HONEYWELL CONNECTED LIFE SAFETY SERVICES CYBER SECURITY OVERVIEW

Version:1.0

Honeywell

TABLE OF CONTENTS

ABOUT THIS DOCUMENT

This document is primarily intended for Honeywell Connected Life Safety Services (CLSS) ESDs, system integrators and technicians who are interested in understanding the approach taken by Honeywell in securing the CLSS solution. This document also provides details on security architecture, procedures and security controls that describe how to configure the CLSS gateway securely in the site.

Disclaimer:

The material in this document is for information purposes only. The content and the product described are subject to change without notice. Honeywell makes no representations or warranties with respect to this document. In no event shall Honeywell be liable for technical or editorial omissions or mistakes in this document, nor shall it be liable for any damages, direct or incidental, arising out of or related to the use of this document. No part of this document may be reproduced in any form or by any means without prior written permission from Honeywell.

INTRODUCTION TO CLSS

CLSS is an innovative, all-in-one cloud platform that enables systems integrators and facilities managers to deliver an enhanced fire safety service, while maximizing the performance efficiencies offered by Honeywell's trusted detection and alarm systems.

CLSS GATEWAY

CLSS Gateway serves as a bridge between the fire alarm control panel and CLSS Cloud platform. It provides a way to securely connect on-premise fire alarm control panel to the cloud, and provides single path from site to cloud ensures all CLSS cloud services and applications use the same audited and monitored method to access on-premise fire alarm control network.

CLSS WEB APP (SITE MANAGER)

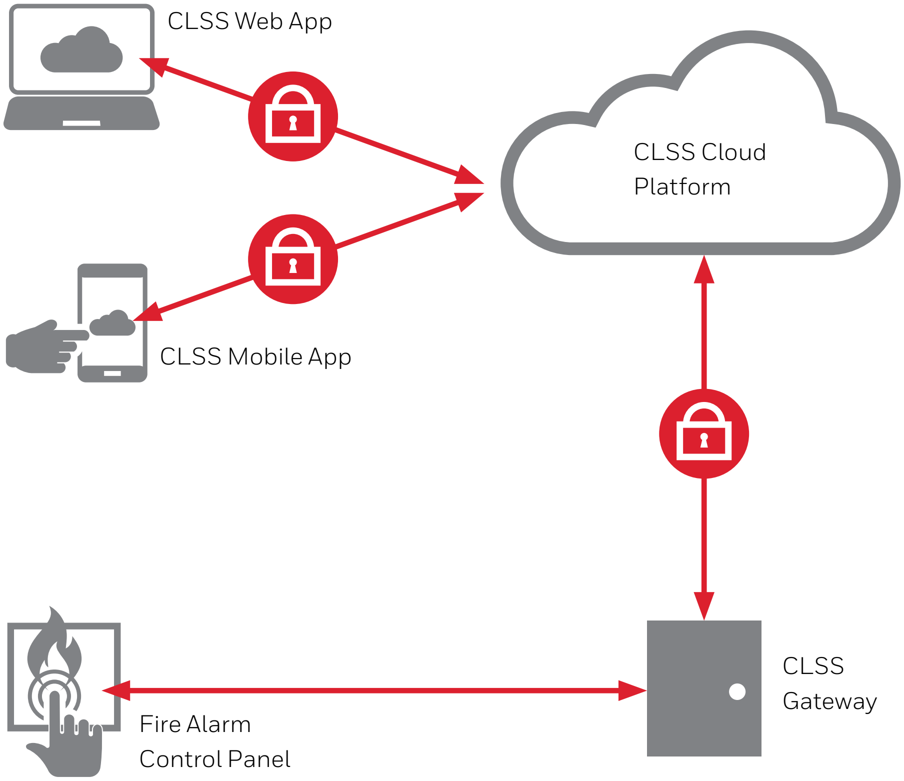
CLSS Site manager is a web application that is used by ESD/SI and technicians to perform back-office administrative and management activities. It provides a consolidated view of their customers' systems. It allows ESDs to onboard their customers' buildings, their users and technicians as well as, configure access privileges for their technicians.

CLSS MOBILE APP

CLSS Mobile App is used by technicians to configure gateway during installation time and to perform regular walk test functionality of both connected and non-connected devices. The app is also used to generate compliance reports.

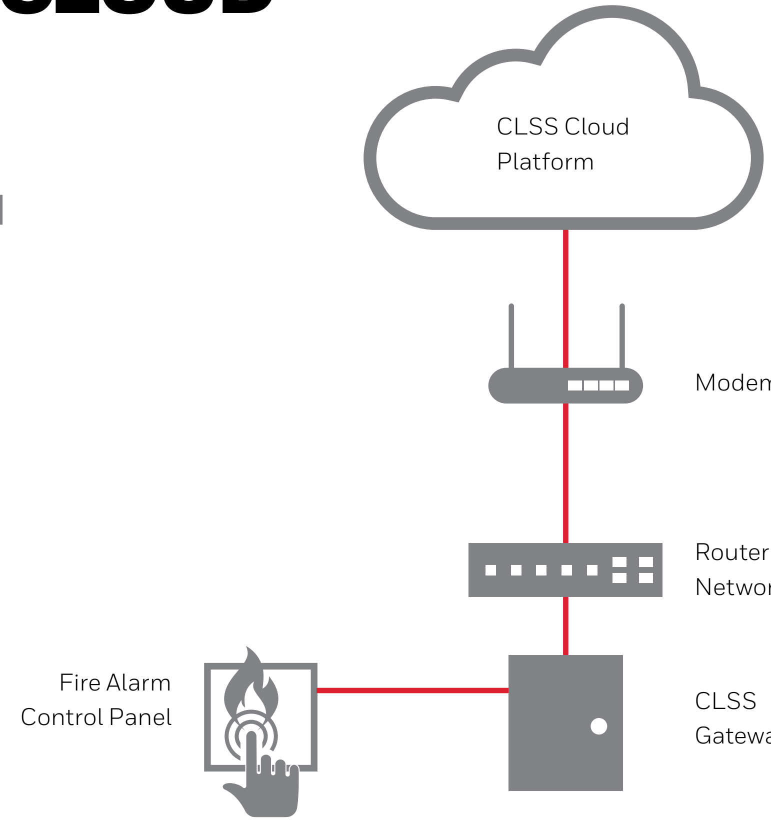
CLSS CLOUD PLATFORM

CLSS Cloud platform contains various micro services to support functionalities of CLSS Gateway, mobile app and web app. It is secure, scalable, standards-based built on the Honeywell Forge enterprise management platform.

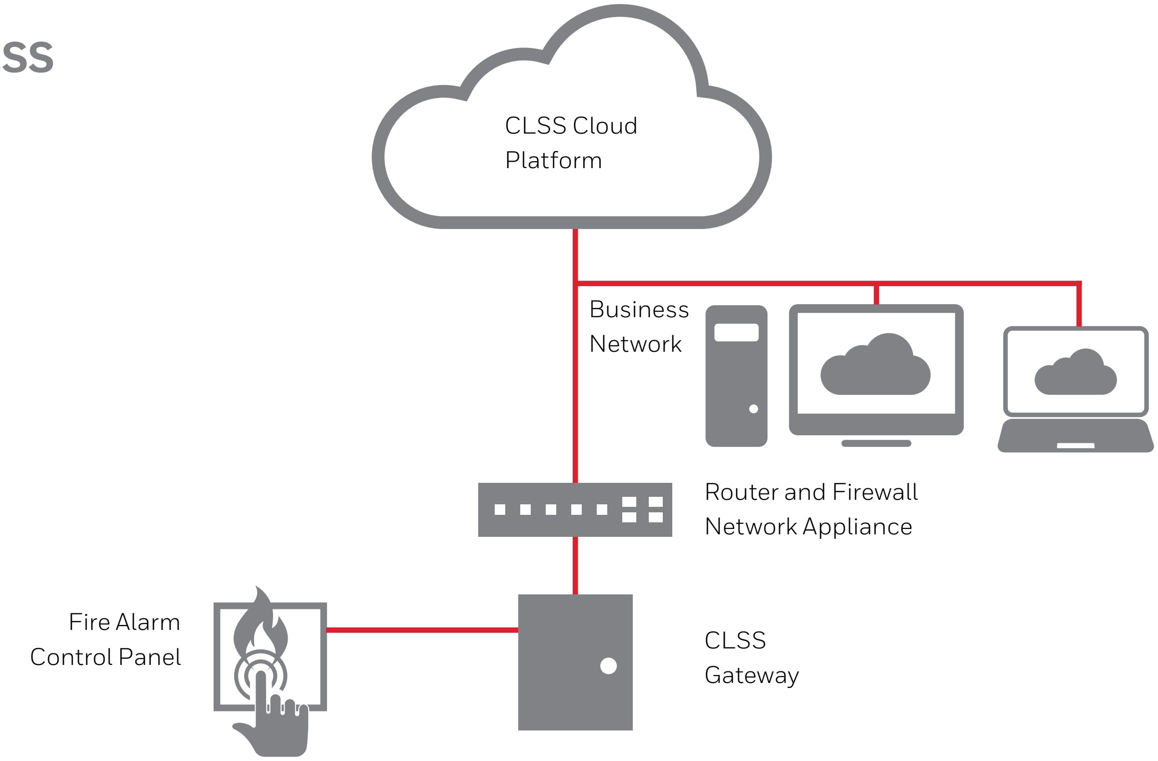


CONNECTING CLSS GATEWAY TO THE CLOUD

APPROACH 1 WITH MODEM



APPROACH 2 WITH BUSINESS NETWORK



WHAT DATA IS TRANSMITTED FROM ON-SITE SYSTEM TO THE CLOUD?

For achieving CLSS Mobile app and Web app (Inspection manager and Site manager) functionality use cases, the following data from the on-site gateway is transmitted to cloud:

- Device inventory received from the fire panel
- Events, alarms and troubles received from the fire panel
- Gateway generated events, alarms and trouble
- Gateway Audit logs with timestamp.

The Device inventory contains all the devices (e.g., detectors, modules) including fire panel connected to the fire alarm system network.

SECURING THE DATA TRANSMISSION

To manage the surface area of the system from a security perspective the CLSS Gateway Cloud Connector only makes outbound calls and no inbound communication is accepted. The outbound connections made are limited to HTTPS for initiating communication and then AMQP over HTTPS for messaging with TLS1.2 and above encryption. AMQP is an OASIS standard messaging protocol designed for reliable and robust messaging which is well suited to scenarios where confirmation of commands and data transfer is required.

Certificate based authentication is used between on-premise gateway and CLSS Cloud platform.

INFRASTRUCTURE NEEDS FOR DATA TRANSMISSION

The cloud connection from on-premise gateway can be achieved using standard security appliances. The CLSS Gateway uses outbound only communication with HTTPS/TLS encryption. The detailed requirements are:

Inbound (In) Port: An inbound port is a port another computer uses to connect to the gateway to access the gateway functionality; that is, an application on the gateway will be actively listening on this port for client connections.

Outbound(Out) Port: The gateway uses outbound ports to connect to Internet/CLSS Cloud platform; that is, the services in the cloud will be listening on these ports waiting for a connection from the gateway.

By Default, block all inbound and outbound connections and allow only the ports listed in the below table:

PORT NUMBER	TYPE	IN / OUT	PURPOSE / REMARKS
443	TCP	Out	Https Communication to CLSS Cloud platform
53	UDP	Out	DNS client to server lookup
2020	TCP	Out	Alarm Transmission

The following are the list of endpoints to communicate to CLSS Cloud platform:

REGION	ALL END-POINTS
Global	https://gaprodpkisystemauthenticationv2.sentience.honeywell.com/ https://gaprodregui.sentience.honeywell.com/ https://sentgaprod.blob.core.windows.net
Europe	https://t02aprodfileupload.sentience.honeywell.com/ https://sentt02aprodfu.blob.core.windows.net https://sentt02aprodv2.azure-devices.net/ https://t02aprodcloudapp.sentience.honeywel.com
US	https://t01aprodfileupload.sentience.honeywell.com/ https://sentt01aprodfu.blob.core.windows.net https://sentt01aprodv2.azure-devices.net/ https://t01aprodcloudapp.sentience.honeywell.com
US-Alarm Transmission	https://honprodeast.rrmsalarm.com https://honprodwest.rrmsalarm.com

SECURE BOOT AND SECURE FIRMWARE UPGRADE

Secure Boot is the process of validating firmware signature prior to executing the firmware. **Secure firmware upgrade** is the process of validating new firmware prior to replacing currently running version. **Firmware signing** is a process of calculating the digital signature of the firmware during the firmware build process and assuring that it cannot be altered without detection.

Honeywell periodically releases security hotfixes and upgrade packages to the gateway's firmware. The released packages are encrypted and digitally signed by Honeywell to ensure the confidentiality, integrity and authenticity (i.e., package originated from Honeywell) of the released package. The gateway verifies the signature during secure boot and firmware upgrade processes.

Sensitive details such as private device key(s) are managed via security chips as per commonly accepted security industry practices and recommendations.

CLSS MOBILE APP AND CLOUD PLATFORM

CLSS MOBILE APP

Communication between mobile and cloud
All communication arising out of the mobile phone to CLSS cloud platform are over HTTPS with TLS 1.2 encrypted tunnel.

Communication between mobile and Gateway
Mobile app being used over Secure BLE Link Connection with CLSS gateway for gateway configuration. The BLE connection works only when the user is near the gateway. The security keys required to pair up with CLSS Gateway are accessible only for authorized technicians through cloud platform.

Data stored and exchanged through CLSS Mobile App
The mobile app exchanges details with the CLSS Cloud platform for gateway configuration, for inspection management use cases. The data is not maintained in the mobile device permanently. It is only for temporary use and details are erased from app memory database when data is synced with cloud.

CLSS CLOUD PLATFORM

The cloud based deployment is managed as per Honeywell's unified compliance framework that is aligned to major IT security frameworks including NIST SP 800-171 and ISO 27001.

Data Communication within cloud
All internal communications between various cloud services use HTTPS for integrity and confidentiality within the cloud.

Cloud Infrastructure security measures

- Strong login and password based authentication is used for mobile and web apps
- Role based authorization enforcement to access different data.
- Firewall in perimeter security is ensured through IPS/ IDS and packet inspection.
- WAF(Web Application Firewall) is enabled for CLSS applications. WAFs provide protection against cyber-attacks like SQL injections, cross-site Scripting, malware uploads, application DDoS etc.
- Sensitive data like security tokens and cryptographic keys are managed through **Azure key vault**. Azure key vault provides FIPS 140-2 Level 2 validated hardware security modules (HSM) to store the sensitive data.
- Security hardening of all servers is segmented via virtual networks and virtual servers
- All CLSS cloud virtual machines are protected with Anti-malware.
- Standard process to apply Security patches periodically with provisions for risk based expedites.
- At application level strong authentication and authorization is used to restrict access to any of the application data.
- System admin level access is restricted to the authorized Honeywell Digital operations team. Regular backups are taken to restore system to normal state in case of accidental loss. At rest, all the data is encrypted using SSE(Solid state encryption).
- CLSS Cloud Platform uses Honeywell Forge, and hosted on the Microsoft Azure Cloud. Honeywell Forge platform is audited under SOC2 Type 1. Microsoft Azure Cloud is certified with: SOC1 Type2, SOC2 Type2, ISO27001. For a complete list please visit **here**.

PERSONAL DATA

Login and passwords, and other personal data is managed in Active directory in encrypted form. Personal data is protected as per GDPR regulatory compliance and Honeywell's privacy standards. Honeywell limits the personal data it collects and processes to the minimum necessary to serve a legitimate business purpose.

APPROACH TO CYBER SECURITY IN PRODUCT DEVELOPMENT

All software should incorporate cybersecurity and privacy best practices to minimize cybersecurity issues from occurring. That's why we believe in including security and privacy when the product development process begins. Honeywell Building Technologies' products undergo stringent security reviews and testing before approved for release, no matter where they are manufactured. Our products are assessed against our cyber standards and require approval by our chief technical officer as a part of our standard new product introduction process.

Honeywell follows the Building Security In Maturity Model (BSIMM) framework and ensures Secure Development Life Cycle standards and requirements for products.

The CLSS platform integrates security considerations in all aspects of development, deployment, and risk management. The system was developed using Honeywell's Secure Software Development Lifecycle (SSDLC) which integrates security considerations in all stages from requirements to testing deployment and ongoing operations. System development covers all aspects from deriving requirements from standards ANSI/ISA 62443 and best practices, secure architecture and design via architectural risk analysis, threat modeling, secure coding guidelines and static and dynamic code analysis, and security testing using manual and automated approaches.

The entire CLSS platform is developed by Honeywell and source code is managed per Honeywell source code management policies. Code reviews are done to detect security loopholes in the source code. Open source libraries used in the product have gone through security clearance as per Honeywell standard practice.

Static code analysis and binary scanning tools are integrated with the CI/CD (Continuous Integration/ Continuous Delivery) pipeline and executed when each build is generated. The security risks are recorded in JIRA tools with CVSS scoring, and remediated per agreed plans to a mandated schedule based on severity.

Penetration Testing and Test Initiation Events

Penetration testing is conducted before any major releases and before deployment of new version of cloud services to production environment. The team performs penetration testing on applications based on identified vulnerabilities and will be re-tested after mitigation to verify corrections. Findings are logged and tracked for closure.

Product applications are assessed in accordance with the latest OWASP testing guide and underlying product infrastructure is assessed as per NIST 800-115 guidelines.

HONEYWELL SUPPORT AND DEVOPS PROCESS

The entire production system is managed by a 24/7 support team which monitors the infrastructure as well as applications. There are detailed internal policies which cover how we detect, investigate and respond to security and privacy incidents.

Honeywell use various application diagnostics tools for different parts of the system to monitor health parameters of the system. We keep track of system health (e.g., CPU usage, memory usage, disk IO operations) and any deviation would trigger an alert.

HOW TO REPORT A SECURITY VULNERABILITY

Honeywell has Product Security Incident Response Team (PSIRT) to monitor and manage incidents and to minimize customers' risk associated with security vulnerabilities by providing timely information, guidance and remediation of vulnerabilities in our products.

Click **here** to learn more about the Honeywell PSIRT process. To report a potential security vulnerability against any Honeywell product, please follow the instructions **here**.

For more information

www.honeywell.com

Honeywell Fire Solutions

12 Clintonville Rd.
Northford CT
203.484.7161
www.honeywell.com

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell