Security Reference Guide

TSS-470E

3.5 in. Desk Scheduling Touch Screen

Crestron Electronics, Inc.

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

Revision History

Rev	Date	Notes	Author(s)
A	October 27, 2023	Initial version	IH, SM
B	August 30, 2024	Updated network diagram and port list to reflect currently supported ports and functions. Added support for WPA2 Enterprise.	IH, SM

Please send comments and change recommendations to:

SecurityDocs@crestron.com

Contents

Introduction

This guide serves as a security reference and provides best practices for deploying the TSS-470E, which is a touch screen designed specifically for desk scheduling applications. The TSS-470E can be installed within a hoteling space to provide a clear indication of its availability and schedule. The TSS-470E also integrates seamlessly with a variety of popular scheduling services.

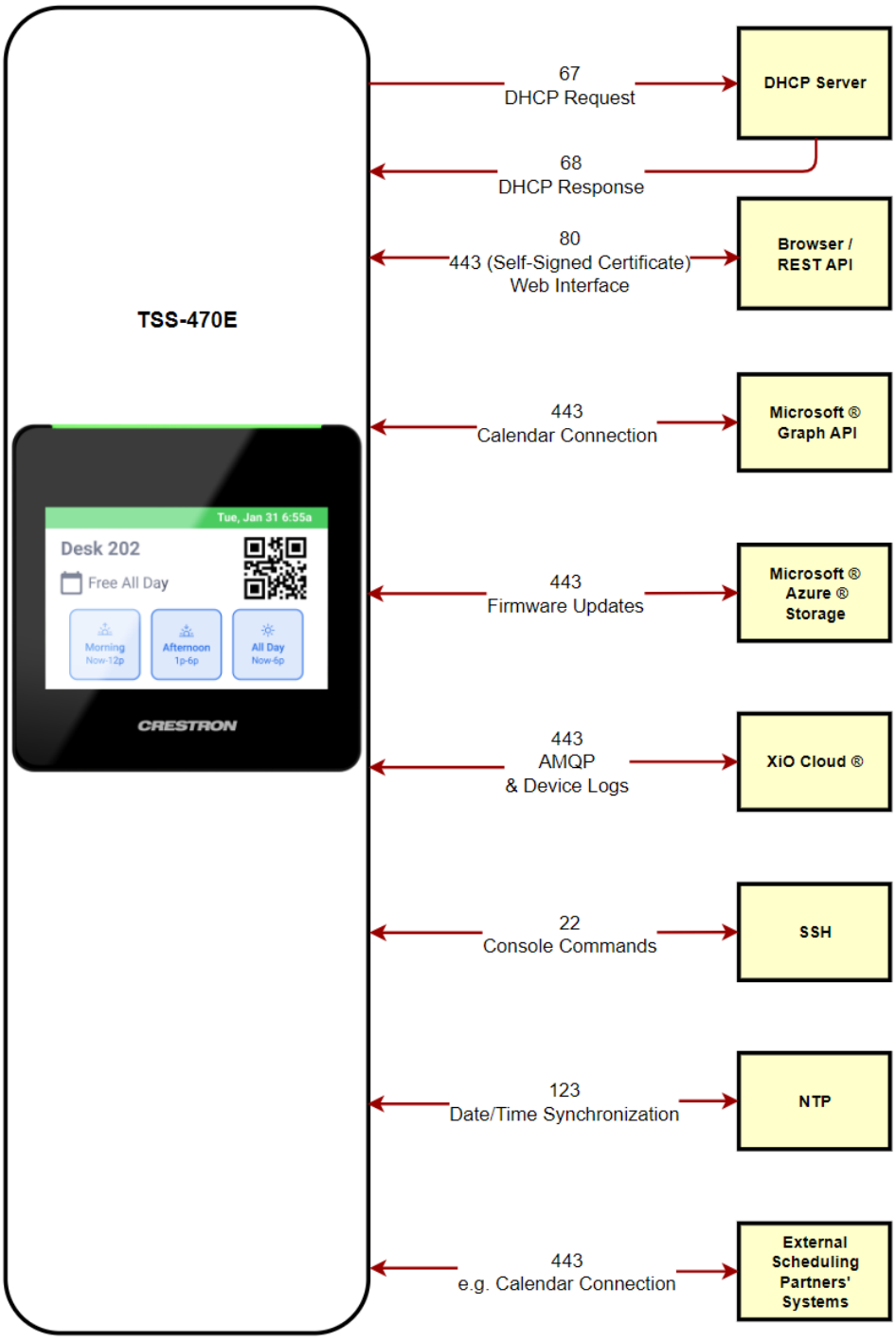
Intended Operational Environment

The TSS-470E is designed for installation in various desk scheduling spaces. Once installed, the TSS-470E connects to the corporate network over Ethernet or Wi-Fi® communications. Running the native Crestron Desk Scheduling App, the TSS-470E integrates directly with the XiO Cloud® service for desk scheduling via a connected Microsoft 365® scheduling calendar resource.

Crestron assumes the following about the TSS-470E 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.

The following diagram shows the TSS-470E network communication flow. For more information on the external ports shown, refer to Network Port List on page 5.



Security Policies

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

System Specifications

For general product specifications, refer to the TSS-470E-B-T product page.

Product Software - Security Features

The following security features are supported.

User Authentication

The first time the web configuration interface is accessed, a page is displayed asking the user to create an admin account. A similar prompt is displayed when connecting to the touch screen via Crestron Toolbox™ software if an admin account has not already been created. The admin account credentials are required for accessing the device web configuration interface.

For the local setup pages, a six-digit PIN code can be configured that must be entered before accessing the Ethernet and Wi-Fi configuration settings or restore option in the setup pages.

Additional groups and users can be created and managed using the device web configuration interface.

Connectivity

The TSS-470E can connect to the XiO Cloud provisioning and management service for monitoring, configuration, and desk scheduling functionality. For more information on the security features provided by the XiO Cloud service, refer to the XiO Cloud Service Security Reference Guide.

The TSS-470E also supports the following encryption and secure connection features:

- WPA2 Personal and WPA2 Enterprise encryption for Wi-Fi networks
- HTTP/HTTPS proxy
- SNTP (MD5/SHA1/SHA256)
- 802.1X IEEE authentication

Software Updates and Patches

Crestron is responsible for providing TSS-470E updates and security patches 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 Systems

The TSS-470E uses a custom-built Android™ operating system. Configuration of the operating system is not required.

Network Configuration

The TSS-470E is configured with the following settings. Additional action 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 Port List on page 5 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 TSS-470E 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 TSS-470E runs 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 TSS-470E. The TSS-470E cannot be interfaced with a control system and cannot be custom programmed for any other functionality. An internet connection is required.

Network Port List

The TSS-470E requires the following external and internal ports to be open while the device is running. These ports are opened by default.

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
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
HTTP	80/TCP	Device	OCSP Server	Typically uses port 80 but will use URL (and optional port number) from certificate

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.

Malware and Vulnerability Protection

The TSS-470E provides the following malware and vulnerability protection.

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.

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 8 characters
- Device Settings PIN: An exponential backoff algorithm is used with up to one hour between failed attempts

For front-end XiO Cloud account user 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 TSS-470E segregates 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 the Microsoft Azure service 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 TLS 1.2 (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. 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 TSS-470E, 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. 9433B
08/30/24
Specifications subject to
change without notice.