1 Produktdatablad Digitale tjenester

1.1 Tilkoblingsmuligheter

Produktet er utstyrt med en funksjonalitet som, når den er aktivert, kobler til Swegon INSIDE Cloud når det får tilgang til Internett. Tilkoblingen skjer enten via bygningens lokale internettilgangspunkt eller ved hjelp av et medfølgende modem. Når du kobler til via bygningens internettilgangspunkt, må den lokale brannmuren være konfigurert til å tillate trafikk i henhold til brannmurinnstillingene. Funksjonaliteten er som standard deaktivert og kan aktiveres i produktet. Ved å aktivere denne funksjonaliteten godtar kunden de generelle vilkårene for Digital Service, DS-23. Kunden kan når som helst deaktivere tilkoblingen til Swegon INSIDE Cloud i produktets brukergrensesnitt.

1.2 Hvilke data som sendes

Gjennom tilkoblingen til Swegon INSIDE Cloud vil produktet utveksle data til Swegon INSIDE Cloud om visse handlinger og parameterinnstillinger for produktet. Hvert datapunkt har ulike terskelverdier for når data skal sendes til Swegon, og dataene som sendes, avhenger derfor av datapunkttype og konfigurasjon. Dataene sendes i intervaller og aggregeres deretter sammen med andre data fra det aktuelle intervallet.

1.3 Hvem som har tilgang til dataene

Opplysningene som sendes til Swegon INSIDE Cloud, brukes av Swegon med henblikk på ytelse, funksjonalitet og utvikling av produktet. Swegon har derfor rett til å bruke dataene som sendes fra alle produkter som er koblet til Swegon INSIDE Cloud. Dataene brukes i samsvar med Swegons generelle vilkår DS-23 og vår salgsavtale med kunden.

1.4 Krav

For å koble et produkt til Swegon INSIDE Cloud kreves det en sikker internettilkobling via eiendommens interne nettverk eller via Swegons eksterne modem. I tillegg til en sikker internettilkobling kreves det også et gyldig sertifikat for hvert enkelt produkt for at de skal kunne dele data med INSIDE Cloud. Noen produkter leveres med et gyldig sertifikat fra fabrikken, mens andre produkter må utstyres med et sertifikat for å få tillatelse til å dele data.

For å finne ut om produktet er INSIDE Ready (dvs. klar til å dele data) eller ikke, kan du gå til INSIDE Ready | www.swegon.com.

1.5 Sikkerhet

Swegon INSIDE-produktet er koblet til Azure IoT Hub. Tilkoblingen bruker MQTT og er sikret ved hjelp av TLS og klientsertifikater (MTLS). DigiCert brukes som registreringsmyndighet og nøkkelhåndtering. Swegons skyplattform bruker Azure SaaS-tilbudet for hosting av applikasjoner og API-er. Digitale tjenester kommuniserer med Swegon Cloud ved hjelp av standardteknologier som Rest API-er og meldingskøer. Brukere og autorisasjon håndteres av en intern identitetsleverandør.

1.6 Brannmurinnstillinger for Swegon Cloud

Swegons skyløsning bruker Microsoft Azure-tjenester og sertifikater fra DigiCert for å sikre tilkoblingen. Hvis brannmuren foran produktene tillater utgående trafikk til internett, vil det fungere. Hvis brannmuren er satt opp til å kontrollere utgående trafikk, må følgende porter og destinasjoner tillates. Hvis bare filtrering på porter, 443 og 8883 brukes.

Domene (inkludert underdomene)	Havn	Protokoll	Merknad
***.azure-devices-provisioning.net** (dps-SwegonCloud-common-we.azure-devices-provisioning.net) global.azure-devices-provisioning.net)	443 8883	https mqtt	Azure Device Provisioning Service
***.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	Azure-lagring
clientauth.one.digicert.com	443	https	DigiCert Enrolment over Secure Transport (EST) for sertifikatregistrering og reenrolment.