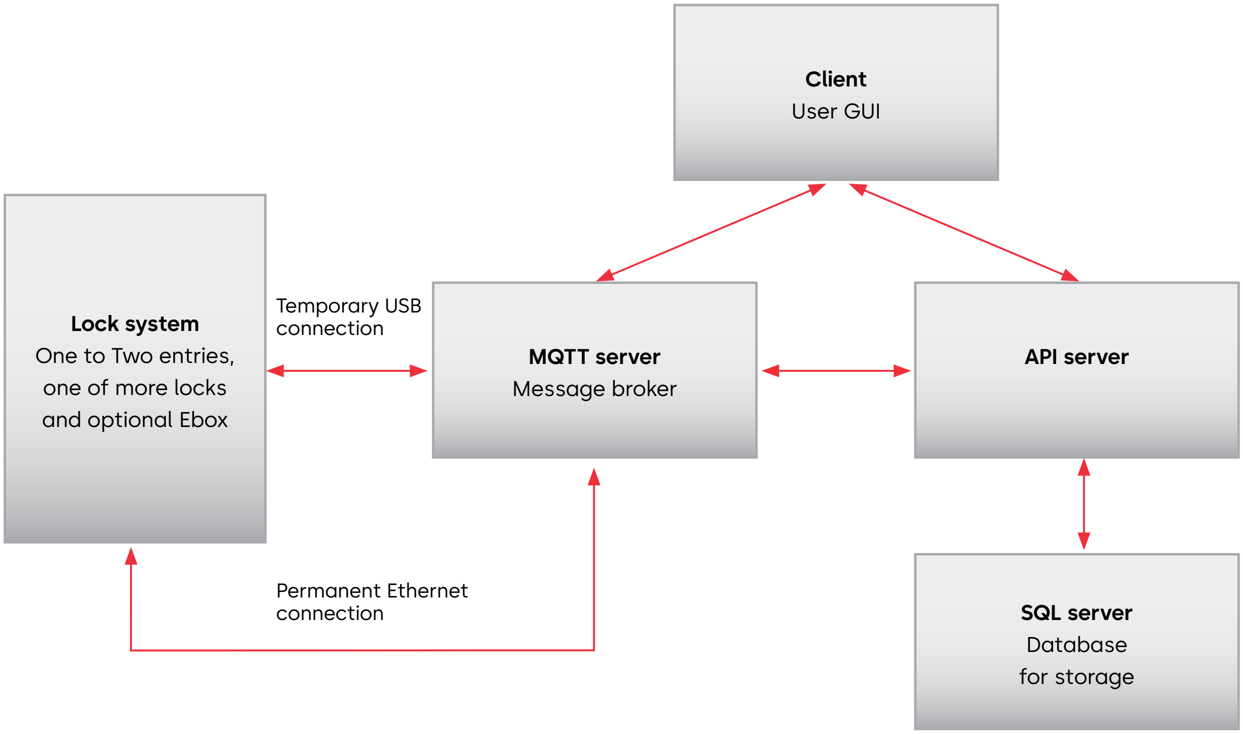
# Axessor Apexx
# IT Security guide

Guide

# Axessor Apexx
## System descriptions

The Apexx solution consist of one or two Entries, one or more locks, up to one E-box and one instance of Apexx SW solution (Local Software). This document will focus on solutions containing E-box.

**The general architecture of the solution is:**
There are two possible connections between the lock system and the local SW. One is direct connection over USB to the entry. This connection must be enabled by an authorized user in the menu selection of the lock. The second connection is from the E-box over Ethernet to the local SW.



**Local SW notes:**

- All parts of the SW (MQTT, client and API) are designed as a Windows 10 applications. To be able to use them in cloud environment, one must be able to manage the communication channels between them.
- The communication channels are established during installation – These rely on DNS (or static IP addresses). Once the installation is completed, certificates will be established for the purpose of security. These certificates need to be properly managed to prevent any attack paths.
- The client supports multiple users but doesn't support multiuser simultaneously on single client. Only one person can be logged into a single client instance at any given moment.
- The communication to-and from the locking system is MQTT over SSL, so the standard ports need to be reachable.
- SW requires Windows certificates subsystem and an SQL19 database to run.

**Pairing of local SW with E-box**
The local SW and E-box need to be paired before a connection can be established.
When a brand-new e-box needs to be installed:

1. The E-box is physically installed on the CAN bus.
2. An authorized user needs to log in into the entry and enable the E-box on the CAN bus (no un-authorized devices can listen to the CAN bus)
3. After authorization of the E-box, the E-box will be able to obtain the encryption keys to the CAN bus (AES-256 with system specific keys).
4. Once the E-box is on the CAN bus, connection needs to be made to the local SW. E-box will see if setting for the local SW was created (through settings menu of the entry). If there is a setting, it will be used. Otherwise, the E-box will assume DHCP to obtain IP address.
5. Once valid Ethernet setting exist, the E-box will attempt to connect to the MQTT server in the local SW (either through direct IP communication based on the settings, or broadcast on local network in case of DHCP). This is done over TLS.
6. If local SW detects a new E-box, it needs to be authorized in the SW before successful log-in using the claim code.
   Once E-box is authorized on the SW, SW will produce a verification PIN that needs to be validated on the Entry of the system (Verification of SW to the E-box, and E-box to SW).
7. After the system is verified, a secure channel is established. This is done using pre-installed factory signed certificates (PKI infrastructure). Any communication afterwards is encrypted using TLS.

**Disaster recovery:**
Local SW connects to SQL19 database for data storage
(SQL19 Express by Microsoft - Reference: https://www.microsoft.com/en-ca/sql-server/sql-server-2019-pricing).
The configuration of the database needs to be input into the local SW in form of config file.
The encryption/protection and data recovery will then follow the path of the SQL19 database. It is expected that the database is managed by local IT department.

Recover path will then be to re-install the API, MQTT and client either with fresh copy from dormakaba, or local backup. All data is at rest in the SQL database. API, MQTT and client don't store any data, only connection setting.

**Key takeaways:**

1. Only servers with local SW needs to be IP addressable - E-box doesn't.
2. Communication between E-box and local SW (traffic over intranet/Internet) is encrypted using TLS.
3. Please include the SQL server in your disaster recovery plan. This database is crucial to the function of the system.

**Access Automation Solutions**

Entrance Automation
Entrance Security

**Access Control Solutions**

Electronic Access & Data
Escape and Rescue Systems
Lodging Systems

**Access Hardware Solutions**

Door Closers
Architectural Hardware
Mechanical Key Systems

**Services**

Technical Support
Installation and commissioning
Maintenance and Repair

**Key & Wall Solutions**

Key Systems
Movable / Sliding Walls

**Safe Locks**

Electronic Safe Locks
Mechanical Safe Locks
Boltworks and Accessories

**Glass systems**

Manual door systems
Glass fittings
Horizontal Sliding Walls

## Our Sustainability Commitment

We are committed to foster a sustainable development along our entire value chain in line with our economic, environmental and social responsibilities toward current and future generations. Sustainability at product level is an important, future-oriented approach in the field of construction. In order to give quantified disclosures of a product's environmental impact through its entire life cycle, dormakaba provides Environmental Product Declarations (EPD), based on holistic life cycle assessments. https://www.dormakabagroup.com/en/sustainability/product-declarations.

SAL_1644_GD_EN CEI 0225
Subject to change without notice

**dormakaba USA Inc.**
1525 Bull Lea Road, Suite 100
Lexington, KY 460511
1-800-950-4744

**dormakaba.com**