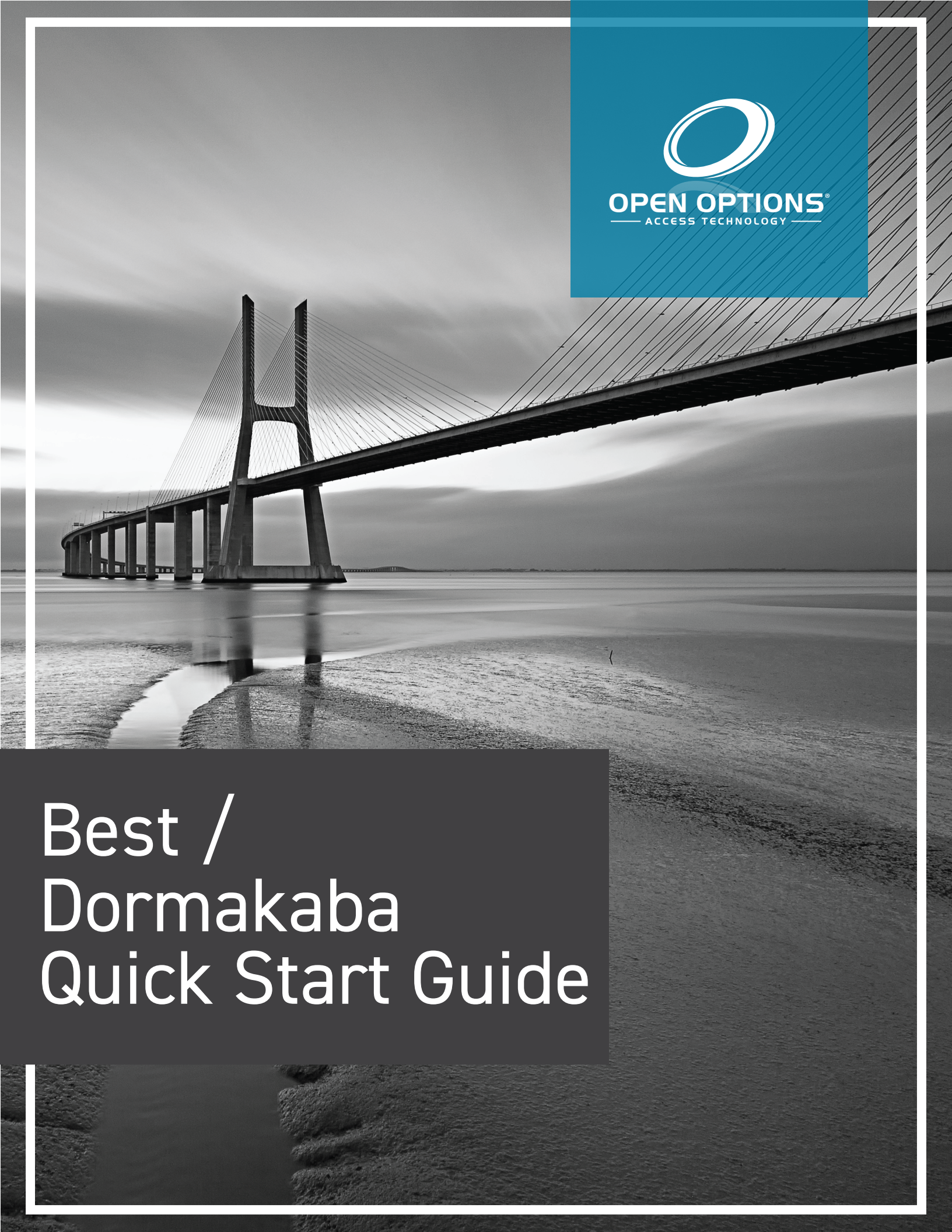


Best / Dormakaba Quick Start Guide

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

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

Publish Date: November 30, 2020
Manual Number: BDQSG 1.1

Warranty

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

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

Open Options Software License Agreement

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

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

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

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

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

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

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

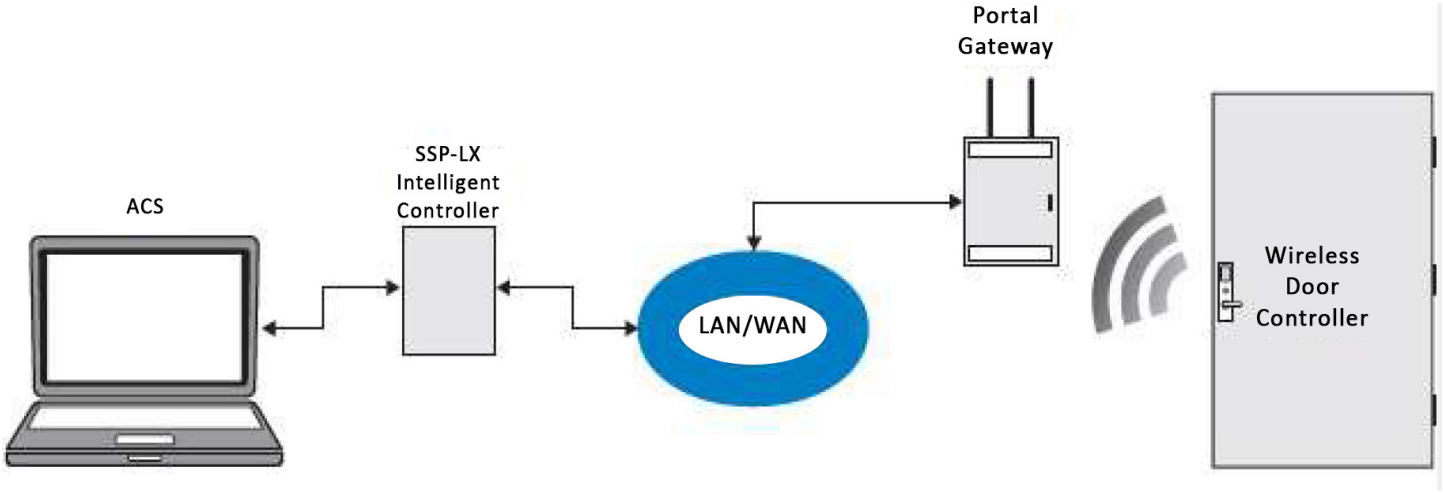
APPLICABLE LAWS: This Agreement is governed by the laws of the State of Texas, including patent and copyright laws. This Agreement will govern any upgrades, if any, to the program that the licensee receives and contains the entire understanding between the parties and supersedes any proposal or prior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

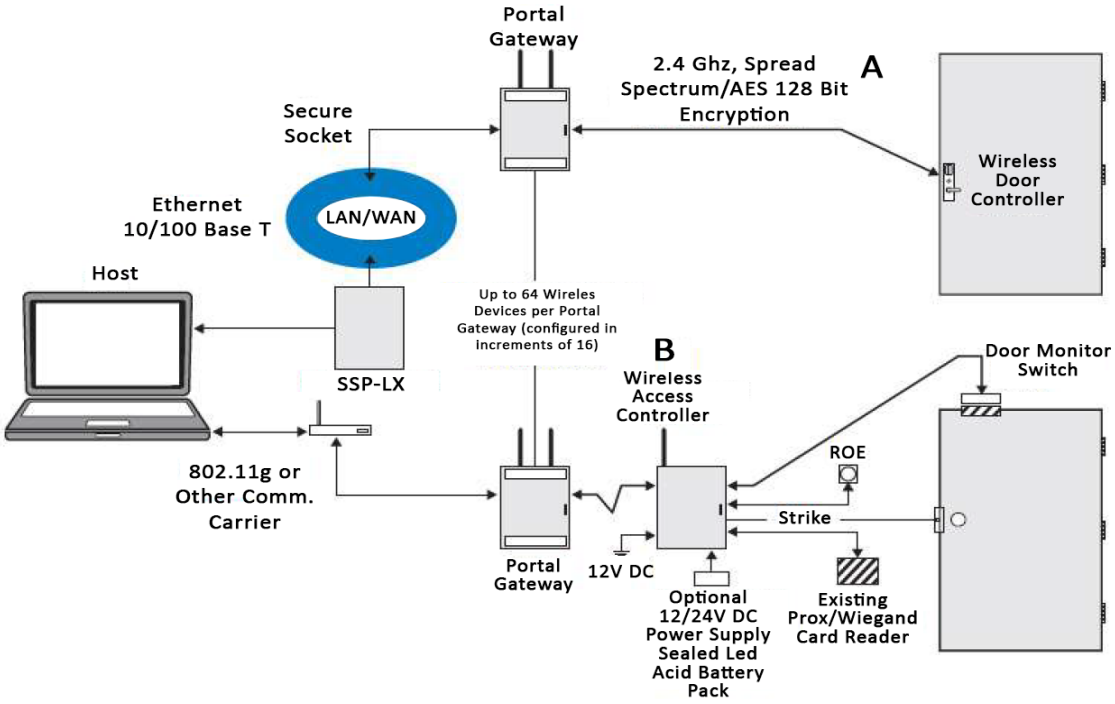
Best/Dormakaba Wi-Q: Quick Start Guide

This Quick Start Guide will explain the installation and configuration process of a Best/ Dormakaba Wi-Q in DNA Fusion. A SSP-LX is required for this installation.

Installation

The SSP-LX can communicate with 10 Wi-Q Gateways. The communication between the SSP-LX and the Wi-Q Gateway is over Ethernet. Each Wi-Q Gateway serves as its own Wi-Fi access point. The diagrams below show typical hardware configurations.





Step 1: *Panel Setup in DNA Fusion* - Ensure that the required licenses have been added to DNA Fusion (Dormakaba Doors, PSIA). Load Over-watch firmware to access the Over-Watch tab in the SSP-LX's internal webpage (Page 3).

Step 2: *Configuring the SSP-LX* - Enter the SSP-LX's internal webpage and adjust the network settings. Download the required .pem and .crt files. In the Over-watch tab add a user (Page 4).

Step 3: Configuring the Wi-Q Gateway - Press the Enable Wi-Fi button on the Wi-Q Gateway. Using a smart device (mobile phone or tablet) or laptop, connect to the Wi-Q via Wi-Fi. Change the network settings and download the required certificates. Add and configure the gateway in DNA Fusion (Page 7).

Step 4: *Configuring the Door Locks* - In the Gateway Web UI, locate the Current Sign on Key. On the door lock, press the token key (5678#) then the Current Sign On Key (XXXXXX#). The lock will flash a green LED twice if the connection was successful (Page 11).

Additional Information - Various door settings are disabled in the Gateway Web UI. Door parameters like Allow Double Swipe and Allow Override Cards require additional configuration in DNA Fusion (Page 13).

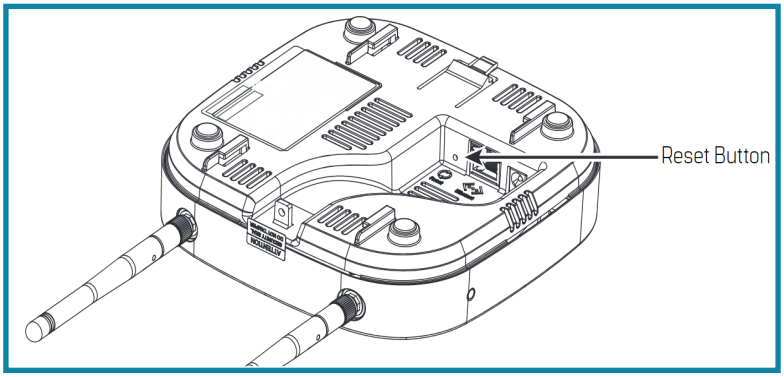
LED Indications

Mode	Color	LED Behavior
Boot	Purple	1 flash every 2 seconds
Waiting for or lost ACS connection	Red	Solid
Online and connected to ACS	Green	Solid
Survey Mode	Blue	Solid
Firmware update	Aqua	Flashing
Boot Error	Purple	Solid
Rebooting	Purple	2 flashes per second
Factory Reset	Purple	4 flashes per second

Deep Resetting the Wi-Q

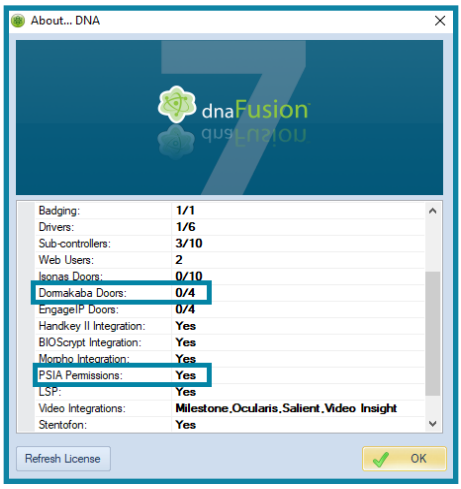
Before configuring the Wi-Q Gateway, ensure that the gateway has not already been configured. Deep reset the gateway using the steps below.

1. **Apply** power to the Wi-Q Gateway.
2. **Flip** the Wi-Q Gateway to reveal the underside of the device.
3. **Insert** a pin to **press** the reset button for 10+ seconds.
   The location is labeled Reset.
4. If the deep reset was successful, the LED will begin to flash purple.
5. **Wait** until the color switches off purple to begin a new configuration.

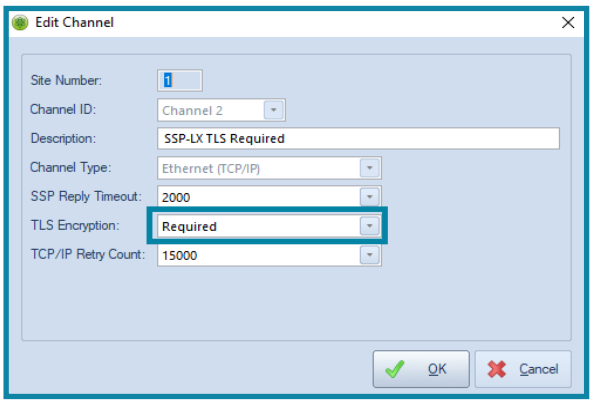


Panel Setup in DNA Fusion

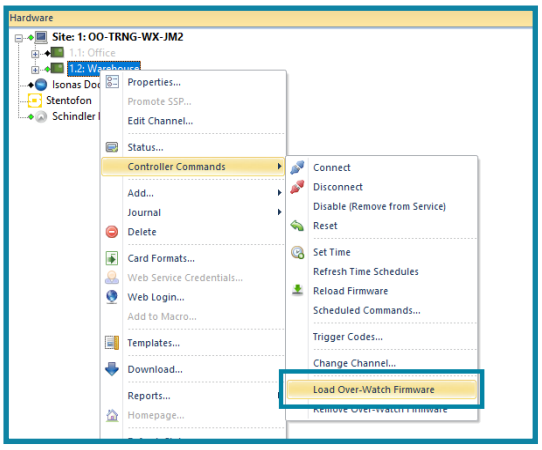
Ensure that the user has the Dormakaba and PSIA licenses set up for the Dormakaba doors. The license is by the door, so the Wi-Q Gateways DO NOT count towards the licensed SIO count. Having the Dormakaba license, enables the option of loading Over-watch firmware.



1. Once the SSP-LX is added to the site, **right-click** on the SSP-LX and **select** Edit Channel.
2. In the Edit Channel dialog, **set** TLS Encryption to Required.



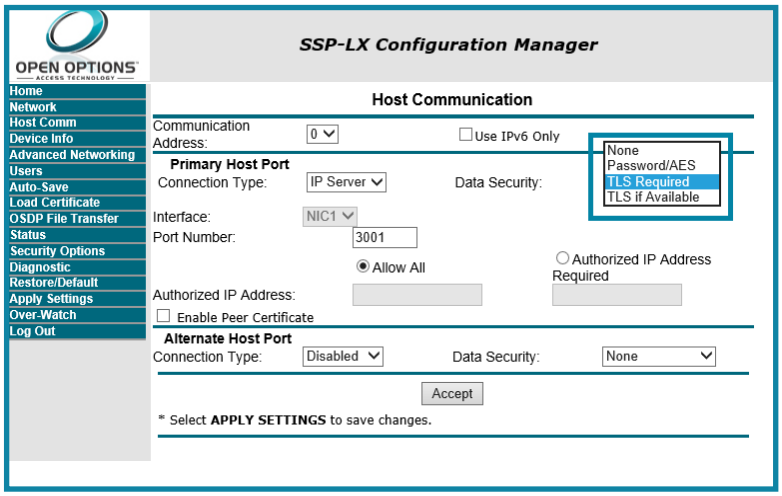
3. **Ensure** that the SSP-LX's firmware version is at or above 1.29.2.0637.
   a. **Right-click** on the SSP-LX and **select** Status.
   b. **Locate** the Firmware section in the SSP Status dialog.
   c. **Ensure** that the firmware version matches the required version (1.29.2.0637).
   c. If necessary, **reload** the firmware.
4. **Right-click** on the SSP-LX and **select** Controller Commands / Load Over-Watch Firmware.



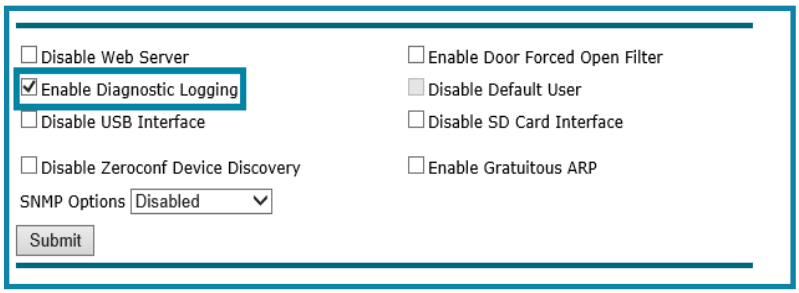
Configuring the SSP-LX

Access the SSP-LX's Configuration Manager. Use the MercZeroConfig tool to locate and access the desired device. Follow the steps below to configure the SSP-LX:

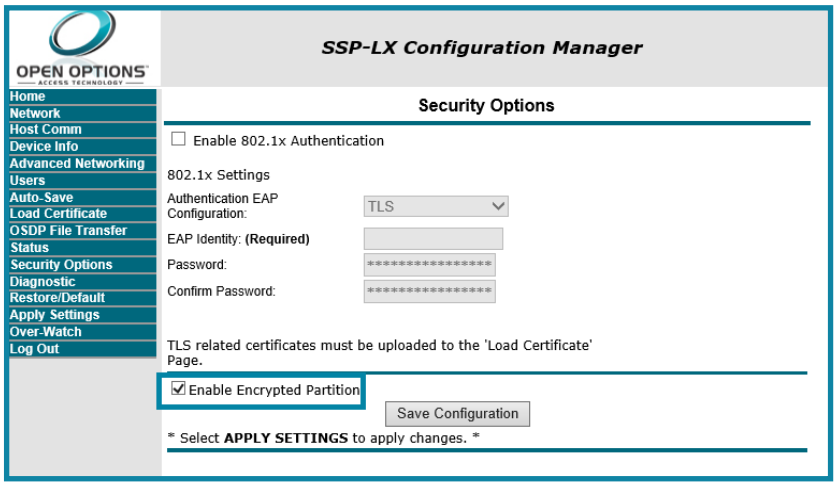
1. Once the user has accessed the Configuration Manager, **select** the Host Comm tab.
2. On the Host Communication page, **ensure** that Data Security is set to TLS Required.



3. **Click** on the Accept button.
4. **Select** the Users tab.
5. **Ensure** that the Enable Diagnostic Logging checkbox is checked.

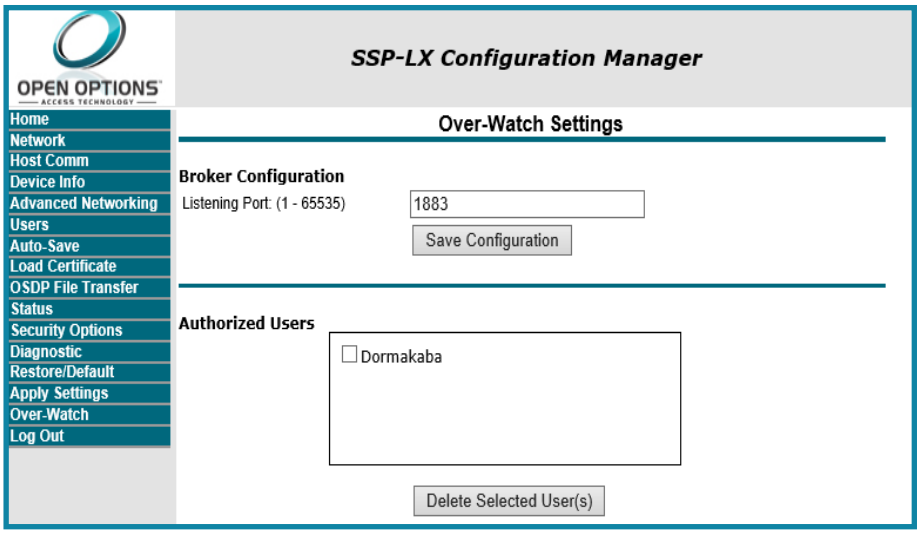


6. **Click** on the Submit button.
7. **Select** the Security Options tab.
8. **Check** the Enable Encrypted Partition checkbox and **click** on the Save Configuration button.



9. **Select** the Over-Watch tab.

10. **Login** to the Over-Watch page.
11. **Add** a New User.
    a. **Add** a Username.
    b. **Add** a Password.
    c. **Confirm** Password.
    d. **Click** on the Add User button.
12. **Set** the Broker Configuration to 1883.



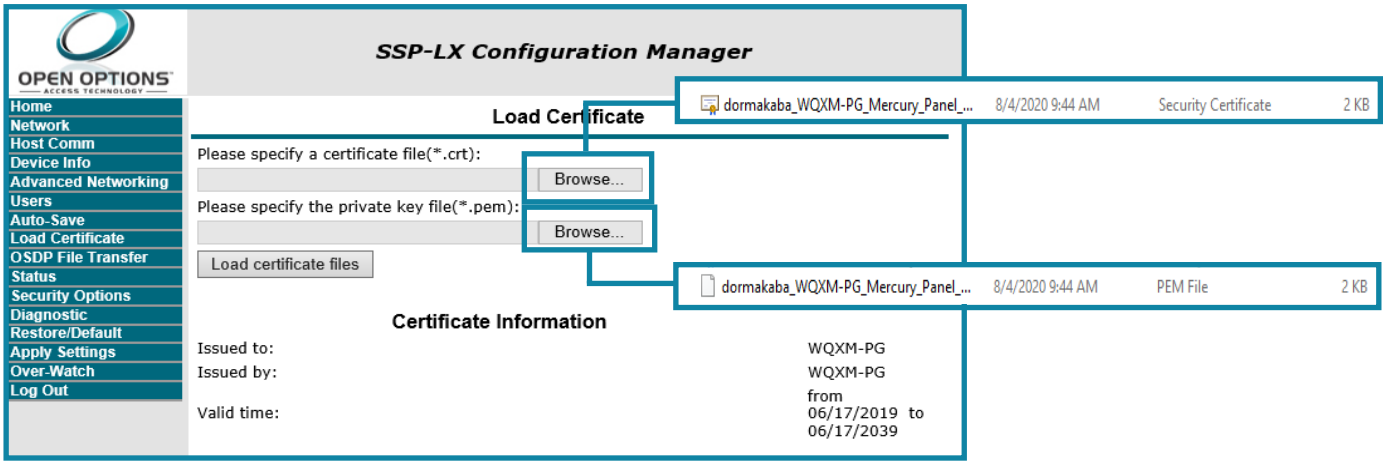
13. **Click** on the Save Configuration button.

Loading Certificates

SSP-LX will require new certificates to be manually uploaded.

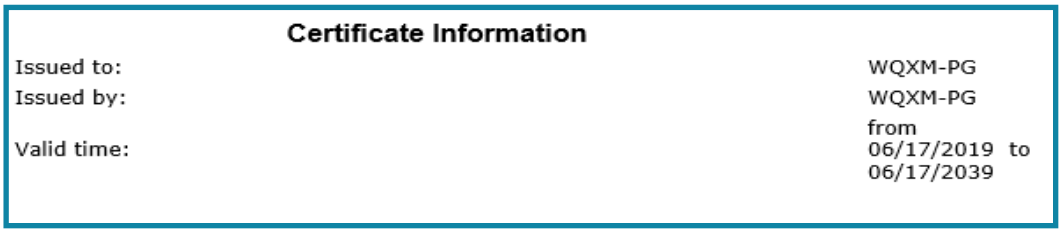
1. **Click** the following link to download the ZIP file.

   Link: http://ooaws.ooaccess.com/Misc/WiQ-Cert/dormakaba_WQXM-PG_Mercury_Panel Certificate.zip
2. **Unzip** the downloaded file. There will be a .crt and .pem file.
3. In the Configuration Manager, **select** the Load Certificate tab.

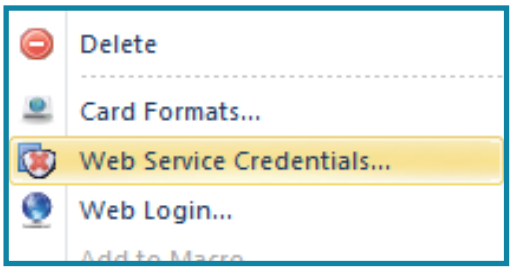


4. Use the two Choose File buttons to select the .crt and .pem files.
5. **Click** on the Load certificate files button.

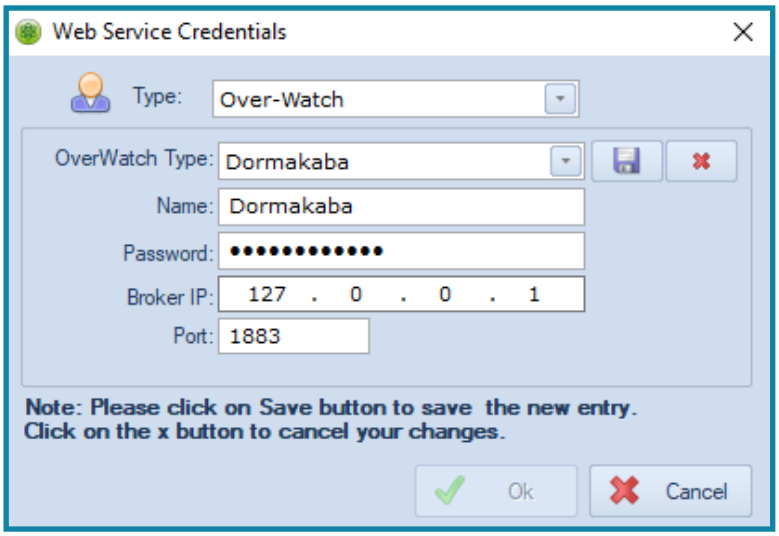
6. After the certificates are loaded, **select** the Apply Settings tab and **click** Apply Settings, Reboot. The image below shows the SSP-LX's Certificate Information after the controller is rebooted.



7. After loading the Over-Watch firmware, **right-click** the SSP-LX and **select** Web Service Credentials. The Web Service Credentials dialog opens.



8. In the first Type drop-down menu, **select** Over-Watch.
9. For the OverWatch Type drop-down menu, **select** Dormakaba.
10. Using the name added in the Configuration Manager (see step 11 on page 5), **insert** the Over-Watch username into the Name text field.
11. **Ensure** that the Password and Port match what was setup in the Configuration Manager.
12. In the Broker IP field, **type** the address 127.0.0.1.



Configuring the Wi-Q Gateway

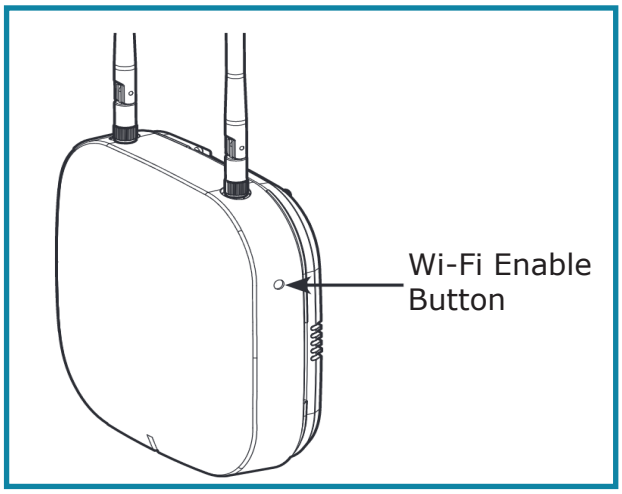
The Wi-Q requires 12 Vdc, 1 A of power. A Category 5e is the minimum cable rating for an Ethernet cable. The Wi-Q is configured through a Wi-Fi network. A mobile device can be used as an option to configure the Wi-Q's IP address.

Wi-Q Gateway Wiring

1. **Insert** Cat 5e Ethernet cable into the Wi-Q Gateway.
2. **Insert** power cable into the Wi-Q Gateway.
3. **Apply** power to the Wi-Q Gateway.

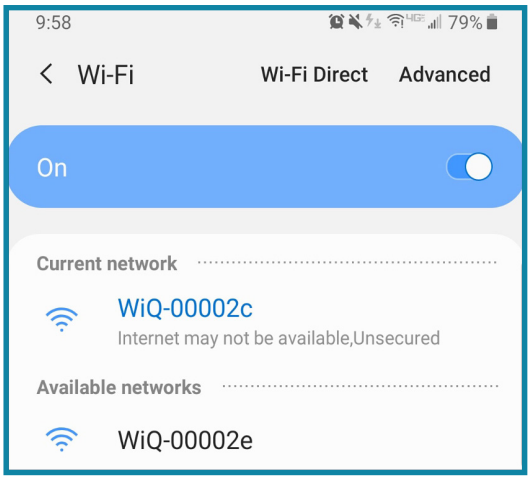
Network Configuration

4. On the Wi-Q Gateway, **press** the Wi-Fi Enable button on the side of the gateway.
   This allows the user to connect to the Wi-Q like a normal Access Point.



5. After pressing the Wi-Fi Enable button, **connect** the Wi-Q to the Wi-Fi network.
   The SSID (Device connection name) will be WiQ-xxxxxx, where xxxxxx are the last six digits of the MAC address for the gateway.

NOTE: *A smart device (smart phone, tablet, etc.) or laptop can be used to initially configure the IP address. After the IP address is configured, the host machine can be used for additional changes in the Gateway Web UI.*



6. After the Wi-Q Gateway is connected, **open** an internet browser and type http://192.168.3.200 (default IP Address) in the URL to open the Gateway Web UI.

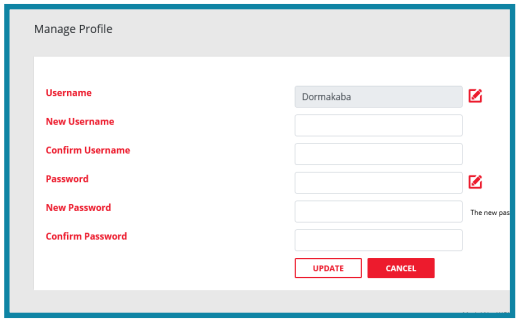
> **NOTE**: *Additional IP addresses:*
> - *http://192.168.2.200*
> - *http://192.168.1.200*

7. **Login** to the Wi-Q Gateway using the default Username and Password.

   Default Username: admin

   Default Password: password

8. The first time a Wi-Q Gateway is logged in to, the Manage Profile screen will appear, prompting to change the Username and Password. To update the Username, **click** the edit button next to the Username text field.



> **NOTE**: *The user will be prompted to change the Password every time the Gateway is logged in to until the password is changed.*

9. **Select** the GATEWAY tab.
10. **Enter** the desired IP address in the IPv4 Address field.

    Typically, the IP address will be a static IP. This IP address will be used to access the Gateway for any future changes.

11. **Select** Update to save the configuration.
12. After the IP address is configured, **press** the Wi-Fi Enabled button to disable the Wi-Fi network.
13. If needed, **use** the host machine (generally a computer or laptop).
14. **Open** an internet browser (Internet Explorer is recommended).
15. In the URL, **enter** the Wi-Q Gateway's new IP address.
16. **Enter** the username and password.

17. **Select** the GATEWAY tab.
18. If needed, **update** the Portal Firmware Version to 4.1.0.7.
    a. **Click** the link below to download the required firmware. The file is located in the Downloads folder.
    Link: http://ooaws.ooaccess.com/Installs/dormakaba/Firmware/WQXM-PG-4.1.0.7-image.gzhe
    b. At the bottom of the GATEWAY page, **click** the Update button.

    c. **Select** Browse.

    d. **Follow** the path: C:\Users\(userprofile)\Downloads, and **select** the WQXM-PG-4.1.0.7-image.gzhe file.

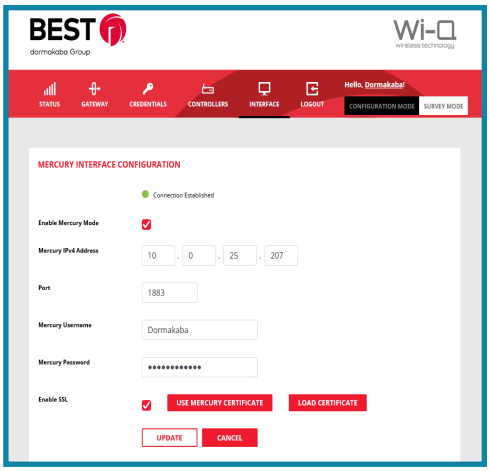
    e. **Select** Apply.

    The Gateway Web UI will close and the Wi-Q Gateway will upload the firmware.

> **NOTE**: *The Wi-Q Gateway will flash purple until the firmware is uploaded. Access to the Gateway Web UI will temporarily be unavailable. Once the firmware update is complete, the light will change to either a solid red or green, depending on if the Wi-Q is connected to DNA Fusion. The process could take several minutes.*

19. **Navigate** to the INTERFACE tab.
20. **Ensure** that the Enable Mercury Mode checkbox is checked.
21. **Insert** the SSP-LX's IP address into the Mercury IPv4 Address text field.
22. **Insert** the Port number (1883).
23. If the Port number was changed, **ensure** that the Port number in the SSP-LX's Configuration Manager matches.
24. **Enter** the Username and Password.

    Use the Username and Password configured in the Over-Watch page. See step 12 on page 6.
25. **Check** the Enable SSL checkbox.
26. In the INTERFACE page, **load** the .crt file that was used for the SSP-LX. See page 10.
27. **Click** the UPDATE button to save the configuration.

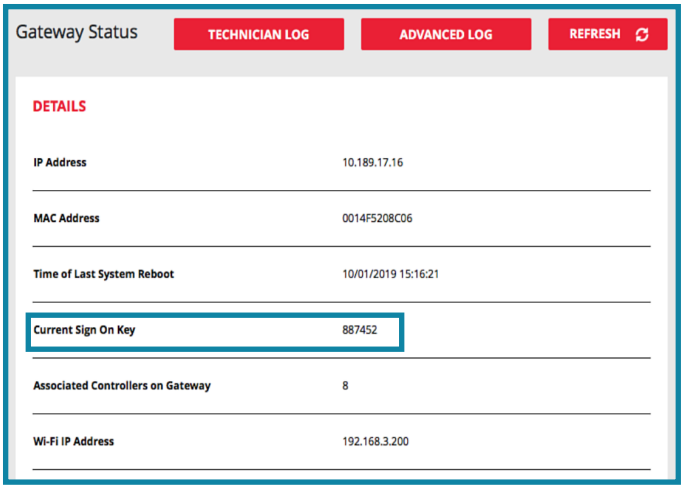


Configuring Certificates in the Gateway Web UI

1. On the Gateway Web UI, **locate** the INTERFACE page.
2. **Click** on the LOAD CERTIFICATE button.
3. **Select** BROWSE.
4. **Select** the .crt file that was used for the SSP-LX's Configuration Manager. See page 5.
5. **Click** on the APPLY button.

   The gateway will internally restart the MQTT Client. The MQTT Client will take roughly one minute to reboot and for the communication to be restored.
6. After the required certificates are loaded, **select** the STATUS tab in the Gateway Web UI.
7. **Ensure** that a Current Sign On Key is visible.

   The Sign On Key is required to link the door locks.



NOTE: *If no key is visible, ensure that all username and password combinations are correct. If all combinations are correct. The user should re-download the SSP-LX in DNA Fusion to "kickstart" the process even if the panel was already downloaded.*

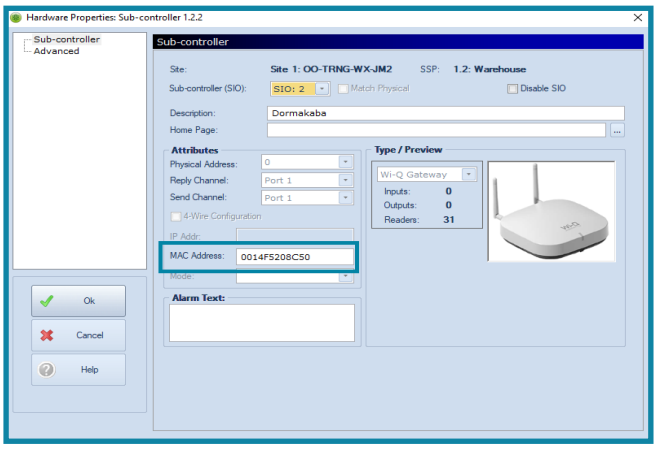
Adding Wi-Q Gateway to DNA Fusion

Open DNA Fusion:

1. **Right-click** the SSP-LX and **select** Add / Add sub-controller.
2. In the Type/Preview drop-down menu, **select** Wi-Q.
3. In the MAC Address text field, **enter** the Wi-Q's MAC address (letters must be Uppercase).

   See the STATUS page on the Gateway Web UI to see the Wi-Q's MAC address.
4. **Select** Ok and Yes to download the configuration.

   The Wi-Q Gateway's light will switch from red to green.



Configuring the Door Locks

The locks used in this guide are the Wi-Q™ Technology 9KQ Cylindrical lock.

1. From a Wi-Fi door lock, **press** 5678# and within three (3) seconds, **enter** the Sign On Key followed by the # key. See step 7 on page 10.

   Example: 5678#, then 837452#

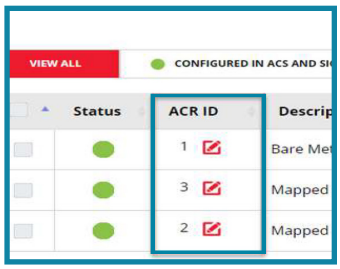
   The lock is now linked to the Wi-Q Gateway. The door lock is displayed at the bottom of the STATUS page in the Gateway Web UI.

> **NOTE**: *If the lock has been linked to another gateway, hard reset the lock. To hard reset the lock, hold the reset button on the back of the keypad reader for up to 30 seconds. After a green LED flashes three times. Then release the button.*

2. **Repeat** first step for any additional door locks.
3. **Select** the CONTROLLERS tab.
4. In the ACR ID column, **click** on the edit icon to the right of the number (not the Edit button in the Action column) to assign a door number link to DNAFusion.

   The ACR ID that is used will be the DNA Fusion Door number minus 1.

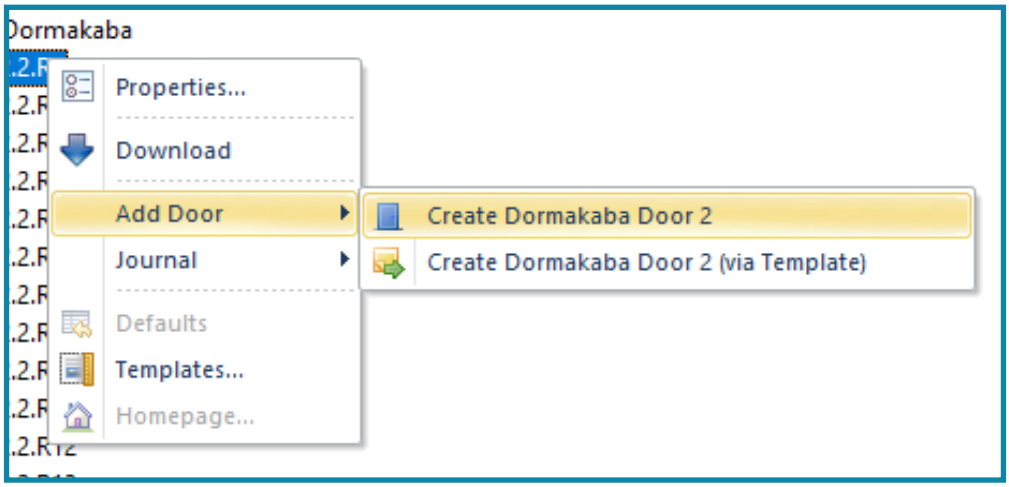
   Example: 1.1.D1 would be ACR 0, 1.1.D2 would be ACR 1.



Adding Door Locks in DNA Fusion

1. In the Hardware browser, **expand** Wi-Q Gateway.
2. **Right-click** on a reader and **select** Add Door / Create Dormakaba Door X.

> **NOTE**: *By default Reader 1 will create Door 1. The user can override that in the Door Configuration screen. Remember, the door number is important to link back to the ACR ID that was set up in the Controllers page of the Gateway Web UI.*

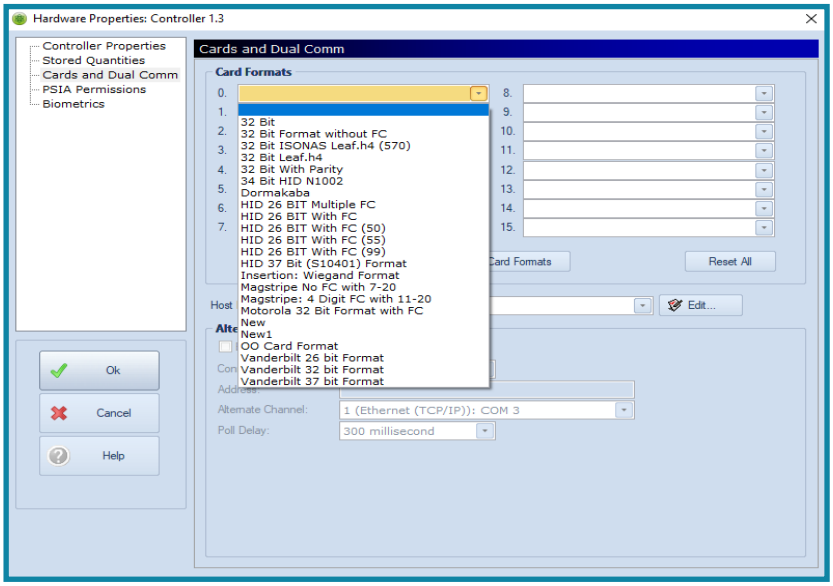


Card Formats

Card formats for the Dormakaba match Mercury card formats.

To add card formats in DNA Fusion:

1. **Right-click** on the SSP-LX.
2. **Select** Properties.
   The Hardware Properties dialog opens.
3. **Select** Cards and Dual Comm.
4. In the Card Formats drop-down menu, **select** the desired card format.



5. After the card format is selected, **click** Ok and Yes to download.
   The update may take 2 to 5 minutes until the lock can recognize the card format.

Index	Event Description	Card #	Last Name	First Name	Personnel Types	Event Data
137	Autosave of Cardholder database completed				NORMAL	Autosave Database code = 0
72	Access Granted: Door Used	1409	Castle	Frank	NORMAL	Fmt: 127 Cab: 0
243	Wi-Q Gateway Message				NORMAL	39 - Update Card Formats
243	Wi-Q Gateway Message				NORMAL	35 - Update User Parameters

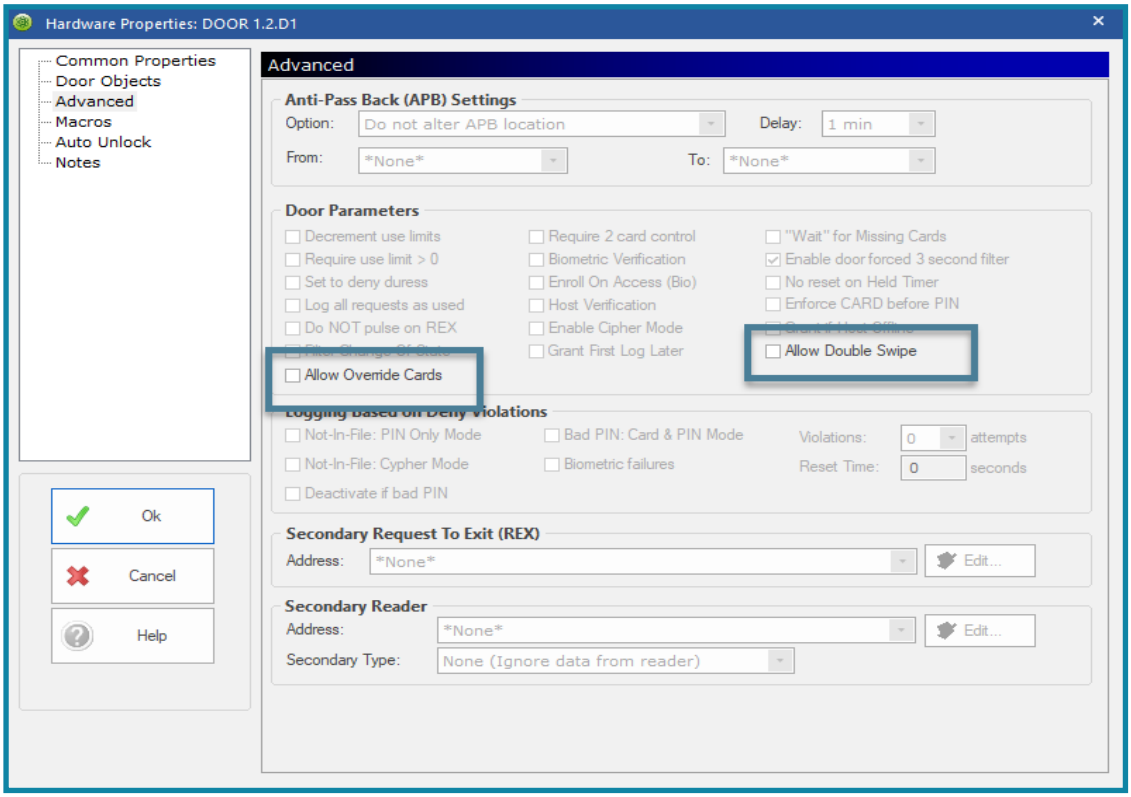
Additional Information

Door settings that are not supported are disabled in the Gateway Web UI. The door settings that are supported are listed below:

- Default Card Mode
- Strike Time
- Held Time
- Allow Double Swipe
- Allow Override Card

The Allow Double Swipe and Allow Override Cards door settings require additional configuration.

Enabling Double Swipe and Allowing Override Cards



The Allow Double Swipe and Allow Override Card parameters are not implemented the same way as standard controllers. The Allow Double Swipe parameter corresponds to Dormakaba's Passage Mode. This mode must be enabled at the door level and credentials must be configured to support Passage Mode.

To enable Allow Double Swipe to a credential:

1. **Select** the desired Personnel profile.
2. **Select** the Card tab.
3. **Set** Trigger Code 7 to 1.

To enable Allow Override Cards to a credential:

1. **Select** the desired Personnel profile.
2. **Select** the Card tab.
3. **Set** Trigger Code 6 to 1.

NOTE: *Ensure that the* Store Trigger Code *is checked in the SSP-LX's* Stored Quantities.

OPEN OPTIONS®
ACCESS TECHNOLOGY

16650 Westgrove Dr | Suite 150
Addison, TX 75001
Phone: (972) 818-7001

Publish Date | November 30, 2020
DNA Fusion Version | 7.8 or Greater
Manual Number | BDQSG 1.1

www.ooaccess.com