1 Produktdatablad Digitale tjenester

1.1 Forbindelsesmuligheder

Produktet er udstyret med funktioner, der, når de er aktiveret, opretter forbindelse til Swegon INSIDE Cloud, når der er adgang til internettet. En sådan forbindelse oprettes enten via bygningens lokale internetadgangspunkt eller ved hjælp af et medfølgende modem. Når der oprettes forbindelse via bygningens internetadgangspunkt, skal den lokale firewall konfigureres til at tillade trafik i henhold til firewallindstillingerne. Funktionaliteten er som standard deaktiveret og kan aktiveres i produktet. Ved at aktivere denne funktionalitet accepterer kunden de generelle vilkår og betingelser for Digital Service, DS-23, som kan findes på Swegons hjemmeside. Kunden kan til enhver tid deaktivere forbindelsen til Swegon INSIDE Cloud i produktets brugergrænseflade.

1.2 Hvilke data der sendes

Gennem forbindelsen til Swegon INSIDE Cloud vil produktet udveksle data til Swegon INSIDE Cloud om visse handlinger og parameterindstillinger for produktet. Hvert datapunkt har forskellige tærskler for, hvornår data skal sendes til Swegon, og de data, der sendes, afhænger derfor af datapunktets type og konfiguration. Dataene sendes i intervaller, og på det tidspunkt aggregeres dataene sammen med andre data fra det pågældende interval.

1.3 Hvem har adgang til dataene?

De data, der sendes til Swegon INSIDE Cloud, anvendes af Swegon med henblik på ydeevne, funktionalitet og udvikling af produktet. Swegon har derfor ret til at bruge de data, der sendes fra alle produkter, der er tilsluttet Swegon INSIDE Cloud. Dataene anvendes i overensstemmelse med Swegons generelle vilkår og betingelser DS-23, fundet på Swegons hjemmeside, og vores salgsaftale med kunden.

1.4 Krav

For at tilslutte et produkt til Swegon INSIDE Cloud kræves der en sikker internetforbindelse via ejendommens interne netværk eller via Swegons eksterne modem. Ud over en sikker internetforbindelse kræves der også et gyldigt certifikat for hvert enkelt produkt for at godkende dem til at dele data med INSIDE Cloud. Nogle produkter leveres med et gyldigt certifikat fra fabrikken, mens andre produkter skal udstyres med et certifikat for at give produktet tilladelse til at dele data.

For at finde ud af, om dit produkt opfylder kravene til at være INSIDE Ready (dvs. klar til at dele data) og få mere at vide om vores digitale tjenester, kan du besøge Connected products | www.swegon.com.

1.5 Sikkerhed

Swegon INSIDE-produktet er forbundet til azure IoT Hub. Forbindelsen bruger MQTT og er sikret ved hjælp af TLS og klientcertifikater (MTLS). DigiCert bruges som registreringsmyndighed og nøglehåndtering. Swegons cloud-platform bruger Azure SaaS-tilbud til hosting af applikationer og API'er. Digitale tjenester kommunikerer med Swegon Cloud ved hjælp af standardteknologier som Rest API'er og Message Queues. Brugere og autorisation håndteres af en intern identitetsudbyder.

1.6 Firewall-indstillinger for Swegon Cloud

Swegons cloud-løsning bruger Microsoft Azure-tjenester og certifikater fra DigiCert til at sikre forbindelsen. Hvis firewallen foran produkterne tillader udgående trafik til internettet, vil det fungere. Hvis firewallen er sat op til at kontrollere udgående trafik, skal følgende porte og destinationer være tilladt. Hvis der kun filtreres på porte, bruges 443 og 8883.

Domæne (inklusive underdomæne)	Havn	Protokol	Bemærk
***.azure-devices-provisioning.net** (dps-SwegonCloud-common-we.azure-devices-provisioning.net global.azure-devices-provisioning.net)	443 8883	https mqtt	Azure-tjeneste til klargøring af enheder
***.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) til certifikatindskrivning og -genindskrivning