OPEN OPTIONS®
ACCESS TECHNOLOGY

Engage Wi-Fi Quick Start Guide

This manual is proprietary information of Open Options, LLC. Unauthorized reproduction or distribution of this manual is strictly forbidden without the written consent of Open Options, LLC. The information contained in this manual is for informational purposes only and is subject to change at any time without notice. Open Options, LLC. assumes no responsibility for incorrect or outdated information that may be contained in this publication.

DNA Fusion™ and SSP™ are trademarks of Open Options, LLC.

The DNA Fusion™ Access Control Software and SSP™ Security System Processor use equipment that generates, uses, and radiates radio frequency energy. If not installed and deployed in accordance with the guidelines of this installation manual, they may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause harmful interference, in which case the user will be required to correct the interference at their own expense.

The DNA Fusion™ Access Control Software and SSP™ Security System Processor shall be installed in accordance with this installation manual and in accordance with the National Electric Code (N.E.C), ANSI and NFPA 70 Regulations and recommendations.

Publish Date: September 4, 2020
Manual Number: EWQSG 1.1

© Copyright 2002-2020 Open Options, LLC. All rights reserved.

Warranty

All Open Options products are warranted against defect in materials and workmanship for two years from the date of shipment. Open Options will repair or replace products that prove defective and are returned to Open Options within the warranty period with shipping prepaid. The warranty of Open Options products shall not apply to defects resulting from misuse, accident, alteration, neglect, improper installation, unauthorized repair, or acts of God. Open Options shall have the right of final determination as to the existence and cause of the defect. No other warranty, written or oral is expressed or implied.

16650 Westgrove Dr | Suite 150
Addison, TX 75001
Phone: (972) 818-7001
Fax (972) 818-7003
www.ooaccess.com

Open Options Software License Agreement

THE ENCLOSED SOFTWARE PACKAGE IS LICENSED BY OPEN OPTIONS, LLC. TO CUSTOMERS FOR THEIR NON-EXCLUSIVE USE ON A COMPUTER SYSTEM PER THE TERMS SET FORTH BELOW.

DEFINITIONS: Open Options shall mean Open Options, LLC, which has the legal right to license the computer application known as DNA Fusion herein known as the Software. Documentation shall mean all printed material included with the Software. Licensee shall mean the end user of this Open Options Software. This Software Package consists of copyrighted computer software and copyrighted user reference manual(s).

LICENSE: Open Options, LLC, grants the licensee a limited, non-exclusive license (i) to load a copy of the Software into the memory of a single (one) computer as necessary to use the Program, and (ii) to make one (1) backup or archival copy of the Software for use with the same computer. The archival copy and original copy of the Software are subject to the restrictions in this Agreement and both must be destroyed or returned to Open Options if your continued possession or use of the original copy ceases or this Agreement is terminated.

RESTRICTIONS: Licensee may not sub license, rent, lease, sell, pledge or otherwise transfer or distribute the original copy or archival copy of the Software or the Documentation. Licensee agrees not to translate, modify, disassemble, decompile, reverse engineer, or create derivative works based on the Software or any portion thereof. Licensee also may not copy the Documentation. The license automatically terminates without notice if Licensee breaches any provision of this Agreement.

TRANSFER RIGHTS: Reseller agrees to provide this license and warranty agreement to the end user customer. By installation of the software, the end user customer and reseller agree to be bound by the license agreement and warranty.

LIMITED WARRANTY: Open Options warrants that it has the sole right to license the Software to Licensee. Upon registration by the Licensee, Open Options further warrants that the media on which the Software is furnished will be free from defects in materials and workmanship under normal use for a period of twelve (12) months following the delivery of the Software to the Licensee. Open Options' entire liability and your exclusive remedy shall be the replacement of the Software if the media on which the Software is furnished proves to be defective. EXCEPT AS PROVIDED IN THIS SECTION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN PARTICULAR, EXCEPT AS PROVIDED IN THIS SECTION, WITH RESPECT TO ANY PARTICULAR APPLICATION, USE OR PURPOSE, LICENSOR DOES NOT WARRANT THAT THE PRODUCTS WILL MEET THE LICENSEE'S REQUIREMENTS, THAT THE PRODUCTS WILL OPERATE IN THE COMBINATIONS OF 3RD PARTY SOFTWARE WHICH THE LICENSEE MAY SELECT TO USE, OR THAT THE OPERATION OF THE PRODUCTS WILL BE UNITERRUPTED OR ERROR FREE. NEITHER OPEN OPTIONS, NOR ITS VENDORS SHALL BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS, NOR FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND WHETHER UNDER THIS AGREEMENT OR OTHERWISE. IN NO CASE SHALL OPEN OPTIONS' LIABILITY EXCEED THE PURCHASE PRICE OF THE SOFTWARE.
The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

TERMINATION: Open Options may terminate this license at any time if licensee is in breach of any of its terms or conditions. Upon termination, licensee will immediately destroy the Software or return all copies of the Software to Open Options, along with any copies licensee has made.

APPLICABLE LAWS: This Agreement is governed by the laws of the State of Texas, including patent and copyright laws. This Agreement will govern any upgrades, if any, to the program that the licensee receives and contains the entire understanding between the parties and supersedes any proposal or prior agreement regarding the subject matter hereof.

Engage Wi-Fi Lock: Quick Start Guide

This Quick Start Guide explains how to configure an Engage Wi-Fi Lock (NDE or LE) in the ENGAGE mobile app and in DNA Fusion. Before adding an Engage Wi-Fi Lock, an Engage Site needs to be configured in DNA Fusion. A site requires the system the be licensed for Engage IP doors and a "parent account" to be issued. For more information on setting up a parent account, contact Open Options Technical Support.

Installation

Engage Wi-Fi Locks are added through the Allegion ENGAGE™ app. The ENGAGE mobile app is a free mobile application that can be found on the App Store (iOS) or the Google Play Store (Android). The app is required to configure any Engage Wi-Fi Lock. Before installing the Wi-Fi lock, ensure that an Engage Site is configured to DNA Fusion.
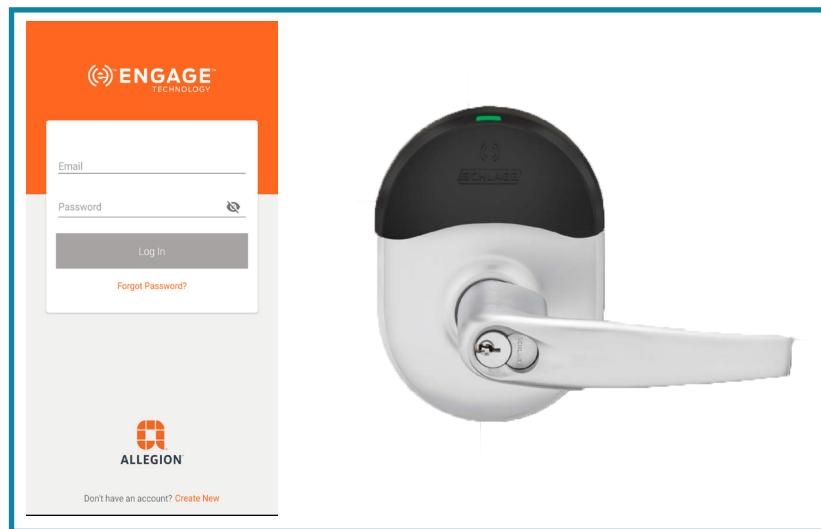
Step 1: *Adding Wi-Fi Locks to the ENGAGE App* - Add the Engage Wi-Fi lock in the ENGAGE mobile app. Once the lock is added to the app, configure the lock to the Wi-Fi network and connect the lock with the host machine. Manually connect to the Engage Driver by accessing the settings of the lock and select Update From Server (Page 3).

Step 2: *Adding Wi-Fi Locks to DNA Fusion* - Add the Wi-Fi lock to DNA Fusion by right-clicking the Engage Site and selecting Resync Hardware. This action will automatically add the Wi-Fi lock to DNA Fusion (Page 7).

Additional Information - The user can update the Wi-Fi configuration of the lock in DNA Fusion. Firmware updates can be implemented with a set date and time through the Engage Door Properties dialog (Page 9).

Troubleshooting - Engage Wi-Fi Lock Troubleshooting - This section explains how to troubleshoot common issues encountered during setup (Page 11).

This Page Intentionally Left Blank

Adding Wi-Fi Locks to the ENGAGE App

Once the site is created, sign in to the ENGAGE mobile app and follow the steps below to add the desired Wi-Fi locks. Ensure that the mobile device is connected to the Wi-Fi network.

> **NOTE**: *Before configuring the lock, ensure that the lock is not configured for a different site. Factory Reset the Lock before adding the lock to the desired site.*
>
> 1. **Open** *the interior door panel.*
>
> 2. **Press** *and* **hold** *the reset button.*
>   *Door LED will flash green twice.*
>
> 3. *Immediately,* **turn** *the door lever 3 times. A beep will sound after each turn of the lever.*

1. Once signed in, **select** the ⊕ icon to add a new lock.
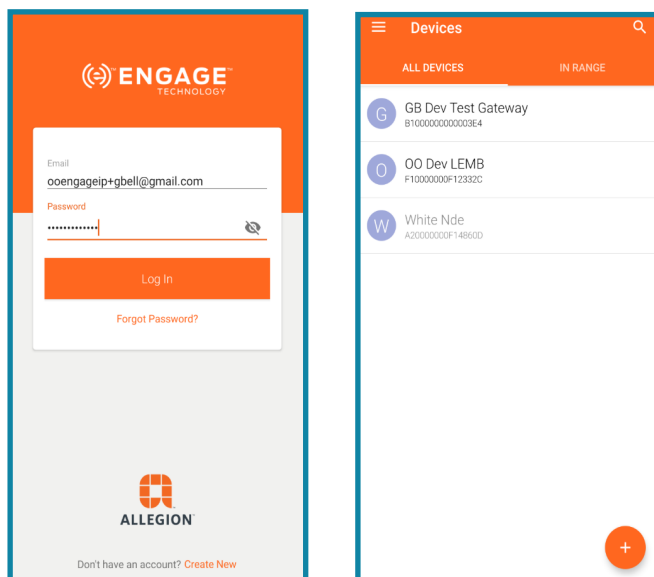
2. **Select** lock type (NDE or LE).

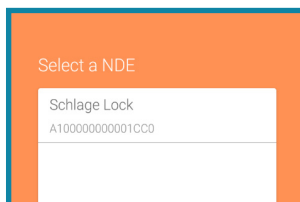   This example uses a NDE lock.
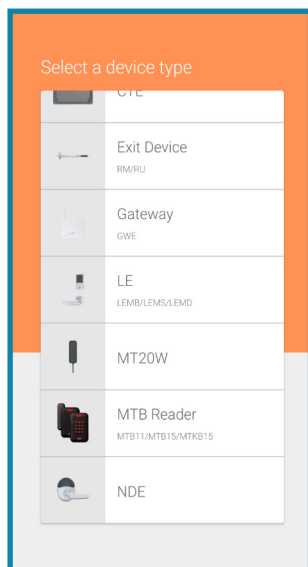
3. **Turn** and **Release** the interior lever.

    This action will "wake up" the lock.
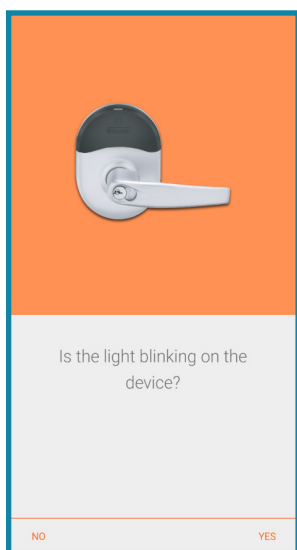

4. **Click** Next.

    A list of available devices that are nearby are shown, along with their serial numbers. If the desired device is not shown, repeat step 3.

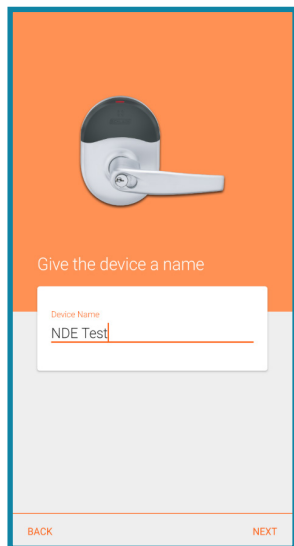5. **Add** the desired lock to the site.

6. **Ensure** that the desired lock is blinking.

    The desired lock will blink if the connection is successful. The ENGAGE mobile app will instruct the user to check the lock.

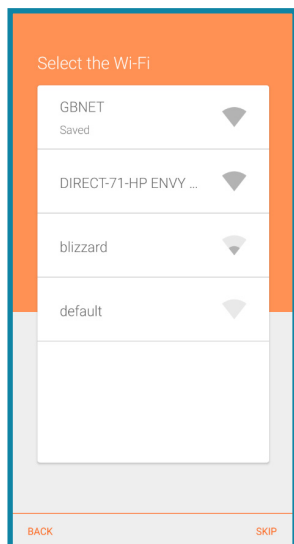7. **Add** a name to the Engage Wi-Fi lock.

   The ENGAGE mobile app will instruct the user to name the device.

8. After the device is named, **click** Next.

9. **Select** the desired Wi-Fi network.

   The lock network settings page opens.

10. In the lock network settings page, **establish** communication with the Engage Driver.

    The Engage Driver will never automatically connect to the lock, the Wi-Fi lock needs to establish the connection.
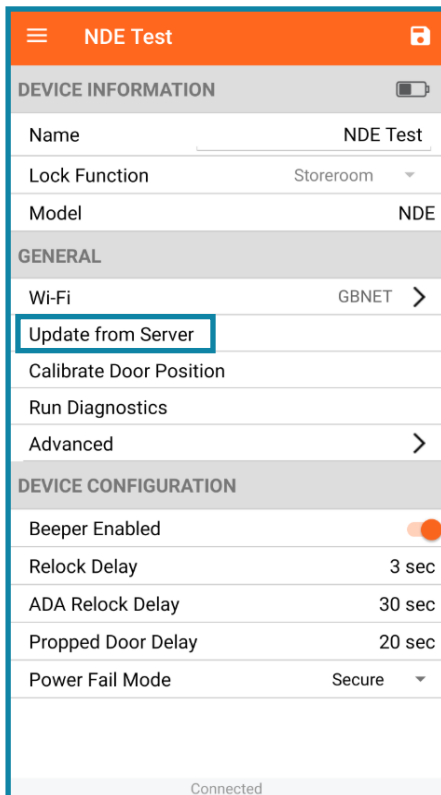
    □ If IP is selected, **enter** the IP address of the host machine (where the Engage Driver is installed).

       Open Options highly recommends that IP is selected and that Secured is selected.

    □ If DNS is selected, **enter** the host machine's DNS name.
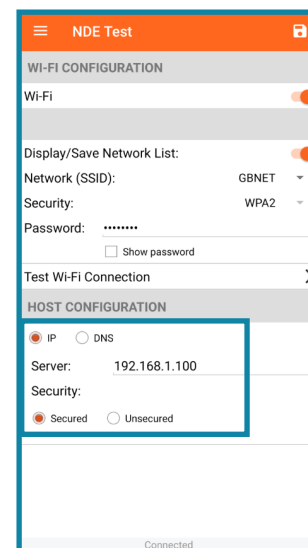
11. To manually force a connection with the Engage Driver, **connect** to the lock via the ENGAGE mobile app.

12. **Click** Settings.

13. **Select** Update From Server.

    This process can take a minute or so and you'll see various status messages.

    - Connecting to server...

    - Update from Server Initiated...

    - Sync Successful...

☰ NDE Test	🗎
DEVICE INFORMATION	🔋
Name	NDE Test
Lock Function	Storeroom ▾
Model	NDE
GENERAL	
Wi-Fi	GBNET ❯
Update from Server	
Calibrate Door Position	
Run Diagnostics	
Advanced	❯
DEVICE CONFIGURATION	
Beeper Enabled	⬤
Relock Delay	3 sec
ADA Relock Delay	30 sec
Propped Door Delay	20 sec
Power Fail Mode	Secure ▾
Connected	

NOTE: *Ensure that the correct firewall settings are in place to allow the following ports to be opened: 80, 443, 8080, 8081. Additionally, this application currently cannot share these ports with IIS or any other application. From an Admin command prompt, run the command below to see if any of the ports listed are taken.*

**Command**: `netsh interface ipv4 show excludedportrange protocol=tcp`

Adding Wi-Fi Locks to DNA Fusion

Once the Wi-Fi lock is set up in the ENGAGE mobile app, the Engage Driver can synchronize with the app to add the newly commissioned lock to the DNA Fusion database. Follow the steps below to add the Wi-Fi locks to the Engage Site in DNA Fusion.
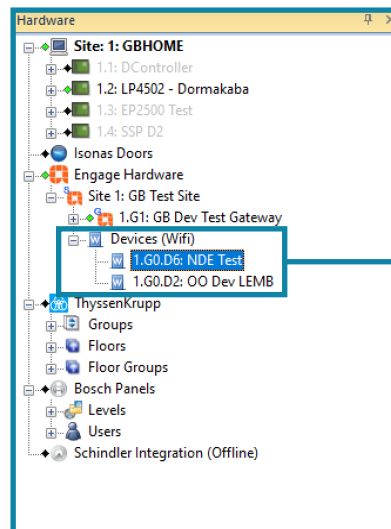
1. **Right-click** on the Engage Site in DNA Fusion.

2. **Select** Resync Hardware.

   The resync process may take 30-60 seconds. If the Engage Site node is expanded, collapsing the node may decrease the resync time.

If the NDE has not connected to the Wi-Fi network, the NDE will be listed under the Devices (Unlinked) tree.
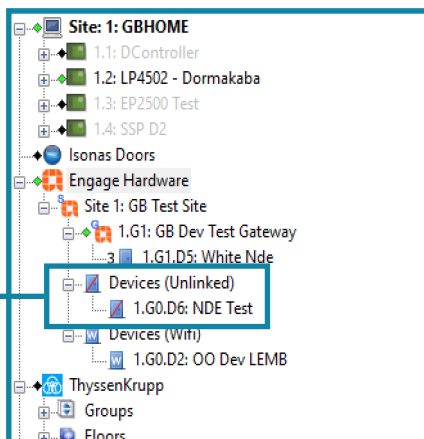
Once linked, the NDE (or LE) will be listed under Devices (WiFI)

Once the lock has connected and is configured as a Wi-Fi lock, the lock can be added to access levels. The Wi-Fi lock sends configuration and cardholder data to the Engage Driver once a day by default. The user can control the frequency via the Wifi Callback Frequency (1-30) in the Engage Door Properties.

To open the Engage Door Properties:

1. **Right-click** on the desired Engage Wi-Fi Lock.

2. **Select** Properties.

   The Engage Door Properties dialog opens.
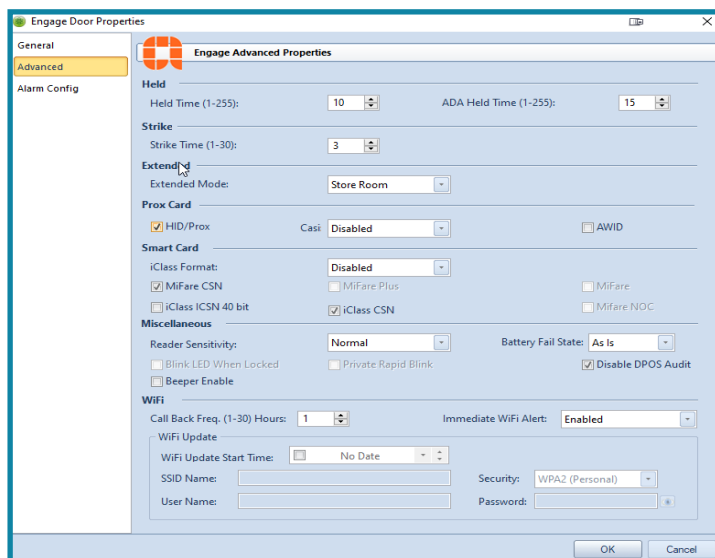
This Page Intentionally Left Blank

Additional Information

The Engage Wi-Fi lock has additional settings that may be helpful once the lock is configured.

Wi-Fi Update

There are situations where the Wi-FI connection information needs to be changed due to infrastructure changes or by policy. This can always be changed by connecting to each Wi-Fi lock with the ENGAGE mobile application and changing the locks parameters. For systems with a large number of Wi-Fi locks, the process of changing the parameters for each lock can be cumbersome. This issue can be alleviated in the Engage Door Properties.
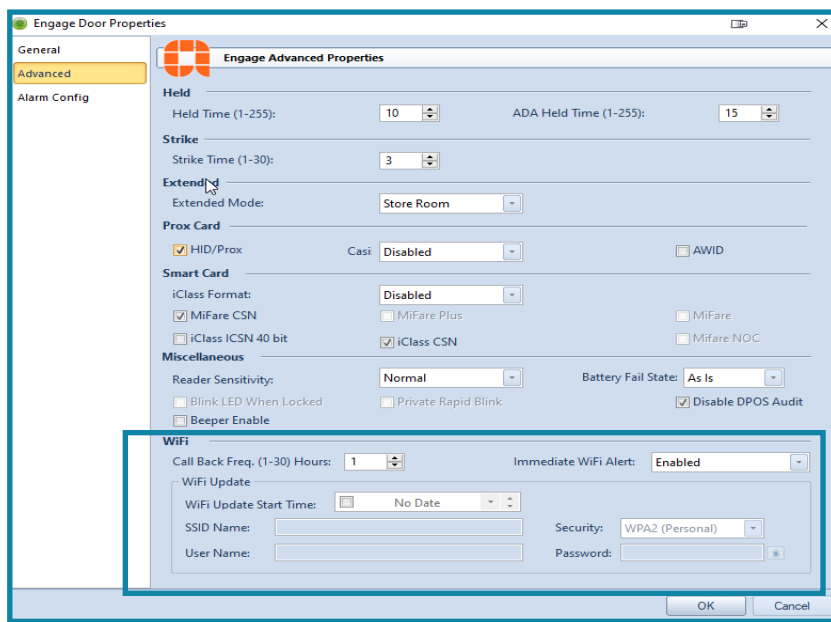

In the Engage Door Properties, the WiFi Update section is used to change the Wi-Fi settings of the Engage Wi-Fi Locks and set a start time for the update. This prevents having to connect to each lock individually through the ENGAGE mobile app.

> **NOTE**: *In a scenario where the password for the Wi-Fi network changes often, the Wi-Fi settings can be adjusted in the WiFi Update section of the Engage Door Properties dialog. The start time of the WiFi update can be set by configuring the WiFi Update Start Time.*

Firmware Upgrades

Each version of the Engage Driver ships with the latest supported firmware files. To upgrade the firmware on Wi-Fi locks select one or more in the Hardware browser.

1. **Right-click** and **select** Firmware Upgrade.
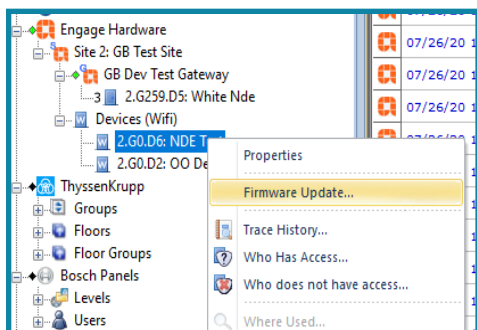
2. In the Firmware Update dialog, **adjust** the date and time to implement the firmware update.

3. **Select** Ok.

    For special cases that require the firmware to be rolled back to a previous version, beta firmware can be provide for the user to enter into the Firmware URL.
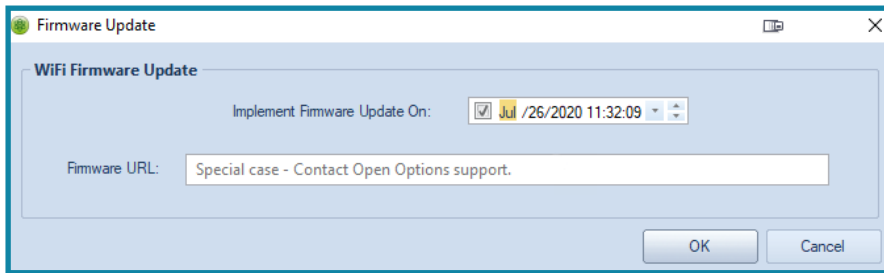
If you select different door types (i.e. NDE and LE) the option to use the URL is disabled because each lock type has their own firmware files.

Open Options Confidential
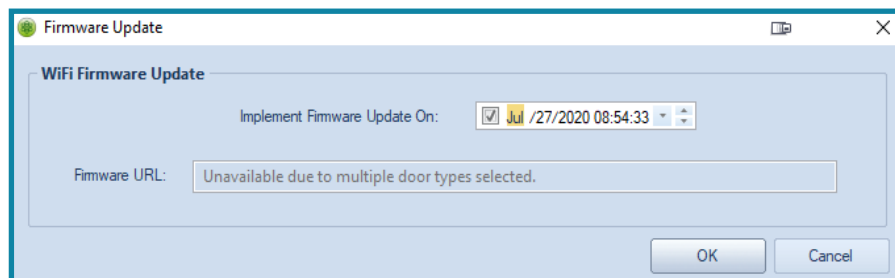
Engage Wi-Fi Lock Troubleshooting

The table below explains the errors that frequently appear and may create problems.

ENGAGE™ MOBILE APP ERROR SCENARIO	NEW MOBILE APPLICATION MESSAGE	POSSIBLE CORRECTIVE ACTION OR SUGGESTIONS
Successful Download	Success gets reported, not an error	No action needed.
Wi-Fi Database Download/Firmware Download **Note:** Database download trigger from MAPP always follows a audit upload: ● Wi-Fi chip not initialized by lock application. ● Wi-Fi Self test failed. ● Wi-Fi chip failing to power on. ● Wi-Fi busy when the download trigger was initiated by MAPP.	**Error** - The Wi-Fi failed to turn on. Please try again. If the problem persists, contact Technical Support at (877) 671-7011. (ref. code 01)	The Wi-Fi chip failed to turn ON. The Wi-Fi chip will not turn on if battery power is low. Check that the battery levels are above 4.6 volts DC. Try again. If the error repeats with new batteries, the product could have a defect.
	Error - The Wi-Fi failed to turn on. Please try again. If the problem persists, contact Technical Support at (877) 671-7011. (ref. code 02)	Wi-Fi self-test fails when Wi-Fi is set to OFF. Battery level could be below 4.6 volts. Check batteries and set Wi-Fi to ON.
	Error - The Wi-Fi failed to turn on. Please try again. If the problem persists, contact Technical Support at (877) 671-7011. (ref. code 03)	Wi-Fi radio on the NDE was already busy. Wait for the AMBLE LED to go out before trying again.
	Error - The Wi-Fi failed to turn on. Please try again. If the problem persists, contact Technical Support at (877) 671-7011. (ref. code 04)	The Wi-Fi chip will not turn onif the battery power is low. Check the battery level is well above 4.6 Vdc. Try again.
Wi-Fi Database Download/Firmware Download **Note**: Database download trigger from MAPP always follows a audit upload: ● Configuration failure. ● Trigger initiated without commissioning the lock. ● Downloading failed to trigger as the tamper is active.	**Error** - Failed to connect to access point. Confirm the Wi-Fi network SSID and Password and try again. (ref. code 06)	Wireless router name (SSID) might have a typo. Wi-Fi Password might have an error. Check security type, SSID and password for errors, and try again.
	Error - The Wi-Fi failed to turn on. Please try again. If the problem persists, contact Technical Support at (8877) 671-7011. (ref. code 45)	
	Error - Tamper detected. Install the battery cover and try again.	Lock Tamper issues, check the tightness of the battery cover to eliminate tamper indication. Check the small black switch is not broken.

Wi-Fi Database Download/Firmware Download **Note:** Database download trigger from MAPP always follows an audit upload: • Failures during connection to Wi-Fi Access Point or Host server.	**Error -** Failed to connect to access point. Cofirm the Wi-Fi network SSID and Password and try again. (ref. code 07)	Wireless Tamper issues, check the tightness of the battery cover to eliminate tamper indication. Check the small that the small switch is not broken.
	In OEM210 Mode: **Error -** Failed to connect to host server. Confirm Host Configuration settings and try again. An active internet connection may be required to reach the host server. (ref. code 10) **For Engage Managed Site:** **Error -** Failed to connect to host server. Confirm the Wi-Fi network is connected to the internet and try again. (ref. code 10)	The device connected with Wi-Fi to the wireless router (SSID), but failed to connect to the ENGAGE server (host) so the internet could be down (ISP problem), server could be down or if a partner account the WB address for the lock to connect with could have an error. (Use a laptop or smartphone entering the same SSID and PW for the wireless and browse to the server/host to confirm wireless and internet connectivity. the ENGAGE managed server can be found at api.allegionengage.com and portal.allegionengage.com both should results in a web page when using a laptop and browser.
	Error - DNS Failure. Failed to resolve host IP. Confirm Host Configuration settings and try again. (ref. code 11)	DNS error means the webpage request was not found by the network, DNS look up server. There could be a link typo error commissioned in the NDE, or a DNS server blocking, or firewall blocking. The ENGAGE managed server can be tested and found at api.allegionengage.com and portal.allegionengage.com. Both should result in a web page when using a laptop and browser over the identical Wi-Fi network the lock is trying to use.
	Error - The access point was not found. Confirm the Wi-Fi network SSID and signal availability and try again. (re. code 54)	The access point (AP) name entered for the lock to use as a wireless router was not found. Could be signal strength, typo in the SSID, or the wireless router is off. Use a loaptop or smart phone toconfirm the signal strength and connection to the SSID (wireless router).
	Error - Failed to connect to access point. Confirm the Wi-Fi network User Name and Password and try again. (ref. code 55)	Failed to connect to the access point (AP), for either weak signal or a ID and password error. Check the ID user name, and password for typos by entering it correctly. Use a laptop or smart phone to confirm the signal strengthand connection to the SSID.
	Error - TLS certificate validation failure. Please try again.	The OEM partner must have made an error loading the TLS certificates during commissioning, or this lock is going to the wrong host server address. Delete the lock form the site, FDR (Factory Default Reset) the lock and start over commissioning the Lock to the site.

Wi-Fi Database Download/Firmware Download (Cont.) **Note:** Database download trigger from MAPP always follows an audit upload: ● Failures during connection to Wi-Fi Access Point or Host server.	**Error -** Failed to connect to access point. Confirm the Wi-Fi network Password and try again. (ref. code 53)	Check security type setting in the lock Wi-FI set up and look for typos in the SSID name and password.
Failures During the Download	**Error -** Lost connection to host server during audit upload. Please try again. (ref. code 21)	An internet drop out or a server drop out. Try again.
	Error - Data handling failure. Please try again. (ref. code 22)	Data handling errors, the data was larger than expected. Cancel, disconnect, and wait for AMBER LED to switch off and try again.
	Error - Buffer failure during download. Please try again. (ref. code 23)	Internal buffer errors. Cancel, disconnect, and wait for AMBER LED to switch off. Check battery voltage and try again.
	Error - UART read failed. Please try again. (ref. code 24)	Internal error. Cancel, disconnect, wait for AMBER LED to switch off. Check battery voltage and try again.
	Error - UART read failed. Please try again. (ref. code 25)	Internal error. Cancel, disconnect, wait for AMBER LED to switch off. Check battery voltage and try again.
	Error - Flash write failed. Please try again. (ref. code 26)	Internal error. Cancel, disconnect, wait for AMBER LED to switch off. Check the battery voltage and try again.
	Error - Flash erase failed. Please try again. (ref. code 27)	Internal error. Cancel, disconnect, and wait for the AMBER LED to switch off. Check battery voltage and try again
	Error - CR check failure. Please try again. (ref. code 28)	Something disrupted the FW download. Could be RF signal noise, internet drop out, timeout, etc. Try again, if it continues switch to AP mode.
	Error - Audit framing error. Please try again. (ref. code 38)	Something disrupted the FW download. Could be RF signal, internet drop out, timeout, etc. Try again, if it continues switch to AP mode.
	Error - Failed to create HTTP header. Please try again. (ref. code 39)	Something disrupted the FW download. Could be RF signal, internet drop out, timeout, etc. Try again, if it continues switch to AP mode.
	Error - No response from host server on audit upload. Please try again. (ref. code 40)	Something disrupted the FW download. Could be RF signal, internet drop out, timeout, etc. Try again, if it continues switch to AP mode.

Failures During the Download (Cont.)	**Error -** No data to handle. HTTP content length is 0. Please try again. (ref. code 43)	Something disrupted the FW download. Could be RF signal, internet drop out, timeout, etc. Try again, if it continues switch to AP mode.
	Error - Failed to enter AP mode. Please try again. (ref. code 44)	Internal error. Cancel, disconnect, wait for AMBER LED to go out Check battery voltage and try again.
	Error - Missing site key. (ref. code 48)	Commissioning error the lock is going to the wrong partner host, delete the lock, FDR, e-commission and try again.
	Error - Invalid security certificate. (ref. code 49)	Commissioning error or the lock is going to the wrong partner host, delete the lock for the site, FDR the locks, re-commission, and try again
	Firmware Download Failure - Attempting to download again. (ref. code 50)	Something disrupted the FW download. Could be RF signal, internet drop out, timeout, etc. Try again, if it continues switch to SoftAP mode by turning Wi-Fi OFF, and try a SoftAP firmware download
Download Interruption or Download Timeout	**Error -** A FDR was Initiated during the download. (ref. code 33)	Allow lock to recover, stop blinking. FDR and re-commission. Reset Wi-Fi and repeat download attempt.
	Error - The host was disconnected during the download. Please try again. (ref. code 35)	An internet drop out or a server drop out. Try again.
	Error - The access point was disconnected during the download. Please try again. (ref. code 36)	Wireless signal was lost during download, try again or switch to SoftAP mode.
	Error - The download timed out. Please try again. (ref. code 37)	Download timed out, wireless router is slow or internet connecting is slow, and took to long. Try again or switch to SoftAP mode.
	Error - The download was interrupted. Please try again. (ref. code 41)	There was a download interruption, may have had an internet drop out or a server drop out, or an alert event at the lock. Try again.
	Error - Lost connection to host server during audit upload. Please try again. (ref. code 21)	May have had an internet drop out or a server drop out. Try again.
Wi-Fi Commissioning	**Error -** The Wi-Fi settings failed to save to the device. Please try again. (ref. code 14)	Failed to write SSID and Password to lock memory. Maybe the SSID or pw is too long and too many characters. Ask the customer how many characters they are trying to enter. They should limit to a maximum of 18 characters.

Wi-Fi Turn on SoftAP	**Error -** The Wi-Fi failed to turn on. Please try again. If the problem persists, contact Technical Support at (877) 671-7011. (ref. code 05)	Confirm you selected the correct SoftAP mode SSID in "Chose a Network" in settings. For SoftAP mode you must select the SSID that is the name of the NDE lock you are updating. Confirm you have good battery voltage. (Wi-Fi stops working at 4.6 volts)
	Error - The device access point timed out. Please try again. (ref. code 51)	In SoftAP mode your smart phone may have timed out, (Auto-Lock). Go to the mobile device settings and increase the time to ten minutes or more so SoftAP mode has time to complete.
	Error - The Wi-Fi failed to turn on. Please try again. If the problem persists, contact Technical Support at (877) 671-7011. (ref. code 01)	The Wi-Fi chip failed to turn ON. The Wi-Fi chip will not turn on if battery power is low. Check the battery level, must be well above 4.6 volts DC. Try again. If batteries are good and error repeats, product could have defect.
	Error - The Wi-Fi failed to turn on. Please try again. If the problem persists, contact Technical Support at (877) 671-7011. (ref. code 02)	Wi-Fi self-test fails when Wi-Fi it set to "OFF" battery could be low at 4.6 volts. Check batteries and set Wi-Fi to ON.
	Error - The Wi-Fi failed to turn on. Please try again. If the problem persists, contact Technical Support at (877) 671-7011. (ref. code 03)	Wi-Fi was already busy, and should have been already turned OFF on the NDE for SoftAP mode to start
	Error - The Wi-Fi failed to turn on. Please try again. If the problem persists, contact Technical Support at (877) 671-7011. (ref. code 04)	The Wi-Fi chip will not turn on if battery power is low. Check the battery level, must be well above 4.6 volts DC. Try again.
HTTP Error Received from Server ERROR 18	**IN OEM210 MODE:** An error from the server prevented connection. Confirm Host Configuration settings and try again. If the problem persists, contact your service provider. (ref. code 18) **FOR ENGAGE MANAGED SITE:** An error from the server prevented connection. Confirm the Wi-Fi network is connected to the internet and try again. (ref. code 18)	

OPEN OPTIONS®
ACCESS TECHNOLOGY