SafeLINC Cloud Connected Services Gateway: Information on configuring bi-directional communication for IT Departments

Introduction

This document contains instructions on how to configure networks and firewall rules for bi-directional communication between gateways, panels, and the SafeLINC Cloud.

SafeLINC Cloud Services is an optional function of the IPC/CSG that allows authorized users to view their fire alarm system activity, in real-time, using the SafeLINC Cloud mobile and web applications. Additional features include push notification services for FACU events and remote access to historical logs and reports.

Gateway configuration use case

For gateway devices commissioned on on-premises networks, ensure that IP traffic is enabled between the following devices:

- IoT Hub
- SafeLINC Cloud
- Central Station, if it is configured

IoT Hub IP addresses and best practices

The Microsoft Azure cloud hosts the SafeLINC Cloud. Microsoft's guidance on network configuration is included in the following section of this document: Configuring the firewall for the SafeLINC Cloud.

ⓘ **Note:** The IoT Hub IP addresses may change without notice. To avoid disruption, always use the hostname when you configure firewall rules.

Configuring the firewall for the SafeLINC Cloud

- To configure the firewall for the SafeLINC Cloud, use DNS hostnames instead of IP addresses to accommodate potential changes in IP addresses.

Configuring the firewall for Central Station

- To configure the firewall for Central Station, the IP addresses and ports specified in the Central Station configuration must be let through the firewall. The protocol is UDP.

Configuring the Connected Services Gateway for Central Station reporting through Ethernet

- To configure Central Station reporting through Ethernet, complete the relevant fields in the Central Station configuration tool. Use the IP addresses and port numbers provided by the Central Station support provider.

18_SafeLinc Cloud Connected Services Gateway
Rev. 2

2025-06-30

Configuring and accessing SafeLINC for the European Union and North America

Use the following information to access the SafeLINC Cloud in the European Union (EU) and North America (NA).

Configuring SafeLINC Cloud for the EU

When you configure firewall or network settings to connect devices to an EU region SafeLINC Cloud, ensure that the firewall accommodates outbound connections for all the listed ports. The customer IT group must provide gateway access to the following sites so that they are not blocked:

SafeLINC Web Architect

https://eu.safelinc.johnsoncontrols.com

https://api-eu.safelinc.johnsoncontrols.com

https://eu-gateway.xaapbuildings.com

Connected Services Gateway

https://global.azure-devices-provisioning.net

https://aihbtsfirestormprod201.azure-devices.net

https://stgpbtsfirestormprod201.blob.core.windows.net

https://aidpsbtsfirestormprod201.azure-devices-provisioning.net

Configuring SafeLINC Cloud for NA

When you configure firewall or network settings to connect devices in a North American SafeLINC Cloud, ensure that the firewall accommodates outbound connections for all the listed ports. The customer IT group must provide gateway access to the following sites so that they are not blocked:

SafeLINC Web Architect

https://safelinc.johnsoncontrols.com

https://api.safelinc.johnsoncontrols.com

https://gateway.xaapbuildings.com

Connected Services Gateway

https://global.azure-devices-provisioning.net

https://aihbtsfirestormprod001.azure-devices.net

https://stgpbtsfirestormprod001.blob.core.windows.net/stciothub

https://aidpsbtsfirestormprod001.azure-devices-provisioning.net

Port numbers

The current gateway devices and the CSG use protocols that operate over TCP to communicate with the SafeLINC Cloud. The following table lists the outbound ports that must be open for device communication and data transmission with the SafeLINC Cloud in the network.

Ensure that all the ports listed are open in the network to facilitate communication.

Table 1: Port numbers

Protocol	Port
AMQP	5671
MQTT	8883
MQTT over WebSockets	443
HTTPS	443

Cybersecurity information for the SafeLINC Cloud

SafeLINC Cloud is developed in Johnson Controls Global Secure Product Development Process. This process is approved to IEC 62443-4-1 by ISAsecure.

A copy of the IEC 62443-4-1 certificate is available here:

https://docs.jci.com/IEC62443-4-1_Certificate

Further information about Johnson Controls cyber security practices is available here:

https://www.johnsoncontrols.com/cyber-solutions/practices

Note: SafeLINC Cloud is not tested by ISAsecure and does not qualify for IEC 62443-4-2 approval but is developed in the certified process listed.