CONNECTED LIFE SAFETY SERVICES

PANORAMICA SULLA SICUREZZA INFORMATICA

Versione:1.0

Honeywell

TABELLA DI CONTENUTI

INFORMAZIONI SU QUESTO DOCUMENTO

Questo documento è destinato principalmente agli ESD, agli integratori di sistemi e ai tecnici Honeywell Connected Life Safety Services (CLSS) che sono interessati a comprendere l'approccio adottato da Honeywell per la sicurezza della soluzione CLSS. Questo documento fornisce inoltre dettagli sull'architettura di sicurezza, sulle procedure e sui controlli di sicurezza che descrivono come configurare il gateway CLSS in modo sicuro nel sito

Esclusione di responsabilità:

.

INTRODUZIONE
A CLSS

CLSS è una piattaforma cloud innovativa e completa che consente agli integratori di sistemi e ai gestori di strutture di fornire un servizio di sicurezza antincendio migliorato, massimizzando l'efficienza delle prestazioni offerte dagli affidabili sistemi di rivelazione e allarme di Honeywell

VIA D'ARRIVO CLSS

CLSS Gateway funge da ponte tra la centrale antincendio e la piattaforma CLSS Cloud. Fornisce una via per collegare in modo sicuro la centrale di rivelazione incendi verso il cloud, e fornisce un unico percorso dal sito protetto al cloud per garantire che tutti i servizi e le applicazioni cloud CLSS utilizzino lo stesso metodo verificato e monitorando tutta la rete delle centrali incendio connesse.

WEB APP CLSS (SITE MANAGER)

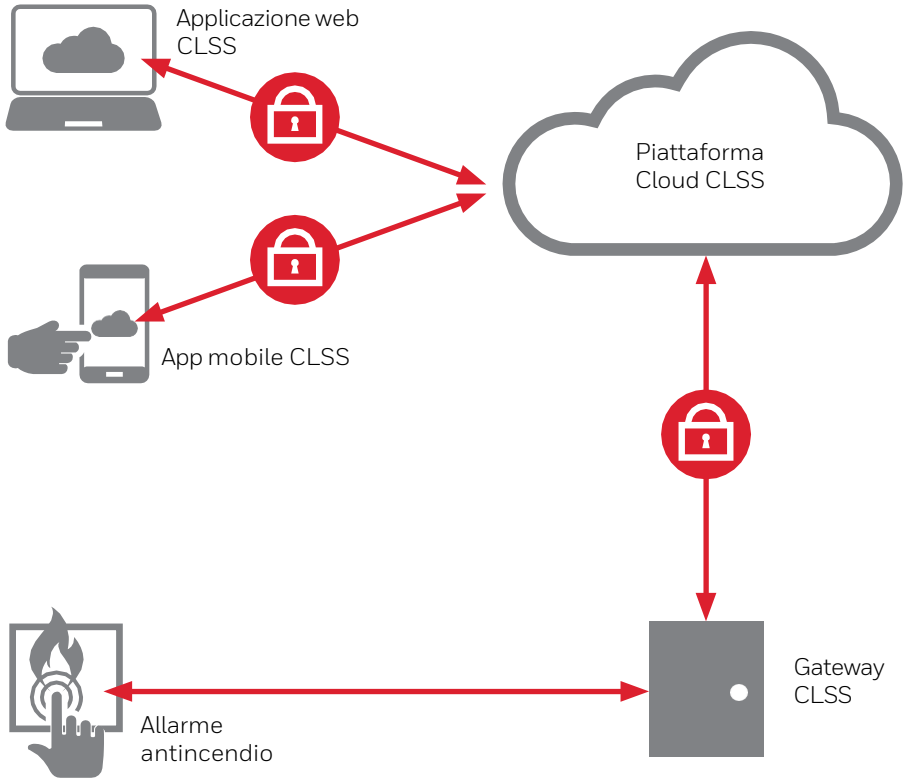
CLSS Site manager è un'applicazione web utilizzata da Facility manager, distributori e tecnici per svolgere attività amministrative e gestionali di back-office. Fornisce una visione consolidata dei sistemi dei loro clienti. Permette agli installatori e manutentori di inserire gli edifici dei loro clienti, i loro utenti e tecnici e di configurare i privilegi di accesso per i loro tecnici.

APPLICAZIONE MOBILE CLSS

L'applicazione mobile CLSS viene utilizzata dai tecnici per configurare il gateway durante l'installazione e per eseguire regolarmente il walk test della funzionalità dei dispositivi indirizzati e non. L'applicazione viene utilizzata anche per generare report di manutenzione in di conformità con le normative vigenti.

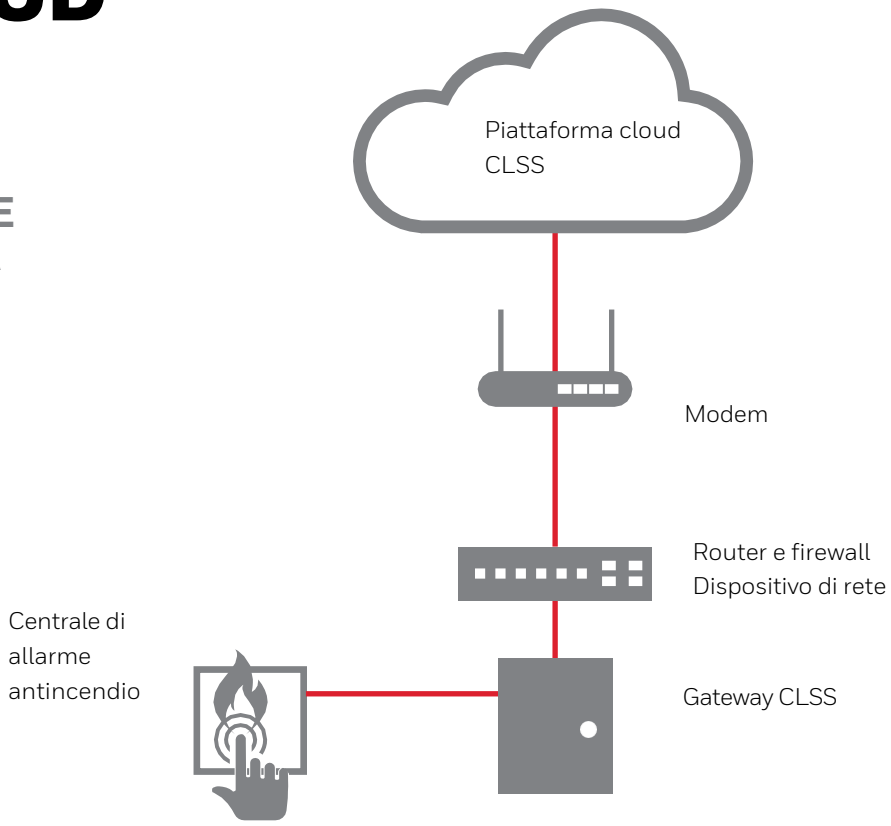
PIATTAFORMA CLOUD CLSS

La piattaforma CLSS Cloud contiene vari microservizi per supportare le funzionalità del gateway CLSS, dell'applicazione mobile e dell'applicazione web. È sicura, scalabile e basata su standard, costruita sulla piattaforma di gestione aziendale Honeywell Forge.

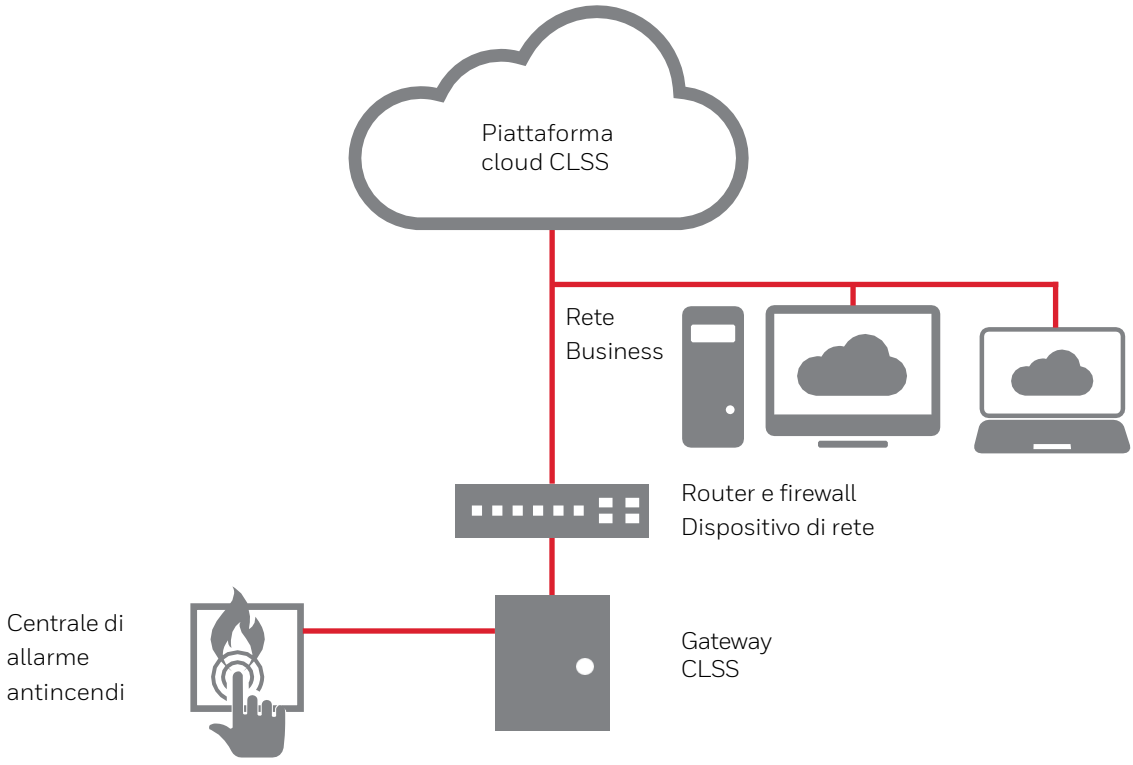


COLLEGAMENTO DEL GATEWAY CLSS AL CLOUD

APPROCCIO 1 CON MODEM E RETE PRIVATA



APPROCCIO 2 CON RETE AZIENDALE



QUALI DATI VENGONO TRASMESSI DAL SISTEMA IN LOCO VERSO IL CLSS?

Per realizzare i casi d'uso delle funzionalità CLSS Mobile app e Web app (Inspection manager e Site manager), i seguenti dati dal gateway in loco vengono trasmessi al cloud:

- Inventario dei dispositivi ricevuto dalla centrale antincendio
- Eventi, allarmi e guasti ricevuti dalla centrale antincendio
- Eventi, allarmi e problemi generati dal gateway
- Registri di audit del gateway con data e ora.

L'inventario dei dispositivi contiene tutti i dispositivi (ad esempio, rivelatori, moduli), compresa la centrale antincendio, collegati alla rete del sistema di allarme antincendio ma si possono aggiungere anche i dispositivi non indirizzati, identificandoli con etichette bar code.

SICUREZZA DELLA TRASMISSIONE DEI DATI

Per gestire la superficie del sistema dal punto di vista della sicurezza, il CLSS Gateway Cloud Connector effettua solo chiamate in uscita e non accetta comunicazioni in entrata. Le connessioni in uscita sono limitate a HTTPS per l'avvio della comunicazione e ad AMQP su HTTPS per la messaggistica con crittografia TLS1.2 o superiore. AMQP è un protocollo di messaggistica standard OASIS progettato per una messaggistica affidabile e robusta, adatta a scenari in cui è richiesta la conferma dei comandi e il trasferimento dei dati.

L'autenticazione basata su certificati viene utilizzata tra il gateway "on-premise" e la piattaforma CLSS Cloud.

INFRASTRUTTURE NECESSARIE PER LA TRASMISSIONE DEI DATI

La connessione al cloud dal gateway "on-premise" può essere realizzata utilizzando dispositivi di sicurezza standard. Il gateway CLSS utilizza solo comunicazioni in uscita con crittografia HTTPS/TLS. I requisiti dettagliati sono:

Porta in entrata (In): Una porta in entrata è una porta che un altro computer utilizza per connettersi al gateway e accedere alle sue funzionalità; ad esempio, un'applicazione sul gateway sarà in ascolto attivo su questa porta per le connessioni dei client.

Porta in uscita (Out): il gateway utilizza le porte in uscita per connettersi alla piattaforma Internet/CLSS Cloud; cioè, i servizi nel cloud saranno in ascolto su queste porte in attesa di una connessione dal gateway.

Per impostazione predefinita, blocca tutte le connessioni in entrata e in uscita e consente solo le porte elencate nella tabella seguente:

NUMERO INGRESSI	TIPO	IN / OUT	SCOPO / OSSERVAZIONI
443	TCP	In Uscita	Comunicazione Https alla piattaforma CLSS Cloud
53	UDP	In Uscita	Ricerca da client a server DNS
2020	TCP	In Uscita	Trasmissione dell'allarme

Di seguito sono elencati gli endpoint per comunicare con la piattaforma CLSS Cloud:

REGIONE	TUTTI I PUNTI FINALI
Globale	https://gaprodpkisystemauthenticationv2.sentience.honeywell.com/ https://gaprodregui.sentience.honeywell.com/ https://sentgaprod.blob.core.windows.net
Europa	https://t02aprodfileupload.sentience.honeywell.com/ https://sentt02aprodfu.blob.core.windows.net https://sentt02aprodv2.azure-devices.net/ https://t02aprodcloudapp.sentience.honeywell.com
STATI UNITI	https://t01aprodfileupload.sentience.honeywell.com/ https://sentt01aprodfu.blob.core.windows.net https://sentt01aprodv2.azure-devices.net/ https://t01aprodcloudapp.sentience.honeywell.com
US-Trasmissione di allarme	https://honprodeast.rrmsalarm.com https://honprodwest.rrmsalarm.com

AVVIO SICURO E AGGIORNAMENTO SICURO DEL FIRMWARE

Secure Boot è il processo di convalida della firma del firmware prima della sua esecuzione. L'**aggiornamento sicuro del firmware** è il processo di convalida del nuovo firmware prima della sostituzione della versione in esecuzione.

Firmware signing è un processo di calcolo della firma digitale del firmware durante il processo di creazione del firmware stesso e garantisce che non possa essere alterato senza essere individuato.

Honeywell rilascia periodicamente hotfix di sicurezza e pacchetti di aggiornamento del firmware del gateway. I pacchetti rilasciati sono crittografati e firmati digitalmente da Honeywell per garantire la riservatezza, l'integrità e l'autenticità (cioè, il pacchetto originato da Honeywell) del pacchetto rilasciato. Il gateway verifica la firma durante i processi di "Secure Boot" e di aggiornamento del firmware.

I dati sensibili, come le chiavi private del dispositivo, sono gestiti tramite chip di sicurezza secondo le pratiche e le raccomandazioni del settore della sicurezza comunemente accettate.

APPLICAZIONE MOBILE CLSS E PIATTAFORMA CLOUD

APPLICAZIONE MOBILE CLSS

Comunicazione tra cellulare e cloud

Tutte le comunicazioni tra il telefono cellulare/tablet e la piattaforma cloud CLSS avvengono tramite HTTPS con tunnel criptato TLS 1.2.

Comunicazione tra smartphone e gateway

Applicazione mobile utilizzata tramite connessione sicura BLE Link con gateway CLSS
per la configurazione del gateway. La connessione BLE funziona solo quando l'utente è vicino al gateway. Le chiavi di sicurezza necessarie per l'accoppiamento con il gateway CLSS sono accessibili solo ai tecnici autorizzati attraverso la piattaforma cloud.

Dati memorizzati e scambiati attraverso l'App CLSS Mobile

L'applicazione mobile scambia i dettagli con la piattaforma CLSS Cloud per la configurazione del gateway, per i casi d'uso della gestione delle ispezioni. I dati non vengono conservati nel dispositivo mobile
in modo permanente. È solo per uso temporaneo e i dettagli vengono cancellati dal database della memoria dell'app quando i dati vengono sincronizzati con il cloud.

PIATTAFORMA CLOUD CLSS

L'implementazione basata sul cloud è gestita in base al quadro di conformità unificato di Honeywell, allineato ai principali standard di sicurezza informatica tra cui NIST SP 800-171 e ISO 27001.

Comunicazione dei dati all'interno del cloud

Tutte le comunicazioni interne tra i vari servizi cloud usano HTTPS per l'integrità e la riservatezza all'interno del cloud.

Misure di sicurezza dell'infrastruttura cloud

- L'autenticazione forte basata su login e password viene utilizzata per le applicazioni mobili e web.
- L'accesso ai diversi dati e funzionalità è basata su diversi ruoli di autorizzazione.
- La sicurezza perimetrale del firewall è garantita da IPS/IDS e dall'ispezione dei pacchetti.
- Il WAF (Web Application Firewall) è abilitato per le applicazioni CLSS. I WAF forniscono protezione contro gli attacchi informatici come le iniezioni di SQL, il cross-site Scripting, il caricamento di malware, il DDoS delle applicazioni, ecc.
- I dati sensibili, come i token di sicurezza e le chiavi crittografiche, sono gestiti tramite **Azure key vault**. Azure key vault fornisce moduli di sicurezza hardware (HSM) convalidati FIPS 140-2 di livello 2 per archiviare i dati sensibili.
- La protezione di tutti i server è segmentata tramite reti virtuali e server virtuali.
- Tutte le macchine virtuali del cloud CLSS sono protette da Anti-malware.
- Processo standard per l'applicazione periodica delle patch di sicurezza con disposizioni per l'accelerazione basata sul rischio.
- A livello di applicazione, l'autenticazione e l'autorizzazione forte vengono utilizzate per limitare l'accesso a qualsiasi dato dell'applicazione.
- L'accesso a livello di amministratore del sistema è limitato al team operativo autorizzato di Honeywell Digital. Backup regolari sono previsti per ripristinare il sistema allo stato normale in caso di perdita accidentale. A ripristino, tutti i dati sono crittografati con SSE (Solid State Encryption).
- La piattaforma cloud CLSS utilizza Honeywell Forge ed è ospitata su Microsoft Azure Cloud. La piattaforma Honeywell Forge è sottoposta a verifica SOC2 Tipo 1. Microsoft Azure Cloud è certificato con: SOC1 Tipo2, SOC2 Tipo2, ISO27001.
  Per un elenco completo, visitate **qui**.

DATI PERSONALI

Login e password e altri dati personali sono gestiti in Active directory in forma criptata. I dati personali sono protetti in conformità alla normativa GDPR e agli standard di privacy di Honeywell. Honeywell limita i dati personali che raccoglie ed elabora al minimo indispensabile per servire uno scopo commerciale legittimo.

APPROCCIO ALLA SICUREZZA INFORMATICA

NELLO SVILUPPO DEL PRODOTTO

Tutti i software dovrebbero incorporare le migliori pratiche di cybersecurity e privacy per ridurre al minimo i problemi di cybersecurity. Ecco perché crediamo che la sicurezza e la privacy debbano essere incluse fin dall'inizio del processo di sviluppo del prodotto.
I prodotti di Honeywell Building Technologies sono sottoposti a rigorosi controlli e test di sicurezza prima di essere approvati per la commercializzazione, indipendentemente dal luogo di produzione. I nostri prodotti sono valutati rispetto ai nostri standard informatici e richiedono l'approvazione del nostro Chief Technical Officer nell'ambito del nostro processo standard di introduzione di nuovi prodotti.

Honeywell segue il framework Building Security In Maturity Model (BSIMM) e garantisce gli standard e i requisiti del Secure Development Life Cycle per i prodotti.

La piattaforma CLSS integra considerazioni sulla sicurezza in tutti gli aspetti dello sviluppo, della distribuzione e della gestione del rischio. Il sistema è stato sviluppato utilizzando il Secure Software Development Lifecycle (SSDLC) di Honeywell, che integra considerazioni sulla sicurezza in tutti gli aspetti dello sviluppo e della gestione dei rischi in tutte le fasi, dai requisiti ai test, all'implementazione e alle operazioni in corso. Lo sviluppo del sistema copre tutti gli aspetti, dalla derivazione dei requisiti dagli standard ANSI/ISA 62443 e dalle best practice, all'architettura e alla progettazione sicure tramite l'analisi dei rischi architettonici, la modellazione delle minacce, le linee guida per la codifica sicura e l'analisi statica e dinamica del codice, fino ai test di sicurezza con approcci manuali e automatici.

L'intera piattaforma CLSS è sviluppata da Honeywell e il codice sorgente è gestito secondo le politiche di gestione del codice sorgente di Honeywell. Vengono effettuate revisioni del codice per individuare le falle di sicurezza nel codice sorgente.
Le librerie open source utilizzate nel prodotto sono state sottoposte a controlli di sicurezza come da prassi standard Honeywell.

Gli strumenti di analisi statica del codice e di scansione binaria sono integrati con la pipeline CI/CD (Continuous Integration/ Continuous Delivery) e eseguito quando viene generata ogni build. I rischi per la sicurezza sono registrati in “JIRA Tools” con punteggio CVSS e rimedio secondo i piani concordati in base a un programma obbligatorio basato sulla gravità.

Test di penetrazione ed eventi di avvio del test
I test di penetrazione vengono condotti prima di qualsiasi rilascio importante e prima della distribuzione di una nuova versione dei servizi cloud nell'ambiente di produzione. Il team esegue i test di penetrazione sulle applicazioni in base ai criteri identificati e saranno nuovamente testati dopo la mitigazione per verificare le correzioni. I risultati vengono registrati e monitorati per la chiusura.

Le applicazioni del prodotto sono valutate in base alla più recente guida ai test di OWASP e l'infrastruttura del prodotto sottostante è valutata in base alle linee guida NIST 800-115.

SUPPORTO HONEYWELL E PROCESSO DEVOPS

L'intero sistema di produzione è gestito da un team di assistenza 24 ore su 24, 7 giorni su 7, che monitora l'infrastruttura e le applicazioni. Esistono politiche interne dettagliate che riguardano il modo in cui rileviamo, indaghiamo e rispondiamo agli incidenti di sicurezza e di privacy.

Honeywell utilizza vari strumenti di diagnostica applicativa per diverse parti del sistema per monitorare i parametri di salute del sistema. Manteniamo traccia dello stato di salute del sistema (ad esempio, utilizzo della CPU, della memoria, delle operazioni di IO su disco) e qualsiasi deviazione fa scattare un allarme.

COME SEGNALARE UNA VULNERABILITÀ DI SICUREZZA

Honeywell dispone di un Team di risposta agli incidenti di sicurezza dei prodotti (PSIRT) per monitorare e gestire gli incidenti e ridurre al minimo il rischio dei clienti associato alle vulnerabilità della sicurezza, fornendo informazioni, indicazioni e rimedi tempestivi alle vulnerabilità dei nostri prodotti.

Fare **clic qui** per saperne di più sul processo PSIRT di Honeywell. Per segnalare una potenziale vulnerabilità della sicurezza di qualsiasi prodotto Honeywell, seguite le istruzioni **qui**.

Per maggiori informazioni
www.honeywell.com

Honeywell Fire Solution
Via Achille Grandi, 22 20097
San Donato Milanese (MI)
Italy
www.honeywell.com

HW_WP_CLSSCyberSec | Rev 01 | 10/2020

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell