

## **Crestron Residential Systems**

Security Reference Guide

Crestron Electronics, Inc.

The original language version of this document is U.S. English. All other languages are a translation of the original document.

#### Regulatory Model: [[[Undefined variable TP-Variables.RegulatoryModel]]]

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 <a href="https://www.crestron.com/legal/software\_license\_agreement">www.crestron.com/legal/software\_license\_agreement</a>.

The product warranty can be found at www.crestron.com/warranty.

The specific patents that cover Crestron products are listed online at www.crestron.com/legal/patents.

Certain Crestron products contain open source software. For specific information, please visit www.crestron.com/opensource.

Crestron, the Crestron logo, 3-Series, 4-Series, Crestron Home, Crestron Pyng, and Crestron Toolbox are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. iPad is either a trademark or registered trademark of Apple, Inc. 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.

©2023 Crestron Electronics, Inc.

## Contents

Introduction	5
Secure a 3-Series® Control System	6
Verify the Firmware Version	6
Create an Administrator Account	
Add a User for SSL	
Enable SSL on the Crestron Mobile App	11
Secure a Crestron Home OS System	
Crestron Home OS Security Features	14
Enable a Remote Connection	14
Secure a Crestron Pyng OS System	
Enable Remote Access	

# Introduction

Crestron<sup>®</sup> systems should be secured against potential security risks. Crestron security results in a safe, stable system, protected from unauthorized access, but only when the proper guidelines are followed. This guide can help ensure your customers' sites are safe.

This document describes how to secure a Crestron residential installation for the following platforms:

- 3-Series<sup>®</sup> control system platform (version 1.601 or later)
- Crestron Home® OS platform (all released versions)
- Crestron Pyng<sup>®</sup> OS platforms (all released versions)

**NOTE:** 4-Series<sup>®</sup> control systems ship with authentication enabled by default and do not require any end user setup. Users are prompted to create an admin account username and password upon connecting to the device for the first time using a web browser or Crestron Toolbox<sup>™</sup> software.

The following resources may also be referenced:

- For detailed information about security features, see the Crestron Security website (https://www.crestron.com/en-US/Security/Security-at-Crestron).
- For information about the MyCrestron Dynamic DNS Service, visit
   <u>https://www.crestron.com/en-US/Support/Tools/Applications/MyCrestron-Dynamic-DNS-Service</u>.
- For information about MyCrestron Residential Monitoring services, visit
   <u>https://www.crestron.com/en-US/Support/Tools/Applications/MyCrestron-Residential-</u>
   <u>Monitoring-Service.</u>

# Secure a 3-Series® Control System

Use the following procedures to secure a 3-Series control system with Crestron Toolbox software.

**NOTE:** For more information on configuring authentication and security settings for a 3-Series control system, refer to the 3-Series Control System Reference Guide.

## **Verify the Firmware Version**

To verify the firmware version of the 3-Series control system:

- 1. Open Crestron Toolbox™ software.
- 2. Navigate to Tools > EasyConfig. The EasyConfig tool is displayed.
- 3. Click the pencil icon at the bottom of the **EasyConfig** tool. A dialog box for editing the connection type is displayed.

### **Connection Type Dialog Box**

		? X
Connection Type:		
TCP	O USB	Indirect
IP Address / Hostname:	172.30.16>	ox <b>v</b>
	SSH	•
< Advanced		
Port (if not default):		
Username:		
Password:		
	🔲 Use Sec	condary Console
Control Subnet		
Hostname:		
Port (if not default):		
	Auto Deteo	t 🔹
< Advanced Device Dete	ction	
Auto-De	etect	-
Address Book	ОК	Cancel

- 4. Select the **TCP** button under **Connection Type**.
- 5. Enter the control system IP address or hostname in the IP Address / Hostname field.

6. Select **SSH** from the drop-down menu under the **IP Address / Hostname** field.

NOTE: SSH uses port 22 by default.

- 7. Configure any additional TCP connection settings as needed.
- 8. Click **OK**. The **EasyConfig** tool is displayed with information about the 3-Series control system.

Easy	Config Tool				
	PRC Versic Serial Author	0 <b>3</b> on: 1.601.3833.16471 Number: 13424668 ntication: Not enabled			
	Network Device Tree	Launch the tool to view ar	nd configure connected devices		
	SIMPL Debugger	Launch the tool to test and	d debug control system programs		
	Firmware	Version:	1.601.3833.16471		
011	Program (Program01)	Program ID Tag: Program Name: Timestamp: Original Path:	SN:		
IP	IP Table (Program01)	Active IP Entries: Total IP Entries:	0 2		
D	Web Projects	Project Name	Туре	Location	
	Ethernet Settings	IP Address: IP Mask: Mac Address:	Host Name: DHCP Enabled: Ye Link Status: Ac	s tive	
	Clock	Device Time: Processor TimeZone:	9/4/2019 06:53:33 Pacific Standard Time ((UTC-08:00) Pac	ific Time (US & Canada))	

9. Verify that the firmware version (listed next to **Version** at the top of the tool) is at least 1.601. For the latest security patches, apply the latest firmware available.

## **Create an Administrator Account**

System UpTime: 34 Days, 0 Hour, 28 Minutes, 48 Se

**NOTE:** If authentication is already enabled on the control system, an administrator account already exists and this procedure is not required. An administrator user name and password is required to access the device in Crestron Toolbox.

The first step in securing the processor is the creation of an administrator account. To create an administrator account:

- 1. In Crestron Toolbox, open the **EasyConfig** tool for the 3-Series control system by following steps 1–8 of Verify the Firmware Version on page 6.
- 2. Navigate to **Functions** > **Authentication**. A dialog box for configuring authentication settings is displayed.

#### Authentication Dialog Box



3. Click the checkbox next to Authentication Enabled.

If authentication is enabled for the first time on the 3-Series control system, a dialog box for creating an administrator account is displayed.

The device currently does not have an account with administrative privileges which is required to turn on Authentication. Please enter a username and password which will be used to create an administrative account				
Username				
Password				
Verify Password				
	OK Cancel			

#### **Create Administrator Account Dialog Box**

- 4. Enter a user name in the **Username** field.
- 5. Enter a password in the **Password** field. The password rules are as follows:
  - The password length must be between 8 and 13 characters.
  - The password must contain at least one of each of the following:
    - Uppercase letter
    - Lowercase letter
    - Numeric digit
    - Special character: ` ~ ! @ \$ % ^ & \* ( ) \_ + = { } [ ] | ; " < > , .
- 6. Enter the password created in step 5 in the Verify Password field.

7. Click **OK**. The 3-Series control system reboots automatically, and the new settings take effect following the reboot.

**NOTE:** After multiple incorrect login attempts (the default is 3), the control system locks out any additional login attempts from the same IP address for a 24-hour period. Any incorrect login attempt over a USB connection is blocked for 5 minutes. For more information, see the Crestron Secure Deployment Guide at <a href="https://www.crestron.com/en-US/Security/Security-at-Crestron">www.crestron.com/en-US/Security/Security-at-Crestron</a>.

# Add a User for SSL

Once authentication is enabled, the administrator may create new users and groups, add users to groups, set permissions, and change user passwords.

It is highly recommended that at least one additional account is created and added to the Users group. This account should be used in the SSL settings of the mobile applications. For more information, refer to the following sections.

To create a new user:

 Access the authentication dialog as described in Create an Administrator Account on page 7.

nencoser obe	- oroups	DIOCKED IPS	Authentication Op	uons
Jsername	Is Activ	e Director	Public Key	Is Blocked
admin	Ne			2000
	NO		No	No
Chappe Liser Pro	Double-C	lick on a user	No for additional infor	mation

2. In the Authentication window, click Create New User.

3. In the **Create New User...** dialog box, enter the user information in the **Username for new user**, **Password for new user**, and **Verify Password** text boxes.

Username for new user: Password for new user: Verify Password:	
Groups To Join	11
Group	Access Level
ADMINISTRATORS PROGRAMMERS OPERATORS USERS CONNECTS	ADMINISTRATOR PROGRAMMER OPERATOR USER CONNECTION
(CTRL + Click to	o select multiple Groups)

- 4. In the **Groups to Join** box, click the **USERS** group to assign the new user to it. The user inherits the groups's access level/rights. Use **Ctrl+click** to assign the new user to multiple groups.
- 5. Click OK.

# Enable SSL on the Crestron Mobile App

NOTE: This is not required with Crestron Home® OS or Pyng® OS.

The Crestron Mobile App icon is shown below.



Once authentication is enabled on the control processor, SSL must be enabled on the Crestron mobile app in order for it to properly connect to the system. To enable SSL on the Crestron mobile app for Crestron control systems:

1. From Crestron Toolbox, click the pencil icon in a supported tool (such as **EasyConfig**) to access the control system connection settings for use later in this procedure.

2. From the Crestron App, tap the pencil icon at the bottom of the screen.

### **Connection List**



3. Select the control system connection.

### The **Edit Location** dialog box is displayed.

### Edit Location Dialog Box

3:09 PM Fri Mar 6		<b>ull 🗢 90% 🔲</b> )
Back	Edit Location	Save
Address 1 (Typically Local LAN)		
Friendly Name / Location		PRO3-IH1
Use Local Project		OFF
Host name or IP Address		172.30.16.186
HTTP Port		80
IP ID		03
CIP		41794
Address 2 (Typically Internet/Mobile)		
Host name or IP Address		
HTTP Port		80
CIP		41794
Enabled		OFF
Enable SSL		OFF
User Name		
Password		
Confirm Password		
Watch / Widget		OFF

- 4. Tap the switch next to **Enable SSL** to set it to **ON**.
- 5. Change the HTTP port for Addresses 1 and 2 from 80 to 443 and the CIP port from 41794 to 41796.
- 6. Enter the SSL User account username and password created for the control system in the **User Name** and **Password** fields, respectively.
- 7. Enter the SSL User account password again in the **Confirm Password** field.
- 8. Click **Save**. SSL is enabled immediately.

# Secure a Crestron Home OS System

The following sections describe how to secure a Crestron Home OS system.

## **Crestron Home OS Security Features**

New Crestron Home OS systems running on the CP4-R or MC4-R are secured by factory default:

- Creston Home OS enables authentication and SSL by default on the CP4-R and MC4-R. SSL is also enabled by default on the Crestron Home app.
- Crestron Home OS uses self-signed certificates.
- Upgrading to Crestron Home OS from Crestron Pyng® OS 2 secures the system automatically during the upgrade:
  - If the CP4-R running Crestron Pyng OS 2 is secured and then upgraded to Crestron Home OS, the credentials are migrated during the upgrade.
  - If the CP4-R running Crestron Pyng OS 2 is not secured and then upgraded to Crestron Home OS, the username is set to "admin" and the password is set to the serial number of the CP4-R or MC4-R (case-sensitive). For more information, refer to the <u>Crestron Home OS Product Manual</u>.

## **Enable a Remote Connection**

To enable connection from outside the home, the following ports must be opened on a router for external control of the Crestron Home and Crestron Home Setup apps.

**NOTE:** Only open ports are required for the necessary functions. Crestron recommends port remapping for enhanced security. For more information on mapping, see Enable Remote Access on page 23.

- To enable end-user access, open port 50001.
- To enable dealer access, open ports 443, 843, and 41796.

**NOTE:** Remote use of XPanel via a web browser is NOT recommended as it does not meet Crestron's minimum security standards. Instead, Crestron recommends using the Crestron Home Setup app on an iPad<sup>®</sup> tablet.

# Secure a Crestron Pyng OS System

The following sections describe how to secure a Crestron Pyng system running on the PYNG-HUB (Crestron Pyng OS 1) and the CP4-R or MC4-R (Crestron Pyng OS 2).

**NOTE:** New Crestron Home systems running on the CP4-R are secured by factory default. Upgrading to Crestron Home from Crestron Pyng OS 2 also secures the system automatically during the upgrade. The procedures in this section are for legacy Crestron Pyng applications.

To secure a Crestron Pyng system:

1. Open the Crestron Pyng application. The **Home** screen is displayed.



Home Screen (Crestron Pyng OS 2)

2. Select **Settings** from the collapsible side menu.

3. Enter the installer password when prompted, and then tap **OK**. The main **Setup** screen is displayed.

Setup Follow the five steps to setup O Tap the help button located in	irestron Pyng. the bottom right corner for	more information at any tim	ıe.	руng
Step 1	Step 2	Step 3	Step 4	Step 5
				1 🕸 🤉

Setup Screen (Crestron Pyng OS 2)

4. Tap the gear button 💮 to display the Installer Settings screen. Installer Settings Screen (Crestron Pyng OS 2)

Installe	er Settings		pyng
		Select Setting	
	System Configuration	Configure System Level Settings	
	Diagnostics	Diagnose System	
	System Control Options	Setup Control Options for System	
	Privacy Controls	Access Privacy Policies and Options	
	Check For Updates	Update System	
			-
			<⇒ (?)

- 5. Navigate to the **Ethernet Settings** screen.
  - For a Crestron Pyng OS 1 system, tap **Ethernet Settings**.



Installer Settings Screen (Crestron Pyng OS 1)

• For a Crestron Pyng OS 2 system, tap **System Configuration** and then tap **Ethernet Settings**.



Installer Settings - System Configuration Screen (Crestron Pyng OS 2)

The **Ethernet Settings** screen is displayed.

Ethernet	Settinas	Screen
E 011011100	occango	0010011

Ethernet	Settings			pyng
Ci	urrent Settings		Settings	
DHCP	On	рнс	P off	On
Host Name:	PYNGVELAB	Host Nam	e: PYNGVELAB	
Domain:	CRESTRON.CRESTRON.COM	Domai	CRESTRON.CRESTRON.CO	м
IP Address	172.30.16.0	IP Addres	: 172.30.16.0	
Subnet Mask:	255.255.255.0	Subnet Masl	255.255.255.0	
Default Router:	172.30.16.1	Default Route	: 172.30.16.1	
MAC Address:	de:ad:be:ef:be:ef		Apply	
		Advanced Settings		<⊳?

6. Tap **Advanced Settings** at the bottom of the screen to display the **Advanced Ethernet Settings** screen.

Advanced	Ethernet S	Settings			p	ÿ'nç	J
Curi	rent Settings		Se	ettings			
192.168.200.133 (DH	DNS Servers +	Authentica	ition:	Cff	On		
192.168.200.134 (DH	(CP)	CIP	Port: 41	1794			
		Secure CIP	Port: 41	1796			
CIP Port:	41794	CTP	Port: 41	1795			
Secure CIP Port:	41796	Secure CTP	Port: 41	1797			
CTP Port:	41795	Web	Port: 80	D			
Secure CTP Port:	41/9/	Secure Web	Port: 4	43			
Web Port:	80						
Secure Web Port:	443			Apply			
		Basic Settings			<	h (	D

Advanced Ethernet Settings Screen

7. Tap **On** next to **Authentication** to enable authentication. The **Enable Authentication** dialog box is displayed.

Enable Auth	nentication
Username:	
Password:	
Re-enter Password	
Clicking 'OK' with valid userr enable authentication. 1	name & password input will The system will reboot.
ок	Cancel

Enable Authentication Dialog Box

- 8. Enter a user name in the **Username** field.
- 9. Enter a password in the **Password** field. The password rules are as follows:
  - The password length must be between 8 and 13 characters.
  - The password must contain at least one of each of the following:
    - Uppercase letter
    - ° Lowercase letter
    - Numeric digit
    - Special character: ` ~ ! @ \$ % ^ & \* ( ) \_ + = { } [ ] | ; " < > , .
- 10. Enter the password created in step 9 in the **Re-enter Password** field.

11. Tap **OK**. The **Enable Authentication Confirmation** dialog box is displayed.

Enable Authentication Confirmation Dialog Box

Enable Authentication Confirmation	
<ul> <li>Warnings: <ol> <li>In order to enable authentication the system must be restarted (The system will take several minutes to restart).</li> <li>You must remember your Username &amp; Password. You will not be able to reconnect to the system without them.</li> </ol> </li> <li>In order connect to the system after authentication has been enabled, the following steps must be followed: <ol> <li>Navigate to the Settings menu of the Crestron Pyng application on your iPad</li> <li>Click the pencil icon and then click on the item used to connect to your Pyng hub</li> <li>Turn 'Enable SSL' ON</li> <li>Enter your Username &amp; Password</li> <li>Select Save</li> <li>Click on the item used to connect to your Pyng hub</li> </ol> </li> </ul>	
OK Cancel	
Basic Settings	<\ ?

12. Tap **OK**. A message is displayed stating that authentication is enabled, and the system reboots. The new settings take effect following the reboot.

After authentication has been enabled:

- 1. Navigate to the **Settings** menu of the Crestron Pyng application on your iPad.
- 2. Tap the pencil icon at the bottom of the screen.

#### **Connection List**



3. Select the control system connection.

The **Edit Location** dialog box is displayed.

Edit Location Dialog Box		
4:05 PM Mon Mar 23		중 ┦ 23% [[]
Back	Edit Location	Save
Address 1 (Typically Local LAN)		
Friendly Name / Location		crestronHome-C
Host name or IP Address		192.168.1.234
HTTP Port		443
CIP		41796
Address 2 (Typically Internet/Mobile)		
Host name or IP Address		
HTTP Port		443
CIP		41796
Enabled		OFF
Enable SSL		ON
User Name		admin
Password		password

4. Tap the switch next to **Enable SSL** to set it to **ON**.

- 5. Enter the SSL User account username and password created for the control system in the **User Name** and **Password** fields, respectively.
- 6. Tap **Save**.
- 7. Click the item used to connect to your Crestron Pyng system.

# **Enable Remote Access**

To enable remote access, the following ports must be opened on a router.

### NOTES:

- Only open ports are required for the necessary functions. Crestron recommends port remapping for enhanced security.
- Remote use of XPanel via a web browser is NOT recommended as it does not meet Crestron's minimum security standards. Instead, Crestron recommends using the Crestron Home Setup app on an iPad.

Many routers do not allow for direct port forwarding of common ports, including 80, 443, and 23. Port mapping is ideal in this scenario, as an arbitrary external port is forwarded to the internal port being used. For example, port 80 (internal) to port 80 (external) may be blocked, but mapping from port 8080 to port 80 or port 8081 to port 80 is allowed.

Port Number	Function	Notes
22	SSH	Secure Shell is a secure network protocol used for Ethernet communication over unsecured networks.
443	HTTPS	Used for Crestron mobile projects and XPanel web support. If neither of these features is in remote use, do not forward.
843	Policy Server	Used for XPanel Browser support. This feature is not recommended for remote use. Do not forward unless required.
41794	CIP	Cresnet over Internet Protocol. Used for XPanel Browser support. This feature is not recommended for remote use. Do not forward unless required.
41796	SCIP	Secure Cresnet over Internet Protocol. Used for Crestron mobile projects.

#### For 3-Series and 4-Series:

### For Crestron Home:

Port Number	Function	Notes
443	HTTPS	Used for Crestron Home Setup application and XPanel web support. If neither of these features is in remote use, do not forward.
843	Policy Server	Used for XPanel Browser support. This feature is not recommended for remote use. Do not forward unless required.
41794	CIP	Cresnet over Internet Protocol. Used for XPanel Browser support. This feature is not recommended for remote use. Do not forward unless required.
41796	SCIP	Used for Crestron Home Setup application. If the feature is not in remote use, do not forward.
50001	Crestron Home	Used by Crestron Home end-user application

### For Crestron Pyng:

Port Number	Function	Notes
443	HTTPS	Used for Crestron Pyng applications
843	Policy Server	Used for XPanel Browser support. This feature is not recommended for remote use. Do not forward unless required.
41794	CIP	Cresnet over Internet Protocol. Used for XPanel Browser support. This feature is not recommended for remote use. Do not forward unless required.
41796	SCIP	Secure Cresnet over Internet Protocol. Used for Crestron Pyng Applications

Do the following to enable remote system access for your customers:

- Change the external ports so they are not the same as the internal ports. Remapping the external ports minimizes the number of attempts to access the system. A hacker will be unable to scan well-known ports for entry and must instead scan all ports and then determine what protocols are supported before attempting to log in to the system.
- Most home routers allow different external and internal ports to be set. An example of a home router setup page is provided below.

Sillyle Port Forwar	uniy					
Application Name		External Port	Internal Port	Protocol	To IP Address	Enabled
None	¥				192 . 168 . 194. 0	
None	¥				192 . 168 . 194. 0	
None	¥				192 . 168 . 194. 0	
None	¥				192 . 168 . 194. 0	
None	¥				192 . 168 . 194. 0	
CIP		9699	41796	TCP 🗸	192 . 168 . 194. 99	✓
SSH		2299	22	TCP 🗸	192 . 168 . 194. 99	✓
eControl		4499	443	TCP 🗸	192 . 168 . 194. 99	•
Policy File		843	843	TCP 🗸	192 . 168 . 194. 99	~

#### Home Router Setup Page Example

Single Dort Converding

- Use external port numbers that are not commonly used. The actual number is not important; it simply must match the entry in the mobile app configuration.
- To enable XPanel web support, the **Internal Port** and **External Port** must be set to 843.
- Open only ports that are required. For example, if mobile applications or XPanel applications are used, open only the secure CIP port (default is 41796) and HTTPS port (default is 443). Ensure that SSL settings are used in the mobile application.
- If XPanel browser support is required, the unsecured CIP port (default is 41794) must be used. The system is still secured because the user is prompted to enter their credentials prior to running the project. The XPanel browser requires port 843 to be routed to the system.
- If ports 41795 or 41797 were opened for external use, reroute the external ports to port 22 and use the SSH console.

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