TECHNICAL Information:

ENGAGE™ Wi-Fi network requirements

SES20180226-E

When discussing how ENGAGE™ devices use Wi-Fi, provide this technical information to customer site IT departments. This note should answer IT department questions when scoping ENGAGE™ product feasibility on their network.

OVERVIEW:

ENGAGE™ devices use the local Wi-Fi network to automatically enable update functions for the property administrator. When Wi-Fi is enabled, the devices will automatically call in with the local wireless network at a time predetermined by ENGAGE™ (typically between midnight and 4am). The devices obtain updates and provide maintenance information to the ENGAGE™ server. The use of Wi-Fi by an ENGAGE™ device is an operational convenience, and not an access control necessity. ENGAGE™ devices can also operate with Wi-Fi disabled in a standalone mode; but this makes some updates and audit collection less convenient.

Product Application:

ENGAGE™ devices with Wi-Fi nightly call in capability are limited to the following: NDE, NDEB, LE, LEB, and CTE. With Wi-Fi enabled, this group will connect once per night to the local Wi-Fi network. When the ENGAGE™ system feature "Wi-Fi Alerts" is enabled, the devices will also connect briefly to report forced door or propped door when the alert occurs.
Please note the following:

1) The MT20W enrollment reader requires a local Wi-Fi network connection to enroll. USB or Wi-Fi can be used when programming user credentials. The MT20W does not call in nightly.
2) When ENGAGE™ devices are LINKED to an ENGAGE™ Gateway, the Wi-Fi network is not used. Device management communication is with Bluetooth through the Gateway. Device Wi-Fi is disabled when linked to an ENGAGE™ Gateway.
3) Schlage Control™ smart devices, FE410 and BE467, are not Wi-Fi enabled.

Wireless Information:

All Wi-Fi enabled ENGAGE™ devices have the following requirements and applications when connecting with the Wi-Fi network:

NOTE: Consult with your IT professional when working with Wi-Fi network connectivity.

1) **Communication Standards:**
   - 2.4 GHz 802.11 **b/g** is required for NDE and MT20W.
   - 2.4 GHz 802.11 **b/g/n** is supported for NDEB, LE, LEB, CTE, and RU/RM.

2) **Connect Data Rate:** Each Wi-Fi network access point supporting specific ENGAGE™ devices requires the Mandatory Connect Data Rate to be set:

- NDE and MT20W devices require the Wi-Fi Mandatory Connection Data Rate to be set no higher than **24Mbps** or they fail to associate with the wireless AP.
- NDEB, LE, LEB, CTE, and RU/RM devices **do not** have any Wi-Fi Mandatory Connection Data Rate restrictions.
- The local IT professional should check this router setting if/when devices fail to associate with the local Wi-Fi network.
- An Automatic Mandatory Connect Data Rate is a typical router setting. IT professionals use this setting to force a minimum data rate for each device to associate with the Wi-Fi access point. The Connect Data Rate setting is intended to increase Wi-Fi network performance and not allow weak signal or slow data rate devices to connect.

3) Wi-Fi network security types supported:

- **WPA2** (PEAP)
  - Wi-Fi SSID - Must be EXACT (case sensitive)
  - USERNAME
  - PASSWORD*
- **WPA2**
  - Wi-Fi SSID - Must be EXACT (case sensitive)
  - PASSWORD*
- **WEP** (not recommended)
  - Wi-Fi SSID - Must be EXACT (case sensitive)
  - PASSWORD*
- **OPEN** (not recommended)
  - No Wi-Fi security

*Maximum 64 Character length. English alpha-numeric characters only.

4) If the building Wi-Fi employs **MAC address** listing, and the device MAC address is needed, each ENGAGE™ device has its MAC address printed on the production labels in human readable and in QR form. The MAC address is also human readable within the ENGAGE™ mobile application when connected to the device.

5) ENGAGE™ devices use both **standard HTTP and HTTPS** connections for communication. Encryption is provided through the TLS connection made over the HTTPS connection to the servers, as well as each credential is individually encrypted with a site-specific scheme automatically generated by the system.

- ENGAGE™ devices browse to allegionENGAGE.com; or a Physical Access Control Software (PACS) server when managed by a PACS System
  - Portal.allegionENGAGE.com – is used by ENGAGE™ system admins inside the firewall when logged into the ENGAGE™ WEB Application.
  - Api.allegionENGAGE.com – is accessed by the ENGAGE™ device for firmware and database updates, as well as reporting audits and alerts.
  - Contact your Access Control Software provider for their server address if your devices are managed by a PACS System.

6) The network can assign a static or DHCP IP address to ENGAGE devices. However, the device cannot be internally configured for a static IP address. Only IPv4 is supported at this time.

7) ENGAGE™ Wi-Fi devices use only two **ports, 80 and 443**
- Port 80 (http) is used for encrypted firmware downloads and updating the root certificate loaded in the device.
- Port 443 (https) is used by the device for providing all maintenance information, updates on the activity of the device, and providing credential access updates to the device.

8) Wi-Fi enabled ENGAGE™ devices will connect to the Wi-Fi network with three individual events per night. Connections are once-per-day for ENGAGE™, and session-based (established, utilized, and released). The ENGAGE™ device reports its configuration in the first event, obtains access control updates in the second event, and reports audit data in the last event.
- Total daily network bandwidth consumption would be approximately ~ 64 kb per device (Assuming the device has 100 user changes, and 15 valid card presentations per day).
- Wi-Fi session events estimates for nightly call:
  - PUT Configuration (from device): ~40 kb
  - GET database (from server): ~20 kb / 100 users (changes)
  - POST Audits (from device): ~4 kb (Assuming 15 valid card presentations per day)
- During this update the ENGAGE™ server schedules the next nightly call in with the device.
- The nightly Wi-Fi call in only takes a few seconds per device.

9) The ENGAGE devices are reliant on the primary DNS server configured in your network. The ENGAGE device is not capable of utilizing a secondary DNS server or complex DNS redirection the way laptops on the network redirect. DNS errors are displayed in the audit reports along with host connection failure. In this case we recommend that ENGAGE Wi-Fi customers are use a publicly available DNS such as google (8.8.8.8 or 8.8.4.4) or ensure that the internal DNS table has a valid entry for api.allegionengage.com.

10) ENGAGE™ devices enabled with Wi-Fi can also update firmware by connecting to the ENGAGE™ server. The firmware update can be enabled with the ENGAGE™ WEB application for an automatic update during the nightly call in, or it can be implemented manually by connecting to the device with the ENGAGE™ mobile application and selecting “Update Firmware.” New ENGAGE™ firmware releases only occur a few times a year. A device firmware update could take only tens of seconds on Wi-Fi, but up to four minutes to complete the file loading and re-boot of the device.

11) When an ENGAGE™ device is using Wi-Fi an AMBER (RED/GREEN mixed) LED will be displayed and the device will briefly ignore card presentations.

Document Revision	COMMENTS	DATE	Author
SES20180226-A	Initial release	2/28/2018	DCX
SES20180226-B	RU/RM, MT20W, and PACS updates	2/4/2020	PX
SES20180226-C	Mandatory Data Rate, DNS, and wording updates	4/13/2020	PX
SES20180226-D	Added information for NDEB, LEB	4/14/2020	PX
SES20180226-E	Added information for IPV4	6/9/2020	PX