



Security Reference Guide

Crestron Videobar 70

Crestron Flex Large Room Conference
Solution with All-In-One Videobar 70
for Microsoft Teams® Rooms and
Zoom Rooms® Software

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.

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.

Crestron, the Crestron logo, and XiO Cloud are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Azure, Azure Active Directory, Microsoft 365, Microsoft Dynamics 365, Microsoft Intune, and Microsoft Teams are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Zoom Rooms is either a trademark or registered trademark of Zoom Video Communications, Inc. in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.

©2025 Crestron Electronics, Inc.

Contents

- Introduction** 1
 - Intended Operating Environment 1
- System Specifications** 2
 - Product Software - Security Features 2
 - Access Control 2
 - Connectivity 2
 - Software Updates and Patches 2
 - Operating System 2
 - 802.1X Authentication 3
 - Third-Party Software 3
 - Microsoft Teams® Rooms Secure Deployment 3
 - Zoom Rooms® Software Secure Deployment 3
- Network Infrastructure** 4
 - Microsoft Network Architecture Diagrams 4
 - Zoom Client Connection Process 4
 - Network Port List 4
- Connection to the XiO Cloud® Service** 6
- Remote System Log** 7
- Firmware Update** 9
- Security Controls** 10
 - Malware and Vulnerability Protection 10
 - Remote Connectivity 10
 - Role-Based Access Control 10
 - Password Security 11
 - Data Segregation 11
 - Audit Logging 11
 - Data Protection 11
 - Security Best Practices 12
 - More Security Information 12

Introduction

This document provides an overview of the security features, protocols and system configuration for the Crestron Videobar 70.

NOTE: The term "device" is used in this document to refer to all applicable Crestron Videobar 70 models unless specified otherwise.

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

Models	Descriptions
UC-B70-A-T	Crestron Flex Large Room Conference Solution with All-In-One Videobar 70 for Microsoft Teams® Rooms
UC-B70-A-T-I	Crestron Flex Large Room Conference Solution with All-In-One Videobar 70 for Microsoft Teams® Rooms, International
UC-B70-A-Z	Crestron Flex Large Room Conference Solution with All-In-One Videobar 70 for Zoom Rooms® Software
UC-B70-A-Z-I	Crestron Flex Large Room Conference Solution with All-In-One Videobar 70 for Zoom Rooms® Software, International

Intended 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 administrative guidance.
- If the Crestron Videobar 70 is placed on the corporate network, it is recommended to open the ports required for the device as detailed in Network Port List.

System Specifications

For general product specifications, refer to the [Crestron Videobar 70 Specifications](#).

Product Software - Security Features

The following security features are supported.

Access Control

Users and groups can be added to the device after an administrator account has been created. User and group management is handled through the Active Directory (LDAP) service. All users and groups must be created in Active Directory before they can be added to the device.

NOTE: The device does not support any local access levels outside of the local admin account. User and group access levels are created and managed through Active Directory.

Connectivity

The videobar supports connectivity to Microsoft Teams® Rooms or Zoom Rooms® software services and can utilize the following management portals:

- XiO Cloud® Provisioning and Management Service
- Microsoft Teams Admin Center
- Zoom Admin Portal

Software Updates and Patches

Software updates are managed through the default auto update feature .

Microsoft Teams Rooms devices can be managed through the Microsoft Teams Admin Center (TAC). For more information, refer to [Manage and Monitor Teams](#).

Zoom devices can be managed through the Zoom Admin Portal (ZDM). For more information, refer to [Zoom Help Center article](#).

Operating System

The videobar uses the Android 10 operating system.

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.

For more information, refer to the [Crestron Flex product manual](#).

Third-Party Software

All third-party and open source software and licenses used in Crestron applications are detailed in the EULA (End-User License Agreement) included with the device. The videobar is shipped with either a Microsoft Teams Rooms system or a Zoom Rooms system. Each of these applications are created and owned by Microsoft or Zoom respectively.

Microsoft Teams® Rooms Secure Deployment

The device runs the Microsoft Teams software app. For more information on how to securely deploy Microsoft Teams across an enterprise, refer to [Security and compliance in Microsoft Teams](#).

Zoom Rooms® Software Secure Deployment

The device runs the Zoom Rooms software app. For more information on how to securely deploy Zoom Rooms across an enterprise, refer to [Security at Zoom](#).

Network Infrastructure

The following sections describe information regarding the videobar network infrastructure.

Microsoft Network Architecture Diagrams

Microsoft provides the following network architecture diagrams that should be referenced as needed depending on your organization's Microsoft Teams deployment. The network architecture diagrams are provided as PDF files.

- [Microsoft Cloud for IT Architects Illustrations](#): Provides information about Microsoft cloud services, including Microsoft 365®, Azure® Active Directory® (Azure AD), Microsoft Intune®, Microsoft Dynamics 365®, and hybrid on-premises and cloud solutions.
- [Microsoft Teams IT Architecture and Voice Solutions Posters](#): Provides information about Microsoft Teams as part of Microsoft 365, groups in Microsoft 365, and Microsoft voice solutions.

Zoom Client Connection Process

Zoom provides the following overview that should be referenced as needed depending on your organization's Zoom deployment. The network architecture diagrams are provided as PDF files.

- [Zoom Client Connection Process](#)

Network Port List

The following ports and protocols are used by the device and are dependent on the system design and configuration:

Crestron Control Devices

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

Function	Destination Port	From (Sender)	To (Listener)	Notes
SSH	22/TCP	Admin Workstation	Device	Used for configuration and console
LDAP	389/TCP	Device	Admin Server	
LDAPS	636/TCP	Device	Admin Server	
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.
HTTPS	443/TCP	Device	Microsoft® Portal	For Microsoft portal services only and not required for device functionality. HTTPS services such as routing lookups and file transfers may be used.
HTTPS	443/TCP	Device	Firmware Server	Firmware upgrade path
HTTPS	443/TCP	Device	APK Server	APK upgrade path
DHCP	67/UDP	Device	DHCP Server	DHCP addressing
DHCP	68/UDP	DHCP Server	Device	DHCP addressing
HTTP	80/TCP	End User Workstation	Device	Web configuration
WPAD	80/TCP	Device	WPAD File Server	Gets the PAC file from the server
Remote Syslog	Configurable	Device	Remote Syslog Server	Uses TLS

Function	Destination Port	From (Sender)	To (Listener)	Notes
HTTP Proxy	Configurable	Device	Proxy Server	
HTTPS Proxy	Configurable	Device	Proxy Server	
Kerberos	88/TCP	Device	KDC (Key Distribution Center)	
DNS	3/TCP/UDP	Device	DNS server	

Connection to the XiO Cloud[®] Service

The device automatically connects to the XiO Cloud service, and allows the device to be claimed if an applicable license is available. If your environment or policies do not permit communications with external services, this settings can be turned off. For XiO Cloud, refer to the [Crestron Flex product manual](#).

Remote System Log

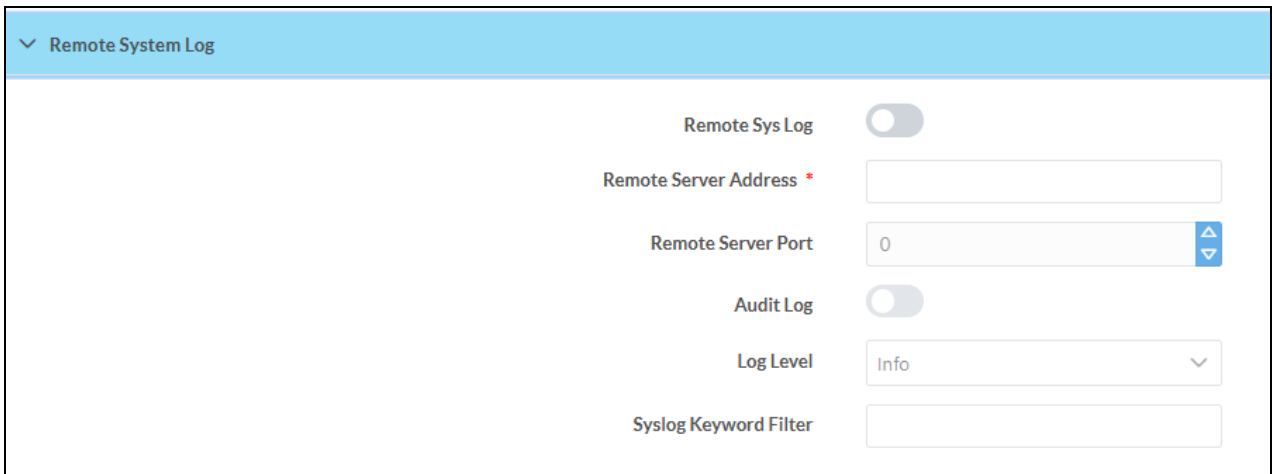
Devices do not send audit logs to a Remote System Log server by default. A connection to a Remote System Log server must be turned on and configured manually.

To turn on sending audit logs to a **Remote System Log** server:

NOTE: The remote server host must have a system log server with applicable security certificates and sufficient disk space to store the active system log. The host must also be configured to archive older system logs and to offload them over time. If TLS is turned on, a TLS-enabled server with the appropriate certificates is required.

1. Select the **Settings** tab.
2. Expand the **Remote System Log** accordion to display settings for the Remote System Log.

Remote System Log



The screenshot shows the 'Remote System Log' settings panel. It features a light blue header with a dropdown arrow and the text 'Remote System Log'. Below the header, there are several configuration options:

- Remote Sys Log:** A toggle switch that is currently turned off.
- Remote Server Address *:** A text input field.
- Remote Server Port:** A numeric input field with the value '0' and a small blue dropdown arrow on the right.
- Audit Log:** A toggle switch that is currently turned off.
- Log Level:** A dropdown menu with 'Info' selected and a downward arrow.
- Syslog Keyword Filter:** A text input field.

3. Turn the **Remote Sys Log** toggle on.

4. Enter the following information for the **Remote Sys Log** configuration:
 - **Remote Server Address:** Enter the IP address or Fully Qualified Domain Name (FQDN) of the Remote System Log server.
 - **Remote Server Port:** Enter a web port number of the Remote System Log server or select using the up/down arrows.
 - **Audit Log:** Turn the toggle on.
 - **Log Level:** Select the INFO, WARNING or ERROR log level for the syslog from the drop-down menu. Syslog messages are sent based on the following events:
 - Product model/version on boot up (INFO level)
 - NAT related info (INFO level)
 - SIP message summary (INFO level)
 - Inbound and outbound calls (INFO level)
 - Registration status change (INFO level)
 - Negotiated codec (INFO level)
 - Ethernet link up (INFO level)
 - SLIC chip exception (WARNING and ERROR levels)
 - Memory exception (ERROR level)
 - **Syslog Keyword Filter:** Enter keywords to filter the System Log entries. Multiple keywords should be entered as a comma-delimited list without any spaces, such as "SIP,registration,codec".
5. Select **Save Changes** from the **Action** menu.

Firmware Update

The videobar is configured to perform firmware updates when connected to the internet. To disable automatic updates on the device, refer to the [Crestron Flex Manual](#).

Manual firmware updates are available for the device as well. For more information on updating the firmware of the Crestron Videobar 70, refer to [Crestron Flex Manual](#).

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 videobar provides the following malware and vulnerability protection.

Security Highlights

The following security features have been incorporated into the Crestron Videobar 70:

- **Firmware Verification:** Secure boot with hardware-based Root of Trust verification of bootloader and BSP firmware is used along with standard [Android Verified Boot](#).
- **Security-Enhanced Linux:** SELinux is running in enforcing mode. For more information refer to [Security-Enhanced Linux in Android](#).
- **Disk Encryption:** User data secure using standard [Android File Based Encryption](#).
- **Application Separation:** [Android Application Sandboxing](#) is used.
- **Update Security:** Firmware updates are signed and validated.

Vulnerability Protection

If vulnerabilities or other issues are found, a patch will be made available. 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 addresses a critical vulnerability, the customer will be notified about the scheduled application of the patch.

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 customer data that may have been accessed. Customers will be notified about the impact of the attack and informed if any of their data has been compromised.

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 users' 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

Ensure all used passwords meet following criteria:

- Minimum length of 7 characters
- Passwords changed every 90 days
- 30 minute lockout after 5 failed attempts in 2 minutes.

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 videobar segregates data as follows.

Cloud Storage

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

Physical Protection

All physical servers are managed by Microsoft Azure® in the United States. Authenticated remote access to servers is limited to selected 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 employees with badge access and invited guests. For more information, refer to the [Microsoft Azure regions list](#).

Audit Logging

Crestron applications write all security events to text based log files on the system that can be manually audited by administrators.

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 send PHI (Protected Health Information) or PII (Personally Identifiable Information). Only NPI (Non-Personal Information) such as business contact information is sent. 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 videobar, observe the following best practices:

- Do not access the internet using a web browser on the device.
- 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](#).

