



XiO Cloud®

Provisioning and Management 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.

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](http://www.crestron.com/legal/software_license_agreement).

The product warranty can be found at [www.crestron.com/warranty](http://www.crestron.com/warranty).

The specific patents that cover Crestron products are listed at [www.crestron.com/legal/patents](http://www.crestron.com/legal/patents).

Certain Crestron products contain open source software. For specific information, visit [www.crestron.com/opensource](http://www.crestron.com/opensource).

Crestron, the Crestron logo, and XiO Cloud are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Active Directory, Azure, and Microsoft are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks, registered trademarks, and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Crestron disclaims any proprietary interest in the marks and names of others. Crestron is not responsible for errors in typography or photography.

©2023 Crestron Electronics, Inc.

# Contents

- Introduction** ..... 1
- User Access** ..... 2
  - Single Sign-On Support ..... 2
  - User Roles and Access Levels ..... 2
  - Azure Tenant Restrictions ..... 3
- Communication Between the Device and Cloud** ..... 4
- Data Storage in the Cloud** ..... 6
  - In-Transit and At-Rest Encryption ..... 6
  - Certifications ..... 6
  - Microsoft Services ..... 7
- Device Claiming** ..... 8
- Policy and Process** ..... 9
  - Cloudware Vulnerability Process ..... 9
  - Audit Logging ..... 9
  - Privacy Policy ..... 10
  - Multifactor Authentication ..... 10
  - Communication Port ..... 10
- URLs and IP Addresses** ..... 11

# Introduction

The XiO Cloud® service allows all supported Crestron® devices and certain supported third-party devices across an enterprise to be managed and configured from one central, secure location in the cloud. The XiO Cloud service may be used to view the status of a device, to configure various device and network settings, to manage licenses, and to update device firmware.

Based on Microsoft's industry-leading Azure® Internet of Things (IoT) platform, this multi-tenant cloud service is designed with security in mind. Documentation on the Azure IoT platform can be accessed at Microsoft's [website](#).

# User Access

Azure Active Directory® software, which is trusted by multinational enterprises for internal directory management, manages user access securely. Crestron has no access to the usernames or passwords used to sign into the cloud provisioning device.

## Single Sign-On Support

The XiO Cloud service supports both SAML and OpenID Connect for single sign-on (SSO). The solutions are supported by all major identity providers including Azure Active Directory.

## User Roles and Access Levels

The following user roles can be assigned to users within the XiO Cloud service.

- **Global Administrator:** This role grants the user complete access to every part of the system. The user may add other global administrators. There must always be at least one global administrator in the system.
- **Standard User:** Grants the user limited levels of access based on assigned groups. This user may not add other global administrators.

Standard users can then be assigned the following access levels to groups and rooms within the XiO Cloud environment:

- **Viewer:** Grants the user read-only access to the group or room. The user may view devices within the group or room but cannot modify them.
- **Tech:** Grants the user read and write access to the group or room. The user may view the status of devices and change device settings within the group or room.
- **Administrator:** Grants the user read and write access to the group or room and allows the user to change the access level of other users to the group or room.
- **Hidden:** Hides the group or room from the user within the group tree.

For more information on setting user access within the XiO Cloud service, refer to the [XiO Cloud Provisioning and Management Service User Guide](#).

For more information on the tasks that can be performed for each user role and access level, refer to [Crestron online help answer ID 100007](#).

# Azure Tenant Restrictions

If using Azure tenant restrictions to restrict user access to the XiO Cloud service through Azure Active Directory, the following information is required:

- **Tenant Domain:** mycrestron.onmicrosoft.com
- **Tenant Directory (Directory-ID or Tenant-ID):** f18b53d2-1513-4b5f-b006-86a395b2a130

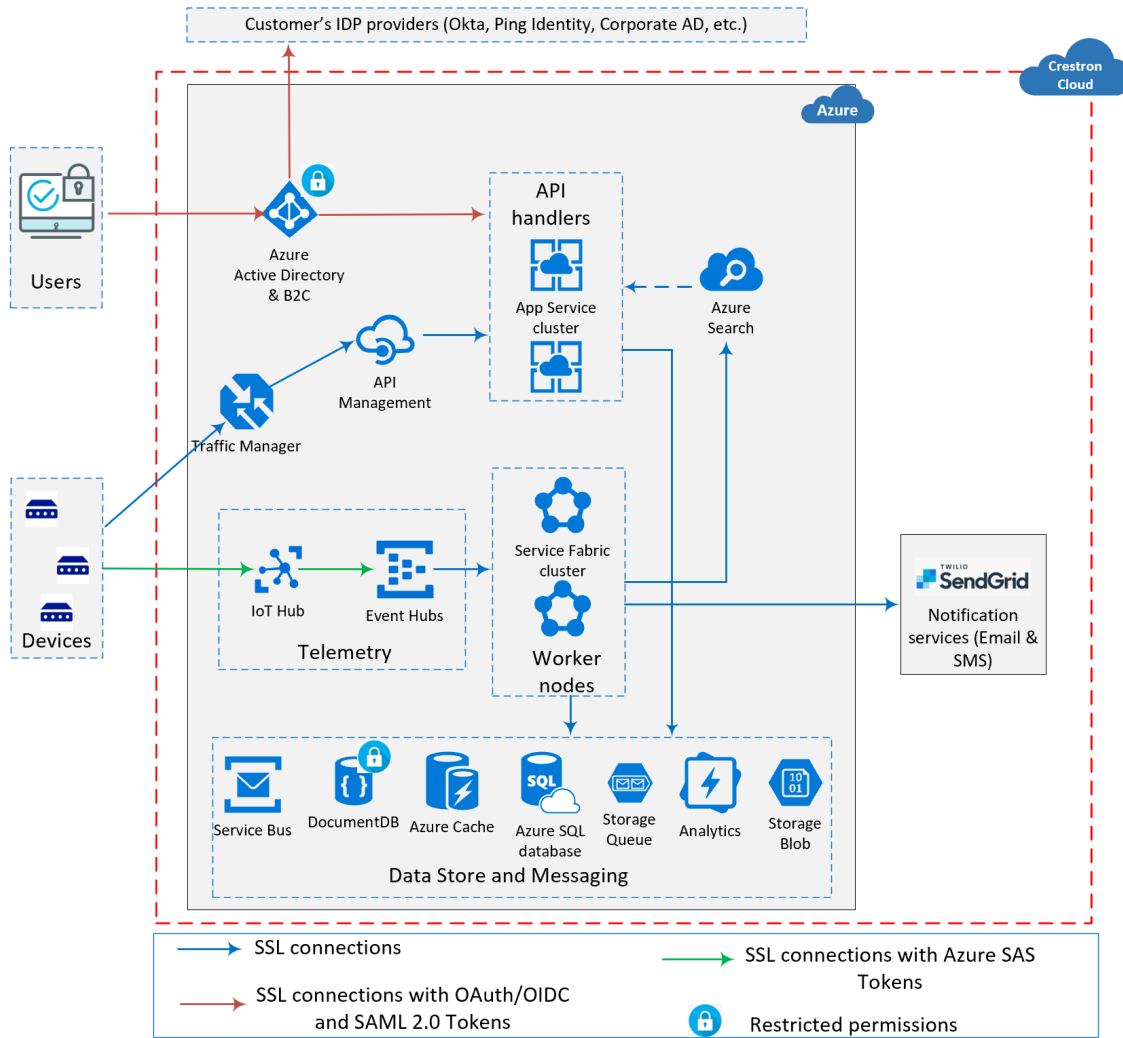
For more information on Azure tenant restrictions, refer to [Microsoft's documentation](#).

# Communication Between the Device and Cloud

The device must initiate communication with the XiO Cloud service. The device will never receive connections from the cloud service. Communication is carried over the Advanced Message Queuing Protocol (AMQP) and encrypted with X.509 certified TLS 1.2 authentication, so no data is exposed between the device and the cloud. The cloud configuration service connection must be enabled on the device for communication. To prevent communication to the XiO Cloud service, this setting can be disabled at any time from the device's local web configuration.

In addition, HTTPS services are used for auxiliary communications such as routing lookups and file transfers.

Refer to the following diagram for a visual representation of how communication occurs between the various components of XiO Cloud.





# Data Storage in the Cloud

The following sections describe how data storage is handled within the XiO Cloud service.

## In-Transit and At-Rest Encryption

Once data is entered into the XiO Cloud service, it is encrypted at rest. The XiO Cloud service is built as a collection of microservices in Microsoft's Azure software. These microservices are authenticated using Azure Active Directory software. All access to data is monitored and audited to identify intrusions or unauthorized access. Passwords for services that are configured on devices are not stored long-term (defined as longer than the minimum amount of time necessary to send the information to the device).

All data is encrypted as follows:

- TLS 1.2 encryption in transit
- AES-256 encryption at rest

**NOTE:** XiO Cloud follows the NIST guidelines for TLS 1.2 as defined at [csrc.nist.gov/publications/detail/sp/800-52/rev-2/final](https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final).

The XiO Cloud service uses Microsoft Key Vault as an encryption agent for establishing and managing cryptographic keys for required cryptography employed within the information system. Microsoft Key Vault is also FIPS 140-2 approved within the Microsoft Azure Commercial Cloud.

The following information is stored in the cloud long-term:

- Settings for your devices and groups
- Group structure you create for your account
- Permissions you give to the users in your account
- Actions within the portal so unauthorized access is automatically monitored

Log files from the device are only sent to the cloud after a user-initiated action.

## Certifications

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

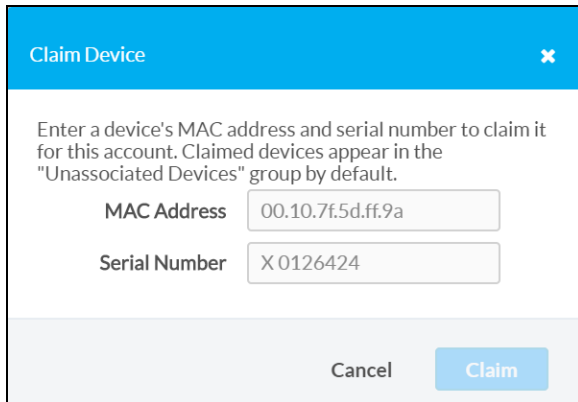
# Microsoft Services

The XiO Cloud service uses the following Microsoft services:

- Azure Active Directory
- Azure Key Vault
- IoT Hub
- Traffic Manager
- API Management

# Device Claiming

Individual devices are claimed to your account in the service using the MAC address and serial number, which includes both a unique identifier and a handshake response. The MAC address and serial number are labeled on the shipping box or on a sticker attached to the device.



Claim Device

Enter a device's MAC address and serial number to claim it for this account. Claimed devices appear in the "Unassociated Devices" group by default.

MAC Address

Serial Number

Cancel Claim

Devices must be claimed by the XiO Cloud service before they may be managed by the service. Devices may be claimed individually or can be claimed as a group using a comma-delimited CSV file.

For more information on claiming devices to the XiO Cloud service, refer to the [XiO Cloud Provisioning and Management Service User Guide](#).

**NOTE:** Supported third-party devices that do not use the Crestron Connected® connection protocol must be claimed using a Crestron control system or the Crestron XiO Cloud™ Gateway software. For more information, refer to the [XiO Cloud® Service Third-Party Device Monitoring Configuration Guide](#).

# 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.

Crestron has both incident response policies with dedicated support and DevOps teams monitoring our cloud services.

XiO Cloud is hosted in Microsoft® Azure software.

Crestron products are regularly subject to internal penetration tests. External penetration tests are also performed at regular intervals. Product security risks are cataloged in a secure area of Crestron's task/defect management system.

Crestron's cloud services have multiple alerts and other monitoring agents in place for issue notification. These services also log all activity, and an audit log is available for end users to monitor their account and device activity.

## Cloudware Vulnerability Process

The Crestron security team responds to discovered vulnerabilities and works closely with our development and devOps teams to ensure security vulnerabilities are fixed and that patches are deployed to all customer instances in a timely manner.

The Crestron security team addresses and discloses vulnerabilities through security advisories for all cloud solutions. XiO Cloud is a SaaS solution that is maintained, patched, and monitored by Crestron, so no user action typically is required.

Service teams may communicate service-related security events to customers through direct notification or a general mass email notification. In addition, the Crestron security team will publish advisory bulletins at [security.crestron.com](https://security.crestron.com).

Crestron uses CVSS scores to rate the severity of discovered vulnerabilities.

## Audit Logging

The XiO Cloud service logs the following information:

- Sign-in activity for non-SSO customers for 30 days
- Sign-in activity for internal accounts for 30 days
- Backend audit logs for 30 days
- Backend activity logs for 90 days

Additionally, users can export the following logs from their XiO Cloud accounts:

- Standard Device Logs
  - Logs taken directly from a claimed device
  - Can be downloaded per device within an account
  - Activity Logs (for the XiO Cloud account)
- Scheduled actions
  - Changed device settings, including the original and new values
  - Licenses that were added to or removed from the device
  - Movement from one group to another
  - Movement between online and offline states

## Privacy Policy

The XiO Cloud service collects, processes, and stores business contact information that may contain limited personal data.

The following data is collected by XiO Cloud:

- Name
- Business email address
- Business phone number
- Device telemetry (geographic location)

Crestron does not collect, process, or store any sensitive personal data such as personal health information (PHI) or financial transactions such as payment card information (PCI).

For more information on Crestron's privacy policy, refer to [www.crestron.com/legal/privacy-policy](http://www.crestron.com/legal/privacy-policy).

## Multifactor Authentication

The XiO Cloud service requires multifactor authentication (MFA) for privileged users (administrative) of the system. XiO Cloud may leverage MFA for provisioned user accounts using a single sign-on solution such as Okta, Azure AD, or SAML 2.0.

## Communication Port

The XiO Cloud service uses port 443 (TCP) to communicate to claimed devices over HTTPS.

# URLs and IP Addresses

The XiO Cloud service is in Azure's US East and US West datacenters. The updated list of IP addresses for these datacenters is available at Microsoft's [website](#).

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

- \*.crestron.io
- \*.azure-devices.net
- manifest.crestron.io
- prdhydrogenfwstorage.blob.core.windows.net
- prduserremoteaccessa.blob.core.windows.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:

- APIM US East: 168.62.165.131
- APIM US West: 40.118.202.13
- FCS US East: 40.71.11.166
- FCS US West: 138.91.240.81
- IoT Hub US East: 20.49.109.145
- IoT Hub US West: 13.86.221.29
- Portal East: 40.121.221.52
- Portal West: 138.91.240.81
- Manifest Hosting: 40.121.221.52
- Firmware Updates: 52.239.153.4
- Remote Access Storage: 52.239.152.138

