



ALLEGION™

PIONEERING SAFETY™

Creating Engage Accounts, using the Mobile App, introduction to Postman usage

August 11th, 2025

What is Engage?

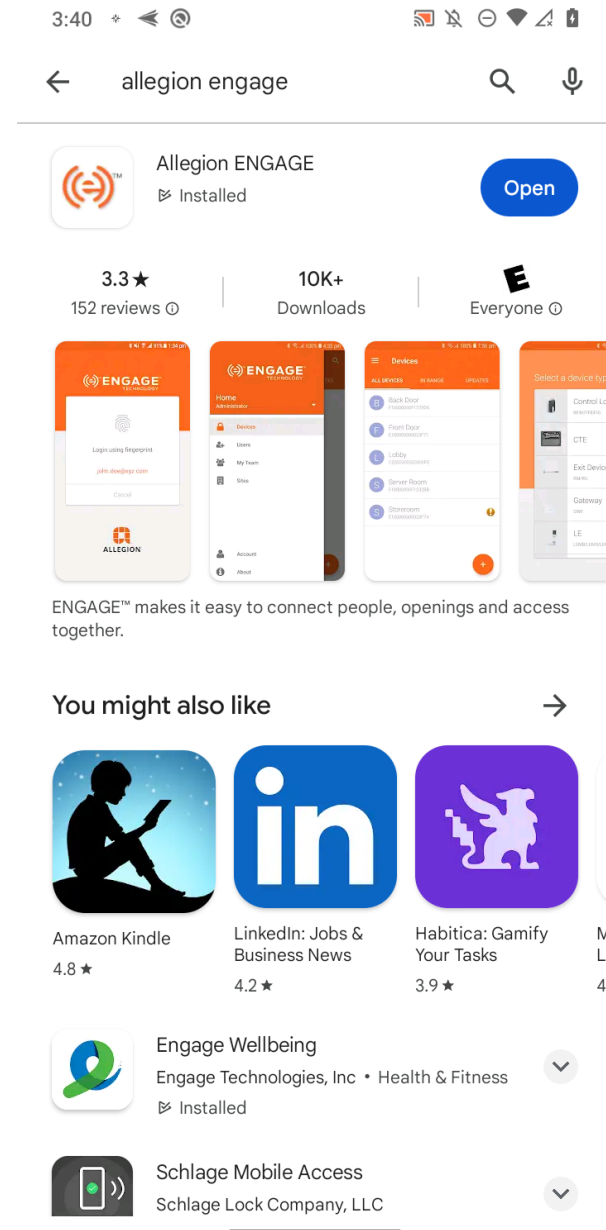
- “Engage” can refer to several different things
 - The line of hardware and associated items being integrated
 - Allegion cloud hosted services:
 - Needed to create sites and provision/enroll devices/locks into the site
 - Hosts a website that offers a simple ACS software
 - Other features - could be future relevant
 - **A mobile app (iOS & Android) that is used in conjunction with partners’ (i.e. “PACS”) software**
 - Most notably to provision/enroll devices & send debug logs
 - PACS can implement their own mobile app instead, but this is not trivial, and likely beyond the scope of this training

Putting the pieces together – accessing cloud services and the mobile app

- We will start by creating an account that can access the Allegion cloud hosted services
- By downloading the mobile app and creating the account there, we can kill two birds with one stone

Getting the app

- Available on both Android and Apple stores
- This demo will use iOS, but Android is very similar
- **Start mobile sharing screen**



Creating and managing accounts

- Can be done via website or mobile app
- Website: <https://portal.allegionengage.com/signup>
- Either method results in typical email notification, verification link, etc.
- Something to consider later after basic understanding is clear
 - “Engage account management”
 - E.g. One “central/main” account for creating all sites for all of a PACs’ customers, vs. “one per premises”
 - Either way, some end users will need lower permission accounts to enroll devices, so multiple accounts are needed
- **Show how to create an account in the app, while sharing Mobile screen**

Sites - what are they?

- The first useful step a “Normal” or PACs Engage account can take is to create a site
- Fundamentally, a site is an abstract container for
 - Devices and links between devices
 - A unique symmetric encryption key (aka the site key)
 - Errata such as default settings
- Sites are required for communication and are the starting point for any use of Engage devices
- Sites for Allegion’s simple Access Control System also contain cardholders, access, etc. – not relevant to software partners (PACS).

Sites (Managed vs. Unmanaged)

- During creation, a site is set to one of two types
 - **Managed** (sometimes called “Engage managed”)
 - Used by the simple Engage ACS
 - Useful for tinkering / debugging, but not used by production PACs
 - These can be created via either API, mobile app, or Engage website
 - The encryption key is hidden from all users
 - ~~Create a site and demonstrate the managed site functionality~~

Sites Unmanaged

- During creation, a site is set to one of two types
- **Unmanaged** (sometimes called “partner” or “PACs managed”)
 - This is what all partners will be using
 - Can only be created via REST API call (not via mobile app or website)
 - Creation requires a name, encryption key (site key), and some metadata
 - **It is very important not to lose the key**

Sites Unmanaged

- **Create a site via Postman**
 - Use “create site.json” (edit your name into the site name) via the POST /engage/sites/register after setting needed environment variables
 - Environment variables needed up front:
 - engageUser
 - engagePassword
 - Later we will use:
 - gatewayIP
 - siteReference
 - linkId
 - user
 - password
- **We will be demonstrating unmanaged sites using 410IP mode, but other modes are similar except the means of transmitting the json – we will discuss on final slide of this deck**

Mobile App Demonstration – Enrolling Devices

- Some basic things to keep in mind
 - To enroll/provision a device to a site, two things must be true:
 - Device must be factory reset (“FDR’ed”) at the hardware itself
 - Any software records in engage cloud referring to that device must be deleted, from any site. **This is very easy to forget and can be tough to debug**
- Point out the FDR document (“FDR List - factory reset.docx”)
- Pics of reset buttons on next slide

Location of reset (FDR) buttons



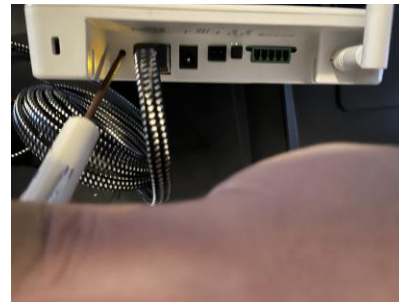
Control



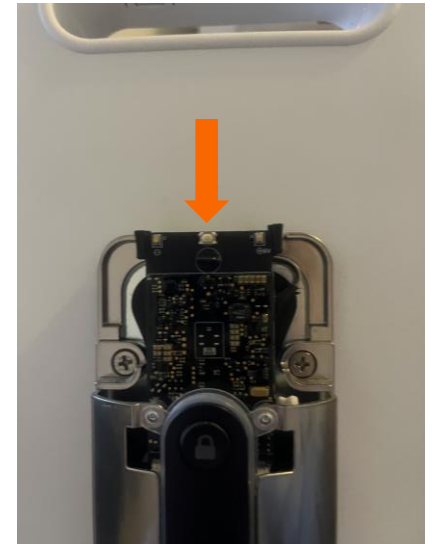
LEB



NDEB



Gateway



XE360

Mobile App Demonstration

- Prep: in this scenario, let us pretend we are reusing a gateway and Leb lock that were previously deployed elsewhere, and we need to connect to our new site. Keep in mind this background information about the devices
- **Switch to live demonstration of mobile app** in order to enroll Control lock and then a gateway, and then link them
- First FDR the lock, then enroll into new unmanaged site using mobile app
- Be sure to remove the lock from any sites it had previously been enrolled into
- Highlighted this problem because very common for techs to assume the factory reset button “blows everything away”
 - Usually true for most ACS hardware – I made this assumption

Mobile App Demonstration – some “lessons”

- **Switch to live demonstration of mobile app** in order to enroll a gateway and LEB, and then link them
- Note devices can be linked without mobile app
- Use GET {{gatewayIP}}/gateway/scanList to get the serial numbers of all nearby devices
- and then POST {{gatewayIP}}/edgeDevices with the device's serial number
- Note the device must first be FDR'ed and then already enrolled in the correct site
 - An FDR'ed lock will not appear in the scan list
 - A lock commissioned to a different site will return a 500 "Link failed to connect" error

Mobile App Demonstration – Review Notes

- Locks are enrolled separately from Gateways, and then linked
 - Can't link an unenrolled lock to a gateway in one step
 - Order of enrollment doesn't matter, but GWE-Lock link can't be created until both devices are enrolled
 - Once linked, can't managed in mobile app
 - Workaround (NDEB/LEB); can temporarily reset this by holding down inner handle and swiping a credential (lasts ~30 seconds)
 - Workaround (Control); can temporarily reset this by swiping a credential and engaging/disengaging the deadbolt 5 times from the secure side

Mobile App Demonstration – Review Notes

- Note the “Send Logs” feature in the mobile app for gateways
- Adds more information to the support portal we use by uploading info to allegion cloud, and can be very helpful in debugging
- PACs can also access this information directly without using our cloud
- Obscure – main URL is not in postman collection
 - {{gatewayIP}}/gateway/GatewayAudit.log
 - Along with {{gatewayIP}}/gateway/gatewayNetworkStatistics, {{gatewayIP}}/gateway/gatewayEventLog, {{gatewayIP}}/edgeDevices/linkList, {{gatewayIP}}/gateway/scanList, {{gatewayIP}}/gateway/deviceInfo
- We now have a mini system to poke around with in Postman

Core Concepts of Lock Management

- But first, let's take a step back
- **At its core, managing a lock is simply managing three json constructs:**
 - 1. Config / Params**
 - 2. Database / Doorfile**
 - 3. Audits (e.g valid access, door forced open, low battery, etc.)**
- Gateways have a slightly more complex set of json
- Database updates can include config updates. Refer to json spec for more info ("ENGAGE_JSON_Data_Structures - 2.18.pdf")
- If you keep in mind these three core concepts, managing a lock seems simpler