Crestron Fusion® Cloud Service Software Application

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.

Contents

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 Cloud Service is deployed on a Crestron® cloud environment and uses a dedicated Virtual Machine (VM) for the Crestron Fusion application and a separate VM for the Microsoft SQL Server® database.

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

The database is hosted on a SQL Server VM, and a dedicated domain service account is created for each deployment.

Access Management

An account is required to login to the Crestron Fusion Cloud Service. 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

Crestron Fusion Cloud Service includes personally identifiable information (PII), specifically names, email addresses, and meeting subjects. Data is stored indefinitely by default. Data retention rules can be modified to suit the customer's needs.

The SQL database is backed up every night. A full backup is performed.

Certification

Crestron Fusion Cloud Service is certified to use the Microsoft Windows Server 2019 and administer the Windows Server® catalog.

Proxy Servers

Crestron devices on the network initiate a connection to the Crestron Fusion Cloud Service. Devices that support utilizing a proxy to reach the hosted Crestron Fusion Cloud Service are defined below. Devices that do not support proxy needs a direct connection to the internet to connect to the Crestron Fusion Cloud Service.

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

Crestron devices that support proxy include: AM-200, AM-300, TSW-560, TSW-760, TSW-1060, TSS-7, TSS-10, TS-1542, DM-TXRX-100-STR, TSW-570, TSW-770, TSW-1070, TS-770, TS-1070, TSS-770, TSS-1070, TSR-310, DGE-100, DM-DGE-200-C, Crestron Mercury®, and Crestron Mercury® X conference devices.

These processors support `cloudproxyurl` and `cloudproxyauth` for Crestron Fusion in the Cloud: MC4, CP4, CP4N, MC4, DIN-AP4, PRO4, and AV4.

Database

A Microsoft SQL database instance is used with the Crestron Fusion Cloud Service. Communication with SQL Server is done utilizing ADO.NET calls. No direct table access is used and all access is done through stored procedures.

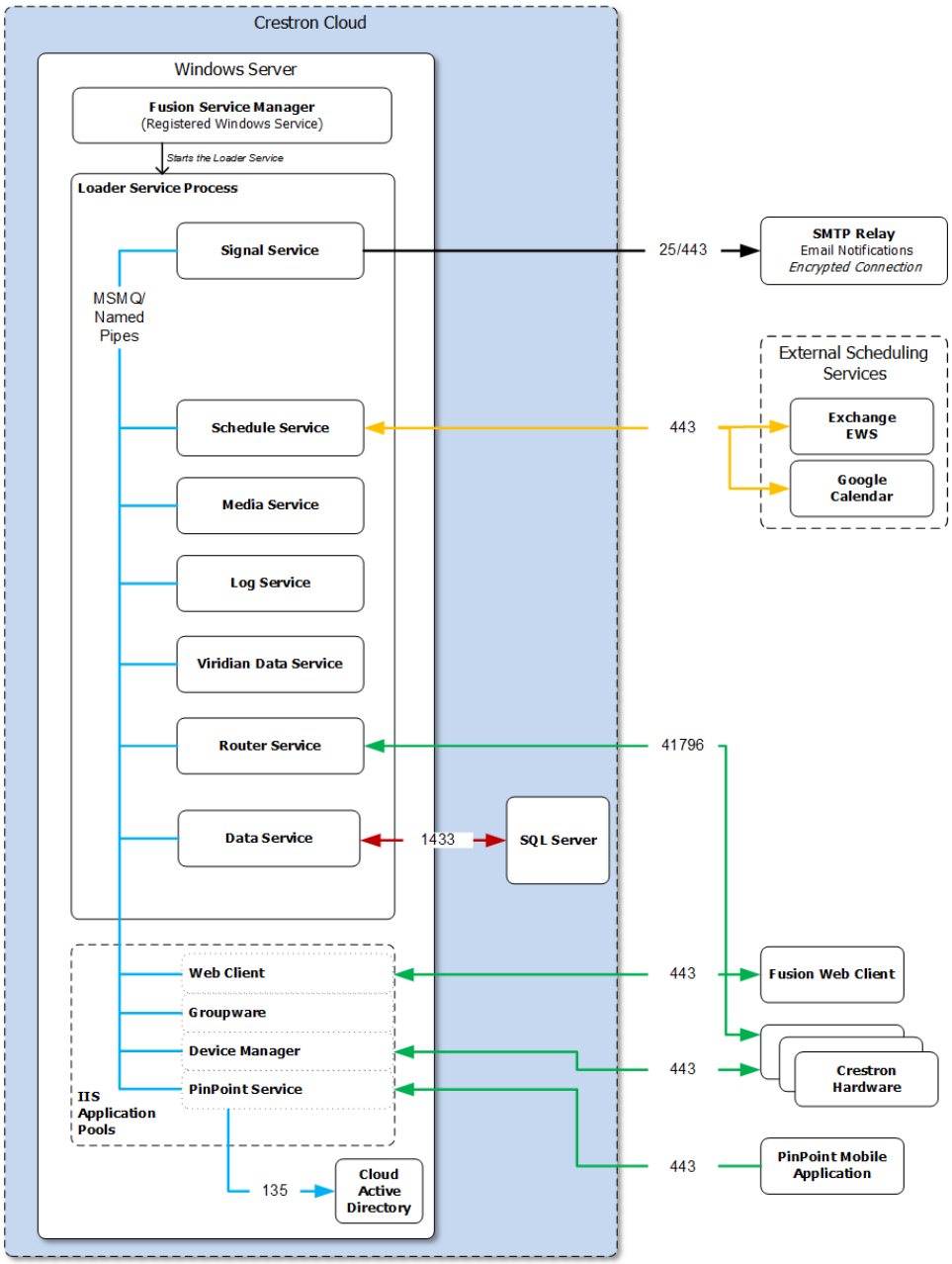
The SQL managed instance performs full backup every week, differential backup every 12-24 hours, and transaction log backup every 5 to 10 minutes.

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 backup 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.

Network Communication Flow

The following image shows the Crestron Fusion Cloud Service communication flow (all external ports utilize TCP):



Virtual Machine Server

Crestron Fusion Cloud Service is an enterprise-level application that requires a Windows IIS Server for hosting the web client and the Crestron Fusion services. The operating system used is Windows Server 2019.

Technologies

The following Windows features are installed or enabled and used with Crestron Fusion Cloud Service:

- .NET 4.5
- IIS 7.0 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 Crestron Fusion Cloud Service (.DLL, .EXE) is digitally signed by Crestron.

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

Connectivity Requirements

Devices communicating with Crestron Fusion Cloud Service 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.

See the Network Communication Flow (on page 3) section 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 Crestron Fusion Cloud Service requires a direct connection to the internet.

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

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

Security Reference Guide — Doc. 9054A

07/21/21
Specifications subject to
change without notice.