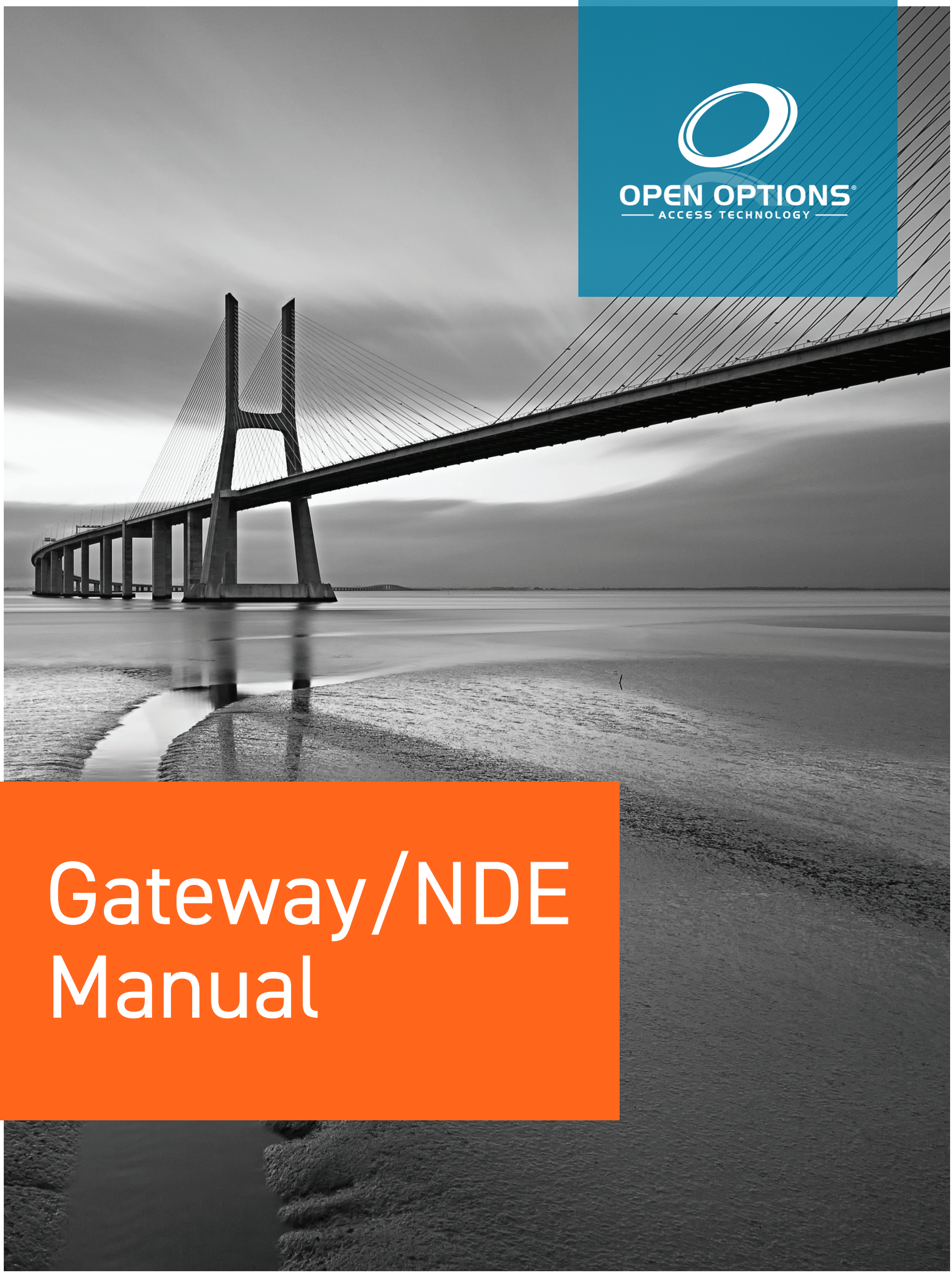


Gateway/NDE Manual

DNA Fusion™ is a trademark of Open Options, L.L.C.

The DNA Fusion™ Access Control and Security Management System uses equipment that generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this installation manual, 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 the user's expense.

The DNA Fusion™ Access Control and Security Management System 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.

The information contained within this manual is for informational purposes only and is subject to change at any time without notice.
Open Options, L.L.C. assumes no responsibility for incorrect or outdated information that may be contained in this publication.

This manual has been written for DNA Fusion™ version 6.0 or higher

Print Date: February 19, 2020
Manual Number: GNDE-I-1.1

Warranty

All Open Options products are warranted against defect in materials and workmanship for one year 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, L.P. Software License Agreement and Warranty

THE ENCLOSED SOFTWARE PACKAGE IS LICENSED BY Open Options, L.P. TO CUSTOMERS FOR THEIR NON-EXCLUSIVE USE ON A COMPUTER SYSTEM PER THE TERMS SET FORTH BELOW.

DEFINITIONS: Open Options shall mean Open Options, Inc., 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, L.P. 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 and acceptance of the software package, 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. 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 ninety (90) days 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. This warranty is void if the media defect has resulted from accident, abuse, or misapplication. Open Options does not warrant that the Software will meet the end user customer requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTIES ARE THE ONLY WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. 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.

Table of Contents

Chapter 4: NDE in DNA Fusion

Introduction 1

In This Chapter	
√	Section Organization
√	DNA Fusion / ENGAGE Overview
√	Supply List

This section is designed to introduce you to DNA Fusion™ and the NDE lock as well as the ENGAGE integration.

How This Section is Organized

This section contains information on the DNA installation and configuration of hardware:

Chapter 1, "Introduction," gives an overview of the integration.

Chapter 2, "RSI NDE Integration," provides information on configuring the RS-485 (RSI) gateway and NDE hardware through the DNA Fusion application.

Chapter 3, "IP NDE Integration," gives installation information on the IP NDE integration.

Chapter 4, "NDE in DNA Fusion," covers the various programming and features available in DNA Fusion.

Icons and Conventions Used in This Manual

This manual uses the following icons to help you find useful or important information easily:

	This icon highlights time-saving hints, helpful shortcuts, and advice that you'll find especially helpful.
	This icon marks information that is important enough for you to keep it filed in an easily accessible portion of your gray matter.
	If something you're doing could damage the system, end up costing big bucks, lock you out of the system, or otherwise bring an end to civilization as we know it, you'll find it highlighted with the icon.

In addition to these icons, this manual uses several other conventions that make the instructions easy to understand:

A Special Font: Text that look like this indicates a menu item, toolbar selection, button, or a message from the system.

Boldface: Boldface text, which usually appears in numbered steps, tells you about specific actions that you should take.

This Page Intentionally Left Blank

DNA Fusion/ENGAGE Overview

The Schlage® NDE Series wireless lock with ENGAGE™ technology is designed for ease of installation. The NDE locks seamlessly integrate with DNA Fusion to provide a cost effective and scalable access control solution. The NDE locks use Bluetooth Low Energy (BLE) and WiFi for communication.

DNA Fusion can integrate with the Allegion Gateway and NDE lock hardware in 2 manners: via the Gateway using the RS-485 port or direct using the native IP Gateway. It's important to remember the differences between running NDE locks under the Mercury integration using the RSI Gateway interface versus running without the Mercury controller via the IP Gateway. See page 1-5 for comparison information. The NDE lock and ENGAGE integrations are licensed features.

Beginning with DNA Fusion version 6.5.0, the Allegion NDE locks are supported via the Allegion Engage Gateway using the RS-485 port connected to a SSP-EP or DController. As of version 7.0.2.24, all Mercury intelligent controllers now support the ENGAGE IP integration as well as the RFI RS-485 integration. The integration also requires controller firmware of 1.25.6 or higher. Please note that not all DNA Fusion features are fully supported by the NDE lock integration. See page 1-5 for more information on supported features.

Mercury Gateway

Open Options connects to the NDE Series locks via the Mercury-powered NDE Gateway. The gateway connects via RS-485 to an Open Options DController, SSP-EP, SSP-LX, or SSP-D2 controller. A controller can support eight (8) gateways per port (sixteen (16) total for the SSP-EP and SSP-LX). Each gateway supports ten (10) NDE locks within a 30-foot radius.

When the hardware is configured using the Mercury controller, the lock behaves more like a reader and not a controller. All cardholders are stored on the Mercury panel and all the higher-level access control functionality is configured through the DNA Fusion system. See page 2-1 for more information.

Native IP Gateway

When integrating the NDE locks using the native IP Gateway, the lock serves as a controller and stores the cardholder database, time schedules, and other programming information. It makes all the access decisions locally and reports those events to DNA Fusion. It is essentially an offline lock, but with some amount of real-time event reporting along with control of downloads, credentials and time schedules. See page 3-1 for more details.

> *The ENGAGE™ Mobile application is utilized for initial commissioning of the gateway and NDE locks. An account is required to register the devices. Once registered, the lock will be linked to the account and will not be available for commissioning on a different account.*
>
> *When commissioning a lock, the device with the ENGAGE application should be within 10-15 feet of the door. Bluetooth communication is limited in range and the device should be as close as possible to the lock for robust Bluetooth communication.*

Configuration Steps

The following items/steps are required prior to configuring the ENGAGE integration.

1. An Apple or Android mobile device with Bluetooth.
2. **Download** and **install** the ENGAGE Mobile App on the mobile device.

Apple Android

3. For Mercury RS-485 integrations, **wire** the Allegion ENGAGE Gateway to the desired controller.
4. **Verify** DNA Fusion NDE or ENGAGE licensing in the DNA Fusion system (Help/About DNA).
5. **Confirm** DNA Fusion version 6.4 or 7.0.2.24 or higher (depends on the controller and integration type).
6. **Install** the NDE lock.
7. **Add** the Gateway to the ENGAGE app.
8. **Add** the NDE to the ENGAGE app.
9. **Add** the Gateway to DNA Fusion or **link** to the ENGAGE site (IP only).
10. **Create** and **link** the NDE door in DNA Fusion (RFI / RS-485 only).

NOTES:

ENGAGE Hardware Installation Overview

Open Options connects to the NDE Series locks via the Mercury-powered NDE Gateway. The gateway connects via RS-485 to an Open Options DController, SSP-EP, SSP-LX, or SSP-D2 controller. A controller can support eight (8) gateways per port (sixteen (16) total for the SSP-EP and SSP-LX). Each gateway supports ten (10) NDE locks within a 30-foot radius.

DNA Fusion can integrate with the Allegion Gateway and NDE lock hardware in 2 manners: via the RS-485 Gateway or by using the IP Gateway. There are a number of differences between running NDE locks under the Mercury integration using the RSI Gateway interface and configuring the system without the Mercury controller via the IP Gateway.

Mercury Gateway (RSI) Configuration

When the hardware is configured using the Mercury controller, the lock behaves more like a reader and not a controller. All cardholders are stored on the Mercury panel and all the higher-level access control functionality is configured through the DNA Fusion system. See page 2-5 for installation information.

Native IP Gateway Configuration

When integrating the NDE locks using the native IP Gateway, the lock serves as a controller and stores the card database, time schedules, and other programming information. It makes all the access decisions locally and reports those events to DNA Fusion. See Chapter 3 for IP Gateway installation information.

Below is a chart that provides a comparison of the two (2) integrations.

Feature	NDE Mercury IP Gateway (RSI Integration)	Native NDE IP Gateway
Cardholders	Limited by the Controller	5000
Download Speeds (To Lock)	20,000 cardholders in 22 seconds	BLE - 15 to 20 minutes to download a fully loaded lock
Download Issues	None	Single download
Triggers and Macros	Yes	No
Auto Unlock	Yes	Yes
First Person Unlock	Yes	Yes
Anti Passback	Yes	No
Time Schedules	255	16
Time Schedule Intervals	16 per Time Schedule	1 per Time Schedule
Max Offline Events	Limited by the Controller	2000
Holidays	255	32
Vacation	Yes	No
Lockdown	Yes	Yes
ADA	Yes	Yes
Access Areas	Yes	No
Use Limit	Yes	No
Direct Commands	Yes	Yes
DNA Fusion Web and Mobile	Yes	No
Card Formats	16 at Controller Level	Card Level

This Page Intentionally Left Blank

RSI NDE Integration 2

In This Section
√ ENGAGE Account Creation √ RSI (RS-485) Gateway Installation and Configuration √ NDE Lock Configuration

The RSI NDE integration is supported by DNA Fusion version 6.5.0 or higher. The integration requires the proper licensing to be in place prior to the configuration of the lock in DNA Fusion. This chapter covers the installation and configuration of the gateway in RS-485 installation as well as NDE lock configuration.

The NDE locks use Bluetooth Low Energy (BLE) and WiFi for communication. DNA Fusion can integrate with the Allegion Gateway and lock hardware in 2 manners: via the Gateway (RSI) or direct using the IP Gateway.

There are numerous steps involved in configuring the gateway and NDE lock. These steps vary depending on the type of integration: RS-485 or IP Gateway. Both installations require the Allegion ENGAGE application however the app is used differently depending on the type of integration installation.

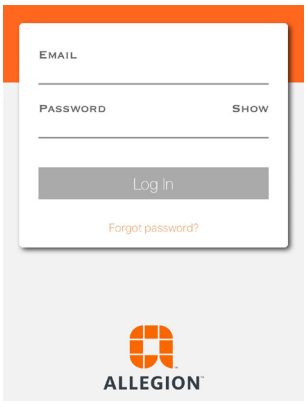
ENGAGE Account Log In

> ***!*** *The ENGAGE™ Mobile application is utilized for initial commissioning of the gateway and NDE lock. An Open Options account has been created on the ENGAGE site. Once commissioned, the hardware will not be available for configuration on a different account.*

1. **Download** the ENGAGE app to the mobile device.

   The ENGAGE mobile application is available for free download for both iOS and Android devices. Search the app store for "Allegion ENGAGE."

   This app is used to commission the gateways and locks in the Allegion portal. Gateways and NDE locks must be commissioned under the same account.



2. Once the app is installed, **log in** to the site using the credentials and password provided by Open Options.

   The account has been configured to use the Open Options 'ooengage' email plus the site number. For example, ooengage+DNA-001122@gmail.com. This combination is used to create a unique identifier for the account.

   If the OO Engage account has not been created, please contact the dealer or the Open Options sales manager.

3. **Continue** to NDE Mercury IP Gateway (RSI Integration) Configuration on page 2-3.

   For IP Gateway Configuration, see Chapter 3.

This Page Intentionally Left Blank

NDE Mercury IP Gateway (RSI Integration) Configuration

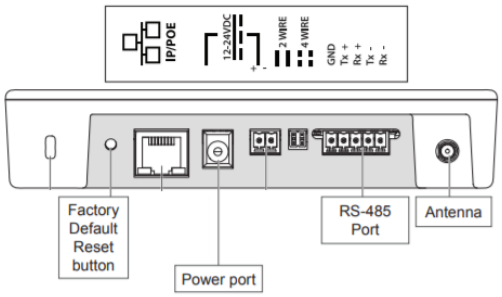
Open Options connects to the NDE Series locks via the Mercury-powered NDE Gateway. The gateway connects via RS-485 to an Open Options DController, SSP-EP, SSP-LX, or SSP-D2 controller. A controller can support eight (8) gateways per port - sixteen (16) total for the SSP-EP and SSP-LX. Each gateway supports ten (10) NDE locks within a 30-foot radius.

A controller's RS-485 port will not support both Mercury hardware and NDE gateways. The selected port can only be used to connect other IP gateways, AD-300 locks and PIM 400 subcontrollers.

Commissioning the NDE Gateway (RS-485)

1. **Wire** the NDE Gateway to the controller.

NDE Gateway	Mercury Controller	DController
TX-	TR+	TB2-4 (TR+)
RX+	TR-	TB2-5 (TR-)
GND	GND	GND



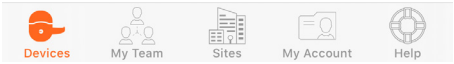
2. **Apply** power to the Gateway.

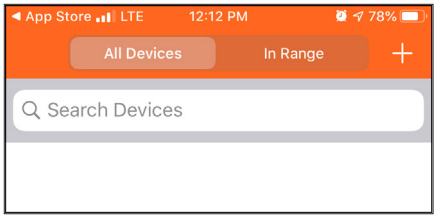
   The Gateway will complete a self test upon power up. During this process, the LED on the Gateway will appear solid amber. Once the light turns solid red, the Gateway is ready to be commissioned.

> *If the Gateway does not turn red, a Factory Default Reset may be performed. To factory reset the device, press and hold the Reset button. Hold the button until the LED flashes green twice and then remains solid. Release the Reset button to complete the process.*

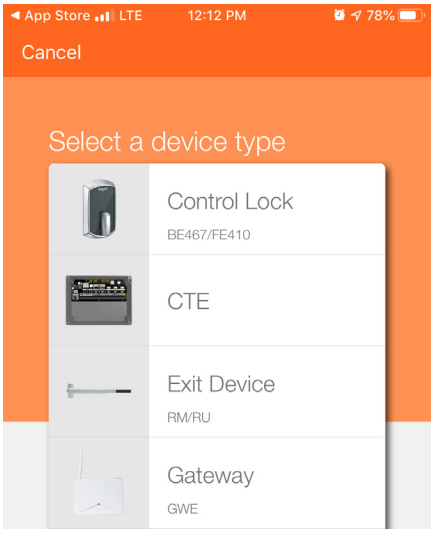
3. **Open** the ENGAGE app and log in with the credentials provided by Open Options.

4. From the Devices tab, **select** the + sign.





5. **Select** the Gateway (GWE) device type from the list.

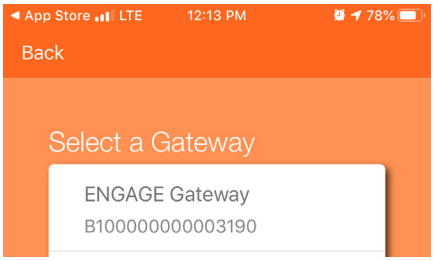


> *When commissioning a lock, the device with the ENGAGE application should be within 10-15 feet of the door. Bluetooth communication is limited in range and the device should be as close as possible to the lock for robust BLE communication.*

6. **Select** the ENGAGE Gateway from the list.

   The Gateway is placed in linking mode and the light will begin to blink. The Gateway can be identified by the serial number.

   A screen will appear inquiring about the light status.

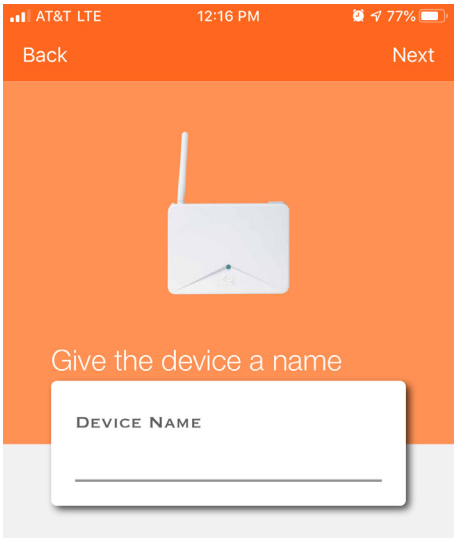


7. **Click** Yes to link the Gateway.

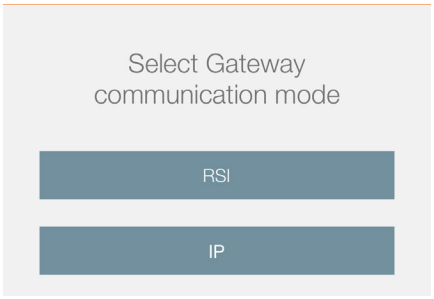
   The app will search for devices in range.

8. **Enter** a Name for the device and **click** the Next button.

   The communication mode screen will appear.



9. **Select** the RSI option.



   The RSI Configuration screen will appear.

10. **Set** the Physical Address.

    This must be a unique value. If the controller has an on-board subcontroller, address 0 will have been utilized. This value must match the subcontroller Physical Address setting in DNA Fusion.

11. **Enter** the Low and High Door Address values and **tap** Next.

    If additional Gateways will be installed, the door range must be unique to the controller. In the example, the Gateway will use address 0 for the low address value and 15 for the high address value. If another Gateway was installed, the low address value would start at 16. Door address values should never match across Gateways.

    The Preparing your device screen will be displayed.

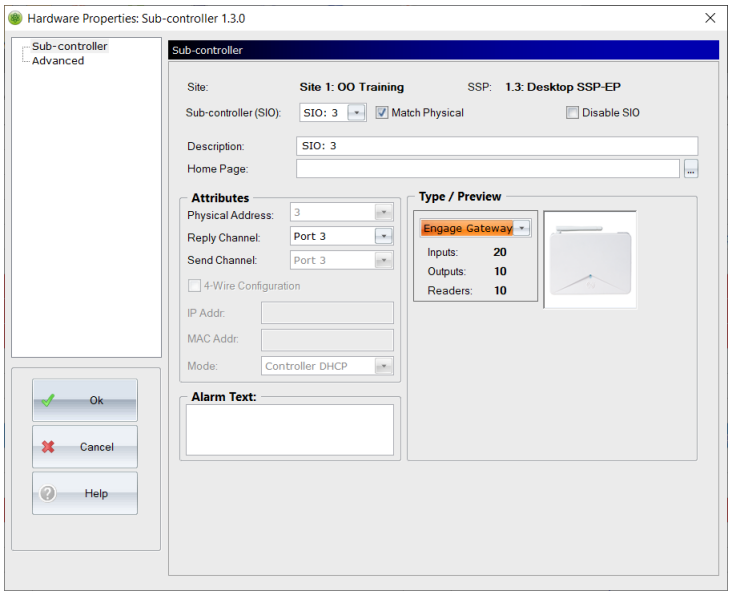
    Once commissioned, a large check will appear.

12. **Tap** the Finish option, close the app, and **proceed** to Adding the Gateway to DNA Fusion on page 2-5.

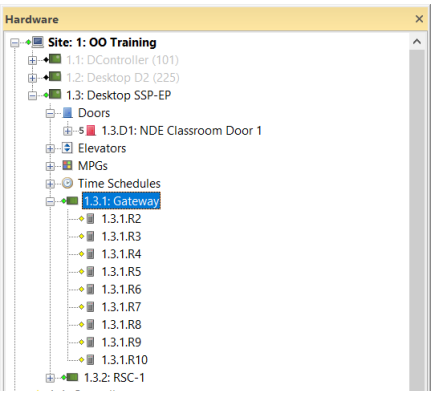
Adding the Gateway to DNA Fusion

Once the Gateway has been configured in the ENGAGE app, it can be added to DNA Fusion.

1. From the Hardware Browser, **right-click** on the desired controller and **select** Add / Subcontroller.
   The Properties Sub-controller dialog opens.



2. **Enter** a Description for the Gateway.
3. **Verify** the Physical Address.
   If needed, **uncheck** Match Physical and **select** the Physical Address from the drop down.
   This value must match the Physical Address set in step 10 on page 2-4.
4. If needed, **select** the Reply Channel to match the port.
5. **Select** the Engage Gateway from the Type/Preview drop down.
6. **Click** the Ok button to save settings.
   The Gateway will appear under the controller in the Hardware Browser. If wired and configured correctly, the subcontroller will come online and the diamond next to the subcontroller will turn green. If the diamond stays black, verify that the wiring and address settings are correct.



7. **Proceed** to Commissioning NDE Doors on page 2-7.

NOTES:

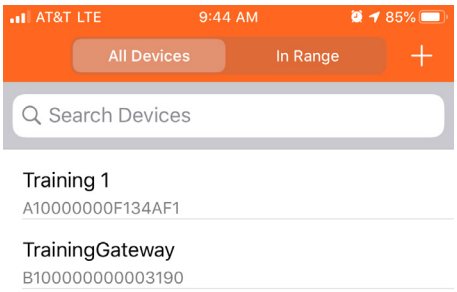
Commissioning NDE Doors

Once the NDE locks have been installed, they will need to be commissioned in the ENGAGE app prior to linking the locks in DNA Fusion. The NDE lock must be fully assembled with the battery connector plugged in and the battery cover in place. If the battery cover is not installed, the lock will NOT enter linking mode.

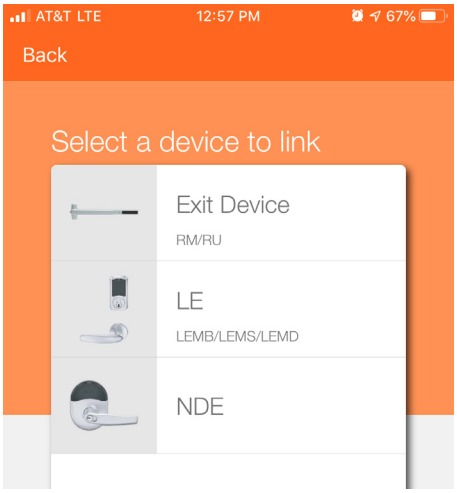
> *If the Lock has been in Standalone/Construction Mode, a Factory Default Reset will need to be performed. To factory reset the lock, remove the battery cover and hold the Reset button for 5 seconds. Release the Reset button. The LED will flash green twice and the lock will beep twice. Turn the interior door handle slowly three (3) times within 20 seconds to complete the process. The lock will beep once and the LED will turn red each time the handle is turned.*

The ENGAGE app is used to commission the NDE locks in the Allegion portal. It is critical that the gateway and NDE locks must be commissioned under the same account. Only one NDE lock can be linked at a time. If linking multiple locks, leave the battery cover off all uncommissioned locks.

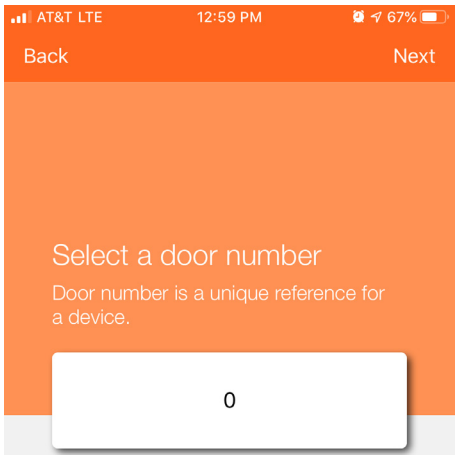
1. **Open** the ENGAGE app and log in.
2. From the Devices tab, **select** the + sign.
   Verify that the Gateway has been added to the ENGAGE app.



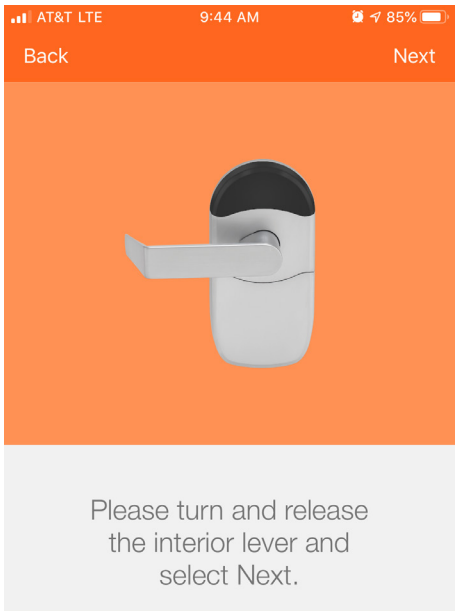
3. **Select** the NDE device type from the list.



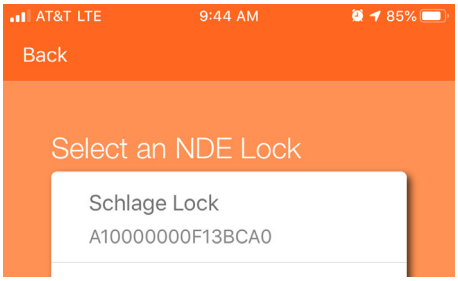
4. **Select** the unique Door Number and **tap** Next.



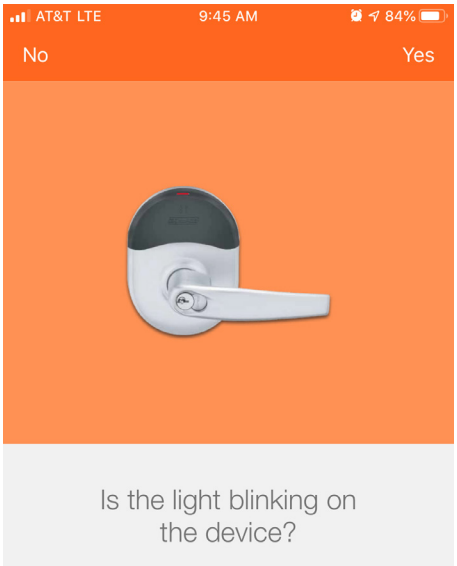
5. **Follow** the on-screen instructions and **tap** Next.
   Turn and release the Interior door handle.



The NDE lock will appear in the list. It can be identified by the serial number.

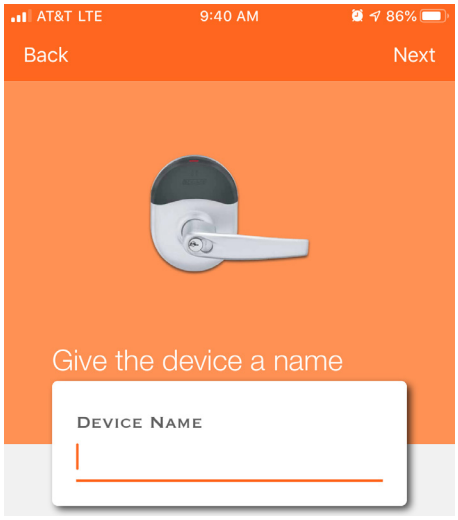


6. **Select** the NDE lock.
   A screen will appear inquiring about the reader LED's status. The light should start to blink.



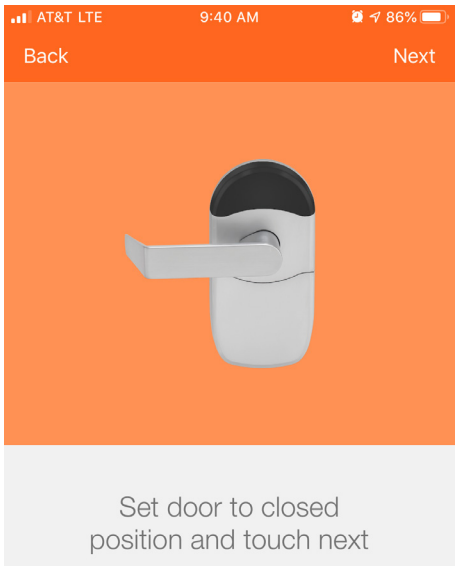
7. **Tap** Yes if the light is blinking.
   If the light is not blinking, repeat steps 5 and 6.
   The Device Name dialog will appear.

8. **Enter** a name for the NDE device and **tap** the Next option.

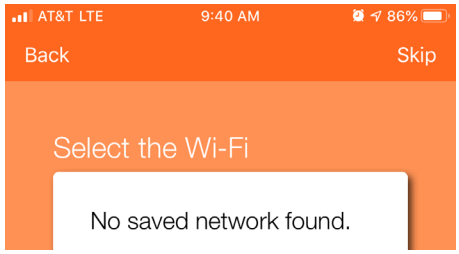


The door calibration screen will appear.

9. **Verify** that the door is closed or apply the door magnets and **touch** the Next option.

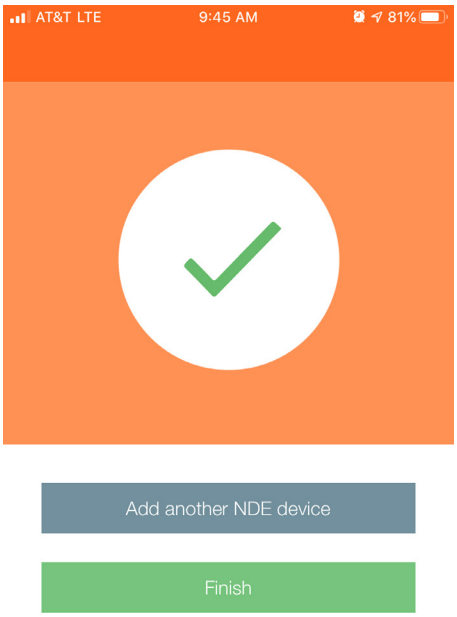


The Select Wi-Fi screen will open.



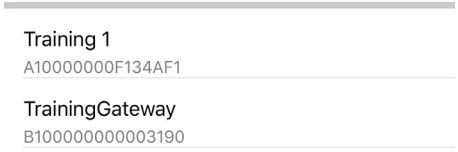
10. **Tap** the Skip option.

Once commissioned, a large check will appear.



11. **Tap** the Finish option.

The lock will appear in the Device List.



12. **Close** the app, and **proceed** to Linking NDE Devices in DNA Fusion on page 2-11.

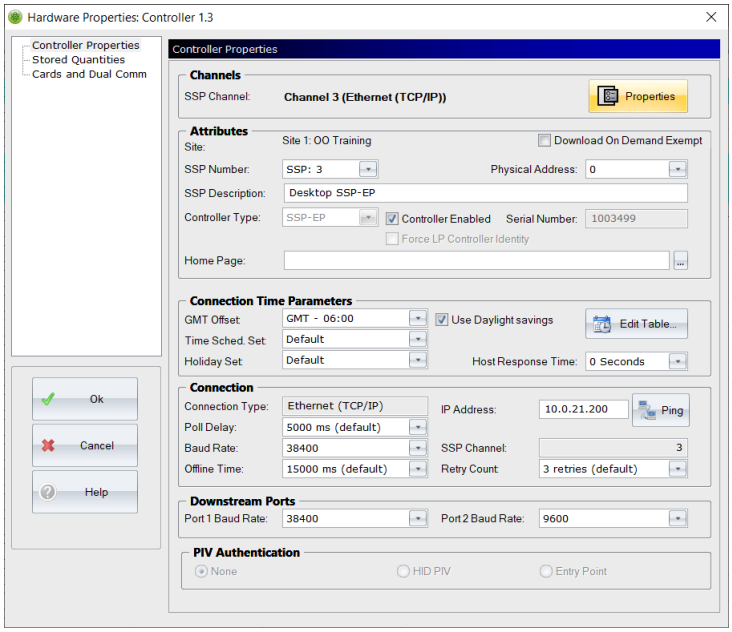
NOTES:

Linking NDE Devices in DNA Fusion

Once the Gateway and NDE locks have been commissioned in the ENGAGE app, they will need to be linked in DNA Fusion.

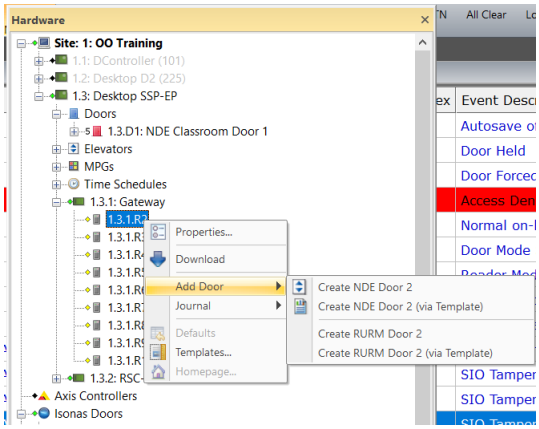
1. From the Hardware Browser, **right-click** on the Gateway's controller and **select** Properties.

   The Controller Properties dialog opens.



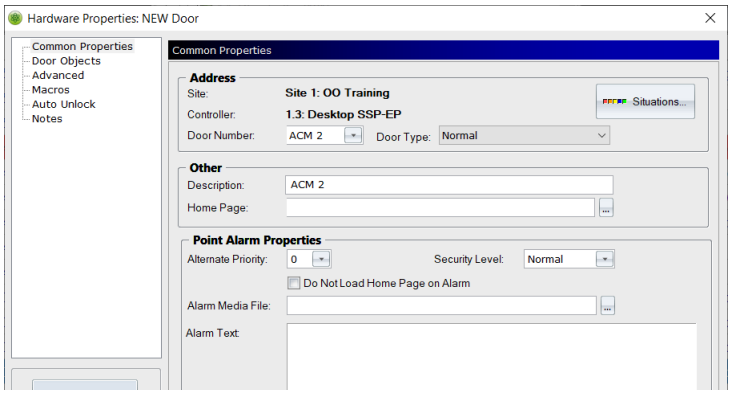
2. **Set** the Baud Rate on the Gateway's Downstream Port to 9600 and **click** the OK button.
3. From the Hardware Browser, **expand** the Gateway and **right-click** on the first reader.

   The doors must be added in numerical order.

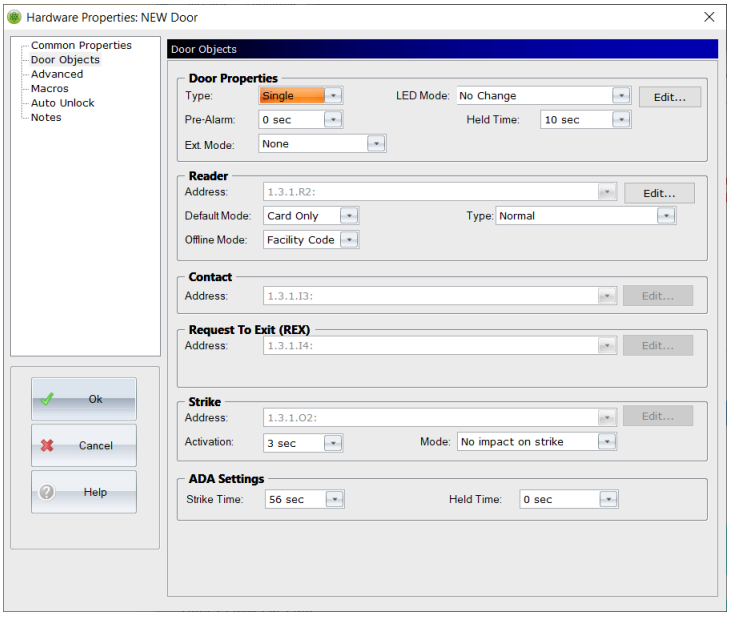


4. **Select** Add Door / Create NDE Door X.

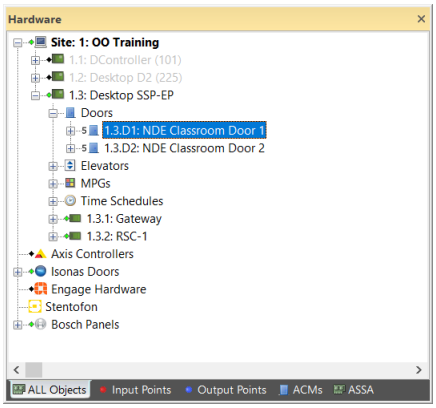
   The Door Properties dialog will appear.



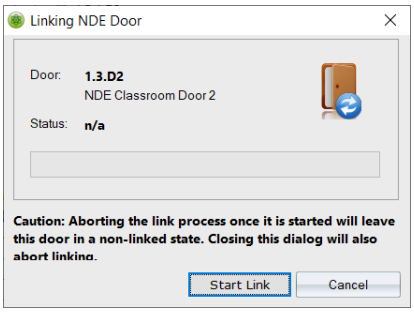
5. **Enter** a Description for the Door.
6. **Select** the Door Objects tab from the menu on the left.
   The door objects are preconfigured for the NDE lock.



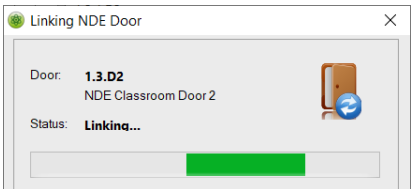
7. If needed, **change** the door properties and **click** the Ok button.
   The door will be added to the Hardware Browser and will appear under the Doors header.



8. **Right click** on the door and **select** Link Door to NDE.
   The Linking NDE Door dialog will open.

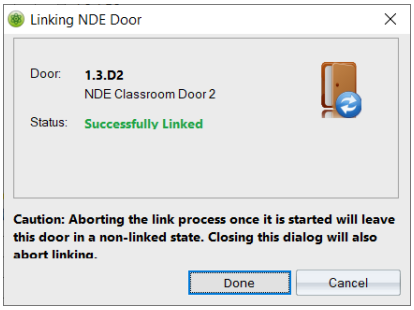


9. **Select** the Start Link option.
   The Linking process will begin.



10. **Place** the NDE door in Link mode.
    a. Hold down the Interior handle.
    b. **Present** a credential to the reader.
    c. **Continue** to hold down the handle until the LEDs start to flash red and green.
    d. **Release** the interior handle.

    Once linked, the door will beep 3 times and the LED will flash green. The dialog will display Successfully Linked.



11. **Click** the Done button.

    The door will appear with a green diamond next to the linked door.

    To verify the linking process, cycle the interior handle and check the DNA Fusion Event grid for a Door Opened event.

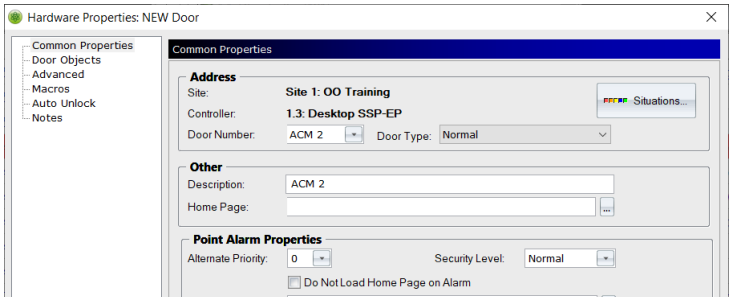
12. **Continue** to Chapter 4: NDE in DNA Fusion.

Configuring a Door to Follow a Time Schedule

The Unlock Schedule option provides a quick way to configure a door(s) to adhere to a specified unlock time schedule. The time schedule must be created prior to the setting up the unlock feature.

1. **Right-click** on the Door and **select** the Properties option.

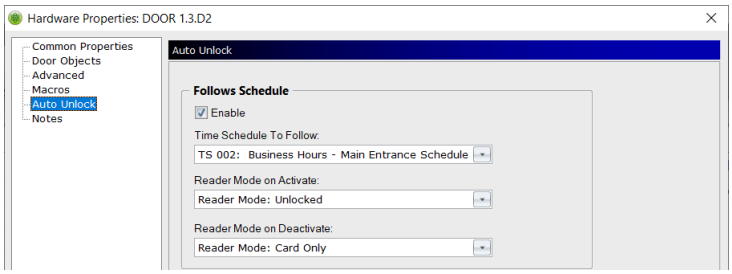
   The Door Properties dialog opens.



2. **Select** the Auto Unlock option from the menu on the left.

   The Auto Unlock dialog opens.

3. In the Follows Schedule section, **select** the Enable checkbox to activate the feature.



4. **Select** the desired time schedule from the Time Schedule to Follow drop-down list.
5. **Select** the Door Mode from the Reader Mode on Activate drop-down.
6. **Select** the Door Mode from the Reader Mode on Deactivate drop-down.
7. **Click** OK to save the changes.

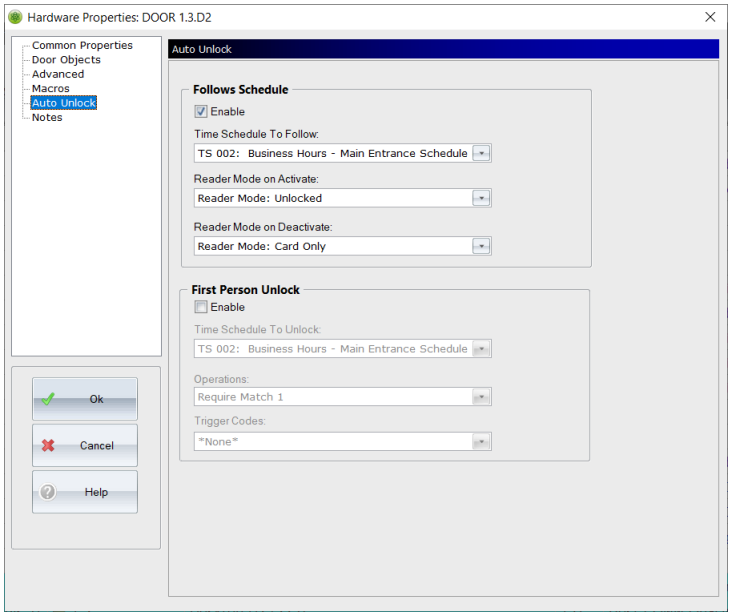
Configuring a Door to Use First Person Unlock

The First Person Unlock feature allows the operator to configure a door that will unlock during a specified time schedule after the first cardholder is granted access to the door. If enabled, the system will generate a trigger-and-macro combination and store it in the controller's memory.

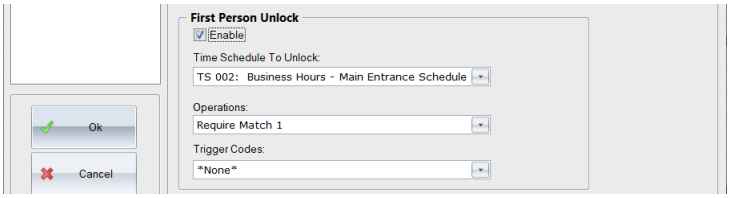
> *The door will remain in a secured mode even when the designated time schedule is active if no cardholders have accessed the door. Likewise, if a cardholder presents their card to the door when the time schedule is inactive, the door will remain secured.*

1. From the Door Properties dialog, **select** the Auto Unlock option from the dialog menu.

   The Auto Unlock dialog opens.



2. In the First Person Unlock section, **select** the Enable checkbox to activate the feature.



3. **Select** the desired time schedule from the Time Schedule to Unlock drop-down list.
4. **Select** an Operation from the drop-down list.

   See the DNA Fusion User Manual page 10-11 for more information.
5. **Select** a Trigger Code from the drop-down list.

   See page 10-11 in the User Manual for more information.
6. **Click** OK to save the changes.

Firmware Downloads

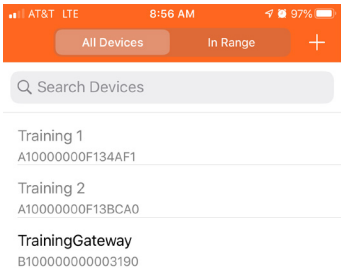
Once the Gateway and NDE lock(s) are online, the firmware should be updated. This process is performed in DNA Fusion and the ENGAGE app depending on the device being updated.

To update the Gateway Firmware:

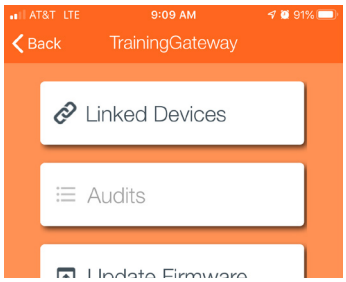
1. From the Hardware Browser, **right click** on the Gateway and **select** Reload Firmware.
   The firmware on the Gateway will be updated.

To update the NDE Lock Firmware:

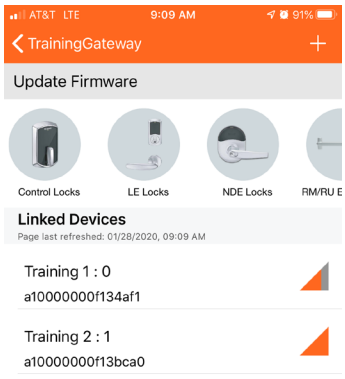
1. **Sign in** to the ENGAGE app on the mobile device.
   The All Devices screen opens.

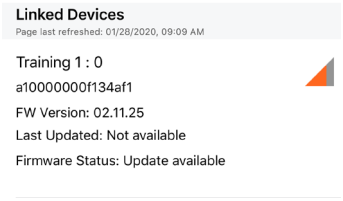


2. **Select** the Gateway from the list.
   The Gateway options will appear.



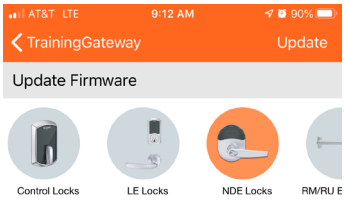
3. **Tap** the Linked Devices option.
   The Linked Devices dialog opens.

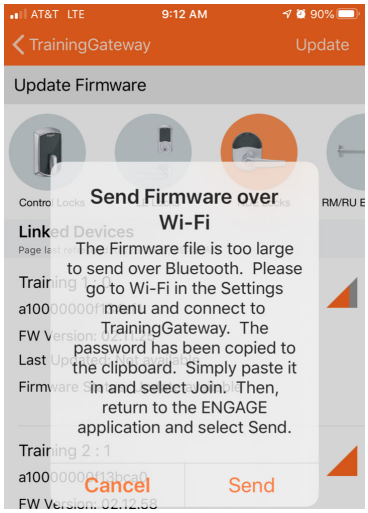


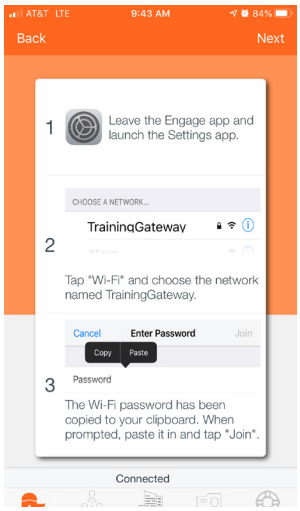


Tapping the device will display the current firmware version and update availability.

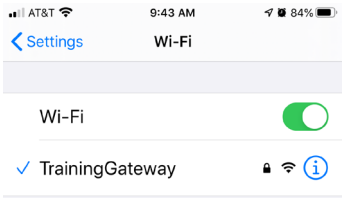
4. From the Update Firmware header, **tap** the NDE lock option and **tap** the Update option.
   The Send Firmware over WiFi dialog will appear.



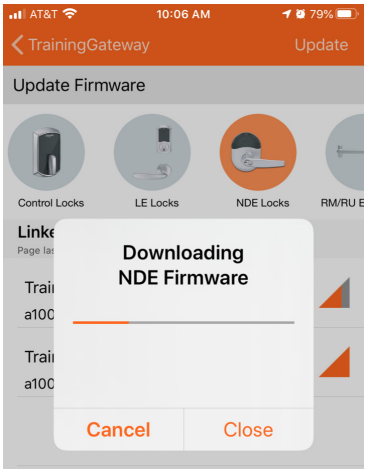


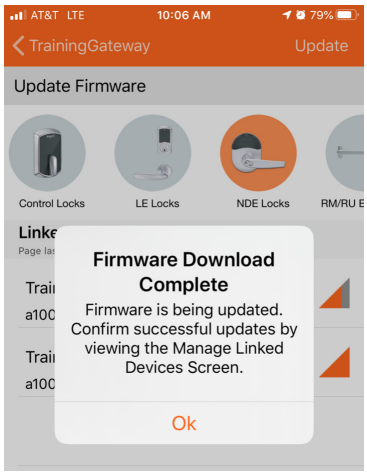


5. **Open** Settings for the mobile device with the ENGAGE app and **select** the WiFi option.
   The available Wi-Fi Networks will appear in the list.

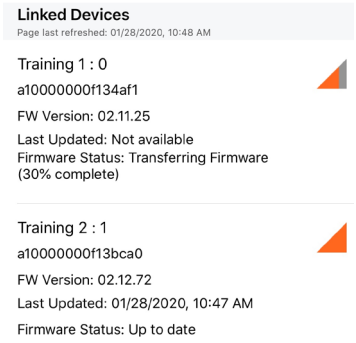


6. If not selected, **tap** the Gateway name in the list.
7. If prompted for a password, **paste** the copied information and **click** Join.
   A check will appear next to the Gateway network.
8. **Return** to the ENGAGE app and **select** the Send option.
   Or
   Select the NDE icon from the Update Firmware header.
   The Downloading NDE Firmware dialog will appear.





   Once if is complete, the Firmware Download Complete dialog will open.
9. **Click** the Ok button.
   Tap the Linked NDE device to view the update status.
   This process can take up to 45 minutes per NDE lock.
10. **Close** the ENGAGE app.
    The locks will continue to update and the Gateway will resume normal once all the firmware has been updated.



Functionality

The RSI Gateway Integration provides access the full range of Open Options features. See the User Manual for management information.

Time Schedules

When utilizing the RSI communication mode for the Gateway, the lock can be programmed with up to 255 time schedules. For more information on time and holiday schedules, see chapter 5 in the DNA Fusion User Manual.

Access Levels

The NDE locks can be configured as either part of a Legacy Access Level or a Global Access Level. See page 6-3 in the DNA Fusion User Manual.

Door Modes

The RSI integration provides access to standard door modes as well as scheduled commands. The Door Mode indicates the state of a door.

Below is an explanation of the various door modes. For more information see page 8-3 in the User Manual.

To change the door mode, **right click** on the Door and **select** the Control option. **Select** the desired Mode.

	Reader Mode: Disabled Icon - Disables the reader. The door and all associated hardware objects remain locked without REX capability.
	Reader Mode: Unlocked Icon - Unlocks the selected point and allows unlimited access. All cardholders will be granted access.
	Reader Mode: Locked Icon - Locks the selected door. Card access will not be allowed, but the door can be used from the inside using the REX button.
	Reader Mode: Facility Code Icon - Matches the facility code(s) stored in the SSP to approve entry. See page 8-81 for more information on facility codes.
	Reader Mode: Card Only Icon - Requires a card with the correct card format and access level to be presented.
	Reader Mode: PIN Icon - Requires a PIN code to be entered to gain access. PIN numbers are set in the Card Tab of the Cardholder's Record.
	Reader Mode: Card AND PIN Icon - Both a card AND a PIN code are required to gain access to the associated point.
	Reader Mode: Card OR PIN Icon - Either a card OR a PIN code is required to gain access to the associated point.
	Override Mode Icon - Opens the Temporary ACR Override dialog. See page 8-5 for more information.
	Cancel Override Mode Icon - Cancels the Temporary Override command. See page 8-6 for more information.

Direct Commands

The Gateway integration offers full functionality for configuring direct commands. Page 8-27 in the User Manual provides more details.

Triggers and Macros

The Gateway RSI integration allows for traditional triggers and macros as well as Host Based Macros. See chapter 10 in the User Manual for detailed information.

This Page Intentionally Left Blank

IP NDE Integration 3

In This Section
√ ENGAGE Account Creation √ IP Gateway Installation and Configuration √ NDE Lock Configuration

The IP NDE integration is supported by DNA Fusion version 7.6. or higher. The integration requires the proper licensing to be in place prior to the configuration of the ENGAGE site in DNA Fusion. This chapter covers the installation and configuration of the gateway as well lock configuration.

The NDE locks use Bluetooth Low Energy (BLE) and WiFi for communication. DNA Fusion can integrate with the Allegion Gateway and lock hardware in 2 manners: via the Gateway (RSI) or direct using the IP Gateway.

There are numerous steps involved in configuring the Gateway and NDE lock. These steps vary depending on the type of integration. Both installations require the Allegion ENGAGE application however the Native IP configuration requires an account be created in the Allegion portal.

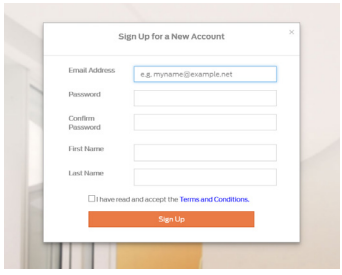
ENGAGE Account Creation and Mobile App

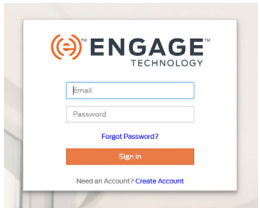
The Native IP Gateway setup requires the user to create an account on the ENGAGE portal as well as download the ENGAGE app on a mobile device.

ENGAGE Portal Account

1. **Visit** the ENGAGE Portal (https://portal.allegionengage.com) and **create** an account.

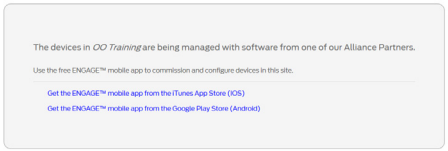
   A registration email containing a link will be sent to the registered email address.





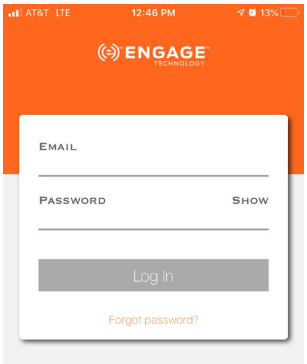
   If you already have an account, **enter** the user name and password.

   A window will open confirming the devices are being managed through DNA Fusion.



ENGAGE App Account

> *The ENGAGE™ Mobile application is utilized for initial commissioning of the gateway and NDE lock. An account has been created on the ENGAGE site. Once commissioned, the hardware will not be available for configuration on a different account.*



1. **Download** the ENGAGE app to the mobile device.

   The ENGAGE mobile application is available for free download for both iOS and Android devices. Search the app store for "Allegion ENGAGE."

   This app is used to commission the gateways and locks in the Allegion portal. Gateways and NDE locks must be commissioned under the same account.

2. Once the app is installed, **log in** to the app using the credentials and password created on page 3-1.

3. **Continue** to page 3-3 to install the integration files.

ENGAGE Integration Considerations

The ENGAGE IP Gateway integration provides a quick seamless lock solution. When integrating the NDE locks using the native IP gateway, the lock serves as a controller and stores the card database, time schedules, and other programming information. It makes all the access decisions locally and reports those events to DNA Fusion.

There are a few limitations when using the Native IP ENGAGE integration. For example, the NDE lock only accepts 16 time schedules and may require the use of Time Schedule Sets in DNA Fusion. There is also no way to store card formats in the NDE so the format must be selected in the Personnel Record on the Card tab. The ENGAGE integration is not currently supported in the web or mobile versions of DNA Fusion.

Feature	Native NDE IP Gateway
Cardholders	5000
Download Speeds (To Lock)	BLE - 15 to 20 minutes to download a fully loaded lock
Download Issues	Single download
Triggers and Macros	No
Auto Unlock	Yes
First Person Unlock	Yes
Anti Passback	No
Time Schedules	16
Time Schedule Intervals	1 per Time Schedule
Max Offline Events	2000
Holidays	32
Vacation	No
Lockdown	Yes
ADA	Yes
Access Areas	No
Use Limit	No
Direct Commands	Yes
DNA Fusion Web and Mobile	No
Card Formats	Card Level

Native IP Gateway Configuration

When integrating the NDE locks using the native IP gateway, the lock serves as a controller and stores the card database, time schedules, and other programming information. It makes all the access decisions locally and reports those events to DNA Fusion.

The following steps should be performed to complete the integration:

1. **Install** the ENGAGE Gateway and NDE locks.
2. **Create** an account on the Allegion Portal.
3. **Download** the ENGAGE app.
4. **Run** the DNA Fusion-ENGAGE Integration application.
5. **Create** the ENGAGE Site in DNA Fusion.
6. **Discover** the ENGAGE hardware in DNA Fusion.
7. **Configure** the access level and card format.

DNA-ENGAGE Integration Installation

Once the ENGAGE Gateway and NDE locks have been installed and configured, the DNA integration can be performed. The installation process is very straightforward and can be performed without any knowledge of the software.

1. **Obtain** the dnaFusion Engage Install application from Open Options Technical Support.

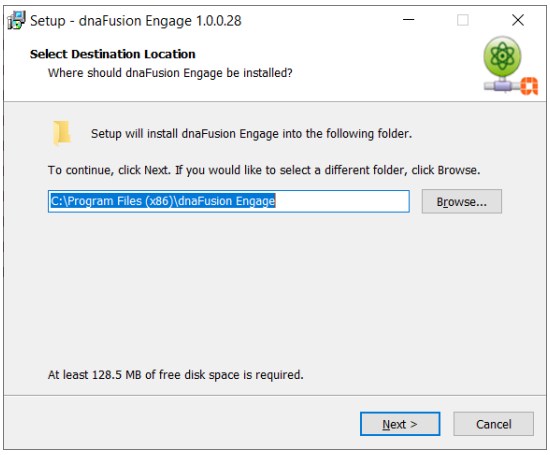
   > *The setup procedure must be performed with an administrator login.*

2. **Verify** the DNA Fusion DNADrvr32 Service Permissions.

   The DNA driver and the Engage driver need to run under the same identity. The account running the services will be used later in the installation process and should be noted for reference. For more information on DNA Fusion services, see page 2-7 in the DNA Fusion Technical Manual.

3. **Run** the dna Fusion Engage Installation.

   The Destination Location dialog appears.

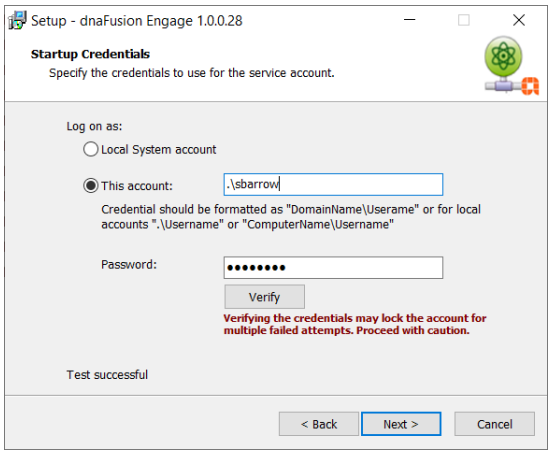


4. **Click** the Next button to continue the installation or **select** the Browse button and specify a different location.

   The default location is C:\Program Files (x86)\dnaFusion Engage.

   The Startup Credentials screen appears.

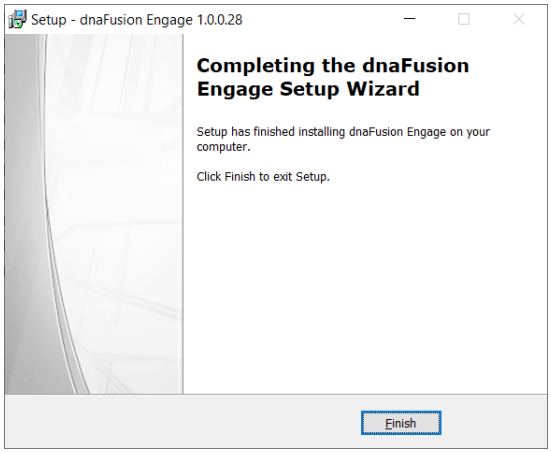
5. **Select** This Account, **enter** the credentials, and **click** Next.



   The Engage driver requires a service account to run the application; this account must be a local machine administrator in order to operate.

   The Ready to Install screen appears.

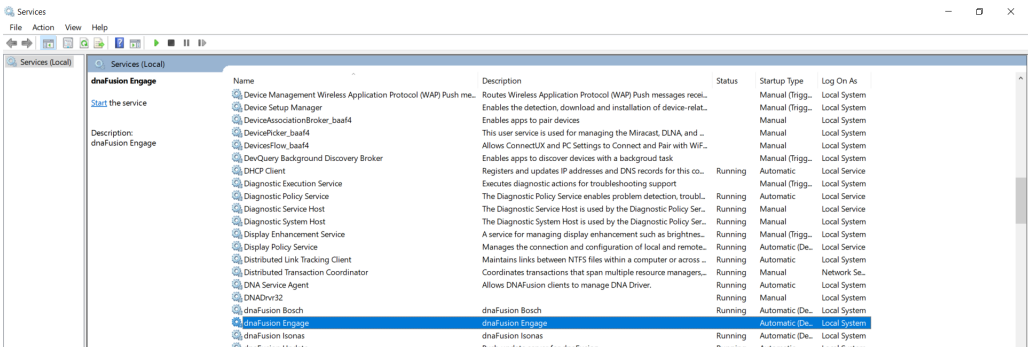
6. **Click** the Install button to start the process.
   When the installation is complete, the Install Complete screen opens.
7. **Click** the Finish button to complete the installation.



8. **Configure** the ENGAGE Site within the DNA Fusion application.
   See page 3-5 for information on configuring the ENGAGE Site.

DNA Fusion Engage Driver

The Engage driver runs as a service on the DNA Fusion server.



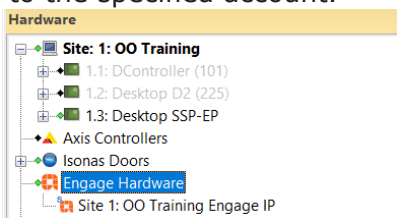
The Engage driver status is reflected by the color of the diamond in the DNA Fusion Hardware Browser. Below is a list of the various driver colors and states.

- Green - The driver is running and all systems are functional. All is right in the world.
- Black - The driver is not running.
  - Verify the DNADrvr32 and Engage services are running under the correct identity.
- Yellow - The driver is running but unable to open the connection used to communicate status to DNA.
  - The oo.Engage.status queue cannot be opened by the DNA Driver. Verify that the Engage Driver is configured to run under a local administrators' group account.
- Red - The driver is running but unable to open the connection used to relay events to DNA.
  - The oo.dnafusion.event queue cannot be opened by the DNA Driver.
- Purple - The driver is running but unable to open either the events or status connections to DNA.
  - Both the oo.Engage.staus or oo.dnafusion.event queues cannot be opened by the DNA Driver.

ENGAGE Site Setup

The ENGAGE IP configuration will require the name and password created in the Allegion portal on page 3-1.

Once the site is created in DNA Fusion, the associated hardware will be linked to the specified account.



1. From the Hardware Browser, **right click** on the Engage Hardware header and **select** Add New Engage Account.

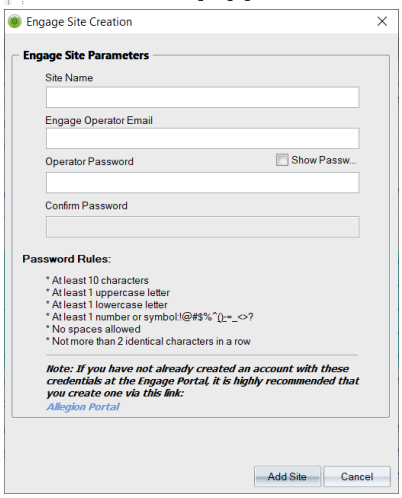
   The Engage Site Creation dialog opens.

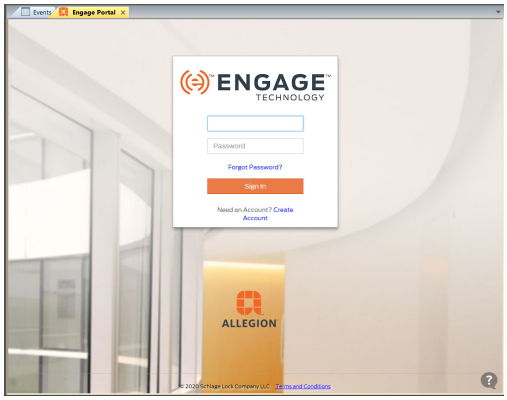
2. **Enter** the desired Site Name.

3. **Enter** the email account and password for the registered account on page 3-1 and **click** the Add Site button.

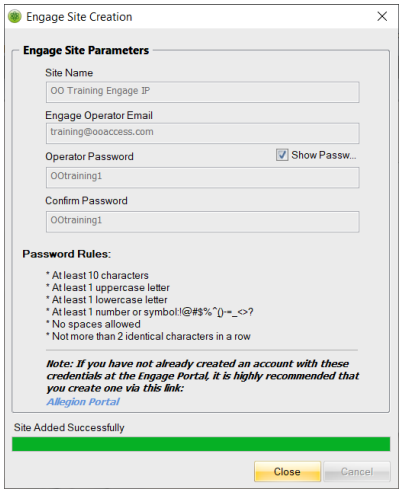
   If an account has not been created on the Allegion portal, **click** the Allegion Portal option and the registration page will open in the DNA Fusion HTML Viewer. **Select** the Create Account option and complete the registration.

   The system will start the process of adding the site.

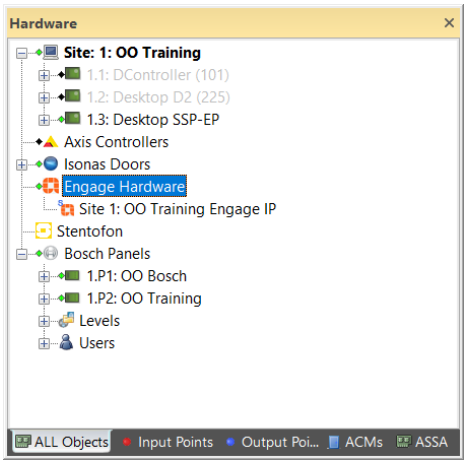




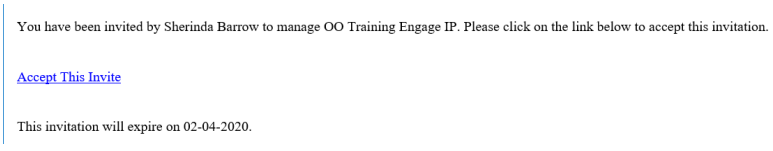
4. Once the site is successfully added to DNA Fusion, **click** the Close button.



The Site will appear in the Hardware Browser and an invitation email will be sent to the registered email.



5. **Open** the email and **select** the Accept This Invite link.



   An Engage web page opens.

6. **Scroll down** to the bottom of the page and **accept** the Terms and Conditions.

7. **Continue** to page 3-7 to commission the gateway and locks.

NOTES:

Commissioning the NDE IP Native Gateway

Open Options connects to the NDE Series locks via the ENGAGE NDE IP Gateway. The ENGAGE Gateway enables these devices to be connected in real-time with Open Options DNA Fusion. The ENGAGE gateway connects using the existing network architecture and can be powered over Ethernet or from the provided power supply. It supports up to ten (10) NDE locks within a 30-foot radius.

1. **Connect** the NDE Gateway to the network.

   If utilizing Power over Ethernet, skip to step 3.

2. **Apply** power to the Gateway: PoE or Wired Power Supply.

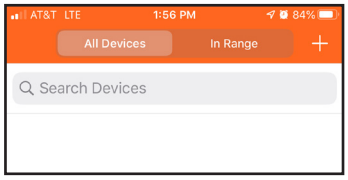
   The Gateway will complete a self test upon power up. During this process, the LED on the Gateway will appear solid amber. Once the light turns solid red, the Gateway is ready to be commissioned.

3. Once the Gateway LED is solid red, **open** the ENGAGE app.

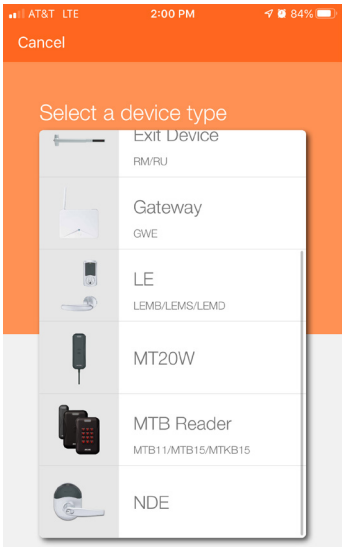
> *If the Gateway does not turn red, a Factory Default Reset may be performed. To factory reset the device, press and hold the Reset button. Hold the button until the LED flashes green twice and then remains solid. Release the Reset button to complete the process.*

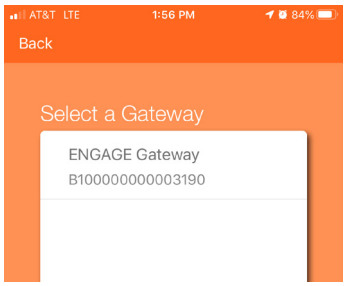
4. **Open** the ENGAGE app and log in.

5. From the Devices tab, **select** the + sign.



6. **Select** the Gateway (GWE) device type from the list.





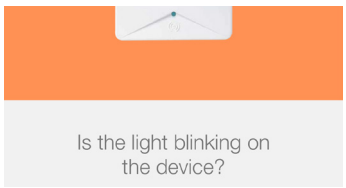
7. **Select** the ENGAGE Gateway from the list.

   The Gateway is placed in linking mode and the light will begin to blink. The Gateway can be identified by the serial number.

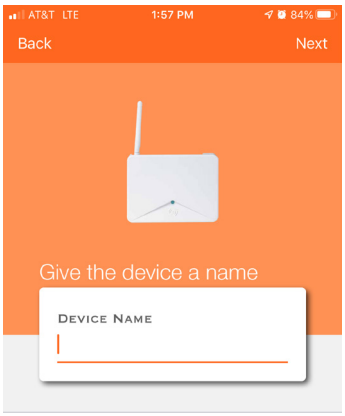
   A screen will appear inquiring about the light status.

8. **Click** Yes to link the Gateway.

   The app will search for devices in range.



9. **Enter** a Name for the device and **click** the Next button.



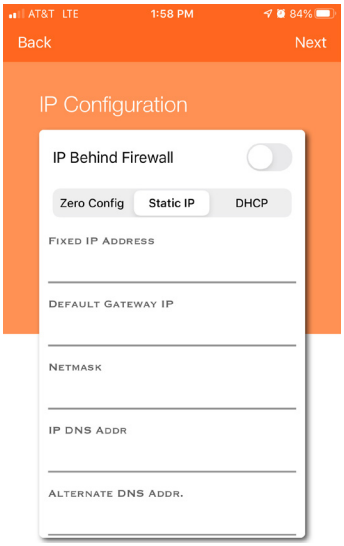
The communication mode screen will appear.

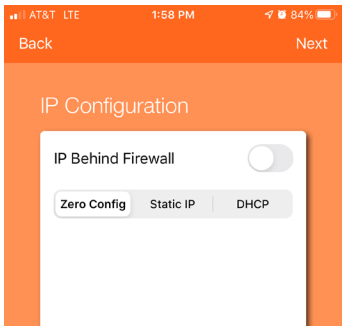
10. **Select** the IP option.

The IP Configuration screen will appear.

11. **Select** the Static IP or DHCP tab.

It is important to work with the IT department to gather the required network information.





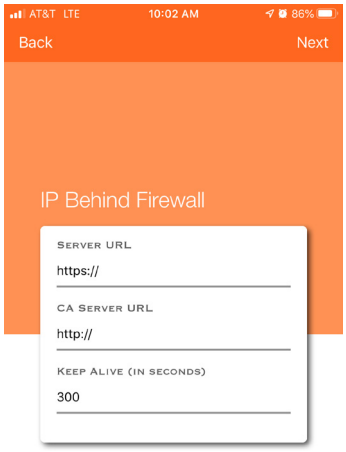
If DHCP is selected the assigned IP address can be located in the ENGAGE app under the Advanced Settings option for the Gateway.

If needed, **toggle** the IP Behind Firewall option to the ON position.

12. If required, **enter** the Network Information and **tap** Next.

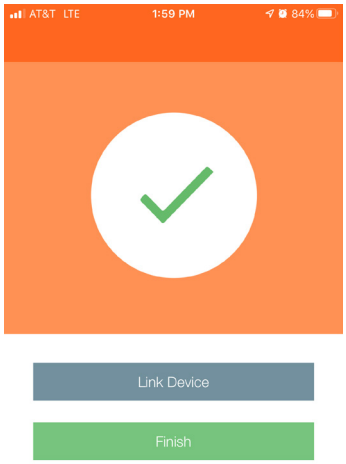
    If the IP Behind Firewall option is ON, the IP Behind Firewall dialog will appear. This allows the DNA Fusion Engage service to act as a server for the Gateway. Utilized when the Gateway is behind a firewall.

    Enter the required information and **tap** Next.



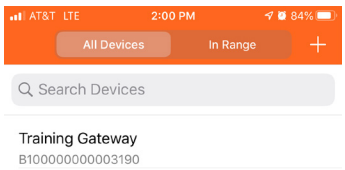
    The Preparing your device screen will be displayed.

    Once commissioned, a large check will appear.



13. **Tap** the Finish option.

    The Gateway will appear in the Device List.



14. **Close** the app, and **proceed** to Commissioning NDE Doors on page 3-11.

NOTES:

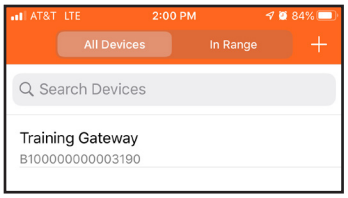
Commissioning NDE Doors

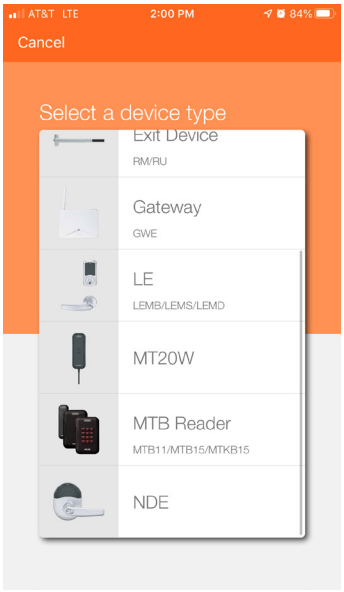
Once the NDE locks have been installed, they will need to be commissioned in the ENGAGE app prior to syncing the hardware in DNA Fusion. The NDE lock must be fully assembled with the battery connector plugged in and the battery cover in place. If the battery cover is not installed, the lock will NOT enter linking mode.

> *If the Lock has been in Standalone/Construction Mode, a Factory Default Reset will need to be performed. To factory reset the lock, remove the battery cover and hold the Reset button for 5 seconds. Release the Reset button. The LED will flash green twice and the lock will beep twice. Turn the interior door handle slowly three (3) times within 20 seconds to complete the process. The lock will beep once and the LED will turn red each time the handle is turned.*

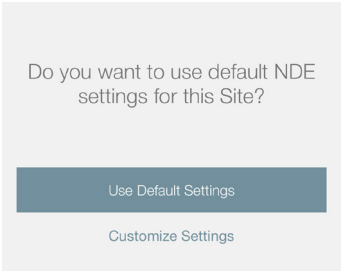
The ENGAGE app is used to commission the NDE locks in the Allegion portal. It is critical that the gateway and NDE locks are commissioned under the same account. Only one NDE lock can be linked at a time. If linking multiple locks, leave the battery cover off all uncommissioned locks.

1. **Open** the ENGAGE app and log in.
   Verify that the Gateway has been added to the ENGAGE app.
2. From the Devices tab, **select** the + sign.

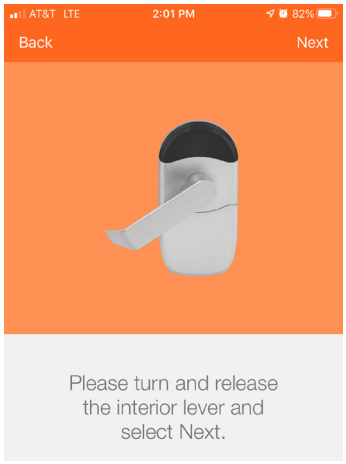


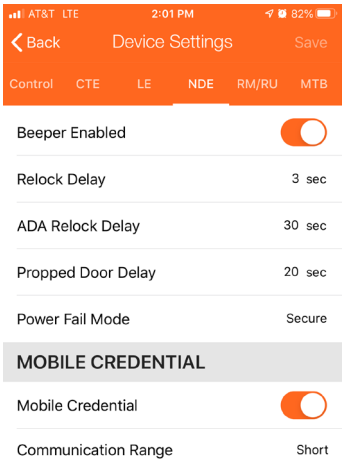


3. **Select** the NDE device type from the list.
   The Settings option will open.

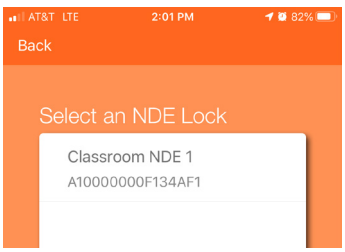


4. **Select** the desired method.
   Open Options recommends selecting the Default Settings option. The NDE lock settings can be changed at any point. The appropriate dialog will open.





5. **Turn and release** the Interior door handle.
   The door will beep once and the NDE lock will appear list. The NDE lock can be identified by the serial number.



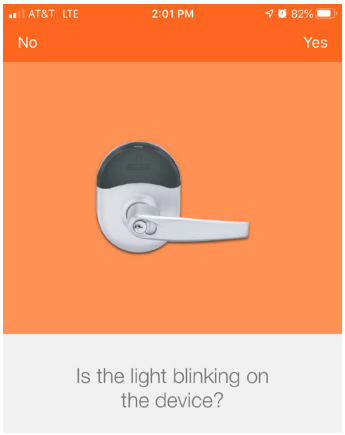
6. **Select** the NDE lock.

   A screen will appear inquiring about the reader LED's status. The light should start to blink.

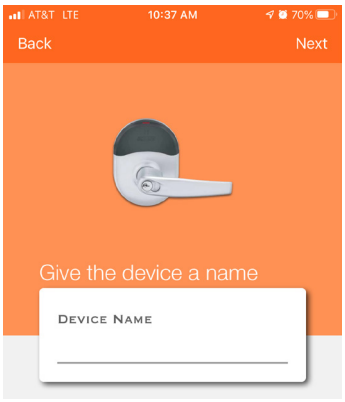
7. **Tap** Yes if the light is blinking.

   If the light is not blinking, repeat steps 5 and 6.

   The Device Name dialog will appear.

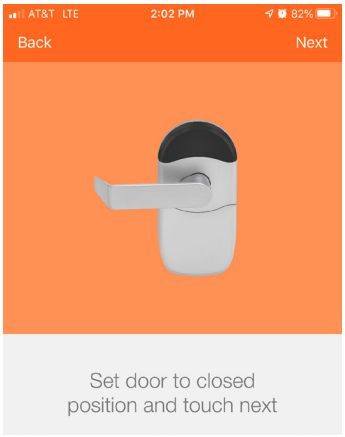


8. **Enter** a name for the NDE device and **tap** the Next option.



   The door calibration screen will appear.

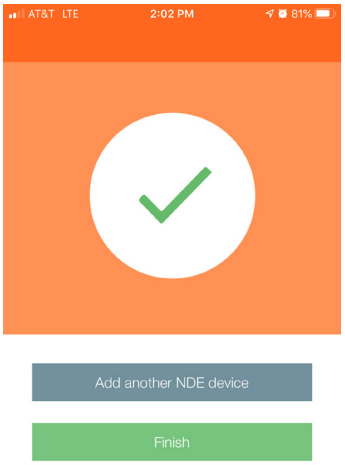
9. **Verify** that the door is closed or apply the door magnets and **touch** the Next option.



   The Select Wi-Fi screen will open.

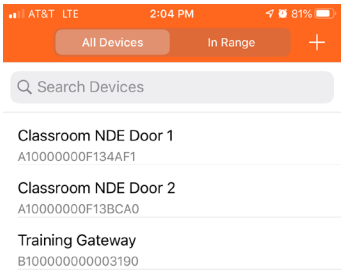
10. **Tap** the Skip option.

    Once commissioned, a large check will appear.



11. **Tap** the Finish option.

    The lock will appear in the Device List.

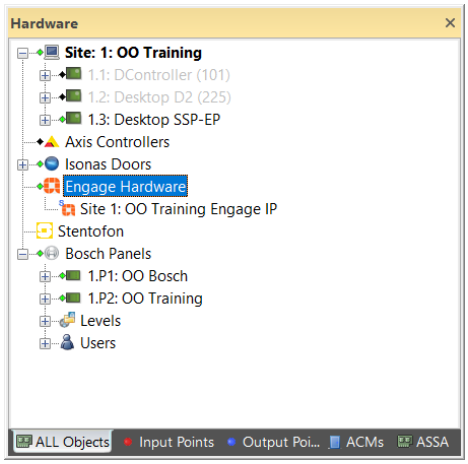


12. Close the app, and **proceed** to Syncing the Gateway and NDE Devices in DNA Fusion on page 3-13.

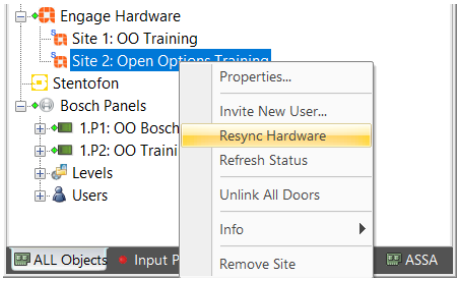
Syncing the Gateway & NDE Devices in DNA

After the Gateway and NDE locks are commissioned in the ENGAGE portal, they will need to be synchronized with DNA Fusion.

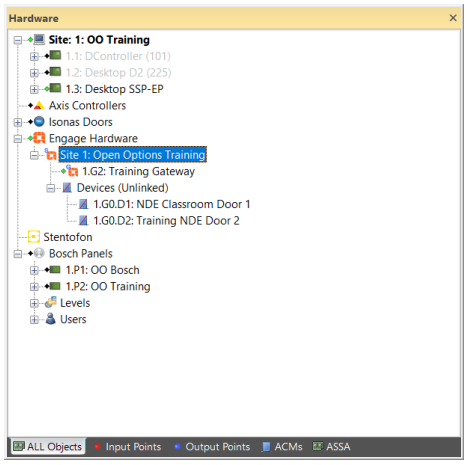
1. **Log in** to DNA Fusion and **open** the Hardware Browser.
2. **Locate** the ENGAGE Site created on page 3-5.



3. **Right click** on the Site and **select** Resync Hardware.



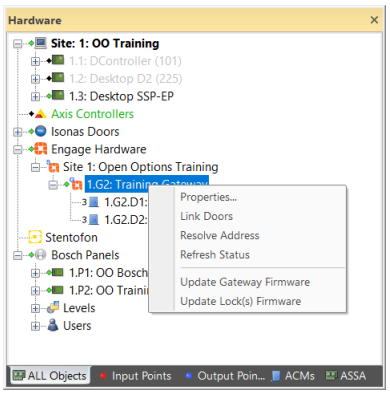
The ENGAGE hardware will auto populate after a moment and the ENGAGE Gateway and NDE locks will appear in the Hardware Browser. The diamond next to the Gateway will turn green. This indicates that the Gateway is online.



4. Continue to Configuring the Gateway on page 3-15.

Firmware Updates

The Gateway and NDE locks firmware should be updated after the integration is complete. Both tasks can be accomplished through the DNA Fusion software.



To upgrade the firmware on the Gateway:

1. From the Hardware Browser, **right click** on the Gateway.
2. **Select** the Update Gateway Firmware option.

   The firmware on the Gateway will be updated.

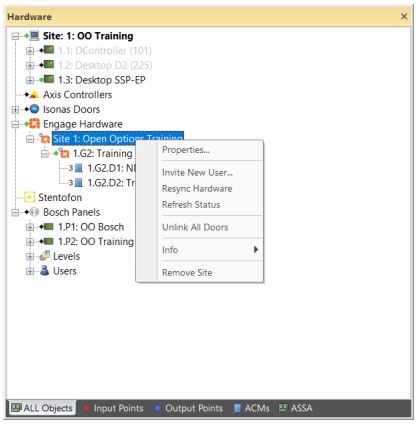
To upgrade the NDE lock firmware:

1. **Right click** on the Gateway.
2. **Select** the Update Lock(s) Firmware option.

   The firmware for all the linked locks will be updated.

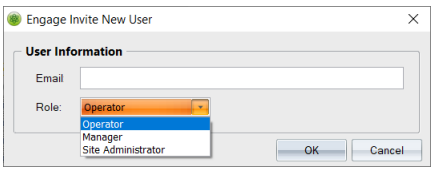
Inviting Users

Engage User's must be invited to "collaborate" on the ENGAGE site. After accepting the invitation and loading the app, the user will have access to the DNA Fusion Engage Site in the Engage app. The user will be able to commission hardware to the site from their ENGAGE phone app.



1. From the Hardware Browser, **right click** on the ENGAGE Site.
2. **Select** the Invite New User option.

   The Engage Invite New User dialog opens.



3. **Enter** the user's Email address.
4. **Select** the user's Role.

   Site Administrators - Unrestricted access to create, modify and delete users, devices and to manage device settings. Administrators can invite other Administrators, Managers or Operators to the ENGAGE app.

   Managers - Unrestricted access to create, modify and delete users, devices and manage property and device settings. Managers CANNOT invite new Administrators to the site however they can add new Operators.

   Operators - Operators have the most restricted permissions. They can manage daily maintenance operations such as updating door files and uploading Audits at the door into the ENGAGE app. Operators may also perform some maintenance items like updating a device's firmware. Operators CANNOT invite other users to the site.

5. **Click** OK.

   The User will receive an email with the Invitation. The receipt will need to open the email and verify their identity by clicking on the link.

   If the new user does not open and verify their invite email before the expiration date listed in the email, the invitation is automatically cancelled and another invite must be resubmitted.

Inviting Users to the ENGAGE *app does not grant access or affect operator permissions in DNA Fusion. Privileges within DNA Fusion are based on the* Operator Profile *applied to the designated operator in DNA. See Chapter 4: Operator in the DNA Fusion User Manual for more information on configuring operator settings.*

Configuring the Gateway

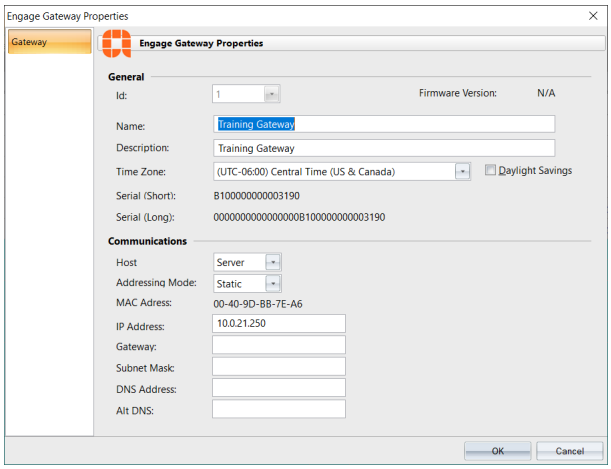
After the ENGAGE hardware has been populated in DNA Fusion, the Gateway Properties will need to be configured.

1. From the Hardware Browser, **right click** on the Gateway and **select** Properties.

   Or

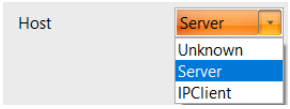
   Double click on the Gateway.

   The Gateway Properties opens.



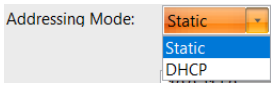
   If desired, **change** the Name or Description.

2. **Verify** the Time Zone and if needed, **check** the Daylight Savings option.

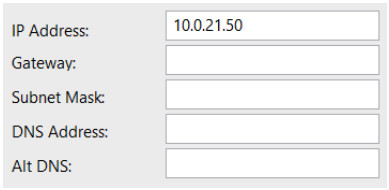


3. Under the Communications Header, **verify** the Host is set to Server.

4. In the Addressing Mode field, **select** the IP Configuration set on page 3-8. Open Options recommends uses Static Addressing.



5. If Static addressing is selected, **enter** information in the required Network Address fields.
   - IP Address - This field will auto populate when the Gateway is linked to DNA Fusion.
   - Gateway - **Enter** the network's Gateway address.
   - Subnet - **Enter** the correct Subnet Mask for the gateway.
   - DNS Address - **Enter** the DNS Address.
   - Alt DNS - If available, **enter** the Alt (Alternative) DNS address.



6. **Click** the Ok button to save the changes.

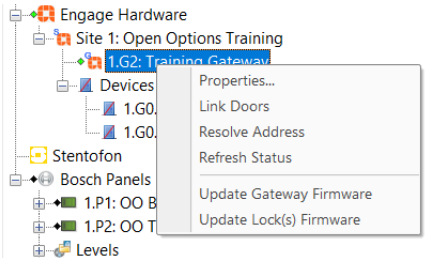
7. **Continue** to Linking the NDE Doors on page 3-16

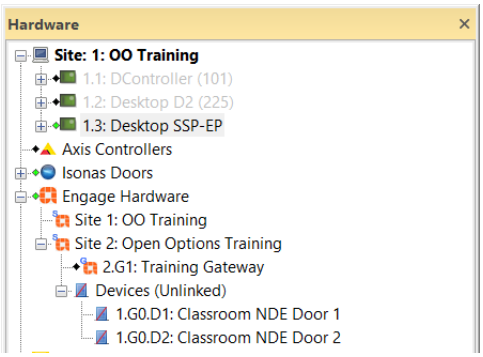
Linking the NDE Doors

Prior to linking the doors, the ENGAGE Doors header will display an Unlinked status.

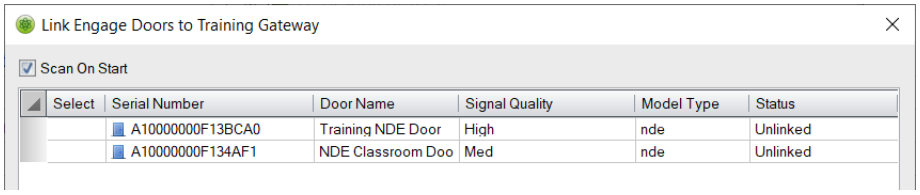
To link the doors:

1. **Right-click** on the Gateway and **select** Link Doors option.





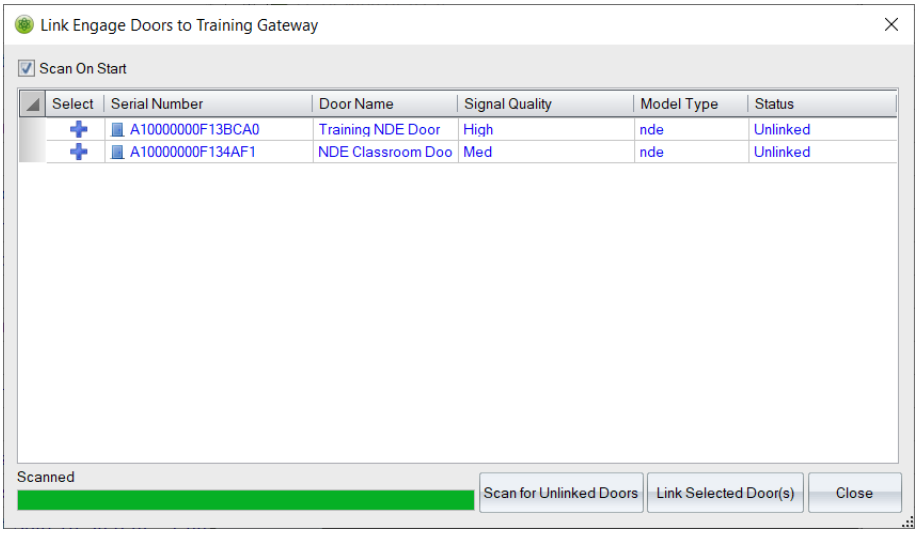
The Link Engage Doors to Gateway dialog will appear. DNA Fusion will start to scan for NDE doors. Once complete, the doors will be displayed in the dialog.



The dialog will indicate the lock's signal quality as well as the device type and link status.

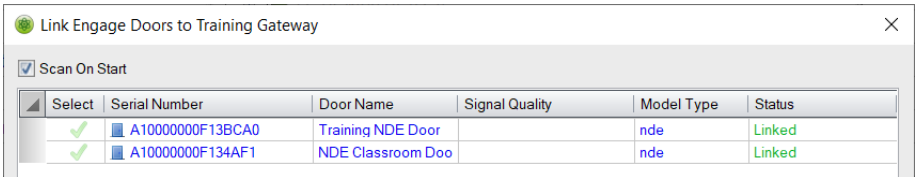
2. **Select** the desired doors to link to the Gateway.

   A checkbox will appear in the Selected column.



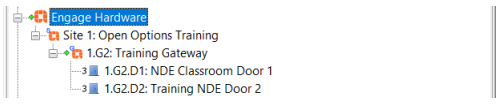
3. Once the NDE locks are selected, **click** the Link Selected Door(s) option.

   The doors will appear with a green checkbox in the Selected column and the Status will update to Linked. Once linked, the door will beep three (3) times and the LED will flash green.



4. **Click** the Close button.

   The locks appear as confirmed in the DNA Fusion application.



5. **Continue** to Chapter 4: NDE in DNA Fusion.

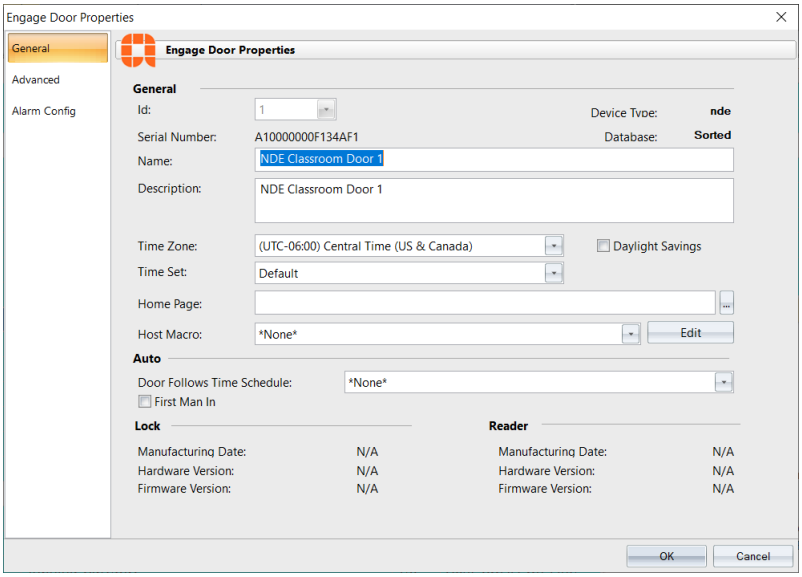
Configuring a Door to Follow a Time Schedule

The Unlock Schedule option provides a quick way to configure a door(s) to adhere to a specified unlock time schedule. The time schedule must be created prior to the setting up the unlock feature.

The Native IP Gateway integration is limited to 16 active time schedules. In this case, the first 16 default time schedules programmed in the DNA Fusion system will be available for selection or Time Schedule Sets can be created and applied to the NDE lock.

1. **Right-click** on the Door and **select** the Properties option.

   The Door Properties dialog opens.



2. In the Auto section, **select** the Door Follows Time Schedule drop down.

   The Time Schedules list appears.

> *Time Schedule information can be found in the DNA User Manual in Chapter 5. Keep in mind the ENGAGE IP NDE lock integration is limited to 16 time schedules.*

3. **Select** the desired Time Schedule from the list.
4. If desired, **check** the First Man In option.

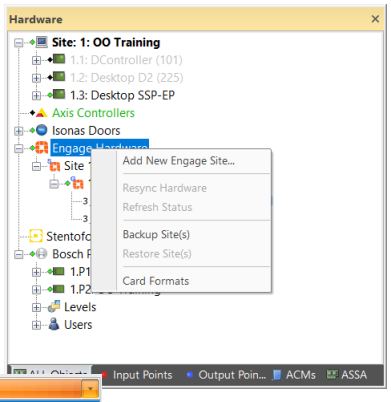
> *The door will remain in a secured mode even when the designated time schedule is active if no cardholders have accessed the door. Likewise, if a cardholder presents their card to the door when the time schedule is inactive, the door will remain secured.*

   If selected, the door will unlock after the first person badges at the reader within the time schedule specified in step 3.

5. **Click** OK to save the changes.

Configuring ENGAGE IP Card Formats

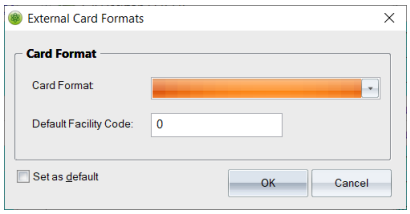
The NDE locks does not store card formats. The integration requires DNA Fusion to send a fully encoded card number to the lock in order for the card to validate access. To format the cards the exact format of the card must be known. DNA Fusion comes preconfigured with common card formats.

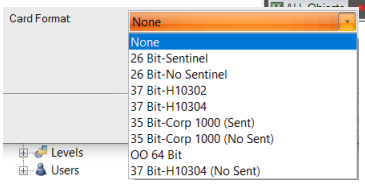


To configure additional card formats:

1. From the Hardware Browser, **right click** on the ENGAGE Hardware main node.
2. **Select** Card Formats from the menu.

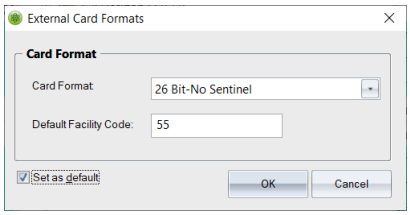
   The External Card Formats dialog opens.





3. **Select** the Card Format from the drop down list.
4. **Enter** the Default Facility Code for the card format(s).

   Each card format can have a default Facility Code. The Facility Code will automatically be populated when a new card is issued for the selected Card Format.
5. If desired, **check** the Set as default option.



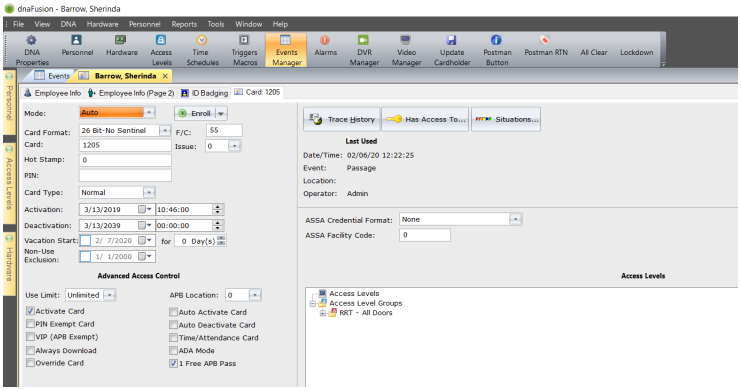
6. **Click** the Ok button to save the card format settings.

NOTE: If additional card formats are required, contact Open Options Technical Support.

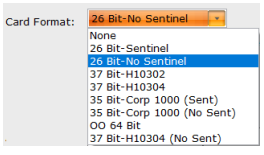
Configuring an ENGAGE IP Cardholder

The IP Gateway integration requires the Card Format be identified at the card level.

1. From the cardholders record, **select** the Card Tab.

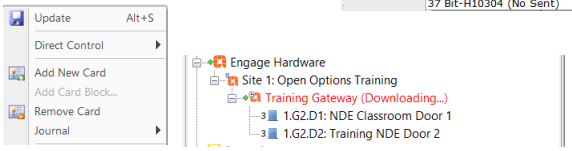


   The Card Type will auto default to the selected format. If no format is set as default, **select** the card format from the drop down list.



2. If needed, **enter** the Facility Code in the F/C field.
3. If needed, **add** an access level to the card.
4. **Right click** in the record and **select** the Update option.

   Downloading will appear next to the Gateway.



The Hardware Browser (IP Gateway)

The Hardware Browser in DNA Fusion is an explorer window that consists of a hierarchical layout of the field devices that make up the system. The tree also displays the status of objects by using status indicators to the left of the tree object.

To open the Hardware Browser:

1. **Select** the Hardware icon from the Standard Toolbar.

   Or

   Select View / Explorers / Hardware from the Main Menu.

   The Hardware Browser will open.

2. **Expand** the ENGAGE Hardware header.

Driver Status Indicators:

- Green Diamond - The ENGAGE driver is running and all systems are good.

- Black Diamond - The ENGAGE driver is not running.
  - Verify the DNADrvr32 and Engage services are running under the correct identity.

- Yellow Diamond - The ENGAGE driver is running but tunable to open the connection used to communicate status to the DNA Driver.
  - The oo.Engage.status queue cannot be opened by the DNA Driver. Verify that the Engage Driver is configured to run under a local administrators' group account.

- Red Diamond - The ENGAGE driver is running but unable to open the connection used to relay events to DNA.
  - The oo.dnafusion.event queue cannot be opened by the DNA Driver.

- Purple Diamond - The driver is running but unable to open either the events or status connections to DNA.
  - Both the oo.Engage.staus or oo.dnafusion.event queues cannot be opened by the DNA Driver.

Door Indicators:

- Blue Door - The door is currently in a normal state; i.e., closed.

- Red Door - The door is currently in an alarm state; i.e., door held open or door forced open.

- Gray Door - The door is in Lockdown mode.

- Green Door - The door is currently in an unlocked state.

- Yellow Door - The door is currently in the Momentarily Unlock status.

NOTES:

Door Control Options

The easiest way to control a door is to right-click on the door and select the option from the Door menu.

1. **Right-click** on the desired door in the Hardware Browser.
2. **Select** the Modes option and **select** the correct Mode.

Locked	Requires a card with the correct format be presented.
Unlocked	Unlocks the selected point and allows unlimited access. No card read required.
Lock Down	The door will ignore all badges except those flagged as VIP.
Remove Lock Down	Returns the doors to the normal state.

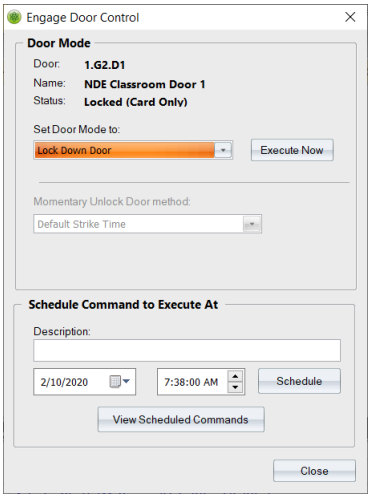
The Door Options menu also includes a Momentary Unlock option.

Door Control Dialog

DNA allows the operator to directly perform various tasks on a selected door using the Door Control dialog.

The dialog offers the following options:

- Change the Door Mode
- Issue a Momentary Unlock
- Schedule One Time Scheduled Commands



To open the Door Control dialog:

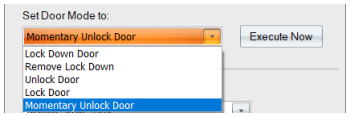
1. **Right-click** the door you wish to control and **select** Control from the context menu.

   The Direct Control dialog will open.

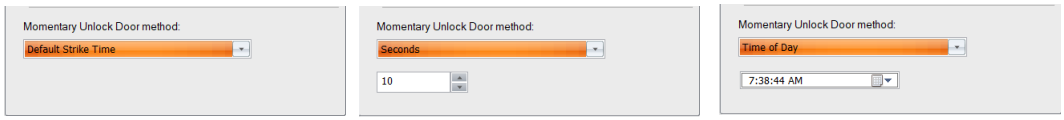
   - Door - Address and description of selected door. (Read Only)
   - Name - Description of lock. (Read Only)
   - Status - Displays the status of the door. (Read Only)

2. **Select** the appropriate option from the Set Door Mode to: drop-down and **click** the Execute Now button.

   Allows the operator to set the reader mode. This setting determines the type of access the reader will allow. See the table above for more door mode information.



If Momentary Unlock is selected, the Unlock Door Method drop-down becomes active. **Select** the desired method and **click** the Execute Now button.



- Default Strike Time - Unlocks the door for the programmed strike time.
- Seconds - **Enter** the time (in seconds) for the door to unlock.
- Time of Day - **Enter** the time for the Momentary Unlock command to be executed.

3. **Click** the Close button or the X icon to close the dialog box.

Scheduling Commands

The Schedule Command to Execute At option allows the operator to schedule door control.

It is a single event with defined start and end times as well as door modes. This type of scheduled control is stored in the host and is initiated from the host at the time of the event. Consequentiality, the host computer must be on at the time of the event.

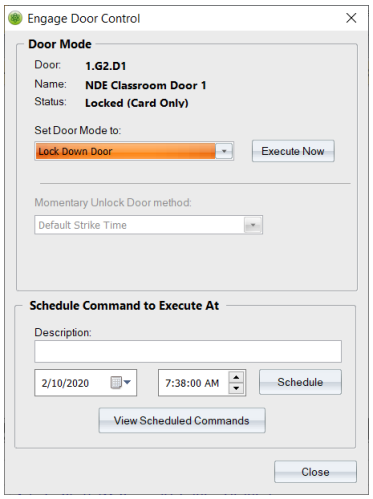
1. From the Door Control dialog, **select** the Door Mode.
2. In the Schedule Command to Execute At section, **enter** a Description for the event.

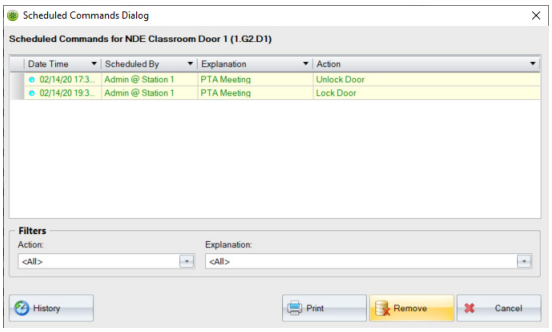
   This is a user-defined description for the action that will appear when the event is viewed in the future.
3. **Enter** a Date and Time.
4. **Click** the Schedule button.

   A confirmation dialog will appear. **Click** OK to close the dialog. Keep in mind you may need to schedule multiple door mode events to return the door to a secured state.

   To view any Scheduled Events, **click** the View Scheduled Commands button.

   Future events are displayed in green while events that have already occurred appear red.





Click the Remove button to delete a selected command.

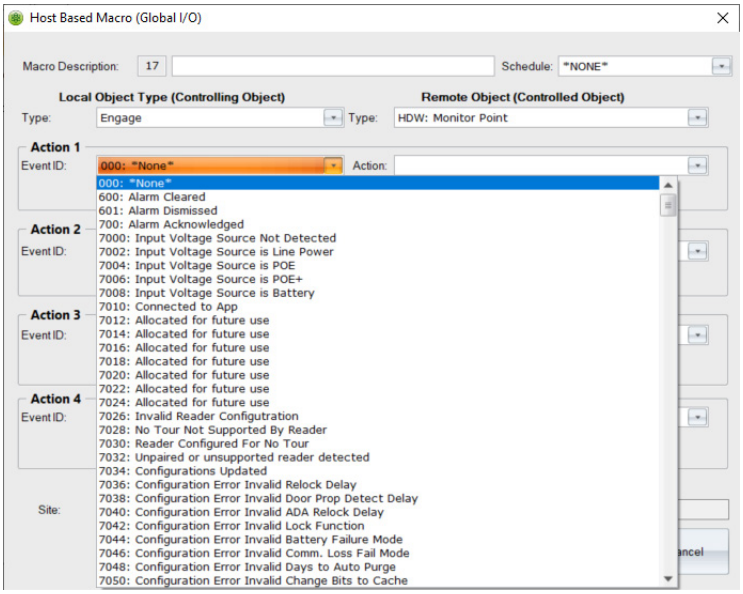
5. **Click** the Close button to exit the dialog.

> *If a door mode is changed, it may require scheduling two (2) events in order to return the door to a secured mode.*

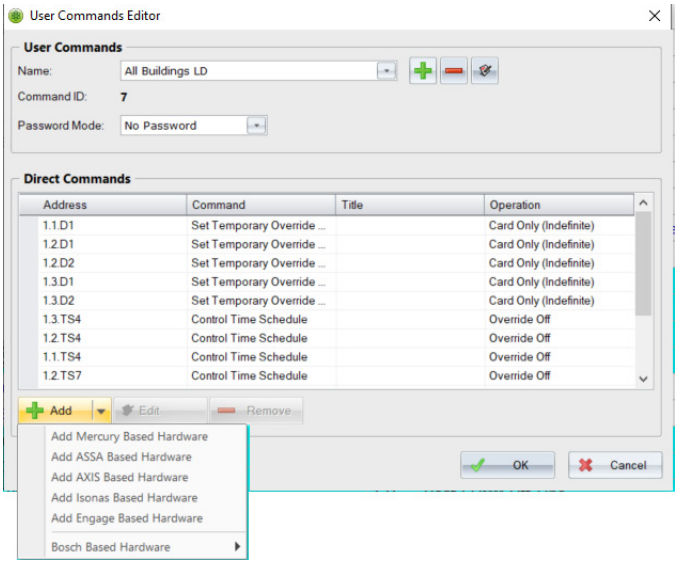
Supported Features

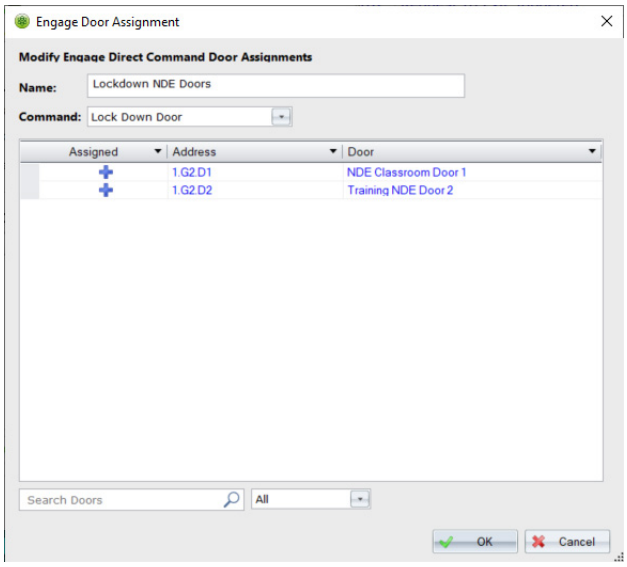
The following features are currently supported in a limited capacity.

- Host Based Macros



- Direct Commands





- Graphic Map Support
- Standard Crystal Reporting

Future Supported Features

The ENGAGE IP Gateway platform is a new and developing solution. There will be some limited functionality in the following areas:

- Conventional Triggers and Macros
- Tenants, SSP Lists and Event Filtering
- API Support for the Mobile application and Web capabilities
- ACM Status Report
- View ENGAGE locks on ACM tab
- ACM Sub Groups

This Page Intentionally Left Blank

NDE in DNA Fusion 4

In This Chapter

- √ Configuring Access Levels
- √ Controlling the NDE Lock Hardware
- √ Generating Reports

Once the NDE locks are commissioned and programmed in DNA Fusion, the properties of the door may be configured. Access levels will need to be created to provide access to the door(s). DNA Fusion also offers a number of different hardware features as well as the ability to generate "Who Has Access" reports on the fly.

If the ENGAGE IP Gateway solution was utilized, cards will need to be properly configured for the encoded data to be downloaded to the lock.

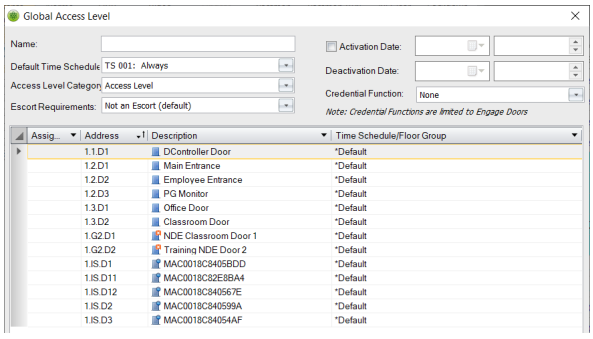
Configuring Access Levels in DNA Fusion

An Access Level consists of an entry point (such as a NDE locks) and an associated time schedule. When the access level is added to a card record, it determines where and when the cardholder has access within the system. When using the Gateway locks, Global Access Level Groups must be utilized.

Access Levels can be added to individual cards or groups of cards in the system. Each card can be assigned 32 access levels per SSP controller in the system. For more information on access levels, see Chapter 6 in the DNA Fusion User Manual.

Creating a Global Access Level Group

A Global Access Level Group provides an easy way for doors and elevators from multiple controllers to be grouped together in a common access level. This will allow a cardholder to have access to doors on multiple controllers with a single global access level group. See page 6-7 in the User Manual for more information.



1. With the Access Levels Browser open, **right-click** on Access Level Groups and **select** Add Global Access Level Group from the resulting menu.

   The Global Access Level dialog opens.

2. **Enter** a Name for the global access level group.

3. **Select** the Assigned column for the desired Doors and NDE Locks.

   A  will appear in the Assigned column once the door(s) have been selected.

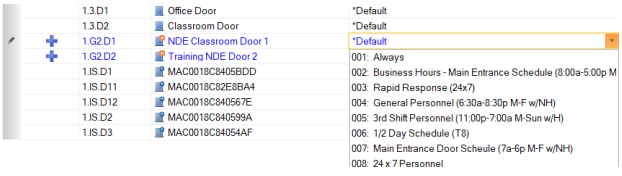
   If the group has doors already assigned, a  will appear in the Assigned column.

   NDE locks appear with A in the address as well as an identifying icon  .

4. From the Default Time Schedule drop down, **select** a Time Schedule for the Access Level.

   Or

   If Time Schedule Sets are utilized, the schedule will need to be selected from the drop down.



5. **Click** OK to close the Global Access Level dialog.

   The Global Access Level Group will appear in the browser and is ready for distribution to cardholders.

   Global Access Level Groups can be identified by the folder with the red access level icon.

ENGAGE Credential Functions (IP Configuration Only)

Credential functions in the ENGAGE IP NDE lock permits a card to perform specialized functions. In version 7.7.0.70 full support for additional ENGAGE credential modes when utilizing the Gateway IP installation method.

The additional credential options are available when configuring a Global Access Levels. If the site is licensed for Engage IP Gateway, a new option will be available on the Global Access Level header. Deploying the feature at the Access Level permits a credential to have different functionality on a door by door basis.

1. Create or edit a Global Access Level.

   See page 4-1 for information on creating Global Access Levels.

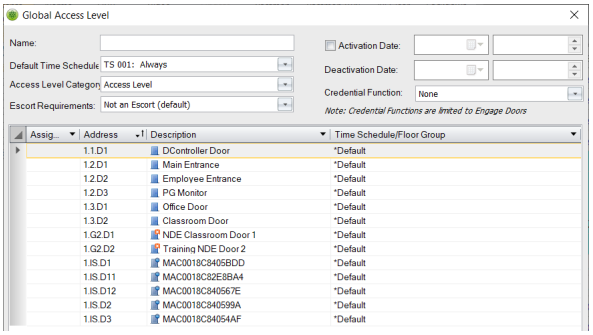
2. **Enter** a Name for the global access level group.

3. **Select** the desired Doors and NDE Locks.

   A  will appear in the Assigned column once the door(s) have been selected.

   If the group has doors already assigned, a  will appear in the Assigned column.

   NDE locks appear with A in the address as well as an identifying icon  .



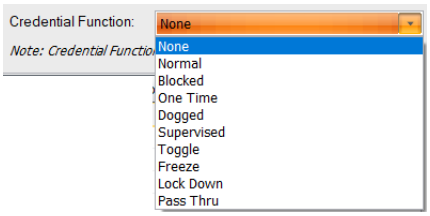
4. From the Default Time Schedule drop down, **select** a Time Schedule for the Access Level.

   Or

   If Time Schedule Sets are utilized, the schedule will need to be selected from the drop down.

5. **Select** the desired Credential Function from the list.

   This setting will have no impact if no ENGAGE doors are selected.



   - One Time - This function opens the selected ENGAGE door(s) only once with the normal function. Once a one time use credential has been used on a door, it will no longer work on that ENGAGE door. It will still provide access on other selected doors in the Access Level.
   - Supervised - These credentials allow access only when a second supervised credential is presented.
   - Toggle - A toggle credential unlocks the ENGAGE door and leaves it unlocked until a toggle credential is presented to the door again. It toggles a door between unlocked and card only.
   - Freeze - A freeze credential disables the credential reader. After a freeze credential has been used on a door, only a pass through credential will operate the lock. To move the freeze, present a freeze credential to the lock a second time to return it back to the normal operational state.
   - Lock Down - A lock-down credential places the lock into the secured mode combined with freeze credential functionality.

6. **Click** OK to close the Global Access Level dialog.

   The Global Access Level Group will appear in the browser and is ready for distribution to cardholders.

   Global Access Level Groups can be identified by the folder with the red access level icon.

NOTE: If a credential is assigned multiple access levels with different Credential Functions enabled, only one will be applied. This is based on a function ranking priority. The credential function with the highest priority will be granted to the card.

The Credential Functions priority is as follows:

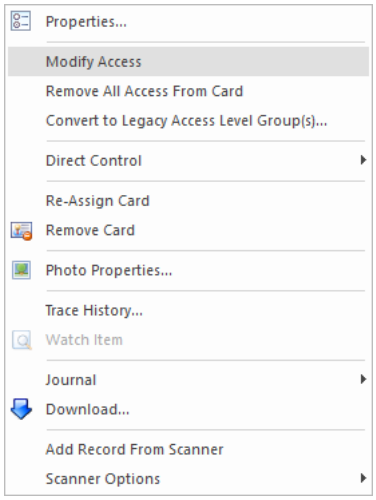
1. Pass Thru
2. Lock Down
3. Freeze
4. Toggle
5. Supervised
6. One Time

Assigning an Access Level to a Cardholder

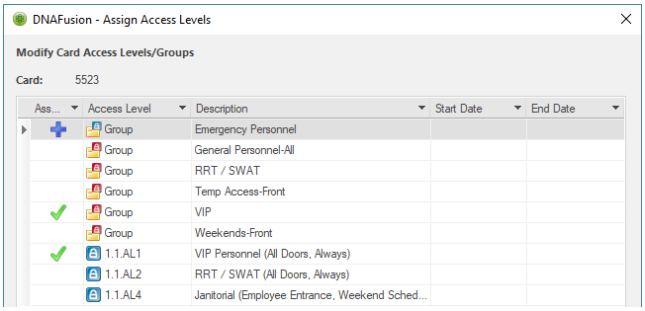
An access level provides the when and where a cardholder can access doors in the system. An access level can be associated with a cardholder numerous ways. See Assigning Access Levels on page 7-13 in the DNA Fusion User Manual for detailed information.

For ENGAGE IP Gateway integrations, an extra step is required to properly encoded the card. Since the locks are storing the card data and they do not account for facility codes, the Card Format and Facility Code will need to be entered in the cardholders record. See page 4-4 for more information.

Assign From the Context Menu



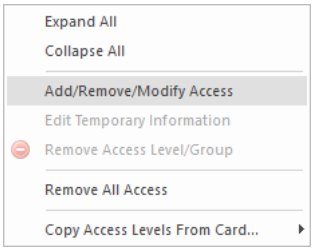
1. **Locate** the desired card in the Personnel Browser.
2. **Right-click** on the Card and **select** Modify Access.
   The Assign Access Levels dialog opens.



- A green check ✓ indicates that the access level is already assigned to the card.
- A red minus sign ▬ indicates that the access level will be removed from the card.
- A blue plus sign ✚ indicates that the access level will be added to the card.

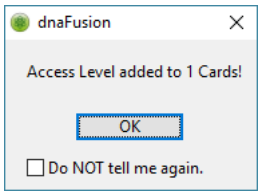
3. **Click** the Assigned field next to the desired access level(s).
   A blue plus sign ✚ will appear next to the access level(s).
4. **Click** the OK button.
   The access level(s) are added to the card.

Assign From the Personnel Record



1. **Select** the Card tab from the Personnel Record.
2. **Right-click** inside the Access Levels section and **select** Add/Remove/Modify Access.
   The Assign Access Levels dialog opens.
3. **Select** the Assigned field next to the desired access level(s).
   A blue plus sign ✚ will appear next to the access level(s).
4. **Click** the OK button.
   The access level(s) are added to the card.

Drag & Drop to an Individual Card or Cardholder

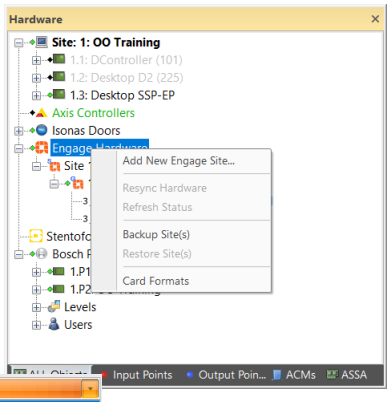


1. **Open** the Personnel Browser and the Access Levels Browser.
2. **Expand** the browser tree.
3. **Drag** and **drop** the Access Level to the desired Card or Cardholder.
   A confirmation dialog appears.
4. **Click** OK.

> *If the access level is dragged and dropped to a cardholder, the access level will be assigned to all of the cardholder's cards.*

Configuring ENGAGE IP Card Formats (IP Gateway Integrations Only)

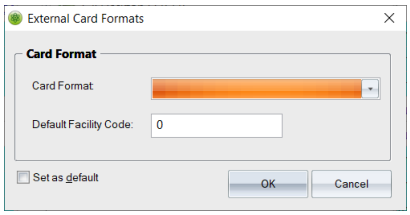
The NDE locks does not store card formats. The integration requires DNA Fusion to send a fully encoded card number to the lock in order for the card to validate access. To format the cards the exact format of the card must be known. DNAFusion comes preconfigured with common card formats.

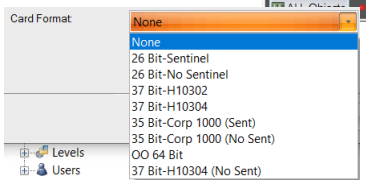


To configure additional card formats:

1. From the Hardware Browser, **right click** on the ENGAGE Hardware main node.
2. **Select** Card Formats from the menu.

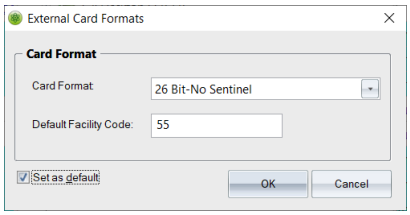
   The External Card Formats dialog opens.





3. **Select** the Card Format from the drop down list.
4. **Enter** the Default Facility Code for the card format(s).

   Each card format can have a default Facility Code. The Facility Code will automatically be populated when a new card is issued for the selected Card Format.
5. If desired, **check** the Set as default option.



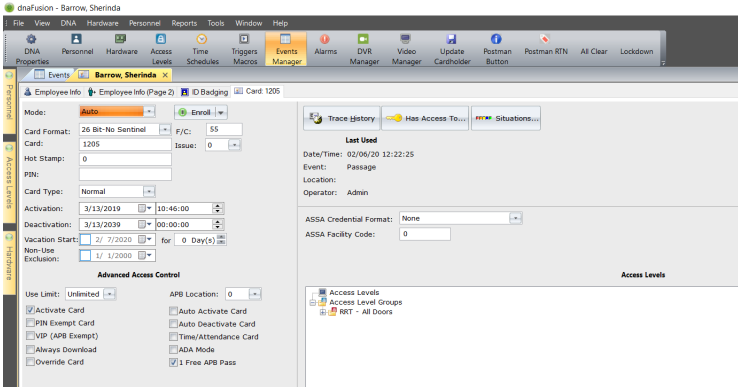
6. **Click** the Ok button to save the card format settings.

If additional card formats are required, contact Open Options Technical Support.

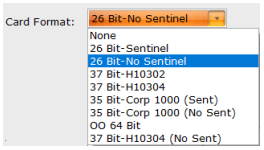
Configuring an ENGAGE IP Cardholder (IP Gateway Integrations Only)

IP Gateway integrations require the Card Format be identified at the card level.

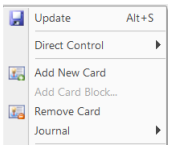
1. From the cardholders record, **select** the Card Tab.



The Card Type will auto default to the selected format. If no format is set as default, **select** the card format from the drop down list.

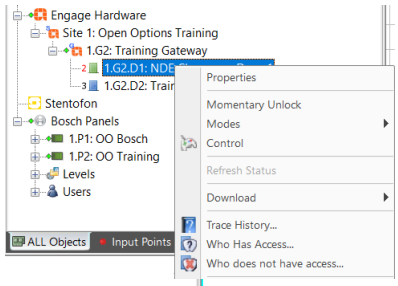


2. If needed, **enter** the Facility Code in the F/C field.
3. If needed, **add** an access level to the card.
4. **Right click** in the record and **select** the Update option.



NDE Door Features

There are a number of features available for NDE locks. For instance, you can see who has access to a specific door or trace the history for the selected lock.



To access these features, right-click on the lock.

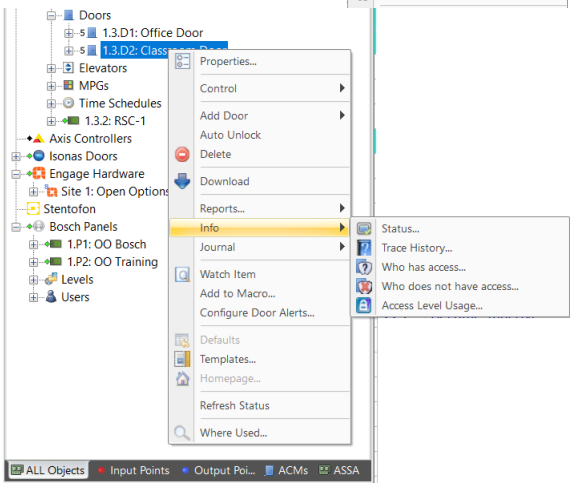
Trace History

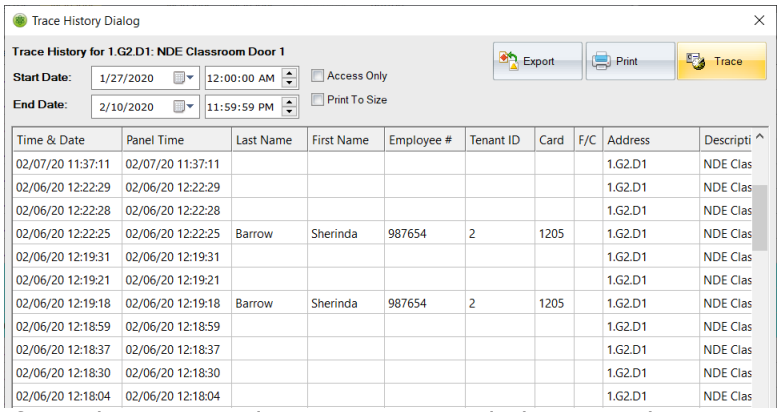
A trace history report can be run on a reader-controller to view the last transactions.

1. **Right-click** on the NDE Lock and **select** Trace History from the menu.

   Or select the Info / Trace History option.

   The Trace History Dialog will open.





2. If a wider time or date range is needed, **enter** the Start and End Date/Time and **click** the Trace button.
3. To view access events, **check** the Access Only option and **click** the Trace button.

   The results will be limited to access granted and denied events.

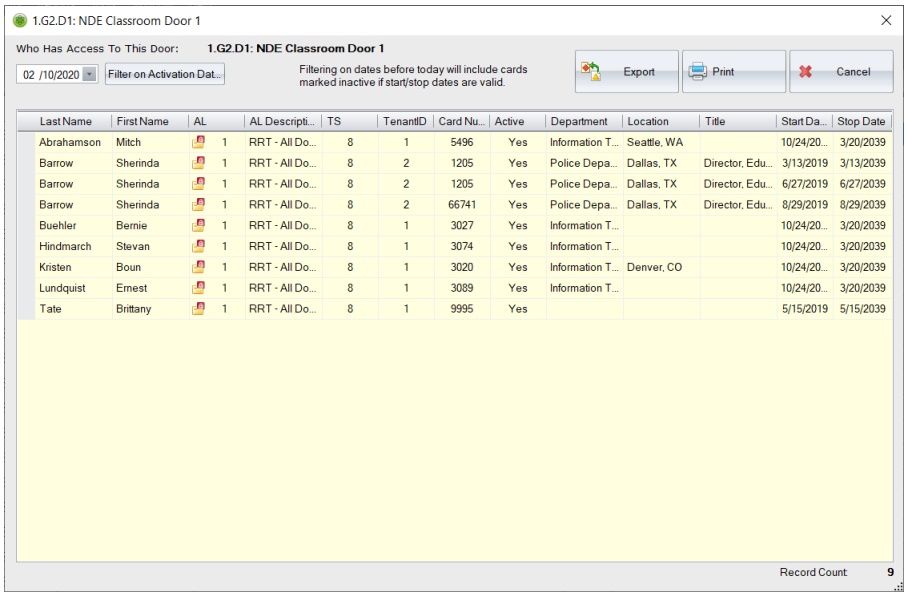
   The results can be printed or exported by selecting the appropriate button. **Select** the Print to Size checkbox to size the report so that all columns appear on the same page without forcing them to a new page.

Who Has Access

This feature allows you to generate an immediate report that details who has access to the selected ACM.

1. **Right-click** on the Door and **select** Who Has Access from the menu.

   The Who Has Access dialog appears.



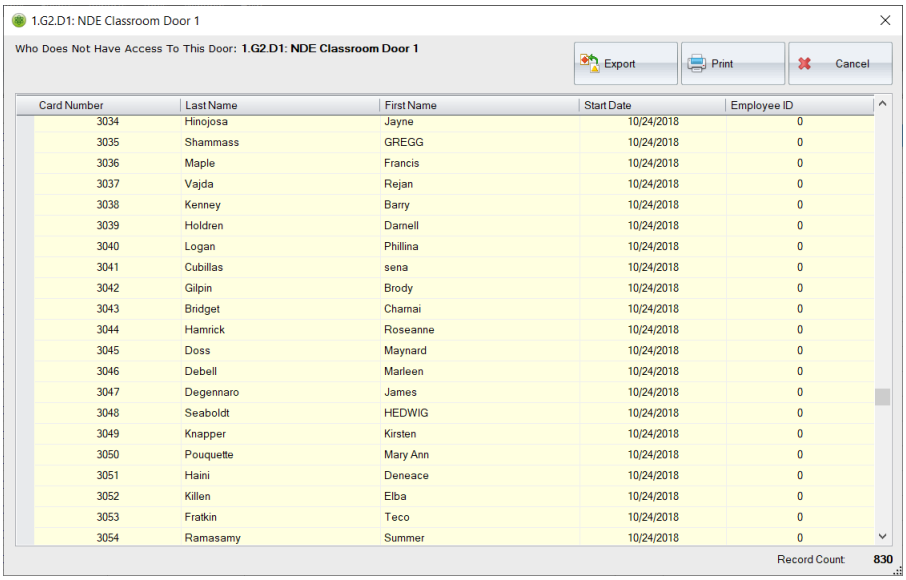
   The results can be exported, printed or e-mailed by selecting the appropriate button.

Who Does Not Have Access

This feature allows you to generate an immediate report that details who does not have access to the selected ACM.

1. **Right-click** on the ACM and **select** Who Does Not Have Access.

   The Who Does Not Have Access dialog appears.



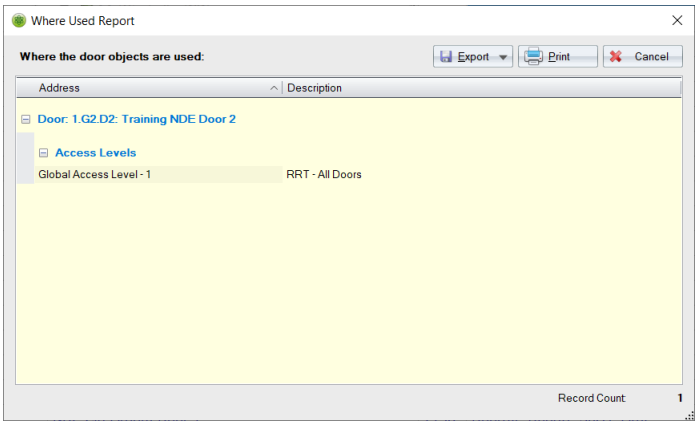
   The results can exported, printed or e-mailed by selecting the appropriate button.

Where Used

The Where Used feature provides a grid displaying the door's associated relationships (i.e. Triggers, Macros, Access Levels, etc.).

1. **Right-click** on the ACM object and **select** Where Used.

   The Where Used Report dialog opens.



   The results can be exported to a CSV file or to the Clipboard.