Med Halton Connect övervakar du dina Halton-ventilationssystem på ett säkert sätt

Målgrupp

Denna vitbok är en introduktion till Halton Connect IoT-lösning samt de cybersäkerhetsfunktioner och metoder som används i den.
Den riktade målgruppen är bygg- och anläggningsägare och operatörer, bygg- och annan underhållspersonal samt slutanvändare. För IT-, säkerhets- och systeminteratörer har Halton annan teknisk dokumentation.

Ditt Halton-ventilationssystem är utrustat med Halton Connect, som gör att du kan övervaka dina Haltonlösningar. Det tillåter också Halton att stödja din drift genom att fjärrkontrollera, felsöka och vid behov även rätta till fel som kan hindra ditt systems funktion.

Halton Connect är baserat på IoT-teknologier, som möjliggör olika intelligenta tjänster till stöd för företag och hjälp för att förbättra verksamheten. T.ex. minska risk för driftstopp, minska energiförbrukningen och öka effektiviteten.

IoT

IoT (Internet of Things) betyder ett nätverk av enheter som är anslutna till varandra via Internet. När enheter blir mer och mer intelligenta kan de samla in data om sin egen prestanda och statistik. De kan lagra data och utbyta data med andra enheter i sitt nätverk. Människor kan sedan använda den insamlade och kombinerade datan för att kontrollera nätverksenheterna mer effektivt. Till exempel är det möjligt att bli uppmärksammad på att justeringar bör göras för att förbättra enheternas prestanda, eller för att upptäcka underhållsbehov innan några verkliga problem uppstår.

Eftersom IoT är en teknik som använder öppet internet, är dess säkerhet och integritet ett vanligt problem för många företag. Denna vitbok ger dig en översikt över Halton Connect-lösningen och beskriver hur Halton tar hand om säkerheten.

Översikt över Halton Connect

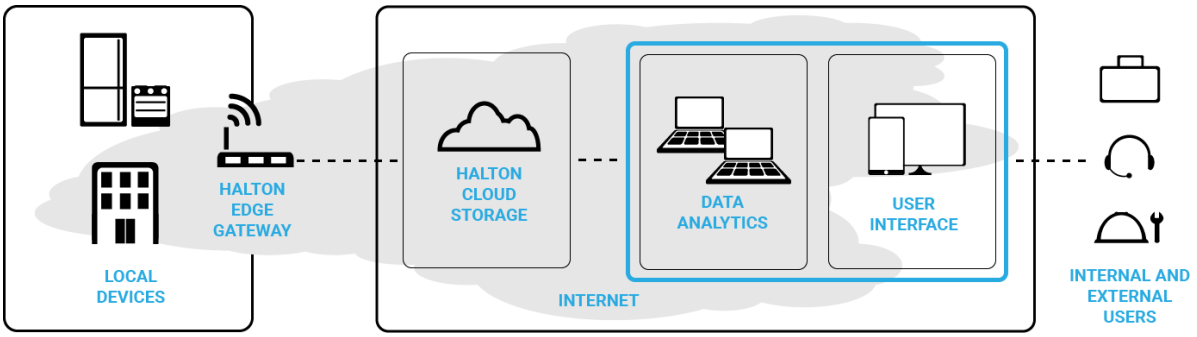
Halton Connect består av styrenheter och sensorer integrerade i ditt ventilationssystem, Halton Edge gateway och Halton IoT molntjänster.

De programmerbara logikstyrenheterna (eller PLC) inuti ventilationssystemet använder data som tillhandahålls genom temperaturen, luftflödet, fuktigheten och andra sensorer för att styra

bör-värden och andra parametrar så att systemet fungerar optimalt och i enlighet med slutanvändarens önskemål.

Halton EDGE Gateway är en liten formfaktordator som läser informationen från styrenheterna och sensorn och skickar den krypterad till Halton-molnet via mobilt 4G-nätverk.

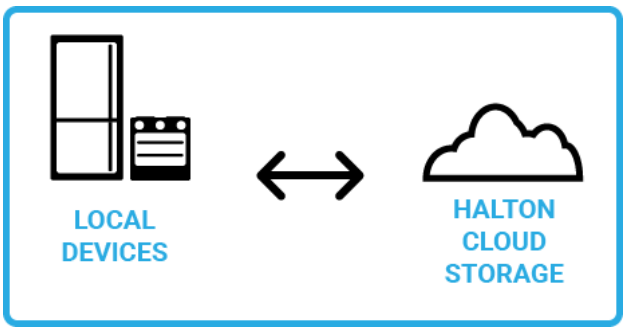
Halton IoT Cloud tar emot och lagrar informationen från alla ventilationssystem som har Halton Connect installerat. Halton Cloud implementeras i Microsoft Azure-plattformen och tillhandahåller fjärrhantering, datavisualisering och andra tjänster.



Säkerheten i Halton Connect

Halton följer industristandardprocesser och använder erkända moderna verktyg för att hålla Halton Connect säkert. Nedan beskrivs några av de viktigaste detaljerna hur säkerheten för system och data säkerställdes.

Anslutningssäkerheten mellan din utrustning och molnet

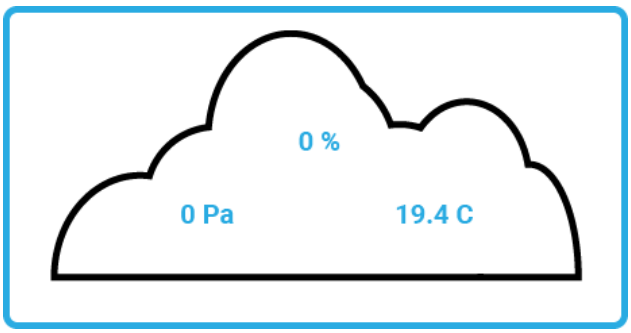


Halton EDGE-gateway ansluter din utrustning till molnet och skickar automatiskt data mellan din utrustning och Halton molnlagring. Anslutningen görs vanligtvis med hjälp av din utrustnings inbyggda 4G-modem för att skicka och ta emot data.

Användning av separat mobilanslutning är den viktigaste säkerhetsfunktionen eftersom den isolerar ditt eget nätverk och Halton-anslutning helt från varandra. Dvs. det finns ingen möjlighet att brott mot Halton-anslutningen skulle äventyra ditt nätverk och data.

Anslutningen mellan din utrustning och molnet säkerställs av ett VPN (Virtual Private Network) och med SSL (Secure Sockets Layer), som tillåter enheter att kommunicera över Internet säkert utan att överföringen är tillgänglig för obehöriga tredje parter. Med VPN och SSL krypteras data på ett sätt som endast godkända och pålitliga enheter kan tolka. Detta säkerställer att dina systemdata förblir konfidentiella.

Om det inte finns någon mobilanslutning, lagras data från din utrustning lokalt i utrustningens egna lokala databas. När anslutningarna blir tillgängliga igen, skickas data från utrustningens databas till molnet. Denna åtgärd säkerställer att inga data går förlorade.



Säkerhet för dina data lagrade i molnet

Data från din utrustning lagras i Halton-molnet. Molnet är byggt på Microsoft Azure-plattformen, som tillhandahåller alla infrastrukturtjänster som lagringsutrymme, säkerhetskopior och policyer.

Microsoft Azure används globalt och har datacenter runt om i världen. Varje datacenter har flera servrar, där data lagras. Dessa servrar är säkerhetskopierade
med en process som kallas replikering. I huvudsak, om en server eller till och med ett datacenter är offline, kan dina data nås från en annan serverplats. Det betyder att dina data alltid är tillgängliga.

Ett problem med molnplattformar är ofta molnens regelefterlevnad, till exempel molnens tillämpning av de olika dataskyddsbestämmelserna. Inga personuppgifter sparas i Halton molnlagring.

Endast behörig personal kan komma åt Haltons molnlagring, och det finns olika typer av konton för vanliga användare och för Haltons servicepersonal. För servicedelen av Halton-molnet används en tvåfaktorautentisering, vilket innebär att förutom ett lösenord måste du ha en annan autentiseringsmetod, t.ex. ett telefonsamtal eller ett meddelande för att få åtkomst.

Åtkomst till din data

Halton Connect är åtkomstkontrollerad och åtkomsten är begränsad. Endast behörig Halton-personal har tillgång till styrenheter och sensorer i din utrustning och till de data de samlar in och skickar till molnet. Halton-personalen får tillgång till utrustningen och data med sitt eget användarnamn och lösenord. Om en person lämnar Halton tas deras åtkomst till alla system bort.

Du som ägare eller användare av en Halton-produkt har ditt eget unika användarnamn och lösenord som du använder för att få åtkomst till dina data i molnet. Ta hand om detta användarnamn och lösenord som du skulle göra med något annat personligt användarnamn och lösenord. Avslöja dem inte för någon annan och förvara dem separat från varandra. Om du glömmer ditt användarnamn och lösenord eller har anledning att tro att obehöriga har tillgång till dem, bör du kontakta din Halton-tekniker för att återställa dem.

Halton Connect har en inloggningsgräns som, när den nåtts, kommer att låsa kontot under en tid. Detta förhindrar till exempel hackare att använda vissa typer av upprepade attacker ("brute force attacker") för att upptäcka ditt lösenord.

I Halton Connect, förutom unika användarnamn och lösenord, har varje utrustning en unik identifierare och de är byggda på ett containeriserat sätt. Med andra ord, var och en av utrustningen är tekniskt inuti en egen ”container” som håller utrustningarna isär. Detta förhindrar säkerhetsrisker för annan utrustning i nätverket om en enda äventyras, till exempel att dess användarnamn och lösenord stulits.

Tillgänglighet, uppdateringar och svagheter

“Alltid på”

Styrenheterna och sensorerna i din utrustning är alltid på, utom när du stänger av utrustningen helt och hållet. Detta kan vara avsiktligt, om du vill stänga av din utrustning eller om det blir strömavbrott. Detta planerade eller oplanerade driftstopp syns i de data som sensorerna samlar in och lagrar.
Genom att basera Halton Cloud på Microsoft Azure kan vi garantera att molnet och dina data alltid är tillgängliga.

Uppdateringar

En viktig del av säkerheten är att hålla enheterna uppdaterade. Halton Connect får regelbundna säkerhetsuppdateringar som installeras med en centraliserad fjärrinstallation. Om det har uppstått några problem under uppdateringen meddelas Haltons personal.

Automatiserade säkerhetskontroller

Ett säkerhetskonsultföretag kör kontinuerligt automatiserade säkerhetsskanningar i Halton Connect. Dessa säkerhetskontroller letar efter eventuella sårbarheter, om någon hittas, korrigeras denna och det skapas och lagras en rapport.

Innan varje ny programvara för Halton Connect släpps så utförs manuella säkerhetskontroller. En tredje part gör också säkerhetsrevisioner på systemet, under vilket säkerhetssårbarheter bedöms.

Version	Description	Date
1.0	Initial version	2020-03-19
1.0.1	Corrected typos	2020-05-29