Crestron Virtual Control Server-Based Control System

Deployment Guide

Crestron Electronics, Inc.

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

Contents

Crestron Virtual Control: Server-Based Control System

Introduction

The Crestron Virtual Control server-based control system provides a scalable solution for deploying programs, rooms, and devices across an enterprise. The control system infrastructure resides entirely on a remote Crestron Virtual Control server, which is installed and configured using supported Linux® operating system platforms.

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

For more information on installing the Crestron Virtual Control service on the Linux platform, refer to the Crestron Virtual Control Installation Guide (Doc. 8274) at www.crestron.com/manuals.

For more information on integrating the Crestron Virtual Control server in an existing intranet site using the secure Crestron Virtual Control REST API platform, refer to the Crestron Virtual Control REST API Programming Guide (Doc. 8316) at www.creston.com/manuals.

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 Ubuntu® software, refer to https://help.ubuntu.com/community/Security.
- To harden the Apache web server, refer to https://httpd.apache.org/docs/2.4/misc/security_tips.html.

Harden the Crestron Virtual Control Server

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

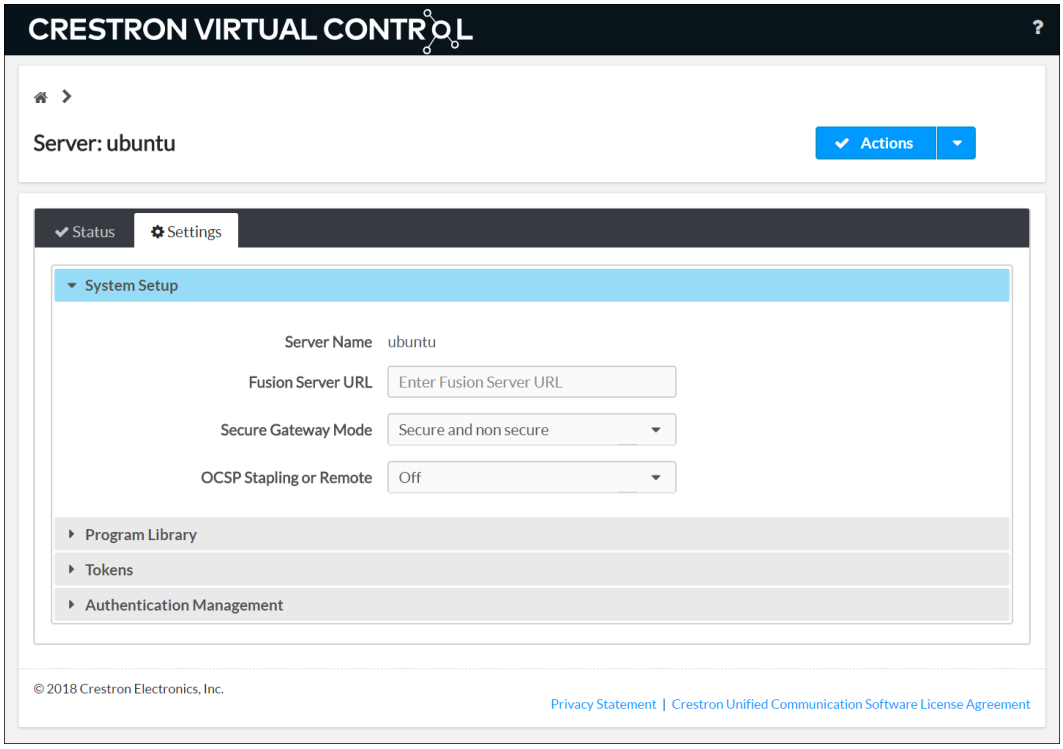
Configure Secure Device Connections

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:

   a. **Only secure**: Only secure device connections are accepted by the server.

   b. **Secure and non secure**: Both secure and non-secure device connections are accepted by the server.

   c. **Non secure from local subnet, only secure from remote subnets:** Non-secure 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.

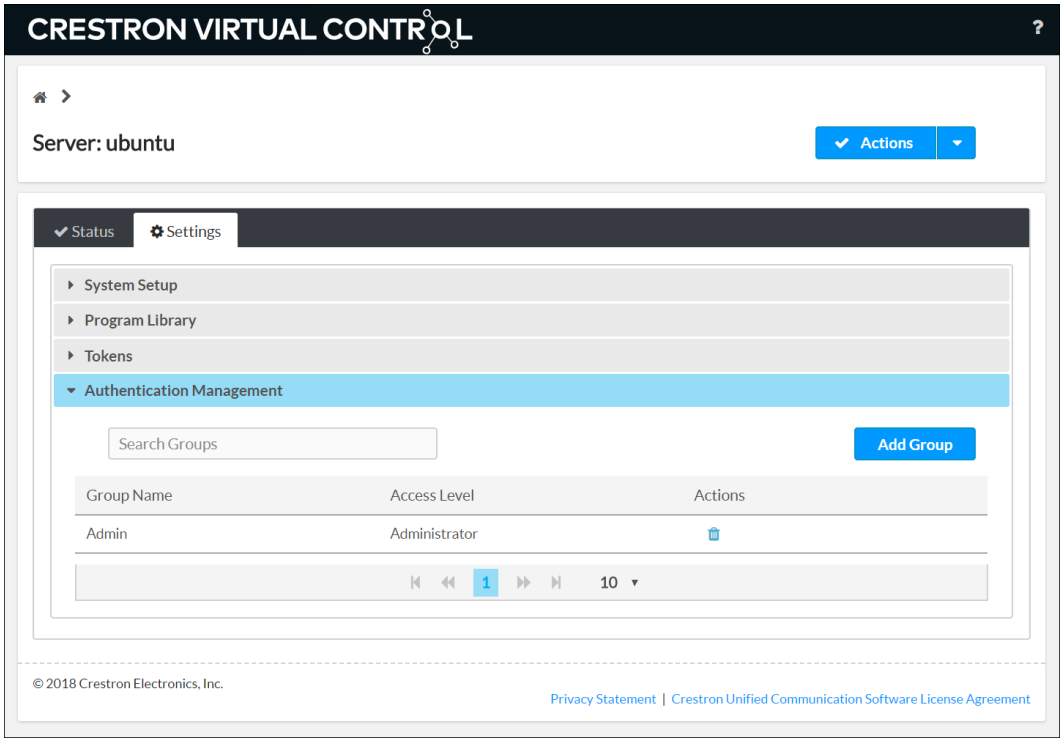
NOTE: If the **Secure Gateway Mode** is changed to **Only secure** while a non-secure device connection is active, including a connection to the web XPanel interface, the non-secure connection is not terminated automatically.

To enable 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



Load SSL Server Certificates

The Crestron Virtual Control server provides built-in support for Secure Sockets Layer (SSL). SSL ensures that the connection between the web browser and the Crestron Virtual Control server is secure via encryption.

NOTE: For more information on configuring SSL on a Crestron control system, refer to the 3-Series® Control Systems Reference Guide (Doc. 7150) at www.crestron.com/manuals.

Prior to configuring SSL for the Crestron Virtual Control server, an SSL 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
- Have a .pem file extension for the SSL server certificate, and a .pem or .key file extension for the private key
- Not be encrypted
- Contain no spaces in the file names

Once the SSL 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 SSL connections. For more information, refer to "HTTPS Configuration" at https://help.ubuntu.com/lts/serverguide/httpd.html.

1. Copy the SSL 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 [VirtualControlHome]/samples/conf_files, where "VirtualControlHome" is the directory set during the Virtual Control installation. The default directory is /opt/crestron/virtualcontrol/.
3. Copy the ssl.conf file to the [VirtualControlHome]/conf directory.
4. Open the ssl.conf file in a text editor application:
    a. Type "[Filepath]/[SSLCertificateFile]" on the first line, where "Filepath" is the file path of the SSL server certificate file and "SSLCertificateFile" is the name of the certificate file (e.g., /home/builduser/crestron/[certificate-name].pem).
    b. Type "[Filepath]/[SSLPrivateKeyFile]" on the second line, where "Filepath" is the file path of the private key file and "SSLPrivateKeyFile" 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.

5. Launch the Crestron Virtual Control service. Any changes to SSL take effect immediately.

   NOTE: Observe the following points about SSL.

   - SSL 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 SSL certificates and keys, open a packet analyzer software (such as Wireshark), and listen on port 41796. The "certificate" argument should show in the public key details.

Configure Secure Flash® Technology 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 SSL server certificate pair for the Flash policy server. For more information on creating and loading SSL certificates, refer to "Load SSL Server Certificates" on page 5.
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 reboots.

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.

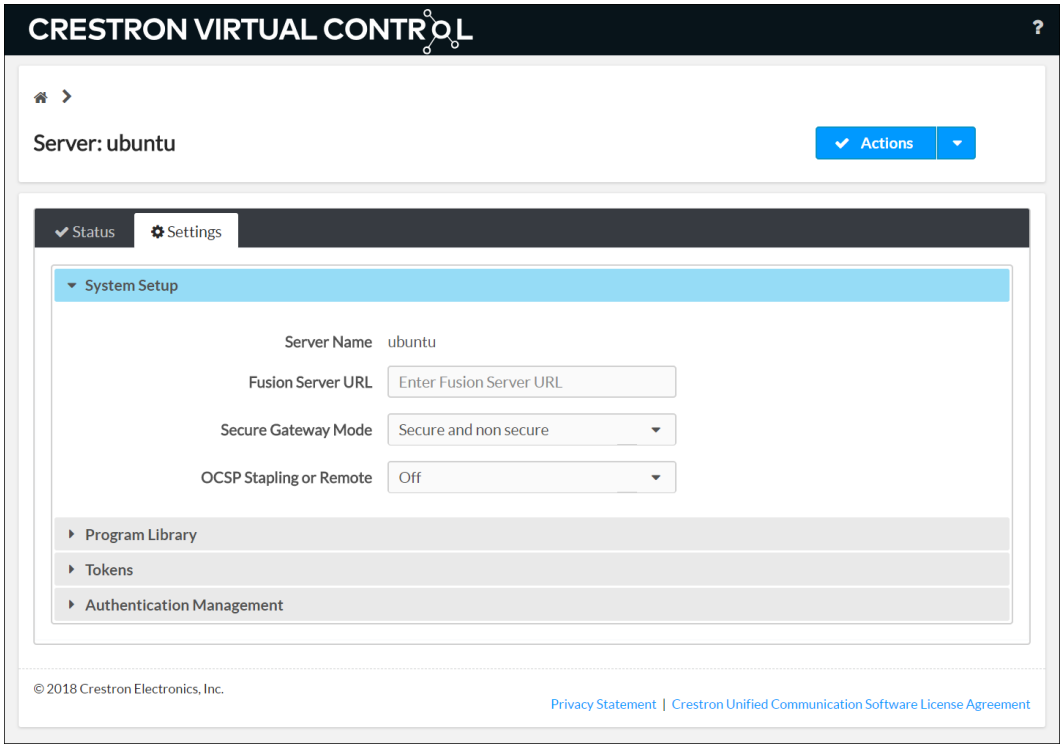
Configure OCSP Client Settings

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 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:

   a. **Off**: Turns OSCP off

   b. **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.)

   c. **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 Access to Web Interface

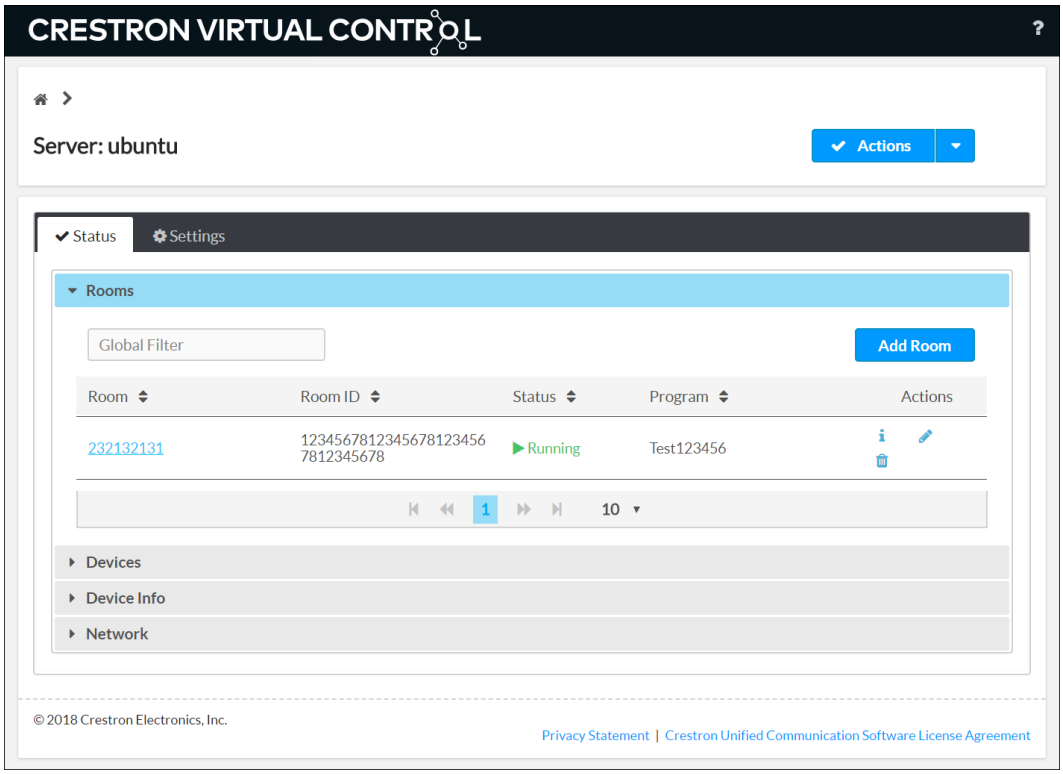
The Crestron Virtual Control server may be monitored and configured using the included web configuration interface. The web interface also provides selections for viewing and configuring rooms, programs, and connected devices.

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 administrator (read/write) access, enter "https://[ServerURL]/VirtualControl/config/settings" into a supported web browser, where [ServerURL] is the URL or hostname of the Linux server running the Crestron Virtual Control service.

  The Crestron Virtual Control web interface displays with the **Status** > **Rooms** page open by default.

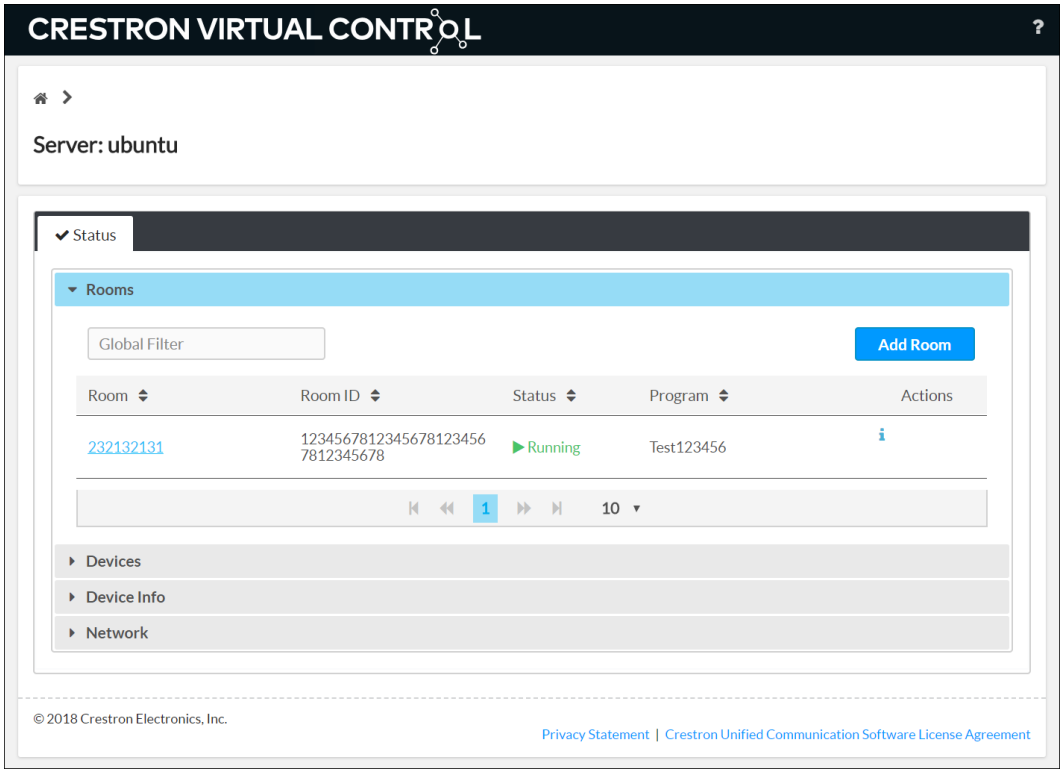
  ### Settings Web Interface Screen



- For user/operator (read-only) access, enter "https://[ServerURL]/VirtualControl/config/status" into a supported web browser, where [ServerURL] is the URL or hostname of the Linux server running the Crestron Virtual Control service.

The Crestron Virtual Control web interface displays with the **Status** > **Rooms** page open by default. The **Settings** tab and the **Action** menu are not provided in the status pages. Additionally, rooms and programs may not be added or modified.

Status Page



Web Interface Authentication with PAM

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 Apache server, users must be authenticated before access to the web interface is granted.

For more information, refer to https://www.adelton.com/apache/mod_authnz_pam/.

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

To enable PAM on the Apache server:

1. Install the required packages on the Linux server where the Crestron Virtual Control service is installed by issuing the following commands:

```
sudo apt-get install libapache2-mod-authnz-external pwauth

sudo apt-get install libapache2-mod-authz-unixgroup

sudo a2enmod authnz_external authz_unixgroup
```

2. Navigate to the /etc/apache2/sites-available directory.
3. Open the crestron.conf file in a text editor application. Administrative privileges are required to edit the file.
4. Add the following user authentication text to the file:

```
###############User Authentication changes ####################
<IfModule mod_authnz_external.c>
AddExternalAuth pwauth /usr/sbin/pwauth
SetExternalAuthMethod pwauth pipe

AddExternalGroup unixgroup /usr/sbin/unixgroup
SetExternalGroupMethod unixgroup environment
</IfModule>

<Location ${CRESTRON_VC_4_WEBROOT}/config/settings/WebApi/>
AuthType Basic
AuthName "Restricted Area"
AuthBasicProvider external
AuthExternal pwauth
Require user [user]
</Location>

<Location ${CRESTRON_VC_4_WEBROOT}/config/status/WebApi/>
AuthType Basic
AuthName "Restricted Area"
AuthBasicProvider external
AuthExternal pwauth
Require user [user]


#GroupExternal unixgroup
</Location>

#############################################################
########
```

5. Replace [user] with the username that will be granted access to the web interface.
6. Save and exit the file.
7. Restart the Apache services by issuing the `sudo service apache2 restart` command.

Configuration and XPanel Interface 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]/Html
AuthType Basic
AuthName "Restricted Area"
AuthBasicProvider external
AuthExternal pwauth
Require user [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
AuthType Basic
AuthName "Restricted Area"
AuthBasicProvider external
AuthExternal pwauth
Require user [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**.

This page is intentionally left blank.

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

Deployment Guide – DOC. 8272A
(2050943)
07.18