Monitoring your Halton ventilation systems securely with Halton Connect

Intended audience

This white paper is a high-level introduction to Halton Connect IoT solution and cyber security features and practices used in it. The targeted audience is building and facility owners and operators, building and other maintenance personnel and end users. For IT, security and system integrator personnel Halton has other technical documentation.

Your Halton ventilation system is equipped with Halton Connect, which enables you to monitor your Halton solutions. It also allows Halton to support your operation by remotely inspecting, troubleshooting and often even fixing faults that might hinder the proper functioning of your system.

Halton Connect is based on IoT technologies, which enable different intelligent services that help companies to improve and enhance their businesses e.g. reducing equipment downtime, decreasing energy consumption and increasing efficiency.

IoT

IoT (Internet of Things) refers to a network of devices that are connected to each other through the Internet. As devices are becoming more and more intelligent, they can collect data about their own performance and statistics, store the data, and exchange the data with the other devices in their network. People can then utilise the collected and combined data to control the networked devices more efficiently. For example, through data it's possible to notice that adjustments should be done to the devices to improve their performance, or to detect maintenance needs before any real problems occur.

As IoT is a technology that uses open Internet, its security and privacy are a common concern for many businesses. This white paper gives you an overview of the Halton Connect solution and describes how Halton takes care of security.

Overview of Halton Connect

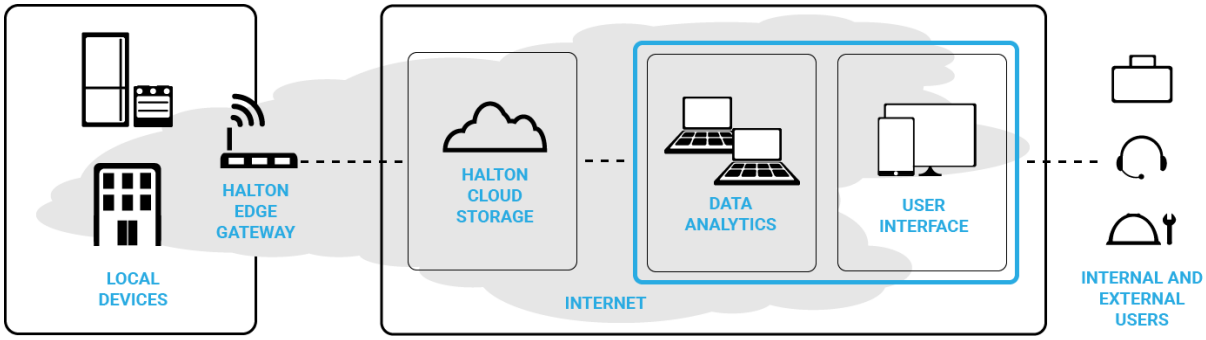
Halton Connect consists of controllers and sensors integrated into your ventilation system, Halton Edge gateway and Halton IoT cloud services.

The programmable logic controller(s) (or PLC) inside the ventilation system use data provided by the temperature, air flow, humidity and other sensors to control the setpoints

and other parameters so that the system performs as optimally and according the to the end-user's requests.

Halton EDGE Gateway is a small form factor computer that reads the information from the controllers and sensor and sends it encrypted to the Halton cloud through mobile 4G network.

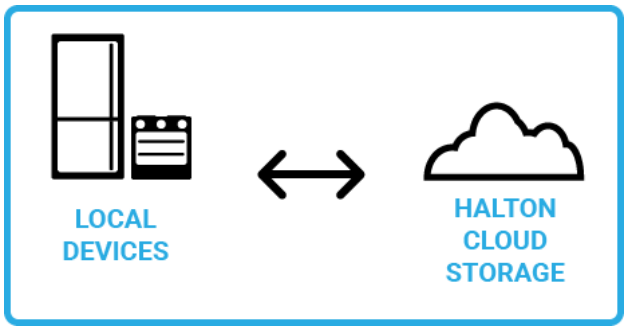
Halton IoT Cloud receives and stores the information coming from all the ventilation systems that have Halton Connect installed. Halton Cloud is implemented in Microsoft Azure platform and it provides remote management, data visualisation and other services.



Security in Halton Connect

Halton follows industry standard processes and uses recognised modern tools in keeping Halton Connect secure. Below are described some of the key details how the security of system and data ensured.

Security of the connection between your equipment and the cloud



The Halton EDGE gateway connects your equipment to the cloud, relaying data automatically between your equipment and the Halton cloud storage. The connection is usually made using your equipment's built-in 4G modem for sending and receiving data.

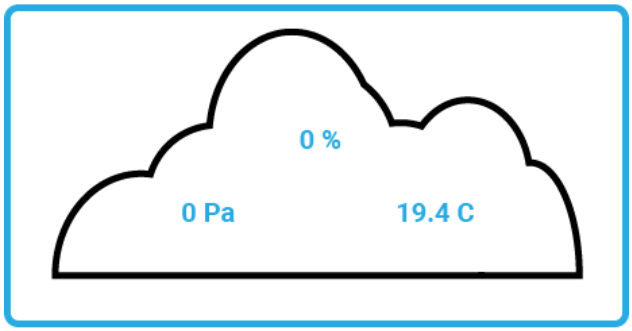
Use of separate mobile connection is the most important security feature as it isolates your own network and Halton connection totally from each other. I.e. there is no possibility that breach of Halton connection would endanger your network and data.

The connection between your equipment and the cloud is secured by a VPN (Virtual Private Network) and with SSL (Secure Sockets Layer), that allow devices to communicate over the

Internet securely without the transmission being accessible by unauthorised 3rd parties. With VPN and SSL, the data that is being transmitted is "scrambled" in a way that only authorised and trusted devices can interpret. This ensures that your systems data stays confidential.

In case no mobile connection is available, the data from your equipment gets stored locally in the equipment's own local database. Once connections become available again, the data is sent from the equipment's database to the cloud. This measure ensures that no data gets lost.

Security of your data stored in the cloud



The data from your equipment is stored in the Halton cloud. The cloud is built on the Microsoft Azure platform, which provides all the infrastructure services such as storage space, backups and policies.

Microsoft Azure is used globally, and it has data centres around the world. Each data centre has multiple servers, where the data is stored. These servers are backed up using a process called replication. In essence, if one server or even a data centre is offline, your data can be accessed from another server location. This means your data is always accessible.

A concern with cloud platforms is often the regulatory compliance of the cloud, for example, the cloud's compliance with the different data protection regulations. No personal data is saved in the Halton cloud storage.

Only authorised personnel can access the Halton cloud storage, and there are different types of accounts for regular users and for Halton administration personnel. For the administration part of the Halton cloud, a two-factor authentication is used, meaning that in addition to a password, you need to have another authentication method such as a phone call or message to get access.

Access to your data

Halton Connect is access-controlled and access is restricted. Only authorised Halton personnel have access to the controllers and sensors in your equipment and to the data they collect and send to the cloud. The Halton personnel access the equipment and data using their own username and password. If a person leaves Halton, their access to all systems is removed when they leave.

You, as the owner or user of a Halton product, have your own unique username and password that you use to access your data in the cloud. Take care of this username and

password as you would do with any other personal username and password. Do not tell them to anyone and store them separately from each other. If you forget your username and password or have reason to believe that unauthorised people have access to them, you should contact your Halton administrator for resetting them.

Halton Connect has a sign-in limit which, once reached, will lock the account for a period of time. This prevents, for example, hackers from using certain types of repeated attacks ("brute force attacks") to discover your password.

In Halton Connect, in addition to unique usernames and passwords, each equipment has a unique identifier and they are built in a containerised fashion. In other words, each equipment is technically inside a "container" which keeps the equipment apart. This prevents security risks to other equipment in the network in case a single one is compromised, for example, its username and password are stolen.

Availability, updates, and vulnerabilities

"Always on"

The controllers and sensors in your equipment are always on, except when you switch off the equipment entirely. This could be on purpose, in case you want to switch off your equipment, or there could be power outages. This expected or unexpected "downtime" is visible in the data that the sensors collect and store.

By basing the Halton Cloud on Microsoft Azure, we can guarantee that the cloud and your data are always available.

Updates

An important part of security is keeping the devices up to date. Halton Connect gets regular security updates which are installed using a centralised remote installation. If there have been any problems during the update, Halton personnel are notified.

Automated security checks

Automated security scans are run continuously in Halton Connect by a security consultation company. These automated security checks look for any vulnerabilities, if any are found, a report is filed, and the issues are fixed.

Before each Halton Connect new software release, manual security checks are carried out. A third party also does security audits to the system, during which security vulnerabilities are assessed.

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