CRESTRON FUSION CLOUD SERVICE SECURITY GUIDE

CRESTRON ELECTRONICS, INC.

DOCUMENT HISTORY

Version	Date	Notes	Author
1.00	July 22, 2016	Preliminary	AS

CONTENTS

OVERVIEW

The purpose of this document is to provide security related information on the various components of Crestron's Fusion Cloud Service software application. In addition, the document will provide information about Windows services and features installed/utilized, as well as any TCP/UDP ports used in communication.

CLOUD INFORMATION

Fusion deployments on Crestron's Cloud environment use a dedicated Virtual Machine (VM) for the Fusion Application and a separate VM for Microsoft SQL.

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

The database is housed on a SQL Server VM.

A dedicated domain service account is created for each deployment.

Remote desktop is enabled but does not use a standard port. Every VM uses a different, randomly generated port for Remote Desktop. Remote desktop and access to the operating system is reserved for Crestron use only.

ACCESS MANAGEMENT

Crestron Fusion Cloud users must have usernames and passwords issued. 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 login to the application. Usernames must be unique in the database.

Passwords are stored using SHA256 encryption. User accounts can be enabled and disabled, and passwords reset from within administrative areas of 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 does include personally identifiable information (PII), specifically names, email addresses of users and subjects of meetings. 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.

VIRTUAL MACHINE SERVER

Fusion is an enterprise level application that requires a Windows IIS Server for hosting the web client and the Fusion services.

Windows Server 2012 R2 is the operating system used.

TECHNOLOGIES

The following technologies/Windows system features are installed/enabled and used with Fusion.

Microsoft Technologies:

- .NET 4.5
- IIS 7.0 or greater
- ActiveX: Used for remote control of older Crestron control systems.

Microsoft Operating System Features activated by the Crestron Fusion installer:

- Active Directory
- 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

Adobe

- Flash Player: Flash may be required in the browser client when remote controlling Crestron systems, depending on the type of web page created for the control system.

SERVICES AND COMMUNICATION

Various services are installed with Fusion. For a detailed view of the services communication flow and their relationships, see the section titled “Network Communication Flow”.

For synchronous communication, all services communicate with each other using Windows Communication Foundation (WCF) over Named Pipes. For asynchronous communication, MSMQ is utilized.

Users connect to the Fusion Web Application using HTTPS for all operations.

Crestron Fusion sends messages out using SendGrid on SMTP port 25 with SSL enabled and an authenticated connection.

LOADER SERVICE

The loader service manages a specific set of Fusion services.

The following is a list of those services and their associated communication properties:

Description	**Internal Intra-Service Communication**	**External Communication**
Signal Service	Named Pipes/MSMQ	N/A
Schedule Service	Named Pipes/MSMQ	Secure TCP: 443
Media Service	Named Pipes	N/A
Log Service	Named Pipes/MSMQ	N/A
Viridian Data Service	Named Pipes	N/A

Router Service	Named Pipes/MSMQ	Secure TCP (Crestron SCIP): 41796
Data Service	Named Pipes/MSMQ	Intra-Cloud TCP: 1433

IIS APPLICATION POOLS

Some of the Fusion services are managed by an individual IIS Application Pool.

The following is a list of those services and their associated communication properties:

Description	**Internal Intra-Service Communication**	**External Communication**
Web Client	Named Pipes	Secure TCP: 443
Groupware	Named Pipes	N/A
Device Manager	Named Pipes	Secure TCP: 443 For AirMedia only: 80
PinPoint Service	Named Pipes	Secure TCP: 443

DATA SERVICE

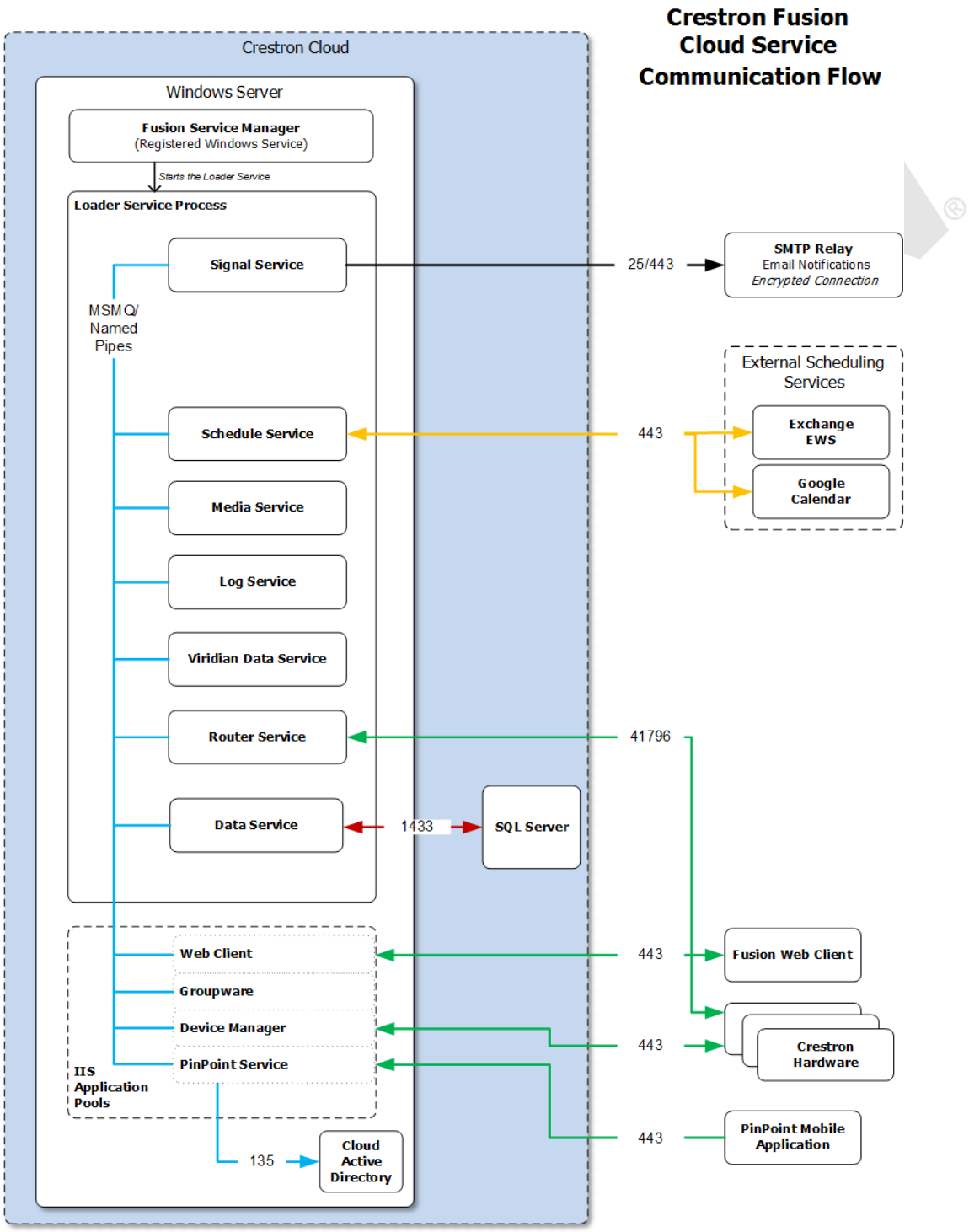
The connection between Fusion's Data Service and SQL uses Windows Authentication. Fusion uses the dedicated domain service account to communicate with SQL. The service account has db_owner rights over its associated database. Installations and upgrades are performed by a Crestron administrator account with SysAdmin rights on the SQL server.

ROUTER SERVICE AND DEVICE MANAGER

Communication between Fusion's Router Service and device endpoints is secured with HTTPS. Communication between Fusion's Device Manager and the endpoints are secured using Crestron's Secure CIP (SCIP).

Registration is initiated by the device over HTTPS using TLS 1.0, 1.1, or 1.2, depending on the capabilities of the device (with the exception of the AirMedia AM-100, AM-101 that uses standard HTTP over port 80). Once registered, communication uses secure CIP over port 41796.

NETWORK COMMUNICATION FLOW



Unless otherwise noted, all external ports utilize TCP.

SECURE COMMUNICATION

Secure communication to and from the Fusion Server is handled by the use of Transport Layer Security (TLS) Version 1.2. If the communicating device does not support 1.2, the Fusion service will fall back to 1.1 or 1.0.

DATABASE

Microsoft SQL Server is used with Fusion. Communication with SQL Server is done utilizing ADO.NET calls. No direct table access is used; all access is done via Stored Procedures.

PROXY SERVERS

Crestron devices on the network initiate connections to the Crestron Fusion Cloud service. This process today does not support going through a Proxy Server. Devices will need a direct connection to the internet in order to connect to Crestron Fusion Cloud service.

CERTIFICATION

MICROSOFT

Fusion has been fully certified for Windows Server 2012 R2 Logo and admission into the Windows Server Catalog.

GOVERNMENT

Fusion has been granted a Certificate of Networthiness (CoN) from the Department of Defense.

SECURITY

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

In addition, Fusion has been scanned for vulnerability, configuration and compliance assessments using Nessus Professional.

CONNECTIVITY REQUIREMENTS

Devices communicating with Crestron Fusion Cloud Service require direct outbound connectivity to the Internet via the following ports:

443: HTTPS port provides stateless Control Connection, SSL encrypted
41796: Crestron proprietary port provides stateful CIP Protocol Connection, SSL encrypted

See the **Network Communication Flow** 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 proxy servers, WAN optimizers, firewalls, etc.