1 Scheda tecnica del prodotto Servizi digitali

1.1 Connettività

Il prodotto è dotato di una funzionalità che, una volta abilitata, si connette a Swegon INSIDE Cloud quando si ha accesso a Internet. Tale connessione può essere effettuata tramite il punto di accesso a Internet locale dell'edificio o utilizzando un modem in dotazione. Quando ci si connette attraverso il punto di accesso a Internet dell'edificio, il firewall locale deve essere configurato per consentire il traffico in base alle impostazioni del firewall. La funzionalità è disattivata per impostazione predefinita e può essere attivata nel prodotto. Abilitando questa funzionalità, il cliente accetta i termini e le condizioni generali del Servizio Digitale, DS-23. Il cliente può disattivare in qualsiasi momento la connessione a Swegon INSIDE Cloud nell'interfaccia utente del prodotto.

1.2 Quali dati vengono inviati

Attraverso la connessione a Swegon INSIDE Cloud, il prodotto scambia dati a Swegon INSIDE Cloud su determinate azioni e impostazioni dei parametri del prodotto. Ogni punto dati ha soglie diverse per l'invio dei dati a Swegon, pertanto i dati inviati dipendono dal tipo di punto dati e dalla configurazione. I dati vengono inviati a intervalli e a quel punto vengono aggregati con altri dati di quell'intervallo.

1.3 Chi ha accesso ai dati

I dati inviati a Swegon INSIDE Cloud vengono utilizzati da Swegon ai fini delle prestazioni, della funzionalità e dello sviluppo del prodotto. Di conseguenza, Swegon ha il diritto di utilizzare i dati inviati da tutti i prodotti collegati a Swegon INSIDE Cloud. I dati vengono utilizzati in conformità ai termini e alle condizioni generali DS-23 di Swegon e al nostro contratto di vendita con il cliente.

1.4 Requisiti

Per collegare un prodotto a Swegon INSIDE Cloud, è necessaria una connessione internet sicura tramite la rete interna della proprietà o tramite il modem esterno di Swegon. Oltre a una connessione internet sicura, è necessario anche un certificato valido per ogni singolo prodotto per autorizzarlo a condividere i dati con INSIDE Cloud. Alcuni prodotti vengono forniti con un certificato valido dalla fabbrica, mentre altri prodotti devono essere dotati di un certificato per autorizzare il prodotto a condividere i dati.

Per sapere se il prodotto è INSIDE Ready (cioè pronto a condividere i dati) o meno, visitate il sito INSIDE Ready | www.swegon.com.

1.5 Sicurezza

Il prodotto Swegon INSIDE è collegato a Azure IoT Hub. La connessione utilizza MQTT ed è protetta da TLS e certificati client (MTLS). DigiCert è utilizzato come autorità di registrazione e gestione delle chiavi. La piattaforma cloud di Swegon utilizza le offerte SaaS di Azure per l'hosting di applicazioni e API. I servizi digitali comunicano con Swegon Cloud utilizzando tecnologie standard come API Rest e code di messaggi. Gli utenti e le autorizzazioni sono gestiti da un identity provider interno.

1.6 Impostazioni del firewall per Swegon Cloud

La soluzione cloud di Swegon utilizza i servizi Microsoft Azure e i certificati di DigiCert per proteggere la connessione. Se il firewall di fronte ai prodotti consente il traffico in uscita verso Internet, funzionerà. Se il firewall è impostato per controllare il traffico in uscita, devono essere consentite le seguenti porte e destinazioni. Se si utilizza solo il filtraggio delle porte, si utilizzano le porte 443 e 8883.

Dominio (compreso il sottodominio)	**Porto**	**Protocollo**	**Nota**
***.azure-devices-provisioning.net** (dps-SwegonCloud-common-we.azure-devices-provisioning.net global.azure-devices-provisioning.net)	443 8883	https mqtt	Servizio di provisioning dei dispositivi Azure
***.azure-devices.net** (iot-SwegonCloud-prod-we.azure-devices.net)	443 8883	https mqtt	Azure IoT Hub
***.blob.core.windows.net** (stswciotfilestorageprod.blob.core.windows.net)	443	https	Storage su Azure
clientauth.one.digicert.com	443	https	DigiCert Enrolment over Secure Transport (EST) per l'enrollment e il reenrolment dei certificati