Crestron Go App

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

Overview

The Crestron Go App turns an Apple® iPhone® or iPad® device into a mobile Crestron® touch screen with Super Retina® display support, enabling complete control of AV systems, lighting, shades, climate control, security, and other systems from virtually anywhere. The Crestron Go App can be programmed with Smart Graphics® technology, making it easy to deliver a custom user experience that is both dynamic and intuitive. Additional capabilities include viewing video from IP-based security cameras, communicating with other Crestron touch screens using the Rava® SIP Intercom, and seamless integration with third-party apps.

This document describes security features and secure configuration instructions for the Crestron Go App on iPhone devices (CRESTRON-GO) and iPad devices (CRESTRON-GO-TABLET).

Ports and Protocols

The following ports and protocols may be used by the Crestron Go App depending on the system design and configuration.

Common Ports

Function	Destination Port	From (Sender)	To (Listener)	Notes
Crestron-CIP	41794/TCP	Application	Control System	Crestron Internet Protocol, used for bidirectional Crestron IP communication
Crestron-SCIP	41796/TCP	Application	Control System	Secure Crestron Internet Protocol, used for bidirectional Crestron IP communication
Crestron Name Resolution	41794/UPD	Application	Control System	UDP broadcast for Crestron name resolution
HTTPS	443/TCP	Application	Control System or Security Camera	Secure HTTP port used to download a Smart Graphics® project, or optionally for MJPEG streaming video playback
HTTP	80/TCP	Application	Control System or Security Camera	Unsecured HTTP port used to download a Smart Graphics® project, or optionally for MJPEG streaming video playback
RTSP	554/TCP	Application	Security Camera or Streaming Server	Optional, used only for streaming video playback, port can vary depending on camera or server
SIP	4060/TCP or 5060/TCP	Application	SIP Server	Optional, used only for Rava® SIP intercom feature (bidirectional SIP endpoint)

User Access

No login credentials are required to access the Crestron Go App, and no user roles or profiles are supported. However, to connect the app to a control system, the username and password for the control system admin account must be provided along with the control system IP address and port on the network.

> **NOTE:** For more information on setting password rules and password best practices for a 4-Series™ control system, refer to the 4-Series Control Systems Security Reference Guide.

Communication Between the App and Device

The Crestron Go App must initiate communication with a connected control system. Communication is encrypted with X.509 certified TLS 1.2 authentication, so no data is exposed between the app and control system. To prevent communication to the control system, its credentials can be deleted from the app at any time. Encryption can be turned off for connections to legacy control systems if desired.

The app supports HTTPS project downloads. The app does not support certificate validation.

Data Storage and Encryption

The following sections describe how data storage is handled within the Crestron Go App.

User Data Storage

The admin account username and password for a connected control system are stored by the app.

Location information based on the Bluetooth™ proximity beacon is captured to allow for use of the PinPoint™ beacon feature. This information is ephemeral and is never transmitted off device or saved. App permissions may be removed if this feature is not desired.

No other personal information is captured or stored by the app.

Password Encryption

The Crestron Go App does not support on-device encryption for the password of a connected control system. However, this is mitigated by OS-level encryption, as the iOS® operating system has supported OS-level encryption since iOS 10.3.

Ensure that your device is running iOS 10.3 or higher for proper password encryption.

Policy and Process

Crestron has a full Software Development Lifecycle to propose and approve changes at the product management level. The implementation of these changes is specified and all source code is reviewed. Source code is kept in a Version Control System (VCS). Both the completion of the code review and the code reviewer are recorded in the VCS.

Maintenance Support Period

The Crestron Go App is currently in the Maintenance Support Period phase of the Software Development Lifecycle, which entails the following:

- Technical support is still provided by Crestron for software issues.
- Crestron will no longer develop new feature enhancements, upgrades, or additional functionality for the app.
- Crestron will conduct security vulnerability monitoring, provide security updates, and make critical bug fixes to ensure that the app generally conforms to published specifications.
- The app must be upgraded to the latest software version to avail itself of any critical bug fixes or security updates made available by Crestron. These updates will be documented in the app release notes for each software version. Crestron will not provide patches to earlier software versions.

App Logging

The Crestron Go App has the ability to capture log files that record app usage and data. Logging is turned off by default and should be turned on only at the request of Crestron technical support or engineering.

Observe the following points about app logging:

- App logs are stored on the mobile device and can be transferred off only via end-user action. Logs are never transmitted off device automatically.
- Uninstalling the app will also delete any captured log files.

Control System Security

For optimal security when using the Crestron Go App, the control system that is connected to the app should be hardened as described in the 4-Series Control Systems Security Reference Guide.

The following best practices should be followed when connecting the Crestron Go App to a control system:

- Use secure ports over nonsecure ports for the control system connection. By default, the secure CIP (Crestron Internet Protocol) port for a 4-Series control system is 41796 and HTTPS port is 443.
- Create a strong password policy to help prevent brute force attacks.
- Use a static IP address when possible, as this can help reduce the chance of a control system connection being redirected.

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

Security Reference Guide — Doc. 9351A
09/22/22
Specifications subject to
change without notice.