ZUM-HUB4

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.

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.

Revision History

Rev	Date	Notes	Author(s)
A	November 30, 2023	Initial version	IH, PC

Please send comments and change recommendations to:

SecurityDocs@crestron.com

Contents

Introduction

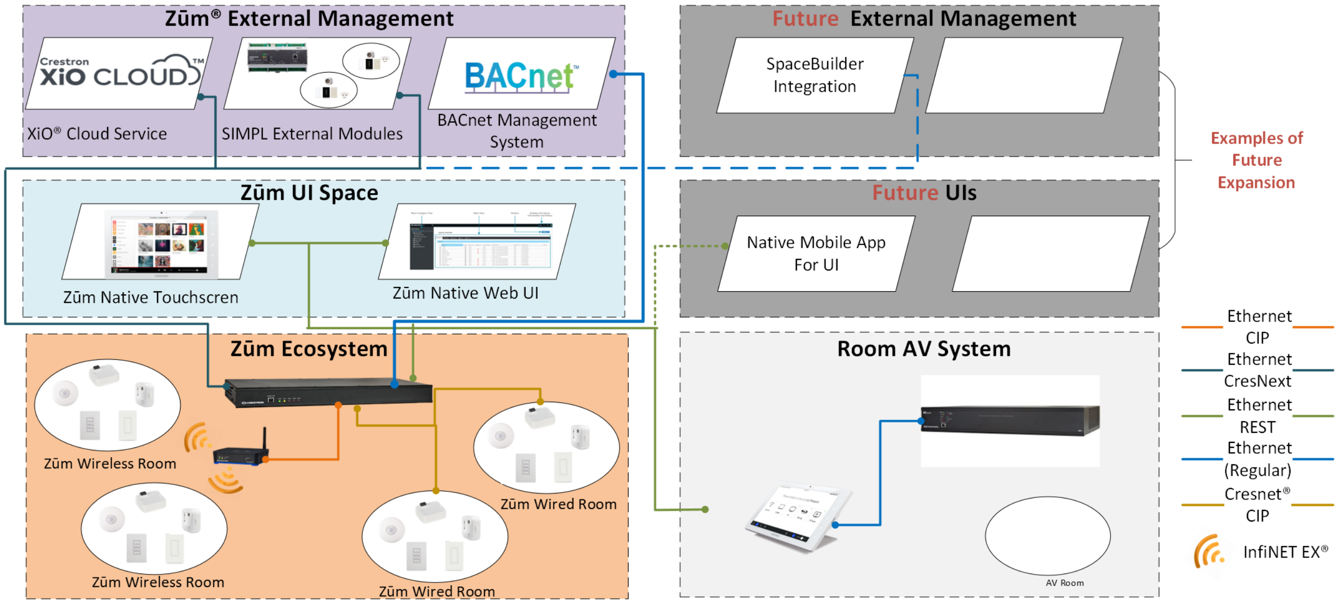
This guide serves as a security reference and provides best practices for deploying the ZUM-HUB4. The ZUM-HUB4 enables centralized management for Zūm® commercial lighting systems of up to 1,000 rooms with an Ethernet switch (sold separately) across Zūm wired, Zūm wireless, and external spaces. The device provides a web-based user interface for control. A built-in time clock enables room lighting and occupancy and vacancy sensing automation. The ZUM-HUB4 can also be integrated with other Crestron lighting systems and control systems.

Intended Operational Environment

The ZUM-HUB4 is designed for installation in various Zūm commercial lighting systems. Crestron assumes the following about the ZUM-HUB4 operating environment:

- The device is not capable of Multi-Factor Authentication (MFA).
- Physical security is commensurate with the value of the system and the data it contains and is assumed to be provided by the environment.
- Administrators are trusted to follow and provide all administrator guidance.

The following diagram shows the ZUM-HUB4 network communication flow. For more information on the external ports shown, refer to Network Port List on page 8.



Security Policies

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

System Specifications

For general product specifications, refer to the ZUM-HUB4 product page.

Product Software - Security Features

The following security features are supported.

User Authentication

The first time the web configuration interface is accessed, a page is displayed asking the user to create an admin account. A similar prompt is displayed when connecting to the touch screen via Crestron Toolbox™ software if an admin account has not already been created. The admin account credentials are required for accessing the device web configuration interface. Additional users can be created and managed using the web configuration interface.

Connectivity

The ZUM-HUB4 can connect to the XiO Cloud® provisioning and management service for monitoring and configuration. For more information on the security features provided by the XiO Cloud service, refer to the XiO Cloud Service Security Reference Guide.

Zūm spaces support connectivity using the following management portals:

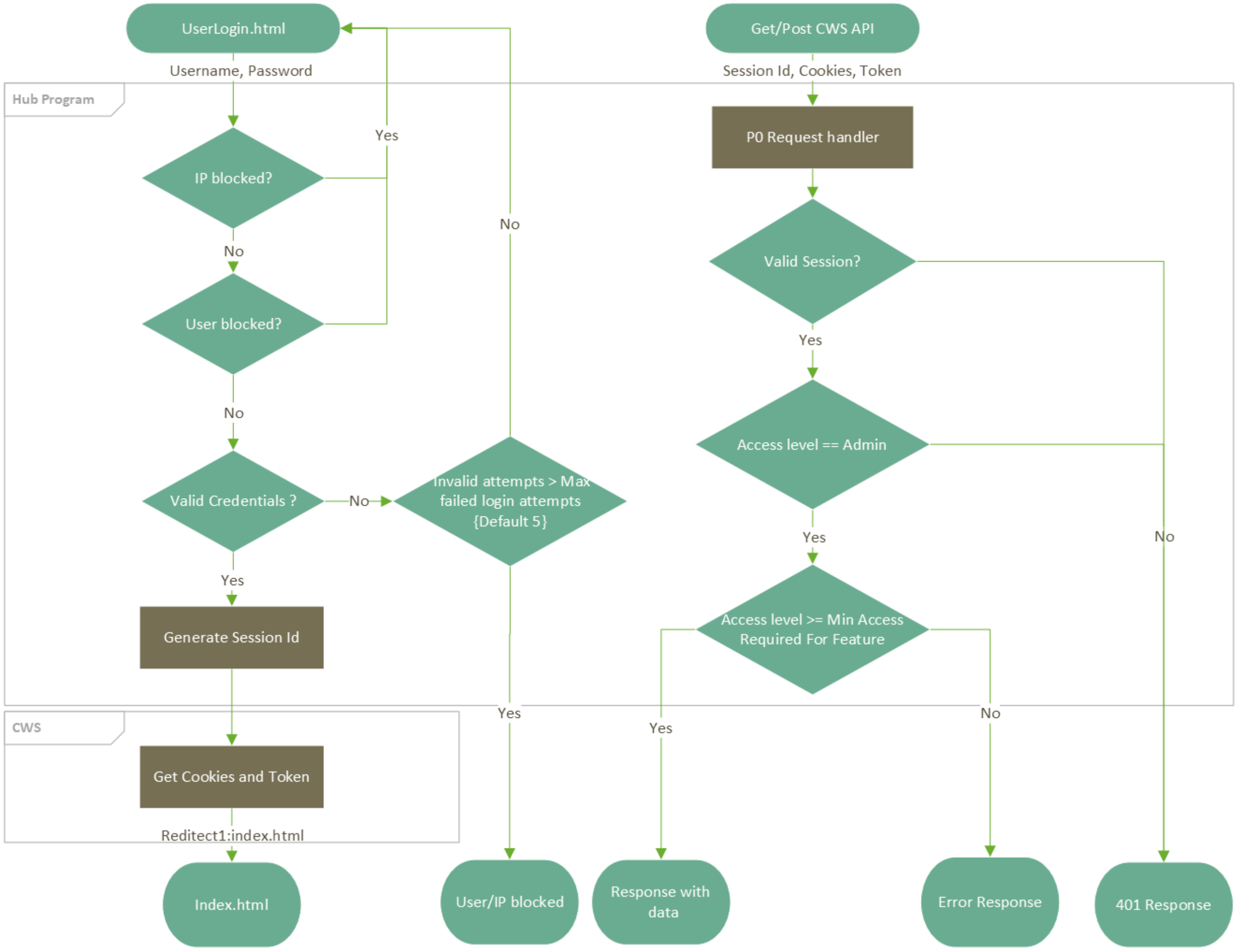
- **Zūm Hub Web Interface**: Provides a central point for viewing and managing Zūm spaces via the device web configuration interface.
- **Zūm App Interface**: The mobile app enables installers to customize and commission rooms within the Zūm ecosystem. With the app, installers can set scenes and set up sensors.

> **NOTE:** The ZUMLINK-KP Bluetooth® connection is required to configure a Zūm wired space with the Zūm app.

The following workflows are provided to describe various ZUM-HUB4 connections.

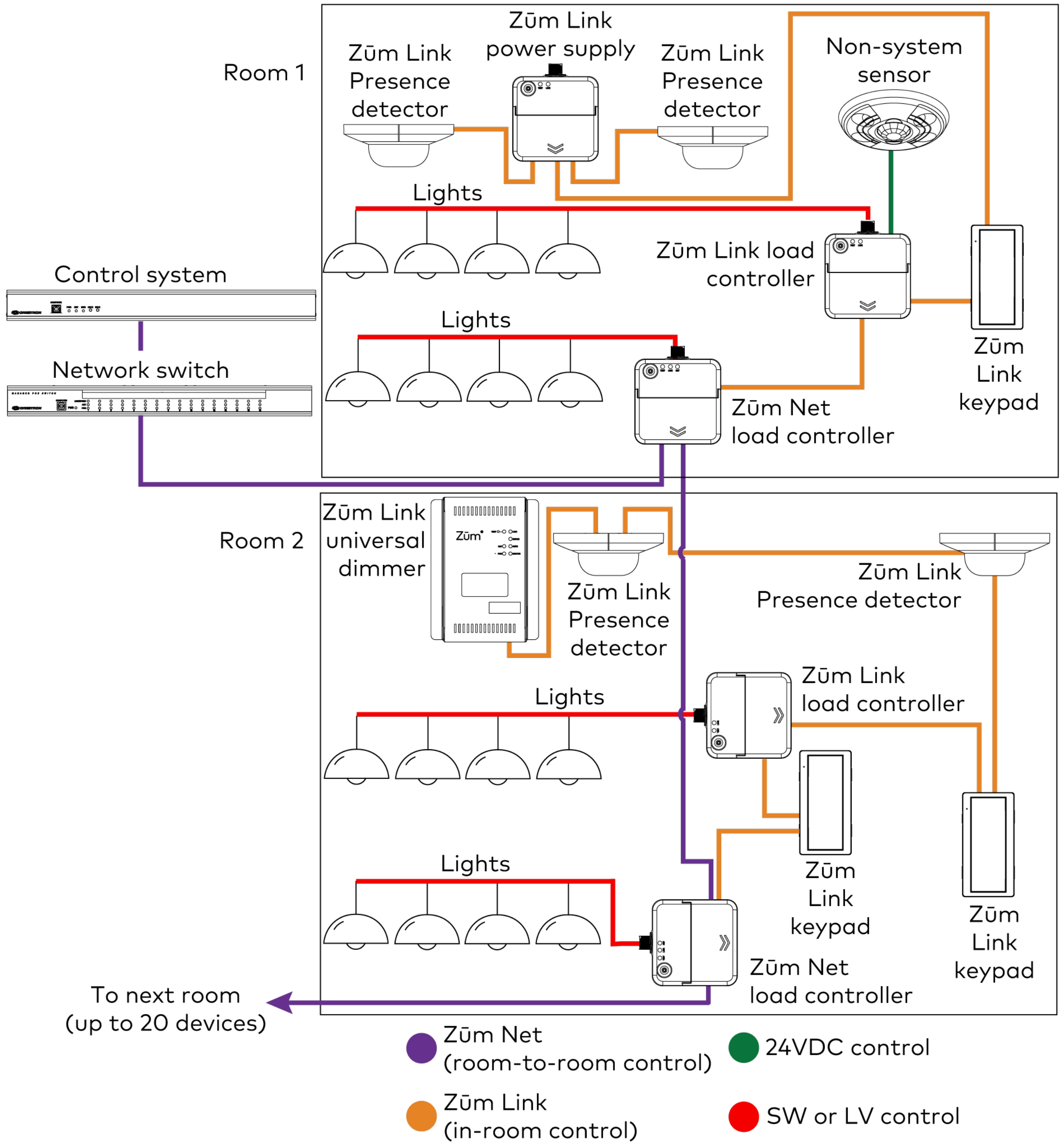
Web User Interface

The following diagram illustrates the process of logging in to the ZUM-HUB4 web user interface.



Zūm Net Connection

The following diagram shows how a Zūm system can be configured via a Zūm Net connection.



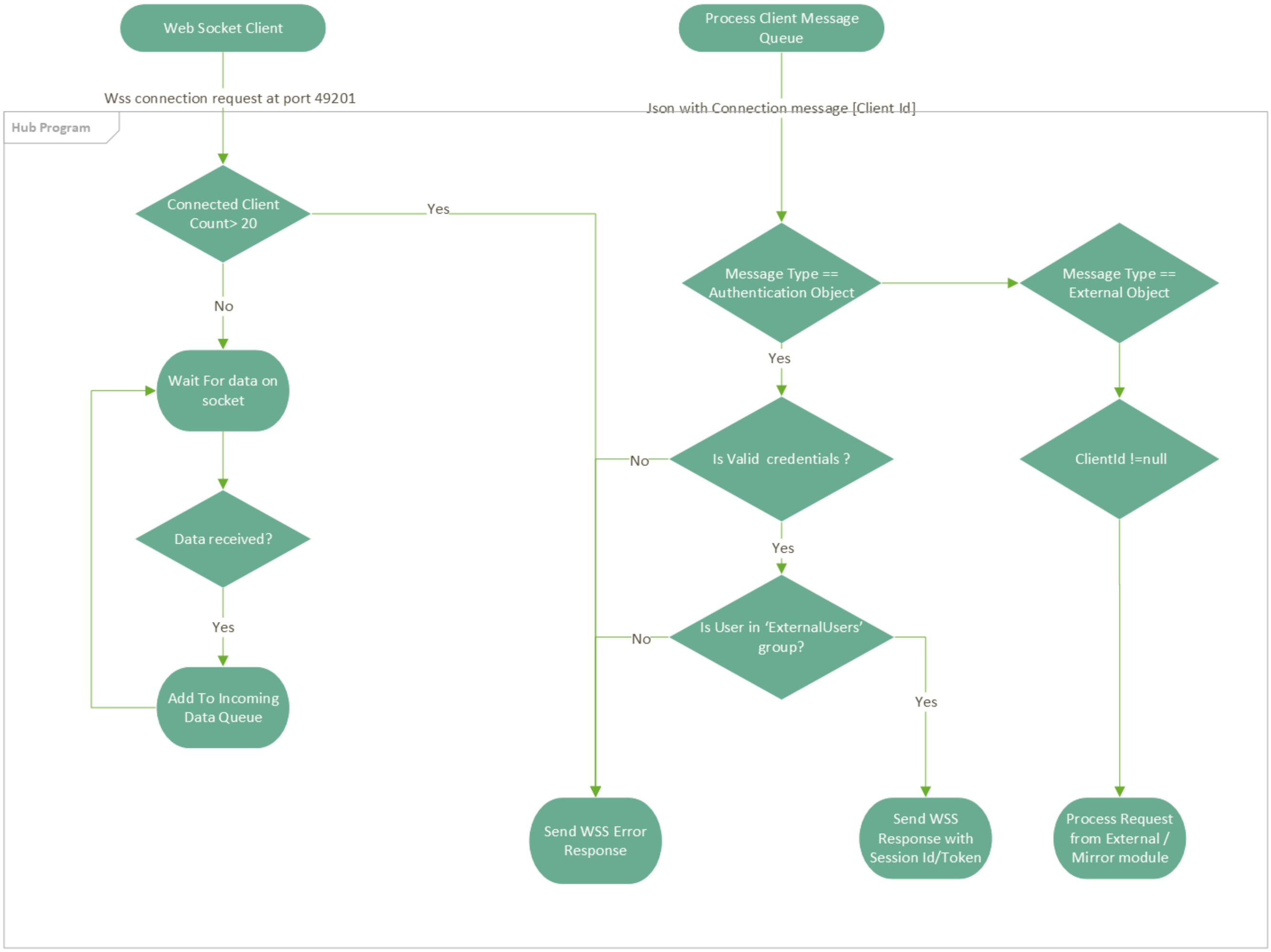
Zūm System Integration with Other Control Systems

In addition to managing rooms equipped with Zūm lighting control, the ZUM-HUB4 enables integration with other Crestron systems over an Ethernet connection. Two methods of integration are available:

- **External Rooms**: A virtual room using legacy or conventional Crestron lighting control can be added to the Zūm network to be monitored, controlled and scheduled.

- **Mirrored Rooms**: An external Crestron system controls and monitors a room equipped with a Zūm system. Mirrored rooms allow for room control with a Crestron touch screen or handheld remote, as well as integration with shading, climate control, AV, and other equipment.

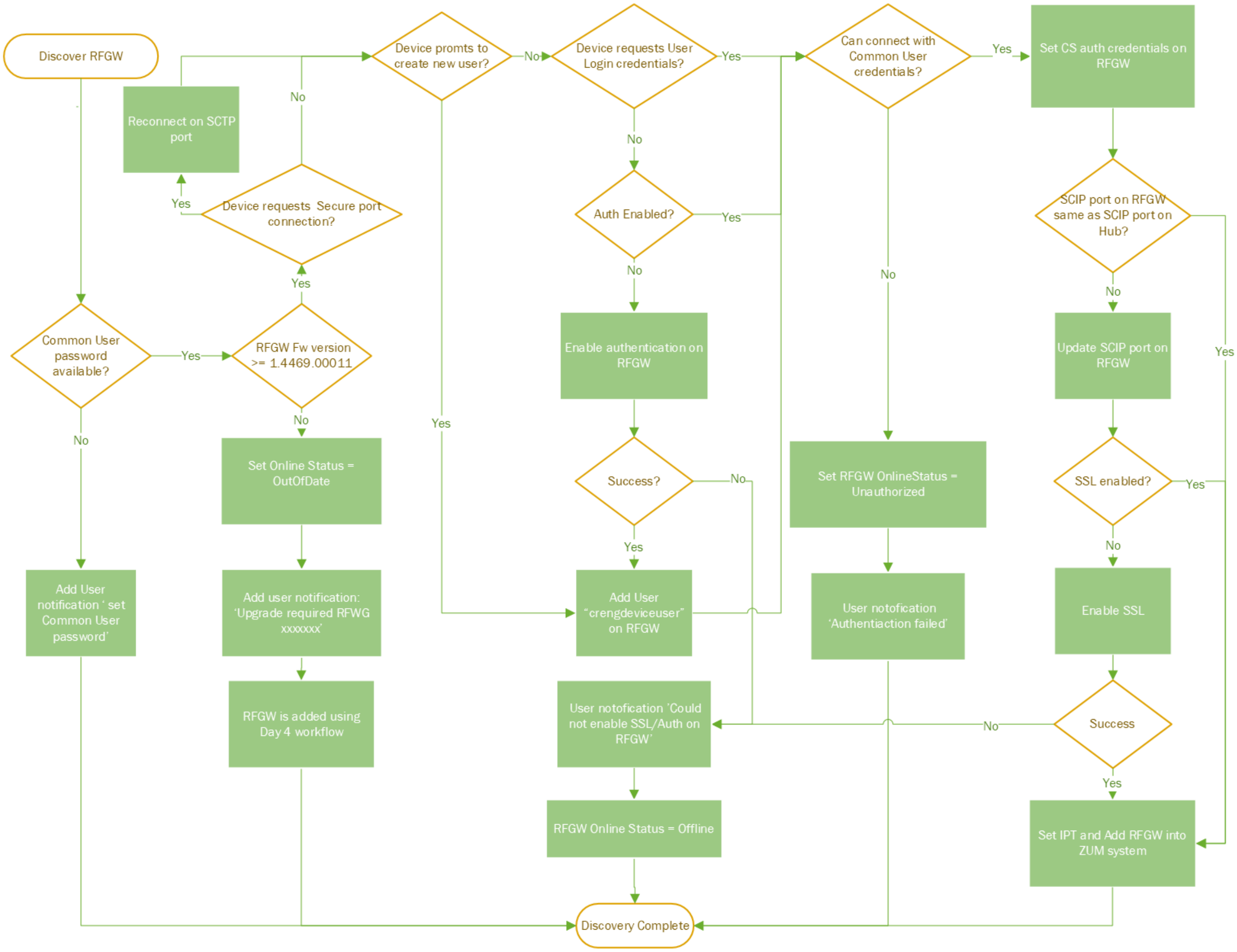
The client program connects over the WebSocket at port 49201. To protect against random access, the connection will require successful authentication with the Zūm Hub before any APIs are available. The user credentials used for authentication must belong to a valid user on the Zūm Hub associated to the **ExternalUsers** group.


Web Socket Client
Process Client Message Queue
Wss connection request at port 49201
Json with Connection message [Client Id]
Hub Program
Connected Client Count> 20
Yes
No
Wait For data on socket
Data received?
Yes
Add To Incoming Data Queue
Message Type == Authentication Object
Message Type == External Object
Yes
No
Is Valid credentials ?
ClientId !=null
Yes
No
Is User in 'ExternalUsers' group?
Yes
Send WSS Error Response
Send WSS Response with Session Id/Token
Process Request from External / Mirror module

RF Gateway Connection

The ZUM-HUB4 connects to a Crestron RF gateway over the SCTP port. The login credentials for **crengdeviceuser** are used to authenticate the device. The password for this user can be updated on the **Security Configuration** accordion under **Settings** in the web configuration interface.

If the Secure CIP port configured on the RF gateway does not match the ZUM-HUB4, the ports on the device will be updated once an Ethernet connection is established.


Discover RFGW
Reconnect on SCTP port
Device promts to create new user?
No
Device requests User Login credentials?
Yes
Can connect with Common User credentials?
Yes
Set CS auth credentials on RFGW
No
Yes
Device requests Secure port connection?
Yes
Auth Enabled?
Yes
No
SCIP port on RFGW same as SCIP port on Hub?
No
No
Common User password available?
Yes
RFGW Fw version >= 1.4469.00011
Enable authentication on RFGW
Update SCIP port on RFGW
Yes
No
No
Yes
Set Online Status = OutOfDate
Success?
No
Set RFGW OnlineStatus = Unauthorized
SSL enabled?
Yes
Yes
No
Add User notification ' set Common User password'
Add user notification: 'Upgrade required RFWG xxxxxxx'
Add User "crengdeviceuser" on RFGW
User notofication 'Authentiaction failed'
Enable SSL
RFGW is added using Day 4 workflow
User notofication 'Could not enable SSL/Auth on RFGW'
No
Success
Yes
RFGW Online Status = Offline
Set IPT and Add RFGW into ZUM system
Discovery Complete

Software Updates and Patches

Crestron is responsible for providing ZUM-HUB4 updates and security patches when necessary via firmware updates. The customer is responsible for running any firmware updates. The customer is also responsible for any custom security configurations and update management.

Operating Systems

The ZUM-HUB4 uses the Linux® OS version 4.19.35 operating system. Configuration of the operating system is not required.

Network Configuration

The ZUM-HUB4 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 off in the Linux OS.
- **Unneeded Ports**: Any ports besides those listed on the Network Port List on page 8 are disabled.
- **Unneeded Applications**: All unnecessary applications have been removed from the Linux OS for the product.
- **8021.X IEEE**: 802.1X authentication is supported.

Network Port List

The ZUM-HUB4 requires the following external and internal ports to be open while the device is running. These ports are opened by default.

Crestron Control Devices

Function	Destination Port	From (Sender)	To (Listener)	Notes
Crestron-CIP	41794/TCP	Remote Device	Device	Crestron Internet Protocol
Crestron-SCIP	41796/TCP	Remote Device	Device	Secure Crestron Internet Protocol
WSS	49200/TCP	Remote Device	Device	Web API for Crestron HTML5 User Interfaces
WSS	49201/TCP	Remote Device	Device	WebSocket Protocol for External Module Interface

Common Ports

Function	Destination Port	From (Sender)	To (Listener)	Notes
NTP	123/UDP	Device	NTP Server	Network Time Protocol (NTP)
SSH/SFTP	22/TCP	Admin Workstation	Device	Used for configuration, console, and file transfer
LDAP	3268/TCP	Device	LDAP Server	LDAP queries targeting global catalogs
HTTPS	443/TCP	Admin or End User Workstation	Device	Secure web configuration
HTTPS	443/TCP	Device	XiO Cloud® Service	For XiO Cloud services only and not required for device functionality. A persistent connection is made via AMQP over WebSockets. HTTPS services such as routing lookups and file transfers may be used.
DHCP	67/UDP	Device	DHCP Server	DHCP addressing
DHCP	68/UDP	DHCP Server	Device	DHCP addressing
HTTP	80/TCP	End User Workstation	Device	Redirect to Secure Web Configuration on port 443
Remote Syslog	Configurable	Device	Remote Syslog Server	Uses TLS

Function	Destination Port	From (Sender)	To (Listener)	Notes
SNMP	161/UDP	SNMP Manager	Device	
SNMP Traps	162/UDP	Device	SNMP Manager	
RADIUS	1812/UDP	Device	RADIUS server/client	RADIUS communications for Authentication and Authorization, for Multi-Factor Authentication (MFA) support.
BACnet	47808-47823/UDP	Device	BMS client	BACnet protocol communications with a Building Management System (BMS)

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 ZUM-HUB4 provides the following malware and vulnerability protection.

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.

Role-Based Access Control

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

Password Security

The following password security rules are enforced by the device:

- Minimum length of characters 10
- Password must contain at least one lower case character.
- Password must contain at least one upper case character.
- Password must contain at least one number.
- Password must contain at least one special character.
- User account locking is supported.

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 ZUM-HUB4 segregates data as follows when connecting the XiO Cloud service.

Cloud Storage

All data stored in the cloud is kept in a Microsoft® Azure® multitennant database.

Physical Protection

All physical servers are managed by the Microsoft Azure service 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

Crestron applications write all security events to text based log files on the system that can be manually audited by administrators. Syslog and audit logging (if enabled) are included in the device logs. Customers must download device logs and share with Crestron manually if a review is requested by the customer.

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 ZUM-HUB4, observe the following best practices:

- 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. 9463A
11/28/23
Specifications subject to
change without notice.