Crestron Virtual Control Server Software

Server-Based Control System

Security Reference Guide

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.

Revision History

Rev	Date	Notes	Author(s)
A	May 15, 2023	Initial version	IH, YS
B	June 30, 2023	Updated communication flow diagram and other minor changes	IH, YS

Please send comments and change recommendations to:

SecurityDocs@crestron.com

Contents

Introduction

This guide serves as a security reference and provides best practices for deploying Crestron Virtual Control (VC-4) software, which is a server-based control system that provides a scalable solution for using 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. The following information applies to both VC-4 variants unless specified otherwise.

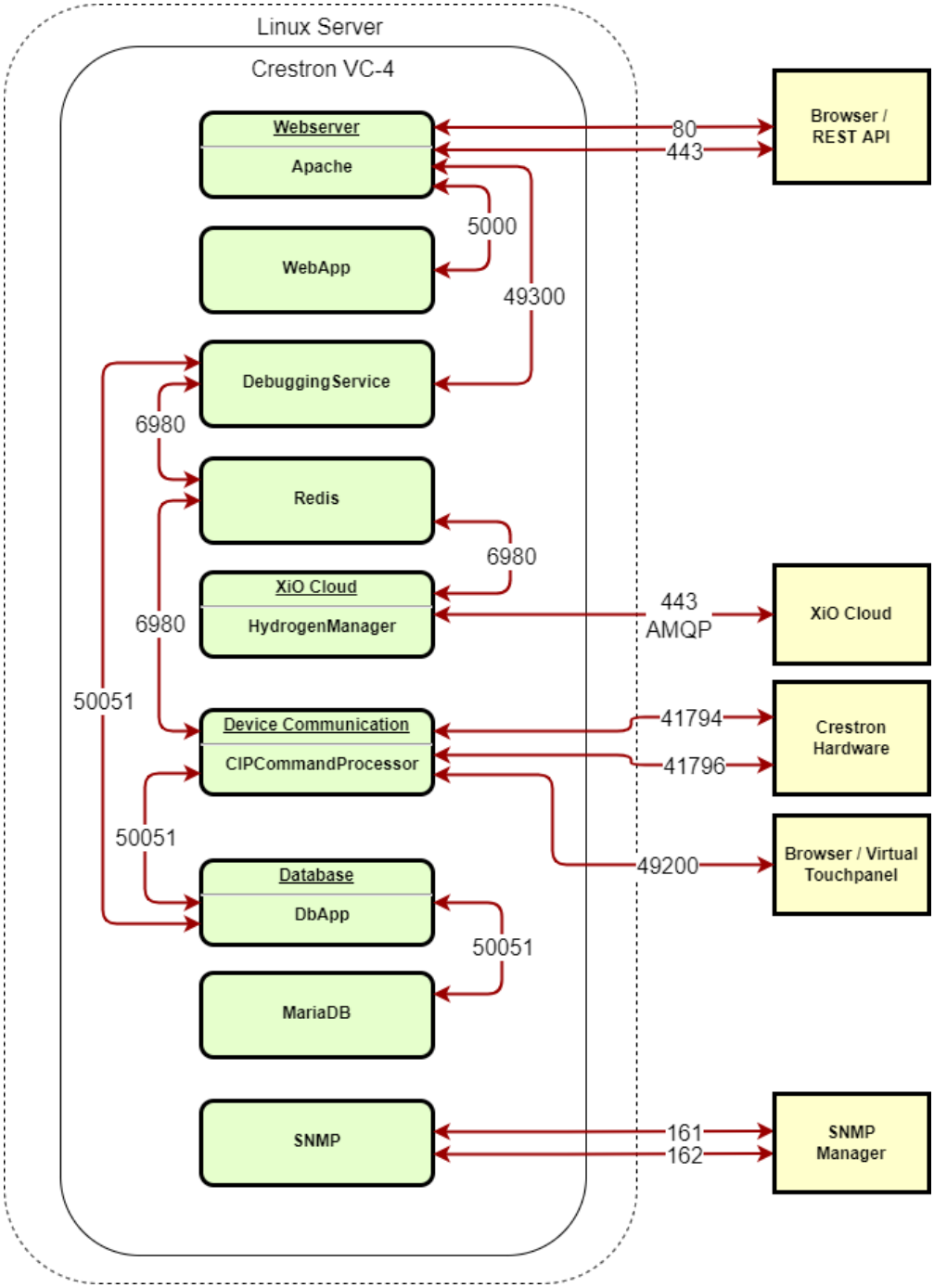
Intended Operational Environment

Crestron Virtual Control is available as a software application that must be installed onto a customer-provided Linux® server as a centralized control server (VC-4), or it comes preinstalled and fully configured on a Dell® micro computer as distributed control (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 Operating System on page 5. The VC-4-PC-3 runs on an AlmaLinux OS® operating system, which is binary compatible with Red Hat Enterprise Linux® server software.

VC-4 can be run in a virtualized environment or on a bare-metal server (such as a standalone computer). When running in a virtualized environment, the deployment can be scaled up (or down), supports taking snapshots, and provides redundancy and fault tolerance features. Running on a bare-metal server has a lower barrier to entry, as it requires no additional IT infrastructure to support the deployment.

The following diagram shows the Crestron Virtual Control communication flow. For more information on the external ports shown, refer to Network Port List on page 8.



Connectivity Requirements

Devices communicating with Crestron Virtual Control require direct outbound connectivity to the internet through the ports listed in Network Port List on page 8. For more information, refer to the diagram in Intended Operational Environment on page 1.

The path to the internet for the required ports needs to be free and unencumbered by other devices such as WAN optimizers, firewalls, and so forth.

Security Policies

For general security policies, refer to the Crestron security web page.

System Specifications

For general product specifications, refer to the VC-4-ROOM and VC-4-PC-3 product pages.

Product Software - Security Features

The following security features are supported.

User Authentication

For VC-4 server installations, user authentication is handled through the Linux platform. A user with administrative privileges must be created on the Linux platform to install and manage the VC-4 server.

For VC-4-PC-3 installations, a Linux admin user is created during the initial configuration of the device. For more information, refer to the Crestron Virtual Control Product Manual.

Additional groups and users must be created on the Linux platform before they can be added to the Crestron Virtual Control server.

Audit Logging

System tasks use Linux standard audit logging. Security-related application tasks are logged and stored in the audit log.

Connectivity

Crestron Virtual Control can connect to the XiO Cloud® provisioning and management service for monitoring, configuration, and licensing. For more information on the security features provided by the XiO Cloud service, refer to the XiO Cloud Service Security Reference Guide.

Software Update and Patches

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 providing VC-4 software updates and security patches for relevant packages when necessary. The customer is responsible for running any software updates. The customer is also 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.

Operating System

Crestron Virtual Control can be installed onto one of the following Linux platforms that resides 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: Version 9.x of any of the listed operating systems is not currently supported.

The VC-4-PC-3 comes with the Alma Linux OS® Linux® 8.6 operating system preinstalled.

Network Configuration

The VC-4-PC-3 is configured with the following settings. Additional action may be taken where applicable.

NOTE: VC-4 is installed on a Linux server and does not have any network settings preconfigured. Any network settings must be configured manually.

- **DHCP**: A standard DHCP configuration is provided.
- **Wi-Fi® Communications**: Wi-Fi communications are disabled in the computer's BIOS.
- **Hardening**: The VC-4-PC-3 is hardened out of the box to the specifications described in Harden the Crestron Virtual Control Software on page 14.
- **File Sharing**: File sharing is turned off.
- **Unneeded Ports**: Any ports besides those listed in Network Port List on page 8 may be blocked by a firewall.
- **Unneeded Applications**: All applications present on the VC-4-PC-3 are required for proper operation and should not be removed.

Third-Party Software

The following third-party software packages are included as part of the Crestron Virtual Control installation:

- openssl-devel-1:1.1.1k-7.el8_6.i686
- libatomic-8.5.*.i686
- libcurl-7.61.1-22.el8_6.3.i686
- net-snmp-agent-libs-1:5.8-25.el8.i686
- redis-5.0.3-2.module_el8.2.0+318+3d7e67ea.x86_64

- net-snmp-libs-1:5.8-25.el8.i686
- libstdc++
- make
- gcc
- yum
- unzip
- zip
- tar
- telnet
- glibc-devel.i686
- rsync
- policycoreutils-python-utils
- glibc-devel
- libstdc++.i686
- yajl.i686
- libcurl.i686
- libuuid.i686
- libevent-devel-2.1.8-5.el8.i686
- mariadb-server
- httpd
- mod_security
- net-tools
- net-snmp
- net-snmp-utils
- krb5-workstation
- krb5-libs
- openldap-clients-2.4.46-11.el8_1.x86_64
- python3-virtualenv
- libcgroup-tools
- libxml2
- libxml2.i686
- xerces-c.x86_64
- python38

Licensing

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

- For online licensing, Crestron Virtual Control must be connected to the XiO Cloud service. For more information on the security features provided by the XiO Cloud service, refer to the XiO Cloud Service Security Reference Guide.
- For offline licensing, Crestron Virtual Control must be connected to the USB-OFFLINE dongle. A Statement of Volatility is available for the USB-OFFLINE.

Network Port List

Crestron Virtual Control 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	Direction	Protocol	Notes
80 / 443	HTTP/HTTP(S)	Inbound	TCP	Local web server used to administer Crestron Virtual Control
161 / 163	SNMP	Inbound	UDP	Simple network management protocol listening port
443	XiO Cloud® service	Outbound	TCP	AMQP over WebSockets and HTTPS
843	Flash® policy server	Inbound	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 16.
9090	Cockpit graphical interface	Inbound	TCP	This port is opened for the VC-4-PC-3 only
41794	CIP communication	Inbound/Outbound	UDP/TCP	Crestron device communication port
41796	Secure CIP communication	Inbound/Outbound	TCP	Crestron device secure communication port
47808	BACnet/IP	Inbound	UDP	BACnet Building Automation and Control networks
49200	HTML5 Web XPanel	Inbound	TCP	For more information on setting up secure communications for the HTML5 Web XPanel, refer to Configure HTML5 UI Authentication with PAM on page 21.

Opened Internal Server Ports

Port Number	Service	Protocol	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 16.
3306	MySQL	TCP	General purpose access is blocked.
5000	WebApp listening messages	UDP	WebApp is the Crestron Virtual Control interface into the web server.
6980	Redis	TCP	Port can be user defined during installation
50051	DBApp listening messages	UDP	DBApp is the Crestron Virtual Control interface into the MariaDB database.

NOTE: A custom program running on Crestron Virtual Control may use additional ports that must be opened manually.

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® Service
- SNTP (Simple Network Time Protocol)

Security Controls

The following security controls are applicable to Crestron Virtual Control.

Role-Based Access Control

Use the principle of least privilege (POLP) when establishing access control for user accounts.

Audit Logging

Standard Linux security logging and auditing is used. Crestron applications write all security events to text based log files on the system that can be manually audited by administrators.

Data Transmission

When VC-4 is connected to XiO Cloud, the only data sent to the cloud from the VC-4 server is licensing information, Ethernet settings, and the device hostname.

All user programs, including any data they contain, are not distributed outside of the VC-4 server. No user information is disclosed to the cloud.

Security Best Practices

For optimal security while operating Crestron Virtual Control, observe the following best practices:

- Do not access the internet using a web browser on the device.
- Do not directly expose the device to the internet.
- Never install unapproved software.
- Use the system only for its intended purpose.
- Ensure all password created on the Linux OS meet the following criteria:

  > **NOTE:** Any password rules are enforced through the Linux OS and not through Crestron Virtual Control.

  - Minimum length of 7 characters
  - Passwords changed every 90 days
  - 30-minute lockout after 5 failed attempts in 2 minutes

More Security Information

For more information regarding security practices for Crestron devices, visit the Crestron security web page.

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:

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/overview-of-security-hardening-security-hardening.
- 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.

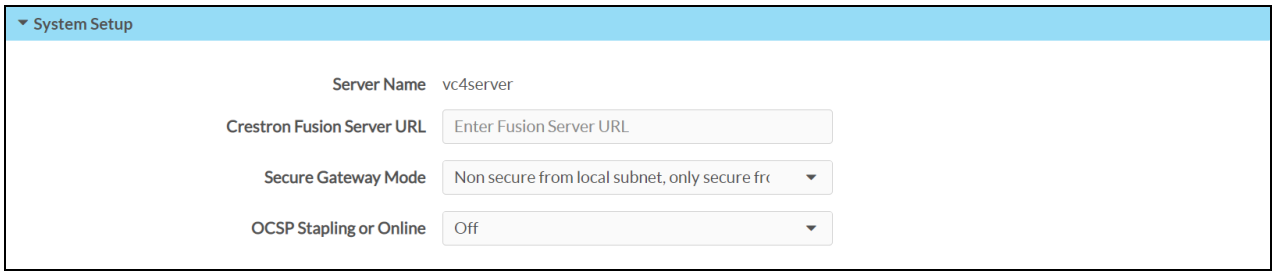
Configure Secure Device Connections

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.

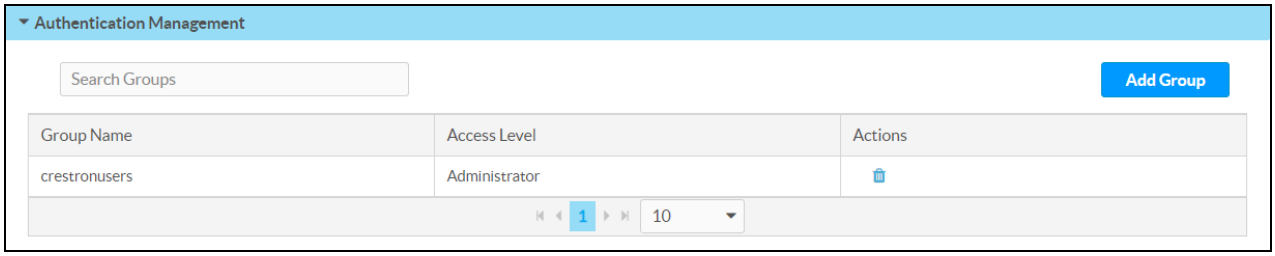
   > **NOTE:** If the **Secure Gateway Mode** is changed to **Only secure** while a non-secure device connection is active, including a connection to the web XPanel interface, the non-secure connection is not terminated automatically.

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.

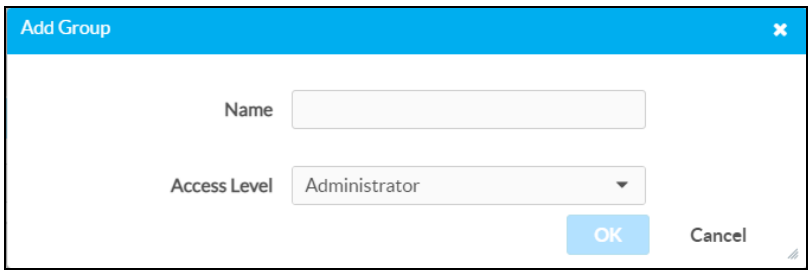
2. With the Crestron Virtual Control service running, navigate to **Settings** > **Authentication Management** in the web user interface.

   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 15.
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.

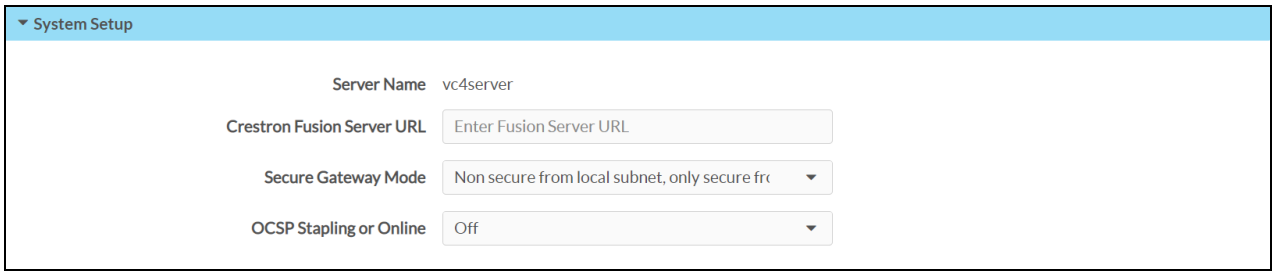
Configure OCSP Client Settings

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 Crestron Virtual Control Product Manual.

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
```

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

Security Reference Guide — Doc. 9396B
06/30/23
Specifications subject to
change without notice.