

Axessor Apexx System Architecture

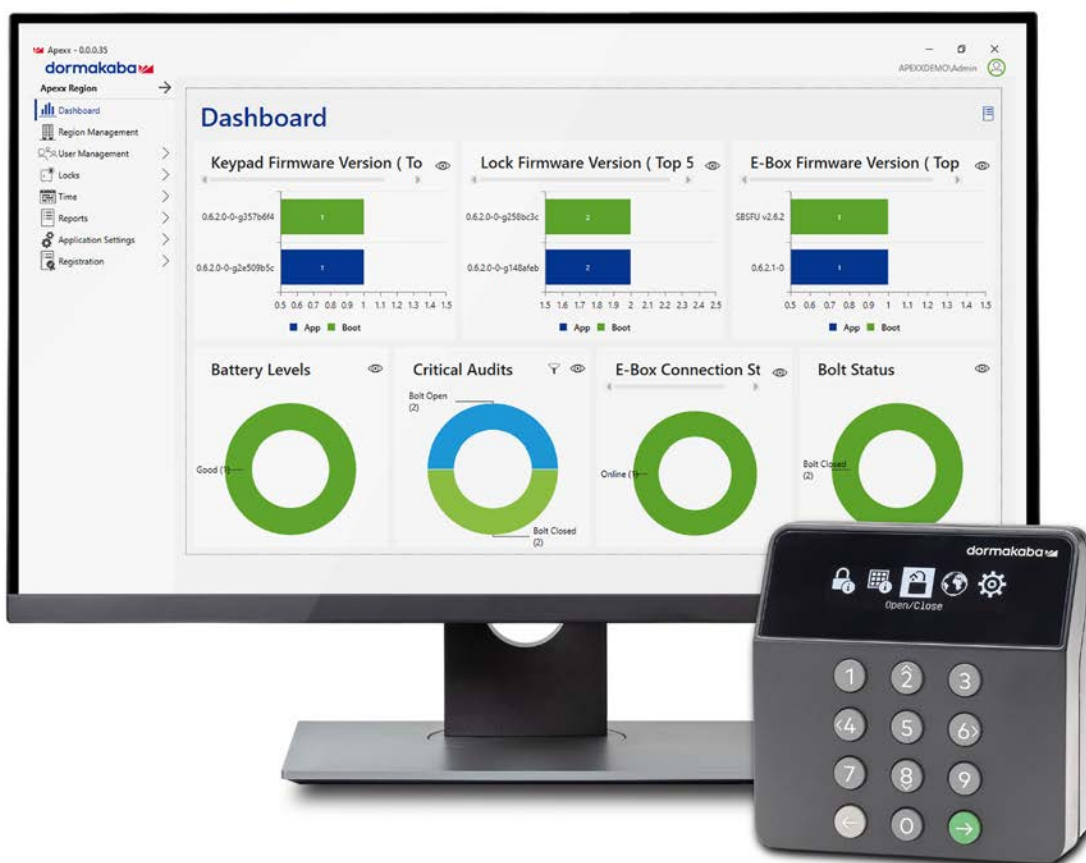


Table of Contents

- Apexx System Architecture - Overview 2
- Apexx API 2
- Apexx Client Software 2
- Apexx Database 2
- MQTT Broker/Server 3
- SMTP 3
- SSO 3
- User Configuration 3
- Licenses 4
- Local vs Remote Firmware Updates 4
- Data Transit 5
- Security & Data Encryption 6
- Public Key Infrastructure (PKI) 6
- Computer Hardware Configurations 7
- Database Considerations 10
- Apexx Recommended Computer Specifications 10

Apexx System Architecture

Overview

Apexx locking systems can be broken into 2 secure communication networks: **The Lock System Can Bus** and **API/Software Network**

The Lock System CAN Bus supports the following components:

- **Apexx Series Keypads** (Maximum = 2, Minimum/Required = 1)
 - Used as a User interface for lock system access and configuration
- **Apexx Series Locks** (Maximum = 16, Minimum/Required = 1)
 - Physical electromechanical lock which controls user access to the safe
- **Apexx eBox** (Required for Networked / IP Connected Mode)
 - Functions as a bridge between the Lock System and the API/Software

The **API/Software** consists of 4 major components:

- Apexx Client Software
- Apexx Database – Microsoft SQL Server 2019 Express
- Apexx API
- MQTT Broker/Server

Apexx API

The Application Programming Interface, or API, acts as both publisher and subscriber in the MQTT architecture.

Apexx Client Software

The Apexx Client Software is a graphical user interface (GUI) that allows Software Users to use the API to perform actions in the system (change system settings, store/retrieve data, etc.)

The Apexx Client supports multiple users but doesn't support multiuser simultaneously on a single client. Only one person can be logged into a single client instance at any given moment.

Apexx Database

The Apexx Database serves as the main location for data storage in the Apexx system. The Apexx Database uses Microsoft's proprietary relational database management system, Microsoft SQL Server 2019 Express, as a means of storing and retrieving system data.

MQTT Broker/Server

Message Queuing Telemetry Transport, or MQTT, is a messaging protocol that utilizes a publish-subscribe model to facilitate communication between devices. The MQTT Broker/Server acts as a centralized messaging hub and utilizes the MQTT protocol to manage communication between devices.

SMTP

Apexx Series Software utilizes Simple Mail Transport Protocol (SMTP) to send the following: Active alerts, and Scheduled Reports.

- Active alerts are sent to recipients based on the occurrence of one or more software user selected Audit Events.
- Scheduled Reports can be emailed to recipients based on a user defined schedule also using SMTP.

SSO

Apexx Series Software utilizes Single Sign-On, ensuring that a Software User can use their credentials to log into the API using a single set of credentials.

User Configuration

Apexx System Users fall into two distinct categories: **Safe Lock Users**, and **Software Users**

Safe Lock Users are users who will be utilizing the Lock System (consisting of the physical Keypads, Locks, eBox, etc.), and will have unique credentials and roles with permissions that dictate their lock system access.

Safe Lock Users use numeric User IDs and PINs to access the lock system using the Apexx Series Keypad.

The three default Safe Lock User types (Administrator, Manager, and User) constitute a hierarchy of users each with pre-defined roles and privileges within the Locking System. In addition to these user types, additional Safe Lock User Roles can be created using Apexx Series Software's administrative tools that have permissions defined by a Software User.

Software Users refers to users who run the Apexx Series Software and use the software tools to perform management and administrative tasks. Unlike Safe Lock Users, Software Users do not directly access the physical Lock System (open/close safe doors) but perform administrative/managerial tasks via software (adding lock users, reset lock user passwords).

Software Users use credentials to gain access to the Apexx Series Software using Single sign-on (SSO). Software Users who have a Software User "Write" permission can add new Software Users and configure the read/write permissions.

Licenses

Apexx Series Software has multiple license types available, each of which unlocks different software functions and features. Consult the Axessor Apexx IP Price Book for more information.

Local vs Remote Firmware Updates

The process of updating your device firmware varies depending on which license you've purchased.

The "Apexx Local" license allows for local firmware updates only, which can be done by establishing a temporary USB connection between the computer hosting the Apexx Series Software and the Keypad of your lock system.

The "Apexx IP" license allows you to perform **Remote Firmware Updates**, that can be done over a network connection via the eBox. This is a three-step process:

1. A Software User initiates the remote firmware update process, pushing the firmware from the API/Software to the locking system over the eBox.
2. The firmware is downloaded and stored on the locking system. A message will appear on the Keypad display informing Safe Lock Users that there is a pending firmware update.
3. A Safe Lock User enters valid credentials (User ID and PIN) at the Keypad, then initiates the firmware update.

For more information on the firmware update process, consult the **Axessor Apexx System User Guide** and the **Apexx Series Software's** help menu.

Data Transit

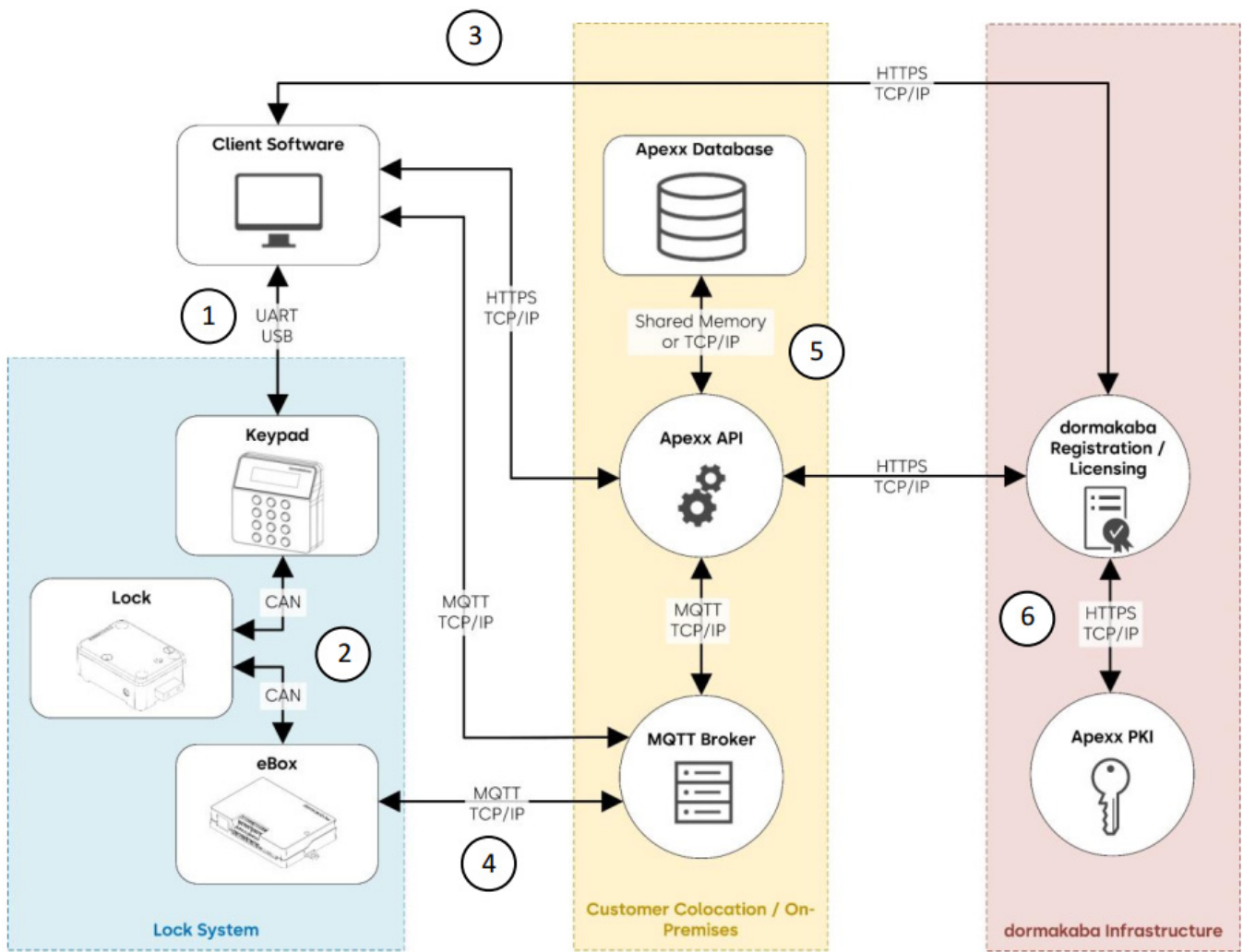


Figure 1 - Apexx System Architecture - System Components and Data Transit

	Communication Protocols	Data flow	Description / Purpose
1	UART over USB	Bidirectional path: <ul style="list-style-type: none"> Client Software to Keypad 	Direct configuration and audit retrieval
2	CAN	Bidirectional path: <ul style="list-style-type: none"> Keypad to Lock Lock to eBox 	Device-to-device communication
3	HTTPS over TCP/IP	Bidirectional path: <ul style="list-style-type: none"> Client Software to dormakaba Registration/Licensing 	Online licensing and registration
4	MQTT over TCP/IP	Bidirectional path: <ul style="list-style-type: none"> Client Software to MQTT Broker Bidirectional path: <ul style="list-style-type: none"> eBox to MQTT Broker 	Networked configuration and audit retrieval
5	Shared memory or TCP/IP	Bidirectional path: <ul style="list-style-type: none"> Apexx API to Apexx Database 	Persistent data storage with SQL Server

Bidirectional path:

- Client Software to Apexx API
- Apexx API to dormakaba Registration/Licensing
- dormakaba Registration/Licensing to Apexx PKI

x.509 certificate issuance

Security & Data Encryption

The Apexx System employs multiple encryption methods, including AES256, PBKDF2, and TLS certificates to ensure the safe and secure communication and storage of data.

Public Key Infrastructure (PKI)

The Apexx System utilizes a Public Key Infrastructure to create, store, and distribute digital certificates to Apexx devices via a certificate authority.

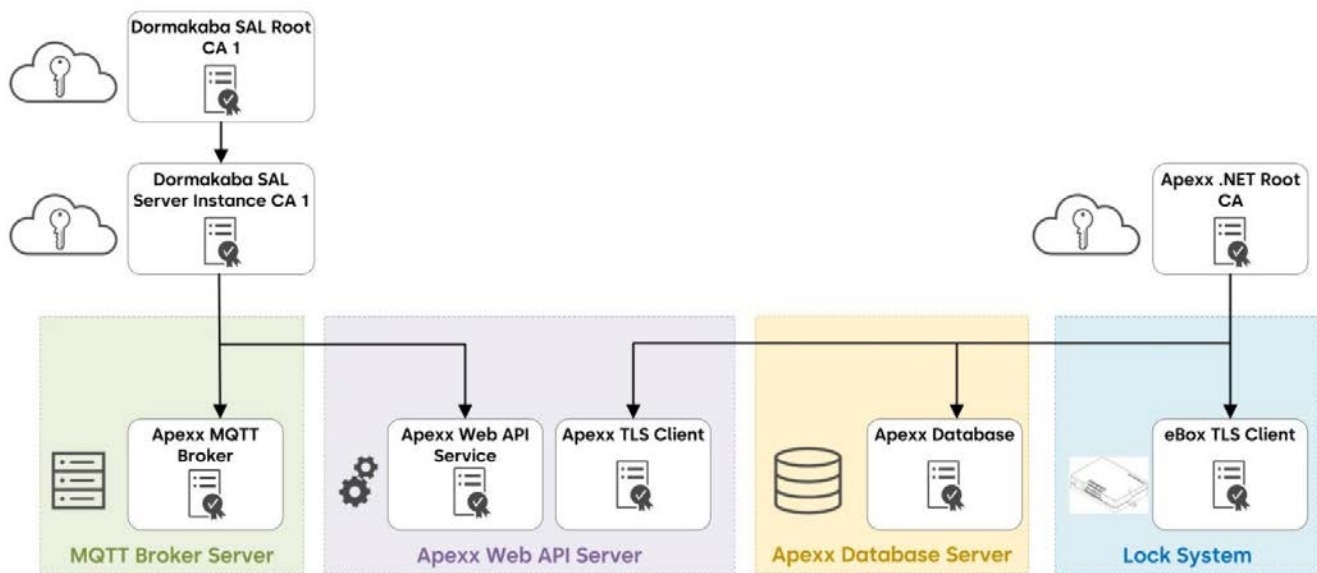


Figure 2 – Public Key Infrastructure

Certificate Type	Description
dormakaba SAL Root CA	<ul style="list-style-type: none"> • This certificate is preloaded on the devices at the factory and replaced via firmware update
dormakaba SAL Server Instance CA	<ul style="list-style-type: none"> • Servers running local software services for Apexx require certificates signed by the dormakaba SAL PKI for devices to trust them • This certificate must be deployed to all servers running local software services • The local software PKI signs certificate requests for all clients of the MQTT broker. • Those certificates are used for both establishing mutual trust Transport Layer Security (TLS) connections and authentication with the MQTT broker. • It can also sign the certificates used by SQL Server for TLS. • If all services are hosted on a single server, multiple certificates are not required to be signed by the Dormakaba SAL PKI. • Even the database can use that certificate if hosted on the same server.

Apexx MQTT Broker	<ul style="list-style-type: none"> • Created during software installation • Used for TLS connections and authentication
Apexx Web API Service	<ul style="list-style-type: none"> • Created during software installation • Contains the server's name (computer where this service is installed), the trusted certificate authority, and the server's public encryption key
Apexx TLS Client	<ul style="list-style-type: none"> • Used for authentication of the Apexx Client • The certificate is a verified user if the issuer matches the installed Apexx .NET Root CA installed on the broker server
Apexx Database	<ul style="list-style-type: none"> • SQL Server on Windows is the only supported database engine • The following settings are enabled on the instance/database: <ul style="list-style-type: none"> • Windows Authentication • Role-based access control (RBAC) is used within, along with Windows Authentication to control permissions
eBox TLS Client	<ul style="list-style-type: none"> • Used for authentication of the eBox • The certificate is a verified user if the issuer matches the installed Apexx .NET Root CA installed on the broker server
Apexx .NET Root CA	<ul style="list-style-type: none"> • Created during software installation • Any computer running the software (client, server, database, etc.) requires a copy of this certificate for security/identification purposes

Computer Hardware Configurations

The Computer Hardware/API/Software portion of the Apexx System can be configured in a number of ways depending on the complexity of your system (number of Apexx Locking Systems, their locations, etc.). This section outlines only a few of the several possible setups. Refer to the Axessor Apexx Price Book for more information on the license requirements for the various computer/hardware configurations.

Note: If desired, any of the software components (Client, Database, API, or MQTT) can be hosted on a virtual machine.

Figure 3 illustrates a basic setup involving just a single computer and one Apexx Locking System. In this setup, all API/Software elements are hosted on a single computer with a USB connection being used to temporarily connect to the Apexx Locking System for programming/system configuration purposes.

This sort of setup works well for small sites where the computer and all Locking System components (Keypads and Locks) are at the same physical location, but lacks the versatility and convenience offered by the networked setups utilizing the Apexx eBox.

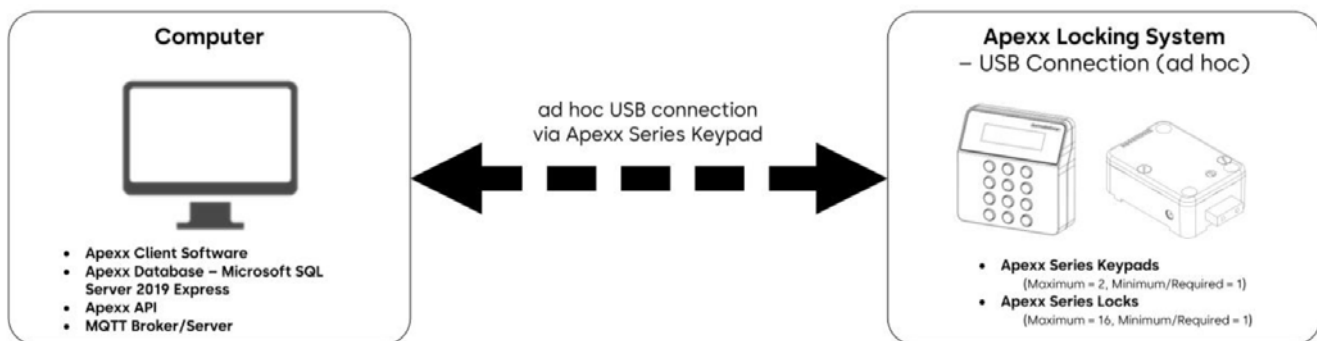


Figure 3 – Single Computer Setup - ad hoc USB connection

Figure 4 shows another simple setup involving just one computer and one Apexx Locking System, but this time the Apexx eBox is used to provide a network/IP connection for continuous/live communication between the computer and locking system.

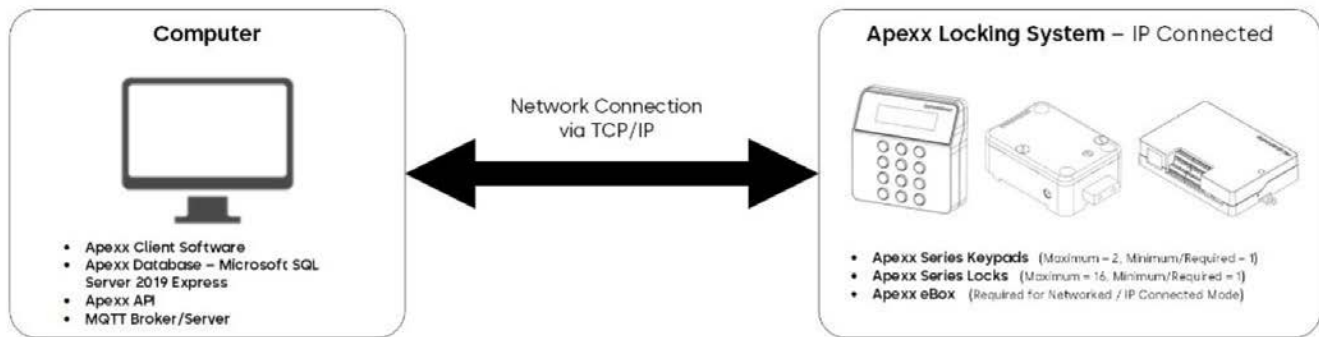


Figure 4 – Single Computer setup - Network via eBox (TCP/IP)

This setup is also useful for smaller setups where all the equipment is at the same physical location, but the inclusion of the eBox allows the system administrator to take advantage of all the features that an active IP connection provides (live audits, active system monitoring, remote firmware updates, and other additional Hardware/Software features)

For larger sites involving bigger buildings and/or multiple Locking Systems, the multiple-computer setup shown in Figure 5 offers additional flexibility.

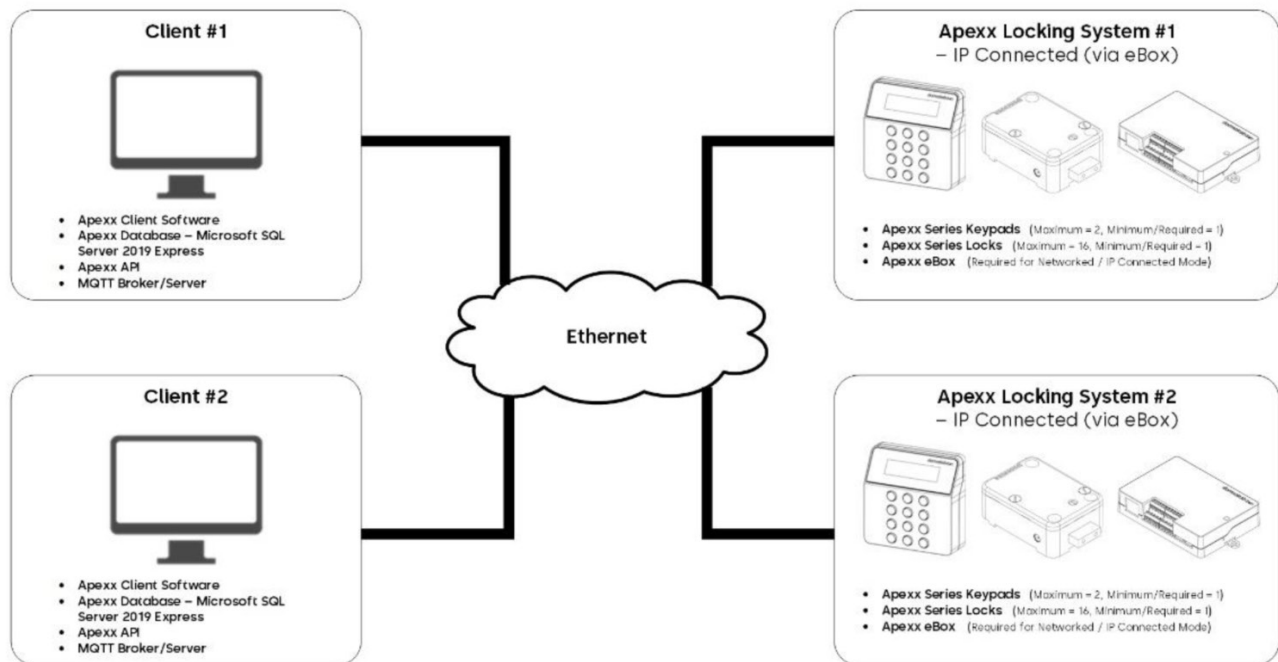


Figure 5 – Multiple Computer Setup with Multiple Locking Systems

In such a setup, any or all of the software components could be installed on one or more computers (or virtual machines), allowing for added convenience and flexibility when it comes to running and configuring your lock systems. Note that each locking system connects to the network via an Apexx eBox.

This concept is expanded further in the system shown in Figure 6, which includes multiple computers and lock systems spread out over multiple buildings.

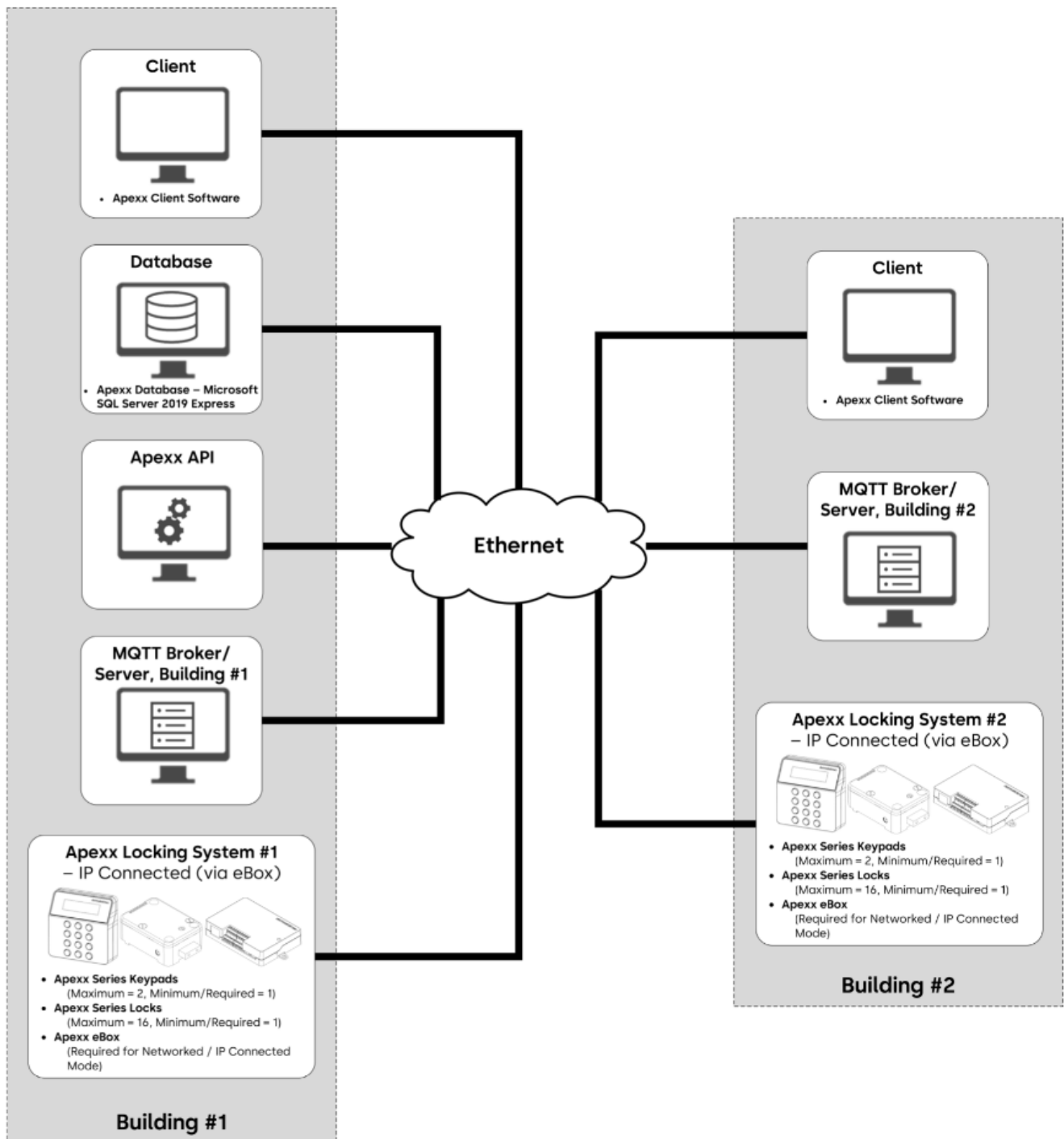


Figure 6 – Multiple Computer/Locking System Setup with multi-server setup

One notable difference between this setup and all the others is that it includes multiple computers hosting different software components. Note how two of the computers in Building #1 host the Apexx API and Apexx Database respectively. These two computers can be configured to be used as the API and Database for the Locking Systems in Building #1, Building #2, and/or any other Apexx System on the entire network.

This final example illustrates that many different setups are possible depending on your organizational needs and IT infrastructure setup.

Database Considerations

Apexx Series Software includes Microsoft SQL Server 2019 Express as its dedicated internal database engine

	Microsoft SQL Server 2019 Express (64-bit)
Database Limit	10 GB
Number of CPUs	1 physical processor
RAM	1 GB
Supported Operating Systems	Windows 10, Windows Server 2016, Windows Server 2019

Apexx Recommended Computer Specifications

Apexx Client Workstation

- Intel Core i7 – 4470 3.40GHz with 4 cores
- 16GB RAM 1600MHz DDR3 NON-ECC
- 500GB Hard Drive
- Windows 10 Professional 64bit
- AMD RADEON HD 8490 1GB Dual Monitor or AMD RADEON HD8570 1GB Dual Monitor
- USB 2.0 Ports
- Ethernet Port - 1Gb Network Card
- Keyboard & Mouse
- UPS Backup

Apexx Broker Server

- Intel Xeon E5 – 2403, 1.80GHz, 10MB Cache
- 16GB RAM 1333MHz, RDIMM
- 500GB Hard Drive
- Windows 2019 Server Standard 64bit
- Integrated HD Graphics Card
- Ethernet Port – 1Gb Network Card
- Keyboard & Mouse
- UPS Backup

Apexx Database Server & Apexx API

- Intel Xeon E5 – 2420, 1.90GHz, 15MB Cache with 6 cores
- 32GB RAM 1333MHz, RDIMM
- 2 x 1TB 7.2K RPM SATA 3Gbps 3.5in Hard Drive
- RAID 1 Configuration
- Dual, Hot-Plug, Redundant Power Supply
- Windows 2019 Server Standard 64bit
- Integrated HD Graphics Card
- Ethernet Port – Gb Network Card
- Keyboard & Mouse
- UPS Backup

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.

www.dormakaba.com/sustainability



Our offering

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



Apexx System Architecture, EN, 02/2024
Subject to change without notice

dormakaba USA Inc.

1525 Bull Lea Road, Suite 100
Lexington, KY 40511

sales.safelocks.us@dormakaba.com

T +1 800 950 4744

+1 888 950 4715 (tech support)

dormakaba.com



AXESSOR APEXX IP
INSTALLATION AND
OPERATION GUIDES

dk.world/AxessorApexxIP