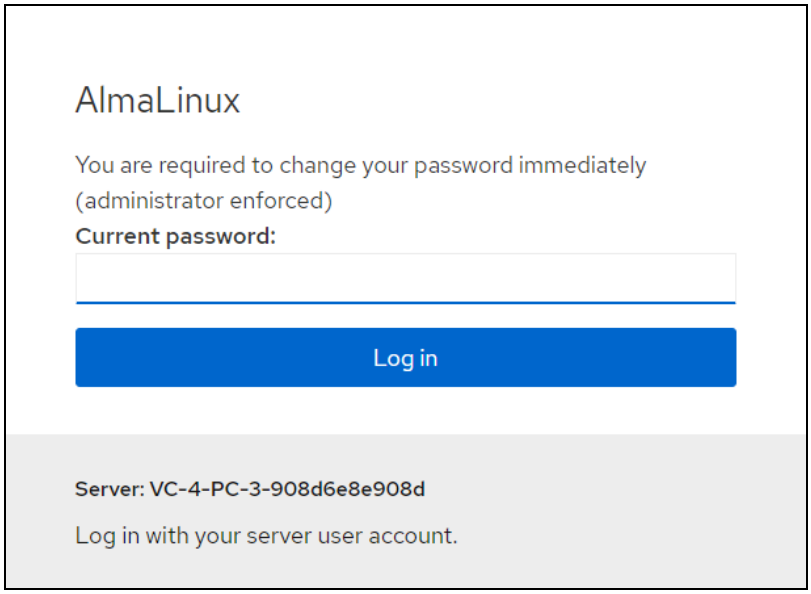
   Alma Linux OS Login Page



4. Enter the default username and password for the Linux admin account (**admin**/**admin**) in the appropriate text fields.

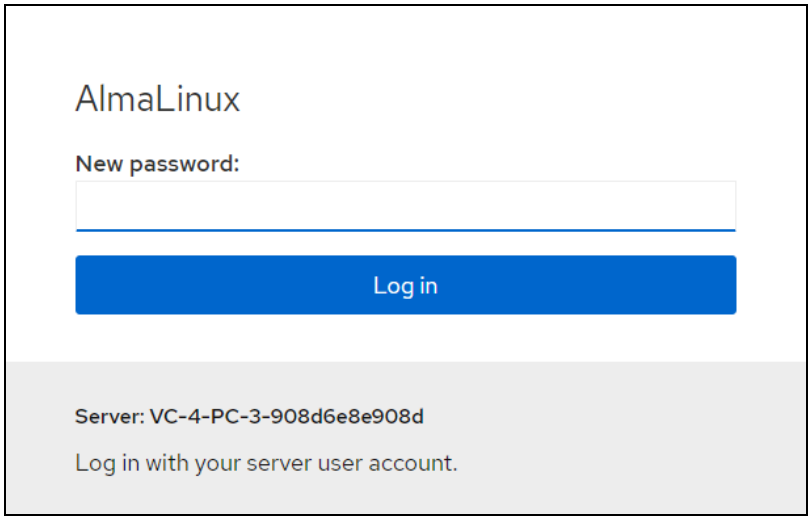
5. Select **Log in**. A prompt is displayed asking you to change the password for the Linux admin account.

   Alma Linux OS Login Page - Current password



6. Enter the current password (**admin**) in the **Current password** text field, and then select **Log in**. A prompt is displayed asking you to enter a new password for the Linux admin account.

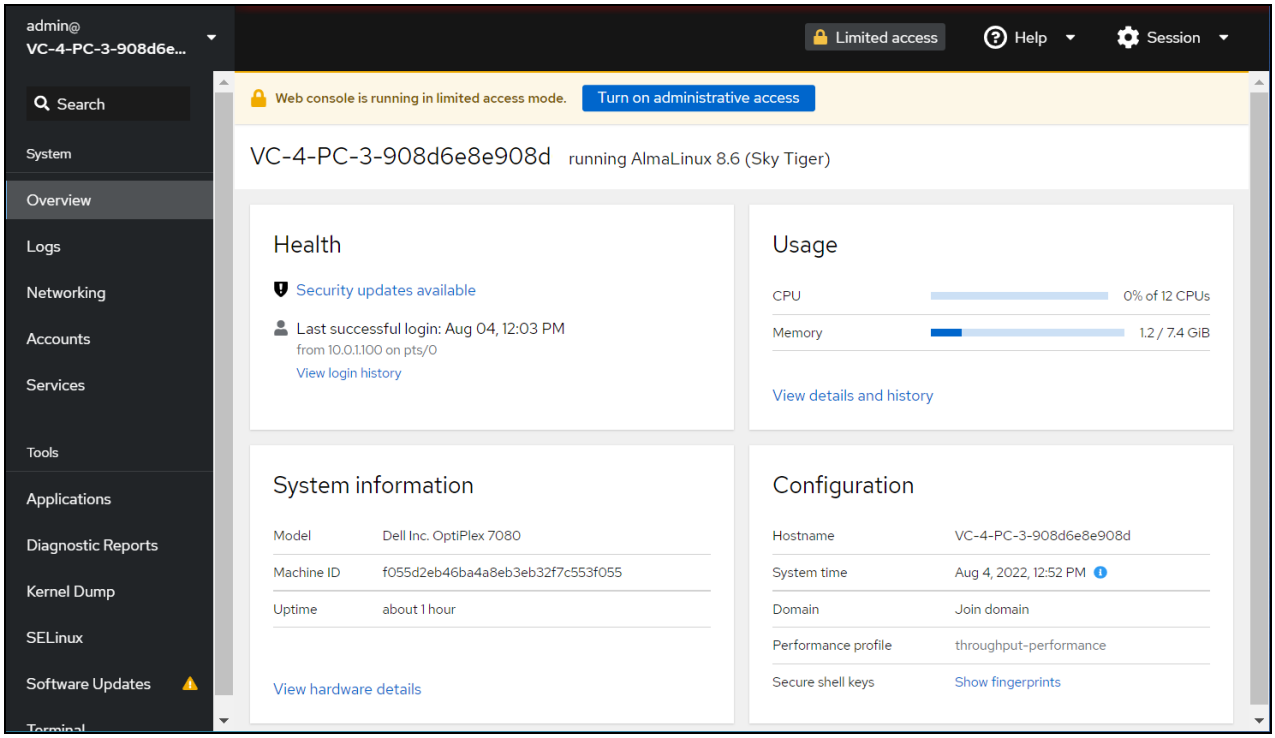
   Alma Linux OS Login Page - New password



7. Enter the new password in the **New password** text field, and then select **Log in**.

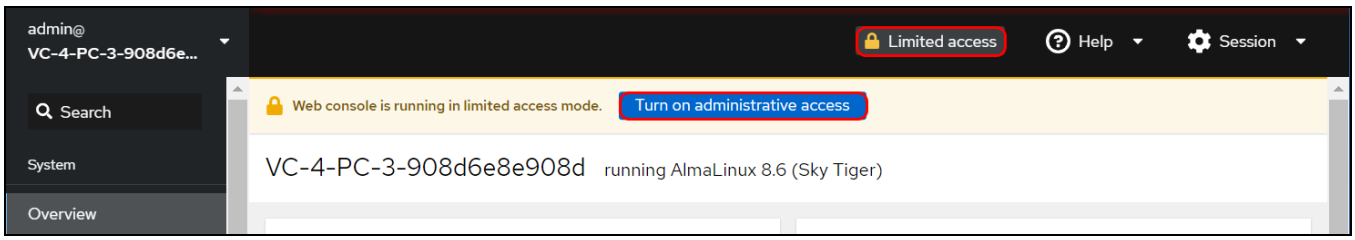
8. When prompted, confirm the password created in step 7, and then select **Log in**. The Cockpit graphical interface opens with the **Overview** page displayed.

Cockpit - Overview Page



By default, Cockpit allows only for limited access to system settings. Administrative access must be granted by selecting the **Limited access** button in the top-left corner of the page and entering the Linux admin account password when prompted. Alternatively, if a banner is displayed stating that the web console is running in limited access mode, select the **Turn on administrative access** button.

Cockpit - Limited access Controls



Once administrative access has been granted, the **Limited access** button changes to an **Administrative access** button, and all system settings can now be configured.

Cockpit - Administrative access Controls



NOTE: Limited access can be restored by selecting the **Administrative access** button and selecting **Limit access** within the dialog box that is displayed.

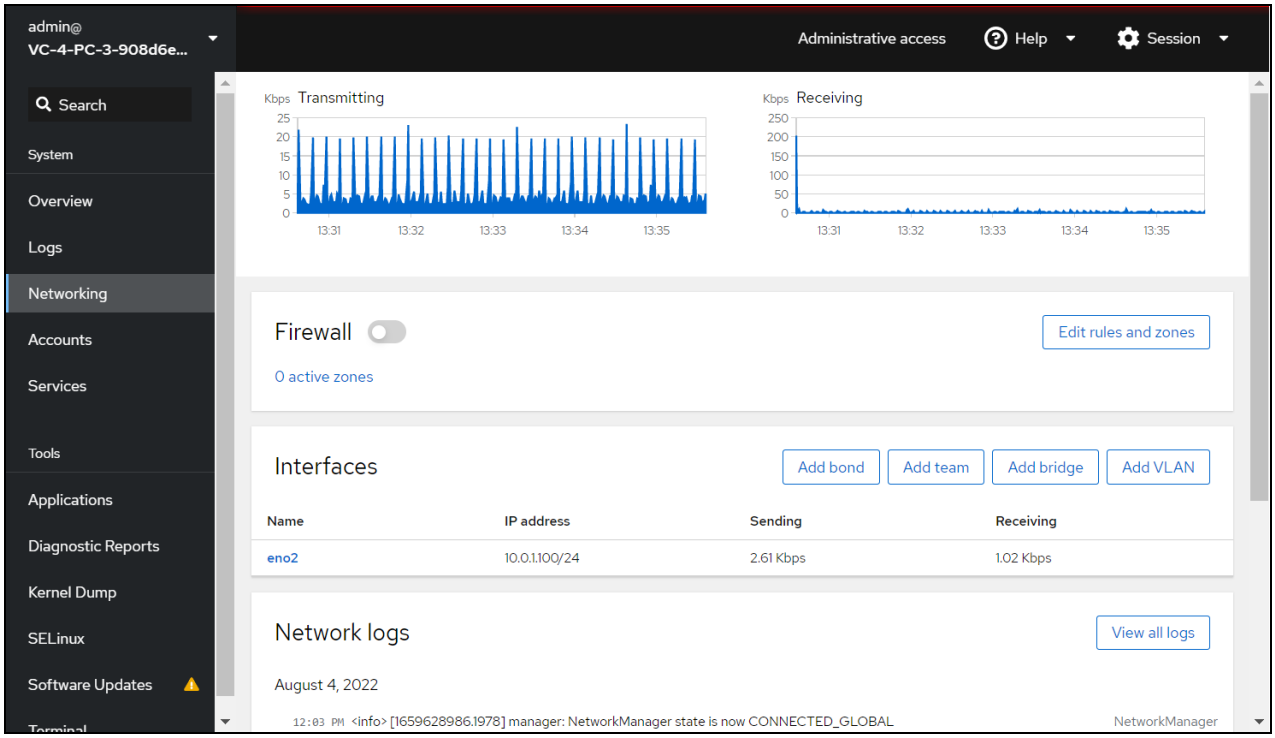
Configure a Static IP Address

The VC-4-PC-3 ships with DHCP turned on by default.

To set a static IP address for the device:

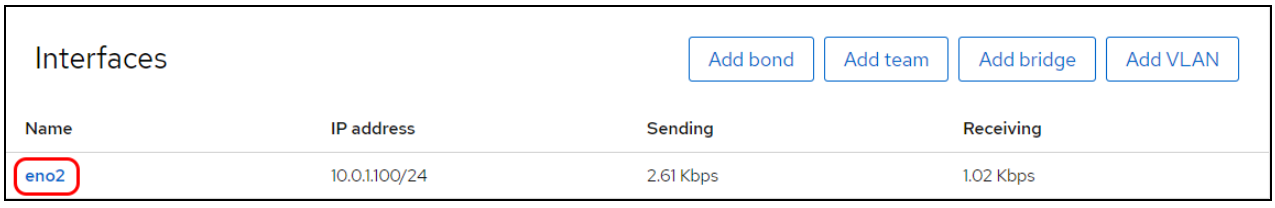
1. Select **Networking** from the navigation menu. The **Networking** page is displayed.

   Cockpit - Networking Page



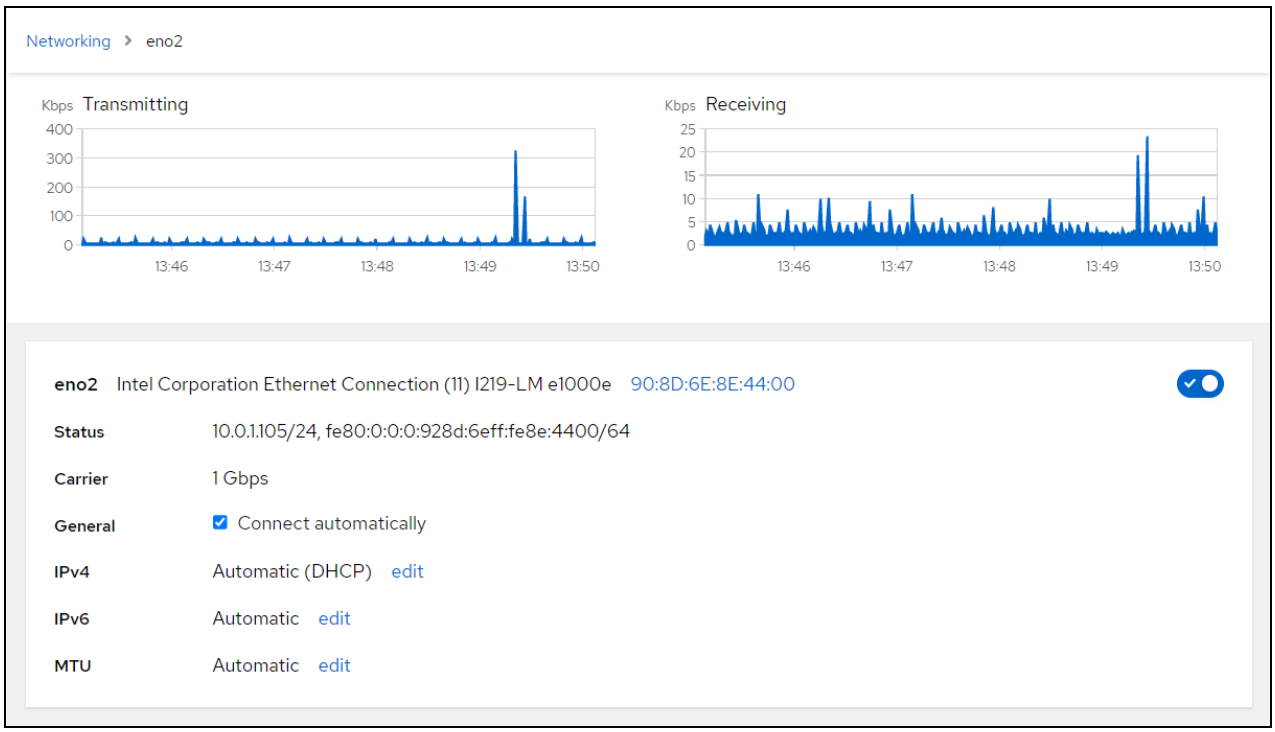
2. Within the **Interfaces** section, select the interface name that corresponds with the device IP address.

   Cockpit - Networking Page (Interfaces)



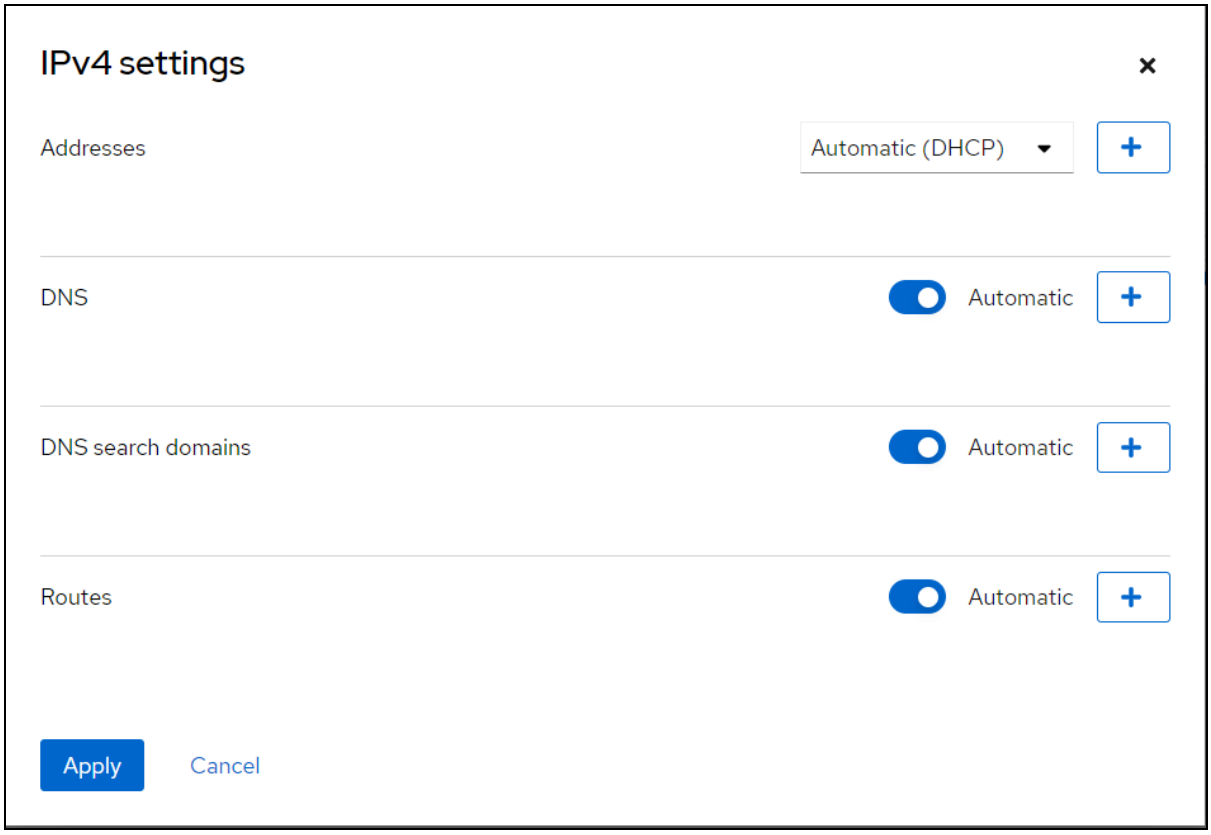
A page is displayed with network information for the selected interface.

Cockpit - Networking Page (Selected Interface)



3. Select **edit** next to the **IPv4** value. The **IPv4 settings** dialog box is displayed.

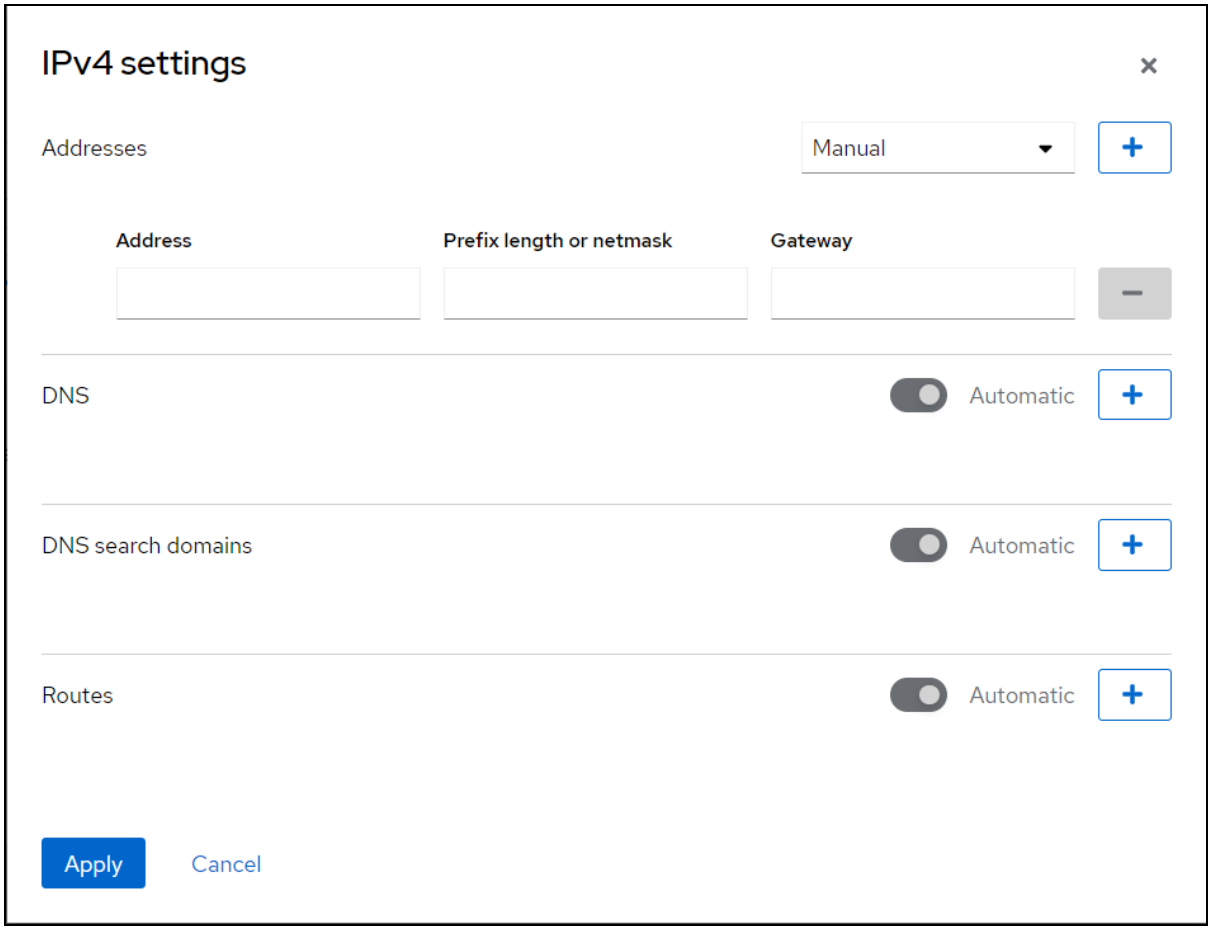
IPv4 settings Dialog Box



4. Select **Manual** from the drop-down menu within the **Addresses** section.

5. Enter the static IP address information in the text fields that are displayed.

IPv4 settings Dialog Box - Static IP Address Entry



6. Select **Apply**. The **IPv4** value for the interface will update to display the new static IP address.

NOTE: A new self-signed certificate must be generated for the web server after changing the device IP address and/or hostname. For more information, refer to Generate a New Self-Signed Certificate on page 72.

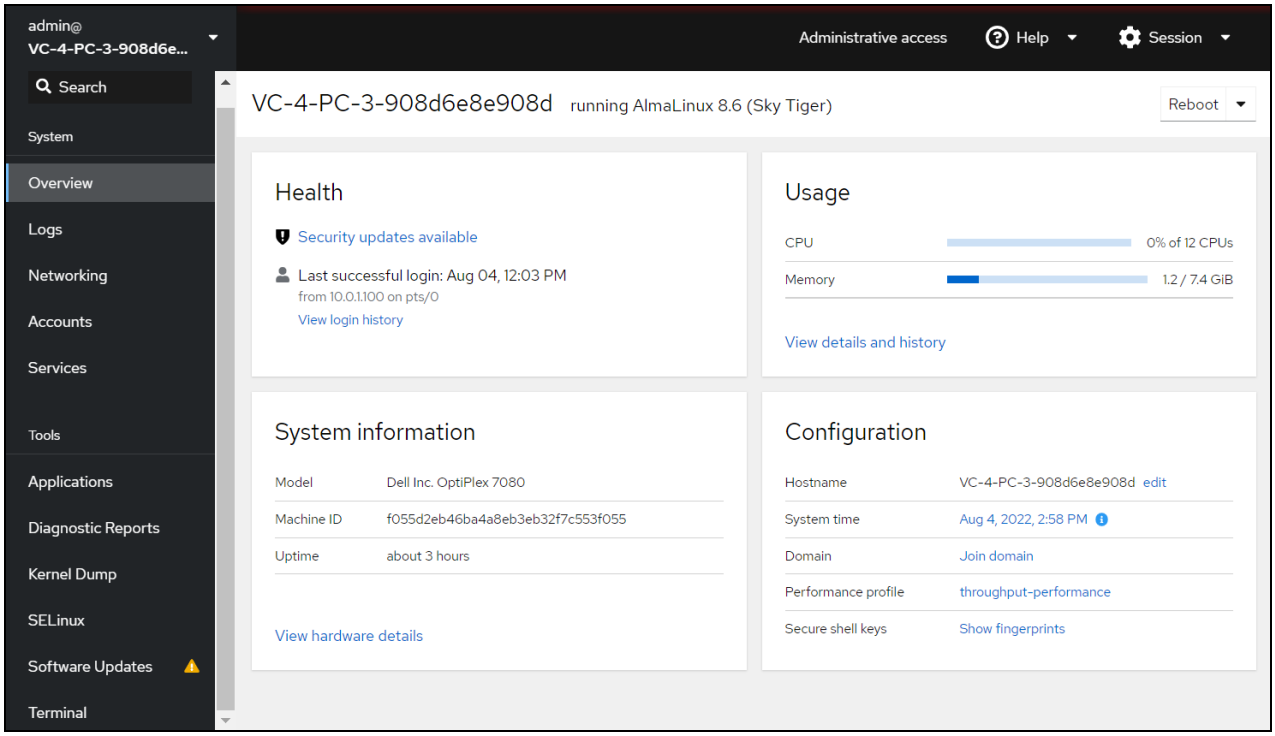
Change the Device Hostname

The VC-4-PC-3 ships with a default hostname of "VC-4-PC-3-*xxxxxxxxxx*", where *xxxxxxxxxx* is the device MAC address.

To change the hostname for the device:

1. Select **Overview** from the navigation menu. The **Overview** page is displayed.

   Cockpit - Overview Page



2. Within the **Configuration** section, select **edit** next to the **Hostname** value. The **Change host name** dialog box is displayed.

   Change host name Dialog Box



3. Enter the new device hostname in the **Real host name** text field.

NOTE: The period (.) and colon (:) characters are not valid for Linux hostnames, even though Cockpit allows these characters to be entered in the **Real host name** text field.

4. Select **Change**. The **Hostname** value for the device will update to display the new hostname.

NOTE: A new self-signed certificate must be generated for the web server after changing the device IP address and/or hostname. For more information, refer to Generate a New Self-Signed Certificate on page 72.

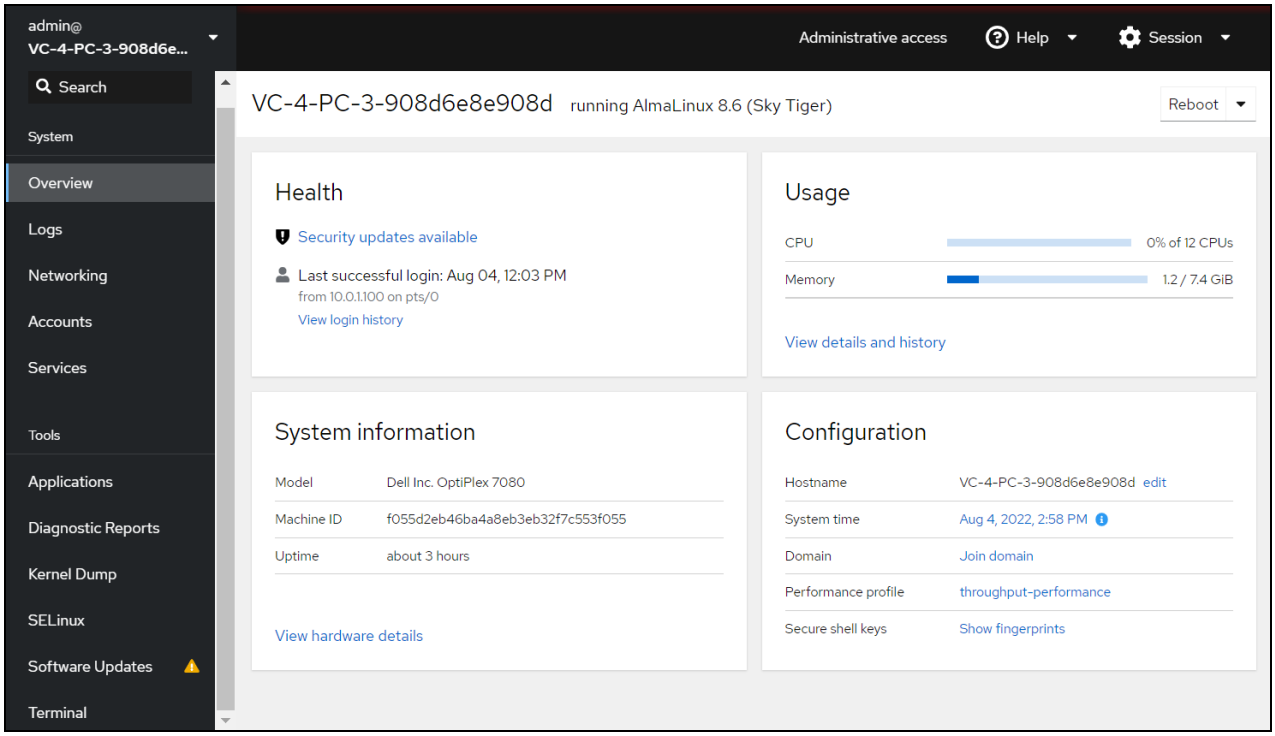
Change the Time Zone

The VC-4-PC-3 ships with its time zone set to **America/New York** by default. The time zone must be changed if it does not match the time zone of the VC-4-PC-3 installation.

To change the time zone for the device:

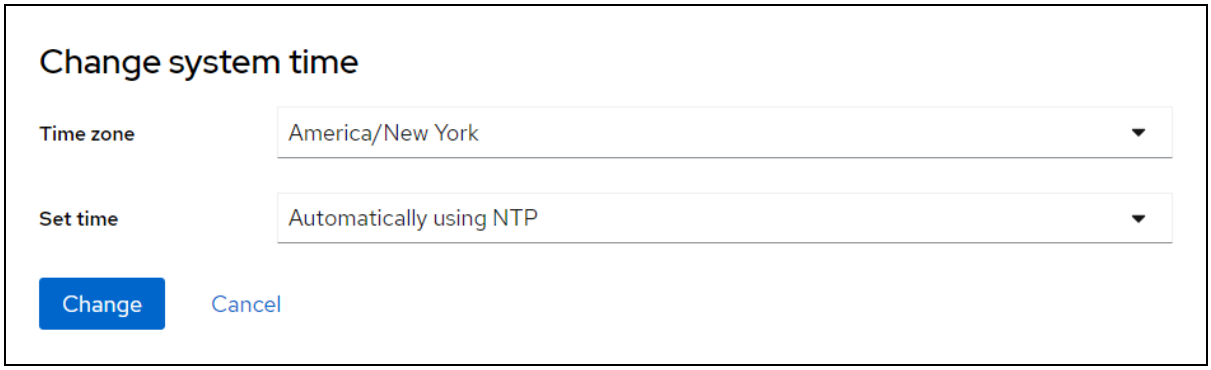
1. Select **Overview** from the navigation menu. The **Overview** page is displayed.

   Cockpit - Overview Page



2. Within the **Configuration** section, select the value listed for **System time**. The **Change system time** dialog box is displayed.

   Change system time Dialog Box



3. Use the **Time zone** drop-down menu to select the required time zone.
4. Select **Change**. The **System time** value for the device will update to reflect selected time zone.

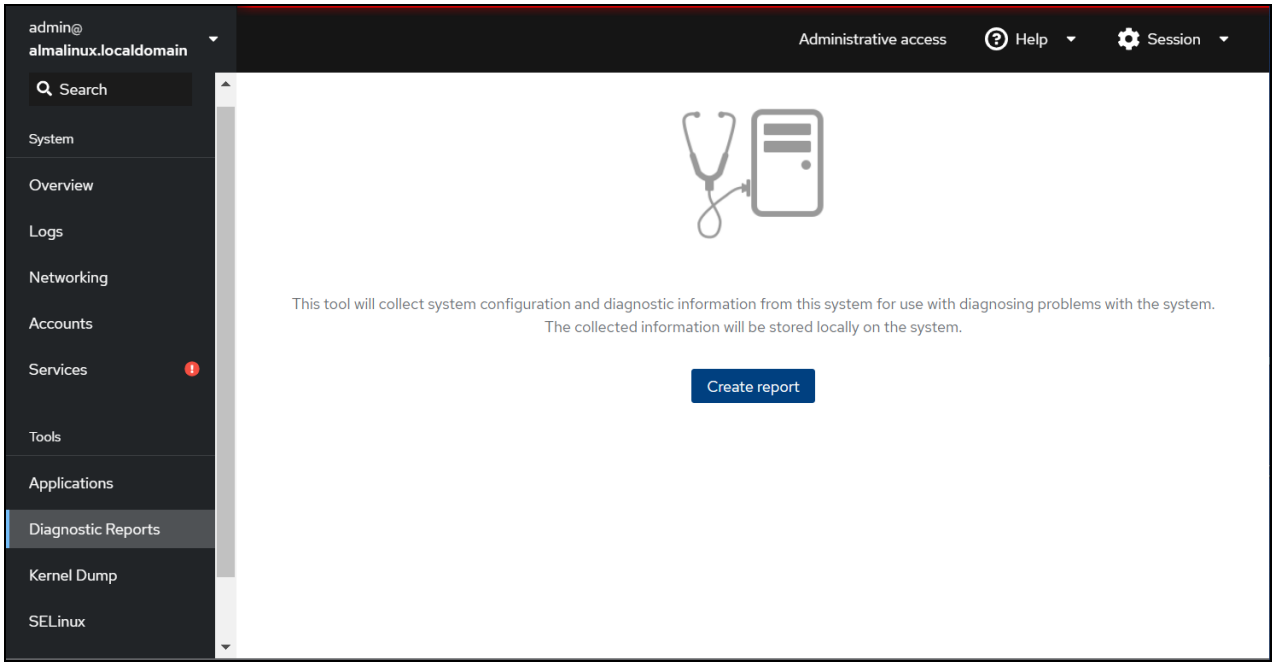
Generate System Logs

The VC-4-PC-3 provides support for local system logging. System logs can be generated and downloaded using Cockpit.

To generate and download system logs for the VC-4-PC-3:

1. Select **Diagnostic Reports** from the navigation menu. The **Diagnostic Reports** page is displayed.

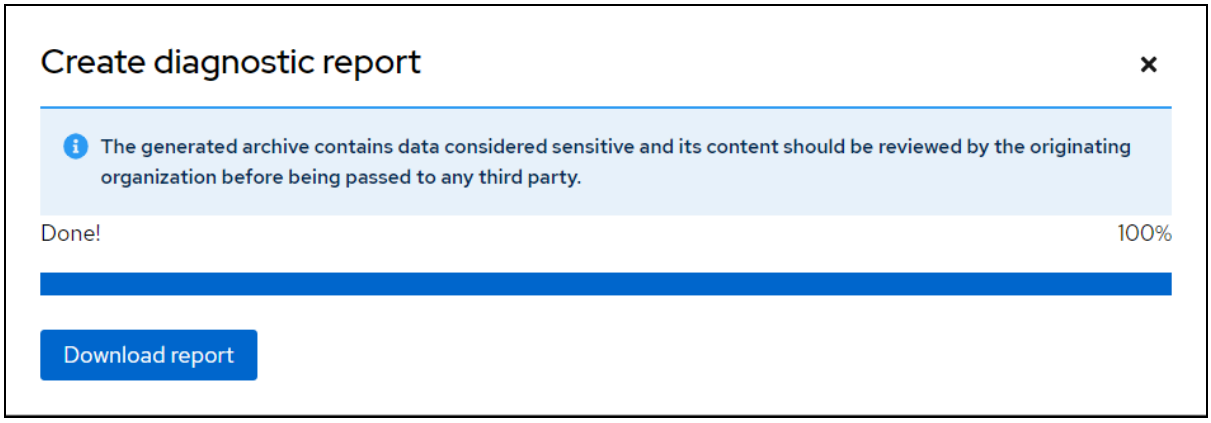
   Cockpit - Diagnostic Reports Page



2. Select **Create report**. The **Create diagnostic report** dialog box is displayed showing the status of the report generation.

3. Once the report is generated, select **Download report**. The system logs are downloaded as a compressed TAR .XZ file to the local computer.

Create diagnostic report Dialog Box



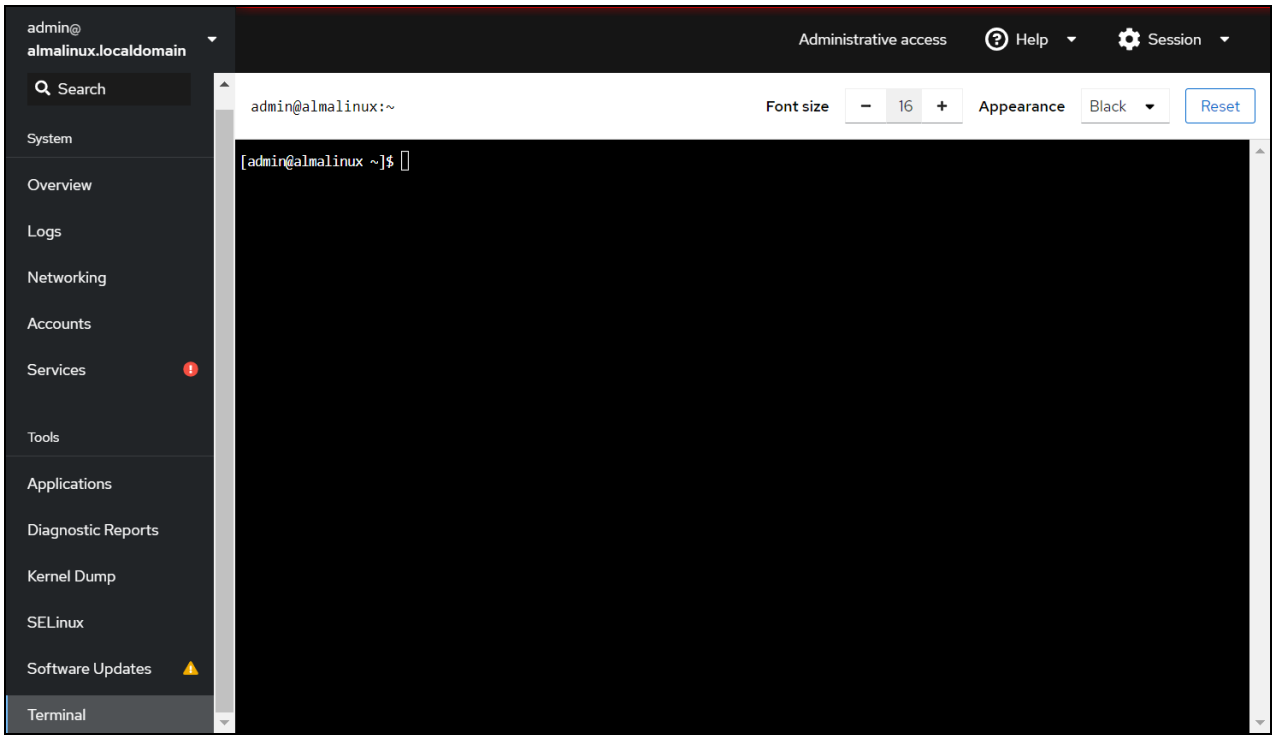
Generate a New Self-Signed Certificate

If the VC-4-PC-3 IP address and/or the hostname are changed, a new self-signed certificate must be generated to ensure the certificate contains the correct web server information.

To generate a new self-signed certificate for the VC-4-PC-3 web server:

1. Select **Terminal** from the navigation menu. The **Terminal** page is displayed with a command prompt.

Cockpit - Terminal Page

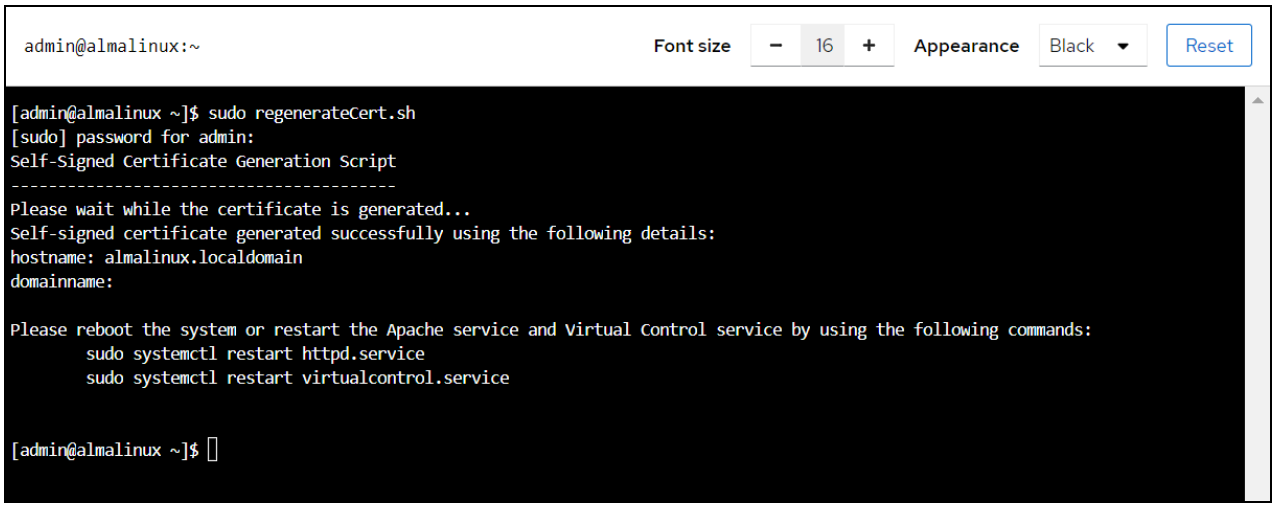


2. Issue the following command:

```
sudo regenerateCert.sh
```

3. When prompted, enter the password for the Linux admin account. The **regenerateCert.sh** script is executed to generate a new self-signed certificate.

regenerateCert Script Execution



4. Once the script has finished, issue the following commands to restart the Apache service and the Crestron Virtual Control service.

```
sudo systemctl restart httpd.service

sudo systemctl restart virtualcontrol.service
```

Access the Web Configuration Interface

The VC-4-PC-3 may be monitored and configured using its web configuration interface. The web configuration interface provides selections for viewing and configuring rooms, programs, and connected devices. For more information, refer to Web Configuration on page 101.

NOTE: The web configuration interface supports the following browsers:

- Chrome® browser
- Firefox® browser
- Microsoft Edge® browser (chromium-based)
- Safari® browser

The interface can be accessed via the device IP address (for configuration and monitoring) or the XiO Cloud® service (for monitoring only) as described in the following sections.

IP Address

To access the web configuration interface via the device IP address:

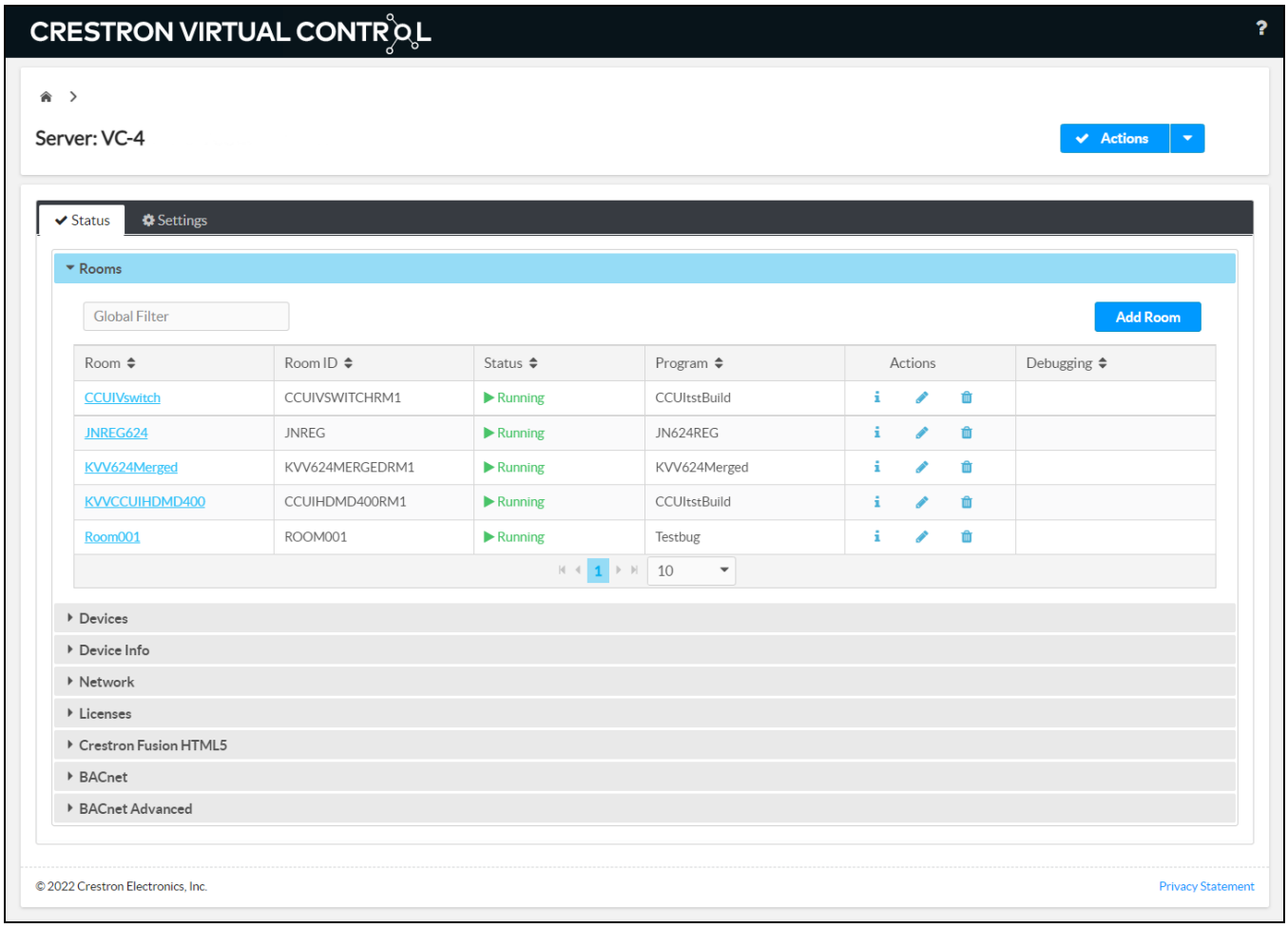
1. Enter the device IP address into a supported web browser.

   > **NOTE:** The web configuration interface can also be accessed by entering **https://[ipaddress]/VirtualControl/config/settings/** into a web browser.

2. When prompted, enter the Linux admin account username and password in the pop-up dialog box that is displayed, and then select **Sign in**.

The **Status** > **Rooms** page displays by default.

Crestron Virtual Control Web Configuration Interface



> **NOTE:** The device IP address is used to access the administrator view (read/write permissions) for the web configuration interface. To access a user/operator view (read-only permissions), enter **https://[ipaddress]/VirtualControl/config/status/** into the web browser. Within the user/operator view, the **Settings** tab and the **Action** menu are not provided for read-only access. Additionally, rooms and programs may not be added or modified.

XiO Cloud Service

The XiO Cloud® service allows the VC-4-PC-3 to be monitored from one central, secure location in the cloud.

> **NOTE:** An XiO Cloud account is required to use the service. To register for an XiO Cloud account, refer to www.crestron.com/Support/Tools/Licensing-Registration/XiO-Cloud-Registration-Room-Licenses.

To connect the VC-4-PC-3 to the XiO Cloud service:

1. Record the MAC address and serial number for the VC-4-PC-3. The MAC address and serial number are required to add the VC-4-PC-3 to the XiO Cloud service.

   > **NOTE:** The MAC address and serial number for the VC-4-PC-3 can be viewed by opening the **Device Info** accordion in the web configuration interface.

2. Log in to your XiO Cloud account at portal.crestron.io.
3. Claim the VC-4-PC-3 to the XiO Cloud service as described in the XiO Cloud User Guide.

Once the VC-4-PC-3 is claimed, select it from the cloud interface to view its status. The VC-4-PC-3 server 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 VC-4-PC-3 must be added to a licensed room before its status and settings can be viewed.

VC-4-SERVER-25 Setup

Use the following procedures to set up the VC-4-SERVER-25 following installation.

> **NOTE:** Screenshots in this section reference the VC-4-PC-3. The interface is otherwise identical.

Discover the VC-4-SERVER-25 on the Network

Crestron Toolbox™ software must be used to discover the VC-4-SERVER-25 and its IP address on the network. The IP address is required for accessing the Cockpit graphical interface or the device web configuration interface.

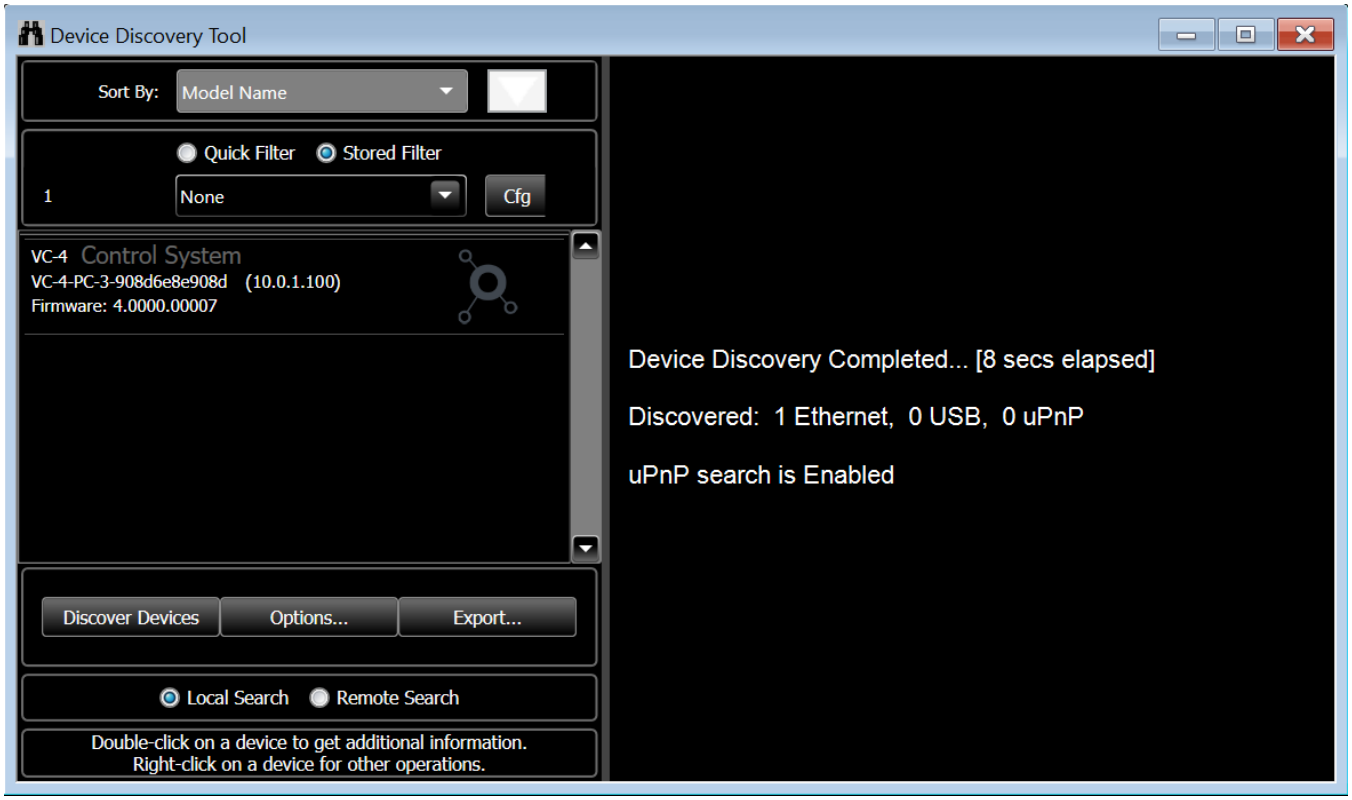
> **NOTE:** The computer running Crestron Toolbox software must be on the same subnet as the VC-4-SERVER-25.

To discover the VC-4-SERVER-25 on the network:

1. Connect the VC-4-SERVER-25 to the Ethernet network.
2. Open Crestron Toolbox software.
3. Navigate to **Tools** > **Device Discovery Tool** to open the **Device Discovery Tool**.
4. If device discovery does not start automatically, select **Discover Devices**.

If the VC-4-SERVER-25 is discovered successfully, it will appear in the left-hand results column with a default hostname of "VC-4-SERVER-25-*xxxxxxxxxx*", where *xxxxxxxxxx* is the device MAC address.

Device Discovery Tool



Access the Cockpit Graphical Interface

The VC-4-SERVER-25 provides a graphical interface (Cockpit) that is used to configure settings for the installed Alma Linux OS® Linux® operating system.

CAUTION: The Cockpit graphical interface can be used to change various settings for the Linux operating system, including advanced settings that can significantly affect the performance and stability of the operating system. Crestron recommends only configuring the settings that are described in the following sections.

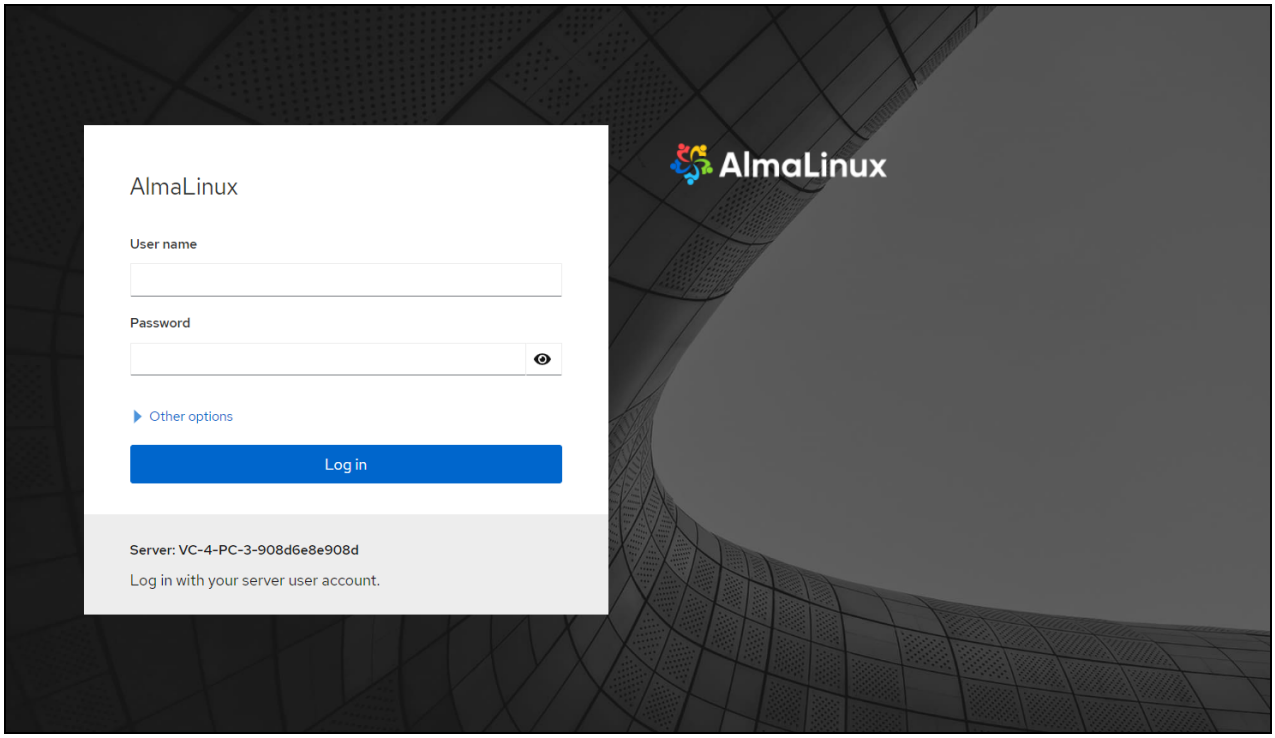
To access the Cockpit graphical interface:

1. Obtain the VC-4-SERVER-25 IP address as described in Discover the VC-4-SERVER-25 on the Network on page 76.
2. Enter **https://[ipaddress]:9090** into a web browser, where **[ipaddress]** is the VC-4-SERVER-25 IP address.

   NOTE: Port 9090 is required for accessing the Cockpit graphical interface. Ensure this port is not blocked and that no control system programs or other processes interfere with this port.

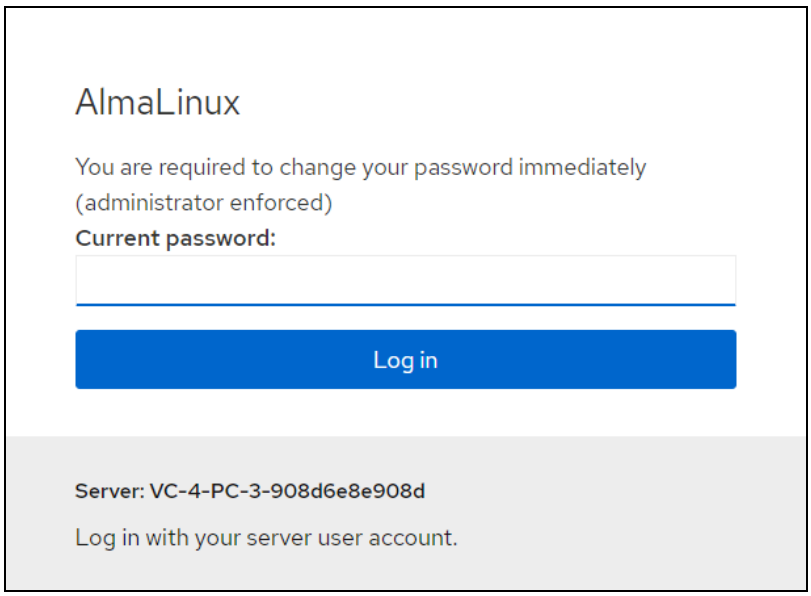
3. When prompted by your web browser, accept the self-signed certificate for the web server. The Alma Linux OS login page is displayed after the self-signed certificate is accepted.

   Alma Linux OS Login Page



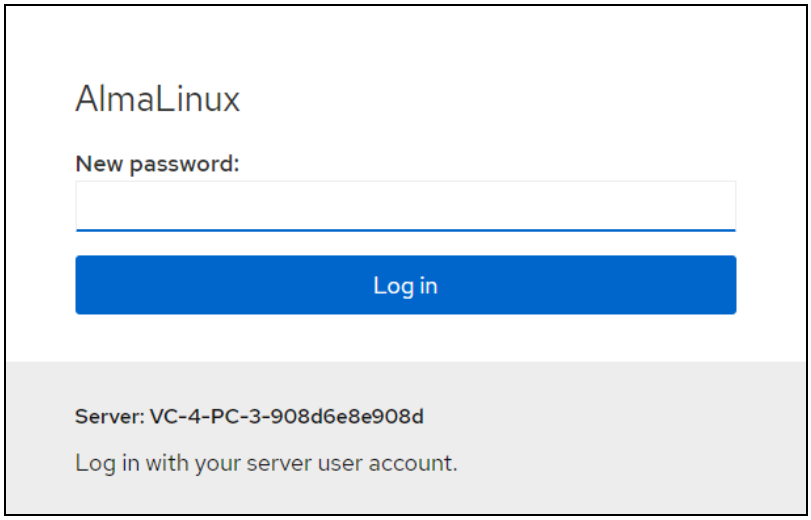
4. Enter the default username and password for the Linux admin account (**admin**/**admin**) in the appropriate text fields.
5. Select **Log in**. A prompt is displayed asking you to change the password for the Linux admin account.

   Alma Linux OS Login Page - Current password



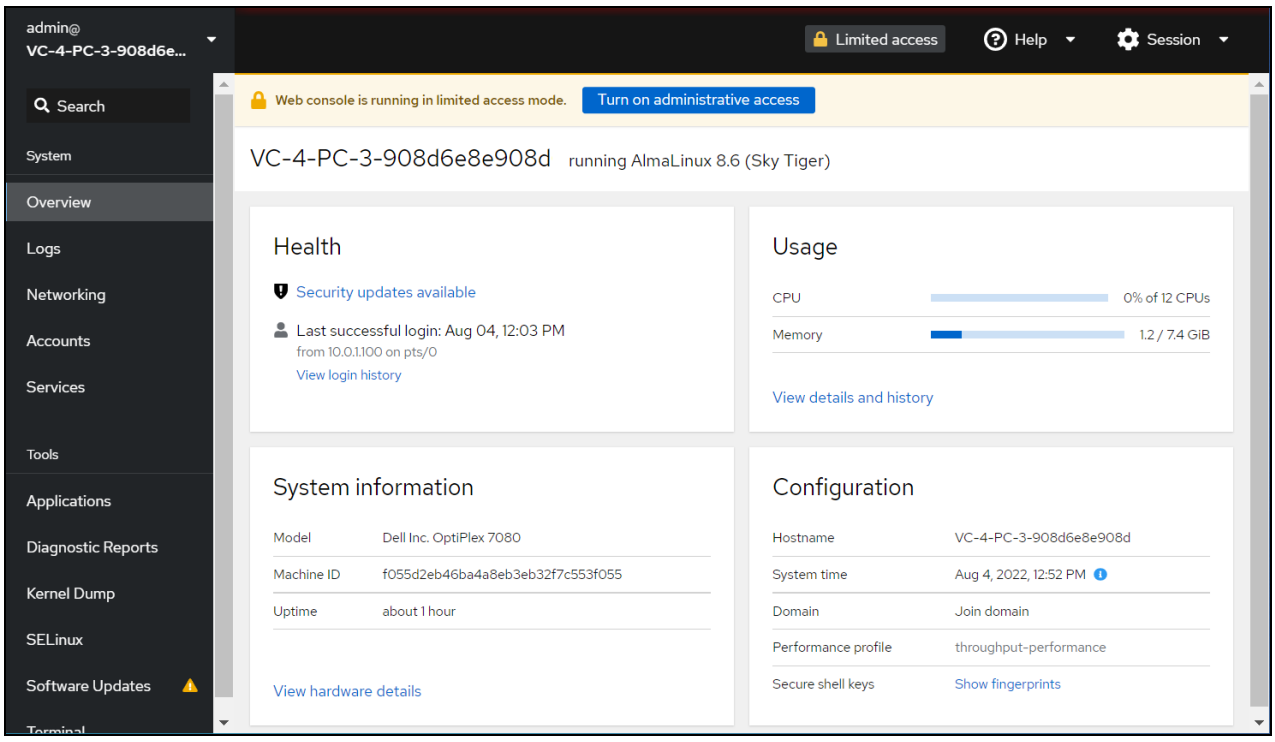
6. Enter the current password (**admin**) in the **Current password** text field, and then select **Log in**. A prompt is displayed asking you to enter a new password for the Linux admin account.

   Alma Linux OS Login Page - New password



7. Enter the new password in the **New password** text field, and then select **Log in**.
8. When prompted, confirm the password created in step 7, and then select **Log in**. The Cockpit graphical interface opens with the **Overview** page displayed.

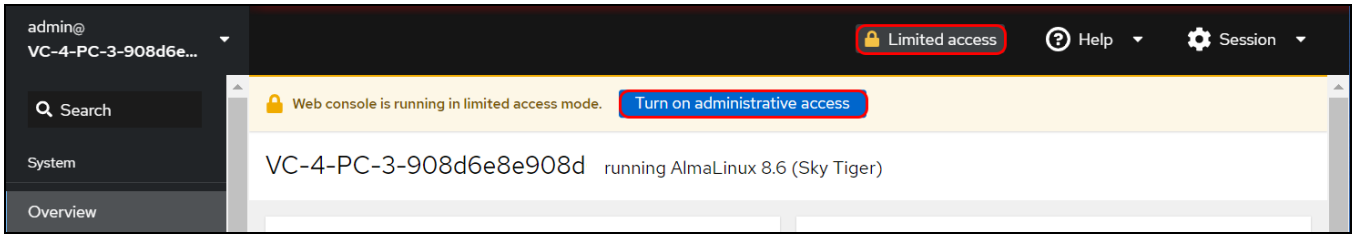
   Cockpit - Overview Page



By default, Cockpit allows only for limited access to system settings. Administrative access must be granted by selecting the **Limited access** button in the top-left corner of the page and entering the Linux

admin account password when prompted. Alternatively, if a banner is displayed stating that the web console is running in limited access mode, select the **Turn on administrative access** button.

Cockpit - Limited access Controls



Once administrative access has been granted, the **Limited access** button changes to an **Administrative access** button, and all system settings can now be configured.

Cockpit - Administrative access Controls



NOTE: Limited access can be restored by selecting the **Administrative access** button and selecting **Limit access** within the dialog box that is displayed.

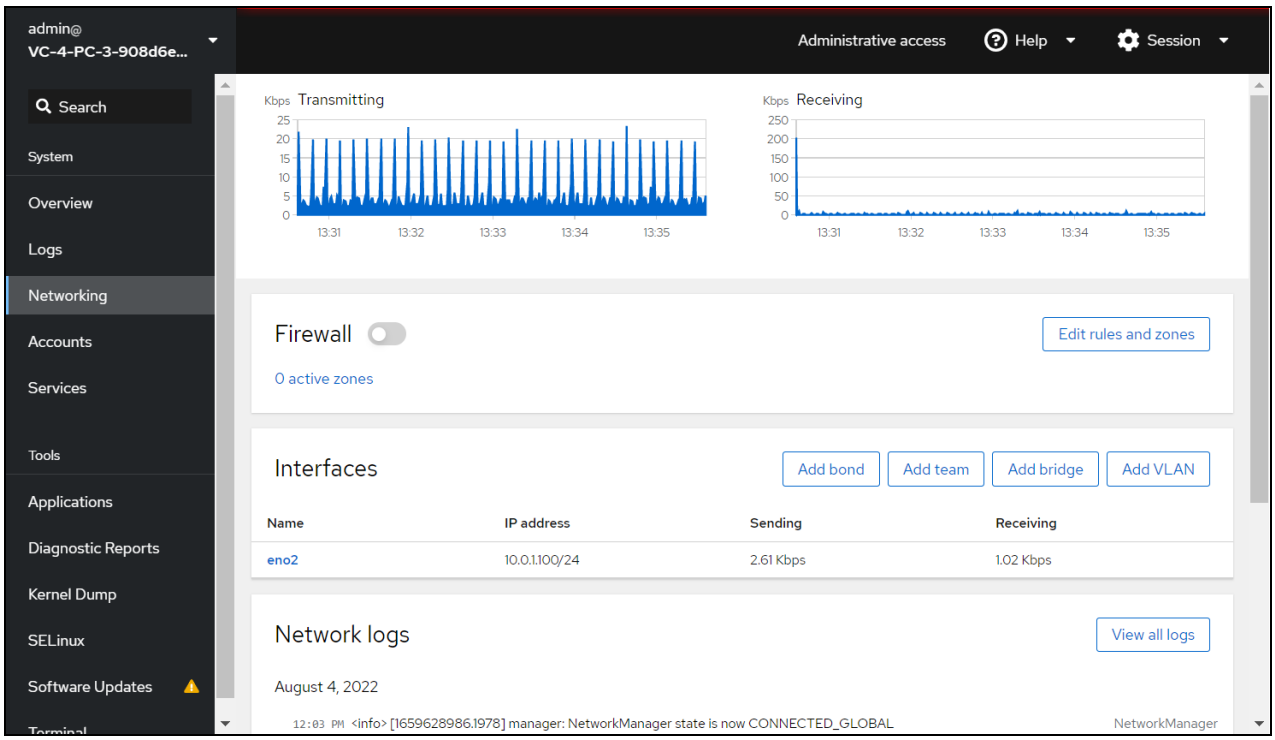
Configure a Static IP Address

The VC-4-SERVER-25 ships with DHCP turned on by default.

To set a static IP address for the device:

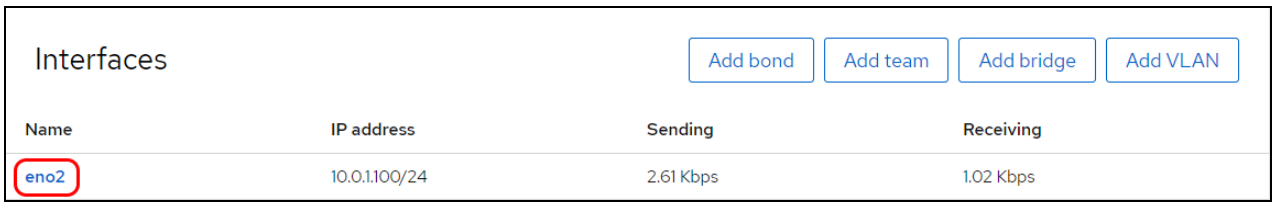
1. Select **Networking** from the navigation menu. The **Networking** page is displayed.

   Cockpit - Networking Page



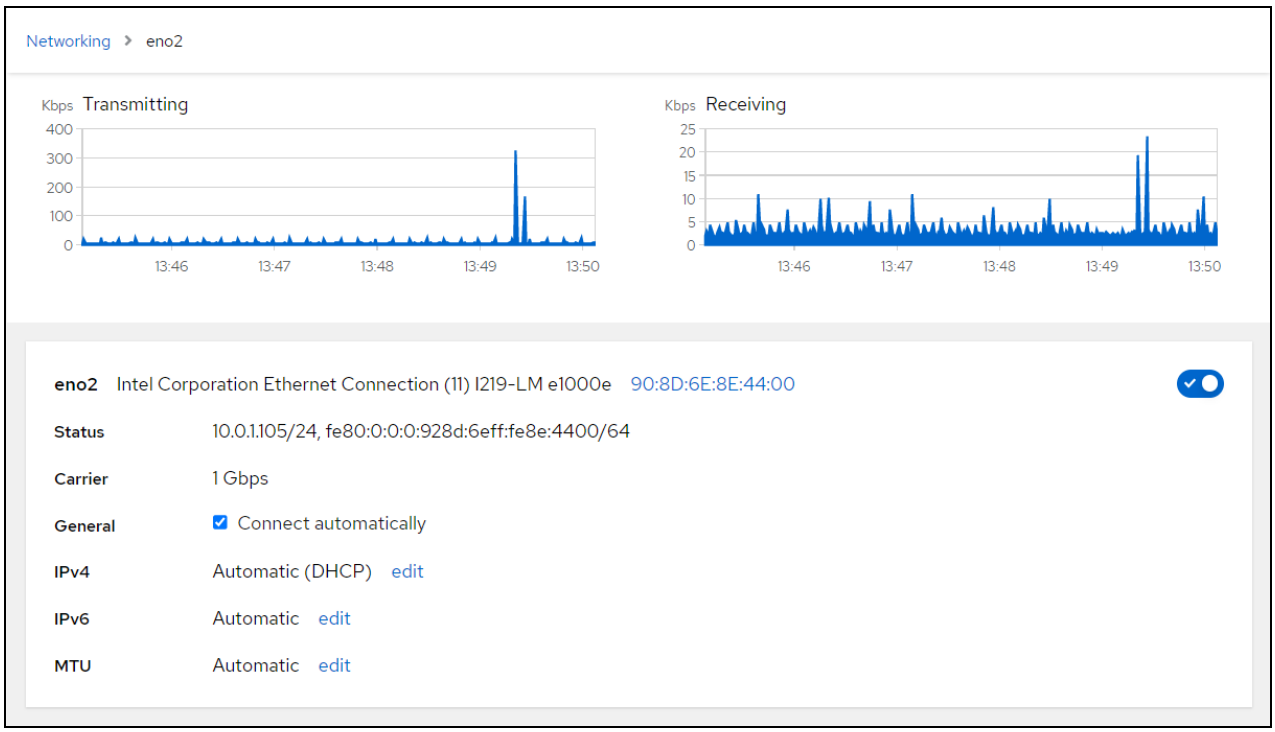
2. Within the **Interfaces** section, select the interface name that corresponds with the device IP address.

   Cockpit - Networking Page (Interfaces)



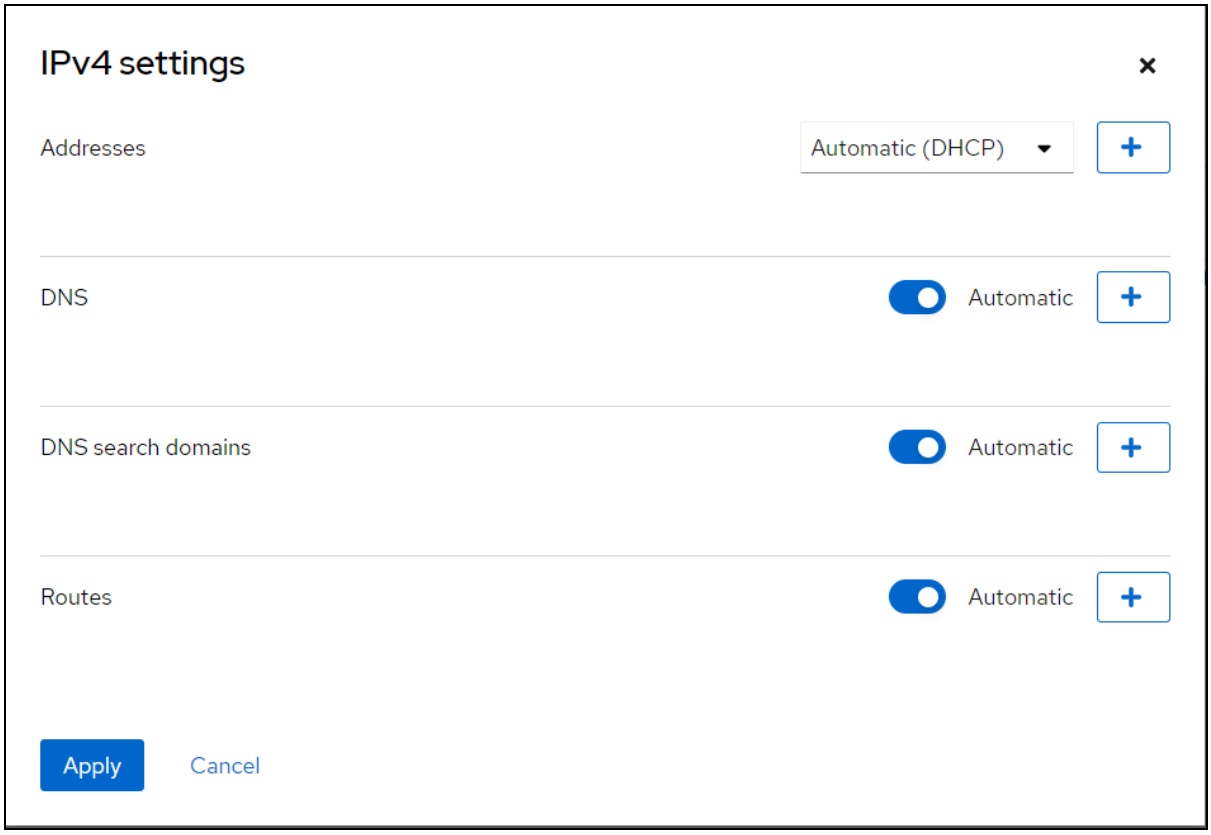
A page is displayed with network information for the selected interface.

Cockpit - Networking Page (Selected Interface)



3. Select **edit** next to the **IPv4** value. The **IPv4 settings** dialog box is displayed.

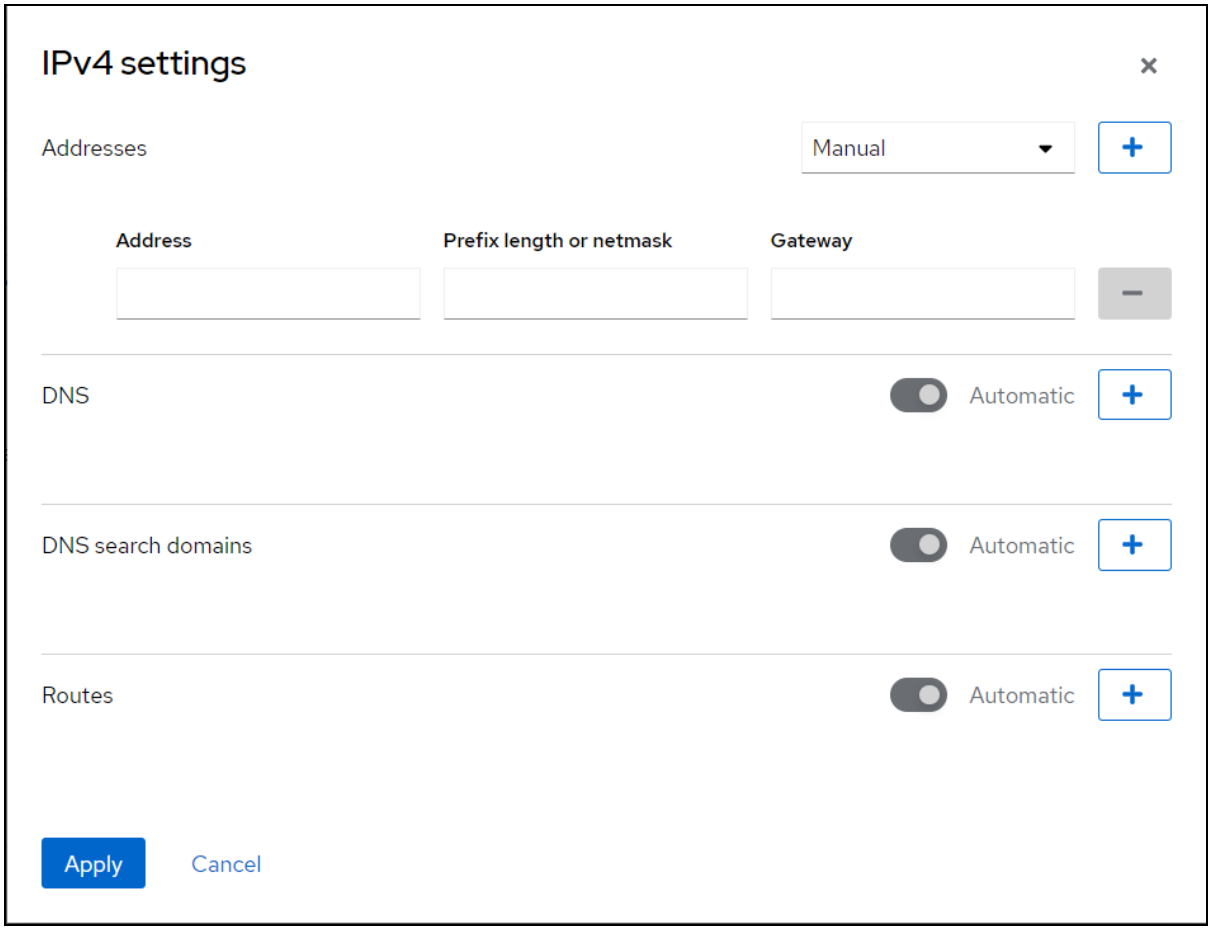
IPv4 settings Dialog Box



4. Select **Manual** from the drop-down menu within the **Addresses** section.

5. Enter the static IP address information in the text fields that are displayed.

IPv4 settings Dialog Box - Static IP Address Entry



6. Select **Apply**. The **IPv4** value for the interface will update to display the new static IP address.

NOTE: A new self-signed certificate must be generated for the web server after changing the device IP address and/or hostname. For more information, refer to Generate a New Self-Signed Certificate on page 88.

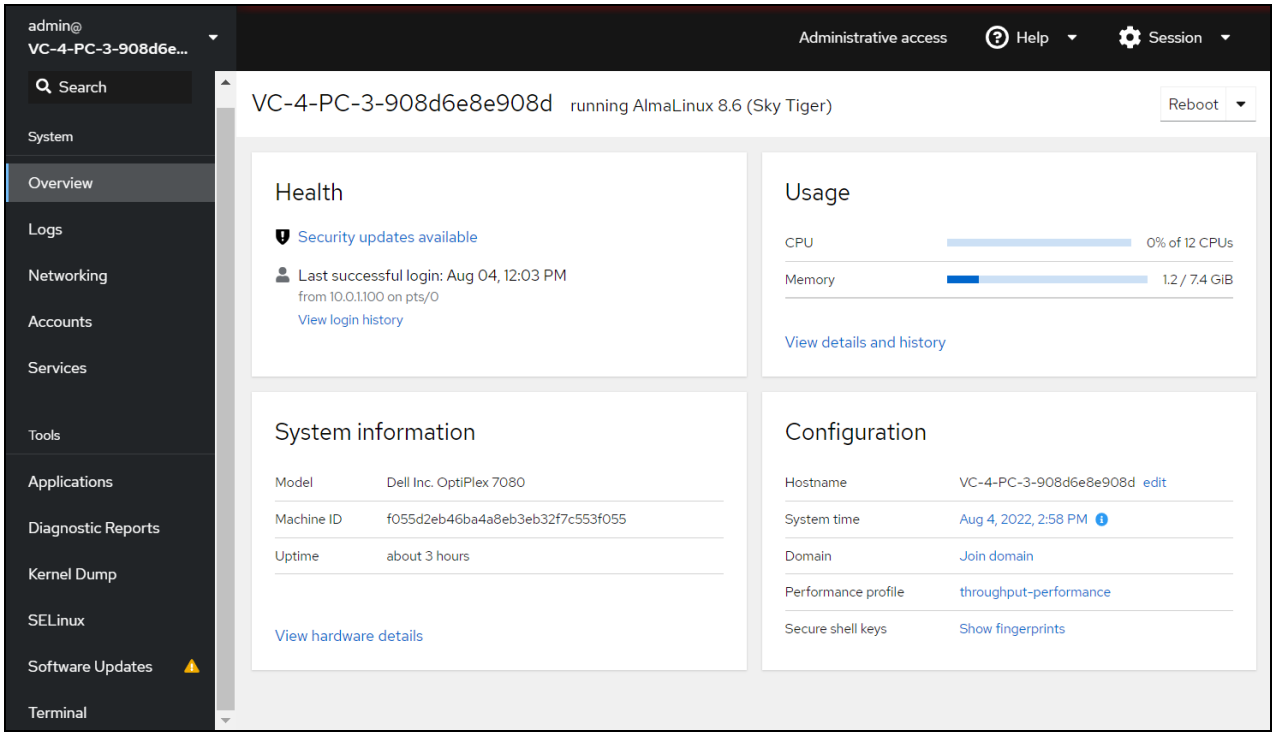
Change the Device Hostname

The VC-4-SERVER-25 ships with a default hostname of "VC-4-SERVER-25-*xxxxxxxxxx*", where *xxxxxxxxxx* is the device MAC address.

To change the hostname for the device:

1. Select **Overview** from the navigation menu. The **Overview** page is displayed.

   Cockpit - Overview Page



2. Within the **Configuration** section, select **edit** next to the **Hostname** value. The **Change host name** dialog box is displayed.

   Change host name Dialog Box



3. Enter the new device hostname in the **Real host name** text field.

NOTE: The period (.) and colon (:) characters are not valid for Linux hostnames, even though Cockpit allows these characters to be entered in the **Real host name** text field.

4. Select **Change**. The **Hostname** value for the device will update to display the new hostname.

NOTE: A new self-signed certificate must be generated for the web server after changing the device IP address and/or hostname. For more information, refer to Generate a New Self-Signed Certificate on page 88.

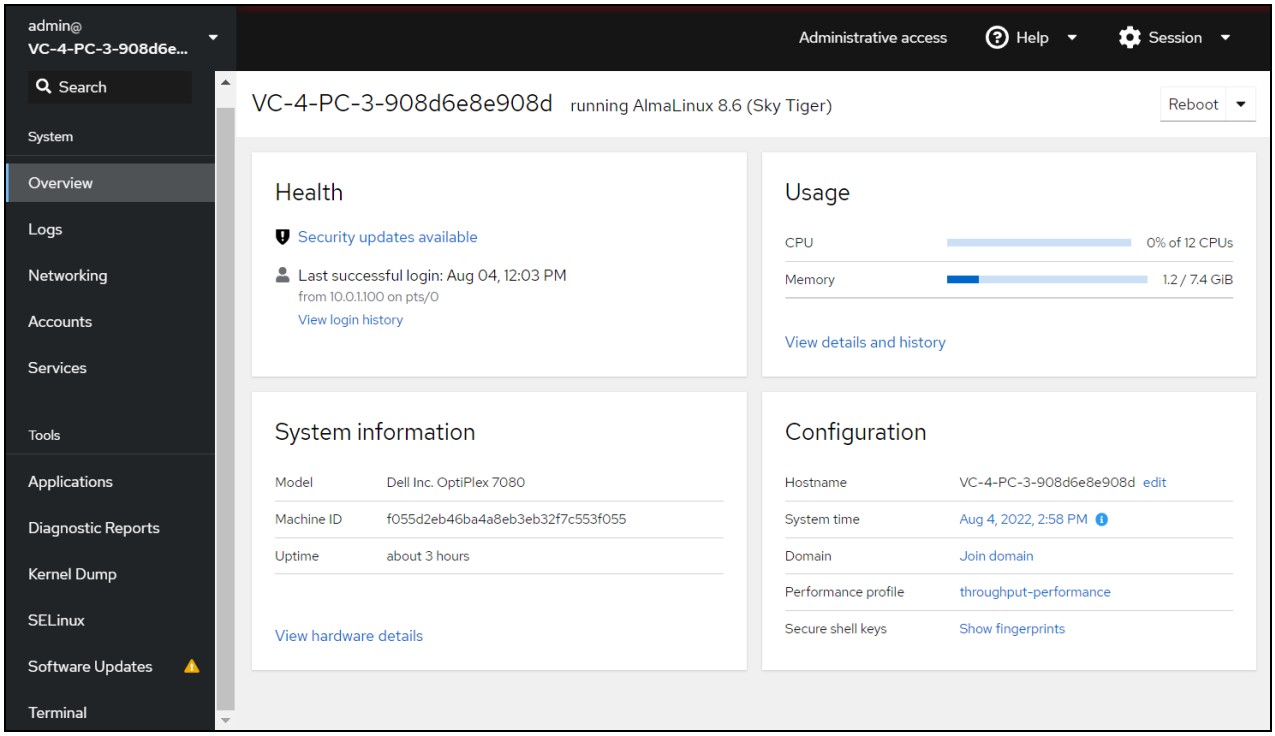
Change the Time Zone

The VC-4-SERVER-25 ships with its time zone set to **America/New York** by default. The time zone must be changed if it does not match the time zone of the VC-4-SERVER-25 installation.

To change the time zone for the device:

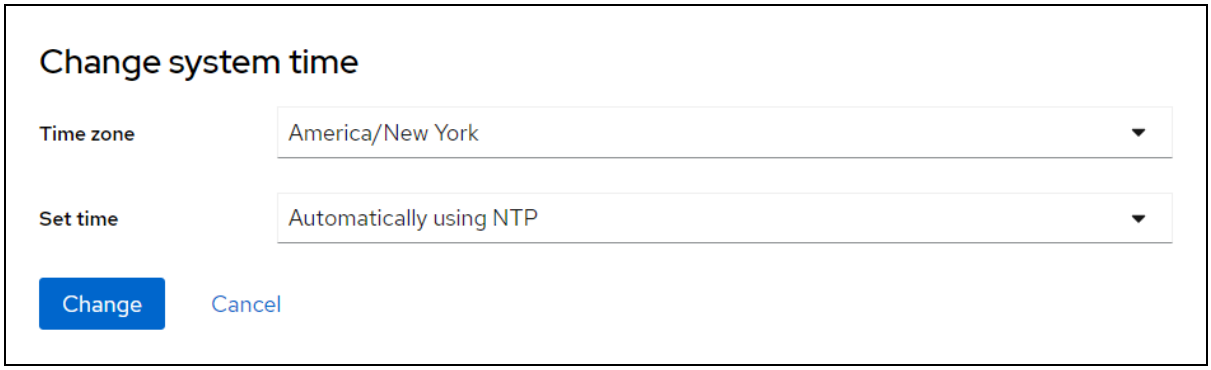
1. Select **Overview** from the navigation menu. The **Overview** page is displayed.

   Cockpit - Overview Page



2. Within the **Configuration** section, select the value listed for **System time**. The **Change system time** dialog box is displayed.

   Change system time Dialog Box



3. Use the **Time zone** drop-down menu to select the required time zone.
4. Select **Change**. The **System time** value for the device will update to reflect selected time zone.

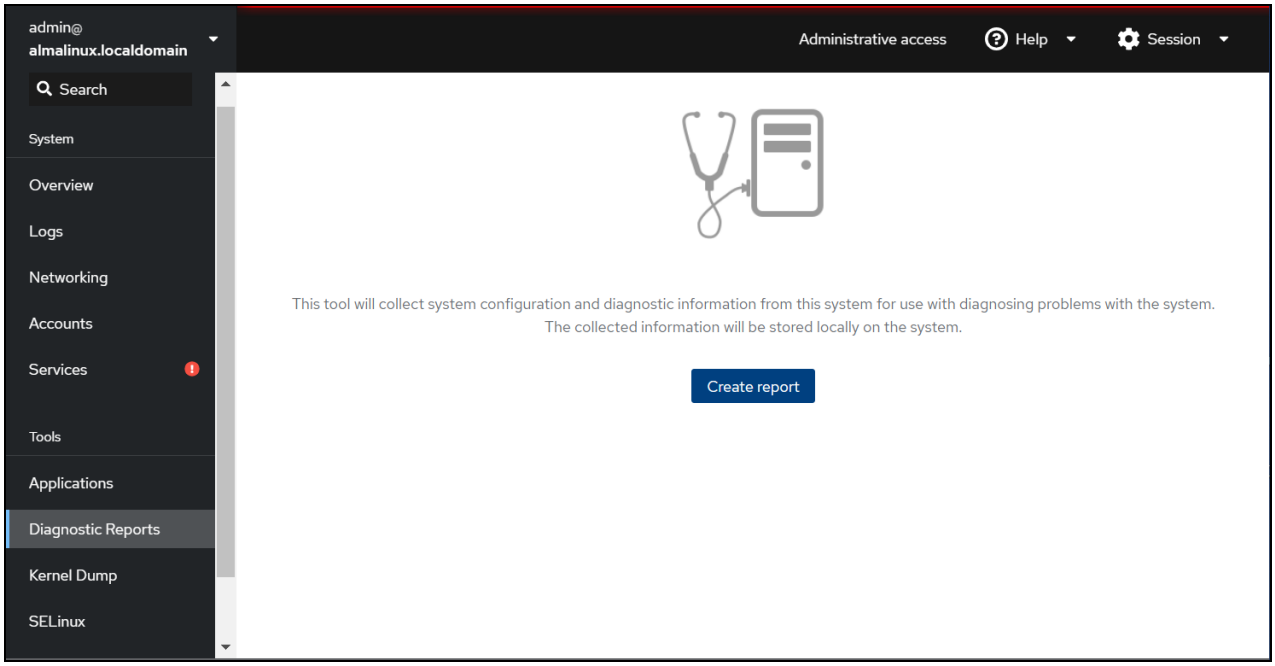
Generate System Logs

The VC-4-SERVER-25 provides support for local system logging. System logs can be generated and downloaded using Cockpit.

To generate and download system logs for the VC-4-SERVER-25:

1. Select **Diagnostic Reports** from the navigation menu. The **Diagnostic Reports** page is displayed.

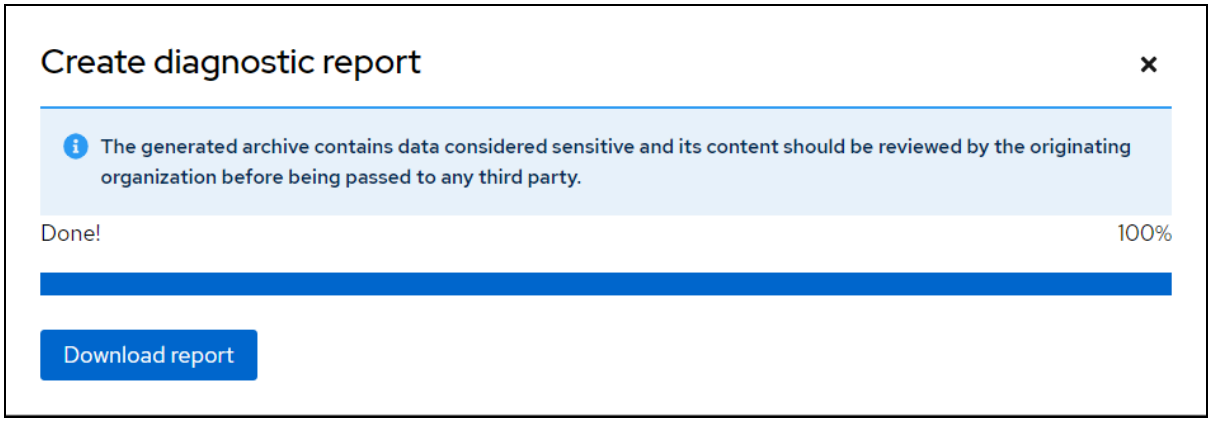
   Cockpit - Diagnostic Reports Page



2. Select **Create report**. The **Create diagnostic report** dialog box is displayed showing the status of the report generation.

3. Once the report is generated, select **Download report**. The system logs are downloaded as a compressed TAR .XZ file to the local computer.

Create diagnostic report Dialog Box



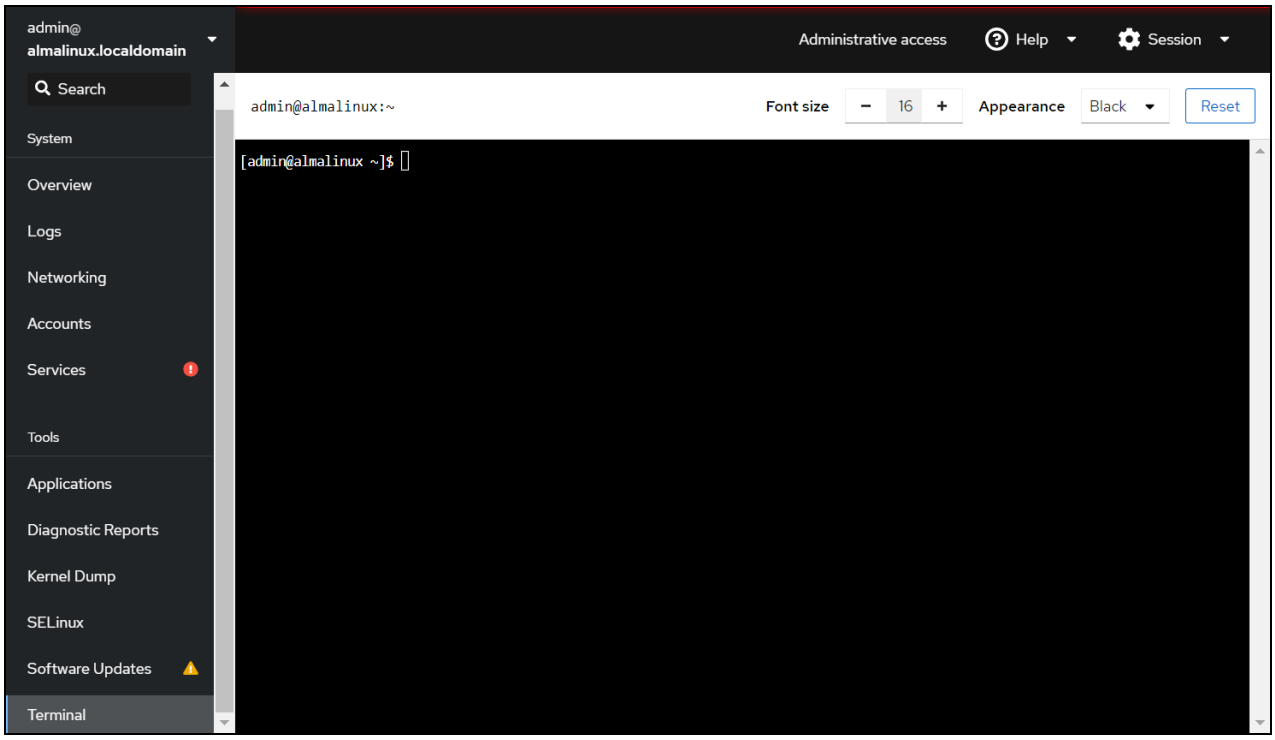
Generate a New Self-Signed Certificate

If the VC-4-SERVER-25 IP address and/or the hostname are changed, a new self-signed certificate must be generated to ensure the certificate contains the correct web server information.

To generate a new self-signed certificate for the VC-4-SERVER-25 web server:

1. Select **Terminal** from the navigation menu. The **Terminal** page is displayed with a command prompt.

Cockpit - Terminal Page

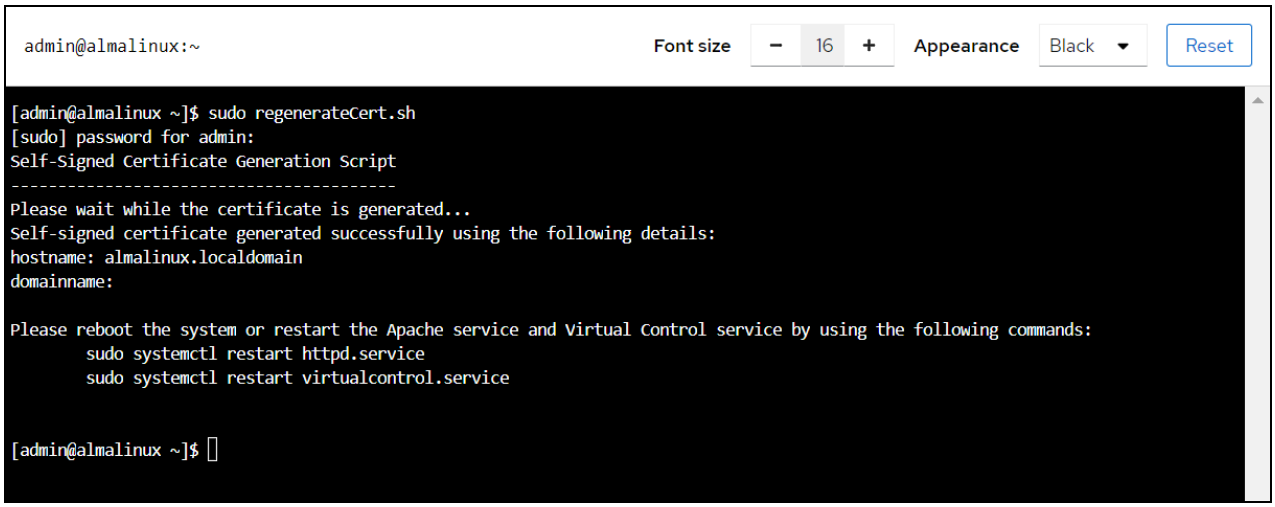


2. Issue the following command:

```
sudo regenerateCert.sh
```

3. When prompted, enter the password for the Linux admin account. The **regenerateCert.sh** script is executed to generate a new self-signed certificate.

regenerateCert Script Execution



4. Once the script has finished, issue the following commands to restart the Apache service and the Crestron Virtual Control service.

```
sudo systemctl restart httpd.service

sudo systemctl restart virtualcontrol.service
```

Access the Web Configuration Interface

The VC-4-SERVER-25 may be monitored and configured using its web configuration interface. The web configuration interface provides selections for viewing and configuring rooms, programs, and connected devices. For more information, refer to Web Configuration on page 101.

NOTE: The web configuration interface supports the following browsers:

- Chrome® browser
- Firefox® browser
- Microsoft Edge® browser (chromium-based)
- Safari® browser

The interface can be accessed via the device IP address (for configuration and monitoring) or the XiO Cloud® service (for monitoring only) as described in the following sections.

IP Address

To access the web configuration interface via the device IP address:

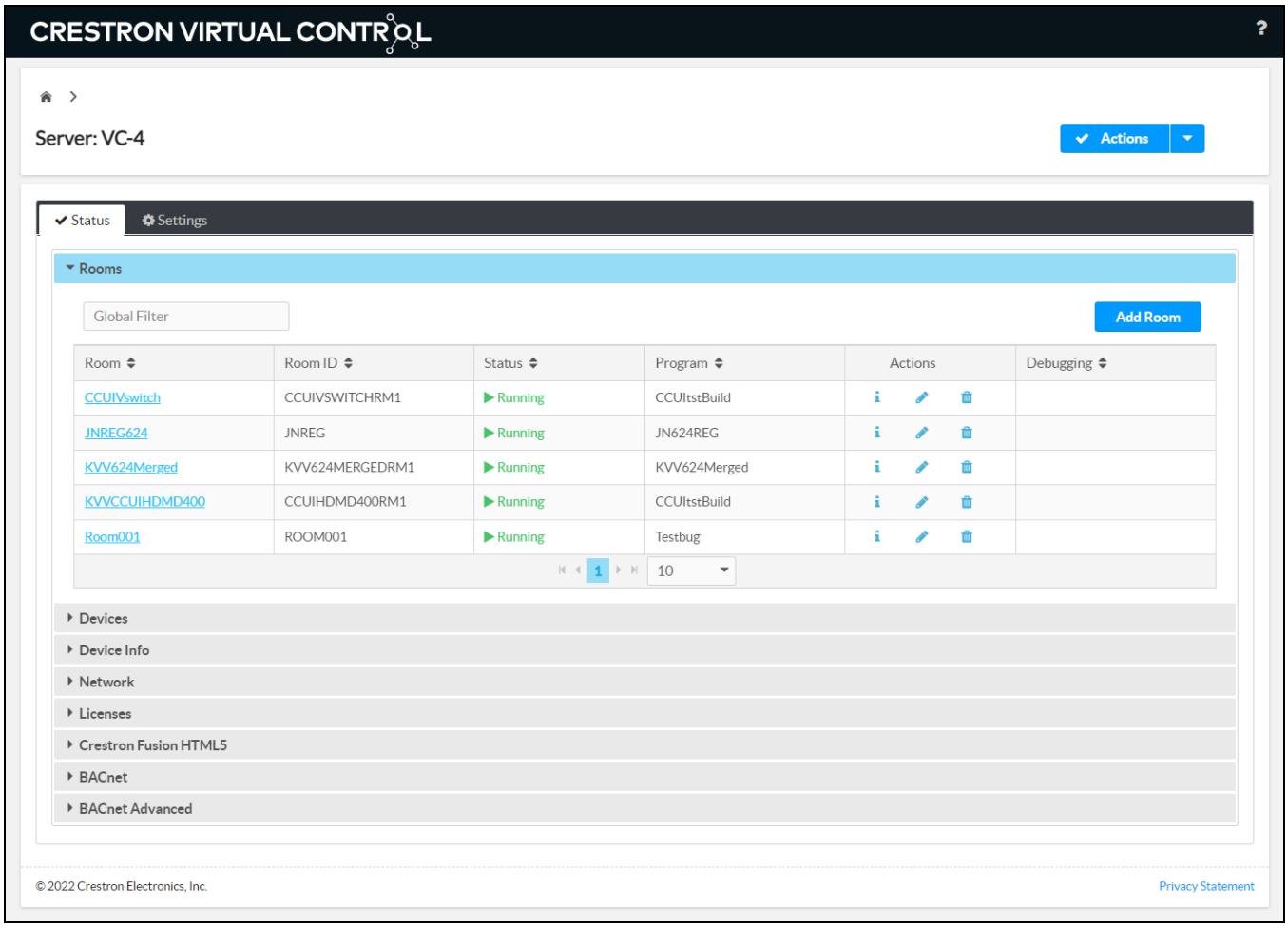
1. Enter the device IP address into a supported web browser.

   > **NOTE:** The web configuration interface can also be accessed by entering **https://[ipaddress]/VirtualControl/config/settings/** into a web browser.

2. When prompted, enter the Linux admin account username and password in the pop-up dialog box that is displayed, and then select **Sign in**.

The **Status** > **Rooms** page displays by default.

Crestron Virtual Control Web Configuration Interface



> **NOTE:** The device IP address is used to access the administrator view (read/write permissions) for the web configuration interface. To access a user/operator view (read-only permissions), enter **https://[ipaddress]/VirtualControl/config/status/** into the web browser. Within the user/operator view, the **Settings** tab and the **Action** menu are not provided for read-only access. Additionally, rooms and programs may not be added or modified.

XiO Cloud Service

The XiO Cloud® service allows the VC-4-SERVER-25 to be monitored from one central, secure location in the cloud.

> **NOTE:** An XiO Cloud account is required to use the service. To register for an XiO Cloud account, refer to www.crestron.com/Support/Tools/Licensing-Registration/XiO-Cloud-Registration-Room-Licenses.

To connect the VC-4-SERVER-25 to the XiO Cloud service:

1. Record the MAC address and serial number for the VC-4-SERVER-25. The MAC address and serial number are required to add the VC-4-SERVER-25 to the XiO Cloud service.

   > **NOTE:** The MAC address and serial number for the VC-4-SERVER-25 can be viewed by opening the **Device Info** accordion in the web configuration interface.

2. Log in to your XiO Cloud account at portal.crestron.io.
3. Claim the VC-4-SERVER-25 to the XiO Cloud service as described in the XiO Cloud User Guide.

Once the VC-4-SERVER-25 is claimed, select it from the cloud interface to view its status. The VC-4-SERVER-25 server 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 VC-4-SERVER-25 must be added to a licensed room before its status and settings can be viewed.

Manage Licenses

The Crestron Virtual Control licensing model is similar to a traditional hardware purchase model: purchase a specified number of room licenses (VC-4-ROOM), and the Crestron Virtual Control installation will run the number of rooms purchased. Each room license also includes one software mobility license (SW-MOBILITY) that enables functionality for various Crestron software solutions.

The number of rooms that may be run on the Crestron Virtual Control server is based on the number of purchased licenses. The Crestron Virtual Control server has an initial 90-day grace period, during which a maximum number of 500 rooms may be run. After the grace period expires, existing rooms may no longer be run, and new rooms may not be added to the server until the appropriate licenses are purchased.

NOTES:

- The VC-4-PC-3 includes three room licenses that must be applied and does not provide a 90-day grace period.
- The VC-4-SERVER-25 includes 25 room licenses that must be applied and does not provide a 90-day grace period.

For Crestron Virtual Control installations that will interface with BACnet network/IP based equipment, an SW-VC4-BN-1000 license is also available that enables support for up to 1000 BACnet objects per license.

Crestron Virtual Control provides two licensing options: online licensing via the XiO Cloud® service, or offline licensing via the USB-OFFLINE dongle. Each licensing mode is covered in the following sections.

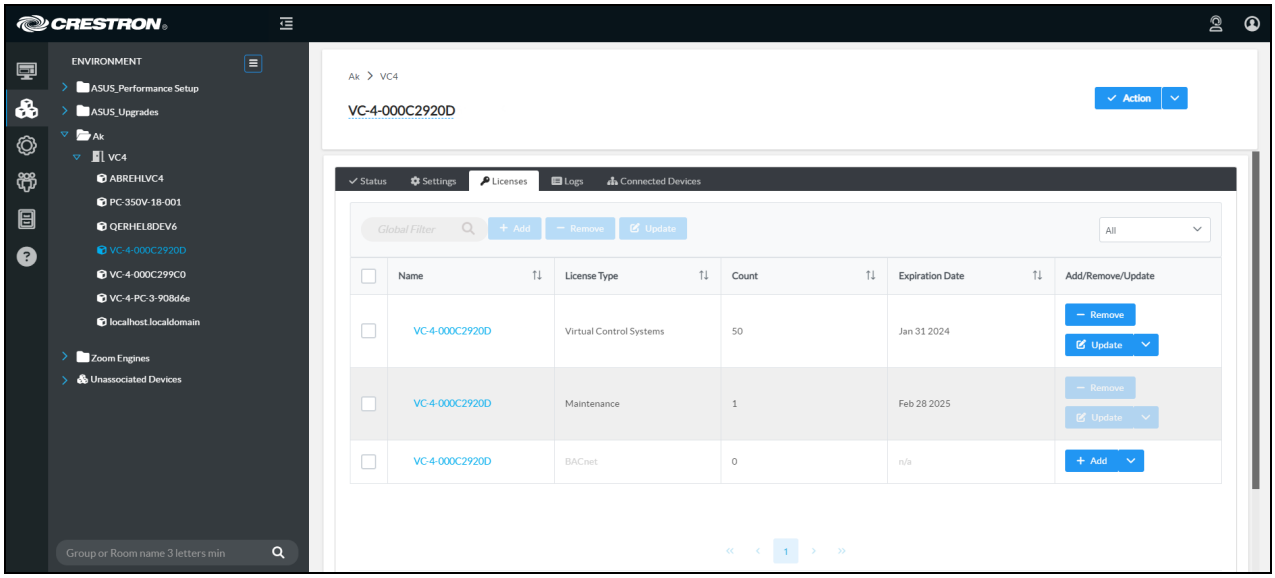
- Manage Licenses with XiO Cloud on page 93
- Manage Licenses Offline on page 95

Manage Licenses with XiO Cloud

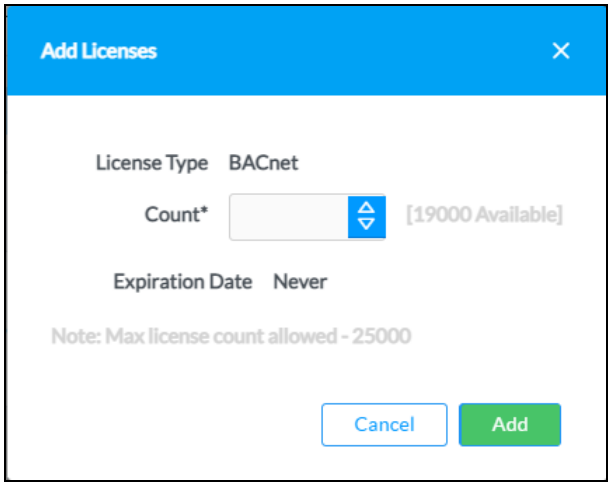
Purchased Crestron Virtual Control licenses can be managed through the XiO Cloud® service portal. For more information on using XiO Cloud, refer to the XiO Cloud Service User Guide.

To add and manage Crestron Virtual Control licenses within XiO Cloud:

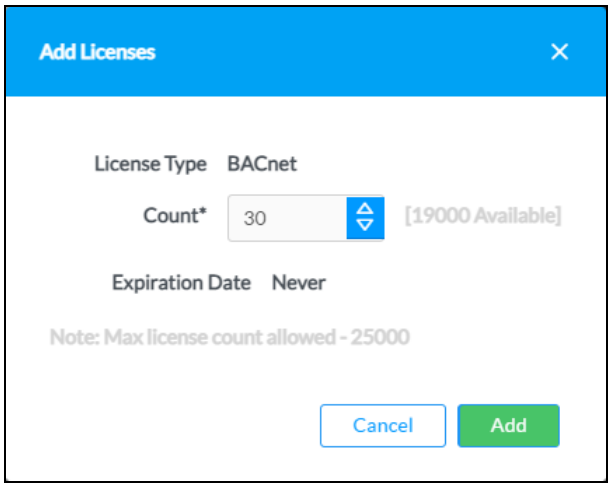
1. Place your Crestron Virtual Control room or BACnet license order(s) with Crestron using the provided form.
2. Claim your installed Crestron Virtual Control server or VC-4-PC-3 to your XiO Cloud account as described in the XiO Cloud Service User Guide.
3. Navigate to your Crestron Virtual Control server or VC-4-PC-3 in the **ENVIRONMENT** menu tree in XiO Cloud.
4. Select the **Licenses** tab in the device settings.



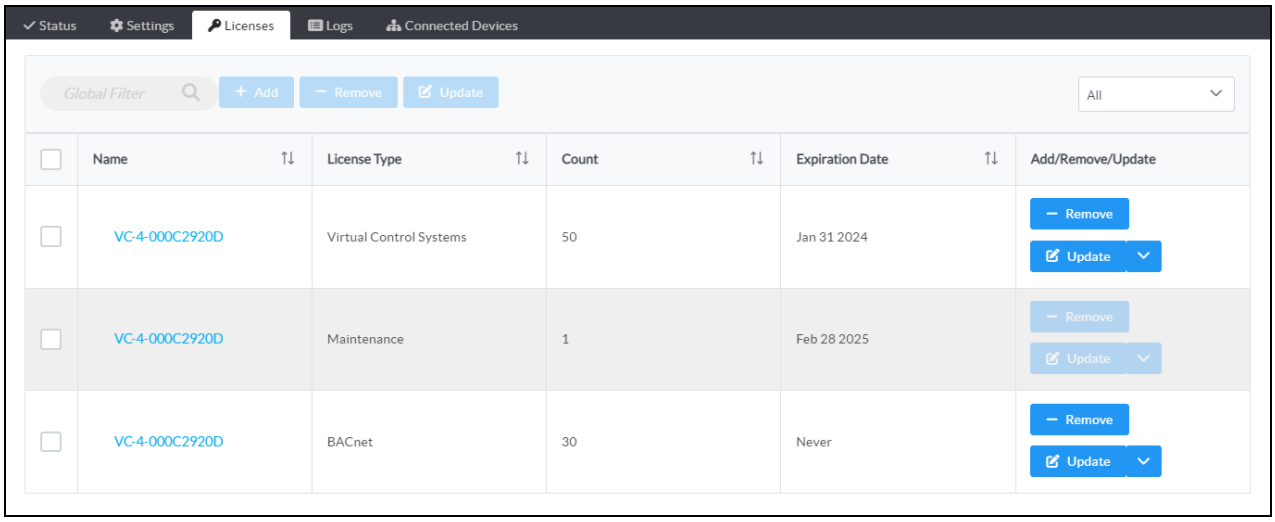
5. Select **+ Add** next to the license type that should be added. The **Add Licenses** dialog box is displayed.



6. Enter the number of licenses that you would like added to your Crestron Virtual Control server or VC-4-PC-3 in the **Count** text field. The total available licenses are shown next to this text field.



7. Select **Add**. The **Licenses** tab updates to show that the selected licenses have been added to the Crestron Virtual Control server or VC-4-PC-3.



The following functions are also provided:

- Select **Update** to update the number of licenses that are available for the Crestron Virtual Control server or VC-4-PC-3.
- Select **- Remove** to remove the license from the Crestron Virtual Control server or VC-4-PC-3. The license is added back to your license pool.

Manage Licenses Offline

Purchased Crestron Virtual Control licenses can be managed offline via the USB-OFFLINE dongle as described in the following procedures.

IMPORTANT! Any existing Crestron Virtual Control licenses within the XiO Cloud service cannot be converted to offline licenses. If switching your Crestron Virtual Control installation from online to offline licensing mode, new room and/or BACnet licenses must be purchased.

NOTE: The USB-OFFLINE dongle must be connected to the VC-4-PC-3 or the host running VC-4 at all times. If the USB-OFFLINE dongle is removed, all licensed rooms will stop, licensed BACnet objects will no longer function, and an error message will be displayed within the web configuration interface indicating that there is no dongle detected.

Configure Offline Licensing Mode

Each Crestron Virtual Control installation that will use offline licensing requires the purchase of one USB-OFFLINE dongle. Once all Crestron Virtual Control licenses and the USB-OFFLINE have been purchased, the offline license mode must be configured using the provided license utility or through the web configuration interface.

To configure your Crestron Virtual Control installation for offline licensing:

1. Order your Crestron Virtual Control room license(s), BACnet licenses (if needed) and one USB-OFFLINE dongle per VC-4 server or VC-4-PC-3.

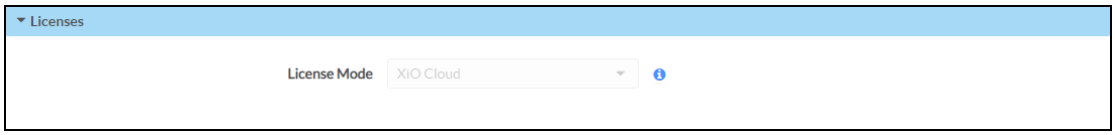
   NOTE: Each offline license key is matched to a unique system key. Therefore, a single USB-OFFLINE dongle cannot be used by more than one Crestron Virtual Control installation at the same time, and multiple dongles cannot be used within a single Crestron Virtual Control installation.

2. For Crestron Virtual Control installations licensed through the XiO Cloud service, remove all existing licenses as described in the XiO Cloud Service User Guide.

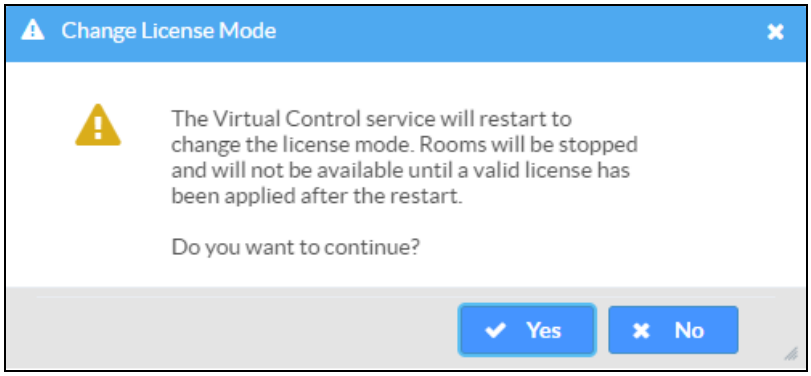
   NOTE: Ensure the VC-4 server or VC-4-PC-3 is online within XiO Cloud prior to removing your existing licenses.

3. Upgrade the VC-4 software to version 4.0000.00057 or later. This is the minimum version that supports offline licensing and includes the license utility.
   - To upgrade software for the VC-4 server, refer to Upgrade or Downgrade Crestron Virtual Control on page 39.
   - To upgrade software for the VC-4-PC-3, refer to Upgrade or Downgrade the VC-4-PC-3 on page 45.
4. Upon successful upgrade, restart the VC-4 server or VC-4-PC-3.
5. Connect the USB-OFFLINE dongle into an available USB port on the VC-4-PC-3 or make it available on the host running VC-4.

6. Switch the license mode using one of the following methods.
   - To use the web configuration interface:
     a. Access the web configuration interface as described in Web Configuration on page 101.
     b. Open the **Settings** tab and then expand the **Licenses** accordion.



     c. Select **Offline Dongle** from the **License Mode** drop-down menu.
     d. When prompted, select **Yes** confirm the selection.



     The Crestron Virtual Control service restarts in the new license mode.

   - To use the **licenseUtility.sh** script:
     a. Open a new terminal window.
     b. (VC-4 server only) Change directories to **/[VirtualControlHome]/scripts**, where **[VirtualControlHome]** is the home directory set during installation.
     c. Issue the following depending on your Crestron Virtual Control installation:
        - For VC-4 servers, issue `./licenseUtility.sh`.
        - For the VC-4-PC-3, issue `licenseUtility.sh`.

     The **licenseUtility.sh** script opens the license utility with the following options:

```
help                          - Lists the help menu
getlicenseinfo                - Shows the current license information
getmode                       - Gets the current license mode
switchmode [1 | 2]            - Switches the current license mode to XiO Cloud
(1) or Offline (2) licensing
addlicense [LICENSEKEY]       - Adds license into control system. User must
pass the "LICENSEKEY"
dellicense                    - Deletes the current license from the control
system
exit                          - Exits this utility
```

     d. Issue `switchmode 2` to switch the license mode from online (XiO Cloud) to offline.

> **NOTE:** All Crestron Virtual Control installations are placed in online license mode by default.

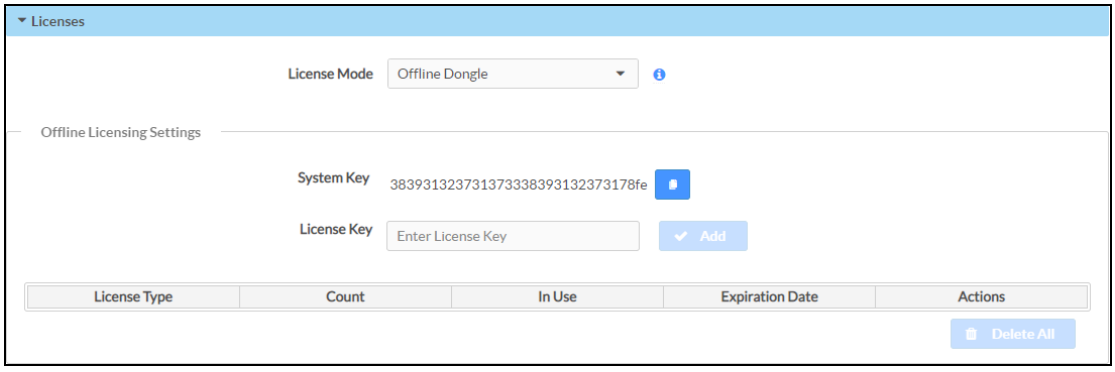
e. Issue `exit` to exit the utility, then issue `sudo systemctl restart virtualcontrol` in the terminal to restart the Crestron Virtual Control service.

Request an Offline License Key

Once the offline license mode has been configured, a license key must then be requested that allows the Crestron Virtual Control installation to validate its licenses offline. Offline license keys are tied to a specific VC-4 system key and number of room licenses or BACnet licenses. If room licenses or BACnet licenses need to be added to a Crestron Virtual Control installation, a new offline license key must be requested.

> **NOTE:** Room licenses and BACnet licenses do not share an offline license key. For Crestron Virtual Control installations that require both license types, two unique offline license keys must be requested and applied.

1. Ensure the USB-OFFLINE dongle is connected to the VC-4-PC-3 or the host running VC-4 and that offline licensing mode has been configured as described in Configure Offline Licensing Mode on page 95.
2. Obtain the VC-4 system key using one of the following methods. The system key will be required in the next step.
   - To use the web configuration interface:
     a. Access the web configuration interface as described in Web Configuration on page 101.
     b. Open the **Settings** tab and then expand the **Licenses** accordion.



     c. Record or use the copy button to copy the value provided in the **System Key** text field.
   - To use the **licenseUtility.sh** script:
     a. Open a new terminal window.
     b. (VC-4 server only) Change directories to **/[VirtualControlHome]/scripts**, where **[VirtualControlHome]** is the home directory set during installation.

c. Issue the following depending on your Crestron Virtual Control installation:
   - For VC-4 servers, issue `./licenseUtility.sh`.
   - For the VC-4-PC-3, issue `licenseUtility.sh`.

   The **licenseUtility.sh** script opens the license mode utility with the following options:

```
help                          - Lists the help menu
getlicenseinfo                - Shows the current license information
getmode                       - Gets the current license mode
switchmode [1 | 2]            - Switches the current license mode to XiO Cloud
(1) or Offline (2) licensing
addlicense [LICENSEKEY]       - Adds license into control system. User must
pass the "LICENSEKEY"
dellicense                    - Deletes the current license from the control
system
exit                          - Exits this utility
```

d. Issue `getlicenseinfo` , and then record the value listed for **System Key**.

3. Fill out and submit the offline licensing form to request an offline license key from Crestron.
   - When requesting a new offline license key, the following information is required:
     - The VC-4 system key (obtained using the license mode utility or web configuration interface as described in step 2 above)
     - The number of purchased room or BACnet licenses
     - The PO (Purchase Order) number for the room licenses or BACnet licenses
     - The USB-OFFLINE dongle serial number (located on the dongle or on its packaging)
   - When updating an existing offline license key, the following information is required:
     - The VC-4 system key (obtained using the license mode utility or web configuration interface as described in step 2 above)
     - The number of additional room licenses or BACnet licenses purchased
     - The PO (Purchase Order) number for the new room licenses or BACnet licenses
     - The USB-OFFLINE dongle serial number (located on the dongle or on its packaging)
     - The current offline license key
     - The current number of room licenses or BACnet licenses (located within the **Licenses** status accordion in the VC-4 web configuration interface)

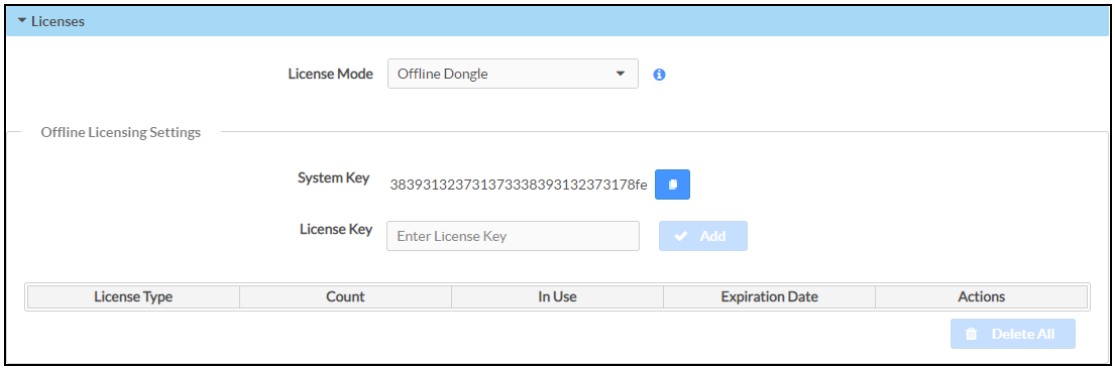
Crestron will send the offline license key via email once the request has been processed. The offline license key must then be applied to the Crestron Virtual Control installation as described in Apply the Offline License Key on page 99.

Apply the Offline License Key

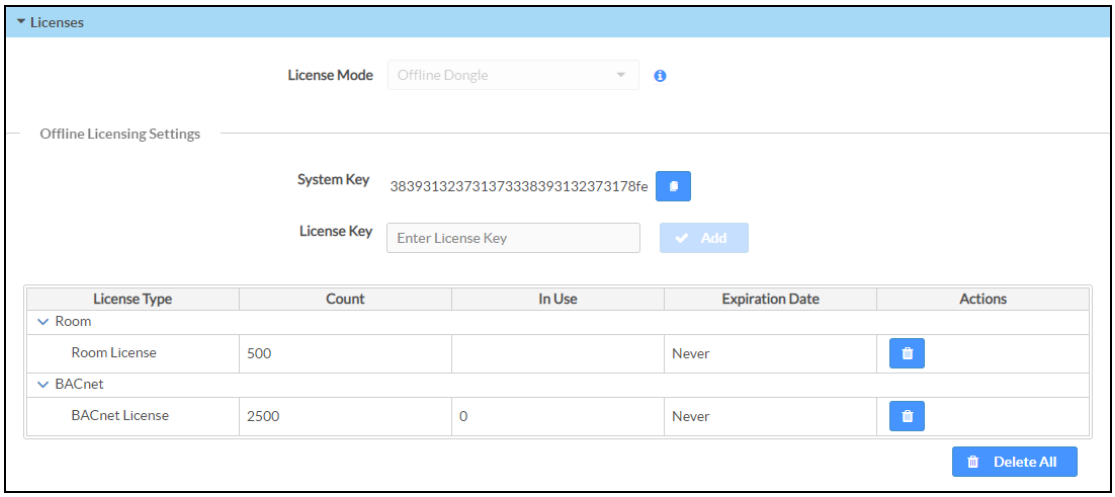
Once an offline license key has been obtained as described in Request an Offline License Key on page 97, it must be applied to your Crestron Virtual Control installation using the provided license utility.

To apply the offline license key:

1. Ensure the USB-OFFLINE dongle is connected to the VC-4-PC-3 or the host running VC-4 and that offline licensing mode has been configured as described in Configure Offline Licensing Mode on page 95.
2. Apply the offline license key using one of the following methods.
   - To use the web configuration interface:
     a. Access the web configuration interface as described in Web Configuration on page 101.
     b. Open the **Settings** tab and then expand the **Licenses** accordion.



     c. Enter the license key provided by Crestron into the **License Key** text field.
     d. Select **Add**. The provided licenses are populated in the table below this setting automatically.



- To use the **licenseUtility.sh** script:
  a. Open a new terminal window.
  b. (VC-4 server only) Change directories to **/[VirtualControlHome]/scripts**, where **[VirtualControlHome]** is the home directory set during installation.
  c. Issue the following depending on your Crestron Virtual Control installation:
     - For VC-4 servers, issue `./licenseUtility.sh`.
     - For the VC-4-PC-3, issue `licenseUtility.sh`.

     The **licenseUtility.sh** script opens the license mode utility with the following options:

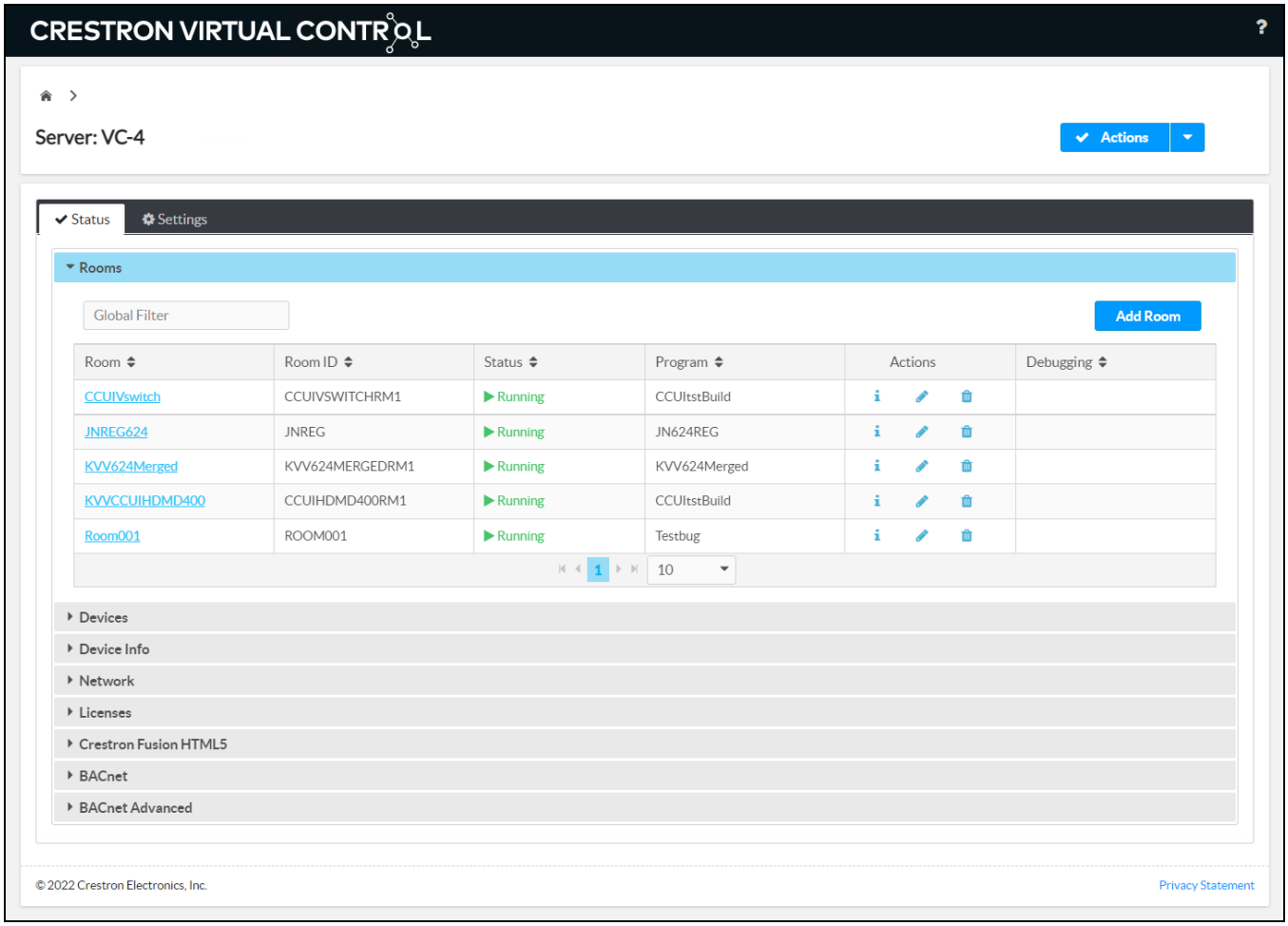
```
help                          - Lists the help menu
getlicenseinfo                - Shows the current license information
getmode                       - Gets the current license mode
switchmode [1 | 2]            - Switches the current license mode to XiO Cloud
(1) or Offline (2) licensing
addlicense [LICENSEKEY]       - Adds license into control system. User must
pass the "LICENSEKEY"
dellicense                    - Deletes the current license from the control
system
exit                          - Exits this utility
```

  d. Issue `addlicense [licensekey]`, where `[licensekey]` is the offline license key provided by Crestron.
  e. Issue `exit` to exit the utility.
  f. To ensure all licensed rooms are started immediately, issue `sudo systemctl restart virtualcontrol` to restart the Crestron Virtual Control service.

Web Configuration

The Crestron Virtual Control server may be monitored and configured using its web configuration interface. The interface can be accessed via the server IP address or the XiO Cloud® service as described in VC-4 Setup on page 55 and VC-4-PC-3 Setup on page 61.

Web Configuration Interface



NOTE: The following sections describe the web configuration interface for a read/write (administrator) view. The read-only (operator/user) view uses a subset of the documented controls.

A home button and the server name are provided in the top-left corner of the web configuration interface. The home button can be used to return to the default page of the interface. A help button is also provided in the top-right corner of the web configuration interface that can be used to access this documentation.

Server Name and Navigation Controls



The configuration interface provides the following tabs:

- **Status**: Used to monitor Crestron Virtual Control server status. Also used to configure and monitor rooms, programs, and connected devices.
- **Settings**: Used to configure Crestron Virtual Control server settings.

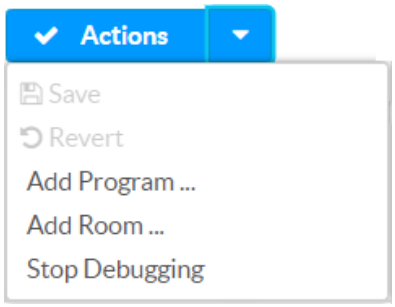
The **Status** tab is the default tab that is displayed, as shown in the preceding image.

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.

> **NOTE:** The **Actions** menu provides different selections depending on whether it is accessed from the general web interface or from a specific room page. For more information on the selections provided from a room page, refer to Action Menu (Rooms) on page 109.

Actions Menu (General)



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

Save

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

Revert

Select **Revert** to revert Crestron Virtual Control back to the last saved configuration settings.

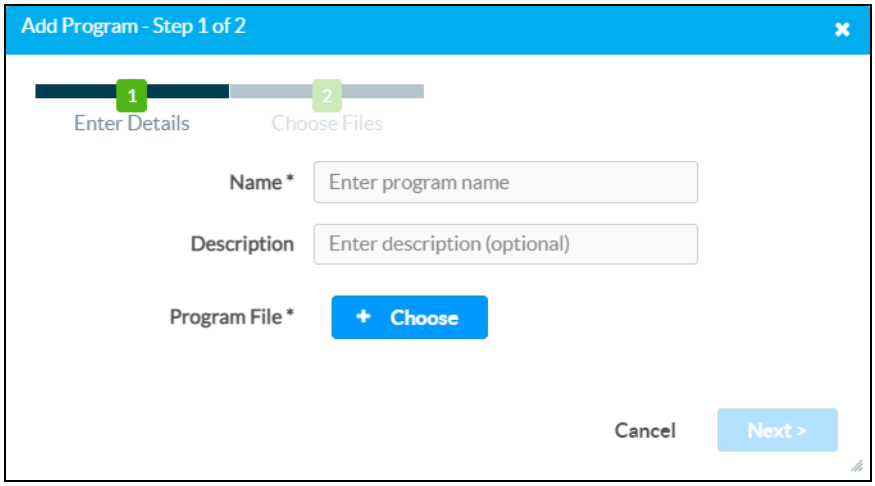
Add Program

Select **Add Program** to add a SIMPL, SIMPL#Pro, or C# program to the Crestron Virtual Control server. A program can be added to rooms after it has been added to the server.

> **NOTE:** Programs can also be added using the **Add Program** button within the **Program Library** accordion.

The **Add Program (Step 1 of 2)** dialog box is displayed.

Add Program (Step 1 of 2) Dialog Box



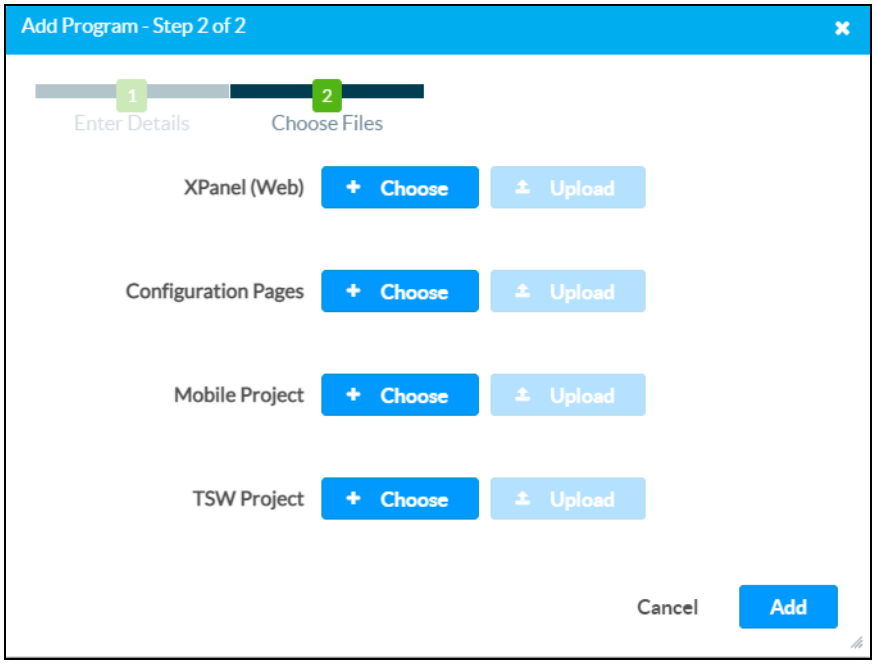
To add a program through the web configuration interface:

1. Enter the following information for the program. Any setting with an asterisk (*) is mandatory.
   - Enter the program name in the **Name** text field.
   - Enter a description for the program in the **Description** text field.
2. Select **Choose**, and then navigate to the program file (.cpz, .lpz, or .zip) on the host computer.
3. Select the program file, and then select **Open**.

   > **NOTE:** If an invalid program file is selected, a message is displayed indicating this, and the **Next** button is grayed out until a valid program file type is selected.

4. Select **Next**. The **Add Program (Step 2 of 2)** dialog box is displayed.

   Add Program (Step 2 of 2) Dialog Box



> **NOTE:** If the program was compiled with an older **include4.dat** file, a growl notification is displayed stating that the program must be recompiled with a newer **include4.dat** file and provides the minimum version that is supported. The program cannot be added until it is recompiled. For more information, refer to the SIMPL help file.

5. Select **Choose** next to the following selections to browse for and add additional files to the program as needed:
   - **XPanel (Web)**: Adds files (.zip) used to generate a web-based XPanel interface for the program.
   - **Configuration Pages**: Adds files (.zip or .tar) used to generate web configuration or scripting pages for the program.
   - **Mobile Project**: Adds files (.zip) used to generate a mobile project for the program.
   - **TSW Project**: Adds files (.vtz or .ch5z) used to generate a touch screen project for the program.
6. Select **Upload** next to any added file to upload that file to the program entry.
7. Select **Add**. Upon successful upload, the new program is displayed in the program library and can be selected and added to a room.

Add Room

Select **Add Room** to add a new room to the Crestron Virtual Control server. A room can be associated with a program that has been added to the server.

The total number of rooms that can be added is dependent on how many room licenses (VC-4-ROOM) have been purchased for the Crestron Virtual Control installation. A status message is shown periodically at the top of the web configuration interface when the number of created rooms are greater or less than the number of purchased licenses.

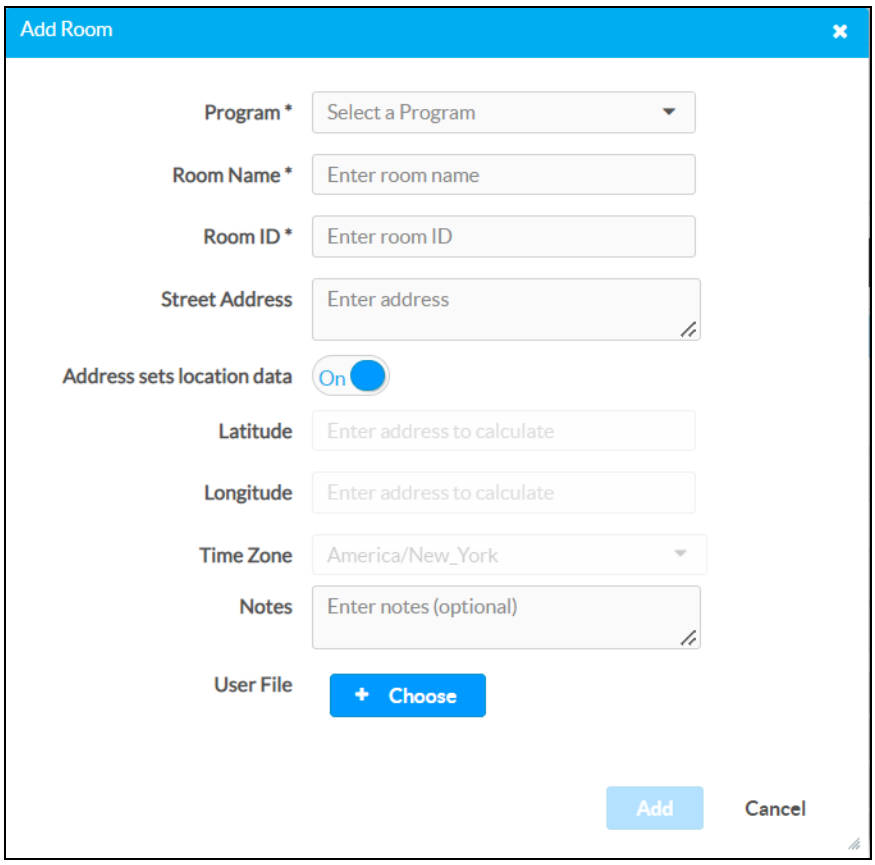
License Status Message



> **NOTE:** Rooms can also be added using the **Add Room** button within the **Rooms** accordion.

The **Add Room** dialog box is displayed.

Add Room Dialog Box



To add a room through the web configuration interface:

1. Enter the following information for the room. Any setting with an asterisk (*) is mandatory.
   - Use the **Program** drop-down to select a program to run in the room.

     > **NOTE:** The program must be added to the Crestron Virtual Control server prior to adding it to a room. For more information, refer to Add Program on page 103.

   - Enter a room name in the **Room Name** text field.
   - Enter a unique room ID in the **Room ID** text field.

     > **NOTE:** The room ID allows Crestron devices to connect to a room automatically over the Connect Request method. The room ID cannot be changed once a room is created and persists across program and server restarts.

   - Enter an address associated with the room in the **Street Address** text field. The address can be entered in the following formats:
     - Full street address (15 Volvo Drive, Rockleigh, NJ)
     - City/town, state/province (Rockleigh, NJ)
     - City, country (Rockleigh, USA)
   - Turn on the **Address sets location data** toggle to allow the address provided for **Street Address** to calculate the time zone, longitude, and latitude for the room automatically using the Microsoft® Azure® service's Geolocation API.

     > **NOTES:**
     >
     > - If a street address is not provided or the Azure Geolocation API does not recognize the provided address, the time zone will default to "America/New_ York".
     > - The time zone is used to ensure programs are started and stopped at the correct time based on the location of the associated room. Therefore, it is important to check within the room's **Details** accordion that the street address provided for a room is resolved to the correct time zone. If the displayed time zone is incorrect, it must be set manually.
     > - For more information on troubleshooting room addresses, refer to Troubleshoot Room Addresses on page 152.

   - If **Address sets location data** is turned off, enter the latitude associated with the room in the **Latitude** text field for scheduling astronomical events.
   - If **Address sets location data** is turned off, enter the longitude associated with the room in the **Longitude** text field for scheduling astronomical events.
   - If **Address sets location data** is turned off, enter the time zone associated with the room in the **Time Zone** text field for scheduling tasks in local time. Crestron Virtual Control uses the IANA Time Zone Database standard.
   - Enter any notes for the room in the **Notes** text field.

- Select **Choose** next to **User File** to browse for an upload a custom user file to the room. The user file can be a .zip file that will be extracted when the room is started.

2. Select **Add** to add the new room. Upon successful creation, the room is displayed in the room list, and the room program is initialized and started immediately.

Stop Debugging

Select **Stop Debugging** to turn off debugging for all SIMPL programs that are currently running on the Crestron Virtual Control server. For more information on turning on debugging for individual rooms, refer to Enable Debugging on page 109.

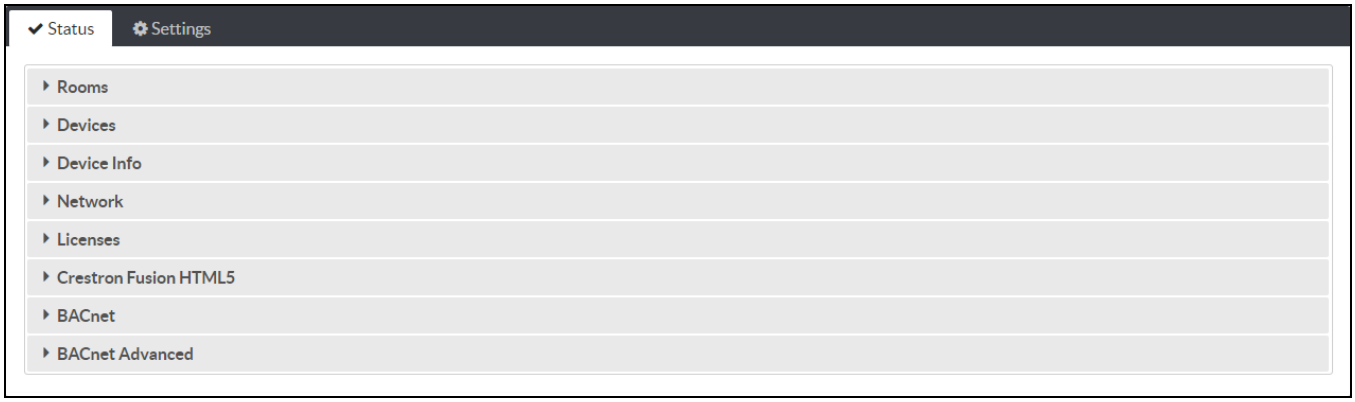
> **NOTE:** Debugging through Crestron Virtual Control is available only for SIMPL programs.

Status

Select the **Status** tab on the top left of the configuration interface to display collapsible accordions for viewing the status of room, device, network, license, and HTML5 Web XPanel support for Crestron Fusion® software settings.

Select an accordion name to expand it. If the accordion is expanded, select the accordion name again to collapse it.

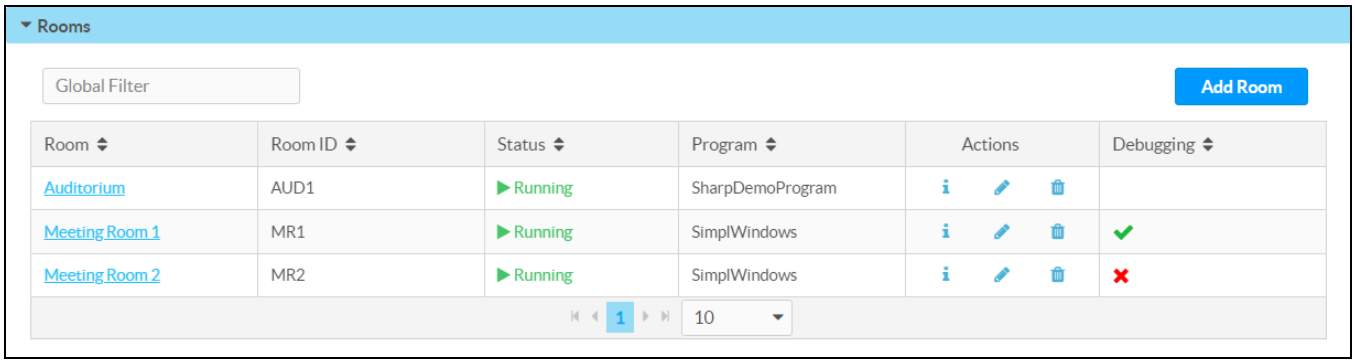
Status Tab Selections



Rooms

Select **Rooms** to view and configure room settings.

Status Tab - Rooms



Select **Add Room** to add a new room to the Crestron Virtual Control server. For more information on adding a room, refer to Add Room on page 105.

> **NOTE:** Rooms can also be added using the **Add Room** selection in the **Actions** menu.

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

- **Room**: The room name. Select the room name to display pages for viewing and configuring settings for the room.
- **Room ID**: The unique room ID that is used by devices to connect to the room automatically.
- **Status**: The status of the program running in the room:
  - **Initializing**
  - **Starting**
  - **Running**
  - **Stopping**
  - **Stopped**
  - **Aborted**

    > **NOTE:** An **Aborted** state indicates that the program was aborted because it did not start or stop properly, the room cannot be run because of insufficient licenses, or another issue has occurred. Check the debugging logs for the room to help determine the root cause of the issue.
- **Program**: The name of the program running in the room.
- **Actions**: Provides the following controls for the rooms:
  - Select the information button to view the **Status** page for the room. For more information, refer to Status (Rooms) on page 110.
  - Select the pencil button to view the **Settings** page for the room. For more information, refer to Settings on page 126.
  - Select the trash can button to delete the room. A dialog box is displayed to confirm the deletion. Select **Yes** to delete the room.
- **Debugging**: Indicates the debugging status of the SIMPL program running in the room:
  - A green check icon is shown if debugging is turned on for the SIMPL program. For more information, refer to Enable Debugging on page 109.
  - A red x icon is shown if debugging is turned off for the SIMPL program. For more information, refer to Disable Debugging on page 110.

Type a full or partial search term into the **Global Filter** text field to search for and display rooms that match the search term.

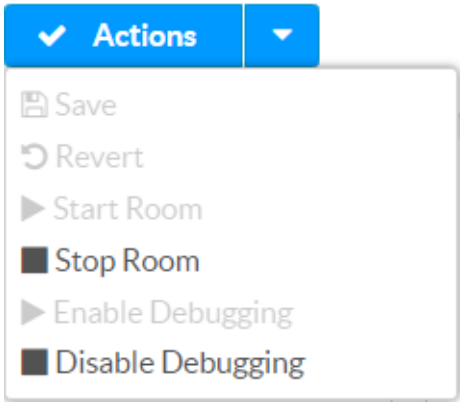
If the rooms list spans multiple pages, use the navigation arrows on the bottom of the page to move forward or backward through the pages, or select a page number to navigate to that page.

Action Menu (Rooms)

Room pages provide an **Actions** drop-down menu on the top right of the page. The **Actions** menu may be accessed at any time.

> **NOTE:** The **Actions** menu provides different selections depending on whether it is accessed from the general web interface or from a specific room page. For more information on the selections provided from the general menu, refer to Actions Menu on page 102.

Actions Menu (Rooms)



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

Save

Select **Save** to save any changes made to the room settings.

Revert

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

Start Room

Select **Start Room** to start the program associated with the room. This option is grayed out if the program is running.

Stop Room

Select **Stop Room** to stop the program associated with the room. This option is grayed out if the program not running.

Enable Debugging

> **NOTE:** This selection is shown only if a SIMPL program has been loaded to the room.

Select **Start Debugging** to turn on debugging for the SIMPL program in the room. This option is grayed out if debugging has been turned on.

When debugging is turned on, a green check icon ✔ is shown in the **Debugging** column for the room in the **Rooms** table.

For more information on debugging a SIMPL program using the **SIMPL Debugger** tool in Crestron Toolbox™ software, refer to the Crestron Toolbox help file.

Disable Debugging

> **NOTE:** This selection is shown only if a SIMPL program has been loaded to the room.

Select **Stop Debugging** to turn off debugging for the SIMPL program in the room. This option is grayed out if debugging has been turned off.

When debugging is turned off, a red x icon ✖ is shown in the **Debugging** column for the room in the **Rooms** table. To turn off debugging for all SIMPL programs, refer to Stop Debugging on page 107.

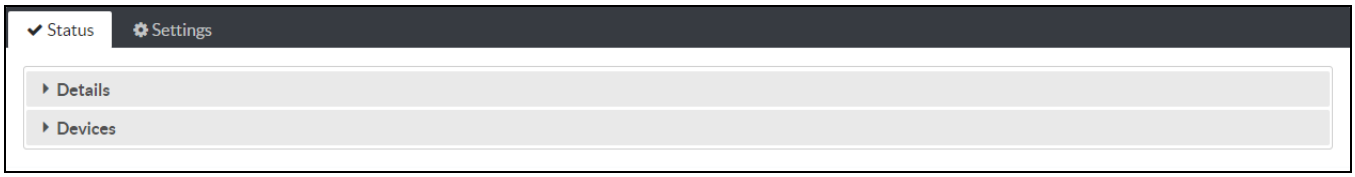
Status (Rooms)

In the **Rooms** accordion, select a room name or the information button ℹ in a room's table row to display the **Status** page for the room. The **Status** page provides collapsible accordions for viewing the status of the room and its connected devices.

> **NOTE:** When a room is selected, the **Actions** menu changes to show selections specifically for that room. For more information, refer to Actions Menu on page 102.

Select an accordion name to expand it. If the accordion is expanded, select the accordion name again to collapse it.

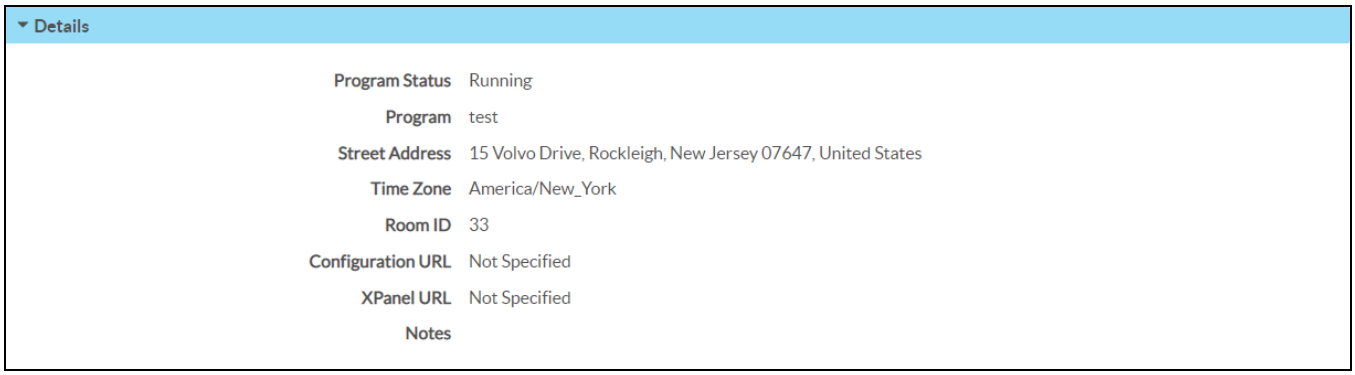
Status Tab Selections (Room-Based)



Details (Room Status)

Select **Details** to view room settings.

Status Tab (Room-Based) - Details



The following information is displayed:

- **Program Status**: Indicates the status of the program running in the room.
- **Program**: The program name.
- **Street Address**: The street address associated with the room.

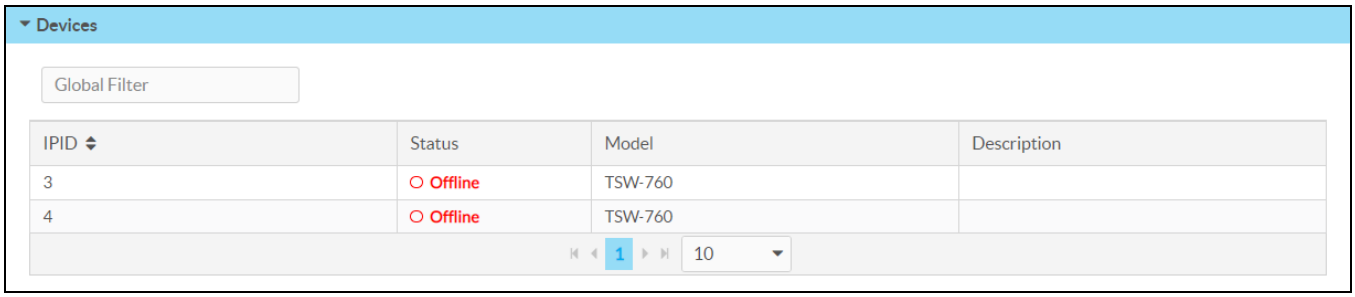
- **Time Zone**: The time zone associated with the room.
- **Room ID**: The room ID associated with the room that is used for device connections.
- **Configuration URL**: If specified, provides a link to web configuration pages for the program.
- **XPanel URL**: If specified, provides a link to a web-based XPanel interface for the program.
- **Notes**: If specified, provides notes about the program.

Devices (Room Status)

Select **Devices** to view the devices that are connected to the room.

> **NOTE:** Devices are added to a room automatically via the Connect Request method or manually via the main **Devices** tab. For more information, refer to Associate a Device with a Room on page 118.

Status Tab (Room-Based) - Devices



Each connected device is represented in a table that provides the following information and controls:

- **IPID**: The IP ID that is used to connect the device to the Crestron Virtual Control server.
- **Status**: Reports the device status on the network (**Online**, **Offline**, or **Unknown**).
- **Model**: The device model.
- **Description**: A description for the device (if provided).

Type a full or partial search term into the **Global Filter** text field to search for and display devices that match the search term.

If the devices list spans 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.

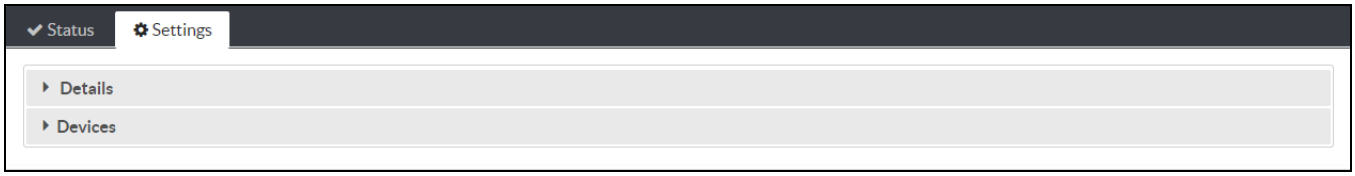
Settings (Rooms)

In the **Rooms** accordion, select a room name or the pencil button in a room's table row to display the **Settings** page for the room. The **Settings** page provides collapsible accordions for configuring the status of the room and its connected devices.

> **NOTE:** When a room is selected, the **Actions** menu changes to show selections specifically for that room. For more information, refer to Actions Menu on page 102.

Select an accordion name to expand it. If the accordion is expanded, select the accordion name again to collapse it.

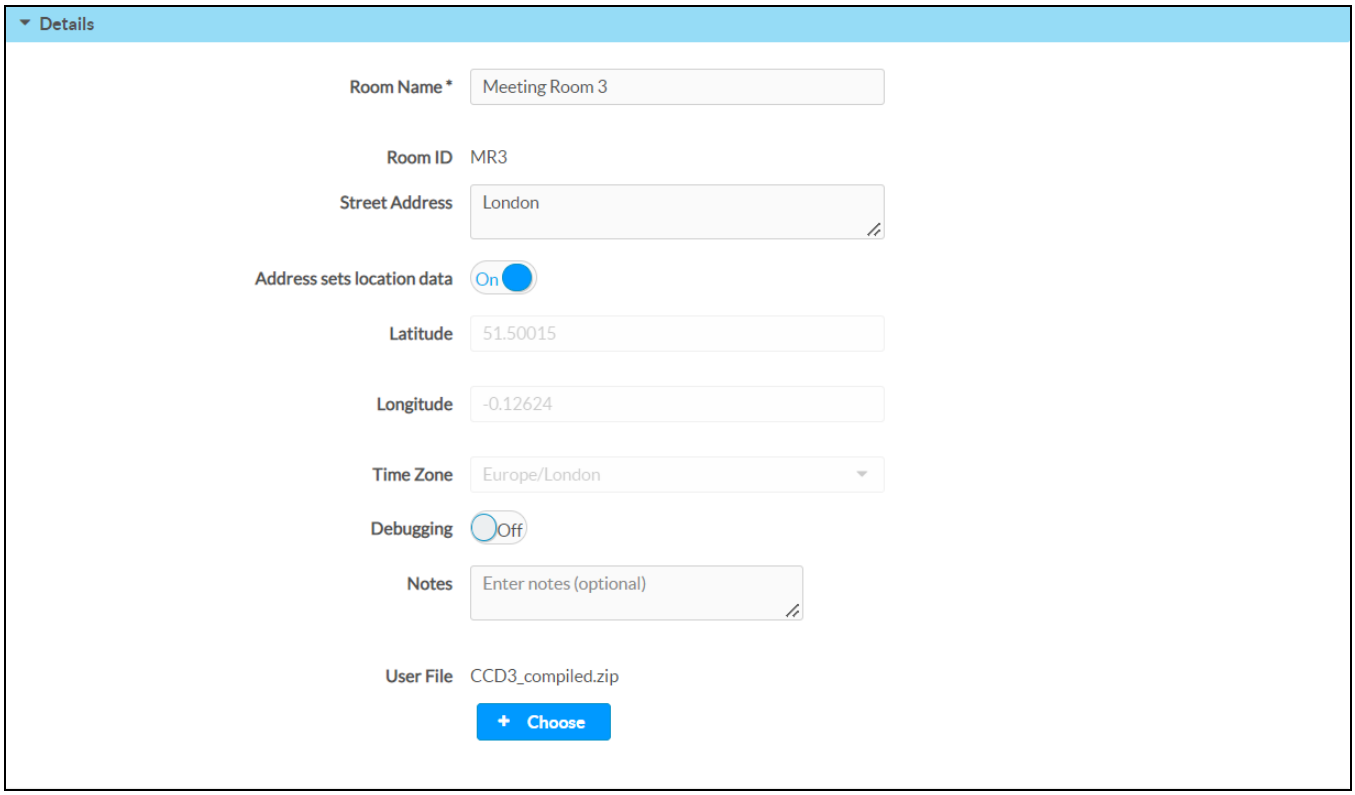
Settings Tab Selections (Room-Based)



Details (Room Settings)

Select **Details** to configure room settings.

Settings Tab (Room-Based) - Details



The following room settings can be configured:

- **Room Name**: Enter a room name.
- **Room ID**: Indicates the room ID associated with the roomy. The room ID cannot be changed after a room has been created.
- **Street Address**: Enter an address associated with the room. The address can be entered in the following formats:
    - Full street address (15 Volvo Drive, Rockleigh, NJ)
    - City/town, state/province (Rockleigh, NJ)
    - City, country (Rockleigh, USA)

- **Address sets location data**: Turn on the toggle to allow the address provided for **Street Address** to calculate the time zone, longitude, and latitude for the room automatically using the Microsoft® Azure® service's Geolocation API.

  > **NOTES:**
  >
  > - If a street address is not provided or the Azure Geolocation API does not recognize the provided address, the time zone will default to "America/New_York".
  > - The time zone is used to ensure programs are started and stopped at the correct time based on the location of the associated room. Therefore, it is important to check within the room's **Details** accordion that the street address provided for a room is resolved to the correct time zone. If the displayed time zone is incorrect, it must be set manually.
  > - For more information on troubleshooting room addresses, refer to Troubleshoot Room Addresses on page 152.

- **Latitude**: If **Address sets location data** is turned off, enter the latitude associated with the room for scheduling astronomical events.
- **Longitude**: If **Address sets location data** is turned off, enter the longitude associated with the room for scheduling astronomical events.
- **Time Zone**: If **Address sets location data** is turned off, enter the time zone associated with the room for scheduling tasks in local time. Crestron Virtual Control uses the IANA Time Zone Database standard.
- **Debugging**: Turn on the toggle to turn on debugging for the SIMPL program in the room. For more information on debugging a SIMPL program using the **SIMPL Debugger** tool in Crestron Toolbox™ software, refer to the Crestron Toolbox help file.

  > **NOTE:** This toggle is shown only if a SIMPL program has been loaded to the room.

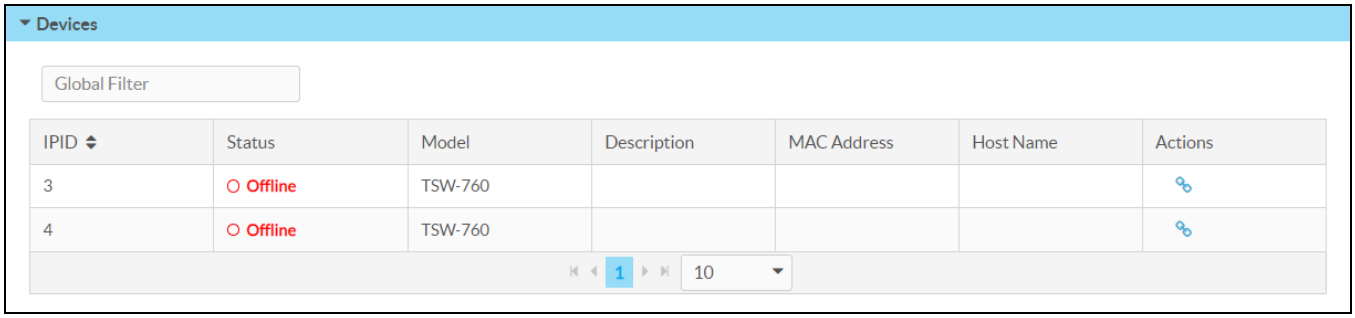
- **Notes**: Enter any notes for the room.
- **User File**: Select **Choose** next to **User File** to browse for an upload a custom user file to the room. The user file can be a .zip file that will be extracted when the room is started.

Devices (Room Settings)

Select **Devices** to configure the devices that are connected to the room.

> **NOTE:** Devices are added to a room automatically via the Connect Request method or manually via the main **Devices** tab. For more information, refer to Associate a Device with a Room on page 118.

Settings Tab (Room-Based) - Devices



Each connected device is represented in a table that provides the following information and controls:

> **NOTE:** Devices that use the Connect Request method (connect to the Crestron Virtual Control server via a room ID) will populate their table rows with data automatically.

- **IPID**: The IP ID that is used to connect the device to the Crestron Virtual Control server.
- **Status**: Reports the device status on the network (**Online**, **Offline**, or **Unknown**).
- **Model**: The device model.
- **Description**: A description for the device (if provided).
- **MAC Address**: The unique MAC (media access control) address for the device's network adapter.
- **Host Name**: The device host name.
- **Actions**: Provides the following controls for associating connected devices:

  > **NOTE:** These controls are provided only for devices running older firmware that do not use the Connect Request method. Devices that use the Connect Request method are associated with rooms automatically via the room ID.

  - Select the link button to associate the device to the room. This button is shown only if the device has not yet been associated with the room.
  - Select the unlink button to disassociate the device from the room. This button is shown only if the device is already associated with the room.

Type a full or partial search term into the **Global Filter** text field to search for and display devices that match the search term.

If the devices list spans 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.

Associate a Device Manually

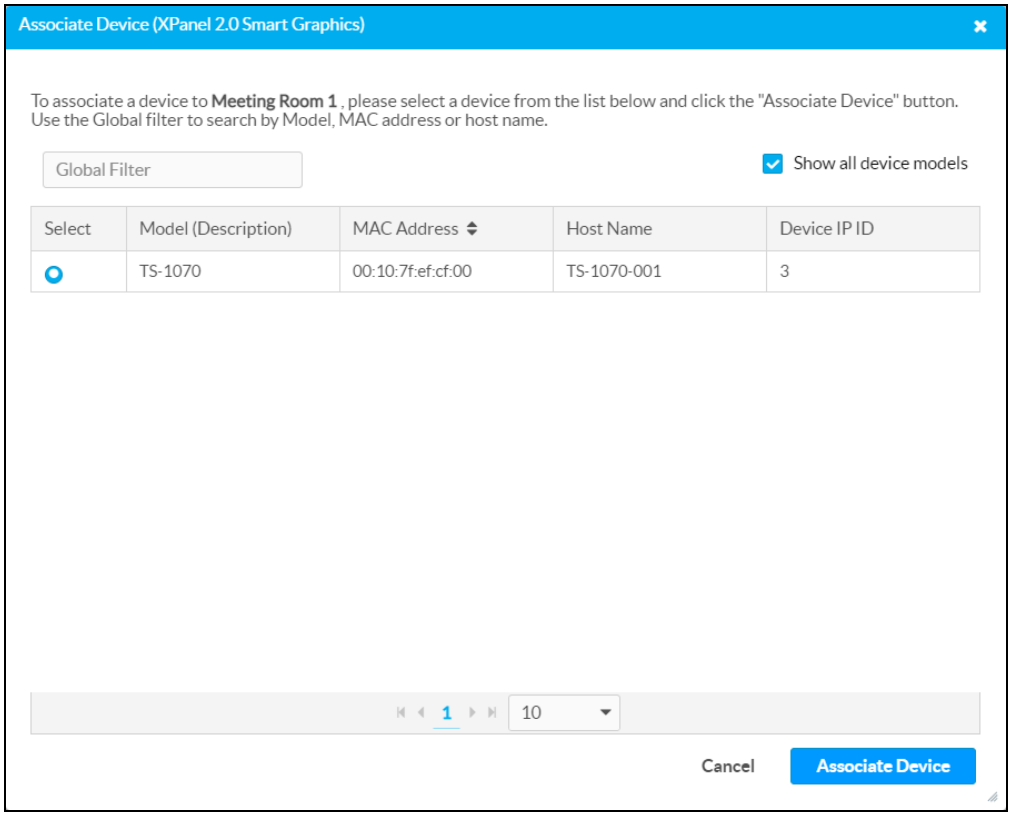
Devices can be associated with a room manually if they do not use the Connect Request method. To associate a device with a room manually:

NOTES:

- A device should be associated with only one room, with the exception of sharable devices or touch screens.
- Touch screens that are associated manually are not able to load touch screen projects from Crestron Virtual Control. The touch screen firmware must be upgraded to a recent version that uses the Connect Request method to avoid this issue.
- Devices that are on different subnets than the Crestron Virtual Control server will not be displayed in the **Devices** table. For more information on associating devices across subnets, refer to Connect Devices across Subnets on page 153.

1. Select the link button in a device's table row. The **Associate Device** dialog box is displayed.

Associate Device Dialog Box

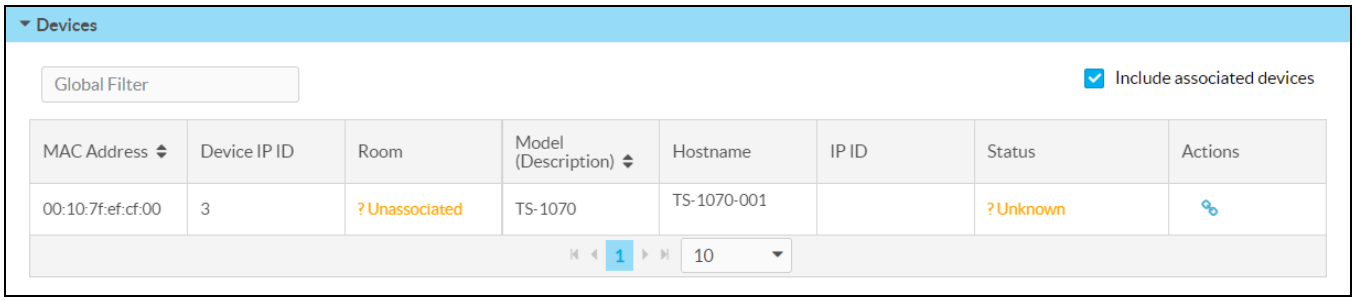


2. Browse for a device using the following controls:
    - Fill the **Show all device models** check box to display all available device models within the Crestron Virtual Control server.
    - Type a full or partial search term into the **Global Filter** text field to search for and display devices that match the search term.
    - Use the up and down arrows in the **MAC Address** column header to sort selections by MAC address.
    - If the devices list spans 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.
3. Fill the check box next to a device in the **Select** column to select the device.
4. Select **Associate Device**. All applicable **Devices** table fields will be populated for the device, and the link button is replaced by an unlink button in the **Actions** column.

Devices

Select **Devices** to view and configure settings for devices that have been added to the Crestron Virtual Control server.

Status Tab - Devices



Each connected device is represented in a table that provides the following information and controls:

> **NOTE:** Devices that use the Connect Request method (connect to the Crestron Virtual Control server via a room ID) will populate their table rows with data automatically.

- **MAC Address**: The unique MAC address for the device's network adapter.
- **Device IP ID**: The IP ID assigned to the device.
- **Room**: The room to which the device is associated. If the device is not associated with a room, an **Unassociated** status is displayed.
- **Model (Description)**: The device model.
- **Hostname**: The device host name.
- **IP ID**: The IP ID of the Crestron Virtual Control room to which the device is associated.
- **Status**: Reports the device status on the network (**Online**, **Offline**, or **Unknown**).

- **Actions**: Provides the following controls for associating connected devices:

  > **NOTE:** These controls are provided only for devices running older firmware that do not use the Connect Request method. Devices that use the Connect Request method are associated with rooms automatically via the room ID.

  - Select the link button to associate the device with a room. This button is shown only if the device has not yet been associated with a room.
  - Select the unlink button to disassociate the device from a room. This button is shown only if the device is already associated with a room.

Type a full or partial search term into the **Global Filter** text field to search for and display devices that match the search term.

Fill the **Include associated devices** check box to show devices that have already been associated with rooms.

If the devices list spans 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.

Connect a Device to Crestron Virtual Control

Devices can be connected to the Crestron Virtual Control server as follows. Devices are shown in the **Devices** table after they have connected successfully to the Crestron Virtual Control server.

- **Ethernet Devices**: Set the IP table of the Ethernet device to point to the IP address or host name of the Crestron Virtual Control server. This can be accomplished via the device's web configuration interface or local setup screens (if applicable) or through the **Network Device Tree** tool in Crestron Toolbox™ software.
- **Cresnet® Network Devices**: Using an Ethernet to Cresnet bridge (such as the DIN-CENCN-2), set the IP table of the bridge to point to the IP address or host name of the Crestron Virtual Control server. Cresnet IDs must also be established for each Cresnet device on the bridge. This can be accomplished via the device's web configuration interface (if applicable) or through the **Network Device Tree** tool in Crestron Toolbox software.
- **RF Devices**: Using a wireless gateway (such as the CEN-GWEXER), set the IP table of the gateway to point to the IP address or host name of the Crestron Virtual Control server. RF IDs must also be established for each RF device on the gateway. This can be accomplished via the device's web configuration interface (if applicable) or through the **Network Device Tree** tool in Crestron Toolbox software.

Associate a Device with a Room

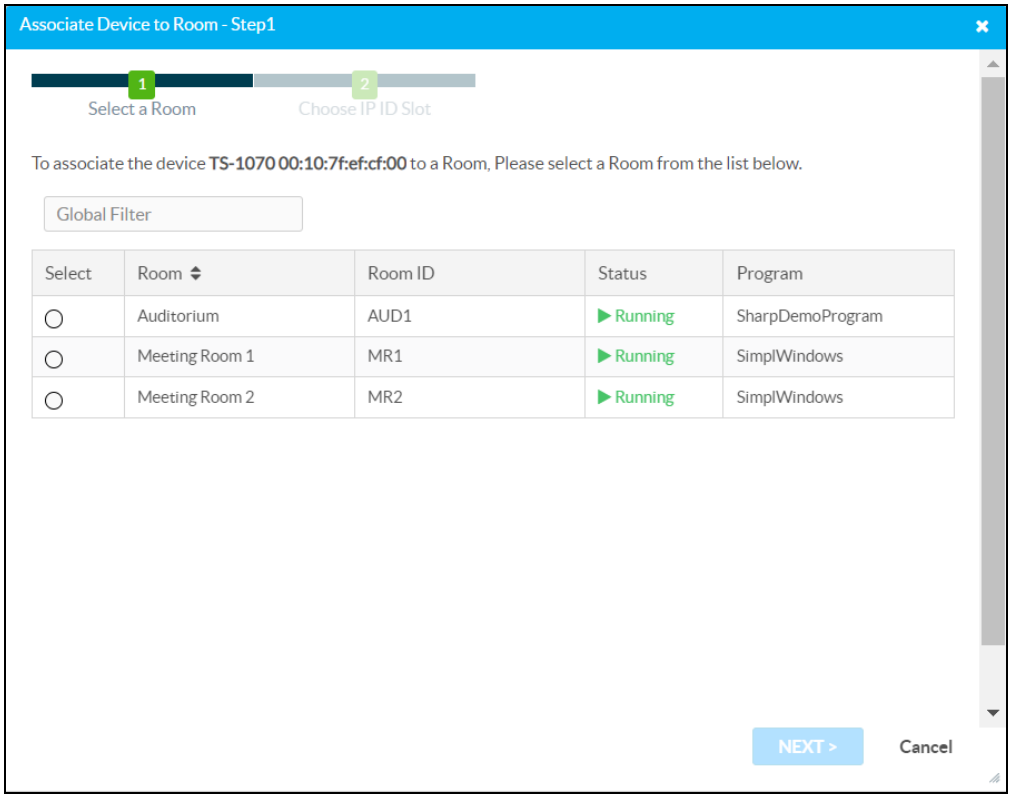
Devices can be associated with a room manually if they do not use the Connect Request method. To associate a device with a room manually:

NOTES:

- A device should be associated with only one room, with the exception of sharable devices or touch screens.
- Touch screens that are associated manually are not able to load touch screen projects from Crestron Virtual Control. The touch screen firmware must be upgraded to a recent version that uses the Connect Request method to avoid this issue.
- Devices that are on different subnets than the Crestron Virtual Control server will not be displayed in the **Devices** table. For more information on associating devices across subnets, refer to Connect Devices across Subnets on page 153.

1. Select the link button in a device's table row. The **Associate Device to Room (Step1)** dialog box is displayed.

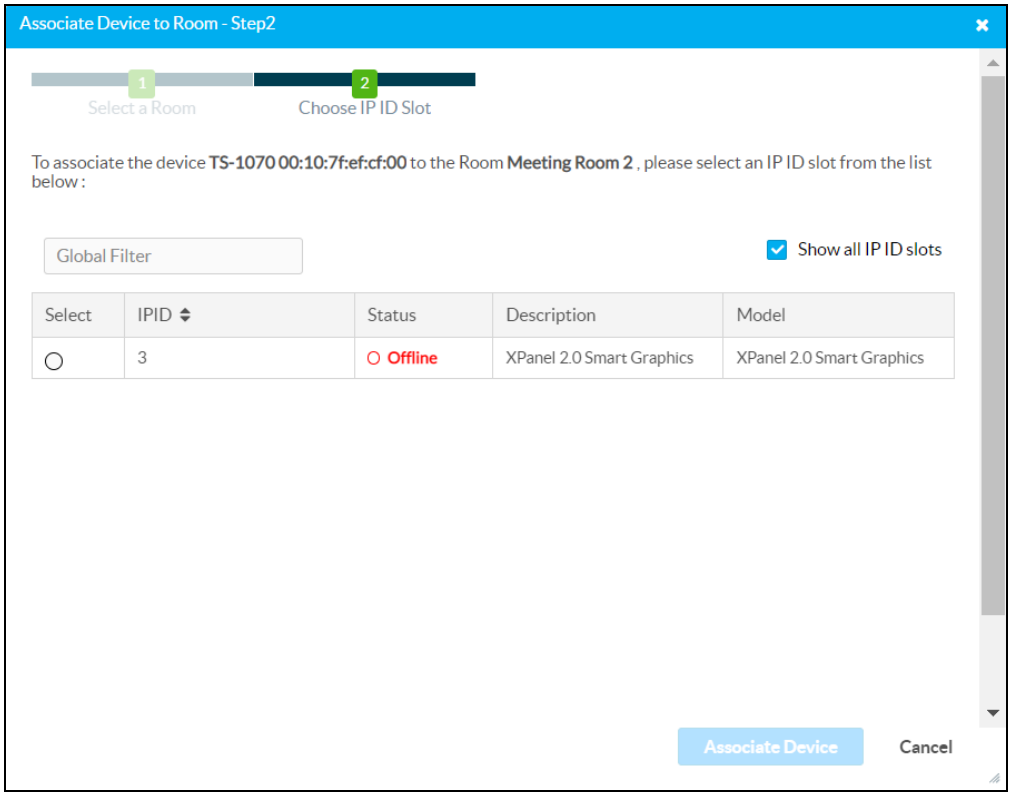
   Associate Device to Room Dialog Box (Step1)



2. Browse for a room using the following controls:
   - Type a full or partial search term into the **Global Filter** text field to search for and display rooms that match the search term.
   - Use the up and down arrows in the **Room** column header to sort selections by room name.
   - If the rooms list spans 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.
3. Fill the check box next to a room in the **Select** column to select the room.

4. Select **NEXT >**. The **Associate Device to Room (Step2)** dialog box is displayed.

Associate Device to Room Dialog Box (Step2)

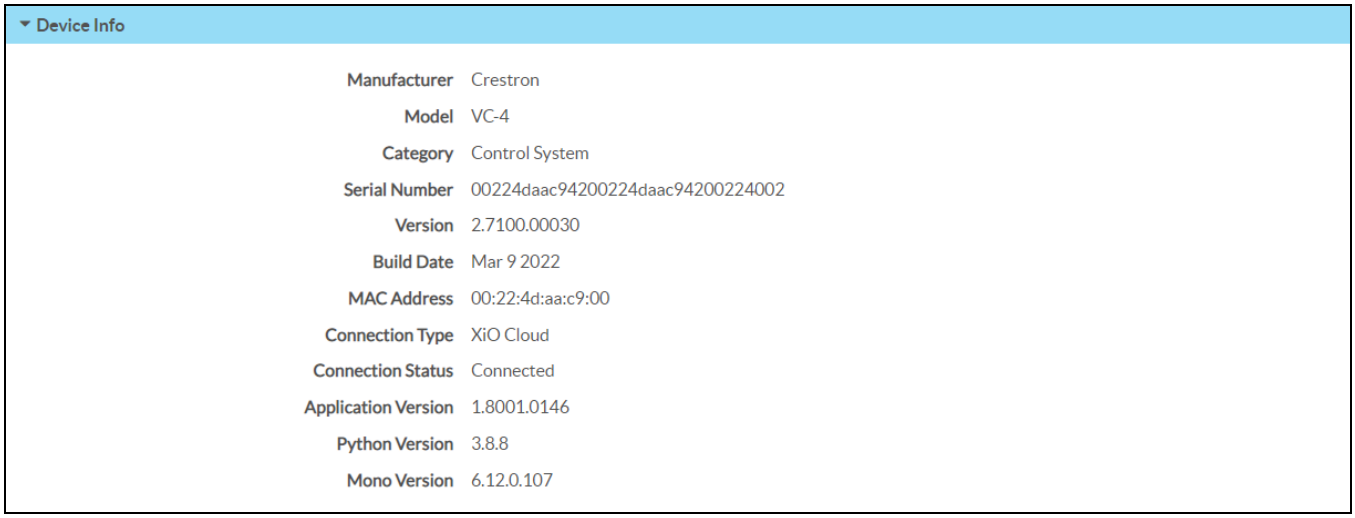


5. Browse for an IP ID slot using the following controls:
   - Type a full or partial search term into the **Global Filter** text field to search for and display IP ID slots that match the search term.
   - Use the up and down arrows in the **IPID** column header to sort selections by IP ID.
   - If the IP ID list spans 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.
6. Fill the check box next to an IP ID slot in the **Select** column to select the IP ID.
7. Select **Associate Device**. The device will be added to the respective room page, all applicable **Devices** table fields will be populated for the device, and the link button is replaced by an unlink button in the **Actions** column.

Device Info

Select **Device Info** to view general device information for the Crestron Virtual Control server.

Status Tab - Device Info



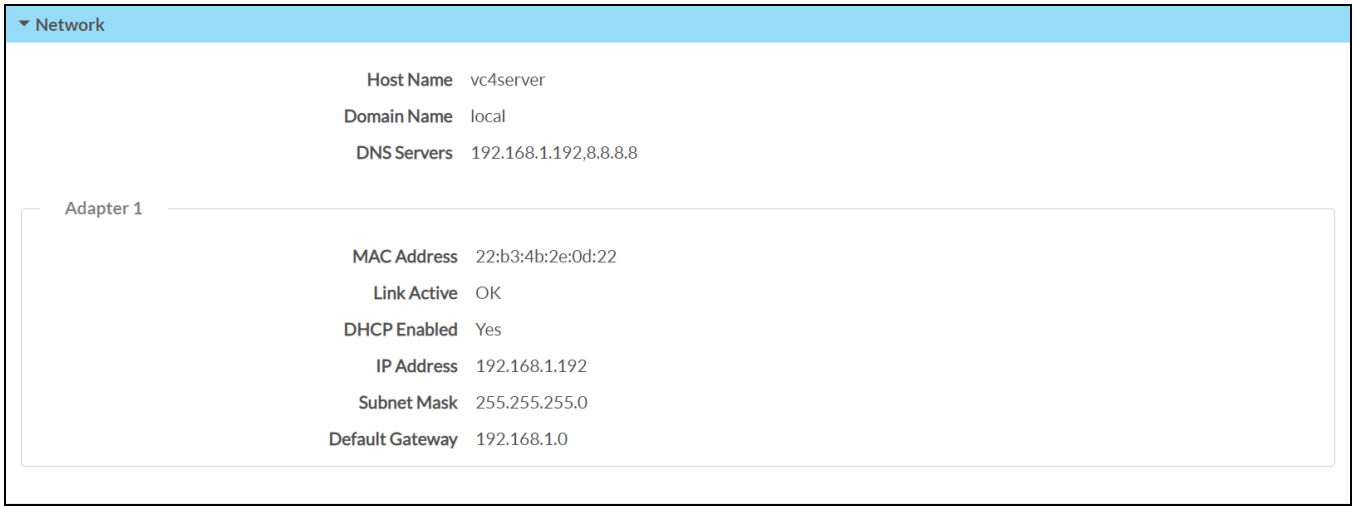
The following **Device Info** information is displayed:

- **Manufacturer**: The device manufacturer (Crestron).
- **Model**: The device model name (VC-4).
- **Category**: The device category (control system).
- **Serial Number**: The serial number for the Crestron Virtual Control server. The serial number is required when claiming the Crestron Virtual Control server to an XiO Cloud account.
- **Version**: The current Crestron Virtual Control software version.
- **Build Date**: The build date of the current software.
- **MAC Address**: The MAC address of the Crestron Virtual Control server. The MAC address is required when claiming the Crestron Virtual Control server to an XiO Cloud account.
- **Connection Type**: Indicates the current licensing connection type (XiO Cloud or offline license dongle).
- **Connection Status**: Indicates the status of the licensing connection.
- **Application Version**: The current Crestron application version used by the Crestron Virtual Control server.
- **Python Version**: The current Python® programming language version used by the Crestron Virtual Control server.
- **Mono Version**: The current Mono® software framework used by the Crestron Virtual Control server.

Network

Select **Network** to view network information for the Crestron Virtual Control server.

Status Tab - Network



The following **Network** information is displayed:

- **Host Name**: The device host name
- **Domain Name**: The device domain name
- **DNS Servers**: The DNS (domain name server) addresses used to resolve the control system domain to an IP address

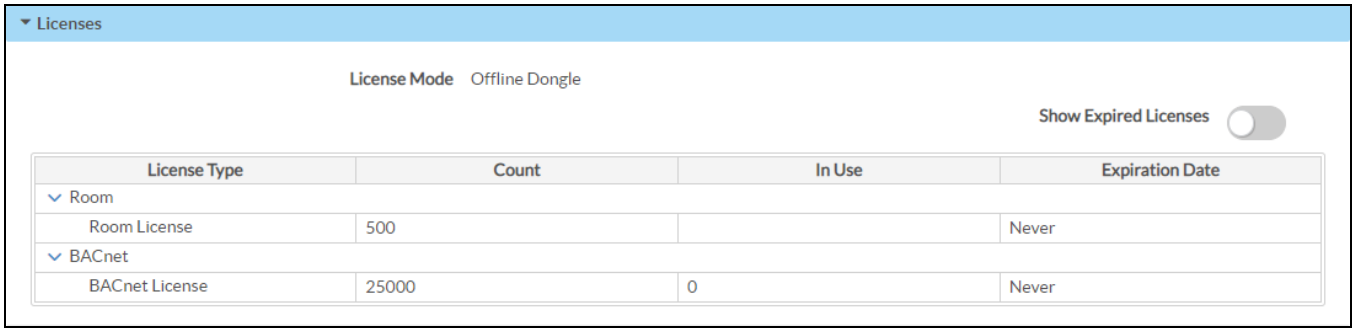
The following information is also provided for the IPv4 Ethernet adapter (**Adapter 1**):

- **MAC Address**: The unique MAC (media access control) address for the Ethernet adapter
- **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.)
- **DHCP Enabled**: Reports whether the IP address is dynamic (**Yes**) or static (**No**).
- **IP Address**: The Crestron Virtual Control server IP address, shown only if an Ethernet connection is active
- **Subnet Mask**: The Crestron Virtual Control server 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

Licenses

Select **Licenses** to view licensing information for the Crestron Virtual Control server.

Status Tab - Licenses



A **License Mode** status is provided that indicates the current licensing connection mode (XiO Cloud or offline license dongle).

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

> **NOTE:** For more information on adding a license to the Crestron Virtual Control installation, refer to Manage Licenses on page 92.

- **License Type**: The room license type. Select the arrow button next to the room license type to show more information about purchased licenses of that type.
- **Count**: The total number of available licenses of a type for the Crestron Virtual Control installation.
- **In Use**: The number of licenses that are currently in use by the Crestron Virtual Control installation.
- **Expiration Date**: The date that the licenses are set to expire (if applicable).

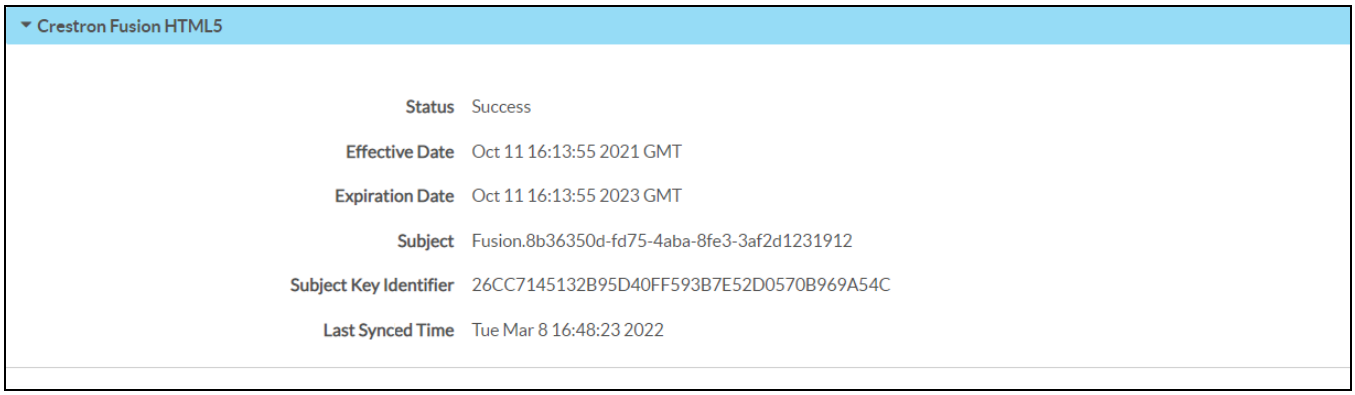
By default, the **Licenses** table shows only active licenses. To show expired licenses, turn on the **Show Expired Licenses** toggle.

Crestron Fusion HTML5

Select **Crestron Fusion HTML5** to view information for the Crestron Fusion® software server certificate that is connected to the Crestron Virtual Control server. The server certificate is used to authenticate an HTML5 Web XPanel project deployed to a static web server for access via the **e-Control** function in Crestron Fusion.

> **NOTE:** For more information on deploying an HTML5 Web XPanel project to a web server, refer to the Crestron HTML5 User Interface Developer Microsite.

Status Tab - Crestron Fusion HTML5



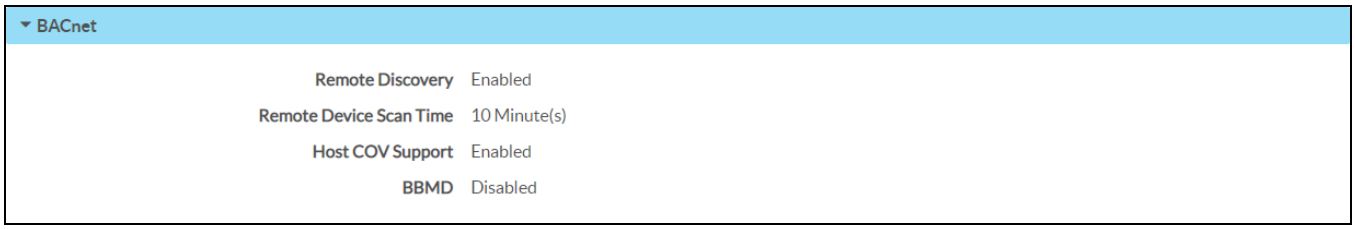
The following **Crestron Fusion HTML5** information is displayed:

- **Status**: The status of the Crestron Fusion server certificate connection.
- **Effective Date**: The effective date of the server certificate.
- **Expiration Date**: The expiration date of the server certificate.
- **Subject**: The subject of the server certificate.
- **Subject Key Identifier**: The unique subject key identifier of the server certificate.
- **Last Synced Time**: The time when the Crestron Fusion server certificate was last synced to the Crestron Virtual Control server.

BACnet

Select **BACnet** to view information for the BACnet network/IP settings within Crestron Virtual Control.

Status Tab - BACnet



The following **BACnet** information is displayed:

- **Remote Discovery**: The status of the auto discovery function for remote BACnet devices and objects.
- **Remote Device Scan Time**: The duration (in minutes) that Crestron Virtual Control will scan for remote BACnet devices and objects.
- **Host COV Support**: The status of the COV (Change of Value) support for host BACnet objects.
- **BBMD**: The status of the BBMD (BACnet Broadcast Management Devices) functionality.

BACnet Advanced

Select **BACnet Advanced** to view information for advanced BACnet network/IP settings within Crestron Virtual Control.

Status Tab - BACnet Advanced



The following **BACnet Advanced** information is displayed:

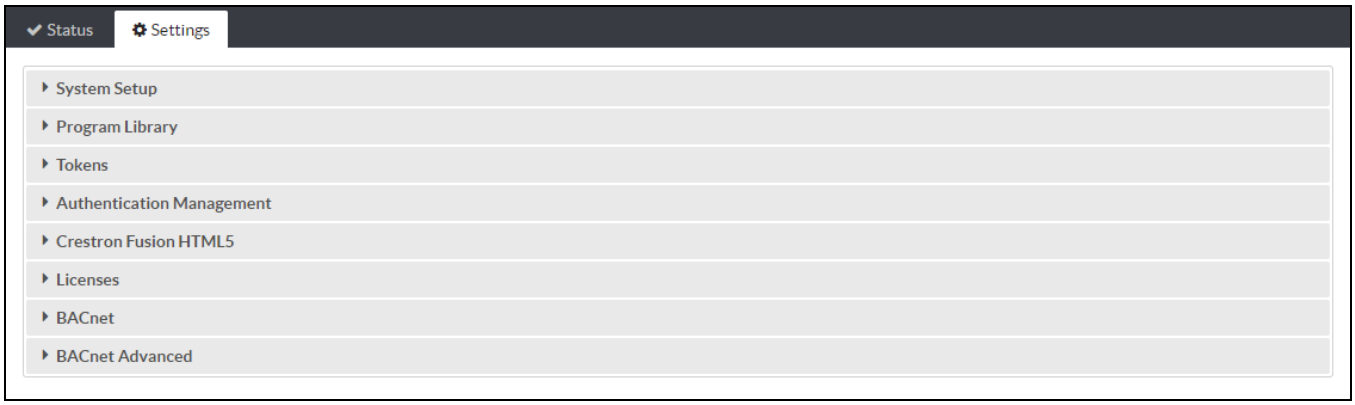
- **Number Of Retries**: The number times that Crestron Virtual Control will attempt to reconnect to a BACnet device if a connection error is discovered.
- **Read After Write**: The status of the read request after write functionality.
- **Remote Object Scan**: The status of the object discovery for remote devices functionality.

Settings

Select the **Settings** tab on the top left of the configuration interface to display collapsible accordions to configure settings for the system, programs, tokens, authentication, and HTML5 Web XPanel support for Crestron Fusion.

Select an accordion name to expand it. If the accordion is expanded, select the accordion name again to collapse it.

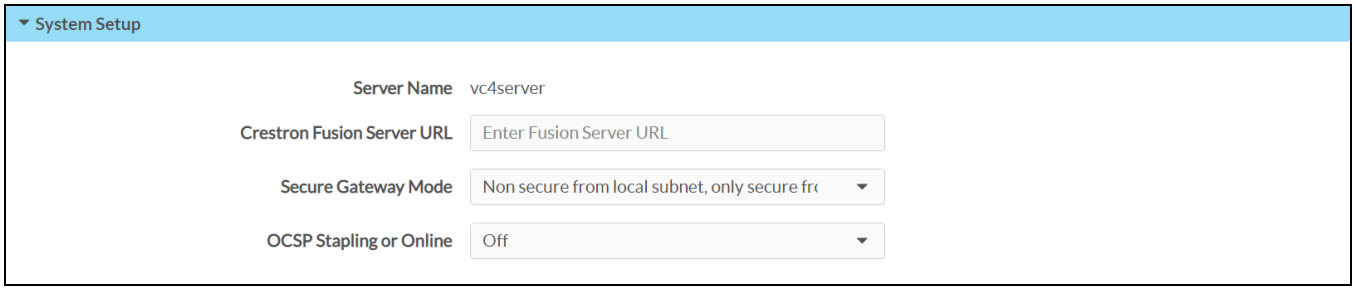
Settings Tab Selections



System Setup

Select **System Setup** to view and configure general system settings for the Crestron Virtual Control server.

Settings Tab - System Setup



- **Server Name**: Displays the name of the Crestron Virtual Control server.
- **Crestron Fusion Server URL**: Enter the IP address or host name of a Crestron Fusion server to establish a connection to that server.

- **Secure Gateway Mode**: Use the drop-down menu to select the secure gateway mode for the Crestron Virtual Control server:
  - **Only secure**: Only secure device connections are accepted by the server.
  - **Secure and non secure**: Both secure and nonsecure device connections are accepted by the server.
  - **Non secure from local subnet, only secure from remote subnets**: Nonsecure device connections from local subnets are accepted by the server, but only secure device connections from remote subnets are accepted by the server.

  NOTE: For more information on secure gateway mode configuration, refer to Configure Secure Device Connections on page 139.

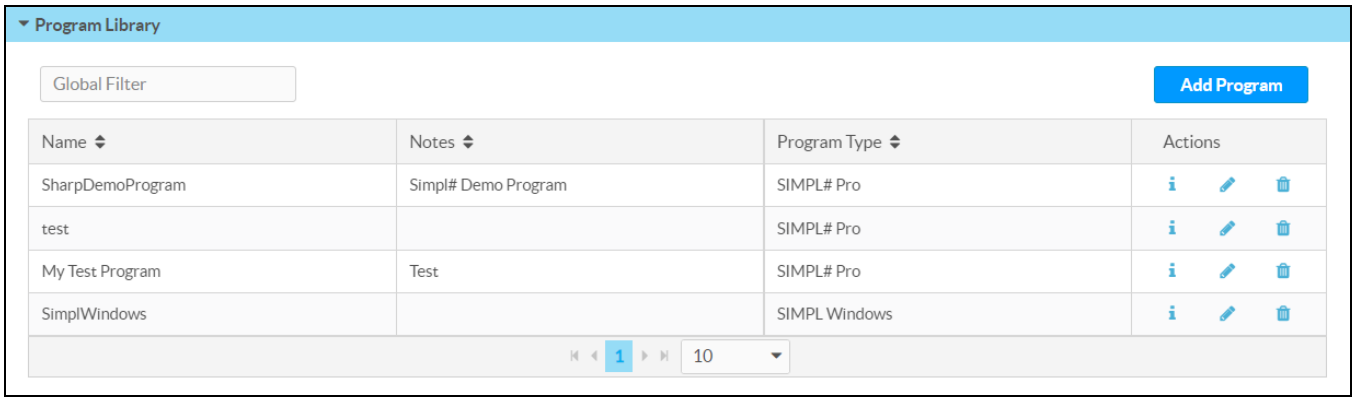
- **OSCP Stapling or Online**: Use the drop-down menu to select the OSCP (Online Certificate Status Protocol) mode for the Crestron Virtual Control server:
  - **Off**: Turns OSCP off.
  - **Staple Only**: Sets the OCSP client behavior to staple only (In this state, the Crestron Virtual Control server appends a time-stamped, self-signed OCSP response to a certificate sent by the web browser client for self-validation).
  - **Remote**: Sets the OCSP client behavior to remote (In this state, the web browser client sends remote certificates that are validated by the Crestron Virtual Control server).

  NOTE: For more information on OSCP configuration, refer to Configure OCSP Client Settings on page 143.

Program Library

Select **Program Library** to view and configure program settings.

Settings Tab - Program Library



Select **Add Program** to add a new program to the Crestron Virtual Control server. For more information on adding a room, refer to Add Program on page 103.

NOTE: Rooms can also be added using the **Add Program** selection in the **Actions** menu.

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

- **Name**: The program name.
- **Notes**: If specified, provides notes about the program.
- **Program Type**: The program type (SIMPL or SIMPL#Pro).
- **Actions**: Provides the following controls for the rooms:
  - Select the information button to open a message window that provides more information about the program. For more information, refer to View Program Information on page 128.
  - Select the pencil button to open a dialog box that provides controls for editing the program. For more information, refer to Edit a Program on page 129.
  - Select the trash can button to delete the program. A dialog box is displayed to confirm the deletion. Select **Yes** to delete the program.

    > **NOTE:** Deleting a program will also stop and delete all rooms running the program.

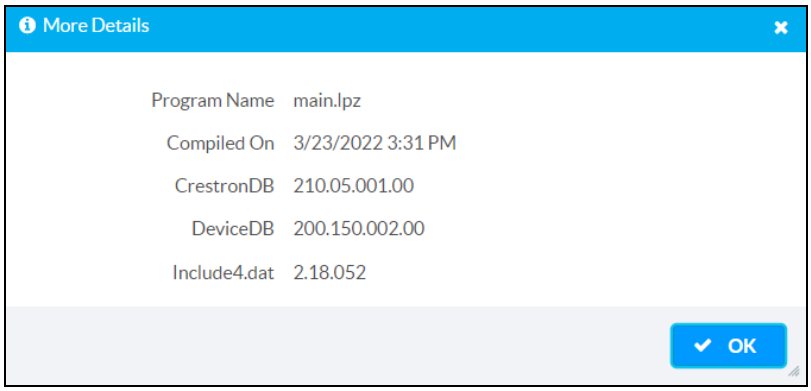
Type a full or partial search term into the **Global Filter** text field to search for and display programs that match the search term.

If the programs list spans 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.

View Program Information

To view more information about a program, select the information button in a program's table row. The **More Details** message window is displayed.

More Details Message Window



The following information is displayed for the program (if applicable):

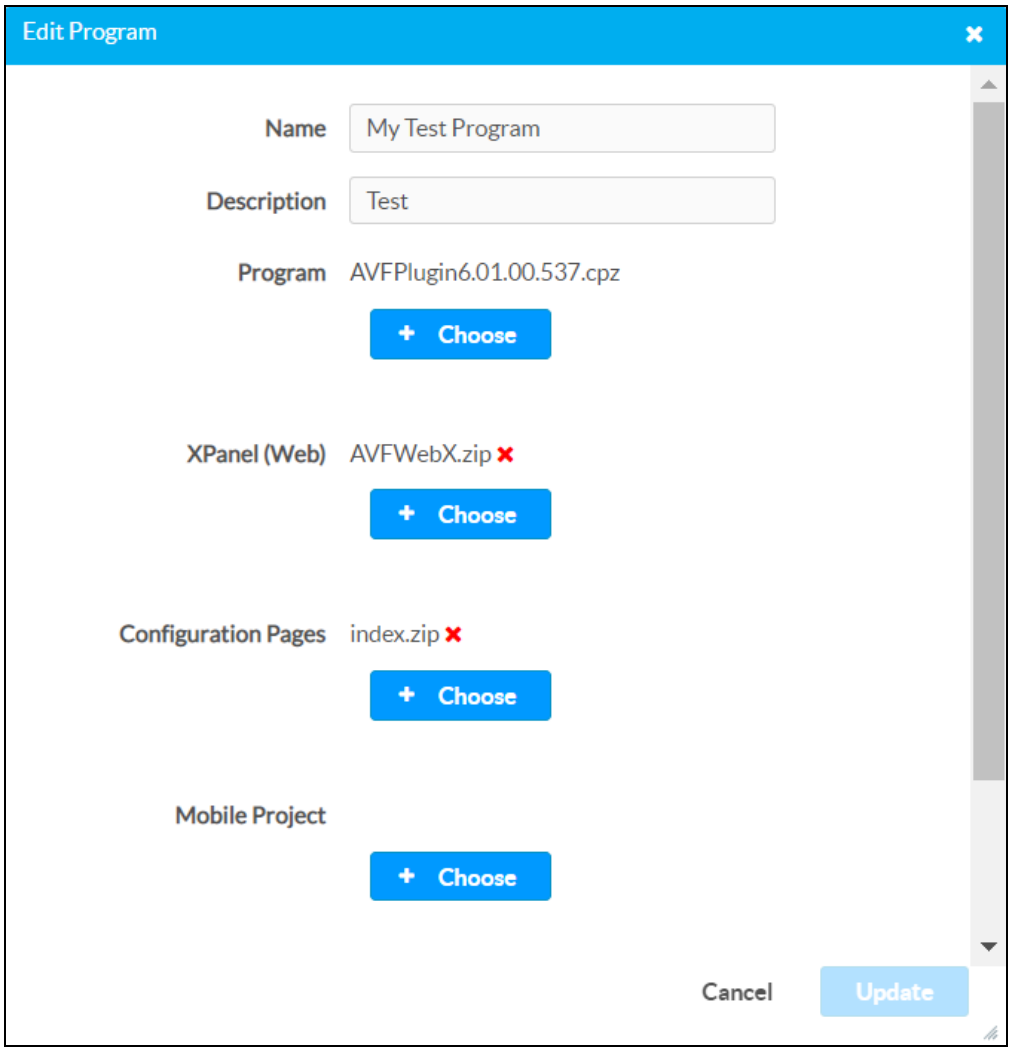
- **Program Name**: The name of the program file.
- **Compiled On**: The date that the program was compiled.
- **CrestronDB**: The Crestron Database version that is compiled with the program.
- **DeviceDB**: The Device Database version that is compiled with the program.
- **Include4.dat**: The Include4.dat file version that is compiled with the program.

Select **OK** to close the message window.

Edit a Program

To edit a program, select the pencil button in a program's table row. The **Edit Program** dialog box is displayed.

Edit Program Dialog Box



The following program settings can be edited:

- **Name**: Enter the program name.
- **Description**: Enter any notes for the program.
- Select **Choose** under a program file type to browse for and add additional files to the program as needed.

  > **NOTE:** If a program file has already been added, choosing a new program file will overwrite the existing file if changes are saved.

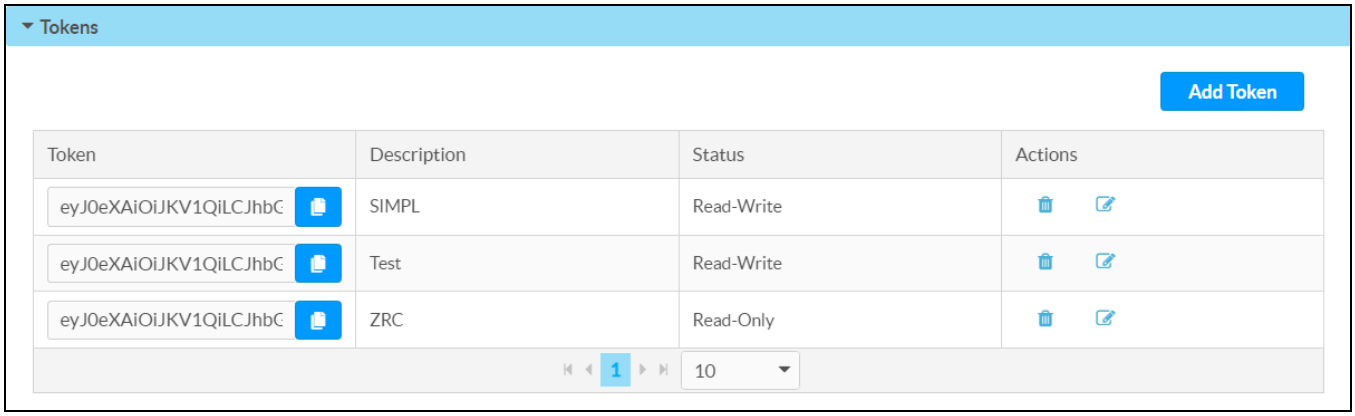
- If a program file has been added to the program, select the x button next to the program file to delete that file.

Select **Update** to save any changes and to add any program files that were selected. Select **Cancel** to cancel any changes.

Tokens

Select **Tokens** to view and add tokens for the Crestron Virtual Control server. Tokens are used for authentication when using features such as the REST API, .AV Framework™ software, and remote debugging.

Settings Tab -Tokens



Tokens are generated in JWT (JSON Web Token) format and consist of three parts: a header, a payload, and a signature. Each part is separated by a dot. The generated token is authenticated by the Crestron Virtual Control server against the list of authorized tokens before a client's request is handled.

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

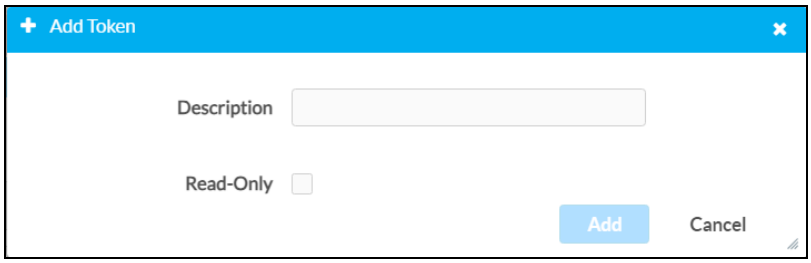
- **Token**: The token name. A copy button is provided that copies the token to the clipboard.
- **Description**: A user-defined description for the token.
- **Status**: Indicates whether the token has read/write or read-only permissions.
- **Actions**: Provides the following selections for performing action:
  - Select the trash can button to delete the token. A dialog box is displayed to confirm the deletion. Select **Yes** to delete the token.
  - Select the pencil button to edit the token. A dialog box is displayed that provides editing controls for the token.

If the tokens list spans 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.

Add a Token

Select **Add Token** to add a new token to the Crestron Virtual Control server. The **Add Token** dialog box is displayed.

Add Token Dialog Box



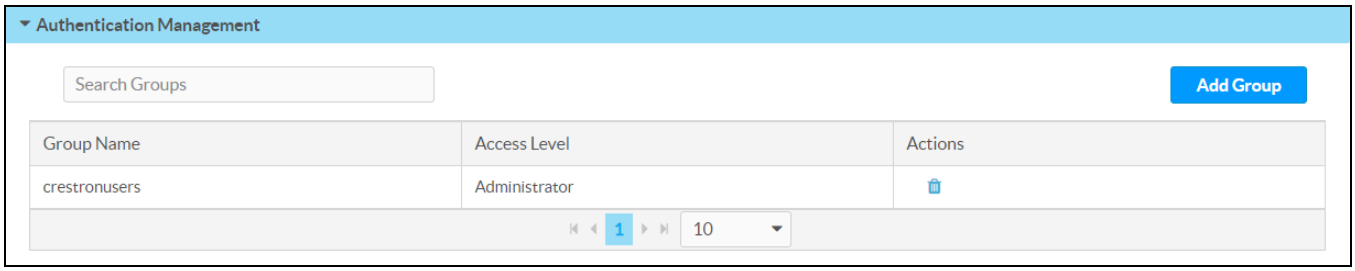
- Enter a description for the token in the **Description** text field.
- Fill the **Read-Only** check box to assign read-only permissions to the token. If this setting is not selected, then the token will have read/write permissions.

Once the token information has been entered, select **Add**. A new token is generated and added to the **Tokens** table.

Authentication Management

Select **Authentication Management** to view and configure authentication group settings for the Crestron Virtual Control server.

Settings Tab - Authentication Management



NOTE: Groups and users must be created on the Linux platform before they can be added to the Crestron Virtual Control server. For more information, refer to Configure Secure Device Connections on page 139.

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

- **Group Name**: The group name.
  - For local Linux groups, enter the group name only (such as "crestronusers").
  - For Active Directory® (LDAP) service groups, enter the domain and group name (such as "CRESTRON.COM\ldapusers"). The operating system must be configured to resolve the LDAP user that is used by the connecting device.
- **Access Level**: An access level for the group (**Administrator**, **Operator**, or **Connect**).

- **Actions**: Provides a trash can button that can be selected to delete the group. A dialog box is displayed to confirm the deletion. Select **Yes** to delete the group.

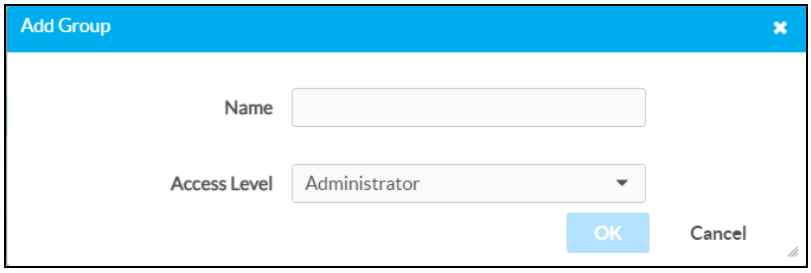
Type a full or partial search term into the **Global Filter** text field to search for and display groups that match the search term.

If the groups list spans 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.

Add an Authentication Group

Select **Add Group** to add a new authentication group to the Crestron Virtual Control server. The **Add Group** dialog box is displayed.

Add Group Dialog Box



Enter the following information for the group.

> **NOTE:** The group name and access level must match exactly the corresponding group that is configured on the Linux platform.

- **Name**: Enter the group name as it appears on the Linux platform.
- **Access Level**: Use the drop-down menu to select the access level assigned to the group on the Linux platform (**Administrator**, **Operator**, or **Connect**).

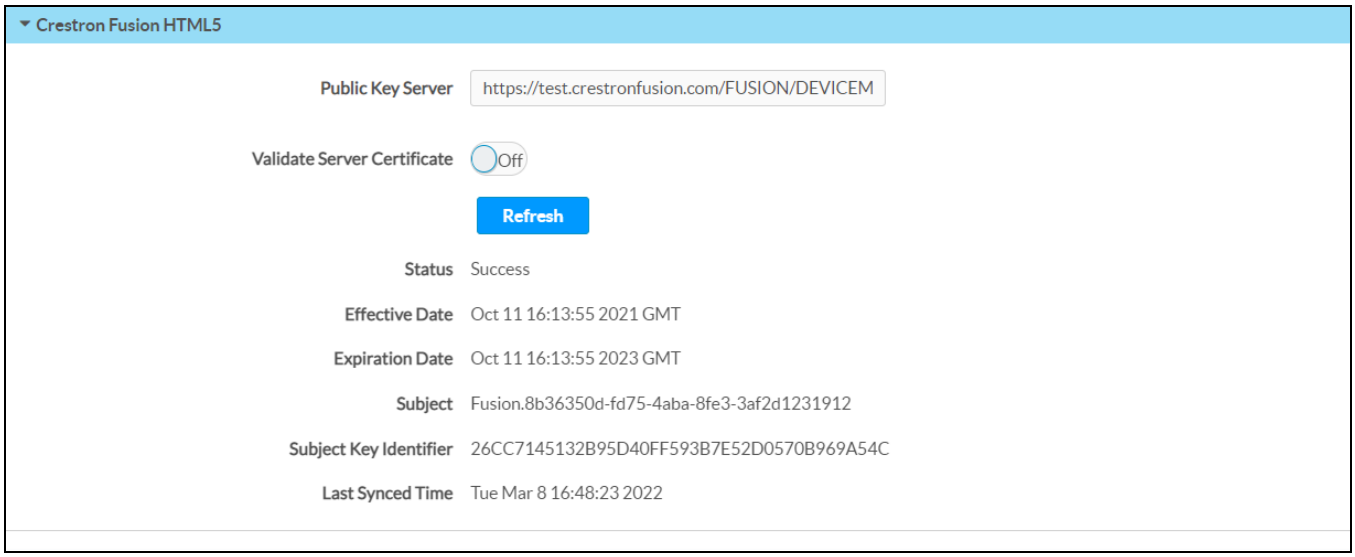
Select **OK**. The new group is added to the **Authentication Management** table.

Crestron Fusion HTML5

Select **Crestron Fusion HTML5** to configure a Crestron Fusion® software server certificate that is connected to the Crestron Virtual Control server. The server certificate is used to authenticate an HTML5 Web XPanel project deployed to a static web server for access via the **e-Control** function in Crestron Fusion.

> **NOTE:** For more information on deploying an HTML5 Web XPanel project to a web server, refer to the Crestron HTML5 User Interface Developer Microsite.

Settings Tab - Crestron Fusion HTML5



The following settings can be configured and viewed:

- **Public Key Server**: Enter the URL of the Crestron Fusion server location that contains the server certificate used to authenticate the HTML5 Web XPanel project.

  The following example shows the format of a public server key URL for a Crestron Fusion server:

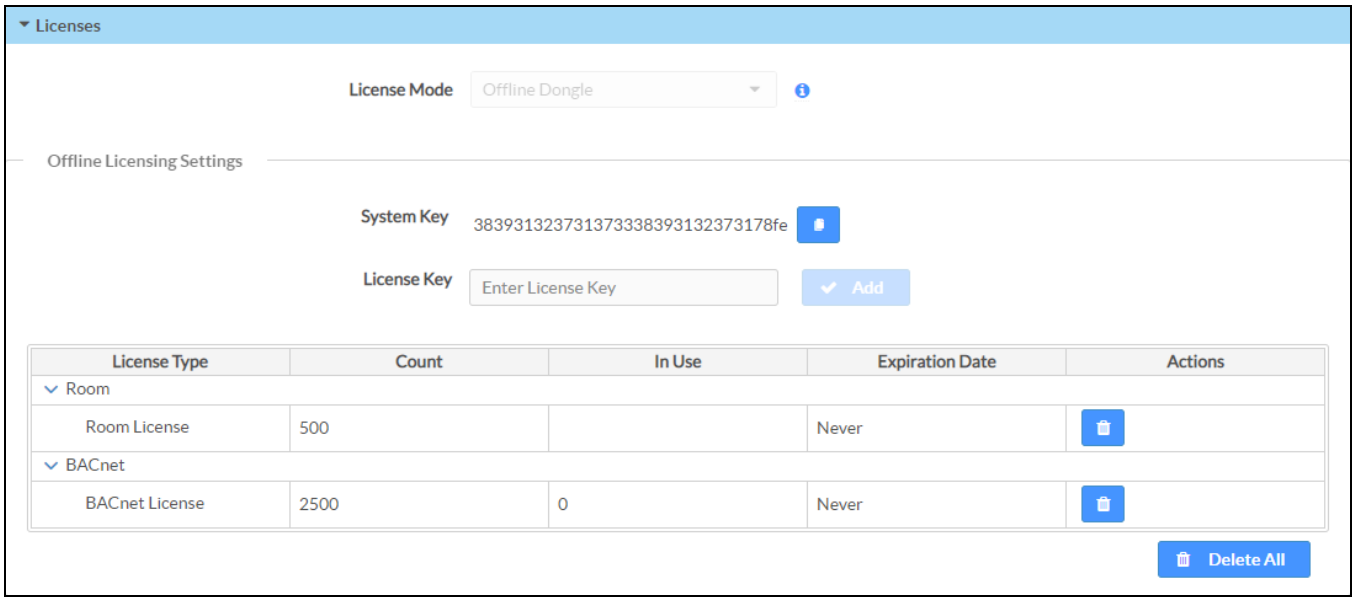
  ```
  https://test.crestronfusion.com/fusion/devicemanager/api/certificate
  ```

- **Validate Server Certificate**: Turn on the toggle to require the server certificate to be validated before it is accepted.
- Select **Refresh** to refresh the connection to the server certificate.
- **Status**: The status of the Crestron Fusion server certificate connection.
- **Effective Date**: The effective date of the server certificate.
- **Expiration Date**: The expiration date of the server certificate.
- **Subject**: The subject of the server certificate.
- **Subject Key Identifier**: The unique subject key identifier of the server certificate.
- **Last Synced Time**: The time when the Crestron Fusion server certificate was last synced to the Crestron Virtual Control server.

Licenses

Select **Licenses** to configure the current license mode for the Crestron Virtual Control server and to add or remove licenses (for offline licensing only).

Settings Tab - Licenses



Use the **License Mode** drop-down menu to change the licensing mode between online (**XiO Cloud**) and offline (**Offline Dongle**) licensing modes.

NOTE: The licensing mode can be changed only if there are no active licenses within the current licensing mode. For more information, refer to Manage Licenses on page 92.

If **Offline Dongle** is selected for **License Mode**, the following offline licensing settings can be configured and viewed:

NOTE: The USB-OFFLINE dongle must be connected to the VC-4-PC-3 or the host running VC-4 at all times if using offline licensing. If the USB-OFFLINE dongle is removed, offline licensing settings cannot be configured.

- **System Key**: The VC-4 system key that is required to obtain an offline license key from Crestron. Use the copy button to copy the system key to the clipboard.
- **License Key**: Enter the offline license key that is tied to a specific VC-4 system key and number of room licenses or BACnet licenses. This license key is provided by Crestron as described in Manage Licenses Offline on page 95.

  Once a valid license key has been entered, select **Add** to add the room or BACnet licenses specified by the license key to the Crestron Virtual Control server. The licenses are populated in the table below this setting.

Each offline license is represented in a table that provides the following information and controls:

> **NOTE:** For more information on adding offline licenses to the Crestron Virtual Control server, refer to Manage Licenses Offline on page 95.

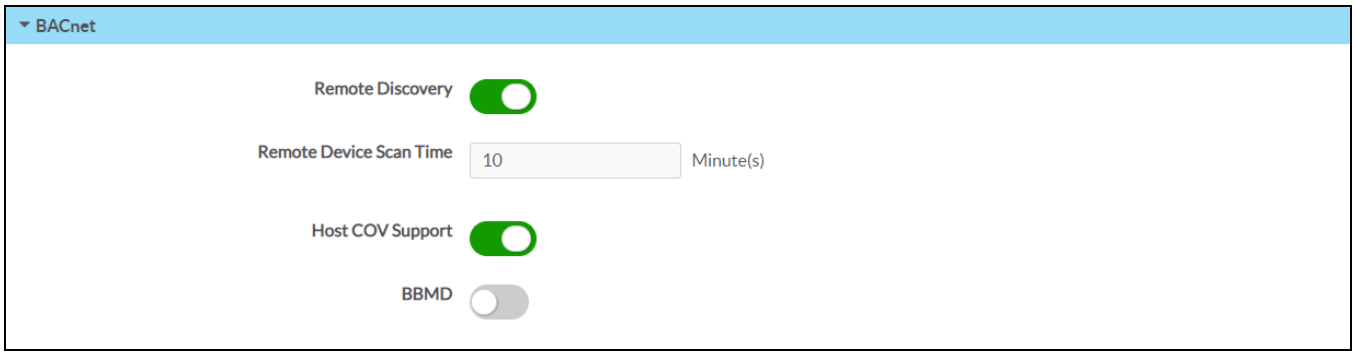
- **License Type**: The room license type. Select the arrow button next to the room license type to show more information about purchased licenses of that type.
- **Count**: The total number of available licenses of a type for the Crestron Virtual Control server.
- **In Use**: The number of licenses that are currently in use by the Crestron Virtual Control server.
- **Expiration Date**: The date that the licenses are set to expire (if applicable).
- **Actions**: Provides a trashcan button that can be selected to delete the license from the Crestron Virtual Control server. If a license is deleted, it must be added back to Crestron Virtual Control before its respective rooms or BACnet objects will function.

Select **Delete All** below the table to delete all active offline licenses from the Crestron Virtual Control server.

BACnet

Select **BACnet** to configure settings for the BACnet network/IP connection within Crestron Virtual Control.

Settings Tab - BACnet



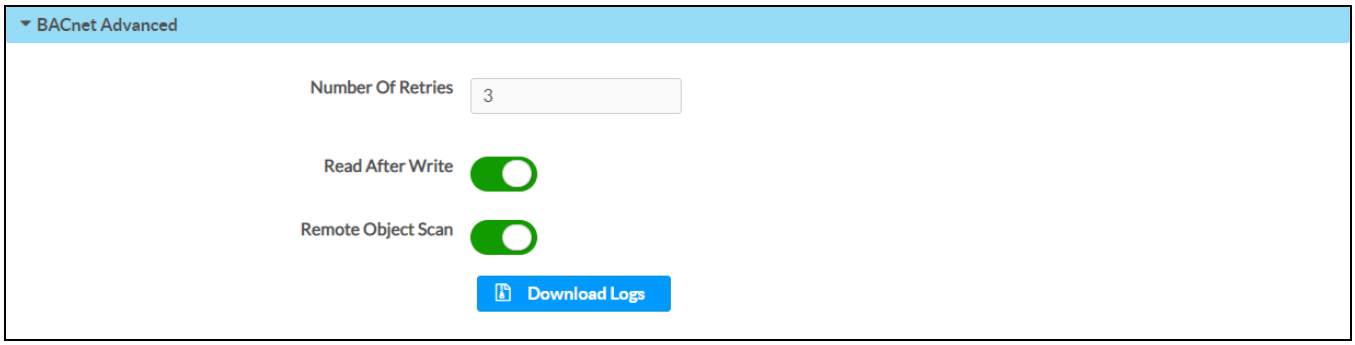
The following **BACnet** settings are displayed:

- **Remote Discovery**: Turn on the toggle to turn on the auto discovery function for remote BACnet devices and objects.
- **Remote Device Scan Time**: Enter the duration (in minutes) that Crestron Virtual Control will scan for remote BACnet devices and objects.
- **Host COV Support**: Turn on the toggle to turn on COV (Change of Value) support for host BACnet objects.
- **BBMD**: Turn on the toggle to turn on the BBMD (BACnet Broadcast Management Devices) functionality.

BACnet Advanced

Select **BACnet Advanced** to configure advanced BACnet network/IP settings within Crestron Virtual Control.

Status Tab - BACnet Advanced



The following **BACnet Advanced** settings are displayed:

- **Number Of Retries**: Enter the number times that Crestron Virtual Control will attempt to reconnect to a BACnet device if a connection error is discovered.
- **Read After Write**: Turn on the toggle to turn on the read request after write functionality.
- **Remote Object Scan**: Turn on the toggle to turn on the object discovery for remote devices functionality.
- Select **Download Logs** to download the BACnet log files as a .zip file to the local computer.

Secure Deployment

This section provides the recommended procedures for deploying the Crestron Virtual Control server securely on a corporate network.

> **NOTE:** The VC-4-PC-3 is hardened out of the box and does not require any secure deployment procedures.

This section provides the following information:

- Security Overview on page 137
- Harden the Linux Platform on page 138
- Harden the Crestron Virtual Control Software on page 139

Security Overview

Crestron Virtual Control is available as a software application that must be installed onto a customer-provided Linux® server (VC-4), or it comes preinstalled and fully configured on a Dell® micro computer (VC-4-PC-3).

Linux is an open-source operating system. The distribution of a Linux operating system consists of various components that are created and maintained by different developers. VC-4 installations require a supported Linux operating system as described in Prerequisites on page 32. The VC-4-PC-3 runs on an AlmaLinux OS® operating system, which is binary compatible with Red Hat Enterprise Linux® server software.

Crestron installation scripts reference updates for the components used by VC-4. In addition, updates for the VC-4-PC-3 include updates for all components present on the device.

For customer-supplied Linux servers, Crestron is responsible for keeping the VC-4 software up to date and will provide security patches when necessary. The customer is responsible for any custom security configurations and update management. The VC-4-PC-3 is hardened out of the box and does not require any secure deployment procedures. Crestron follows industry-standard best practices for configuring the VC-4-PC-3 server.

For both VC-4 and the VC-4-PC-3, Crestron follows the guidance of package owners regarding the stability of the provided components and will provide updates accordingly. Customers may choose to update individual components to meet their own security requirements.

Harden the Linux Platform

Prior to hardening the Crestron Virtual Control server for secure deployment, the Linux platform and the Apache® web server must first be hardened.

Refer to the following resources for more information:

- To harden the Linux platform on Red Hat Enterprise Linux software, refer to https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/index.
- To harden the Apache web server, refer to https://httpd.apache.org/docs/2.4/misc/security_tips.html.

SELinux may also need to be disabled to perform certain installation or deployment tasks for Crestron Virtual Control. Any task that requires disabling SELinux will be called out within Crestron Virtual Control documentation.

To configure or disable SELinux for Red Hat software, refer to https://linuxize.com/post/how-to-disable-selinux-on-centos-7/.

Harden the Crestron Virtual Control Software

The following sections describe the procedures that must be performed to harden the Crestron Virtual Control server, as well as other recommended security protocols.

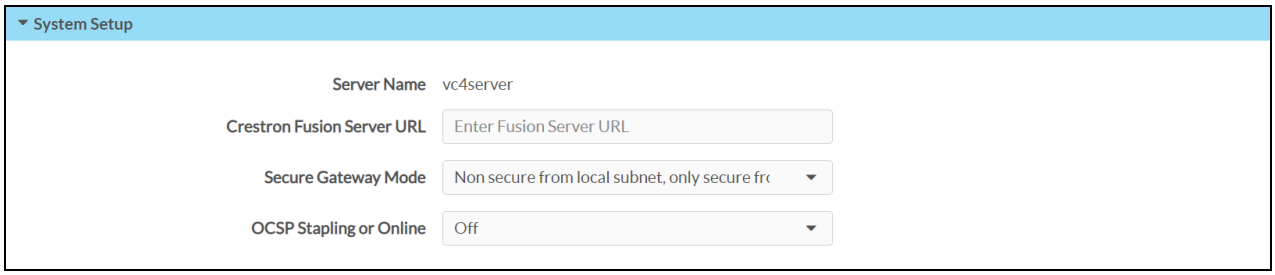
Configure Secure Device Connections

The Crestron Virtual Control server provides settings for configuring secure device connections between the server and controlled devices. Secure device connections are established by configuring the secure gateway settings for the Crestron Virtual Control server or by enabling authentication for secure CIP (Cresnet over IP) connections.

To configure secure gateway mode settings for the Crestron Virtual Control server:

1. With the Crestron Virtual Control service running, navigate to **Settings** > **System Setup** in the web user interface.

   Settings Tab - System Setup

2. Use the **Secure Gateway Mode** drop-down menu to select one of the following options:
   - **Only secure**: Only secure device connections are accepted by the server.
   - **Secure and non secure**: Both secure and nonsecure device connections are accepted by the server.
   - **Non secure from local subnet, only secure from remote subnets**: Nonsecure device connections from local subnets are accepted by the server, but only secure device connections from remote subnets are accepted by the server.
3. Select **Save** from the **Actions** drop-down menu on the top right of the screen to save any changes.

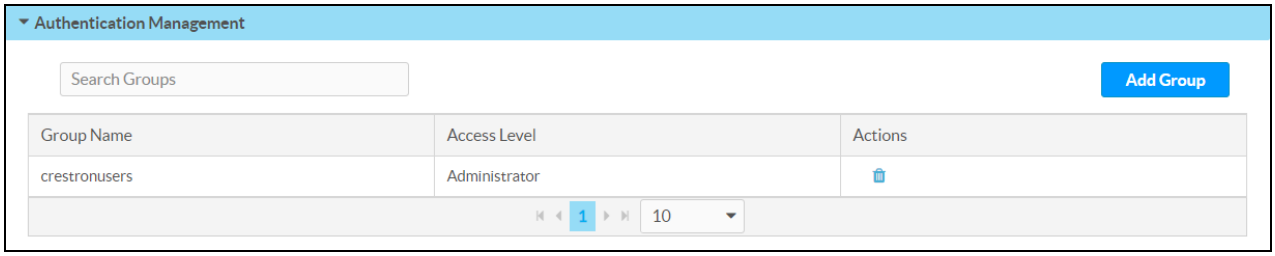
   > **NOTE:** If the **Secure Gateway Mode** is changed to **Only secure** while a non-secure device connection is active, including a connection to the web XPanel interface, the non-secure connection is not terminated automatically.

To configure authentication for secure CIP connections:

1. Create authentication groups on the Linux platform, and add users to the groups based on the desired access level for each user.

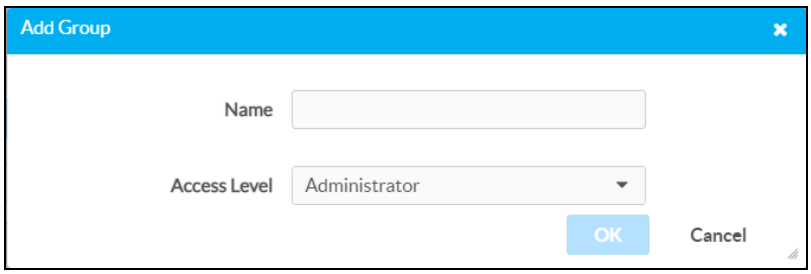
2. With the Crestron Virtual Control service running, navigate to **Settings** > **Authentication Management** in the web user interface.

   Settings Tab - Authentication Management



3. Select **Add Group**. The **Add Group** dialog box is displayed.

   Add Group Dialog Box



4. Enter the group name and select the access level exactly as it is configured on the Linux platform.
5. Select **OK**. The new group is added to the **Authentication Management** table.

Load TLS Certificates

The Crestron Virtual Control server provides built-in support for Transport Layer Security (TLS) 1.2. TLS ensures that the connection between the web browser and the Crestron Virtual Control server is secure via encryption.

Prior to configuring TLS for the Crestron Virtual Control server, a TLS server certificate (public key) and a private key must be generated.

These files must have the following properties:

- Be either self-signed or CA (Certificate Authorities)-signed
- Be in PEM format and matched as a public and private RSA key pair
- Not be encrypted
- Contain no spaces in the file names

Once the TLS server certificate and private key are generated, load them into the Linux platform that is running the Crestron Virtual Control service as follows:

> **NOTE:** HTTPS must be enabled on the Apache server in order to accept TLS connections, including downloading mobile projects and touch screen projects from secure touch screens.

1. Copy the TLS server certificate and private key files into a directory on the Linux platform that may be accessed by the Crestron Virtual Control service's runtime.
2. Navigate to the **[VirtualControlHome]/conf** directory.
3. Open the **ssl.conf** file in a text editor application:
    a. Type "SSLCertificateFile [Filepath]/[TLSCertificateFile]" on the first line, where "Filepath" is the file path of the TLS server certificate file and "TLSCertificateFile" is the name of the certificate file (e.g., **/home/builduser/crestron/[certificate-name].pem**).
    b. Type "SSLPrivateKeyFile [Filepath]/[TLSPrivateKeyFile]" on the second line, where "Filepath" is the file path of the private key file and "TLSPrivateKeyFile" is the name of the private key file (e.g., **/home/builduser/crestron/[private-key].pem**).

        NOTE: Ensure that there are no spaces in the file path or the certificate files.

    c. Save and exit the file.
4. Launch the Crestron Virtual Control service. Any changes to TLS take effect immediately.

NOTE: Observe the following points about TLS.

- Crestron Virtual Control only supports TLS 1.2. Crestron Virtual Control does not support TLS 1.0 and TLS 1.1.
- TLS certificates and keys may be loaded while the Crestron Virtual Control service is running. However, the service must be restarted before changes take effect.
- To test the TLS certificates and keys, open a packet analyzer software (such as Wireshark® software), and listen on port 41796. The "certificate" argument should show in the public key details.

Configure Secure Flash Policy Files

If using the Virtual Control server's built-in web XPanel interface for program testing and control, an Adobe® software Flash® technology policy server must be implemented. The Crestron Virtual Control server defaults to an unsecured Flash policy server for use with the web XPanel interface.

For more information on configuring the Flash policy server, refer to www.adobe.com/devnet/flashplayer/articles/socket_policy_files.html.

To implement a secured Flash policy server:

1. Create and load a CA-certified TLS server certificate pair for the Flash policy server. For more information on creating and loading TLS certificates, refer to Load TLS Certificates on page 140.
2. Navigate to **[VirtualControlHome]/samples/flashpolicyserver**, where **[VirtualControlHome]** is the Virtual Control home directory set during installation (the default is **/opt/crestron/virtualcontrol**).
3. Copy the appropriate .conf file to the **[VirtualControlHome]/conf** directory:
    a. To implement a secured Flash policy server, copy the **SecureFlashPolicyServer.conf** file.
    b. To implement an unsecured Flash policy server, copy the **UnsecuredFlashPolicyServer.conf** file.

> **NOTE:** Although an unsecured Flash policy server is enabled on the Virtual Control server by default, the **UnsecuredFlashPolicyServer.conf** file may be implemented to disable the Flash policy server or to change the listening port.

4. Rename the filename of the copied file to "FlashPolicyServer.conf".
5. Open the FlashPolicyServer.conf file in a text editing application.
6. Edit the following lines as required by the implementation:
   a. To disable the Flash Policy Server, enter "FlashPolicyServer = Disabled" in line 3. The Flash Policy Server is enabled by default.
   b. To turn off a secure connection for the Flash Policy Server, enter "Secure = Off" in line 5. A secure connection is turned on by default.
   c. Set the domain to validate the server against by entering "Domain = [domain]" in line 7, where [domain] is the domain name that the server should be validated against. The default value for [domain] is "*", which represents a generic domain.
   d. Set the internal listening port that will be mapped to the web XPanel interface by entering "Port = [port] on line 9, where [port] is the port that will be used for mapping. The default value for [port] is "1025".

   > **NOTE:** Observe the following mapping rules for the Flash policy server:
   >
   > - The internal listening port for the Flash policy server must be mapped to external port 843 using the `iptables` command. If the internal listening port is changed from the default port 1025, issue the `iptables -t nat -A PREROUTING -p tcp --dport 843 -j REDIRECT --to-ports [port#]` command, where `[port#]` is the desired internal listening port.
   > - • If the internal listening port is changed after the rule above is applied, the rule must be deleted by issuing the `iptables -t nat -D PREROUTING -p tcp --dport 843 -j REDIRECT --to-ports [port#]` command, where `[port#]` is the current internal listening port. Then, issue the add command provided in the note above with the new internal port number.
   > - Any `iptables` rules that are added persist across server restarts.

7. Save and exit the file.
8. Restart the Crestron Virtual Control service by issuing the `sudo systemctl restart virtualcontrol` command.

Configure File Access to Crestron Files

Whenever the **ssl.conf** file or the **FlashPolicyServer.conf** file is copied in the **[VirtualControlHome]/conf/** path, the ownership must change to "virtualcontroluser."

To change the ownership for these files, issue the `sudo chown virtualcontroluser.virtualcontroluser [filename]` command in the terminal, where `[filename]` is the filename of the copied .conf file.

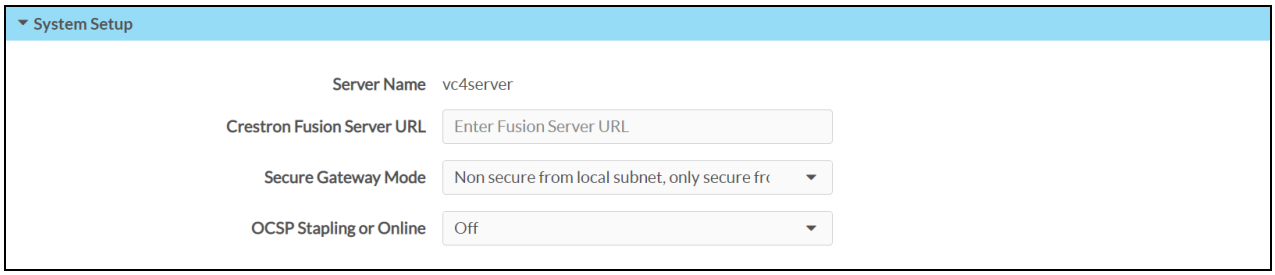
Configure OCSP Client Settings

OSCP (Online Certificate Status Protocol) is an internet protocol for validating X.509 digital certificates (such as SSL), which is used to maintain the security of the Crestron Virtual Control server and network resources. The Crestron Virtual Control web interface provides settings for configuring the OSCP behavior of the web browser client when connecting to the Crestron Virtual Control server to validate certificates.

To configure OCSP client settings:

1. With the Crestron Virtual Control service running, navigate to **Settings** > **System Setup** in the web user interface.

   Settings Tab - System Setup

2. Use the **OCSP Stapling or Remote** drop-down menu to select one of the following options:
   - **Off**: Turns OSCP off
   - **Staple Only**: Sets the OCSP client behavior to staple only (In this state, the Crestron Virtual Control server appends a time-stamped, self-signed OCSP response to a certificate sent by the web browser client for self-validation.)
   - **Remote**: Sets the OCSP client behavior to remote (In this state, the web browser client sends remote certificates that are validated by the Crestron Virtual Control server.)
3. Select **Save** from the **Actions** drop-down menu on the top right of the screen to save any changes.

Configure PAM Authentication

The Crestron Virtual Control server may be monitored and configured using the included web configuration interface. The web interface also provides selections for viewing and configuring rooms, programs, and connected devices.

> **NOTE:** The Crestron Virtual Control web interface is accessible via two different URLs: one for administrators (read/write permissions), and one for users/operators (read-only permissions). For more information, refer to the Initial Setup on page 54.

The Apache server may be configured to use PAM (Pluggable Authentication Module) to add an extra layer of security to the web interface. When PAM is enabled on the Linux server, users must be authenticated before access to the web interface is granted.

For more information on configuring PAM for the Red Hat server, refer to https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/managing_smart_cards/pluggable_authentication_modules.

NOTE: Timeout settings should be configured for the Linux server to ensure that an authenticated session is terminated after a set timeout duration.

To enable PAM on Crestron Virtual Control:

1. Enable HTTPS on the Crestron Virtual Control server with default certificates.

```
sudo dnf -y  install mod_ssl

sudo firewall-cmd --zone=public --permanent --add-service=https

sudo firewall-cmd --reload
```

2. Install mod_authnz_pam.

```
# dnf -y install mod_authnz_pam

# vi /etc/httpd/conf.modules.d/55-authnz_pam.conf

# uncomment
LoadModule authnz_pam_module modules/mod_authnz_pam.so
```

3. Issue `vi /etc/pam.d/httpd-auth` to create a new PAM authentication file.
4. Add the following three lines to the end of the file.

```
auth       required     pam_listfile.so item=user sense=deny
file=/etc/httpd/conf.d/denyusers onerr=succeed
auth       include      system-auth
account    include      system-auth
```

5. Issue the following commands.

```
sudo chgrp apache /etc/shadow

sudo chmod 440 /etc/shadow
```

6. Change directories to **/etc/httpd/conf.modules.d/**.
7. Open the **crestron.conf** file in a text editor application. Administrative privileges are required to edit the file.
8. Add the following lines above the "# Settings api redirect" section of text.

```
<Location ${CRESTRON_VC_4_WEBROOT}/config/settings/WebApi/>
   SSLRequireSSL
   AuthType Basic
   AuthName "PAM Authentication"
   AuthBasicProvider PAM
```

```
   AuthPAMService httpd-auth
   Require valid-user
</Location>

<Location ${CRESTRON_VC_4_WEBROOT}/config/status/WebApi/>
   SSLRequireSSL
   AuthType Basic
   AuthName "PAM Authentication"
   AuthBasicProvider PAM
   AuthPAMService httpd-auth
   Require valid-user
</Location>
```

9. Save and exit the file.
10. Issue `sudo setsebool -P httpd_mod_auth_pam 1` to allow HTTPD access to PAM authentication.
11. Restart the HTTPD services by issuing the `systemctl restart httpd` command.

Configure XPanel Authentication with PAM

The configuration and web XPanel interface pages for individual rooms may also be configured to require authenticated access.

To configure the configuration pages for a room, add the following lines to the authentication changes text in the **crestron.conf** file:

```
<Location ${CRESTRON_VC_4_WEBROOT}/Rooms/[RoomID]/cws/>
   SSLRequireSSL
   AuthType Basic
   AuthName "PAM Authentication"
   AuthBasicProvider PAM
   AuthPAMService httpd-auth
   Require valid-user
</Location>
```

To configure the web XPanel interface pages for a room, add the following lines to the authentication changes text in the **crestron.conf** file:

```
<Location ${CRESTRON_VC_4_WEBROOT}/Rooms/[RoomID]/XPanel/Core3XPanel.html>
   SSLRequireSSL
   AuthType Basic
   AuthName "PAM Authentication"
   AuthBasicProvider PAM
   AuthPAMService httpd-auth
   Require valid-user
</Location>
```

NOTE: [RoomID] is the unique room identification value that is assigned to a room in the Crestron Virtual Control server. To obtain the room ID from the web interface, click the information button ℹ next to the room name, and note the value listed for **Room ID**.

Configure HTML5 UI Authentication with PAM

To configure authenticated access for HTML5 User Interface projects with PAM, add the following lines to the authentication changes text in the **crestron.conf** file:

```
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1

AliasMatch "^/cws/websocket/getWebSocketToken" "${CRESTRON_VC_4_
HOME}/CrestronApps/websocket/getWebSocketToken"
<Directory ${CRESTRON_VC_4_HOME}/CrestronApps>
  Require all granted
  RewriteRule "websocket/getWebSocketToken" "/cws/websocket/getWebSocketToken" [PT,E=MATCH_ROOM_
ID:websocket,H=proxy:unix:${CRESTRON_VC_4_HOME}/var/run/app-
websocket.socket|fcgi://localhost/cws]
</Directory>

<Location /cws/websocket/getWebSocketToken>
  SSLRequireSSL
  AuthType Basic
  AuthName "PAM Authentication"
  AuthBasicProvider PAM
  AuthPAMService httpd-auth
  Require valid-user
</Location>

<Directory  ${CRESTRON_VC_4_HOME}/RunningPrograms>
  SSLRequireSSL
  AuthType Basic
  AuthName "PAM Authentication"
  AuthBasicProvider PAM
  AuthPAMService httpd-auth
  Require valid-user
</Directory>
```

Configure Cgroup Settings

Cgroups is a Linux kernel feature that provides options for configuring the resource usage of certain Linux processes. For more information on the specific controls and functions available within cgroups, refer to https://linux.die.net/man/5/cgconfig.conf.

For Crestron Virtual Control, cgroups is used primarily to configure CPU and memory limits for the service, although other processes can also be configured.

To configure cgroup settings for Crestron Virtual Control:

1. Change directories to **/opt/crestron/virtualcontrol/conf/**.
2. Open the **vc4cgconfig.conf** file in a text editor application.
3. Make any necessary changes in the file and save.

> **NOTE:** Do not delete any fields from the .conf file, even if they are not required for your deployment.

4. Issue the following command to load the updated configuration to the cgroups parser:

```
sudo cgconfigparser --load=/opt/crestron/virtualcontrol/conf/vc4cgconfig.conf
```

5. Issue the following restart commands to have the updated configuration take effect:

```
sudo systemctl restart cgconfig.service

sudo systemctl restart virtualcontrol.service
```

Reference Topics

The following topics provide detailed reference information for Crestron Virtual Control installations.

This section provides the following information:

- Turn On Local System Logging on page 149
- Opened Server Ports on page 151
- Troubleshoot Room Addresses on page 152
- Connect Devices across Subnets on page 153
- Build a Custom VC-4 Computer on page 154

Turn On Local System Logging

The Crestron Virtual Control service provides support for local system logging. Sample **syslog.conf** files are provided in the installation package that may be modified as needed.

To access the sample .conf files, navigate to **[VirtualControlHome]/samples/conf_files**, where **[VirtualControlHome]** is the home directory set during installation.

To turn on local system logging for the Crestron Virtual Control server:

> **NOTE:** Local Crestron log files are created in the **/var/log/crestron/** directory.

1. Move the **50-default.conf** file from **[VirtualControlHome]/samples/conf_files** to the **/etc/rsyslog.d/** directory.
2. Open the **50-default.conf** file.
3. Configure local logging settings by commenting, uncommenting, or modifying the appropriate lines as follows:
    a. Use the template below to create a customized log format for Crestron logs:

    ```
    $template crestron_template,"<%syslogseverity-text%> %timegenerated%
    %HOSTNAME% %syslogtag% %msg%\n"
    ```

    b. Use the template below to create a customized log file name per application (Use if a separate log file is needed for the application instead of a common log file):

    ```
    $template CUSTOM_LOGS,"/var/log/crestron/%syslogtag:F,58:1%.log"
    ```

    > **NOTE:** In the log file format above, "F" is the FromChar field, "58" is the ASCII value of the delimiter, and "1" is the first field before the delimiter.

    c. Use the template below to create a single log file for all applications:

    ```
    $template SINGLE_LOG,"/var/log/crestron/crestron.log"
    ```

    d. Comment any filters between lines 33–68 to send the commented item to the system log instead of the single log (shown on line 25).

    > **NOTE:** Comment all filters to send all items to the system log.

    e. Configure any other Linux syslog settings as needed.
4. Save and exit the file.
5. Issue `sudo systemctl restart rsyslog.service` to restart the system logging service.

If SELinux is turned on for the Linux platform, the Linux OS logs to **/var/log/messages** by default. To use the Crestron-provided sample .conf files with SELinux, issue the following commands:

```
sudo semanage fcontext -a -t syslog_conf_t /etc/rsyslog.d/50-default.conf
```

```
sudo restorecon -v /etc/rsyslog.d/50-default.conf
```

Opened Server Ports

The Crestron Virtual Control server requires the following external and internal ports to be open while the server is running. These ports are opened when installing Crestron Virtual Control.

Opened External Server Ports

Port Number	Service	Notes
80 / 443	HTTP/HTTP(S) (TCP)	Local web server used to administer Crestron Virtual Control
161 / 163	SNMP (UDP)	Simple network management protocol listening port
843	Flash® policy server (TCP)	This port may be disabled if a Flash policy server is not used. For more information, refer to Configure Secure Flash Policy Files on page 141.
9090	Cockpit graphical interface (TCP)	This port is opened for the VC-4-PC-3 only
41794	CIP communication (UDP/TCP)	
41796	Secure CIP communication (TCP)	
49200	HTML5 Web XPanel	For more information on setting up secure communications for the HTML5 Web XPanel, refer to Configure HTML5 UI Authentication with PAM on page 146.

Opened Internal Server Ports

Port Number	Service	Notes
1025	Listening port for Flash policy server (UDP)	This port may be disabled if a Flash policy server is not used. For more information, refer to Configure Secure Flash Policy Files on page 141.
3306	MySQL (TCP)	
5000	WebApp listening messages (UDP)	WebApp is the Crestron Virtual Control interface into the web server.
(User Defined)	Redis (TCP)	Default port is 6980.
50051	DBApp listening messages (UDP)	DBApp is the Crestron Virtual Control interface into the MariaDB database.

For any outbound connections made from the Crestron Virtual Control server, such as connections to Crestron Fusion® software, .AV Framework™ software, or XiO Cloud, the appropriate ports must be opened on the Linux server.

The Crestron Virtual Control server must also be configured to allow the following services to run:

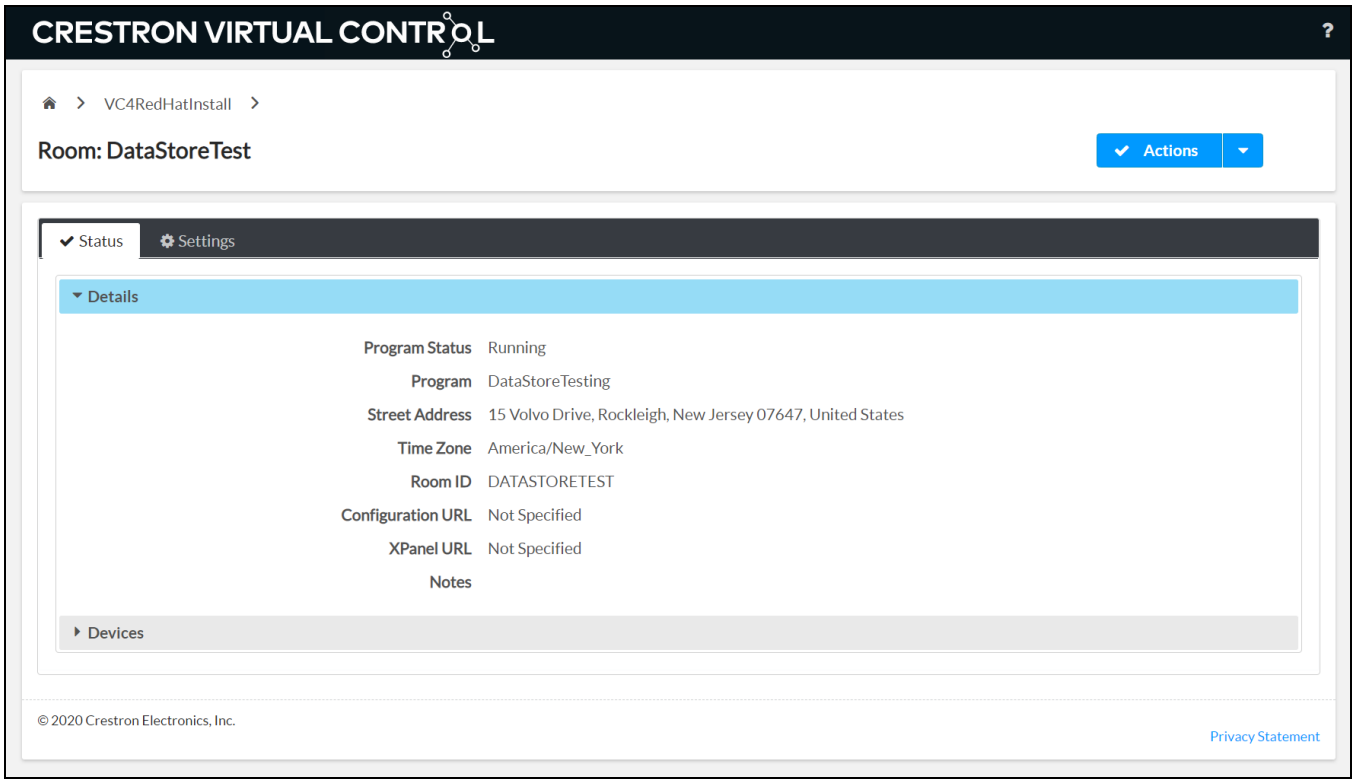
- DNS Client
- Active Directory
- SNTP (Simple Network Time Protocol)

Troubleshoot Room Addresses

When a room is added to the Crestron Virtual Control server, a street address may be entered to return a time zone for the room automatically. Programs use time zones to ensure that programmatic events are started and stopped at the correct time based on the location of the associated room.

For more information on setting room addresses, refer to Add Room on page 105.

Status Page - Details Tab



Addresses are checked against the Microsoft® Azure® service's Geolocation API. If the Geolocation API recognizes the address, the time zone associated with the address is returned for the room. If the Geolocation API does not recognize the address, the default "America/New_York" value is returned as the **Time Zone** status for the room.

If a street address does not return the correct time zone, the following solutions may be attempted:

- Confirm that the address is typed and formatted correctly.
- Enter a city-level address instead of a street-level address (for example, "Toronto, Canada").
- Enter the latitude, longitude, and time zone of the location manually. The **Address sets location data** toggle must be turned off to use these fields.

Connect Devices across Subnets

Most Crestron devices with newer firmware use the Connect Request method (which specifies a Room ID) to connect automatically to rooms in the Crestron Virtual Control server. Devices with older firmware and Crestron control systems used for remote Ethernet processing must be associated manually with a room. However, if these devices are not on the same subnet as the server, they cannot be discovered.

As a workaround, the admin may create a **device_resolution.cfg** file that contains the FQDN (fully qualified domain name), MAC address, and device type for any cross-subnet devices that do not use the Connect Request method. The **device_resolution.cfg** file behaves as follows:

- The Crestron Virtual Control service reads this file on startup and then once every hour while the service is running.
- Each time the file is read, the server attempts to resolve the listed FQDN(s) via DNS.
- If the FQDN of a device is resolved, the device IP address is made available to the server, which provides the rest of the information required to make a connection. The device may then be associated manually with a room.

To connect to cross-subnet devices using a **device_resolution.cfg** file:

1. Log into an account with sudo privileges on the Linux platform where Crestron Virtual Control package is installed.
2. Navigate to **[VirtualControlHome]/samples/deviceresolution**, where **[VirtualControlHome]** is the Virtual Control home directory set during installation (the default is **/opt/crestron/virtualcontrol**).
3. Copy the **device_resolution.cfg** file to the **[VirtualControlHome]/conf** directory.
4. Open the copied **device_resolution.cfg** file in a text editing program.
5. Enter the following information for each cross-subnet device on one line of text, separated by commas (with no spaces):
   a. The fully qualified domain name ("tsw-770-1.yourdomain.com")
   b. The MAC address, using periods or colons ("11.22.33.44.55.66" or "11:22:33:44:55:66")
   c. The device type ("TSW-770")

   Example

   ```
   tsw-770-1.yourdomain.com,11.22.33.44.55.66,TSW-770
   tsw-770-2.yourdomain.com,00.11.22.33.44.55.66,TSW-770
   ```

6. Save and exit the file.

Crestron Virtual Control begins to read the file once every hour. To have the service read the file immediately (on startup), issue `sudo systemctl restart virtualcontrol`.

Build a Custom VC-4 Computer

Crestron Virtual Control software (VC-4) can be run on a custom computer that meets the following specifications:

- Use an NVMe (nonvolatile memory express) SSD (solid-state drive), as these have no moving parts. For server deployments, use an enterprise-grade HDD (hard drive disk) or SSD.
- It is recommended to select a drive with high TBW (terabytes written) and DWPD (drive writes per day) values, as these are indications that the drive will have a longer lifespan than drives with lower TBW and DWPD values.
- Ensure the computer is capable of running one of the supported Linux OS versions that are described in Prerequisites on page 32.

Refer to the following sample specifications for a custom computer drive that is capable of running VC-4:

- **DWPD**: 1.55
- **MTBF** (mean time before failure): 5,500,000 hours
- **Warranty**: 3 Years

Connecting an HTML5 XPanel with Self-Signed Certificates

Follow the instructions below to connect an HTML5 XPanel to a VC-4 room when using self-signed certificates.

> **NOTE**: This does not apply to the VC-4-PC-3 or to CA-signed certificates.

1. Configure PAM authentication through one of the following methods.
   - Follow the instructions in Configure PAM Authentication on page 143.
   - Use the scripts in Scripts for Hardening the Server.
2. Create a local Linux group and add it to Virtual Control. For more information, refer to Authentication Management on page 131.
3. Use one of the following methods.
   - Accept the self-signed certificate in a web browser.
     a. Navigate to the IP address or hostname followed by :49200. For example, **https://192.168.1.194:49200**.
     b. When prompted, accept the self-signed certificate. The browser will display a 404 error.
   - Use the same self-signed certificate for the Web UI as for the HTML5 XPanel communication.
     a. Using the terminal, connect to the VC-4 server.
     b. Issue the following command: `sudo nano /etc/httpd/conf.d/ssl.conf`
     c. Navigate to the line that begins with `SSLCertificateFile` and change it to `SSLCertificateFile /opt/crestron/virtualcontrol/data/ssl/certs/server.crt`.
     d. Navigate to the line that begins with `SSLCertificateKeyFile` and change it to `SSLCertificateKeyFile /opt/crestron/virtualcontrol/data/ssl/certs/server.key`.
     e. Save the file.
     f. Restart the web server with the `sudo systemctl restart httpd` command.

The HTML 5 XPanel will now connect to the VC-4 room.

Resources

The following resources are provided for the Crestron Virtual Control Server Software.

> **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
- Crestron Virtual Control - Steps in using SIMPL Programs CTI Course
- CAD Block Drawings for Crestron Virtual Control Application Scenarios

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

- .AV Framework Software for Crestron Virtual Control Software Operations Guide
- Crestron Fusion Software Help File
- Crestron Programming Design Guide
- REST API for Crestron Virtual Control Server-Based Control System Programming Guide
- XiO Cloud User Guide

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

Product Manual — Doc. 8912N
02/21/24
Specifications subject to
change without notice.