Security Reference Guide

IV-SAM-VX2 Series

Automate VX System Series 2 Voice-Activated, Multi-Camera Switching Solution

Crestron Electronics, Inc.

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

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.

Contents

Introduction

This guide serves as a security reference and provides best practices for deploying all variants of the Crestron 1 Beyond Automate VX2 series. The IV-SAM-VX2 Series camera switching systems bring a full multicamera studio experience to meetings, town halls, and classrooms. Crestron 1 Beyond cameras automatically switch based on the location of the active speaking participant. Visual AI enhanced camera switching intelligently frames camera shots with the participants centered.

The information in this document applies to the IV-SAM-VX2-S and IV-SAM-VX2-P models.

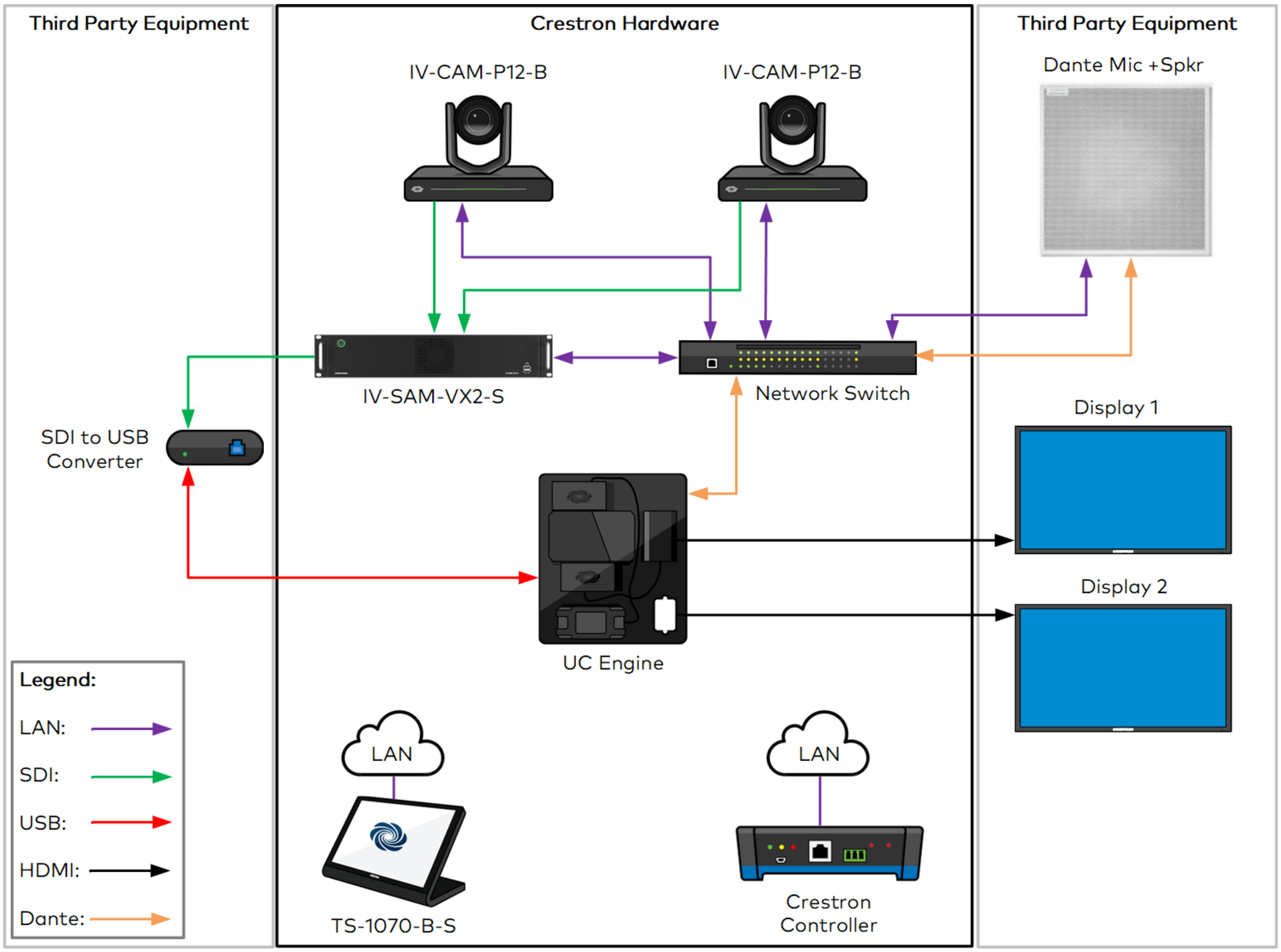
Intended Operation Environment

Automate VX2 is central to a Crestron multicamera solution. Automate VX2 is designed for installation within a corporate, government, or educational environment, and it connects directly or indirectly to supported Crestron 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:

- Any cameras, microphones, control systems, and digital signal processors (DSPs) that connect to the Automate VX2 system can also be placed on an isolated LAN or VLAN.
- The output signal from the Automate VX2 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 VX2 system is placed on the corporate network, it is recommended to open the ports required for the device as detailed in Network Port List.

The following diagram provides an example of devices and connections that are common within a typical Automate VX2 deployment.



System Specifications

For general product specifications, refer to the IV-SAM-VX2-S and IV-SAM-VX2-P product pages.

Product Software - Security Features

The following security features are supported.

User Authentication

There are two accounts available on Automate VX2 systems; the user account and the administrator account. When the Automate VX2 is turned on, by default it signs into the user account of the system. The user account displays the IP address, Model Name, Software Version, and time of day on the splash screen. There is no password required for the user account.

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

- **Username**: Admin
- **Password**: crestron

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. For more information on changing the password for the admin account, refer to the IV-SAM-VX2 Series Product Manual.

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-VX2 Series Product Manual.

> **NOTE:** The Automate VX2 system supports user management via domains (such as the Active Directory® service). However, the settings cannot be changed for the user account **Automate VX** and a password cannot be set for it. An account can be added via the admin account.

Secure the BIOS

The BIOS password for the Automate VX2 is the serial number of the system, and each serial number is unique to the system. If the BIOS password must be changed, refer to the ASRock® documentation for the motherboard.

> **NOTE:** To access the BIOS of Automate VX2, press either the **F2** or **Delete** key on a keyboard during system initialization.

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 Automate VX2 is connected to the internet, Windows software updates are managed automatically through Windows Update. Automate VX2 can be updated through most network domain management systems, or it can be updated with a firmware package manually. 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

Automate VX2 uses the Windows 11 IoT Enterprise operating system with Windows Firewall turned on by default. Configuration of the operating system is required (refer to Network Configuration on page 7).

Antivirus and Antimalware

Standard Windows 11 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 Automate VX2 to the network via any of the Ethernet ports on the system.
- **Hardening:** The Automate VX2 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).
- **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 may be disabled.
- **Unneeded Services:** All required services must remain turned on (refer to Network Infrastructure). Any standard Windows services can be turned off as needed.
- **Unneeded Applications:** All required applications must remain turned on (refer to Network Infrastructure). 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 Automate VX2 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 of Wirecast streaming software (created by Telestream) is preinstalled on Automate VX2 during production by Crestron. The software starts automatically upon system startup. Access to the software is available on the computer running Automate VX2 during configuration and maintenance. Wirecast is automatically updated with Automate VX2 firmware updates.

Network Infrastructure

The following sections describe the network infrastructure for Automate VX2.

Network Port List

The following ports are in use:

Function	Category	Destination Port	From (Sender)	To (Listener)	Notes
Crestron-CIP	Crestron Control	41794/TCP	Remote Device	Device	Crestron Internet Protocol
Crestron-SCTP	Crestron Control	41795/TCP	Remote Device	Device	Secure Crestron Terminal Protocol for Ethernet communication
Crestron-SCIP	Crestron Control	41796/TCP	Remote Device	Device	Secure Crestron Internet Protocol
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	

Function	Category	Destination Port	From (Sender)	To (Listener)	Notes
RTMP	Telestream Wirecast	1935/TCP	Admin or End User Workstation	Device	
RTMPS	Telestream Wirecast	2935/TCP	Admin or End User Workstation	Device	
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

VLAN

In order to ensure proper functionality, ensure that any cameras, microphones, control systems, and digital signal processors (DSPs) that connect to Automate VX2 are on the same VLAN as the Automate VX.

Security Controls

The following security controls are applicable to Automate VX2.

Malware and Vulnerability Protection

Automate VX2 provides the following malware and vulnerability protection.

Security Applications

The following Microsoft applications are included on Automate VX2:

- 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 application to remote into a customer's Automate VX2 during initial setup. 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 Automate VX2, observe the following best practices:

- Ensure that any cameras, microphones, control systems, and digital signal processors (DSPs) that connect to Automate VX2 are on the same VLAN as Automate VX2.
- 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. 9497A
06/06/24
Specifications subject to
change without notice.