# Security for Crestron Residential Systems

## Setup & Configuration

Crestron Electronics, Inc.

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

# Contents

# Security for Crestron Residential Systems

## Introduction

Crestron® systems that use port forwarding to enable external access (for mobile or browser applications) may be exposed to potential security risks. To reduce these risks, it is highly recommended that Crestron residential systems be secured using the procedures provided in this document.

**NOTE:** This document assumes that the user is familiar with operating Crestron Toolbox™ software.

Systems that use Virtual Private Networks (VPNs) for external access should also implement the security measures provided in this document to prevent unauthorized access from within the network.

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

- 2-Series control system platform (version 4.007.004 or higher)
- 3-Series® control system platform (version 1.11 or higher)
- Crestron Home™ OS 3 platform (all released versions)
- Crestron Pyng® OS 1 and OS 2 platforms (all released versions)

The following resources may also be referenced:

- For detailed information about security features, refer to the Crestron Security website at https://www.crestron.com/en-US/Security/Security-at-Crestron.
- For information about the myCrestron Dynamic DNS Service, visit https://www.crestron.com/en-US/Support/Tools/Applications/MyCrestron-Dynamic-DNS-Service.
- For information about myCrestron Residential Monitoring services, visit https://www.crestron.com/en-US/Support/Tools/Applications/MyCrestron-Residential-Monitoring-Service.

# Secure a 2-Series Control System

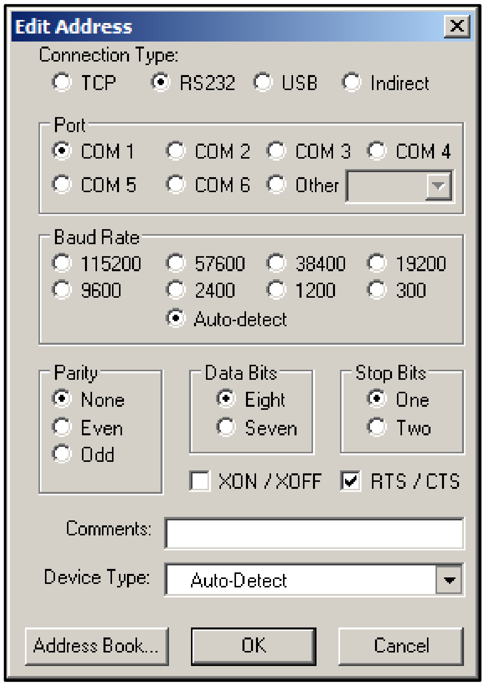
Use the following procedures to secure a 2-Series control system with Crestron Toolbox software.

## Verify the Firmware Version

To verify the firmware version of the 2-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.

Edit Address Dialog Box



Edit Address

Connection Type:
○ TCP ● RS232 ○ USB ○ Indirect

Port
● COM 1 ○ COM 2 ○ COM 3 ○ COM 4
○ COM 5 ○ COM 6 ○ Other

Baud Rate
○ 115200 ○ 57600 ○ 38400 ○ 19200
○ 9600 ○ 2400 ○ 1200 ○ 300
● Auto-detect

Parity
● None
○ Even
○ Odd

Data Bits
● Eight
○ Seven

Stop Bits
● One
○ Two

☐ XON / XOFF ☑ RTS / CTS

Comments:

Device Type: Auto-Detect

4. Select the **RS232** button under **Connection Type**.
5. Configure any RS-232 connection settings as needed.
6. Click **OK**. The **EasyConfig** tool is displayed with information about the 2-Series control system.
7. Verify that the firmware version (listed next to **Version** at the top of the tool) is 4.007.004 or higher. Update the device firmware to the required version if necessary.

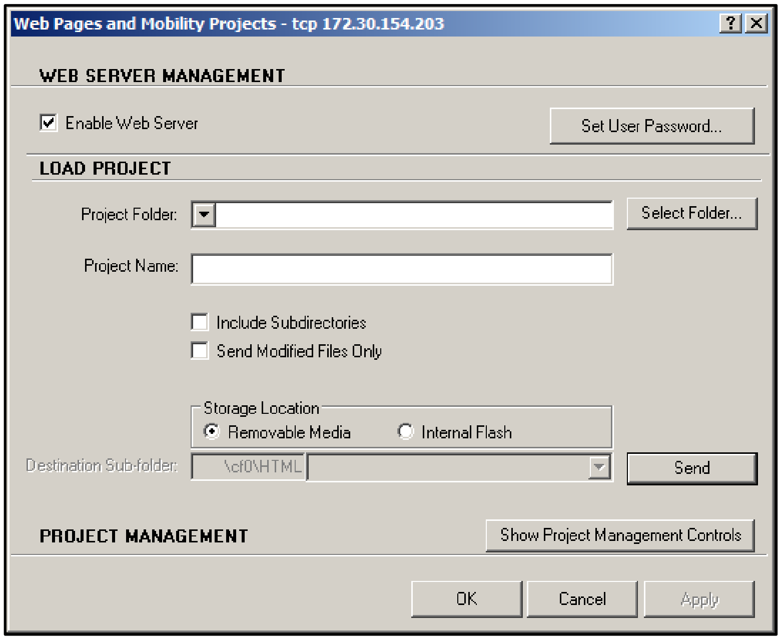
## Set a Web Server Password

To set a user password for the 2-Series control system web server:

1. Open the **EasyConfig** tool for the 2-Series control system by following steps 1–5 of Verify the Firmware Version on page 2.

2. Navigate to **Functions** > **Web Pages and Mobility Projects**. The **Web Pages and Mobility Projects** dialog box is displayed.

### Web Pages and Mobility Projects Dialog Box



Web Pages and Mobility Projects - tcp 172.30.154.203

WEB SERVER MANAGEMENT

☑ Enable Web Server

LOAD PROJECT

Project Folder:

Project Name:

□ Include Subdirectories

□ Send Modified Files Only

Storage Location

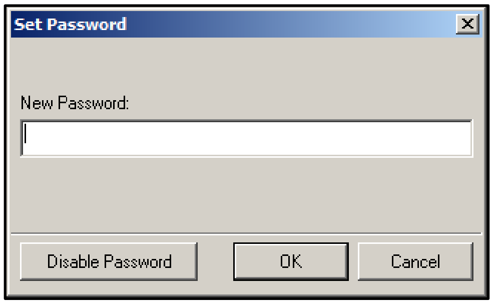
● Removable Media ○ Internal Flash

Destination Sub-folder: \cf0\HTML

PROJECT MANAGEMENT

3. Click **Set User Password**. The **Set Password** dialog box is displayed.

### Set Password Dialog Box

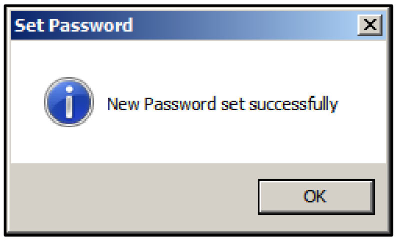


Set Password

New Password:

4. Enter a password in the **New 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: ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /
5. Click **OK**. A window confirming that the password has been set successfully is displayed.

Set Password Message Window



New Password set successfully

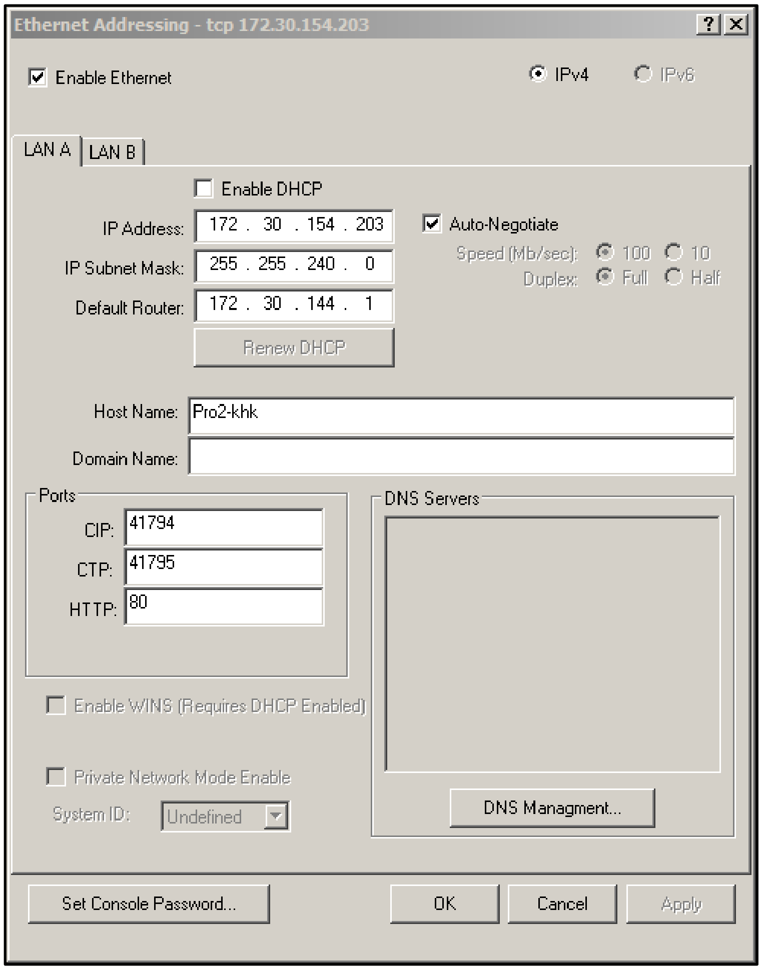
6. Click **OK.**

## Set a Console Password

To set a console password for the 2-Series control system:

1. Open the **EasyConfig** tool for the 2-Series control system by following steps 1–5 of Verify the Firmware Version on page 2.
2. Click **Ethernet Settings**. A dialog box for editing Ethernet settings is displayed.

### Ethernet Settings Dialog Box



Ethernet Addressing - tcp 172.30.154.203

☑ Enable Ethernet

● IPv4 ○ IPv6

LAN A | LAN B

☐ Enable DHCP

IP Address: 172 . 30 . 154 . 203

IP Subnet Mask: 255 . 255 . 240 . 0

Default Router: 172 . 30 . 144 . 1

☑ Auto-Negotiate

Speed (Mb/sec): ● 100 ○ 10

Duplex: ● Full ○ Half

Host Name: Pro2-khk

Domain Name:

Ports

CIP: 41794

CTP: 41795

HTTP: 80

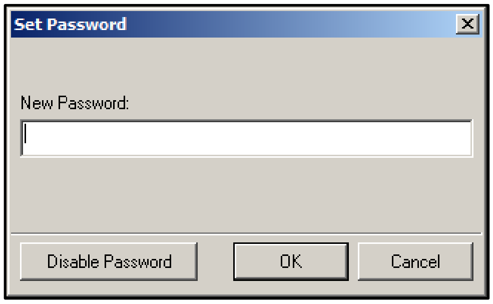
☐ Enable WINS (Requires DHCP Enabled)

☐ Private Network Mode Enable

System ID: Undefined

3. Click **Set Console Password**. The **Set Password** dialog box is displayed.

### Set Password Dialog Box

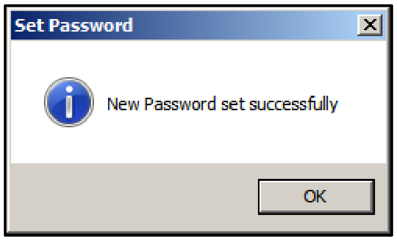


Set Password

New Password:

4. Enter a password in the **New 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: ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /
5. Click **OK**. A window confirming that the password has been set successfully is displayed.

    Set Password Message Window

    New Password set successfully

6. Click **OK.**

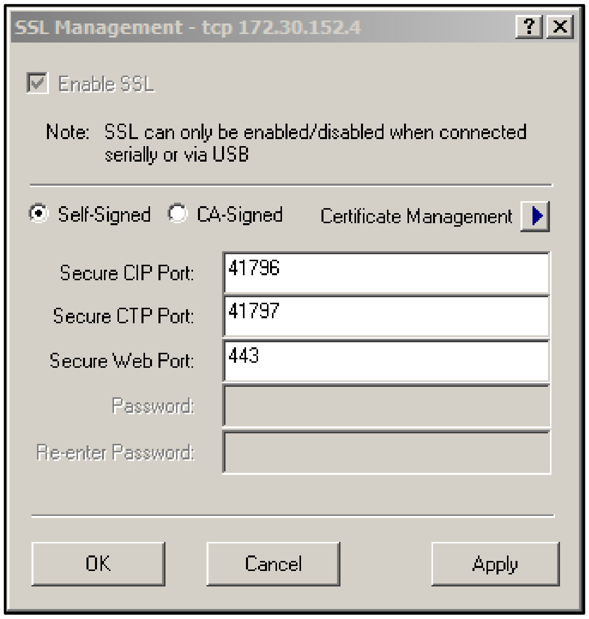
## Configure SSL

To configure SSL (Secure Socket Layers) for the 2-Series control system:

1. Open the **EasyConfig** tool for the 2-Series control system by following steps 1–5 of Verify the Firmware Version on page 2.

2. Navigate to **Functions** > **SSL Management**. A dialog box for configuring SSL is displayed.

SSL Management Dialog Box



SSL Management - tcp 172.30.152.4

☑ Enable SSL

Note: SSL can only be enabled/disabled when connected serially or via USB

● Self-Signed ○ CA-Signed Certificate Management

Secure CIP Port: 41796

Secure CTP Port: 41797

Secure Web Port: 443

Password:

Re-enter Password:

3. Click the check box next to **Enable SSL**. A filled check box indicates that SSL is enabled.

**NOTE:** SSL can be enabled on a 2-Series control system over a serial or USB connection only. The **Enable SSL** check box is not available over other connections.

4. Click the **Self-Signed** radio button.

5. If required, change the default ports by entering new port numbers in the **Secure CIP Port**, **Secure CTP Port**, and **Secure Web Port** text fields. These ports are used to set up remote access for mobile or browser applications.

6. Click **OK**. The 2-Series control system reboots automatically, and the new settings take effect following the reboot.

# Secure a 3-Series Control System

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

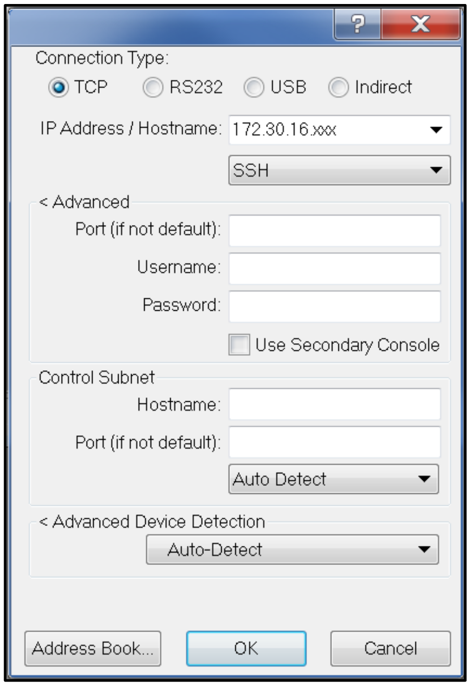
NOTE: For more information on configuring authentication and security settings for a 3-Series control system, refer to the 3-Series Control System Reference Guide (Doc. 7150) at www.crestron.com/manuals.

## 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



Connection Type:

● TCP ○ RS232 ○ USB ○ Indirect

IP Address / Hostname: 172.30.16.xxx

SSH

< Advanced

Port (if not default):

Username:

Password:

□ Use Secondary Console

Control Subnet

Hostname:

Port (if not default):

Auto Detect

< Advanced Device Detection

Auto-Detect

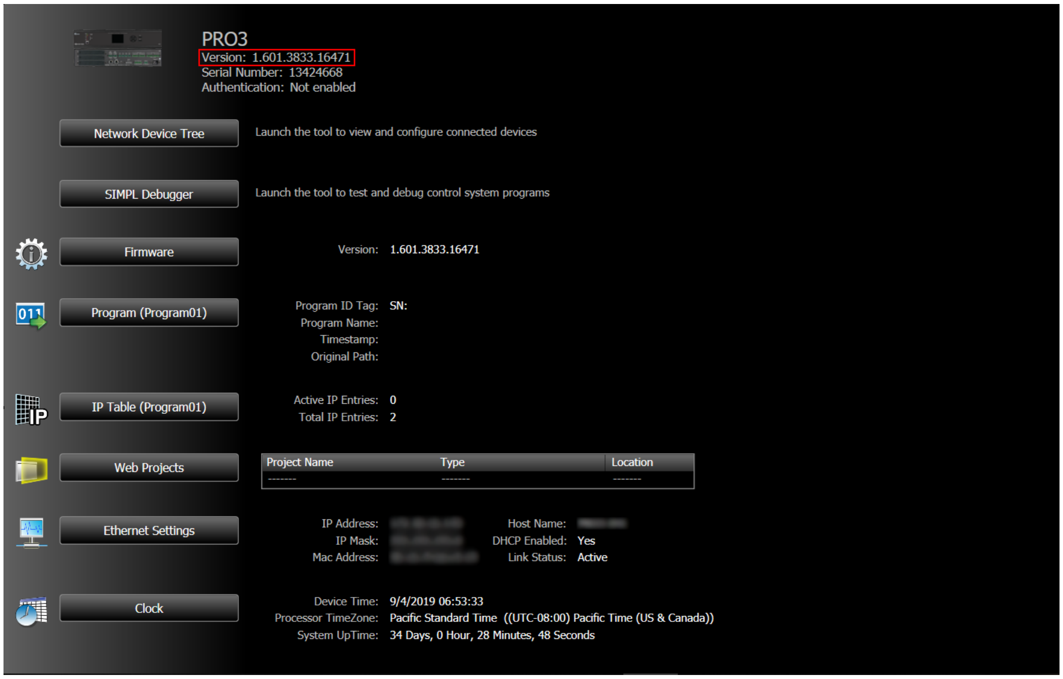
4. Select the **TCP** button under **Connection Type**.
5. Enter the control system IP address or hostname in the **IP Address / Hostname** text field.
6. Select **SSH** from the drop-down menu under the **IP Address / Hostname** text field.

NOTE: If a console port is currently open for external use, route it to port 22.

7. Configure any additional TCP connection setting as needed.

8. Click **OK**. The **EasyConfig** tool is displayed with information about the 3-Series control system.

**EasyConfig - 3-Series Control System**



PRO3
Version: 1.601.3833.16471
Serial Number: 13424668
Authentication: Not enabled

Launch the tool to view and configure connected devices

Launch the tool to test and debug control system programs

Version: 1.601.3833.16471

Program ID Tag: SN:
Program Name:
Timestamp:
Original Path:

Active IP Entries: 0
Total IP Entries: 2

| Project Name | Type | Location |
|---|---|---|
| ------- | ------- | ------- |

IP Address: [redacted]
IP Mask: [redacted]
Mac Address: [redacted]
Host Name: [redacted]
DHCP Enabled: Yes
Link Status: Active

Device Time: 9/4/2019 06:53:33
Processor TimeZone: Pacific Standard Time ((UTC-08:00) Pacific Time (US & Canada))
System UpTime: 34 Days, 0 Hour, 28 Minutes, 48 Seconds

9. Verify that the firmware version (listed next to **Version** at the top of the tool) is 1.11 or higher. Update the device firmware to the required version if necessary.

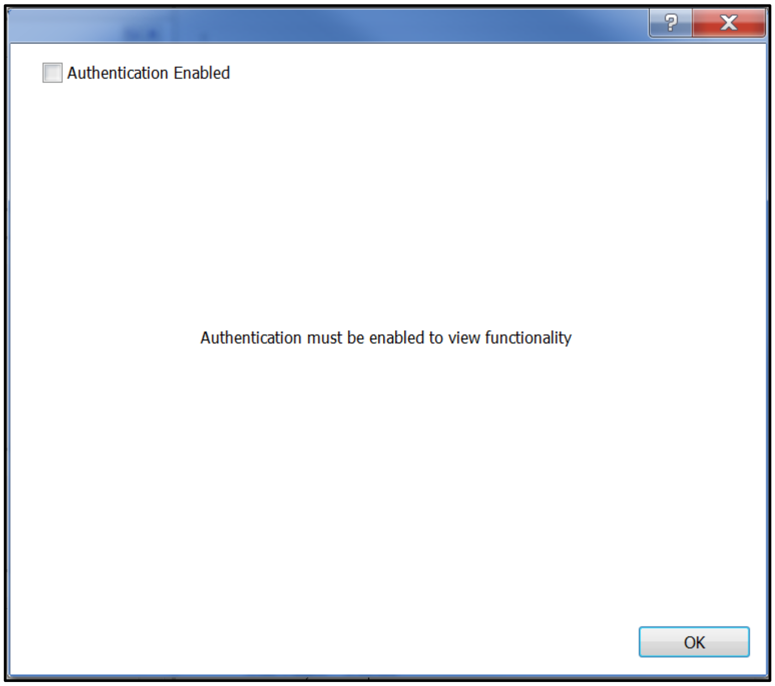
## Configure Authentication

To configure authentication settings for the 3-Series control system:

1. Open the **EasyConfig** tool for the 3-Series control system by following steps 1–7 of Verify the Firmware Version, starting on page 8.

2. Navigate to **Functions** > **Authentication**. A dialog box for configuring authentication settings is displayed.

### Authentication Dialog Box



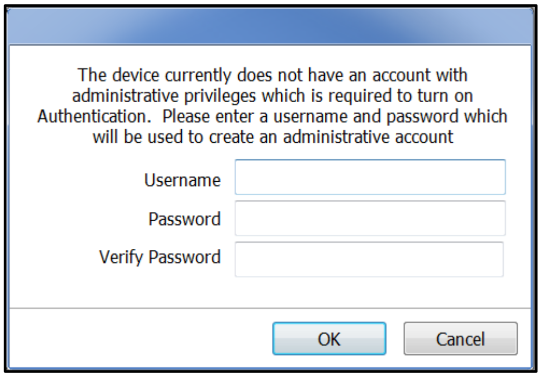
□ Authentication Enabled

Authentication must be enabled to view functionality

3. Click the check box next to **Authentication Enabled**. A filled check box indicates that authentication is 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.

### Create Administrator Account Dialog Box



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

4. Enter a username in the **Username** text field.

5. Enter a password in the **Password** text 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** text 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 (3 by default), the control system locks out any additional login attempts from the same IP address for a 24-hour period. After one incorrect login attempt over a USB connection, the control system blocks any additional login attempts over USB for 5 minutes. For more information, refer to the Crestron Secure Deployment Guide at www.crestron.com/en-US/Security/Security-at-Crestron.

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

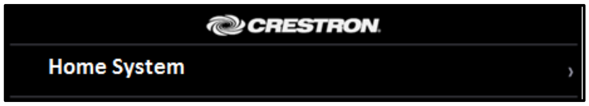
It is highly recommended that at least one additional account is created and added to the Users group. This account should be used in the SSL settings of the mobile applications. For more information, refer to the Crestron Secure Deployment Guide at OLH article 5571.

# Enable SSL on the Crestron App

To enable SSL on the Crestron App for Crestron control systems:

1. From Crestron Toolbox, click the pencil icon in a supported tool (such as **EasyConfig**) to edit the control system connection settings.
2. From the Crestron App, select the desired control system connection from the connection list.

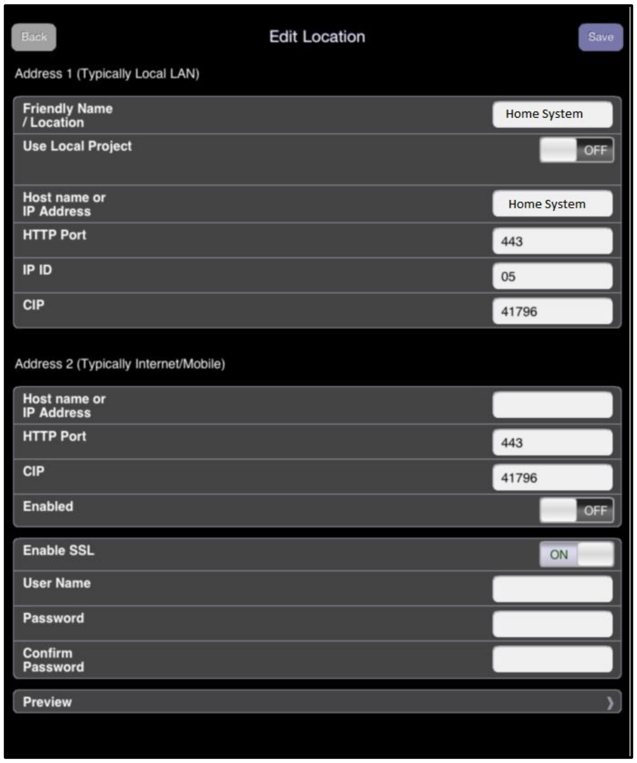
### Connection List



Home System ›

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

### Edit Location Dialog Box



Edit Location

Address 1 (Typically Local LAN)

| | |
|---|---|
| Friendly Name / Location | Home System |
| Use Local Project | OFF |
| Host name or IP Address | Home System |
| HTTP Port | 443 |
| IP ID | 05 |
| CIP | 41796 |

Address 2 (Typically Internet/Mobile)

| | |
|---|---|
| Host name or IP Address | |
| HTTP Port | 443 |
| CIP | 41796 |
| Enabled | OFF |
| Enable SSL | ON |
| User Name | |
| Password | |
| Confirm Password | |

Preview ›

3. Tap the switch next to **Enable SSL** to set it to **On**. The HTTP port for Addresses 1 and 2 changes from 80 to 443 and the CIP port changes from 41794 to 41796.
4. Enter the administrator username and password created for the control system in the **User Name** and **Password** fields, respectively.
5. Enter the administrator password again in the **Confirm Password** text field.
6. Click **Save**. SSL is enabled immediately (no reboot is required).

# Secure a Crestron Home OS 3 System

New Crestron Home OS 3 systems running on the CP4-R are secured by factory default:

- Crestron Home OS 3 enables authentication and SSL by default on the CP4-R. SSL is also enabled on the Crestron Home app by default.
- Crestron Home OS 3 uses self-signed certificates.
- The **Web Pages and Mobility Projects** function in Crestron Toolbox does not work with Crestron Home OS 3.
- Upgrading to Crestron Home OS 3 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 3, 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 3, the username is set to "admin" and the password is set to the serial number of CP4-R (case-sensitive). For more information, refer to the Crestron Home OS 3 Product Manual (Doc. 8525) at www.crestron.com/manuals.

The following ports must be opened on a router for external control of the Crestron Home and Crestron Home Setup apps.

**NOTE:** Only map ports that are required for the necessary functions.

- **50001:** Used by the Crestron Home app for secure system access.
- **41796 (CTP):** Used by the Crestron Home Setup app for connecting to the processor in Crestron Toolbox software.
- **443 (HTTPS):** Used by the Crestron Home Setup app for serving files from the \HTTP\ folder on the processor (Crestron Home web XPanel interface, app manifest file, and so forth).

  **NOTE:** The `webport` command may be issued using the Text Console tool in Creston Toolbox to change the processor's HTTPS port if the router is not capable of port mapping.

For more information on port mapping, refer to "Enable Remote Access" on page 20.

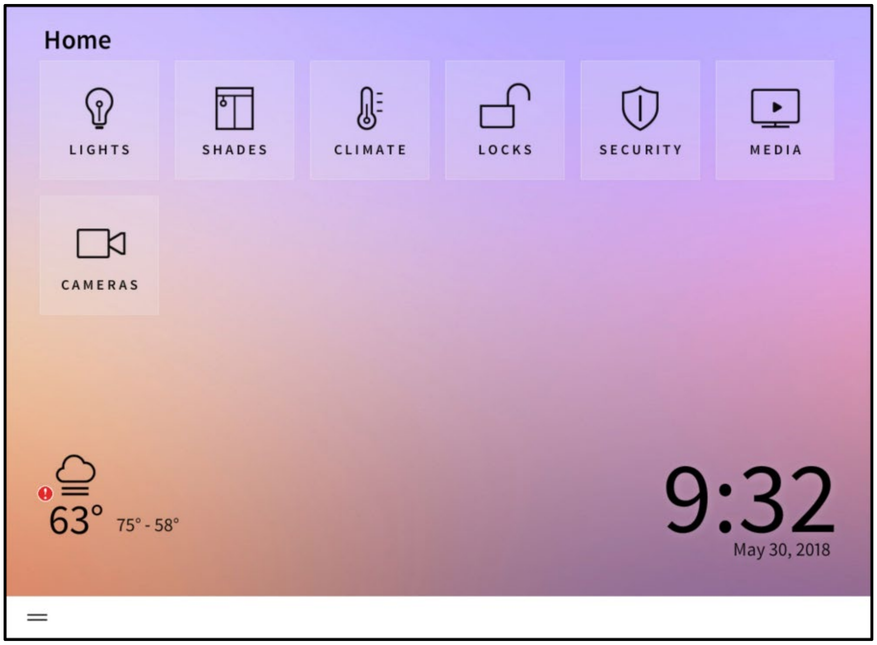
# Secure a Crestron Pyng OS 1 or OS 2 System

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

To secure a Crestron Pyng system:

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

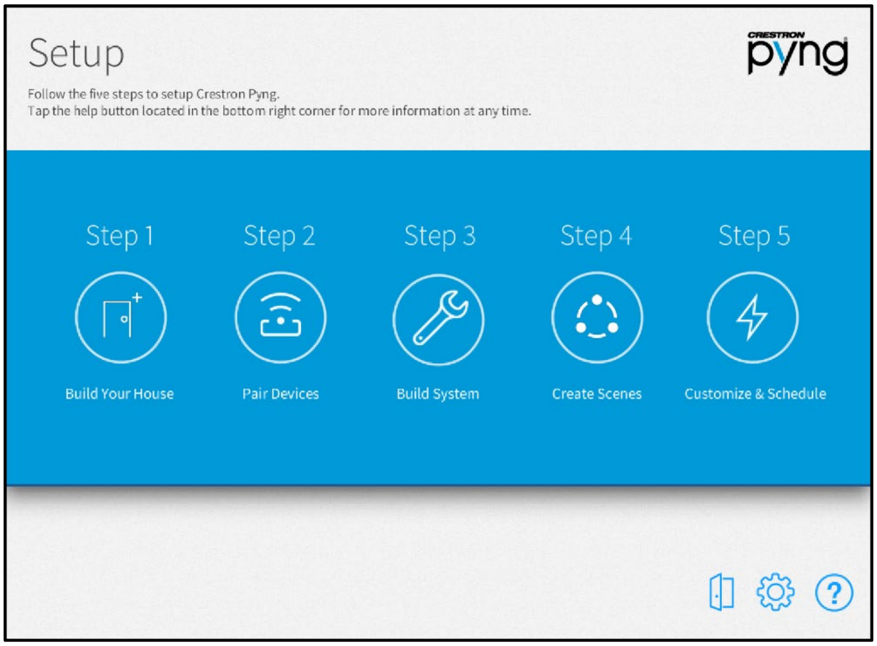
   Home Screen (Crestron Pyng OS 2)

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 Screen (Crestron Pyng OS 2)

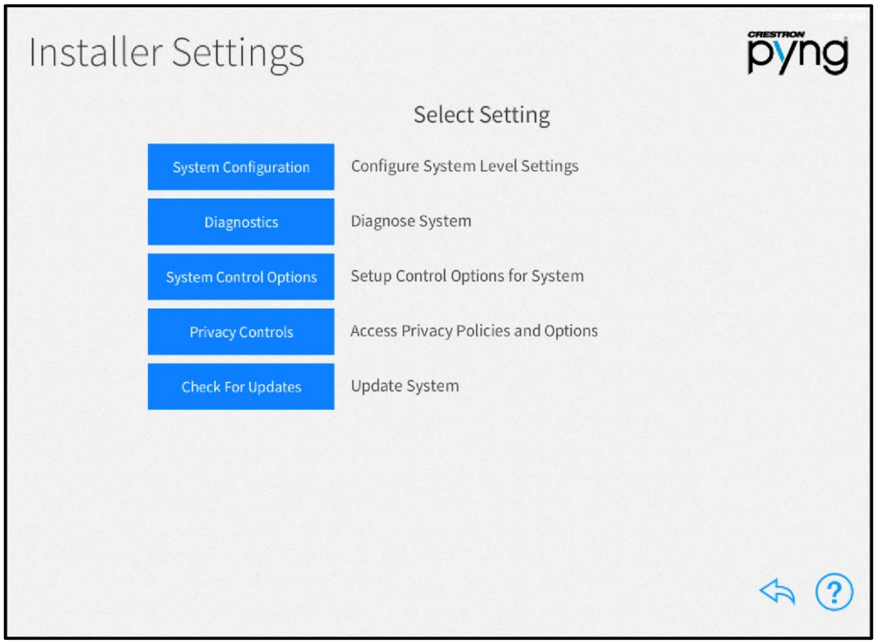


Setup

Follow the five steps to setup Crestron Pyng.
Tap the help button located in the bottom right corner for more information at any time.

4. Tap the gear button ⚙ to display the **Installer Settings** screen.

Installer Settings Screen (Crestron Pyng OS 2)



Installer Settings

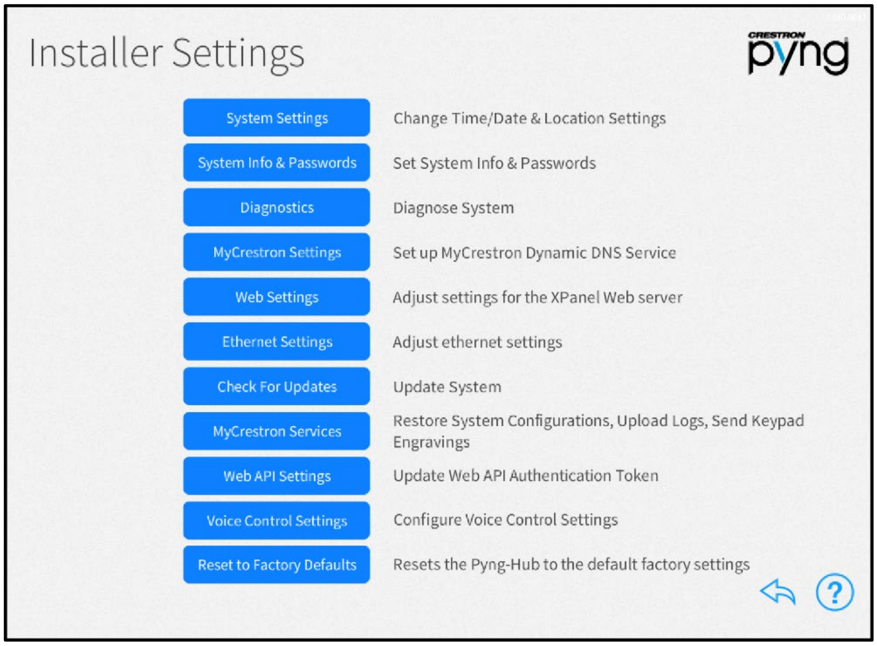
Select Setting

| | |
|---|---|
| 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)



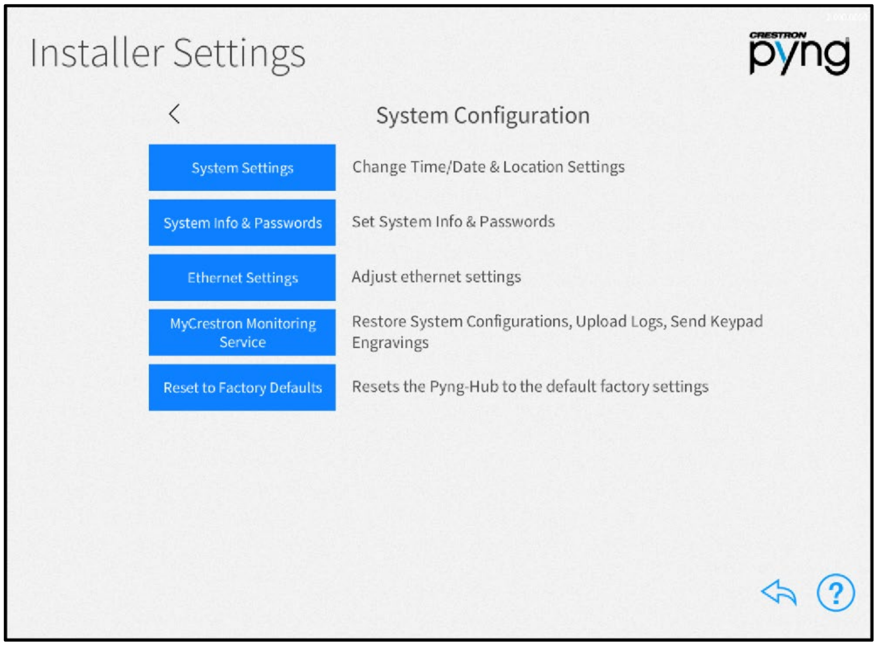
Installer Settings

CRESTRON pyng

| | |
|---|---|
| System Settings | Change Time/Date & Location Settings |
| System Info & Passwords | Set System Info & Passwords |
| Diagnostics | Diagnose System |
| MyCrestron Settings | Set up MyCrestron Dynamic DNS Service |
| Web Settings | Adjust settings for the XPanel Web server |
| Ethernet Settings | Adjust ethernet settings |
| Check For Updates | Update System |
| MyCrestron Services | Restore System Configurations, Upload Logs, Send Keypad Engravings |
| Web API Settings | Update Web API Authentication Token |
| Voice Control Settings | Configure Voice Control Settings |
| Reset to Factory Defaults | Resets the Pyng-Hub to the default factory settings |

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

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



Installer Settings

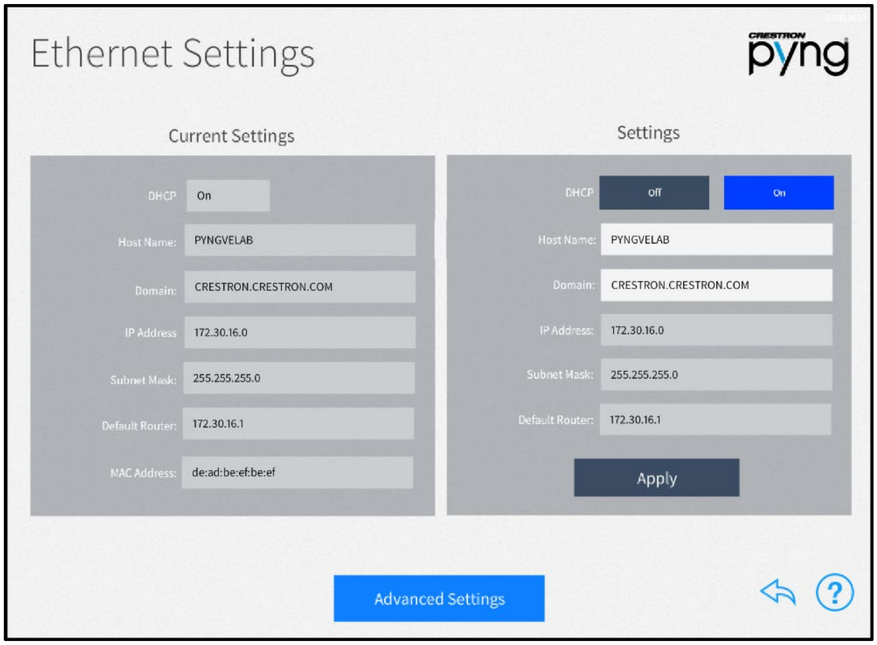
CRESTRON pyng

System Configuration

| | |
|---|---|
| System Settings | Change Time/Date & Location Settings |
| System Info & Passwords | Set System Info & Passwords |
| Ethernet Settings | Adjust ethernet settings |
| MyCrestron Monitoring Service | Restore System Configurations, Upload Logs, Send Keypad Engravings |
| Reset to Factory Defaults | Resets the Pyng-Hub to the default factory settings |

The **Ethernet Settings** screen is displayed.

### Ethernet Settings Screen



Ethernet Settings

Current Settings

DHCP: On

Host Name: PYNGVELAB

Domain: CRESTRON.CRESTRON.COM

IP Address: 172.30.16.0

Subnet Mask: 255.255.255.0

Default Router: 172.30.16.1

MAC Address: de:ad:be:ef:be:ef

Settings

DHCP: Off [✓ On]

Host Name: PYNGVELAB

Domain: CRESTRON.CRESTRON.COM

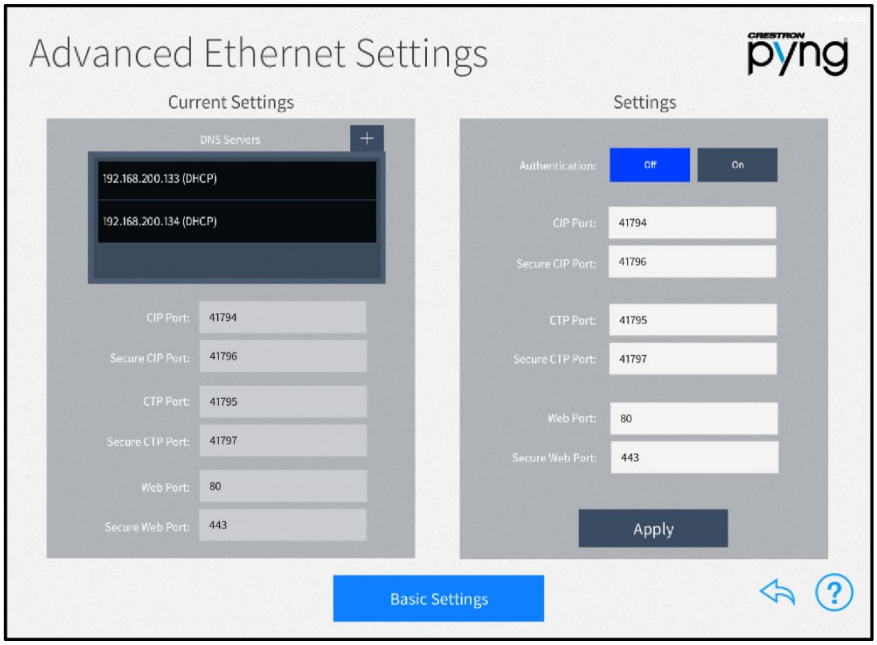
IP Address: 172.30.16.0

Subnet Mask: 255.255.255.0

Default Router: 172.30.16.1

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

### Advanced Ethernet Settings Screen



Advanced Ethernet Settings

Current Settings

DNS Servers

192.168.200.133 (DHCP)

192.168.200.134 (DHCP)

CIP Port: 41794

Secure CIP Port: 41796

CTP Port: 41795

Secure CTP Port: 41797

Web Port: 80

Secure Web Port: 443

Settings

Authentication: [✓ Off] On

CIP Port: 41794

Secure CIP Port: 41796

CTP Port: 41795

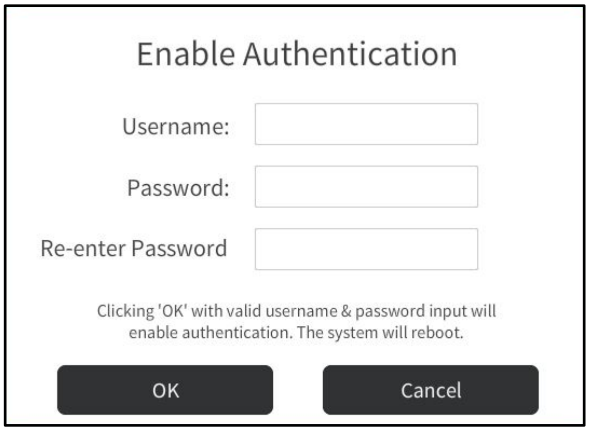
Secure CTP Port: 41797

Web Port: 80

Secure Web Port: 443

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

Enable Authentication Dialog Box

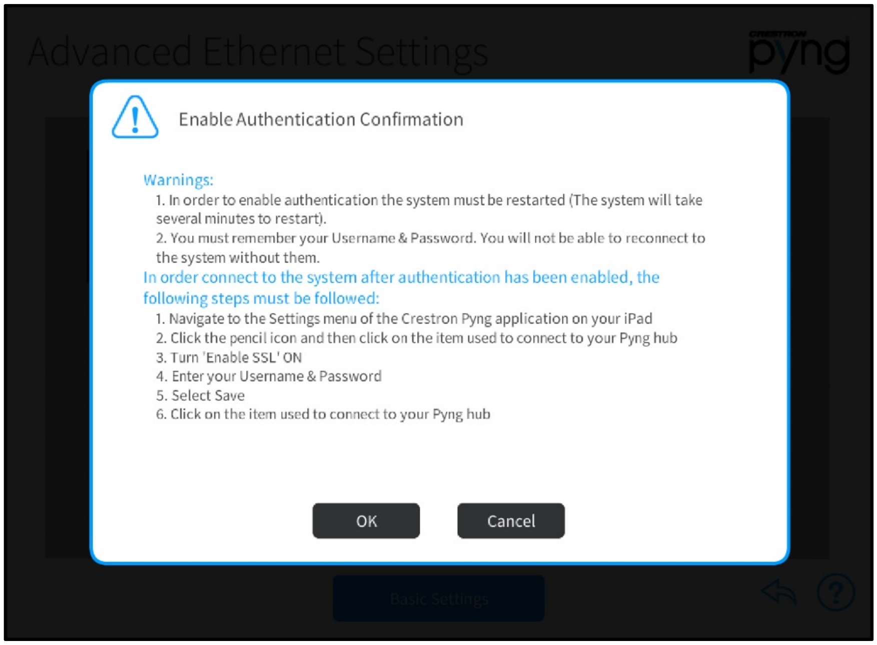


Clicking 'OK' with valid username & password input will enable authentication. The system will reboot.

8. Enter a username in the **Username** field.
9. Enter a password in the **Password** text 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 **Verify Password** text field.

11. Tap **OK**. The **Enable Authentication Confirmation** dialog box displays.

Enable Authentication Confirmation Dialog Box



Enable Authentication Confirmation

Warnings:

1. In order to enable authentication the system must be restarted (The system will take several minutes to restart).
2. You must remember your Username & Password. You will not be able to reconnect to the system without them.

In order connect to the system after authentication has been enabled, the following steps must be followed:

1. Navigate to the Settings menu of the Crestron Pyng application on your iPad
2. Click the pencil icon and then click on the item used to connect to your Pyng hub
3. Turn 'Enable SSL' ON
4. Enter your Username & Password
5. Select Save
6. Click on the item used to connect to your Pyng hub

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

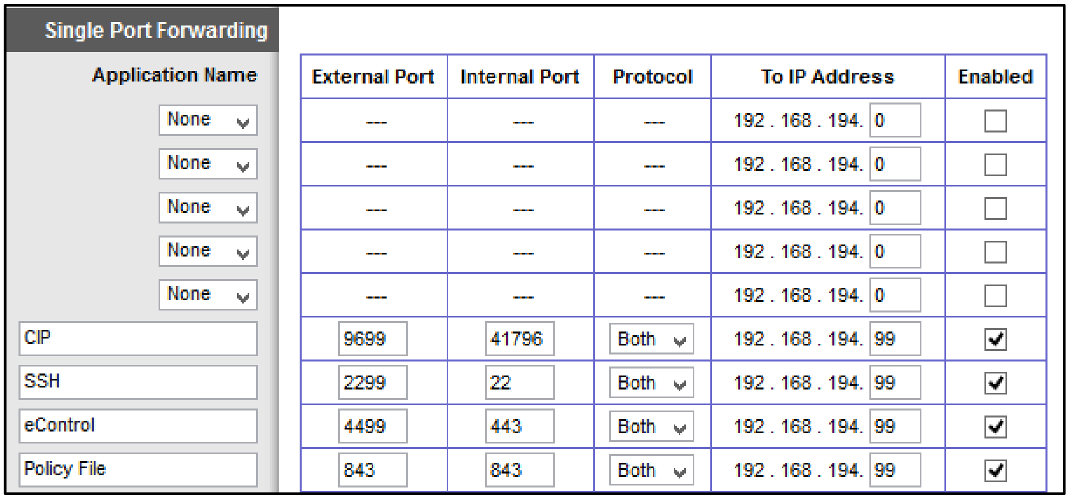
# Enable Remote Access

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.

Observe the following points to provide connections from outside the local network for mobile and browser applications.

- Remap the external ports from the initial defaults. Remapping the external ports minimizes the number attempts that can access the system. A hacker is unable to scan well-known ports for entry and must instead scan all ports and 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.

Home Router Setup Page Example



Single Port Forwarding

| 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 | Both | 192 . 168 . 194. 99 | ☑ |
| SSH | 2299 | 22 | Both | 192 . 168 . 194. 99 | ☑ |
| eControl | 4499 | 443 | Both | 192 . 168 . 194. 99 | ☑ |
| Policy File | 843 | 843 | Both | 192 . 168 . 194. 99 | ☑ |

- 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.
- Note the exception on the policy file support. If the XPanel web browser is used, open port 843 under **External Port**.
- 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 his or her credentials prior to running the project. The XPanel browser required port 843 to be routed to the system.
- If ports 41794 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: 201.767.7576
www.crestron.com

**Setup & Configuration – DOC. 7818E**
**(2044775)**
**10/11/19**
Specifications subject to
change without notice.