IV-SAM-VXN-1B, IV-SAM-VXP-1B, and IV-SAM-VXS-1B

1 Beyond Automate™ VX Series

Security Reference Guide

Crestron Electronics, Inc.

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

Contents

Introduction

This guide serves as a security reference and provides best practices for deploying all variants of the 1 Beyond Automate VX™ series. The 1 Automate VX series provides voice-activated camera switching solutions that bring a full multicamera studio experience to meetings, town halls, and classrooms. Camera switching and movement are done automatically based on the active speaking participant. Automate VX comes with built-in recording and streaming capability along with outputs for video conferencing.

The information in this document applies to the IV-SAM-VXN-1B, IV-SAM-VXP-1B, and IV-SAM-VXS-1B models.

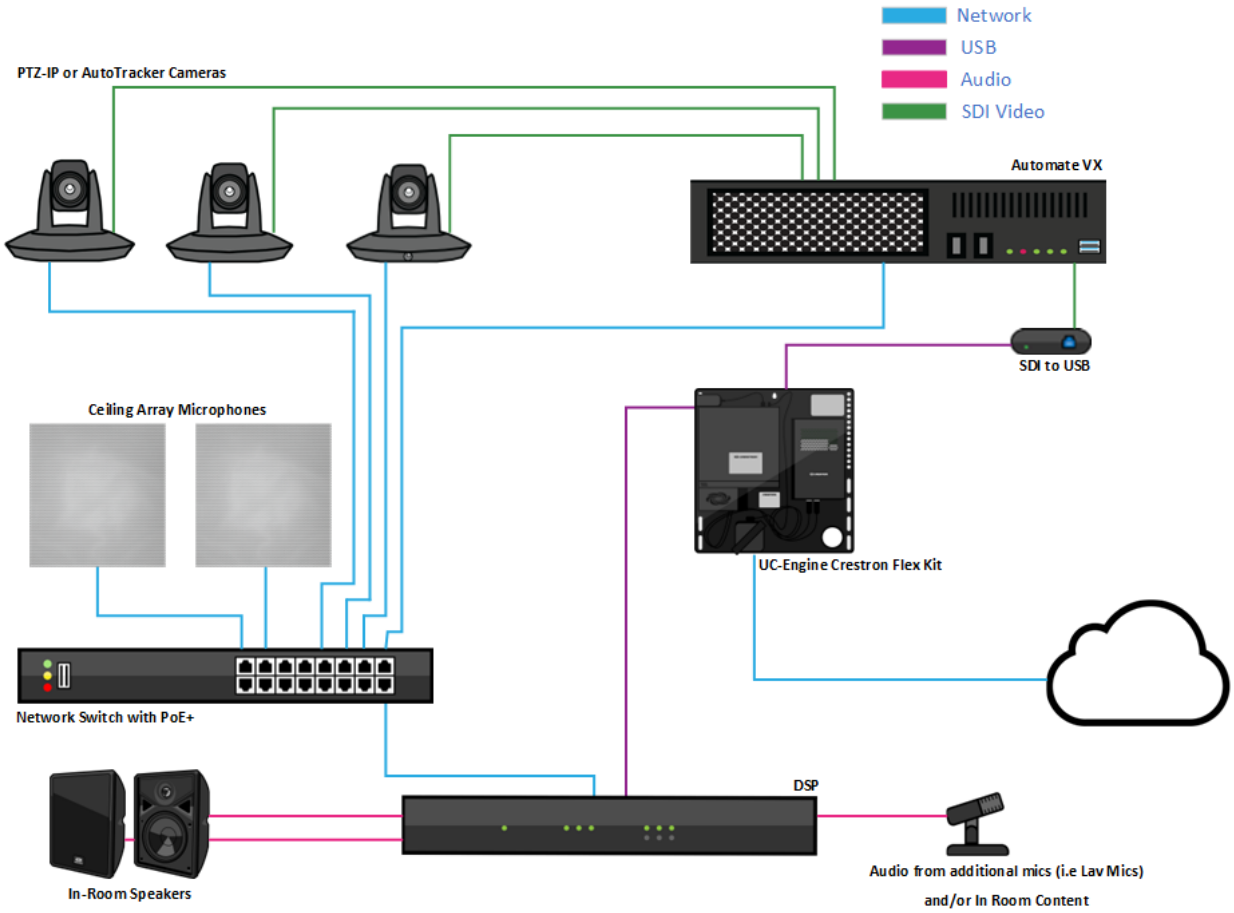
Intended Operation Environment

The Automate VX system is central to a Crestron® multicamera solution. The Automate VX system is designed for installation within a corporate, government, or educational environment, and it connects directly or indirectly to supported 1 Beyond cameras, Crestron Flex conferencing devices, and third-party microphones that are supplied by the user.

Observe the following points when setting up the operating environment:

- It is recommended to put the Automate VX system its own LAN or VLAN that is isolated from the corporate network. The Automate VX system does not need to be connected to the corporate network or internet to operate.
- Any cameras, microphones, control systems, and digital signal processors (DSPs) that connect to the Automate VX system should also be placed on an isolated LAN or VLAN.
- The output signal from the Automate VX system is SDI converted to USB for input to a Crestron UC-ENGINE device (or other codec). The latter device will be placed on the corporate network and connected to the internet.
- If the Automate VX system must be placed on the corporate network for any reason (such as for remote monitoring or support), it is recommended to open the ports required for the device as detailed in Network Port List on page 6.

The following diagram provides an example of devices and connections that are common within a typical Automate VX system deployment.



System Specifications

For general product specifications, refer to the IV-SAM-VXN-1B, IV-SAM-VXP-1B, and IV-SAM-VXS-1B product pages.

Product Software - Security Features

The following security features are supported.

User Authentication

A single admin account is set up by default with the following credentials:

- **Username**: Valued Customer
- **Password**: 1beyond

The default admin account username and password can be changed to support your organizational security policies or if the system will be placed on the corporate network. However, because the computer running the Automate VX system is set to log in automatically using the default credentials, a Windows® Registry change is required if these credentials change. Contact Crestron True Blue Support if this change is required.

> **NOTE:** Because the Automate VX system is configured to use automatic login, it is recommended that the computer running the Automate VX system is kept in a secure location (such as a locked closet) to prevent unauthorized access.

Additional user accounts can be set up in the Automate VX system to allow additional access to the system. User accounts can be configured to limit access to certain system functions. For more information, refer to the IV-SAM-VXP-1B and IV-SAM-VXS-1B Product Manual.

> **NOTE:** The Automate VX system does not support user management via domains (such as the Active Directory® service).

Audit Logging

System tasks use Windows® standard audit logging. Security-related application tasks are logged and stored in the audit log.

Software Updates and Patches

If the Automate VX system is connected to the internet, Windows software updates are managed automatically through Windows Update. The Automate VX and any of its related applications are not updated via Windows Update. The Automate VX system can be updated through most network domain management systems. Any software updates and patches will be installed automatically between 02:00 and 04:00 (AM) local time (this time is adjustable). For best practices in using and managing Windows Update, refer to the Manage Windows Updates document.

Operating System

The Automate VX system uses the Windows 10 IoT Enterprise operating system with Windows Firewall turned on by default. Configuration of the operating system is required (refer to Network Configuration on page 4).

Antivirus and Antimalware

Standard Windows 10 services including Windows Defender and Windows Firewall are turned on by default and are updated automatically.

Network Configuration

The Automate VX system is configured with the following settings. Additional action may be taken where applicable.

- **DHCP:** A standard DHCP configuration is provided when connecting the Automate VX device to the network via its **ETH2** port.

  > **NOTE:** The **ETH1** port is used for static IP addressing.

- **Wi-Fi® Communications:** Wi-Fi communications are turned off by default in Windows. Wi-Fi communications may be used only during installer setup and should not be turned on otherwise. If required for secure deployments, the Wi-Fi chip can be physically removed from the Automate VX device.
- **Hardening:** The Automate VX system may be hardened like any other Windows device under the condition that all required services and ports are left active (refer to Network Infrastructure on page 6).
- **Unneeded Accounts:** The built-in Admin account cannot be removed or disabled. Domain-level admin accounts are not supported.
- **File Share:** No file share is turned on by default.
- **Unneeded Ports:** Any ports besides those listed on the Network Port List on page 6 may be disabled.
- **Unneeded Services:** All required services must remain turned on (refer to Network Infrastructure on page 6). Any standard Windows services can be turned off as needed.

- **Unneeded Applications:** All required applications must remain turned on (refer to Network Infrastructure on page 6). Any standard Windows applications can be turned off as needed.
- **Restriction of External (USB) Devices:** There is no restriction of external USB devices.
- **Authentication of External Devices (such as USB Type-C® Authentication Specification):** No authentication is provided.

Third-Party Software

All third-party and open source software and licenses used in the Automate VX system are detailed at www.crestron.com/Legal/Open-Source-Software. The device ships with Wirecast® software, which is created and owned by Telestream.

Wirecast

The full version Wirecast streaming software (created by Telestream) is preinstalled on the Automate VX system during production by Crestron. The software is started automatically upon system startup. Access to the software is available on the computer running the Automate VX system during configuration and maintenance.

Crestron recommends using the Wirecast software version that ships with the Automate VX system. If a software update is required, it must be initiated manually by the admin user.

Network Infrastructure

The following sections describe the network infrastructure for the Automate VX system.

Network Port List

The following ports are in use:

Function	Category	Destination Port	From (Sender)	To (Listener)	Notes
HTTP	Common Service Port	3579/TCP	Admin or End User Workstation	Device	Unsecure access to Automate VX system/REST API layer
HTTPS	Common Service Port	4443/TCP	Admin or End User Workstation	Device	Secure access to Automate VX system/REST API layer
RTSP video stream	1B Cam Manager	554/TCP	Admin or End User Workstation	Device	RTSP video stream for 1B Cam Manager software
App ports	1B Cam Manager	5000, 5002/TCP	Admin or End User Workstation	Device	
VISCA over IP	1B Cam Manager	5500/TCP	Admin or End User Workstation	Device	External control using VISCA over IP
HTTP/HTTPS	Telestream Wirecast	80/TCP	Admin or End User Workstation	Device	
SSL	Telestream Wirecast	443/TCP/UDP	Admin or End User Workstation	Device	
RTMP	Telestream Wirecast	1935/TCP	Admin or End User Workstation	Device	
RTMPS	Telestream Wirecast	2935/TCP	Admin or End User Workstation	Device	

Function	Category	Destination Port	From (Sender)	To (Listener)	Notes
STUN/ Rendezvous	Telestream Wirecast	3478, 5349/TCP/UDP	Admin or End User Workstation	Device	
mDNS	Telestream Wirecast	5353/UDP	Admin or End User Workstation	Device	Used for NDI sources
NDI® Communications	Telestream Wirecast	5960–59xx/TCP/UDP	Admin or End User Workstation	Device	One port used per NDI source
Remote Desktop Presenter	Telestream Wirecast	7272/TCP	Admin or End User Workstation	Device	
WebRTC Media/ Rendezvous	Telestream Wirecast	49152–65535/UDP	Admin or End User Workstation	Device	Port is selected at random from within this range
Web API	Shure Designer	10000–65535	Admin or End User Workstation	Device	Port(s) dynamically allocated at install using available port(s) within this range
MongoDB® Database	Shure Designer	10000–65535	Admin or End User Workstation	Device	Port(s) dynamically allocated at install using available port(s) within this range
Shure® System API	Shure Designer	10000–65535	Admin or End User Workstation	Device	Port(s) dynamically allocated at install using available port(s) within this range

VLAN

In order to ensure proper functionality, ensure that any cameras, microphones, control systems, and digital signal processors (DSPs) that connect to the Automate VX system are on the same VLAN as the Automate VX.

Security Controls

The following security controls are applicable to the Automate VX system.

Malware and Vulnerability Protection

The Automate VX system provides the following malware and vulnerability protection.

Security Applications

The following Microsoft applications are included on the Automate VX system:

- Backup Solutions
- Windows Defender

Vulnerability Protection

If vulnerabilities or other issues are found, a patch will be made available to customers. Any security patches will be installed automatically between 02:00 and 04:00 (AM) local time (this time is adjustable).

Remote Connectivity

Crestron support teams use the RDP or TeamViewer applications to remote into a customer's Automate VX system during initial setup. A customer must be on site to grant Crestron support remote access into the Auotmate VX system. No activities are logged during this time outside of the standard Windows and application logging.

Role-Based Access Control

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

Audit Logging

Standard Windows security logging and auditing is used for performance-related troubleshooting.

Security Best Practices

For optimal security while operating the Automate VX system, observe the following best practices:

- Ensure that any cameras, microphones, control systems, and digital signal processors (DSPs) that connect to the Automate VX system are on the same VLAN as the Automate VX.
- Do not access the internet using a web browser on the system.
- 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. 9373A
12/19/22
Specifications subject to
change without notice.