Security Reference Guide

TS-80, TSS-80, and TSW-80

80 Series Touch Screens

Crestron Electronics, Inc.

Have feedback on this document? Contact docfeedback@crestron.com.

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

This product is licensed under the Crestron Software End-User License Agreement, available at www.crestron.com/Legal/software-license-agreement/Crestron-Software-End-User-License-Agreement.

Crestron product development software is licensed to Crestron dealers and Crestron Service Providers (CSPs) under a limited nonexclusive, nontransferable Software Development Tools License Agreement. Crestron product operating system software is licensed to Crestron dealers, CSPs, and end-users under a separate End-User License Agreement. Both of these Agreements can be found on the Crestron website at www.crestron.com/legal/software_license_agreement.

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

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

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

Certain Crestron products collect information that may include personal data. For further details regarding those Crestron products that collect, process, and transmit information directly to Crestron via the internet, refer to the Crestron Privacy Statement Regarding Internet Data Collection, located at www.crestron.com/legal-data-collection-privacy.

Crestron, the Crestron logo, Crestron Home, Crestron Toolbox, and XiO Cloud are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Azure and Microsoft Teams are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Android is either a trademark or registered trademark of Google Inc. in the United States and/or other countries. Wi-Fi is either a trademark or registered trademark of Wi-Fi Alliance in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.

©2026 Crestron Electronics, Inc.

Revision History

Rev	Date	Notes
A	July 31, 2026	Initial version

Send comments and change recommendations to SecurityDocs@crestron.com.

Contents

Introduction 1
Security Policies 2
Prerequisites 3
Intended Operational Environment 3
Device Access 3
Default Configuration Settings 3
System Specifications 4
Product Software - Security Features 4
User Authentication 4
Connectivity 4
Software Updates and Patches 4
Operating System 5
Network Configuration 5
Third-Party Software 5
Network Infrastructure 6
Network Port List 6
Crestron Control Devices 6
Common Ports 6
Required Configuration 8
DHCP or Static IP Address Configuration 8
802.1X Authentication 8
802.1X Configuration 9
Set Password Policy 11
Set Date and Time 12
Disable Auto Discovery 13
Disable Cloud Features 13
Enable User Account Locking 13
Change Login Failure Count 14
Change Lockout Time 14
Display Last Logged-In Information 14
Enable Session Inactivity Timeout 14
Enable Audit Logging 15
Initial Login Process 15
Enable All Certificate Verifications 16
Load Web Server Certificates 16
Optional Configuration 17
Enable or Disable Web Server 17

Enable User Login IP Blocking 17
Change Login IP Failure Count 17
Change IP Blocked Time 17
Configure SNMP 18
Enable or Disable SNMP 18
Add or Remove an SNMP Manager 18
Enable or Disable Unrestricted SNMP Access 18
Configure SNMP Access Information 19
Enable or Disable SNMP Notifications 19
Domain-Joined Authentication and Authorization 20
Secure Control System Connection 20

Management Functions 21

Firmware Update 21
User Login IP Blocking Management 21
List Blocked IP Addresses 21
Add IP Address to Blocked List 21
Remove IP Address from Blocked List 21
User Account Locking Management 22
Add User to Locked List 22
Remove User from Locked List 22
List Locked User 22
Certificate Management 22
Certificate Requirements 23
Certificate Commands 23
Add a Certificate (Specified File Name) 24
Remove a Certificate 25
View a Certificate 25
List Certificates 26
Backup and Restore Functionality 26

Security Controls 28

Malware and Vulnerability Protection 28
Vulnerability Protection 28
Remote Connectivity 28
Role-Based Access Control 28
Password Security 28
Data Segregation 29
Cloud Storage 29
Physical Protection 29
Audit Logging 29
Data Protection 29
Security Best Practices 29
More Security Information 30

Introduction

This guide serves as a security reference and provides best practices for hardening the 80 Series touch screens, which are touch screens designed for government, residential, and enterprise applications. The 80 series touch screens feature a capacitive display with custom programmable control buttons, support for HTML5-based custom UI projects, and can integrate seamlessly with a variety of popular scheduling services.

NOTES:

- The term "device" is used in this document to refer to all applicable touch screen models unless specified otherwise.
- Some security features are model dependent.

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

Model	Description
TS-880-B	8.1 in. Tabletop Touch Screen, Black
TS-880-W	8.1 in. Tabletop Touch Screen, White
TS-880R-B	8.1 in. Tabletop Touch Screen, Crestron Home® OS Version, Black
TS-880R-W	8.1 in. Tabletop Touch Screen, Crestron Home® OS Version, White
TS-880-GV-B	8.1 in. Tabletop Touch Screen, Government Version
TS-1080-B	10.1 in. Tabletop Touch Screen, Black
TS-1080-W	10.1 in. Tabletop Touch Screen, White
TS-1080R-B	10.1 in. Tabletop Touch Screen, Crestron Home® OS Version, Black
TS-1080R-W	10.1 in. Tabletop Touch Screen, Crestron Home® OS Version, White
TS-1080-GV-B	10.1 in. Tabletop Touch Screen, Government Version
TS-1080-UC-B	10.1 in. Tabletop Touch Screen, Unified Communication Version
TSS-880-B	8.1 in. Room Scheduling Touch Screen, Black
TSS-880-W	8.1 in. Room Scheduling Touch Screen, White
TSS-880-GV-B	8.1 in. Room Scheduling Touch Screen, Government Version
TSS-1080-B	10.1 in. Room Scheduling Touch Screen, Black
TSS-1080-W	10.1 in. Room Scheduling Touch Screen, White
TSS-1080-GV	10.1 in. Room Scheduling Touch Screen, Government Version
TSW-880-B	8.1 in. Wall Mount Touch Screen, Black
TSW-880-W	8.1 in. Wall Mount Touch Screen, White

Model	Description
TSW-880R-B	8.1 in. Wall Mount Touch Screen, Crestron Home® OS Version, Black
TSW-880R-W	8.1 in. Wall Mount Touch Screen, Crestron Home® OS Version, White
TSW-880-GV-B	8.1 in. Wall Mount Touch Screen, Government Version
TSW-1080-B	10.1 in. Wall Mount Touch Screen, Black
TSW-1080-W	10.1 in. Wall Mount Touch Screen, White
TSW-1080R-B	10.1 in. Wall Mount Touch Screen, Crestron Home® OS Version, Black
TSW-1080R-W	10.1 in. Wall Mount Touch Screen, Crestron Home® OS Version, White
TSW-1080-GV-B	10.1 in. Wall Mount Touch Screen, Government Version
TSW-1080-UC-B	10.1 in. Wall Mount Touch Screen, Unified Communication Version

Security Policies

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

Prerequisites

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

Intended Operational Environment

The 80 series touch screens are designed for installation in various commercial, enterprise, and residential spaces. Once installed, the touch screens connect over Ethernet or Wi-Fi® communications.

Crestron assumes the following about the 80 series operating environment:

- The device is not capable of Multi-Factor Authentication (MFA).
- 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.

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 server is disabled by default and can be enabled through the web configuration interface. For more information on accessing the web interface, refer to the TSS-880 and TSS-1080 Product Manual.

The device also provides local setup pages for commonly used configuration settings. The local setup pages can be accessed by placing five fingers on the touch screen display and holding for approximately 15 seconds.

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`

System Specifications

For general product specifications, refer to the 80 series product pages.

Product Software - Security Features

The following security features are supported for the product software.

User Authentication

The first time the web configuration interface is accessed, a page is displayed asking the user to create an admin account. The admin account credentials are required for accessing the device web configuration interface. An admin account can also be created using the Setup Wizard on the touch screen.

For the local setup pages, the admin account credentials must be entered before accessing the Ethernet and Wi-Fi configuration settings or the restore option in the setup pages.

A user profile must be created if accessing the Setup Wizard from the touch screen. Groups and users can be created and managed using the device web configuration interface.

Connectivity

The 80 series touch screens can connect to various enterprise scheduling applications as well as the XiO Cloud® provisioning and management system for monitoring, configuration, and scheduling functionality.

For more information on the security features provided by the XiO Cloud service, refer to the XiO Cloud Service Security Reference Guide.

For more information on the security features provided by the Microsoft Teams® software app, refer to the Microsoft Teams security page.

The 80 series touch screens support the following encryption and secure connection features:

- WPA2/WPA3 Personal and WPA2 Enterprise encryption for Wi-Fi networks
- HTTP/HTTPS proxy
- SNMP
- IEEE 802.1x authentication

Software Updates and Patches

Crestron is responsible for providing updates and security patches for the 80 series touch screens when necessary via firmware updates. The customer is responsible for running any firmware updates. The customer is also responsible for any custom security configurations and update management.

Operating System

The 80 series touch screens use a custom-built Android™ operating system. Configuration of the operating system is not required.

Network Configuration

The 80 series operating system is configured with the following settings. Additional actions may be taken where applicable:

- **DHCP**: A standard DHCP configuration is provided.
- **Wi-Fi® Communications**: Wi-Fi communications are turned on in the Android OS.
- **Unneeded Ports**: Any ports besides those listed on Network Infrastructure on page 6 are disabled
- **Unneeded Applications**: All unnecessary applications have been removed from the Android OS for the product (such as launcher, camera, and browser).

Third-Party Software

All third-party and open source software and licenses used in Crestron applications are detailed in the EULA included with the device.

The 80 series includes support for various third-party scheduling applications. New providers are made available via firmware updates. The selected app downloads from the cloud and installs on the touch screen without any programming or control system required. The devices run only one app at a time, which is selected using the XiO Cloud service or the web configuration interface. Only the apps approved and delivered by Crestron can run on the touch screen. An internet connection is required.

Network Infrastructure

The following section describes the network infrastructure for the TS-80, TSS-80, and TSW-80.

Network Port List

The following ports are in use on the TS-80, TSS-80, and TSW-80:

Crestron Control Devices

Function	Destination Port	From (Sender)	To (Listener)	Notes
Crestron CIP	41794/TCP	Device	Control	Crestron Internet Protocol System
Crestron SCIP	41796/TCP	Device	Control System	Secure Crestron Internet Protocol

Common Ports

Function	Destination Port	From (Sender)	To (Listener)	Notes
SSH/SFTP	22/TCP	Admin Workstation	Device	Used for configuration, console, and file transfer
HTTPS	443/TCP	Admin or End User Workstation	Device	Secure access to web configuration interface
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 Web Sockets. HTTPS services such as routing lookups and file transfers may be used.

Function	Destination Port	From (Sender)	To (Listener)	Notes
DNS	53/TCP and UDP	DNS Server	Device	Domain name service
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
HTTP	80/TCP	Device	End User Workstation	Typically uses port 80 but will use URL (and optional port number) from certificate

Required Configuration

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

DHCP or Static IP Address Configuration

The following settings must be configured to allow the device to communicate on a LAN. 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. These configuration settings may be set through the local setup pages or by connecting the device to a network which supports DHCP, and then setting them through the web pages or SSH console. If using the console, the network information can be configured by using the following commands:

```
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 only by attaching the device to a temporary network that 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 certificate into the device. These may be Root or Intermediate certificates.
- If EAP-TLS authentication is going to be used, a client certificate will be needed and must be loaded into the device.

Once 802.1X configuration is complete, restart the device to activate those settings. The device will attempt 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` - 802.1Xis enabled
- `off` - 802.1Xis disabled
- No parameter - Displays the current setting

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` commands 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` commands 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 connected to the device:

- 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 allowed: ` ~ ! @ $ % ^ & * ( ) _ + = { }[ ] | ; " <>, .

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

Crestron devices use NTP to synchronize their clocks. 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 UTC (code 000). 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.

Disable Auto Discovery

All devices support an auto discovery 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
```

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.

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 an IP address. 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 do 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 console, web, and local setup page 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

Crestron 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`

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 the setup wizard or the web configuration interface, log in by entering an admin username and 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.

For more information on accessing the setup wizard or the web interface, refer to the TSS-880 and TSS-1080 Product Manual.

NOTES:

- Do not lose this information. The system cannot be accessed without it.
- The SSH server is disabled by default and can be enabled through the web configuration interface.

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 Web Server Certificates

The device requires a web server certificate for proper web server operation and to properly secure incoming CIP communications from other devices.

For more information on managing web server certificates, refer to Certificate Management on page 22 and the TSS-880 and TSS-1080 Product Manual.

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 webserver, 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.

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 5.
- 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 (suffix `h`) or minutes (suffix `m`) to block an IP address. A value of 0 specifies an indefinite amount of time. The maximum amount of time is `750h` (hours) or `45000m` (minutes). The default value is `30m`.
- No parameter - Displays the current setting

Example: `setlockouttime 24h`

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 SNMPv3, the SNMP Manager must support EngineID Discovery (RFC5343) 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
```

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 wasconfigured 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

Domain-Joined Authentication and Authorization

This section describes domain-joined user authentication and authorization (A/A). This enhancement makes the original implementation of Active Directory® service user login more secure by restricting login-related interactions to the following:

- Crestron devices that are known by a domain.
- Domains that are known by Crestron devices.

When comparing domain-joined A/A with legacy Active Directory (AD), there are a few key similarities and differences:

- There is no change in how users and domain groups are configured with either approach.
- Legacy AD does not require any device-identifying or device-authenticating configuration on either the domain side or the device itself. Domain-joined A/A requires configuration of both.
- Legacy AD supports only Active Directory, while domain-joined A/A supports Active Directory and Remote Authentication Dial-In User Service (RADIUS). It also provides a framework for other A/A methods in the future.

Legacy AD has been deprecated since the introduction of domain-joined A/A, though Crestron devices will support both types for the foreseeable future. Only one of the two types can be active at any given time.

Secure Control System Connection

If this device is connected to a 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 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

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.
- **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.

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 Commands

The following sections provide information about commands that allow the user to add, remove, and show certificates.

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 **namedroot_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 webserver 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 webserver 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 webserver 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.

Backup and Restore Functionality

Crestron products provide users with the ability to back up and restore configuration information for a product.

- This functionality is currently supported only using the console interface.
- A configuration backed up on a certain device type can only be restored on the same device type.
- The configuration file generated is password protected. The following password rules apply:
  - The password must be less than 128 characters.
  - The string must be double quoted if it contains spaces.
  - Printable characters including spaces (with the exception of the single quote character) are permitted.
- If the directory option is given for `exportall`, then the same directory option must be given for `importall`.

> **NOTE:** A backup can be created only when there are no user programs running on the control system. To stop all programs, issue the `stopprog-p:all` command.

To use the backup and restore function, issue the following command:

```
configutils [exportall|importall] [-p[:password]] [-d:directory]
```

- `exportall` - Exports all data settings to the device firmware folder.
- `importall` - Imports all data settings from the device firmware folder.
- `-f` - Add to not prompt for an import.
- `-p[:password]` - Password to encrypt data. If a password is not provided, the console will prompt to enter it.
- `-d[:directory]` - An alternate directory to store the backup.

Example: `configutils importall-p:password`

CAUTION: Issuing `configutils importall` will restart the device.

Security Controls

Crestron devices use industry standards like Build Security in Maturity Model (BSIMM) benchmarks, Open Group ACS Trusted Technology Provider Framework, and NIST when considering security.

The following sections describe additional details regarding security controls on the TS-80, TSS-80, and TSW-80.

Malware and Vulnerability Protection

The 80 Series touch screens provide the following malware and vulnerability protections.

Vulnerability Protection

If vulnerabilities or other issues are found, a patch will be made available to customers. If the patch is not urgent, the Crestron support team will work with the customer to identify a time to apply the patch. If the patch fixes a critical vulnerability, the customer will be informed when the patch will be applied.

Upon identifying an attack, immediate steps will be taken to close access as soon as possible. Once the attack is halted, forensic analysis will be taken to identify any customer data that may have been accessed. Customers will then be alerted about the impact of the attack and any of their data that may have been accessed.

Remote Connectivity

This device can be accessed and configured by using a web browser. Additionally, some aspects of configuration can be performed via the XiO Cloud® service. Remote user activities are logged by Crestron and may be reviewed as needed. No third parties are granted access to this information.

Role-Based Access Control

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

Password Security

The following password security features are supported:

- Admin account password: Minimum length of 7 characters
- 30 minute lockout after 5 failed attempts in 2 minutes

For front-end XiO Cloud account passwords, single sign-on (SSO) may be used, allowing for corporate password policies to be applied. For back-end accounts, two-factor authentication is used.

Data Segregation

The 80 Series touch screens segregate data as follows.

Cloud Storage

All data stored in the cloud is kept in a Microsoft® Azure® multitenant database.

Physical Protection

All physical servers are managed by Microsoft Azure in the eastern and western United States. Authenticated remote access to servers is limited to named members of Crestron's engineering and operations teams. Access to business premises containing servers is managed by Microsoft Azure. Access to Crestron facilities is limited to invited guests and employees with badge access.

Audit Logging

Crestron applications write all security events to text based log files on the system that can be manually audited by administrators. Syslog and audit logging (if enabled) are included in the device logs. Customers must download device logs and share with Crestron manually if a review is requested by the customer.

Data Protection

Data transmitted via Crestron cloud-based software, such as the XiO Cloud service, is encrypted over TLS1.2 (AES 256 in transit, AES 128 at rest). The device does not sent PHI (Protected Health Information) or PII (Personally Identifiable Information), only NPI (Non-Personal Information) such as business contact information classified as such in the United States. The only exception for PII is that the XiO Cloud service can collect full names of users. Data at rest is protected with encrypted hard disks. No data is stored on company servers.

Software development follows OWASP (Open Web Application Security Project) best practices.

Security Best Practices

For optimal security while operating the device, observe the following best practices:

- Do not directly expose the device to the internet.
- Never install unapproved software.
- Use the system only for its intended purpose.

More Security Information

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

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

Security Reference Guide — Doc. 9604A
08/03/26
Specifications subject to
change without notice.