Crestron Flex Care Cloud Connect Service

Security Reference Guide

Crestron Electronics, Inc.

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

Use of the Crestron Flex Care Cloud Connect service is governed by the terms of the Crestron Cloudware License Agreement and Cloudware License Addendum for Complimentary Subscription Cloudware, which can be found on the Crestron website at https://www.crestron.com/Legal/software-products-on-premises-and-cloudware.

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 at www.crestron.com/legal/patents.

Certain Crestron products contain open source software. For specific information, visit www.crestron.com/opensource.

Contents

Introduction

The Crestron Flex Care Cloud Connect service is an optional service that is available at no additional charge with the purchase of a Crestron Flex Care subscription plan, which is offered subject to the terms and conditions set forth at www.crestron.com/FlexCareTerms. Opt-in to the Crestron Flex Care Cloud Connect service is available during the registration of Crestron Flex conference system products for coverage under the Crestron Flex Care subscription plan. The Crestron Flex Care Cloud Connect service enables the Crestron Support team to remotely connect to your covered Crestron Flex conference system within minutes to provide a streamlined remote support experience.

Various Unified Communications (UC) parameters are visible to the Crestron Support team for the purpose of providing remote support for Crestron Flex conference systems registered for the Crestron Flex Care Cloud Connect service (refer to Appendix A for additional information). For details regarding data transmitted to Crestron through the Crestron Flex Care Cloud Connect service, see the Crestron Privacy Statement Regarding Internet Data Collection, which is available at www.crestron.com/legal-data-collection-privacy.

Customer Benefits

The Crestron Flex Care Cloud Connect service provides a streamlined remote support experience for the covered Crestron Flex conference systems:

- Crestron Support has access to covered device status, setting, and firmware version information.
- Crestron Support has access to covered device event logs.
- Crestron Support can remotely update firmware for covered Crestron Flex conference systems.

Crestron Flex Care Cloud Connect Service Details

The Crestron Support team will **not** deploy firmware, programs, or applications, or schedule any events or operations enabled by the Crestron Flex Care Cloud Connect service for the covered devices, except in connection with a remote support request to the Crestron Support team.

The Crestron Flex Care Cloud Connect service does **not** collect or transmit any data regarding meeting scheduling or meeting attendees.

The Crestron Flex Care Cloud Connect service does **not** enable Crestron to access any conference call or room audio or video content from covered devices.

Cybersecurity

The following sections provide information related to cybersecurity:

Firewall

Hosted on the Microsoft® Azure® IaaS platform, the Crestron Flex Care Cloud Connect service uses the Azure Firewall cloud network security service. Information about Azure Firewall is available on the Microsoft website (www.microsoft.com).

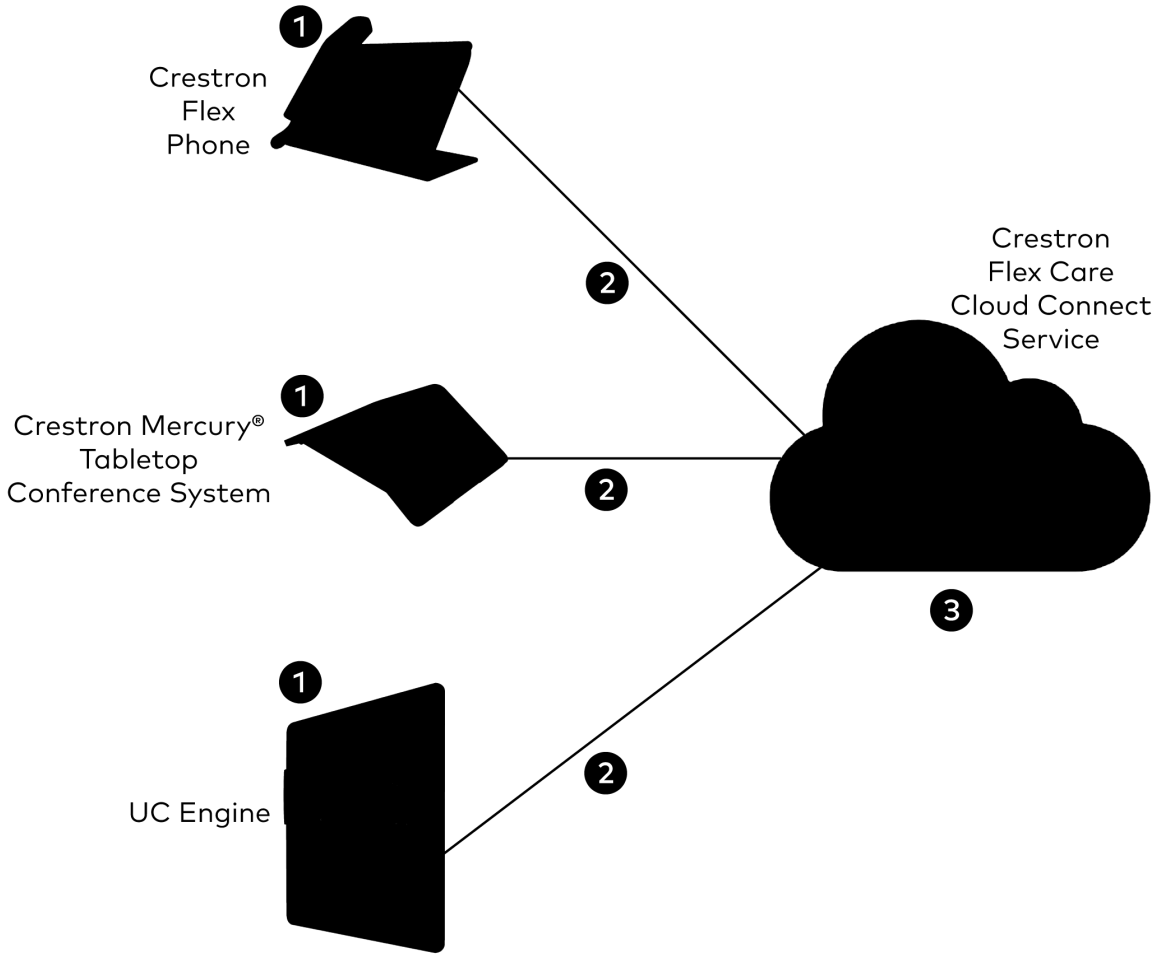
Communication Between Devices and the Cloud

Covered Crestron Flex devices connect directly to the Crestron Flex Care Cloud Connect service to exchange data and control message traffic. Communication is carried over the Advanced Message Queuing Protocol (AMQP) and encrypted with X.509 certified TLS 1.2 authentication so that no data is exposed between the devices and the cloud. The cloud configuration service connection must be enabled on the devices for communication. To prevent communication to the Crestron Flex Care Cloud Connect service, this setting can be disabled at any time from the local web configuration interface of the devices.

Devices connect to the cloud on TCP Port 443 (AMQP over WebSockets).

The following illustration provides an example of communication between devices and the cloud.

Communication Between Devices and the Cloud



1. Device makes a persistent outbound connection to Crestron Flex Care cloud servers.
2. Crestron Flex Care Cloud Connect data in transit is encrypted using TLS 1.2 as it travels over the client network and the Internet.
3. Crestron Flex Care Cloud Connect data at rest is stored in Microsoft Azure cloud storage and is secured with AES-128 encryption.

Data Encryption: In Transit and At Rest

Data is encrypted in transit and at rest. The Crestron Flex Care Cloud Connect service is built as a collection of microservices in the Microsoft Azure platform. The microservices are authenticated using Active Directory® credential management. All access to data through the Crestron Flex Care Cloud Connect service is monitored by Crestron to identify intrusions or unauthorized access.

The Crestron Flex Care Cloud Connect service uses Azure Key Vault as an encryption agent that establishes and manages cryptographic keys for required cryptography employed within the information system. Azure Key Vault is also FIPS 140-2 approved within the Microsoft Azure Commercial Cloud.

The following information is stored by the Crestron Flex Care Cloud Connect service:

- Settings for your devices
- Registration information
- Log files from the device, which are sent to the Crestron Flex Care Cloud Connect service only after an action is initiated

Certifications

Crestron does not currently possess a SOC 2 Type 2 certification. However, since the Crestron Flex Care Cloud Connect service is hosted on the Microsoft Azure platform, several technical controls in use have been verified as a part of the Microsoft SOC 2 report for the Azure platform.

Auditing

The following sections describe the log information available for auditing:

- User Access Logs (below)
- Activity Logs (below)

User Access Logs

The Crestron Flex Care Cloud Connect service enables audit information to be stored in the Microsoft Active Directory event log and includes the following user access data:

- User ID
- Date and time of the event
- Type of event
- Origin of request (e.g., originating host's IP address) for Identification and Authentication events only
- Name of data object modified or deleted for modification or deletion events only (locally)
- Results of the events (i.e., successful/unsuccessful login, access denied, list of attempts)

The Crestron Flex Care Cloud Connect service audit information is managed through the integration of Microsoft Active Directory credential management and the Microsoft Azure Commercial Cloud remote management service.

Customers can request access to user access logs by contacting Crestron Support.

Activity Logs

In addition to the audit information stored in the Microsoft Active Directory event log, all device operations initiated by Crestron Support from the Crestron Flex Care Cloud Connect service are recorded in cloud activity logs and retained for 30 days. The logged events include but are not limited to the following operations:

- Device reboots
- Log file retrieval
- Firmware updates
- Changes to settings
- Scheduled actions

The activity log also includes the user name of the Crestron Support team member who started or stopped the operation and the date and time of the operation.

Customers can request access to activity logs by contacting Crestron Support.

The following table provides a sample activity log.

Sample Activity Log

Date and Time	User	Device Model	Device or Room or Group	Event
02/15/2021 12:56 PM	*Crestron Support User Name*	UC Engine	UC-ENGINE 54B2038CCDB3	Moved the device:Old value:Unassociated | New value:CHA-E7NE
02/15/2021 12:48 PM	*Crestron Support User Name*	UC Engine	CHA-E7NE	Device Unclaimed: CHA-E7NE-UCE-M
02/23/2021 11:19 AM	*Crestron Support User Name*	UC Engine	CHA-E7NE	Device Unclaimed: CHA-E7NE-UCE
02/15/2021 12:57 PM	*Crestron Support User Name*	UC Engine	UC-ENGINE 54B2038CCDB3	Setting Changed:Firmware Update Allowed|Old value:True | New value:False
02/24/2021 9:47 AM	*Crestron Support User Name*	UC Engine	CHA-HOW-Atrium-UCE	Scheduled firmware update:Old value:1.00.16.883 | New value:1.00.16.889 for Teams
02/24/2021 9:47 AM	*Crestron Support User Name*	UC Engine	CHA-HOW-Atrium-UCE	Firmware update initiated:Old value:1.00.16.883 | New value:1.00.16.889-Team

Appendix A. UC Device Parameters Stored by Crestron Flex Care Cloud Connect Service

The following table lists the device parameters stored by the Crestron Flex Care Cloud Connect service for Crestron Flex phones, Crestron Mercury® tabletop conference systems, and UC engines.

Crestron Flex Phone (UC-P8 and UC-P10 Series)	Crestron Mercury® Tabletop Conference System	UC Engine
Model	Model	Provisioning Version
Microsoft Teams® Audio Call Status	Microsoft Teams Audio Call Status	Windows® OS Build
Serial Number	Serial Number	Serial Number
Firmware Version	Firmware Version	Software Version
Microsoft Teams Android™ App Version	Microsoft Teams Android App Version	Software Build
—	Zoom Rooms™ Controller Android App Version	—
Language	Language	—
Occupancy	Occupancy Status	Room Occupancy
Occupancy Enabled	—	—
Microsoft Teams Audio Presence	Microsoft Teams Audio Presence	—
Android Version	Android Version	Version
System Version	System Version	Upgrade Status
U-boot Version	U-boot Version	Uptime
Kernel Version	Kernel Version	Genius Framing
Hardware Version	Hardware Version	—
DSP (AVS) Version	DSP (AVS) Version	—
Host Name	Host Name	—
Domain Name	Domain Name	—
Primary DNS Server	Primary DNS Server	Primary Static DNS
Secondary DNS Server	Secondary DNS Server	Secondary Static DNS

Crestron Flex Phone (UC-P8 and UC-P10 Series)	Crestron Mercury® Tabletop Conference System	UC Engine
DHCP Enabled	DHCP Enabled	DHCP
IP Address	IP Address	IP Address
Subnet Mask	Subnet Mask	Subnet Mask
Default Gateway	Default Gateway	Default Gateway
MAC Address	MAC Address	—
Link Active	Link Active	—
Proxy	Proxy	—
802.1x	802.1x	—
Wi-Fi® Status	Wi-Fi Status	—
Wi-Fi Diagnostics	Wi-Fi Diagnostics	—
Mic Mute Status	Mic Mute Status	—
Speaker Volume	Speaker Volume	—
Phone Status	Bluetooth® Pairing Mode	—
Bluetooth	Bluetooth	—
Accessory	Accessory	—
Screen Saver	Application Mode	—
Time Zone	Time Zone	—
PC Port	—	—
USB Connections	—	—
DHCP VLAN	—	—
Static VLAN	—	—
VLAN TAG	—	—
PC Port Mode	—	—
PC Port VLAN TAG	—	—
Friendly System Name	Friendly System Name	—
Standby Timeout (Minutes)	Standby Timeout (Minutes)	—
SImple NTP	Simple NTP	—
Custom Time Server	Customer Time Server	—
—	Mic Mute Status	—
—	Speaker Volume	—
Time	Time	—

Crestron Flex Phone (UC-P8 and UC-P10 Series)	Crestron Mercury® Tabletop Conference System	UC Engine
Date	Date	—
—	Wi-Fi	—
Bluetooth Beaconing	Bluetooth Beaconing	—
Phone Lock	Friendly Bluetooth Name	—
—	Bluetooth Idle Disconnect Time	—
Screen Saver	Domain Name	—
Screen Saver Time Out Minutes	Application Mode	—
Pin Unlock Code	—	—
Phone Lock Time Out (Minutes)	—	—
—	Zoom Ultrasonic Volume	—
—	UC-ENGINE Hostname/IP Address	—
—	UC-ENGINE Port	—
—	UC-ENGINE Username	—

Appendix B. URLs and IP Addresses

The service is in the Azure US-East and US-West data centers. The updated list of IP addresses for these data centers is available on the Microsoft website at www.microsoft.com/en-us/download/details.aspx?id=56519.

The following domains are used by connected devices and may be whitelisted:

- *.crestron.io
- *.azure-devices.net

The following specific IoT Hub domains may be listed instead of the wildcard, but they are subject to change at any time without notice:

- Prd-use-iothub.azure-devices.net
- Prd-usw-iothub.azure-devices.net

Current IP addresses are listed below and subject to change at any time without notice:

- FCS & Portal US-East: 168.62.165.131
- FCS & Portal US-West: 138.91.240.81
- IoT Hub US-East: 40.76.71.185
- IoT Hub US-West: 40.83.177.42

This page is intentionally left blank.

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

Security Reference Guide — Doc. 8956B

03/04/21
Specifications subject to
change without notice.