Crestron Flex UC-ENGINE

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.

Revision History

Rev	Date	Notes	Author(s)
A	March 7, 2020	Initial version	SD, JZ
B	February 7, 2023	Significant update to all topics based on latest UC-ENGINE functions and specifications	IH, JZ, MH

Please send comments and change recommendations to:

SecurityDocs@crestron.com

Contents

Introduction

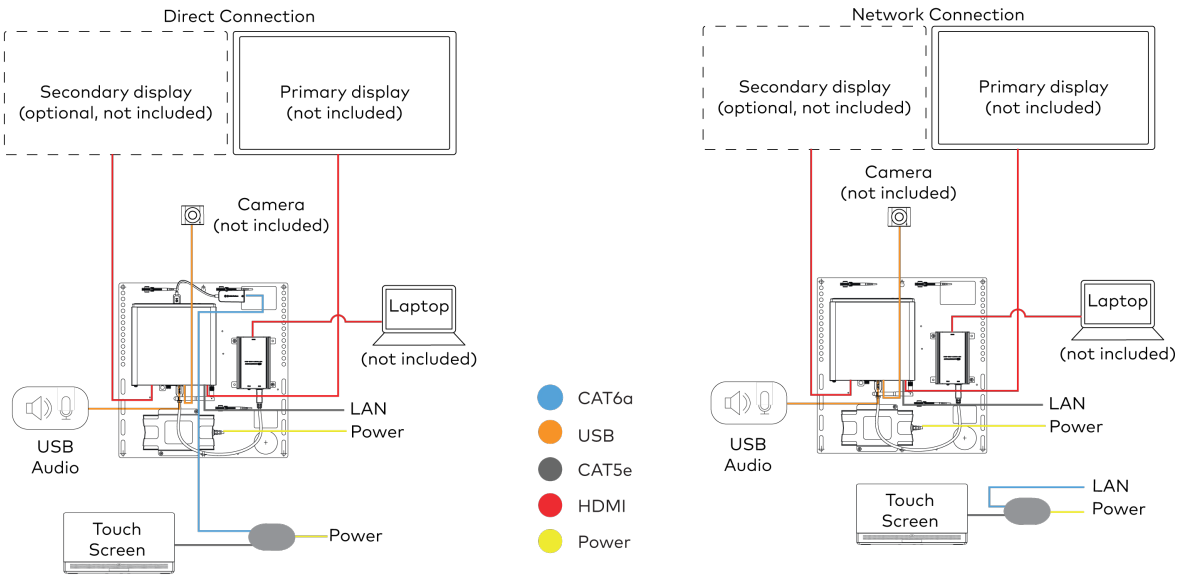
This guide serves as a security reference and provides best practices for deploying all variants of the Crestron UC-ENGINE, a powerful Mini PC sold exclusively as part of a complete Crestron Flex UC system and designed for use in a Microsoft Teams® or Zoom Rooms™ software environment. The following information applies to the Dell® and Intel® Mini PCs that are included within various Crestron Flex kits.

Intended Operational Environment

The UC-ENGINE is central to a complete Crestron Flex system, providing powerful processing performance, Gigabit Ethernet, and complete connectivity for one or two HD displays, USB cameras, and one USB audio conferencing device. It is designed for installation in meeting rooms to host video calls when connected to a Microsoft Teams or Zoom Video Meeting service.

The UC-ENGINE comes preassembled on a bracket assembly as part of a Crestron Flex kit. Other peripherals must be provided by the user. For more information on Crestron Flex kits, refer to the Crestron Flex feature page.

The following diagram provides an example of devices and connections that are common within a typical Crestron Flex system.



Security Policies

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

System Specifications

For general product specifications, refer to the product page for your Crestron Flex kit.

Product Software - Security Features

The following security features are supported.

> **NOTE:** To view security features for other Crestron devices that may be included within a Crestron Flex deployment (such as touch screens or AirMedia® presentation), refer to the applicable security documentation at security.crestron.com.

User Authentication

When using a Microsoft Teams device, two accounts are set up by default: a Microsoft Teams account and a default Admin account for administrating the UC-ENGINE.

When using a Zoom Rooms device, two accounts are setup as default: a CrestUC account and a default Admin account for administrating the UC-ENGINE.

> **CAUTION:** The password for the default CrestUC or default Microsoft Teams account must not be changed. If changed, the device will require a reimage.

Audit Logging

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

Connectivity

The UC-ENGINE supports connectivity to Microsoft Teams or Zoom Meeting services and can utilize the following management portals:

- XiO Cloud® Provisioning and Management Service
- Crestron Fusion® Cloud Software
- Microsoft Teams Admin Center
- Zoom Admin Portal
- Microsoft Intune® Service

Software Updates and Patches

Software updates are managed automatically through Windows Update. The UC-ENGINE can be updated through most network domain management systems. For best practices in using and managing Windows Update, refer to the Manage Windows Updates document.

Optionally, Zoom devices may be managed through the Zoom admin portal. For more information, refer to the Zoom Help Center article.

Operating System

The UC-ENGINE 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 3).

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 UC-ENGINE 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 Windows, but not supported on the UC-ENGINE.
- **Hardening:** The UC-ENGINE may be hardened like any other Windows device under the condition that all Crestron services and ports are left active. Microsoft Teams or Zoom Rooms must be left accessible.
- **Unneeded Accounts:** The built-in Admin account can be removed or disabled as long as the device is domain attached. Doing so allows administrators to use any domain-level admin account to log in.
- **File Share:** No file share is turned on by default.
- **Unneeded Ports:** Any ports besides those listed on the Network Port List on page 5 may be disabled.
- **Unneeded Services:** All Crestron services must remain turned on. Any standard Windows services can be turned off as needed.
- **Unneeded Applications:** All Crestron applications must remain turned on. Any standard Windows applications can be turned off as needed.
- **Restriction of External (USB) Devices:** There is no restriction of external USB devices. However, Crestron recommends only connecting USB devices that are included in the Crestron Flex kit, sold by Crestron, or are certified for use with Crestron Flex systems.

- **Authentication of External Devices (such as USB Type-C® Authentication Specification):** No authentication is provided.
- **Certified Software**: The UC-ENGINE is compatible with third-party software and firmware that has been certified for use with Crestron Flex systems.
    - Certified firmware versions for USB audio and video peripherals (for Microsoft Teams deployments)

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 UC-ENGINE 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

The Microsoft Teams Rooms app is a customized Microsoft Teams client created by Microsoft specifically for room systems. The application is preinstalled as part of the device image created by Crestron and starts automatically as the main interface on the UC-ENGINE.

All updates to the Microsoft Teams Rooms application, including security and feature updates, are automatically installed by the Windows Store. All security and feature updates are delivered in this manner. Users may not manually install updates to the Microsoft Teams Rooms application. Configuration of the Microsoft Teams Rooms application is done by selecting the **Settings** option under the **More** button on the main interface screen.

For information on the configuration options available, refer to the Microsoft Teams Rooms Deployment Guide.

Zoom Rooms

The Zoom Rooms app is a customized Zoom Meetings client created by Zoom specifically for room systems. The application is preinstalled as part of the device image created by Crestron and starts automatically as the main interface on the UC-ENGINE when it is in Zoom mode.

All updates to the Zoom Rooms application can be applied either manually or automatically through the Zoom admin portal. Crestron also periodically provides updates to the Zoom Rooms application that can be installed manually on the UC-ENGINE. However, Crestron does not publish all Zoom Rooms updates.

For configuration instructions, refer to the Zoom documentation.

Network Infrastructure

The following sections describe information regarding the UC-ENGINE 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.

Network Port List

The following ports are in use:

Function	Category	Destination Port	From (Sender)	To (Listener)	Notes
Miracast A/V	AirMedia	4570/UDP	End User Workstations	Device	The default port for Miracast A/V, only open during video presentation
AirMediaV2 Audio/Video	AirMedia	47000/TCP	End User Workstations	Device	AirMedia client control, used by AirMedia application running on PC
AirMediaV2 Audio/Video	AirMedia	47010/TCP	End User Workstations	Device	AirMedia audio/video streams

Function	Category	Destination Port	From (Sender)	To (Listener)	Notes
AirMediaV2 Discovery	AirMedia	5353/UDP	End User Workstations	Device	AirMedia Presentation Gateway discovery, used for autodiscovery
AirMediaV2 Audio/Video	AirMedia	6000–7000/TCP/UDP	End User Workstations	Device	AirMedia audio/video streams
AirMediaV2 Control	AirMedia	7011/UDP	End User Workstations	Device	AirMedia control channel information
AirMediaV2 Control	AirMedia	7100/TCP	End User Workstations	Device	AirMedia client control, used by AirMedia application running on PC
AirMediaV2 Control	AirMedia	7200–7201/TCP	End User Workstations	Device	AirMedia control channel information
Miracast RTSP	AirMedia	7236/TCP	Device	End User Workstations	Default port for Miracast RTSP
Miracast MS-MICE	AirMedia	7250/TCP	End User Workstations	Device	Microsoft extension for Miracast Infrastructure Mode
AirMedia V2 Control	AirMedia	7300/TCP	End User Workstations	Device	Chrome® extension signaling channel (AirMedia support for Chromebooks) (Day 9)
NTP	Common Service Ports	123/UDP	Device	NTP Server	Network Time Protocol (NTP)

Function	Category	Destination Port	From (Sender)	To (Listener)	Notes
SSH/SFTP	Common Service Ports	22/TCP	Admin Workstation	Device	Used for Cloud Configuration, Console, and File Transfer
LDAP	Common Service Ports	3268/TCP	Device	LDAP Server	LDAP queries targeting global catalogs
HTTPS	Common Service Ports	443/TCP	Admin or End User Workstation	Device	Secure Web Configuration for Crestron Mercury® device
DHCP	Common Service Ports	67/UDP	Device	DHCP Server	DHCP Addressing
DHCP	Common Service Ports	68/UDP	DHCP Server	Device	DHCP Addressing
HTTP	Common Service Ports	80/TCP	Admin or End User Workstation	Device	Main web page for downloading AirMedia application
Crestron-CIP	Crestron Control	41794/TCP	Device	Fusion	Crestron Internet Protocol - used for Fusion Servers
Crestron-CIP	Crestron Control	41794/TCP	Third-Party Display	Device	Crestron Connected® protocol
Crestron-CIPS	Crestron Control	41796/TCP	Device	Crestron Fusion	Crestron Internet Protocol Secure, used for Crestron Fusion Servers
Crestron-CIPS	Crestron Control	41796/TCP	Third-Party Display	Device	Crestron Connected protocol

Function	Category	Destination Port	From (Sender)	To (Listener)	Notes
Autodiscovery of UC-ENGINE	Flex UC-Engine	42872/UDP	Device	UC-ENGINE	Crestron Mercury device
Touch and signaling (TLS 1.2)	Flex UC-Engine	49500/TCP or UDP	Device	UC-ENGINE	Crestron Mercury device
Video (TLS 1.2)	Flex UC-Engine	49501/TCP or UDP	Device	UC-ENGINE	Crestron Mercury device
HTTPS	XiO Cloud	443/TCP	Device	XiO Cloud service	XiO Cloud service

VLAN

In order to ensure proper functionality, ensure the display devices and UC-ENGINE are on the same VLAN.

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 UC-ENGINE provides the following malware and vulnerability protection.

Security Applications

The following Microsoft applications are included on the Crestron Flex UC-ENGINE:

- Enhanced Mitigation Experience Toolkit (EMET)
- AppLocker
- Backup Solutions
- User Account Control
- Windows Defender

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

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 UC-ENGINE segregates data as follows.

Cloud Storage

All data stored in the cloud is kept in a multitennant 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

Standard Windows security logging and auditing is used. 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 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 Crestron Flex UC-ENGINE, 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.

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

Security Reference Guide — Doc. 8726B
02/10/23
Specifications subject to
change without notice.