



Security Reference Guide

# Crestron Fusion® Cloud Service Software Application

Have feedback on this document? Contact [docfeedback@crestron.com](mailto:docfeedback@crestron.com).

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

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

The Crestron Fusion® Cloud Service Software Application is licensed under Crestron's Cloudware License Agreement, available at [www.crestron.com/Legal/software-products-on-premises-and-cloudware/cloudware-license-agreement](http://www.crestron.com/Legal/software-products-on-premises-and-cloudware/cloudware-license-agreement).

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

Certain Crestron products collect information that may include personal data. For further details regarding those Crestron products that collect, process, and transmit information directly to Crestron via the internet, refer to the Crestron Privacy Statement Regarding Internet Data Collection, located at [www.crestron.com/legal-data-collection-privacy](http://www.crestron.com/legal-data-collection-privacy).

Crestron, the Crestron logo, 4-Series, Crestron Fusion, and eControl are either trademarks or registered trademarks of Crestron Electronics, Inc. in the United States and/or other countries. Active Directory, ActiveX, Microsoft, PowerShell, SQL Server, Windows, and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Nessus is either a trademark or registered trademark of Tenable 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.

©2026 Crestron Electronics, Inc.

# Revision History

| Rev | Date          | Notes                                                |
|-----|---------------|------------------------------------------------------|
| A   | July 21, 2021 | Initial version                                      |
| B   | July 17, 2026 | Updated content to the latest available information. |

Send comments and change recommendations to [SecurityDocs@crestron.com](mailto:SecurityDocs@crestron.com).

# Contents

- Overview ..... 1
- Cloud Information ..... 2
  - Access Management ..... 2
  - Data and Information ..... 2
- Certification ..... 3
- Proxy Servers ..... 4
- Database ..... 5
- Network Communication Flow ..... 6
- Virtual Machine Server ..... 7
  - Technologies ..... 7
  - Client-Side Technologies ..... 8
- Security ..... 9
- Connectivity Requirements ..... 10

# Overview

This document provides security-related information for various components of the Crestron Fusion® Cloud Service software application. In addition, the document provides information about Microsoft® Windows® services and features installed or utilized by the Crestron Fusion Cloud Service, as well as any TCP or UDP ports used in communication.

# Cloud Information

Crestron Fusion In the Cloud Service (FITC) is installed on a dedicated Virtual Machine (VM).

All VMs in the deployment are joined to a domain to provide better security and efficient account maintenance.

The database is hosted on an Azure® SQL managed instance. Each customer's FITC subscription consists of one or more VMs and one Azure SQL managed instance. If multiple VMs are required, an Azure load balancer is also implemented.

## Access Management

Three forms of access management are supported by FITC:

- IIS Forms authentication
- Azure AD authentication
- Security Assertion Markup Language (SAML)

The following information applies only to IIS Forms authentication:

- An account is required to login to the FITC instance. Groups and user accounts are created within the application and stored in the SQL database. Users are required to provide a username and password to log in to the application. The username must be unique in the database.
- Passwords are stored using SHA-256, which is a one-way hash method. User accounts can be enabled or disabled, and passwords can be reset from within the application. There is one default administrator account that can be renamed or disabled.
- Segregation of duties is accomplished by assigning groups to functional and object security policies. These policies control what each user can access within the application.

## Data and Information

FITC includes personally identifiable information (PII), specifically names and email addresses. Data is stored indefinitely by default. Data retention rules can be modified to suit the customer's needs. Other data, such as meeting information and logged attribute data, is retained for one year by default.

Each SQL database is backed up every night. A full backup to a secure blob is performed.

# Certification

FITC is certified to use Microsoft Windows Server 2025 and administers the Windows Server® catalog. FITC requires .NET Framework 4.8.1 to be installed.

# Proxy Servers

Crestron devices on the network can initiate a connection to FITC. Certain Crestron devices support proxy utilization to reach the hosted FITC instance. Devices that do not support proxy need a direct connection to the internet to connect to the FITC instance.

All Crestron devices require local DNS resolution. Some enterprise networks do not support local DNS and rely on a proxy server instead for DNS lookups. The device's `proxyallow` command is used if the device's DNS cannot resolve external addresses.

Other Crestron devices (such as 4-Series® control systems) support `cloudproxyurl` and `cloudproxyauth` commands to reach the hosted FITC instance.



# Database

A Microsoft SQL database instance is used with FITC. Communication with the SQL Server® instance is accomplished using ADO.NET calls. No direct table access is used and all access is done through stored procedures.

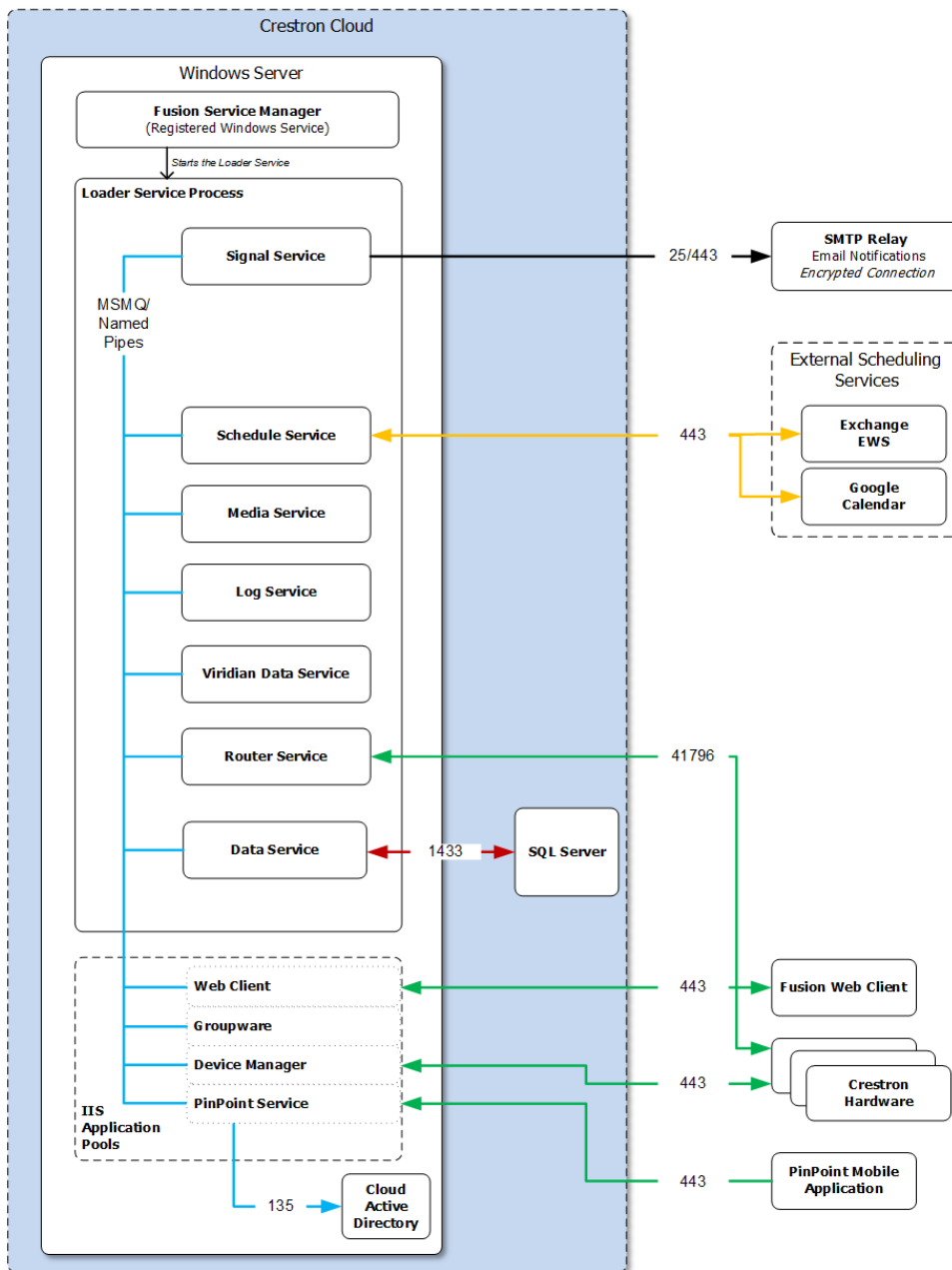
The SQL managed instance performs a full backup every week, a differential backup every 12–24 hours, and a transaction log backup every 5–10 minutes.

By default, the SQL managed instance data is backed up. The backups are encrypted with Transparent Data Encryption (TDE). All backups are encrypted at rest, including Long-Term Retention (LTR) backups. The specifics of TDE (including strength) are defined by Microsoft and cannot be changed.

Additional full backups of the SQL managed instance are made to a local blob storage container on a nightly basis. These additional backups are also encrypted using TDE. The full nightly backups are retained for one year.

# Network Communication Flow

The following image shows the FITC communication flow (all external ports utilize TCP):



# Virtual Machine Server

FITC is an enterprise-level application that requires a Windows IIS Server for hosting the web client and Crestron Fusion services. The operating system used is Windows Server 2025.

## Technologies

The following Windows features are installed or enabled and used with FITC:

- .NET 4.8.1
- IIS 10.0 or greater
- ActiveX™ service: Used for remote control of older Crestron control systems.

Microsoft Operating System features activated by the Crestron Fusion Cloud Service installer:

- Active Directory® service
- Application Server (AS)
- AS HTTP Activation
- Windows Communication Foundation (WCF) Activation
- .NET HTTP Activation
- .NET Non-HTTP Activation
- MSMQ Server
- MSMQ HTTP Support
- RPC Over HTTP Proxy
- ASP.NET
- Web Server (IIS) Tools
- Windows Process Activation Service (WAS)
- WAS .NET Environment
- WAS Configuration APIs
- WAS Process Model
- ADLDS
- AS Ent Services
- AS TCP Port Sharing
- AS Web-Support
- AS MSMQ Activation
- AS Named Pipes
- AS TCP Activation
- Web ODBC Logging

- Web Sockets
- Web Legacy Management Console
- .NET WCF MSMQ Activation45
- .NET WCF Pipe Activation45
- .NET WCF TCP Activation45
- SMTP Server
- PowerShell-V2
- WINS
- eControl® -XPanel

## Client-Side Technologies

XPanel Desktop setup is required on client PCs when using eControl to remotely control Crestron systems. The XPanel Desktop installs an application on the user's computer that is required to load and run a compiled .c3p desktop XPanel project.

# Security

Every component of FITC (.DLL, .EXE) is digitally signed by Crestron.

In addition, FITC is scanned for vulnerability, configuration, and compliance assessments using Nessus® Professional Software.

# Connectivity Requirements

Devices communicating with FITC require direct outbound connectivity to the internet through the following ports:

- 443: HTTPS port provides a stateless-control connection with SSL encryption.
- 41796: Crestron proprietary port provides a stateful CIP protocol connection with SSL encryption.

Refer to [Network Communication Flow on page 6](#) for a detailed diagram.

The path to the internet for the above ports needs to be free and unencumbered by other devices such as WAN optimizers, firewalls, and so on.

Proxy support on proxy enabled devices (other than control systems) only supports HTTP/HTTPS traffic. The CIP connection component for FITC requires a direct connection to the internet.

The proxy on control systems allows HTTP/HTTPS/SOCKS.

