



ALLEGION™

PIONEERING SAFETY™

Allegion Engage IP Gateway Mode Integrations

August 11th, 2025

Training overview

- We will go in depth into communicating with locks in Gateway IP Mode.
- Folders:
 - ENGAGE IP Test Tool – a tool that can be used to exercise gateways
 - face to face documents – Original training material used for engage partners
 - json examples – Sample json we will use / analyze is stored here
 - Postman Scripts – The collections to import into postman to use during training
 - PPT slideshows – A copy of these slideshows
 - Decrypt Encrypt Utility – a Windows utility for encryption/decryption using site keys.
(Apple users can use webpage utilities noted in slide shows)

What is Engage?

- “Engage” can refer to several different things
 - **The line of hardware and associated items being integrated**
- Allegion hosted cloud services:
 - A simple ACS software for small and mid-sized installs
 - Needed to create sites and provision/enroll devices/locks into a “site” for partner (i.e. “PACS” or “SAMs”) integrations. More on sites later
 - Other features – e.g. “no tour”
- A mobile app (MAPP) (iOS & Android) that is used in conjunction with PACS’ software
 - Allegion’s own Engage app is the most notable example
 - Most notably to provision/enroll devices & send debug logs
 - PACS can implement their own mobile app instead, but this is not trivial

Allegion Products Options

- **ENGAGE™ Products**

- NDE/NDEB (cylindrical lock & reader, 2.4 GHz wireless, WiFi & BLE)
- LE/LEB (mortise lock & reader, 2.4 GHz wireless, WiFi & BLE)
- Control (deadbolt lock & reader BE467/FE410, 2.4 GHz wireless, BLE only – no Wi-Fi)
- RU/RM (exit trim controller, 2.4 GHz wireless, WiFi & BLE, no reader)
- CTE (access point controller, 2.4 GHz wireless, WiFi & BLE)
- Schlage Reader Controller (SRC) series [11/15] (reader controller with i/o for DPS, strike, etc., 2.4GHz, Ethernet & BLE for commissioning only, no firmware update via BLE)
- Gateway (GWE) (interface module, BLE, Ethernet & RS485 wired)
- MT20W (USB smart credential reader/encoder, 2.4 GHZ wireless. WiFi & BLE)
- XE360 (mortise lock & reader, BLE Communication Only – no wi-fi unlike in YP)

Allegion Products Options

- ENGAGE™ Products
 - NDE vs NDEB and LE vs LEB
 - The “B” revisions support mobile Bluetooth credentials, whereas the originals do not
 - NDEB always has an inside push button (IPB), whereas NDE does not.
 - IPB for instance used in “privacy” mode to disable normal credentials (more on modes later)
 - NDE does not support TLS 1.2, so going forward cannot really be part of Wi-Fi implementations. There is an upgrade kit available (see below)
 - Original versions are no longer sold
 - **Pricebook** – Go to <https://360portal.allegion.com/store>, then select pricebooks at the bottom right, then choose the latest “Electronics” PDF.
 - LE(B)/NDE(B) Chassis need DPS for privacy and apartment modes. These are options in the pricebook, so it’s important to acquire the right hardware.
 - NDE/NDEB/LE/LEB/Control/ControlB/ControlBM all work with the GWE
 - Note three generations of control locks, control is no longer sold.

Allegion Integration Architecture Options

- **Ethernet (online, 410IP)** – We will focus on this most for our examples using postman and an “Unmanaged Site” (or “PACs managed - we will define sites later)
- Note that “IP” is a misnomer, since it implies any IP (which can include Wi-Fi). It would be more accurate to call this “410Ethernet”, since the gateway must have a network drop to communicate on the network, no wi-fi is involved
- Direct Wi-Fi (offline, 210)
- BLE (Mobile Application, offline, 200)
- Smart Credential and Schlage Mobile Credential (No Tour, “viral”)
- RS-485 (online, 410RSI, Mercury controller integration) – We will touch briefly on this, but not go into depth, as the RS-485 integrations are very different from other engage topologies

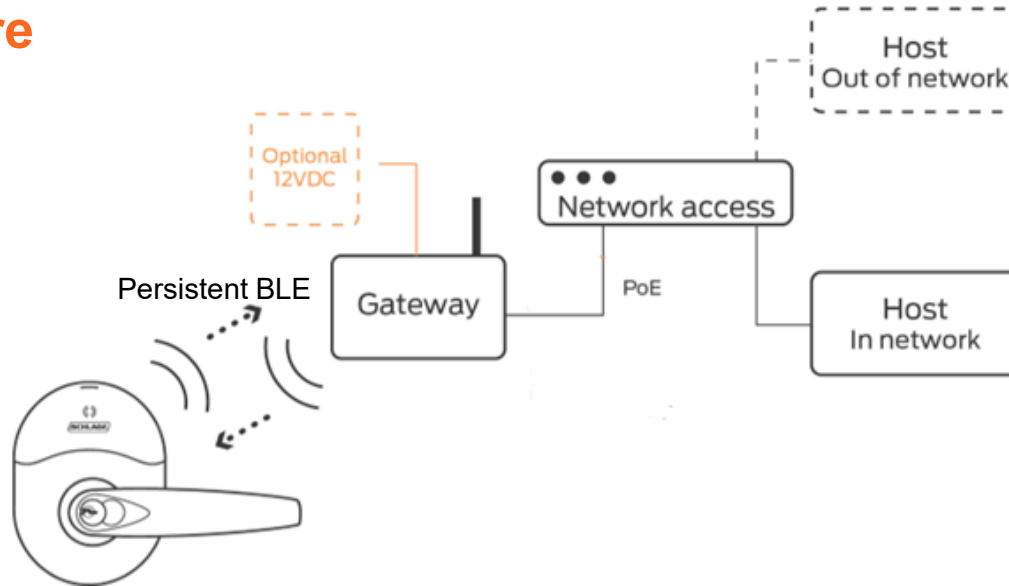
Allegion Integration Architecture Options

See “Communication Mode Table.xlsx”

Comm mode	(Near) Real time control	Need to implement mobile app	Compatible devices	Need to tour	PACS can be in cloud	PACS can be on premise	No-Tour integration	Requires Access Control Panel	Notes
Gateway with (410) Ethernet/IP (Typical)	Yes - constant communication over network from PACS to Gateway, then from gateway to locks with low frequency comms	No - can enroll devices with Engage Mobile app and the rest is http(s) calls	NDE/NDEB/LE/LEB/Control/ControlB/ControlBM/XE360	No	Generally not (requires firewall and/or VPN adjustments for PACS client to make HTTP calls on gateway server)	Yes	Not needed since can add cards to database in real time (although will work technically)	No	Door decisions on opening are instantaneous as the decision is made on locks; other items may have a small latency (~5 secs or less) such as remote unlock, or audit retrieval
Gateway with (410) Ethernet/IP (Websockets)	Yes - constant communication over network from PACS to Gateway, then from gateway to locks with low frequency comms	No - can enroll devices with Engage Mobile app and the rest is an http(s) call to establish websockets	NDE/NDEB/LE/LEB/Control/ControlB/ControlBM/XE360 (RC can perform this function as well)	No	Yes, since the gateway is the client, it can more easily initiate a call to the PACS server without extensive firewall / VPN adjustments.	Yes	Not needed since can add cards to database in real time (although will work technically)	No	Door decisions on opening are instantaneous as the decision is made on locks; other items may have a small latency (~5 secs or less) such as remote unlock, or audit retrieval
Direct Wi-Fi (210)	No - Periodic (typically 8, 12 or 24 hours) call in updates initiated by lock to PACS system for door file updates and audit retrieval. Can dial in on demand from app or special credential	Not generally - can enroll devices with Engage Mobile app and the rest is http(s) calls. However Yes when used with no tour.	NDEB/LE/LEB/CTE	No	Yes, since the locks are making the client call, they only need access to the cloud server (firewall adjustment may be needed).	Yes, this is the easiest communication setup.	Yes, very useful to issue access between call in intervals). However, note this requires a mobile app be implemented, to update door files when needed.	No	Door decisions on opening are instantaneous as the decision is made on locks; other items will only be updated periodically
BLE Mobile Application Touring (200)	No - updates only when toured	Yes, since engage app will not know how to translate server's access levels and schedules and such into appropriate json format	NDE/NDEB/LE/LEB/Control/ControlB/ControlBM/XE360	Yes	Yes	Yes	Yes, very useful to issue access between tours	No	Door decisions on opening are instantaneous as the decision is made on locks; other items will only be updated when toured

Ethernet (online, 410IP – aka “410Ethernet”)

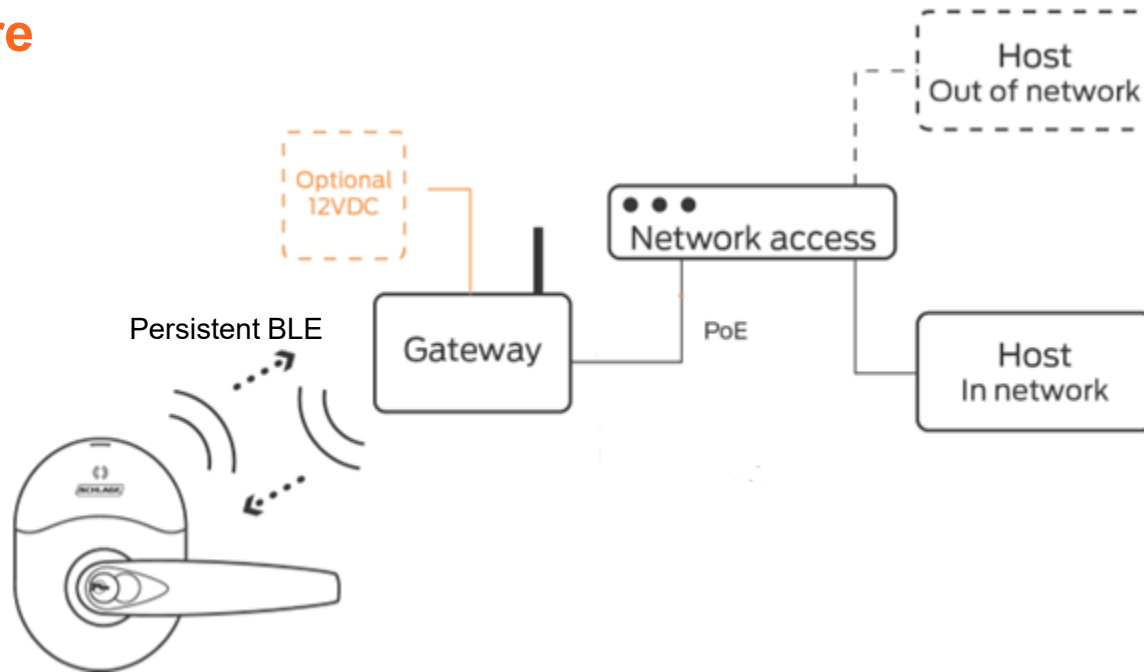
Architecture



- Database in NDE/LE/Control lock (access control decision is made in lock)
- Connection is real time (downloads database/configuration changes & uploads any new audits) – gateway acts as a passthrough to/from lock
- Must have a client
- Client is either on the LAN, (atypically in WAN, or in the Cloud)
- No access control panel (ACP)
- The Gateway can be the server (typical) or client (“Websockets”)
- The SRC can also act as a websockets client

Ethernet (online, 410IP) – typical server

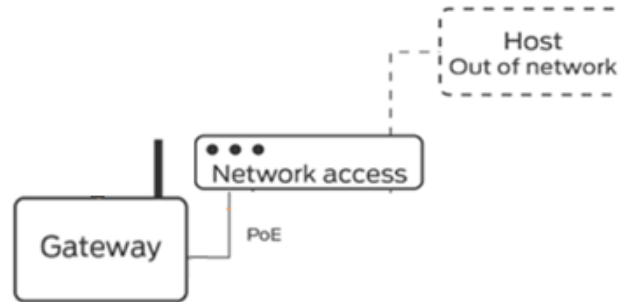
Architecture



- The PACS system calls https functions (PUT, POST, GET, DEL) on the gateway to poll for audits, upload new door data files, etc.
- The PACS system also calls https functions to the engage cloud to manage the site(s)
- The Gateway is the server for the PACS calls, PACS is the client
- Almost always requires the Access Control System to be on premise, rather than cloud (although it is theoretically possible for a cloud client, if firewalls / VPN are setup for this)

Ethernet (410IP online, Websockets)

Architecture



- The Gateway (GW) is the client for the PACS system (opposite typical setup)
- PACS system serves as a host server (opposite of typical setup)
- DB in Locks (access control decision made in lock)
- GW handshakes to Host via http(s), then establishes a socket communication (Bidirectional constant communication for door data files or audits as they occur)
- Host is either on the LAN, WAN, or in the Cloud.
- No access control panel (ACP)
- Activated by clicking “IP Behind Firewall” when enrolling into site
- See “Schlage ENGAGE WebSockets App Note-1.06.pdf”
- The GW only communicates on Websockets (no mix/match client/server).
- The SRC can also act as a gateway in websockets mode

Engage door “functions” (sometimes called “modes”)

Function / Mode	Description
Classroom/Storeroom (70)	Lockset is normally secure. Inside lever always allows free egress. Valid toggle credentials on the exterior may be used to change to a passage or secured status.
Office (50)	Lockset is normally secure. Inside lever always allows free egress. Interior push button on inside housing may be used to select a passage or secured status. Meets need for lockdown function for safety and security. NOTE: Valid toggle credentials on the exterior may be used to change to a passage or secured status.
Privacy (40)	Lockset is normally secure. Inside lever always allows free egress. Interior push button on inside housing may be used to select a privacy status (normal credentials disallowed from access, pass-thru permitted). Opening the door or pressing the interior push button a second time on the inside housing deactivates the privacy status. The AD-Series is available with six different credential reader options which are adaptable in the field.
Apartment (60)	Lockset is normally secure. Inside lever always allows free egress. Interior push button on inside housing may be used to select a passage or secured status. Opening the door or pressing the interior push button causes the lockset to toggle unsecured. While toggled unsecured, the lockset can only be secured while the door is closed by pressing the interior push button or using a normal credential on the exterior. Normal electronic access from the exterior is always allowed. *
	* This mode was derived from housing requirements in some parts of Canada

- See “Door Modes - Functions Explanation and State Change Table for Apartment Mode.xlsx” for a more complete explanation
- In particular, different trims (no IPB, IPB, Deadbolt) support these functions (or not) in different ways. That is explained in the excel file

Engage - Tools, Artifacts

- Tools
 - Engage Mobile App (MAPP)
 - Downloadable on iOS and Android, needed to enroll locks in any mode of communication (or a PACS MAPP)
 - IP Test Tool
 - Allows you to communicate with Gateways in real time, server and client
 - RSI Test Tool
 - Useful in debugging RS485 RSI protocol implementations
 - Engage Device Quick Start App
 - Hosted on github, need to compile ourselves
 - Contains basic implementation of all needed functionality in a Mobile Application (MAPP)
 - Gateway Client Websockets Integration
 - A sample websockets integration written in python, for demonstration purposes

Engage - Validations

- **Validation Sheets**

- File a ticket at: <https://developersupport.allegion.com/hc/en-us/requests/new>
- In the ticket form:
 - Select "Engage" as the category.
 - Choose "Integration Validation Request" as the Engage Type to access the correct form.
- A validation sheet will be sent out, for you to mark which features you implemented
- An OEM Engineer will then provide the validation