4-Series™ Control Systems

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	July 8, 2021	Initial version	IH
B	January 7, 2022	Incorporated major updates from Military Unique version of document	IH, JD
C	May 20, 2022	Added information about default user roles and permissions	IH, JD

Please send comments and change recommendations to:

SecurityDocs@crestron.com

Contents

Overview

This document describes the steps needed to harden a Crestron® installation with 4-Series™ control systems and assumes a basic understanding of security functions and protocols. This guide provides information about the system configuration used for 4-Series control systems firmware release 2.7000.00014 or later.

> **NOTE:** The term "device" is used in this document to refer to all applicable 4-Series control system models unless specified otherwise.

The information in this guide pertains to the following device models:

Model	Description
AV4	4-Series™ Control System
CP4	4-Series™ Control System
CP4N	4-Series™ Control System
DIN-AP4	4-Series™ DIN Rail Control System
MC4	4-Series™ Control System
MC4-I	4-Series™ Control System, International
PRO4	4-Series™ Control System
RMC4	4-Series™ Control System

Ports and Protocols

The following ports and protocols may be used by the device depending on the system design and configuration.

Crestron Control Devices

Function	Destination Port	From (Sender)	To (Listener)	Notes
Crestron-CIP	41794/TCP	Remote Device	Device	Crestron Internet Protocol
Crestron-SCIP	41796/TCP	Remote Device	Device	Secure Crestron Internet Protocol
HTTPS	49200/TCP	Remote Device	Device	Web API for Crestron HTML5 User Interfaces

Common Ports

Function	Destination Port	From (Sender)	To (Listener)	Notes
NTP	123/UDP	Device	NTP Server	Network Time Protocol (NTP)
SSH/SFTP	22/TCP	Admin Workstation	Device	Used for configuration, console, and file transfer
LDAP	3268/TCP	Device	LDAP Server	LDAP queries targeting global catalogs
HTTPS	443/TCP	Admin or End User Workstation	Device	Secure web configuration
HTTPS	443/TCP	Device	XiO Cloud® Service	For XiO Cloud services only and not required for device functionality. A persistent connection is made via AMQP over WebSockets. HTTPS services such as routing lookups and file transfers may be used.
DHCP	67/UDP	Device	DHCP Server	DHCP addressing
DHCP	68/UDP	DHCP Server	Device	DHCP addressing
HTTP	80/TCP	End User Workstation	Device	Redirect to Secure Web Configuration on port 443
Remote Syslog	Configurable	Device	Remote Syslog Server	Uses TLS

Function	Destination Port	From (Sender)	To (Listener)	Notes
SNMP	161/UDP	SNMP Manager	Device	
SNMP Traps	162/UDP	Device	SNMP Manager	

Prerequisites

In order to perform a secure configuration, the following prerequisites must be met.

Operating Environment

Crestron assumes the following about the operating environment of its systems:

- The system is not capable of Multi-Factor Authentication (MFA). If your organization's policy requires MFA, you cannot use the system.
- Physical security is commensurate with the value of the system and the data it contains and is assumed to be provided by the environment.
- Administrators are trusted to follow and provide all administrator guidance.

Firmware Version

4-Series control systems must be running firmware version 2.7000.00014 or later.

Device Access

The administrator can access and configure the device by using a web browser or an SSH client. This document describes device configuration using an SSH client, which provides access to console commands. Some configuration capabilities can only be performed by issuing console commands. Additionally, some aspects of configuration can be performed via Crestron Toolbox™ software, or the XiO Cloud® service.

> **NOTE:** The SSH client that is used must be capable of connecting to the device using SSHv2 and must be compatible with FIPS 140-2 validated algorithms.

As an alternative to using an SSH client, the same console commands can be executed through the USB port.

Default Configuration Settings

In order to configure the device, it must first be placed in its factory default state. A device can be returned to this state by entering the following command on the console:

```
RESTORE
```

If you do not have access to the console (for example, the password has been lost), a factory reset may be performed as follows:

1. Press and release the **HW-R** button on the front panel of the control system.
2. Quickly press the **SW-R** button on the front panel of the control system 5 times, with less than a one-second gap between each press.
3. Wait 5 to 10 minutes for the self-recovery process to complete.
4. Proceed with the network configuration.

Required Configuration

The following sections describe the configuration changes required for the device for a secure deployment.

Configure the Network

The following sections provide information about the tasks necessary to configure the network.

DHCP or Static IP Address Configuration

To configure the device to communicate on the local LAN, the following changes must be made. If DHCP is available on the local network, then no additional configuration changes are necessary. If DHCP is not available or if the administrator wishes to manually set the network configuration, then the IP address, IP mask, default gateway, and DNS server settings must be set.

```
dhcp 0 off
```

Turns off DHCP so that the manually configured network information is used.

```
ipaddress 0 192.168.1.2
```

Sets the IP address of the device to the specified address.

```
ipmask 0 255.255.255.0
```

Sets the IP mask of the device to the specified mask.

```
defrouter 0 192.168.1.1
```

Sets the default network gateway to the specified IP address.

```
adddns 192.168.1.10
```

Sets the DNS server to use for DNS name lookups.

802.1X Authentication

802.1X is an IEEE network standard designed to enhance the security of both wireless and wired Ethernet networks. This device supports 802.1X on its primary wired Ethernet interface only. If the network requires 802.1X, the device must be configured for 802.1X before being put on the network. This configuration can be done through the USB port console or by attaching it to a temporary network which does not require 802.1X.

Before configuring 802.1X, perform the following tasks as necessary:

- Unless server authentication is going to be disabled, the trusted x.509 certificate or certificates that will be used to verify the 802.1X server's certificate must be loaded into the device. Use the certificate management commands to load the trusted certificates into the device. These may be Root or Intermediate certificates. Refer to the Required Configuration (on the previous page) section for instructions.
- If EAP-TLS authentication is going to be used, a client certificate will be needed and must be loaded into the device. Refer to the Required Configuration (on the previous page) section for instructions to load a client certificate into the "machine" store.

Once 802.1X configuration is complete, restart the device to activate those settings. The device will try to connect to the 802.1X network when it starts up.

802.1X Configuration

In order to configure and use 802.1X, various aspects of 802.1X will need to be configured, including enabling it, setting up server authentication, and selecting a client authentication method. The following commands are used for this configuration:

Enable 802.1X

To enable 802.1X, issue the following command:

```
8021xauthenticate [on/off]
```

- `on` - 802.1X is enabled
- `off` - 802.1X is disabled
- No parameter - Displays the current setting

Example: `8021xauthenticate on`

Set Trusted Server Certificates

Unless server validation will be disabled, the trusted certificates that 802.1X will use to verify the server's certificate must be indicated. The full list of trusted Root and Intermediate certificates loaded into the device is not used for 802.1X—only the specific certificates selected by the `8021xtrustedcas` command are used. As indicated earlier, the trusted certificates must first be loaded into the device using the standard Certificate Management commands.

The following commands can be used to list, add, and remove certificates from the list of certificates that will be used by 802.1X.

List Certificates

To list available certificates, issue the following command:

```
8021xtrustedcas [list|listn|listu]
```

- `list` - Shows all Root and Intermediate certificates for the device
- `listn` - Shows all Root and Intermediate certificates for the device and also includes identification number of each certificate
- `listu` - Shows Root and Intermediate certificates that are used by 802.1X

Example: `8021xtrustedcas listn`

This certificate list will show the name and UID of each certificate, along with an indication of whether or not it is being used by 802.1X.

Add Certificate to 802.1X Trust List

To add a certificate to the list of trusted certificates to be used by 802.1X, issue the following command:

```
8021xtrustedcas use [certificate number] [certificate name] [certificate UID]
```

- `certificate number` - Number that identifies the specific certificate to use
- `certificate name` - Name that identifies the specific certificate to use
- `certificate UID` - UID that identifies the specific certificate to use

Only one identifier (number, name, or UID) is needed. These identifiers can be determined by listing the certificates using the `8021xtrustedcas list` or `8021xtrustedcas listn` described above. Only the `listn` command will show the certificate number.

Remove Certificate from 802.1X Trust List

To remove a certificate from the list of trusted certificates to be used by 802.1X, issue the following command:

```
8021xtrustedcas dontuse [certificate number] [certificate name] [certificate UID]
```

- `certificate number` - Number that identifies the specific certificate to remove
- `certificate name` - Name that identifies the specific certificate to remove
- `certificate UID` - UID that identifies the specific certificate to remove

Only one identifier (number, name, or UID) is needed. These identifiers can be determined by listing the certificates using the `8021xtrustedcas list` or `8021xtrustedcas listn` described above. Only the `listn` command will show the certificate number.

Removing a certificate from 802.1X does not remove the certificate from the device. The certificate will still be present in the Root or Intermediate store.

Enable 802.1X Server Validation

Under most circumstances, validation of the 802.1X server should be enabled. By default, server validation is disabled on this device.

To enable 802.1X server validation, issue the following command:

```
8021xvalidateserver [off | on]
```

- `off` - 802.1X supplicant will not validate authentication server's certificate.
- `on` - 802.1X supplicant will validate authentication server's certificate.
- No parameter - Displays the current setting

Example: `8021xvalidateserver on`

Select 802.1X Client Authentication Method

802.1X requires that the device authenticate with the server before it will be allowed on the network. The device supports two client authentications methods: PEAPv0/EAP-MSCHAPv2 and EAP-TLS. PEAPv0/EAP-MSCHAPv2 requires a user name and password, and EAP-TLS requires a client certificate.

To select the 802.1X client authentication method, issue the following command:

```
8021xmethod [password/certificate]
```

- `password` - Uses PEAPv0/EAP-MSCHAPv2 authentication
- `certificate` - Uses EAP-TLS authentication

Example: `8021xmethod password`

If EAP-TLS is selected, a client certificate must be loaded into the device as explained earlier in the 802.1X instructions.

If PEAPv0/EAP-MSCHAPv2 is selected, the user name and password to use for authentication must be entered with the following commands:

```
8021xusername [username]
```

```
8021xpassword [password]
```

Additional 802.1X Options

Additional 802.1X options may need to be configured if required by the network to which the device is connected:

- If the 802.1X server requires that a specific domain name be included with the 802.1X authentication request, the domain name can be set by issuing the following command:

  ```
  8021xdomain [domain_name]
  ```

- If using PEAPv0/EAP-MSCHAPv2 authentication and the server requires the PEAP version to be sent as part of the authentication request, the PEAP version can be enabled with the `on` option in the following command:

  ```
  8021xsendpeapver [on/off]
  ```

Set Password Policy

To set the password policy, issue the following command:

```
setpasswordrule{-all|-none}|{-length:minpasswordlength}{-mixed}{-digit}{-special}
```

- `-all` - All password rules are applied.
- `-none` - No password rules are applied.
- `-length:` - Specifies the minimum password length. By default, the minimum password length is six characters.
- `-mixed` - Specifies that the password must contain a lower and upper case character.
- `-digit` - Specifies that the password must contain a numeric character.
- `-special` - Specifies that the password must contain a special character.

> **NOTE:** The `-length`, `-mixed`, `-digit`, and `-special` parameters cannot be combined with `-none`.

Example: `setpasswordrule -length:9 -mixed -digit -special`

> **NOTE:** The following special characters are permitted: ` ~ ! @ $ % ^ & * ( ) _ + = { } [ ] | ; " < > , .

All passwords that are created, updated, or reset for local users must follow the password rules set by this command to be considered valid.

As a security best practice, Crestron recommends setting the password policy to the following:

```
setpasswordrule -length:15 -all
```

Set Date and Time

All devices use NTP to synchronize their clock. To disable NTP synchronization and set the current date and time manually, issue the following commands:

```
sntp stop
```

```
timedate hh:mm:ss mm-dd-yyyy
```

> **NOTE:** Enter the current time (24-hour clock format, including minutes and seconds) and date.

By default, the time zone is set to EST (code 014). This is never changed automatically and must be changed manually if desired. To set the time zone, issue the following command:

```
timezone [list | zone]
```

- `list` - Returns a list of all time zones and codes
- `zone` - Enter the code of the time zone to be used

Example: `timezone 005`

By default, NTP is enabled and is configured to get the time from pool.ntp.org. The device supports using up to three NTP servers, including authentication servers. Issue the following command to configure custom NTP servers for time synchronization:

`sntp [start|stop|sync|delete {server|server2|server3}|server {args}|server2 {args}|server3 {args}]`

- `start` - Starts synchronization
- `stop` - Stops synchronization
- `sync` - Forces synchronization one time
- `delete {server|server2|server3}` - Deletes configuration for NTP server1, server2, or server3
- `server:{address} [optional args]` - Address of primary NTP server with optional arguments
- `server2:{address} [optional args]` - Address of secondary NTP server to synchronize with optional arguments
- `server3:{address} [optional args]` - Address of secondary NTP server to synchronize with optional arguments
- `optional args`:
  - `port:{1-65535}` - NTP port (default 123)
  - `auth:{mac}` - Secured NTP MAC authentication
  - `keytype:{md5(less secured)|sha1|sha256}` - Key type for MAC authentication only (default `sha1`)

    > **NOTE:** `md5` is not allowed when FIPSMODE is on.

  - `key:{shared key}` - Preshared key between NTP client and server (MAC authentication only)
  - `keyid:{1-65535}` - Preshared key index between NTP client and server (MAC authentication only)
- No parameter - Displays the current settings

Example: `SNTP SERVER:macntp.example.com AUTH:mac KEYID:1 KEY:e5fa44f2b31c1fb553b6021e7360d07d5d91ff5e`

> **NOTE:** NTP servers are configured into a particular slot. The server configured into the `SERVER` slot will be the primary server used for time synchronization. The servers configured into the `SERVER2` and `SERVER3` slots will be used as secondary servers.

Control Subnet

Certain 4-Series control system models provide support for a separate network called a Control Subnet and have one or more network ports specifically for connecting devices to the Control Subnet. If your device has a Control Subnet, it must be configured.

The Crestron AV4, CP4N, and PRO4 have a dedicated Control Subnet, which allows for dedicated communication between the control system and Crestron Ethernet devices without interference from other network traffic on the LAN. The AV4 and PRO4 provide four Control Subnet ports that also support PoE+ using the optional PW-5430DUS power supply.

CAUTION: Do not connect the **CONTROL SUBNET** port to the LAN. The **CONTROL SUBNET** port must only be connected to Crestron Ethernet devices.

When using the Control Subnet, observe the following:

- The control system acts as a DHCP server to all devices connected to the Control Subnet and assigns IP addresses as needed.
- A DNS server is built in to the control system to resolve host names.
- Only connect Crestron Ethernet devices to the Control Subnet.
- The control system operates in isolation mode by issuing the `isolatenetworks on` command. When in isolation mode, the firewall is configured so that no communication can occur between the LAN and devices on the Control Subnet. Using this mechanism, customers can protect their corporate LAN from devices on the Control Subnet.
- When in isolation mode, devices on the Control Subnet do not have any resources on the LAN side. For example, if a touch screen with a SmartObjects® technology object requiring network access is installed on the Control Subnet, the object will not work.
- Devices on the LAN do not have access to any devices on the Control Subnet. Crestron Toolbox also does not have access to these devices when it is connected to the LAN. To configure devices on the Control Subnet with Crestron Toolbox (outside of runtime), the computer running Crestron Toolbox must be connected to the Control Subnet.
- Any NAT/port mapping rules that were previously created do not work when the control system is in isolation mode.

NOTE: If the control system is running in isolation mode, Crestron Ethernet devices requiring internet access should not be connected to the **CONTROL SUBNET** port (directly or indirectly) and should be instead connected to the LAN.

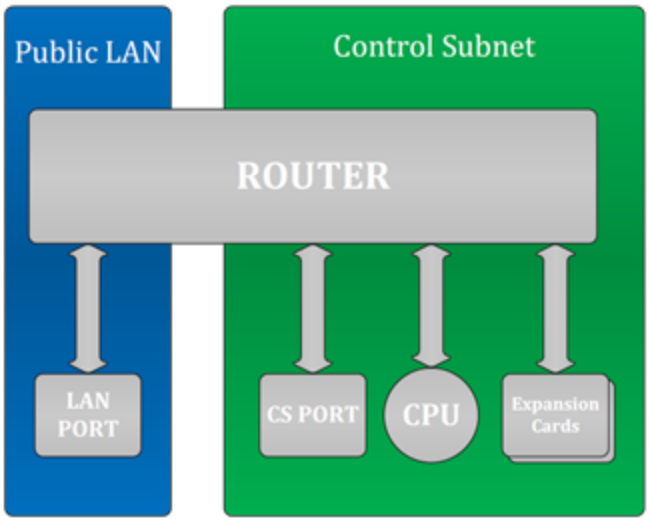
Control Subnet Architecture

Even if nothing is plugged into the **CONTROL SUBNET** port(s) on the back on the control system, the following are still present on the Control Subnet:

- Control System CPU (where AV programs run)
- Optional Expansion cards (PRO4 and AV4 only)

This design is in place to ensure that the Crestron CPU and optional expansion cards are protected from malicious packets on the LAN. Refer to the diagram below for more information on how these components work together.

Public LAN/Control Subnet Diagram



The firewall rules permit entry to only the traffic that is listened to by the CPU. As a result, a port scan will only show ports that are listened to by the CPU. Users can set up manual port forwarding rules to make custom connections to the devices on the Control Subnet.

Control Subnet Configuration

For increased security, the device supports a mode of operation called isolation mode. In isolation mode, the firewall is preconfigured to limit access to the Control Subnet, port mapping between the primary network and devices on the Control Subnet are blocked, and manual configuration of port forwarding is not available. To configure isolation mode, issue the following command:

`isolatenetworks [state]`

- `state` - {ON | OFF}
- No parameter - Displays the current setting

Example: `isolatenetworks on`

As a security best practice, the device should have its Control Subnet in isolation mode.

Control Subnet Router Configuration

By default, the Control Subnet router is configured to use 10.0.0.0/8 for the Control Subnet. If the device detects that the primary network is using that network address, the device will automatically switch to using 172.22.0.0/16 for the Control Subnet. To verify if the device is automatically choosing the Control Subnet address, issue the `CSINAutoMode` command. To confirm what address is being used, issue the `ipconfig` command to show the addresses assigned to the device's network interfaces.

If the control system will use a specific network address, that address can be configured using the following command:

`CSRouterPrefix [IP_Address/Prefix_Size]`

- `IP_Address` - The desired IP address
- `Prefix_Size` - The number of leading bits of the routing prefix
- No parameter - Displays the current Control Subnet configuration

Example: `CSRouterPrefix 192.168.0.0/24`

Control Subnet DHCP Configuration

By default, the device provides a DHCP server on the Control Subnet to issue IP addresses for anything connected to the Control Subnet. IP addresses that have been issued can be displayed by using the `DHCPLeases` command.

The `DHCPLeases` command will return a list of IP address that have been issued and information about them.

In addition, specific IP addresses can be assigned to specific devices on the Control Subnet. This can be done by issuing the following command:

`RESERVEDLeases [ADD | REM | CLEAR_ALL]`

- `ADD` - Adds an IP address to a device using the following syntax: `MAC_Address IP_Address Description`

    - `MAC_Address` - The device MAC address
    - `IP_Address` - The device IP address
    - `Description` - A description of the device
- `REM` - Removes a previously created IP address from the device using the following syntax: `MAC_Address`
    - `MAC_Address` - The device MAC address
- `CLEAR_ALL` - Clears all previous created IP addresses
- No parameter - Displays all current reserved DHCP leases in table format

Example: `RESERVEDLeases ADD 81:51:CA:48:73:24 10.0.0.9 TestDevice`

The MAC address should be in the format XX:XX:XX:XX:XX:XX on the command line.

Control Subnet Firewall Configuration

In isolation mode, the firewall is preconfigured to limit access to the Control Subnet and cannot be further configured. The firewall configuration in isolation Mode is as follows:

Control System Firewall Rules - Isolation Mode

Direction	Port(s)	Rule	Description
Inbound from LAN	22	To CPU	SSH
Inbound from LAN	80, 443	To CPU	Web server (if enabled)
Inbound from LAN	41794, 41796	To CPU	Crestron communication protocols
Inbound from LAN	Listen ports used by program	To CPU	Programmatic listeners
Inbound from LAN	49200	To CPU	Crestron HTML5 User Interface
Inbound from LAN	64000–64299	Blocked	In isolation mode, Crestron management tools cannot connect to any devices on the Control Subnet
Control Subnet Outbound to LAN	Any port	All other devices: Blocked	No outbound traffic is allowed
Inbound from LAN	User defined	Blocked	In isolation mode, no port forwarding can be managed by the user

Disable Auto Discovery

All devices support an autodiscovery feature which allows them to be detected, report basic information, and do some basic configuration remotely. This feature is not protected by any type of authentication. Disable auto discovery with the following command:

```
autodiscovery off
```

Disable Cloud Features

All devices connect to cloud services for remote monitoring and management. If your environment or policies do not permit communications with external services, disable cloud features by entering the following commands:

```
enablefeature cloudclient off
```

```
hydrogenenable off
```

Disable Wireless Communications

Certain control system models support infiNET EX® wireless communications. As a security best practice, this support should be disabled by issuing the following command:

```
rfgateway off
```

Enable User Account Locking

To prevent brute force attacks against a user's password, the device can automatically lock an account after a number of failed login attempts. This functionality operates independently and simultaneously with the device's User Login IP Blocking capability.

> **NOTE:** Access to an account over the USB port is never blocked.

Change Login Failure Count

To change the value for the login failure count, issue the following command:

```
setuserloginattempts [number]
```

- `number` - Number of login attempts a user can have before the console is blocked. A value of `0` indicates an infinite number of login attempts. A value of `-1` restores the default value.
- No parameter - Displays the current setting

Example: `setuserloginattempts 3`

As a security best practice, the failure count should be set to `3`.

Change Lockout Time

To change the duration that an IP address is blocked by the console, issue the following command:

```
setuserlockouttime [number]
```

- `number` - Number of hours (suffix `h`) or minutes (suffix `m`) to block a user. A value of `0` specifies an indefinite amount of time. The maximum amount of time is `750h` (hours) or `45000m` (minutes). A value of -1 restores the default value.
- No parameter - Displays the current setting

Example: `setuserlockouttime 15m`

As a security best practice, the lockout time should be set to `15m`.

Display Last Logged-In Information

Devices ido not display information about a user's last login or failed login attempts by default. To have this information displayed, issue the following command:

```
showlogininfo on
```

Enable Session Inactivity Timeout

> **NOTE:** The Enable Session Inactivity Timeout command affects both console and web sessions.

Devices do not terminate a user session due to inactivity by default. Configure the device to terminate inactive user sessions by issuing the following command:

```
setlogoffidletime 10
```

The number set with the `setlogoffidletime` command is the number of minutes after which the session will be terminated. The number can range from `1` to `9999`.

Enable Audit Logging

All devices have limited audit logging. Audit logging is turned off by default.

To configure audit logging, issue the following command:

```
auditlogging[on|off]{[all]|[none]|{[admin][prog][oper][user]}[remotesyslog]}
```

- `on` - Enables audit logging
- `-off` - Disables audit logging
- No parameter - Displays the current audit logging setting
- The following parameters are optional and are used to log commands by access level:
  - `admin` - Logs administrator-level commands
  - `prog` - Logs programmer-level commands
  - `oper` - Logs operator-level commands
  - `user` - Logs user-level commands
  - `all` - Logs all commands
  - `none` - Logs no commands
- `remotesyslog` - Writes to the remote syslog server only

Example: `auditlogging on admin oper`

Sample Log Output: `[2021-11-30T07:02:44-08:00]: EVENT: COMMAND(SHELL 172.30.255.255) USER: admin # AUDITLogging on all`

As a security best practice, full audit logging should be turned on by entering the following command:

```
auditlogging on all
```

Initial Login Process

A user name and password account must be created when the device is accessed for the first time. Using an SSH client, log in by entering `Crestron` and a blank password. To create the account, enter the desired user name and password (the password must be a minimum of 8 characters). Confirm the password by entering the password again. After the account is created, enter the user name and password to log in to the device.

> **NOTE:** Do not lose this information. The system cannot be accessed without it.

Enable All Certificate Verifications

By default, outgoing TLS connections for some protocols will not perform a full set of verifications on the server certificate if it is presented. Enable these verifications by issuing the following command:

```
sslverify all
```

Load Default Server Certificates

The device requires a default server certificate for proper web server operation and to properly secure incoming CIP communications from other devices. Refer to the Required Configuration (on page 6) section for instructions to load the default server certificate and any other needed certificates.

Optional Configuration

The following sections provide information about optional device configuration settings.

Enable or Disable Web Server

All devices have an active web server. If desired, disable the web server with the following command:

```
webserver off
```

To enable the web server, issue the following command:

```
webserver on
```

Enable User Login IP Blocking

To prevent distributed brute force attacks against user logins, the device can automatically block an IP address after a number of failed login attempts from that IP address. This functionality operates independently and simultaneously with the device's User Account Locking capability.

> **NOTE:** Access to an account over the USB port is never blocked.

Change Login IP Failure Count

To change the value for the logon failure count, issue the following command:

```
setloginattempts [number]
```

- `number` - Number of login attempts allowed before the console is blocked. A value of `0` enables unlimited attempts. The default value is `3`.
- No parameter - Displays the current setting

Example: `setloginattempts 3`

Change IP Blocked Time

To change the duration that an IP address is blocked by the console, issue the following command:

```
setlockouttime [number]
```

- `number` - Number of hours to block an IP address. A value of `0` blocks the IP address indefinitely. The maximum value is `255`. The default value is `24`.
- No parameter - Displays the current setting

Example: `setlockouttime 24`

Configure SNMP

The device supports SNMP v2x and v3. To configure an SNMP Manager to access SNMP on this device, it must be added with the `SNMPMANager` command and given access with the `SNMPAccess` command. When using SNMP v3, the SNMP Manager must support EngineID Discovery (RFC 5343) since there is no current way to display the EngineID being used by the device.

Enable or Disable SNMP

To enable or disable SNMP, issue the following command:

```
snmp [enable | disable | wipe]
```

- `enable` - Enables SNMP
- `disable` - Disables SNMP
- `wipe` - Clears the configuration and disables SNMP
- No parameter - Displays the current setting

Example: `snmp enable`

Add or Remove an SNMP Manager

Add information about an SNMP Manager that will be accessing the device or receiving notifications from the device. An SNMP Manager must be added even if the Manager will not be receiving notifications from the device. The Manager can be removed when no longer in use.

To add or remove an SNMP Manager, issue the following command:

```
snmpmanager [add/remove] [name] [community name] [address] [params]
```

- `params` - Specifies one of the following:

  ```
  noauthnopriv-v1
  noauthnopriv-v2
  noauthnopriv-v3
  authnopriv-v3
  authpriv-v3
  ```

  - `auth` = authentication
  - `priv` = privacy

Examples:

```
snmpmanager add testsitemanager testsitename 192.168.0.255 authpriv-v3
```

```
snmpmanager remove testsitemanager
```

For SNMPv2, the `community name` parameter is the SNMP community string. For SNMPv3, the `community name` parameter is used as the SNMPv3 user name. Entering the command with no parameters will list all the SNMP Managers that have been added.

As a security best practice, `authpriv-v3` (full SNMPv3) should be used.

Enable or Disable Unrestricted SNMP Access

By default, SNMP managers sending requests with a community string as the only authentication must send those requests from the IP address indicated when the manager was defined with the `SNMPMANager` command. The following command can be used to remove that restriction by changing the setting to `on`:

```
snmpallowall [on/off]
```

- `on` - Allows all managers
- `off` - Allows only permitted managers
- No parameter- displays current setting

By default, the command is set to `off`.

SNMPv3 requests are not affected by this command. SNMPv3 security is used to control access and does not check IP addresses.

Configure SNMP Access Information

This enables SNMP requests and provides the needed information for an SNMP Manager that has been created with the `SNMPMANager` command.

```
snmpaccess [community] [param] [-a:securitytype -p:password [-e:privacytype [-k:key] ] ]
```

- `param` = readonlyaccess, readwriteaccess, noaccess
- `securitytype` = MD5, SHA
- `privacytype` = DES, AES

The `-a` and `-p` options are required if the SNMP Manager was configured with `authnopriv-v3`, `authpriv-v3`.

The `-e` and `-k` options are required if the SNMP Manager was configured with `authpriv-v3`.

The string passed to the `-p` and `-k` options must be at least 8 characters long.

The `MD5` authentication type and `DES` privacy types are not available when the device is in FIPS 140-2 operation.

Example: `testsitename readwriteaccess -a:sha -p:secretstring1 -e:aes -k:secretstring2`

Enable or Disable SNMP Notifications

Notifications will be sent to all SNMP Managers that have been configured via the `SNMPMANager` and `SNMPAccess` commands. The device currently supports TRAP notifications and does not support INFORM notifications.

To enable or disable SNMP notifications, issue the following command:

```
snmptrap [on|off]
```

- `on` - Enables traps
- `off` - Disables traps
- No parameter- Displays the current setting

Example: `snmptrap on`

Add Users and Groups

It is likely that additional users—either local or via Active Directory® credential management—will need to be given access to the device. Refer to the Optional Configuration (on page 20) section for instructions.

Enable Sending Audit Logs to Remote Syslog Server

Devices do not send audit logs to a remote Syslog server by default. To enable sending to a remote Syslog server, issue the following command:

```
remotesyslog [-s:] {-e:} {-a} [-i:address] [-p:port] {-t:protocol} {-v:on|off}
```

- `-s:on|off` enables or disables remote system error logging
- `-e:ok|info|notice|warning|error|fatal` decides which types of errors are logged. Selecting a tier results in logging errors of that level of importance and above in a hierarchy from `ok` to `fatal`.
  - `ok` - Logs all "OK" errors and above to Syslog
  - `info` - Logs all "info" errors and above to Syslog
  - `notice` - Logs all "notice" errors and above to Syslog (default)
  - `warning` - Logs all "warning" errors and above to Syslog
  - `error` - Logs all "error" errors and above to Syslog
  - `FATAL` - Logs all "fatal" errors and above to Syslog

- `-a log`
  - Accesses Syslog contents of the audit log if remote system error logging is enabled
- `-i:address`
  - Replaces `address` with the remote Syslog server IP address in dot decimal notation or an ASCII string containing the server host name (max 255 characters)
- `p:port`
  - Replaces `port` with the remote Syslog server port number in decimal notation
- `-t:tcp|udp|ssl`
- `-v:on|off`
  - If `ssl` is selected, select `on` to verify the server or `off` to not verify the server. Not entering a parameter displays the current setting.

To test the command, run the following script:

```
rsyslog -s:on -a -i:172.30.144.58 -p:23456 -t:SSL -v:off
```

As a security best practice, the options `-t:ssl` and `-v:on` should be used.

Secure Control System Connection

If this device is connected to another control system, set the user name and password for the control system CIP connection by issuing the following command:

```
setcsauthentication -n:username -p:password
```

- `n` - Specifies name of the user (domain users enter domain\username)
- `p` - Specifies password

Example: `setcsauthentication -n:remotecs -p:randompassword string`

Management Functions

The following sections provide information about device management functions.

Firmware Update

To perform a firmware update:

1. SFTP the .puf firmware file to the **/firmware** location on the device.
2. Enter the `puf <filename>` command in the console, where `<filename>` is the complete filename of the .puf file, including the filename extension.

User and Group Management

Local users and groups can be added to the device after an administrator account has been created. Additionally, the device can grant access levels to existing Active Directory users and groups.

The following sections describe how to manage users and groups on the device.

User Group Rights

The device has built-in access levels representing various roles that can be assigned to a group. These access levels apply to all users within that group. Each access level is associated with a set of specific permissions:

1. Access system information and status (read-only).
2. Connect to the device Web XPanel interface.
3. Authenticate CIP and gateway connections.
4. Receive complete administrator access, including managing user accounts and all system settings.
5. Issue programmer commands for user programs, such as loading programs and related files.
6. Issue operator commands for user programs, such as restarting programs.

The following table indicates the permissions that are given to each of the available access levels. The numbers in the table header row correlate with the numbered list items above.

Default Rights of Local Groups

	1	2	3	4	5	6
Administrator	Yes	Yes	Yes	Yes	Yes	Yes
Programmer	Yes	Yes	Yes	No	Yes	Yes
Operator	Yes	Yes	Yes	No	No	Yes
User	No	Yes	No	No	No	No
Connection Only	No	Yes	Yes	No	No	No

By default, the device has five groups available (one for each access level): Administrator, Programmer, Operator, User, and Connection Only. The initial user is added to the Administrator group. The default groups may be used, or custom groups can be created with the appropriate access level permissions as needed.

Add Local User

To add a local user to the device, issue the following command:

```
adduser -n:username -p:password
```

- `username` - Specifies the name of the local user that is to be created
- `password` - Specifies a password for the local user

Example:`adduser -n:jsmith -p:user01`

A local user is created without access rights. To assign access rights to a local user, the user must be added to at least one local group. For more information, refer to the Add User to Group (on page 30) section.

Delete Local User

To remove a local user from the device, issue the following command:

```
deleteuser username
```

- `username` - Specifies the name of the local user who is to be removed

When a local user is removed, the user is also removed from any local groups.

Add Local Group

To add a local group to the device, issue the following command:

```
addgroup -n:groupname -l:accesslevel
```

- `groupname` - Specifies the name of the local group that is to be created
- `accesslevel` - Specifies the access level for the local group:
  - a - Administrator
  - p - Programmer
  - o - Operator
  - u - User
  - c - Connection only

Example: `addgroup -n:cresprogs -l:p`

> **NOTE:** A predefined access level must be assigned to a group when it is created.

When a user is added to a group, the user inherits the access level set for the group. Certain device functions and console commands are accessible only to users with corresponding access levels.

If a user belongs to multiple groups, the user's access level is the combined access level of all groups that contain the user.

Delete Local Group

To remove a local group from the device, issue the following command:

```
deletegroup groupname
```

- `groupname` - Specifies the name of the local group

When a local user group is removed, users in the group are not removed from the device. However, the user will lose the access rights associated with the removed group.

List Local Groups

Users with administrator privileges can view all local groups added to the device. The device comes with the following built-in groups that cannot be deleted by any user: Administrators, Programmers, Operators, Users, and Connects.

To view a list of all local groups added to the device, issue the following command:

```
listgroups [a] [p] [o] [u] [c]
```

- `a` - Groups with administrator rights are listed
- `p` - Groups with programmer rights are listed
- `o` - Groups with operator rights are listed

- `u` - Groups with user rights are listed
- `c` - Groups with connect-only rights are listed

Example:`listgroups p`

Add Active Directory Group

To add an existing Active Directory group to the device, issue the following command:

```
adddomaingroup -n:groupname -l:accesslevel
```

> **NOTE:** Use the `adlogin` command to log in to the Active Directory server.

- `groupname` - Specifies the name of the Active Directory group to be added
- `accesslevel` - Specifies the access level for the Active Directory group:
  - a - Administrator
  - p - Programmer
  - o - Operator
  - u - User
  - c - Connection only

Example:`adddomaingroup -n:adprogs -l:p`

> **NOTE:** The device cannot create or remove a group from the Active Directory service, but it can grant an access level to an existing Active Directory group.

All users of the Active Directory group inherit the access level set for the group. Certain device functions and console commands are accessible only to users with corresponding access levels.

Remove Active Directory Group

To remove an Active Directory group from the device, issue the following command:

```
deletedomaingroup groupname
```

- `groupname` - Specifies the name of the Active Directory group

When an Active Directory group is removed from the device, it is not deleted from the Active Directory service. Once the group is removed from the device, all members of that group lose access to the device.

List Active Directory Groups

Users with administrator privileges can view all Active Directory groups that were added to the device by issuing the following command:

`listdomaingroups [a] [p] [o] [u] [c]`

- `a` - Active Directory groups with administrator rights are listed
- `p` - Active Directory groups with programmer rights are listed
- `o` - Active Directory groups with operator rights are listed
- `u` - Active Directory groups with user rights are listed
- `c` - Active Directory groups with connect-only rights are listed

Example:`listdomaingroups p`

List Users

To view all users (local and domain) that have been added to local groups, issue the following command:

`listusers`

- No parameter - Lists all users that have been added to local groups

List Group Users

To view all users that have been added to a specific group, issue the following command:

`listgroupusers groupname`

- `groupname` - Specifies the group name that should be queried

Example:`listgroupusers cresprogs`

Show User Information

To view the access rights of a particular user, issue the following command:

`userinformation username`

- `username` - Specifies the user name that should be queried

Example:`userinformation jsmith1`

Add User to Group

To add a local or an Active Directory user to a local group, issue the following command:

```
addusertogroup -n:username -g:groupname
```

- `username` - Specifies the name of the local or Active Directory user
- `groupname` - Specifies the name of the local group

Example:`addusertogroup -n:jsmith1 -g:cresprogs`

Local users are created on the device without any access rights. Adding a user to a local group grants the user the access level assigned to the group.

> **NOTE:** The device cannot create or remove a user from the Active Directory service, but it can grant an access level to an existing Active Directory user. This may be accomplished either by adding the Active Directory user to a local group on the device or by adding the Active Directory group(s) of which the user is a member to the device.

Remove User from Group

To remove a local or an Active Directory user from a local group, issue the following command:

```
removeuserfromgroup -n:username -g:groupname
```

- `username` - Specifies the name of the local or Active Directory user
- `groupname` - Specifies the name of the local group

Example:`removeuserfromgroup -n:jsmith1 -g:cresprogs`

Update Local Password

To update the current user's password, issue the following command:

```
updatepassword
```

Users may update their password. The user is prompted to enter the current password once and the new password twice. If the old password does not match the current password, the operation fails and the password is not changed.

Reset User Password

To reset a user's password, issue the following command:

```
resetpassword -n:username -p:defaultpassword
```

- `username` - Specifies the user whose password will be reset
- `defaultpassword` - Specifies a default password that can be provided to the user following the reset

Example:`resetpassword -n:jsmith1 -p:Default321!`

User Login IP Blocking Management

When User Login IP Blocking is enabled and a user reaches the maximum number of login attempts over an Ethernet connection, the client's IP address is blocked. Administrators have access to commands that allow them to manage the blocked IP addresses, including manually blocking and unblocking IP addresses.

List Blocked IP Addresses

To view all blocked IP addresses, issue the following command:

`listblockedip`

- No parameter - Lists all blocked IP addresses

Add IP Address to Blocked List

To add an IP address to the blocked list manually, issue the following command:

`addblockedip [ipaddress]`

- `ipaddress` - Enter the IP address that is to be blocked
- No parameter - Lists all blocked IP addresses

Example: `addblockedip 255.255.255.255`

Remove IP Address from Blocked List

To remove an IP address from the blocked list manually, issue the following command:

`remblockedip [ALL|ipaddress]`

- `ipaddress` - Enter the IP address that will be removed from the blocked list
- `ALL` - Remove all blocked IP addresses
- No parameter - Lists all blocked IP addresses

Example: `remblockedip 255.255.255.255`

User Account Locking Management

When User Account Locking is enabled and a user reaches the maximum number of login attempts, the user account is locked. Administrators have access to commands that allow them to manage the user accounts, including manually locking and unlocking accounts.

Add User to Locked List

To add a user to the locked list, issue the following command:

```
addlockeduser [name]
```

- `name` - Specifies the user account that is to be locked.
- No parameter - Lists all locked user accounts

Example:`addlockeduser jsmith1`

Remove User from Locked List

To remove a user from the locked list, issue the following command:

```
remlockeduser [name]
```

- `name` - Specifies the user account that is to be removed from the locked list.
- No parameter - Lists all locked user accounts

Example:`remlockeduser jsmith1`

List Locked User

To view a list of locked user accounts, issue the following command:

```
listlockeduser
```

- No parameter - Lists all locked user accounts

Certificate Management

X.509 certificates are used for a number of purposes by the device, including authentication by various protocols. These certificates can be added, removed, and managed from the console. It is important to understand the different kinds of certificates, their purpose, and how to install and configure each of them.

The device supports three basic types of certificates:

- **Trust Certificates:** These certificates are used to determine whether certificates presented by other entities are trusted. There are two types of trust certificates: Root and Intermediate. Both types serve the same purpose.
- **Server Certificates:** A server certificate is a certificate presented by a protocol when acting as a server to prove its identity. Clients connecting to that server will verify that server certificate. Server certificates loaded onto the device must also load the associated private key for that certificate since the private key is required as part of the process of proving identity.
- **Client Certificates:** A client certificate is a certificate presented by a protocol when acting as a client to prove its identity. When a client connects to a server, that server will verify that client certificate. Client certificates loaded onto the device must also load the associated private key for that certificate since the private key is required as part of the process of proving identity.

> **NOTE:** There are some certificates that can be both a server and client certificate and, therefore, can be used for either purpose.

The device stores certificates by category based upon how they are used:

- **Root:** These are the default Trust Certificates to which the device will verify server certificates against when acting as a TLS client. Root certificates are the start of a certificate chain and can be identified by the Issuer and Subject fields of the certificate being the same. The device may use an alternate list of trusted certificates for certain protocols or use cases but, unless specifically indicated, this Root store will be used.
- **Intermediate:** This is identical to the Root category, except that this store contains only intermediate certificates, which are Trust Certificates that were signed by another certificate (the Issuer field will be different than the Subject field). The default list of trusted certificates is the combination of all the Root and Intermediate certificates.
- **Default Server:** This category contains a single server certificate and is the default server certificate. This must include a private key. If a server certificate is needed by the device, and none is specifically loaded for a particular purpose, then this one will be used. This certificate cannot be loaded by the standard certificate management commands, but is instead loaded by special commands and is required as part of activating full authentication on the device. Refer to the Default Server Certificate (on page 37) section for more information.

- **Machine:** This category contains a single client certificate and is used only for 802.1X, and only when EAP-TLS authentication is chosen. This must include a private key.
- **Web Server:** This category contains a single server certificate and is the server certificate used by the web server. This must include a private key. If no web server certificate is loaded, the default server certificate will be used.

Certificate Requirements

The device supports standard X.509v3 certificates. The following algorithms are supported for the public key and signatures:

- **RSA**: Key lengths of 2048, 3072, or 4096 bits
- **ECC**: secp256r1, secp384r1, and secp521r1
- **Hash**: SHA-1, SHA-256, SHA-384, or SHA-512

Certificate Signing Request (CSR) generation for the default server certificate can only generate a 2048 bit RSA key and can only use a SHA-256 hash for its signature.

Certificate Commands

The following sections provide information about commands that allow the user to add, remove, and show certificates. These commands do not apply to the default server certificate.

Add a Certificate (Fixed File Name)

To add a certificate that has a predefined file name, load the certificate file into the **/cert** directory on the device using SFTP. The file must have the file name specified below, depending on the type of certificate.

```
certificate add <certificate store> [password]
```

- `certificate store` - Specifies the category name indicating the purpose of the certificate: `root`, `intermediate`, `machine`, or `webserver`.
- `password` - Specifies the password required to access a private key in the file. It is optional and only used when a password-protected private key is included in the file.

Example:`certificate add intermediate`

The file name to use along with the format and contents of the certificate file all depend on the category chosen:

- `root`: The file must be named **root_cert.cer** and must be in standard pem format. It should only contain a root certificate.
- `intermediate`: The file must be named **intermediate_cert.cer** and must be in standard pem format. It should only contain an intermediate certificate.

- `machine`: The file must be named **machine_cert.pfx** and must be in standard PKCS #12 format. It should only contain a client certificate and its associated private key. If a password is needed to access the file, it must be provided as part of the command.
- `webserver`: The file must be named **webserver_cert.pfx** and must be in standard PKCS #12 format. It should only contain a server certificate and its associated private key. If a password is needed to access the file, it must be provided as part of the command. Make sure to load the web server certificate's signing chain into the Root and Intermediate Trust stores before loading the web server certificate itself. If the signing chain is not present, loading of the web server certificate will fail. If that signing chain is not available, or loading it into the device is not desired, disable the verification check prior to loading the web server certificate by issuing the `sslverify -s:off` command.

Certificates are stored by category, which must be specified when using any of the standard certificate management commands.

Add a Certificate (Specified File Name)

To add a certificate that has a user-defined file name, the command is identical to the previous command for loading certificates with a fixed file name—the only difference is that the file name to be used is specified as part of the command. Load the certificate file into the **/cert** directory on the device using SFTP. The file must have the file name specified below, depending on the type of certificate.

```
certificate addf <certificate name> <certificate store> [password]
```

- `certificate name` - Specifies the file name containing the certificate
- `certificate store` - Specifies the category name indicating the purpose of the certificate: `root`, `intermediate`, `machine`, or `webserver`
- `password` - Specifies the password required to access a private key in the file. It is optional and only used when a password-protected private key is included in the file.

Example:`certificate addf device-server.pfx webserver secretpass`

The format and contents of the certificate file depend on the category chosen:

- `root`: The file must be in standard pem format. It should only contain a root certificate.
- `intermediate`: The file must be in standard pem format. It should only contain an intermediate certificate.
- `machine`: The file must be in standard PKCS #12 format. It should only contain a client certificate and its associated private key. If a password is needed to access the file, it must be provided as part of the command.
- `webserver`: The file must be in standard PKCS #12 format. It should only contain a server certificate and its associated private key. If a password is needed to access the file, it must be provided as part of the command. Make sure to load the web server certificate's signing chain into the Root and Intermediate Trust stores before loading the web server certificate itself. If the signing chain is not present, loading of the web server certificate will fail. If the signing chain is not available, or loading it into the device is not desired, disable the verification check prior to loading the web server certificate by issuing the `sslverify -s:off` command.

Remove a Certificate

To remove a certificate from the device, issue the following command:

```
certificate rem <certificate store> [certificate number] [certificate name]
[certificate uid]
```

- `certificate store` - Specifies the category name indicating the purpose of the certificate: `root`, `intermediate`, `machine`, or `webserver`
- `certificate number` - Specifies the number that identifies the specific certificate to remove
- `certificate name` - Specifies the name that identifies the specific certificate to remove
- `certificate uid` - Specifies the UID that identifies the specific certificate to remove

Example:`certificate rem intermediate 1`

Only one identifier (number, name, or UID) is needed. These identifiers can be determined by listing the certificates using the command described below.

View a Certificate

To view additional details about a certificate, issue the following command:

```
certificate view <certificate store> [certificate number] [certificate name]
[certificate uid]
```

- `certificate store` - Specifies the category name indicating the purpose of the certificate: `root`, `intermediate`, `machine`, or `webserver`
- `certificate number` - Specifies the number that identifies the specific certificate to view
- `certificate name` - Specifies the name that identifies the specific certificate to view
- `certificate uid` - Specifies the UID that identifies the specific certificate to view

Example:`certificate view intermediate 1`

Only one identifier (number, name, or UID) is needed. These identifiers can be determined by listing the certificates using the command described below.

List Certificates

To show the list of certificates loaded in the device for a specific category, issue the following command:

```
certificate listn <certificate store>
```

- `certificate store` - Specifies the category name indicating the purpose of the certificate: `root`, `intermediate`, `machine`, or `webserver`

Example:`certificate listn root`

The certificates will be listed with their name and identifiers, which can be used for the remove and view commands.

Default Server Certificate

The default server certificate must be loaded into the device in order for clients to properly authenticate TLS connections.

Make sure to load the default server certificate's signing chain into the Root and Intermediate Trust stores before loading the default server certificate itself. If the signing chain is not present, loading of the default server certificate will fail. If the signing chain is not available, or loading it into the device is not desired, disable the verification check prior to loading the default server certificate by issuing the `sslverify -s:off` command.

Prior to a default server certificate being loaded, a certificate that is self-signed and self-generated by the device will be used as the default server certificate.

Load Default Server Certificate and Enable Authentication

To load the default server certificate of the device, issue the following command:

```
ssl [off | self | ca [-p:privatekeypassword]]
```

- `off` - No effect, TLS cannot be turned off
- `self` - Reverts to using the self-signed and self-generated certificate
- `ca` - Loads the default server certificate and enables use of the certificate
- `p:privatekeypassword` - Indicates that the private key associated with the default server certificate is password protected and specifies the password that should be used to access it

Example:`ssl ca`

As a security best practice, a default server certificate should be loaded by issuing the `ssl ca` command.

After issuing the SSL command, the device must be rebooted in order for the changes to take effect.

If the private key is protected by a password and the `-p` option is not provided, the command will ask for the password interactively.

To replace the existing default server certificate with a new one, issue the `ssl ca` command again.

When the `ssl ca` command is executed, the default server certificate information must be in a specific location in specific file names. Some information may also need to be installed using the standard certificate management commands. The following requirements for this information must be met before executing the `ssl ca` command:

- All information related to the default server certificate must be broken up into separate files. This means one file for the server certificate, one file for the private key, one file for the root certificate, and one file for each intermediate certificate. If a CSR was generated on the device (see instructions below), no private key file will be needed because it is already on the device.
- Load the intermediate certificates into the intermediate store using the `certificate add` or `certificate addf` command as described above in the standard certificate management commands.
- Load the root certificate into a filed named **rootCA_cert.cer** in the **/sys** directory of the device using SFTP. The file must be in standard pem format. Because the **/sys** directory is not directly accessible via SFTP, transfer the file to the **/user** directory and use the `move` command to move the file to the **/sys** directory (for example. `move /user/rootCA_cert.cer /sys/rootCA_cert.cer`). It is recommended to use the `delete` command to delete any existing file with that name in the **/sys** directory (for example, `delete /sys/rootCA_cert.cer`).
- Load the server certificate into a filed named **srv_cert.cer** in the **/sys** directory of the device using SFTP. The file must be in standard pem format. Because the **/sys** directory is not directly accessible via SFTP, transfer the file to the **/user** directory and use the move command to move the file to the **/sys** directory (for example, `move/user/srv_cert.cer /sys/srv_cert.cer`). It is a recommended to use the `delete` command to delete any existing file with that name in the **/sys** directory (for example, `delete /sys/srv_cert.cer`).
- Load the private key for the server certificate into a filed named **srv_key.pem** in the /sys directory of the device using SFTP. The file must be in standard pem format. Because the **/sys** directory is not directly accessible via SFTP, transfer the file to the **/user** directory and use the `move` command to move the file to the **/sys** directory (for example, `move /user/srv_key.pem /sys/srv_key.pem`). It is recommended to use the `delete` command to delete any existing file with that name in the **/sys** directory (for example, `delete /sys/srv_key.pem`). As previously noted, if the device generated a Certificate Signing Request (CSR) for this certificate, no private key is needed because it is already on the device.

The `ssl CA` command can then be issued and the device can be rebooted.

Generate a Certificate Signing Request (CSR)

The device has the capability to generate a CSR for the default server certificate. This CSR is limited to using a 2048-bit RSA key pair and a SHA-256 hash for its signature. If any of the other algorithms supported by the device are required, do not generate the CSR with the device. Instead, generate the CSR externally and load the private key with the certificate.

To generate a CSR, issue the following command:

```
createcsr c:st:l:o:ou:cn:e [-i:<option>] [-s:<altname>[,<altname>],...]
```

- `c` - Two-letter country code
- `st` - State or province name
- `l` - Locality or city name
- `o` - Organization or company name
- `ou` - Organizational unit name or division
- `cn` - Site name or domain name
- `e` - Email address
- `-i` - Ignores blank parameters. <option> is `true` or `false`.
- `-s` - Subject Alternative Name parameter(s); <`altname`> is a type:value; valid types are `DNS`, `IP`, `email`, `URI`

> **NOTE:** Values that contain spaces must be enclosed in quotation marks.

Example:`createcsr us:nj:rockleigh:"Crestron Electronics"::device.crestron.com: -i:true -s:dns:altname.crestron.com,ip:192.168.0.1`

Be aware that generating a CSR will overwrite any previous CSR and private key, rendering that previous CSR useless. It will not affect any certificate and private key in use that may have been loaded.

Only the `ou` and `e` fields may be left blank and not included in the CSR by specifying the `-i:true` option. Other fields are not affected by the `-i` option and will always be included in the CSR. If the `-i:true` option is not specified, the `ou` and `e` fields will also always be included in the CSR, even if left blank. Fields that are left blank, but still in the CSR, will be set to default values. Because these default values are not likely to be accurate for most environments, it is recommended to always fill in all fields except `ou` and `e`, use the `-i:true` option, and fill in `ou` and `e` if needed.

Once generated, the CSR can be retrieved using SFTP. The CSR will be stored in a file named **request.csr** in the **/sys** directory of the device. Because the **/sys** directory is not directly accessible via SFTP, move the file to the **/user** directory and transfer the file from there (for example, `move /sys/request.csr /user/request.csr`). It is recommended to use the `delete` command to delete any existing file with that name in the **/user** directory (for example, `delete /user/request.csr`).

Additional Instructions

The instructions in this section are not specific to this device. However, they may be useful to an administrator when setting up and configuring the device.

Use OpenSSL to Create a Certificate Signing Request (CSR)

In most cases, a CSR must be provided to a certificate signing authority to receive a signed certificate. When requesting a signed certificate for this device, you may not want to or be able to generate the CSR on the device itself. In these cases, OpenSSL may be used to create the CSR.

This process can be accomplished by following these instructions on any Windows® or Linux® OS-based computer with OpenSSL version 1.0.2 or newer installed. As a security best practice, ensure that the version of OpenSSL installed is FIPS 140-2 certified.

> **NOTE:** In the following instructions, the example file names include a generic *name* descriptor. It is recommended to replace *name* with a string that identifies the device that will receive the requested certificate so you can more easily match the certificate files with the appropriate device.

Create a Configuration File

First, a configuration file that will be used to generate the CSR must be created. This file will contain information about the CSR and any information that should be included in the CSR.

Create a text file called *name*-csr-openssl.cnf with the following contents:

```
# OpenSSL configuration file for CSR generation

# CSR configuration - Change sha256 to alternate hash function if desired
[ req ]
default_md          = sha256
distinguished_name  = req_distinguished_name
string_mask         = utf8only
utf8                = yes
prompt              = no
req_extensions      = req_ext

# Extensions to be included - Currently SAN only
[req_ext]
subjectAltName = @alt_names

# Information to put in certificate Subject field - fill in desired values
# Comment out any items not desired (only commonName is required)
[ req_distinguished_name ]
commonName                      = Device.Fully.Qualified.Domain.Name
countryName                     = optional
stateOrProvinceName             = optional
localityName                    = optional
0.organizationName              = optional
organizationalUnitName          = optional
emailAddress                    = optional

# List of information to put in SAN extension - fill in desired values
# Additional names or IP addresses can be added if necessary
[ alt_names ]
DNS.1 = Device.Fully.Qualified.Domain.Name
```

Modify the text file to include the information specific to the device and the network site. This information will be put into the Subject field of the certificate and is specified in the `[ req_distinguished_name ]` section of the text file. The `commonName` entry must be filled in and should be the FQDN of the device.

All other fields are optional and should be filled in or commented out (if not commented out, the certificate will contain "optional" as the value of that field). Note that the `countryName` field is only allowed to be 2 characters.

The following example shows a sample of this section containing filled and empty fields:

```
[ req_distinguished_name ]
commonName                      = deviceName.crestron.com
countryName                     = US
stateOrProvinceName             = NJ
localityName                    = Rockleigh
0.organizationName              = Crestron Electronics
#organizationalUnitName          = optional
#emailAddress                    = optional
```

This CSR will also request the standard Subject Alternate Name (SAN) extension to be included in the certificate. The information to include in this extension is specified in the `[ alt_names ]` section of the text file. At least one entry is required, and that entry should match the FQDN specified in the `commonName` field above.

Add additional names that may be used when connecting to the device. Each additional name must use an incremented number in the suffix for the "DNS" identifier. IP addresses are also supported if needed.

The following example shows a sample of this section filled out for a device with three names and two IP addresses:

```
[ alt_names ]
DNS.1 = deviceName.crestron.com
DNS.2 = alternateName.crestron.com
DNS.3 = thirdname.crestron.com
IP.1 = 192.168.0.10
IP.2 = 10.0.0.5
```

Finally, if your certificate signing authority requires the CSR to be signed with a stronger hash than SHA256, the `default_md` field in the `[ req ]` section can be changed. Change `sha256` to `sha384` or `sha512` as needed.

Generate the Private Key

Generate a 2048 bit RSA key by issuing the following command:

```
openssl genrsa -out name.key.pem 2048
```

If desired, replace the `2048` parameter with `3092` or `4096` to generate a longer key of that length.

Create the CSR

Create the CSR using the key and information in the configuration file:

```
openssl req -config name-csr-openssl.cnf -key name.key.pem -new -out
name.csr.pem
```

If you wish to view the CSR in text form to confirm it contained the expected information, use the following command:

```
openssl req -noout -text -in name.csr.pem
```

Create and Sign the Certificate

The certificate must be created and signed by the trusted signing authority for the network the device will be used on. Provide the CSR file (name.csr.pem) to your signing authority to create and sign the certificate. The signing authority should return the signed certificate along with the signing chain for that certificate.

Load the Certificate

To load the certificate as the Default Server Certificate, use the *name*.key.pem file that was created, along with the server certificate and signing chain from the signing authority, and follow the instructions provided in the Required Configuration (on page 6) and Required Configuration (on page 6) topics.

If you wish to load the certificate as the Web Server certificate, the certificate and key must be placed into a PKCS #12 file. Ensure that the certificate provided by the signing authority is in PEM format, and then issue the following command, where *name*.cert.pem is the file from the signing authority with the certificate in PEM format.:

```
openssl pkcs12 -export -out name.certandkey.pfx -inkey name.key.pem -in
name.cert.pem
```

OpenSSL will ask for an "Export Password". Enter a password which will be used to protect the PKCS #12 file. It will then ask you to confirm that password.

Next, follow the instructions in Required Configuration (on page 6) for loading a Web Server certificate. Make sure to provide the Export Password that was entered above when loading the certificate file into the device.

Clean Up

Once successfully loaded onto the device, wipe the local copy of the private key (in the file *name*.key.pem) on the computer used to generate the CSR, as this contains the secret information specific to that certificate for that device.

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

Security Reference Guide — Doc. 9063C

05/19/22
Specifications subject to
change without notice.