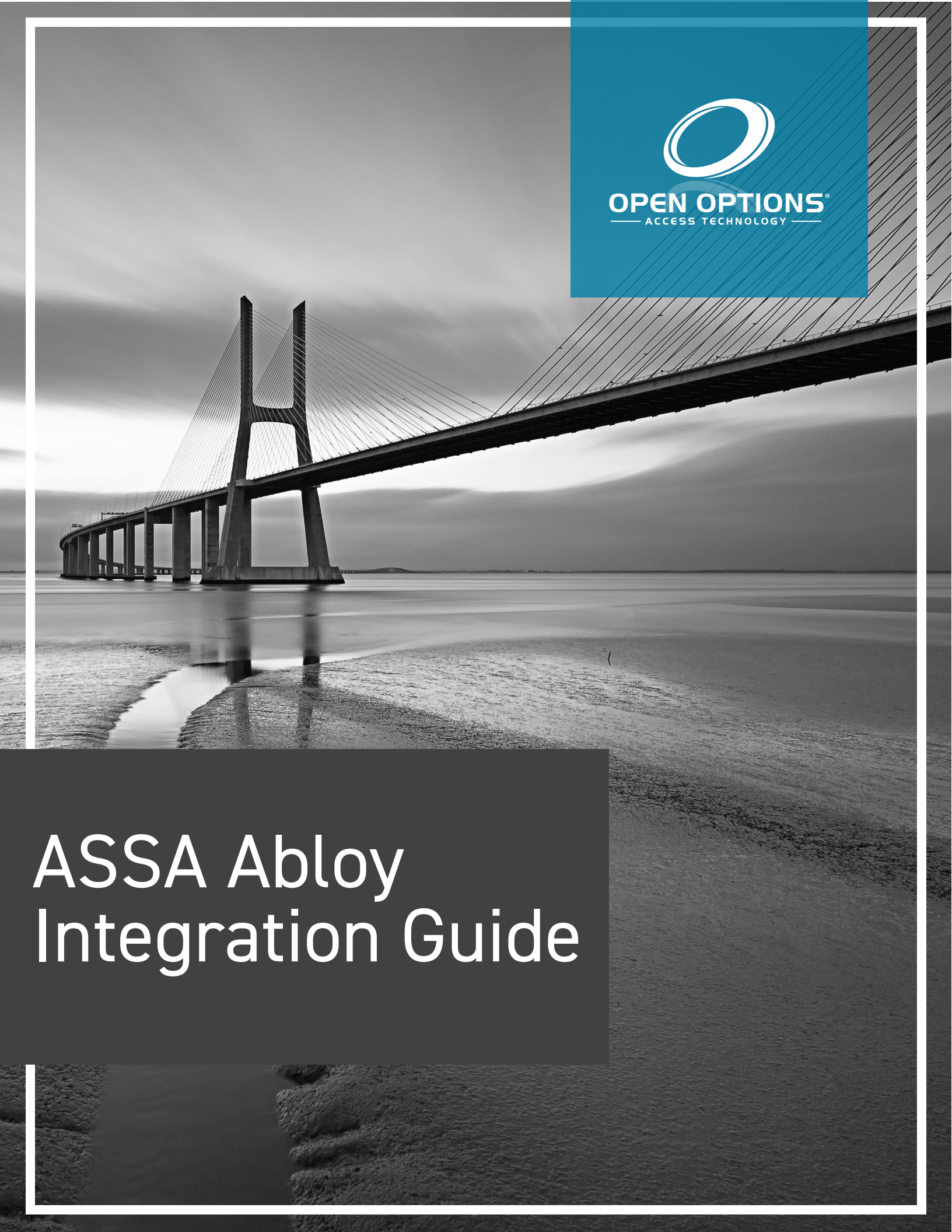


ASSA Abloy Integration Guide

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: September 28, 2020
Manual Number: AIG-1.0

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.

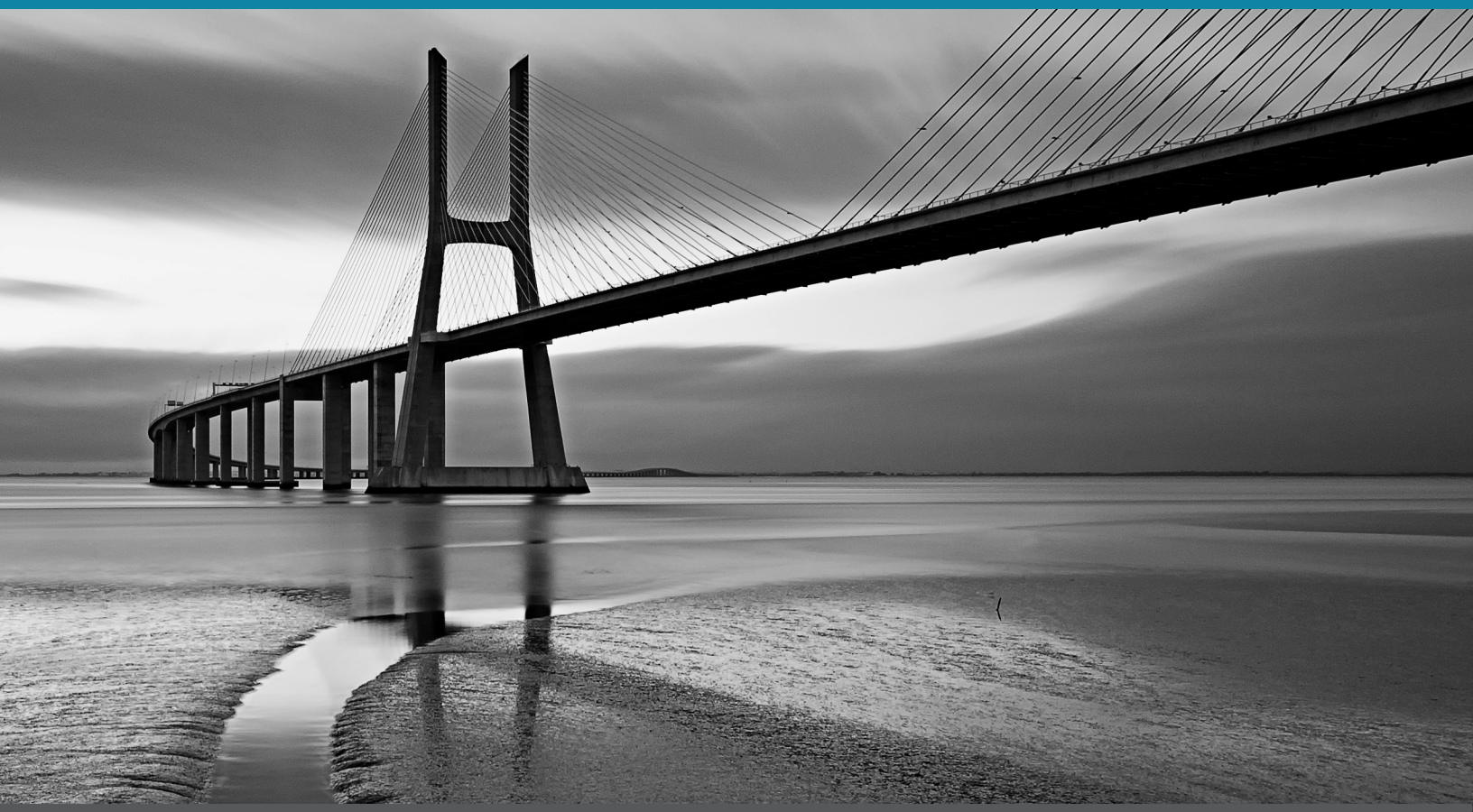
TERMINATION: Open Options may terminate this license at any time if licensee is in breach of any of its terms or conditions. Upon termination, licensee will immediately destroy the Software or return all copies of the Software to Open Options, along with any copies licensee has made.

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.

Table of Contents

Aperio Integration

Introduction



In This Section:

- Hardware Overview
- Software Overview
- Minimum Requirements

In this Guide

This guide explains how to integrate ASSA Abloy hardware with the DNA Fusion Access Control Software. The ASSA Abloy hardware covered in this guide include ASSA WiFi Locks, ASSA PoE Locks, and the Aperio WiFi Locks.

Aperio WiFi Lock

ASSA WiFi and PoE Locks (IN220)

Integration Instructions

Step 1: *Installing the DSR* - Install and configure the DSR on a server that is separate from the DNADrvr32. Configure the security settings of the DSR.

Step 2: *Installing The LCT and configuring the Locks* - Install the LCT and add ASSA locksets to the LCT and the DSR Support Tool.

Step 3: *Configuring the DSR and the ASSA Locks in DNA Fusion* - Add the DSR and ASSA locksets in DNA Fusion. Configure ASSA Access levels.

Aperio Integration - Adding the Aperio Hub and configuring the Aperio Lockset in DNA Fusion.

DNA Fusion/ASSA DSR

ASSA ABLOY developed the Door Service Router (DSR), which translates commands from the DNA Fusion access control system to the ASSA lock hardware. The DSR utilizes a Java-based web service that allows the lock to quickly and efficiently communicate with DNA Fusion for real-time monitoring.

Since communication between DNA Fusion and each lock uses the existing IP infrastructure via the DSR, a separate controller is unnecessary. All personnel information is configured in DNA Fusion and stored directly on the lock.

ASSA does not support earlier versions of the DSR. In that regard, the user's DNA Fusion version must support the most recent version of the DSR that ASSA supports.

Minimum Requirements

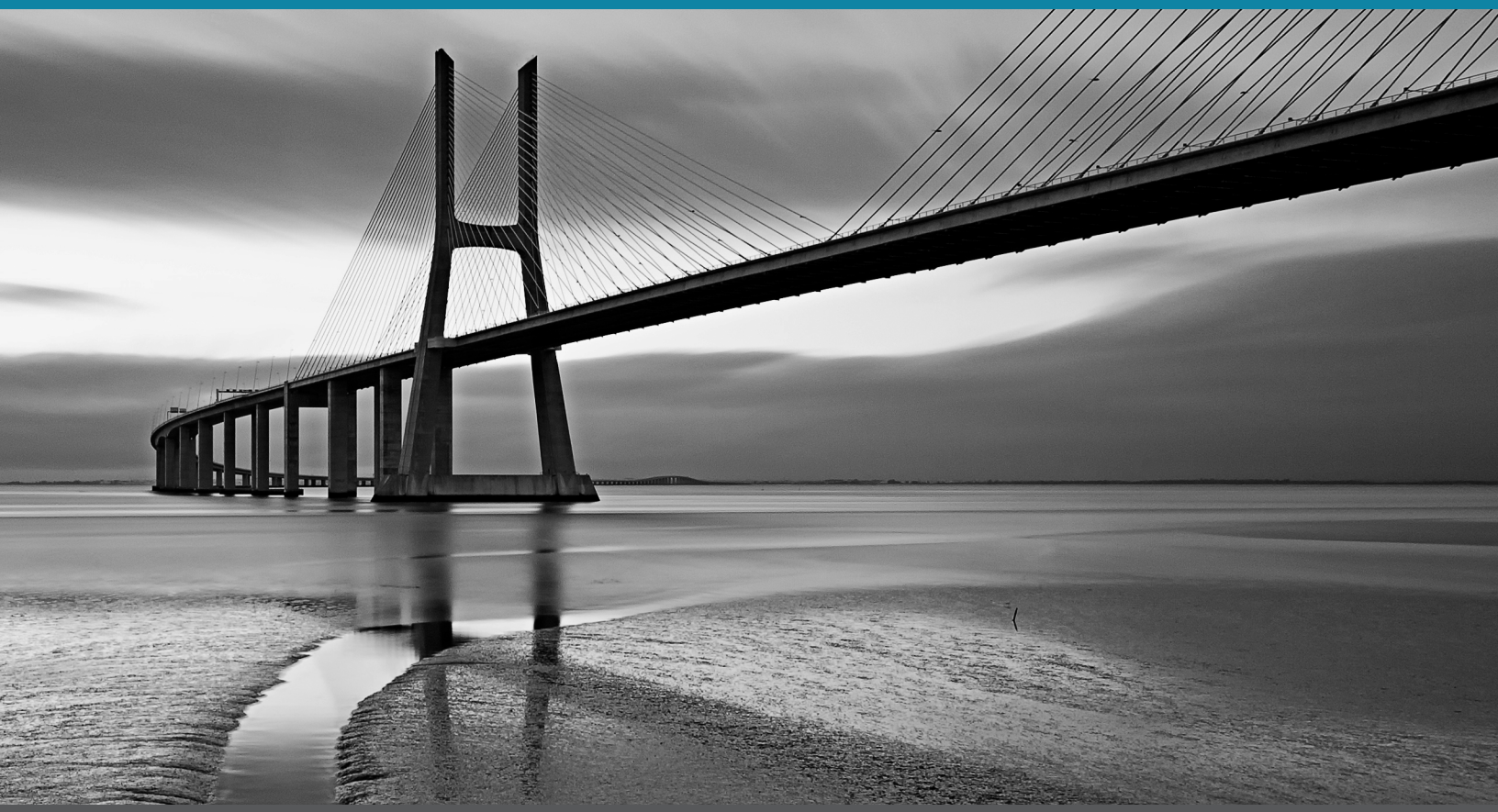
The ASSA Door Service Router (DSR) and the DNA Fusion Server must be installed on a separate Windows workstation, or on independent VM sessions.

Each DSR will support a maximum of 1,024 PoE and Wi-Fi locks, and DNA can communicate with multiple Door Service Routers if needed.

Parameter	Minimum Software Requirements
Operating System	Windows 10 Pro (64-Bit) or greater
DNA Fusion	Version 7.7 or higher
MS SQL	MS SQL Server 2012 or greater
Additional Applications (Installed with DSR)	Java Runtime Environment 1.8.0.51 (Installed with DSR) Apache Tomcat 8.0.21 (Installed with DSR)
• DNA ships with Microsoft SQL 2012 Express. SQL Express has a database size limit of 10 GB.	

Parameter	Minimum Software Requirements
Processor	Intel Core i3 (4 cores) or greater
System Memory (RAM)	8 GB
Hard Drive Size	5 GB Free Space
* Virtual machine environments must have the equivalent resource allocations	

Step 1: Installing the DSR

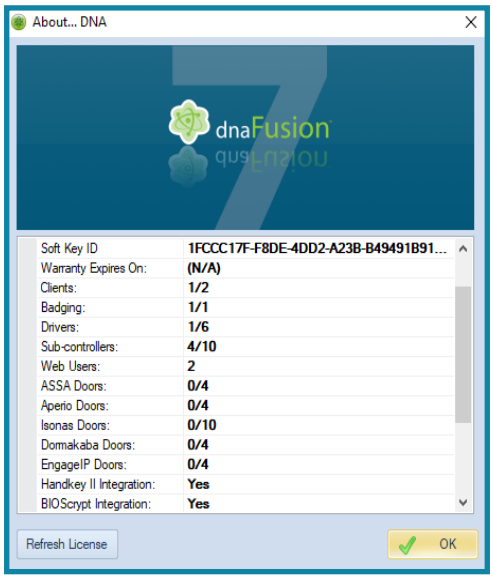


In This Section:

- DSR Oveview
- ASSA DSR Integration Installation
- Uninstalling the DSR

DSR Overview

The ASSA DSR integration is supported by DNA Fusion version 7.7 or higher. The integration requires the proper licensing to be in place prior to the installation of the integration software.



The ASSA ABLOY's PoE access control solution leverages an existing LAN for both power and data while their Wi-Fi locks use an existing Wi-Fi network. The following lock solutions are supported by the DSR.

Wi-Fi Locksets

- SARGENT Profile Series v.S2
- SARGENT Passport 1000 P2
- Corbin Russwin Access 700 PWI1
- Corbin Russwin Access 800 WI1
- Corbin Russwin IN120
- SARGENT IN120

PoE Lockset

- SARGENT Profile Series v.S1
- SARGENT Passport 1000 P1 & P2
- Corbin Russwin Access 700 PIP1
- Corbin Russwin 780 IP1

PoE locksets allow real-time command and control of the lock in DNA Fusion. They also provide live, real-time events utilizing existing infrastructure.

The Wi-Fi locksets leverage the wireless technology to communicate with locks. Wireless locksets are offline by nature which means the locks are not communicating with DNA in real-time. This communication path does not support real-time control or events from the lock.

Each DSR will support a maximum of 1,024 locks and DNA Fusion can communicate with multiple DSR's if needed.

Wi-Fi Lock Considerations

Wi-Fi locksets utilize the existing wireless infrastructure and communicate to the locks directly with no additional hardware required.

While the Wi-Fi locksets appear in the DNA Fusion hardware tree, there is no real-time command or control of the Wi-Fi locks. This also limits the ability to retrieve events in real-time. Events will appear once the locks communicate with the DSR and the events have been uploaded to the database. This can be configured in the DNA Fusion Door Properties Device Settings section of the ASSA lockset.

Wi-Fi locks operate using battery power, and only communicate on a specified schedule. If constant power is supplied, the lock will provide the same functionality as a PoE lockset.

PoE Considerations

ASSA PoE locksets utilize the existing network infrastructure and communicate to the locks directly with no additional hardware required.

The PoE locksets appear in the DNA Fusion hardware tree and offer real-time command, and control of the PoE locks. This also allows the lockset's events to be configured to initiate other types of functions, such as camera call up.

Network Considerations

When placing devices on the network, whether Ethernet or wireless, communication paths must be considered. Keep in mind that IP address ranges may vary from Ethernet to wireless networks. If the locks will be utilizing a wireless network for communication, the password for the network must be obtained for configuration purposes. If wireless is used, the server must be able to communicate with the wireless network as well as the internal network. It is important to work with the Information Technology department to ensure communication with the various networks.

Another consideration is port 8080, which is used to communicate with DNA Fusion and the DSR without encryption. If encryption is enabled, port 8443 is used for communication between the DNA driver and the DSR. Ensure the port selected for the DSR is also set in the DNA Fusion software.

Port 9000 must be opened on the server running the DNA Driver. This port is used to send status and event information from the DSR to DNA Fusion.

ASSA DSR Installation

The following tasks must be completed before the DNA Fusion/ASSA DSR integration will function properly.

Installation and Configuration Steps

1. **Install** the Door Service Router (DSR).

   This installation can be located by visiting ooaccess.com and selecting Resources > Software.

   An Open Options account is required in order to access the DSR software.

2. **Install** the Lock Configuration Tool (LCT).

   This is used to configure the locksets as well as define network parameters. Determine if the locksets will use DHCP or a static IP address.

3. **Program** the locksets using the LCT.

   This step will require connection to the lockset via USB cable.

4. **Add** the DSR to DNA Fusion.
5. **Install** and run the DNA DSR Utility.
6. **Verify** the lockset auto populates in DNA Fusion.
7. **Configure** the Door Properties.
8. **Create** ASSA Time Schedules and Holidays.
9. **Create** Access Levels for the ASSA locksets and **configure** ASSA Access Point Modes.

DSR Installation

Once the ASSA door hardware has been installed and wired, the ASSA DSR will need to be installed. The DSR installation process is very straightfoward and can be performed without any knowledge of the software.

> **NOTE**: *The DSR is required to be installed on a separate server or on an independent VM session from the DNA Fusion Access Control System.*

1. **Download** the DSRInstaller from www.ooaccess.com.
2. **Verify** the DNA Fusion DNADrvr32 Service Permissions.

   The DNA driver and the ASSA 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 and reference the DNA Fusion Technical Manual.

3. **Run** the DSRInstaller.

   The Introduction screen will open.

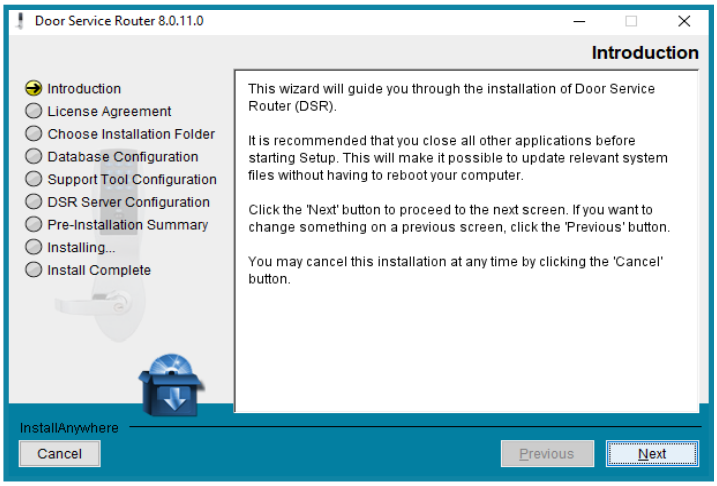
4. **Click** the Next button.

   The License Agreement screen opens.

5. **Select** the I accept radio button and **click** the Next button.

   The Installation Folder dialog appears.

   The default location is C:\Program Files\DSR.

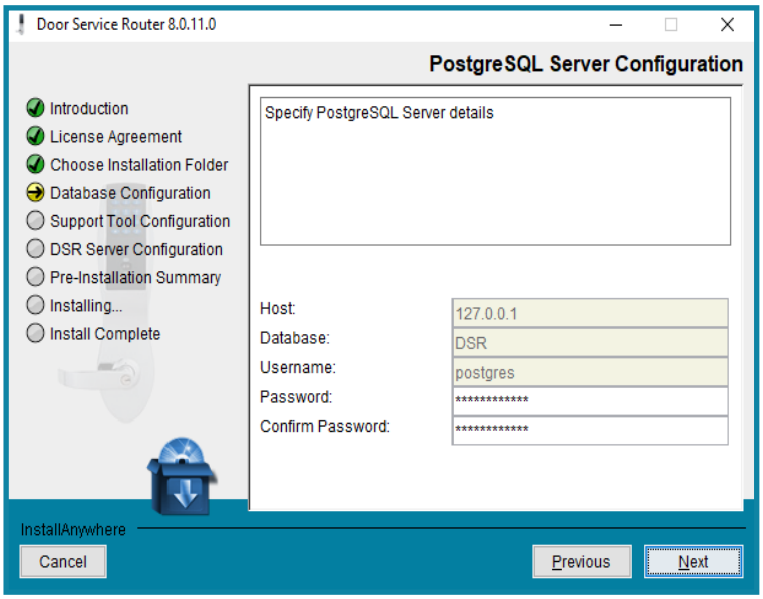


6. **Click** the Next button to continue the installation or **select** the Browse button and specify a different location.

   The Database Configuration screen appears.

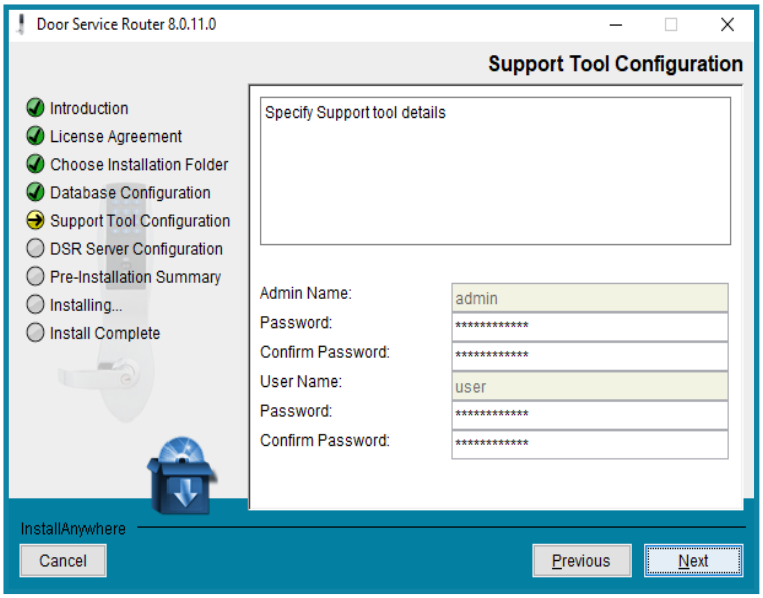
7. **Click** the Next button to continue the installation or **select** the Choose button and specify a different location.

   The default location is C:\Program Files\PostgreSQL\PostgreSQL94.



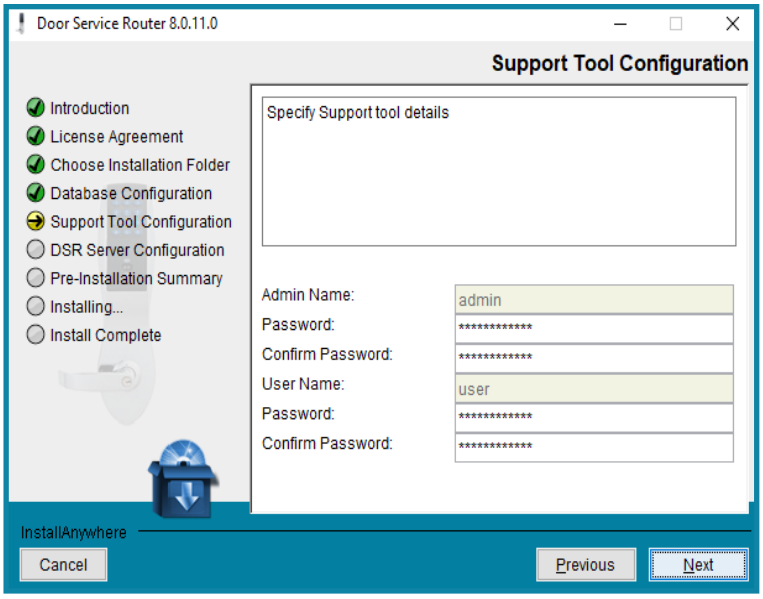
8. **Enter** a Password for the database, **re-enter** the password and **click** the Next button.

> **CAUTION**: *Remember to save the password in a secure location. There is no way to retrieve the password once it is set and will require re-installation.*



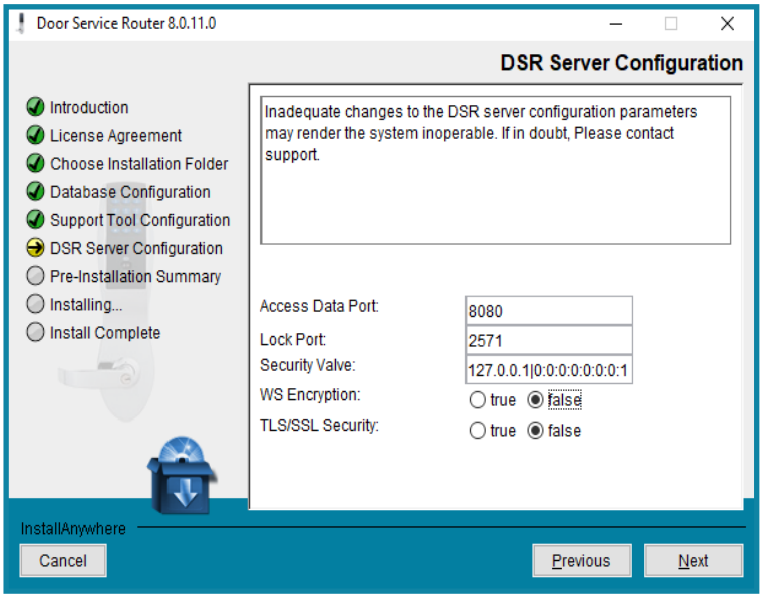
9. **Enter** a Password for the Admin account, confirm the password, and **click** the Next button.

   The password will be used to login to the ASSA Abloy DSR Support Tool.



CAUTION: *Remember to save the password in a secure location. There is no way to retrieve the password once it is set and will require re-installation. Information on Uninstalling is on page 1-7.*

10. **Set** the WS Encryption to False.
    WS Encryption is not supported in DNA Fusion.
11. If needed, **choose** whether to enable TLS/SSL security
    The DNA Fusion ASSA integration supports SSL/TLS Encryption. See page 1-7 for more information.
12. **click** Next.



Note: *If the default Data Port, 8080, is already in use, insert a different port.*

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

Note: *Restarting the system is required to complete the installation of the DSR. The IP address of the DSR Server is required for the configuration of the LCT.*

This Page Intentionally Left Blank

Additional Information

If a re-installation is required, the user will be required to uninstall the DSR and PostgreSQL. The method recommended by ASSA ABloy for uninstalling both is provided in this section. This section also provides information on how to enable SSL/TLS encryption for the DSR.

Basic DSR Uninstall

1. **Stop** communication between DNA Fusion and the DSR.
2. **Stop** Assaabloy DSR/Apache Tomcat service and DSR-Adapter service.
3. **Stop** PostgreSQL services.
4. **Uninstall** the DSR (and it's database, when prompted).
   Path: C:\Program Files\DSR\uninstall.exe or Programs.
5. **Restart** the machine when prompted.
6. After the machine restarts, **ensure** that PostgreSQL is only being used for the DSR.
7. If the PostgreSQL is only being used for the DSR, **uninstall** PostgreSQL.
8. **Delete** the DSR folder in the directory (c:\Program files).
9. **Delete** the PostgreSQL folders from the directory (C:\program Files and c:\Users).
   If this step fails, follow the Regedit Uninstall Process, if not, continue with step 10.
10. **Empty** the Recycling Bin.
11. **Uninstall** Java.
12. **Restart** the machine.
    The machine is ready for a fresh DSR install.

Regedit Uninstall Process

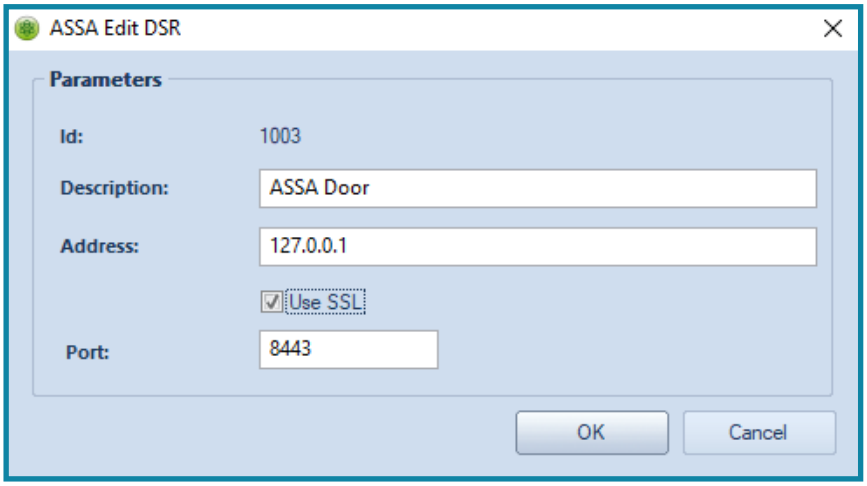
1. **Stop** communication between DNA Fusion and DSR**.**
2. **Stop** Apache Tomcat/Assa Abloy Door Service Router and PostgreSQL services**.**
3. **Uninstall** DSR and PostgreSQL**.**
4. **Delete** DSR folder in the directory (C:\Program Files\DSR).
5. **Delete** PostgreSQL folder(s) from directory (C:\Program Files and c:\Users).
6. **Delete** Postgre files from the directory (C:\Data).
7. Do a regedit uninstall of the DSR, Postgre, and PGadmin (Regedit Computer\HKEY_LOCAL_MACHINE\SOFTWARE and do a search and remove all DSR, Postgre, and PGadmin).
8. **Restart** the machine.
9. **Re-install** the DSR.
10. **Start** comm services.

SSL/TLS Encryption

Support for SSL/TLS is enabled with DNA Fusion version 7.7.0.67. This option can be turned on during the DSR installation as well as through DSR Support Tool. The WS Encryption feature is not supported.

1. From the DSR Support Tool interface, **select** Configuration Settings / Server Settings.
2. **Select** the WS Encryption & Port Configuration option.
   The WS Security & Port Configuration page opens.
3. **Set** TLS/SSL-Security option to true.
   The default port is 8443.

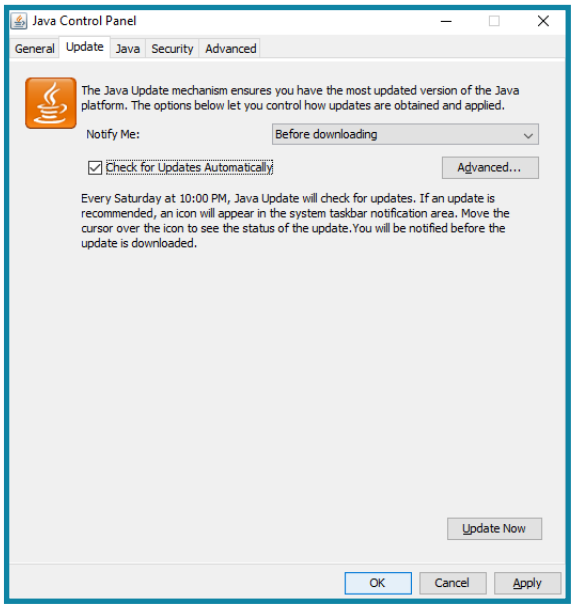
4. **Click** the Update Configuration button to save the setting.
   The DSR Restart dialog will appear. This dialog will prompt the user to start the DSR service.
5. **Click** the Ok button.
6. **Restart** the DSR service.
7. If needed, **change** the DSR Port in DNA Fusion.



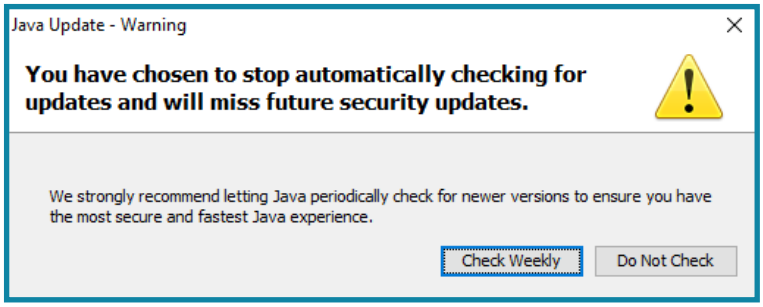
Disabling Java Updates

Java updates disable the ASSA DSR service. Follow the steps below to disable Java updates.

1. **Locate** the Java Control Panel.
2. **Select** the Update tab.



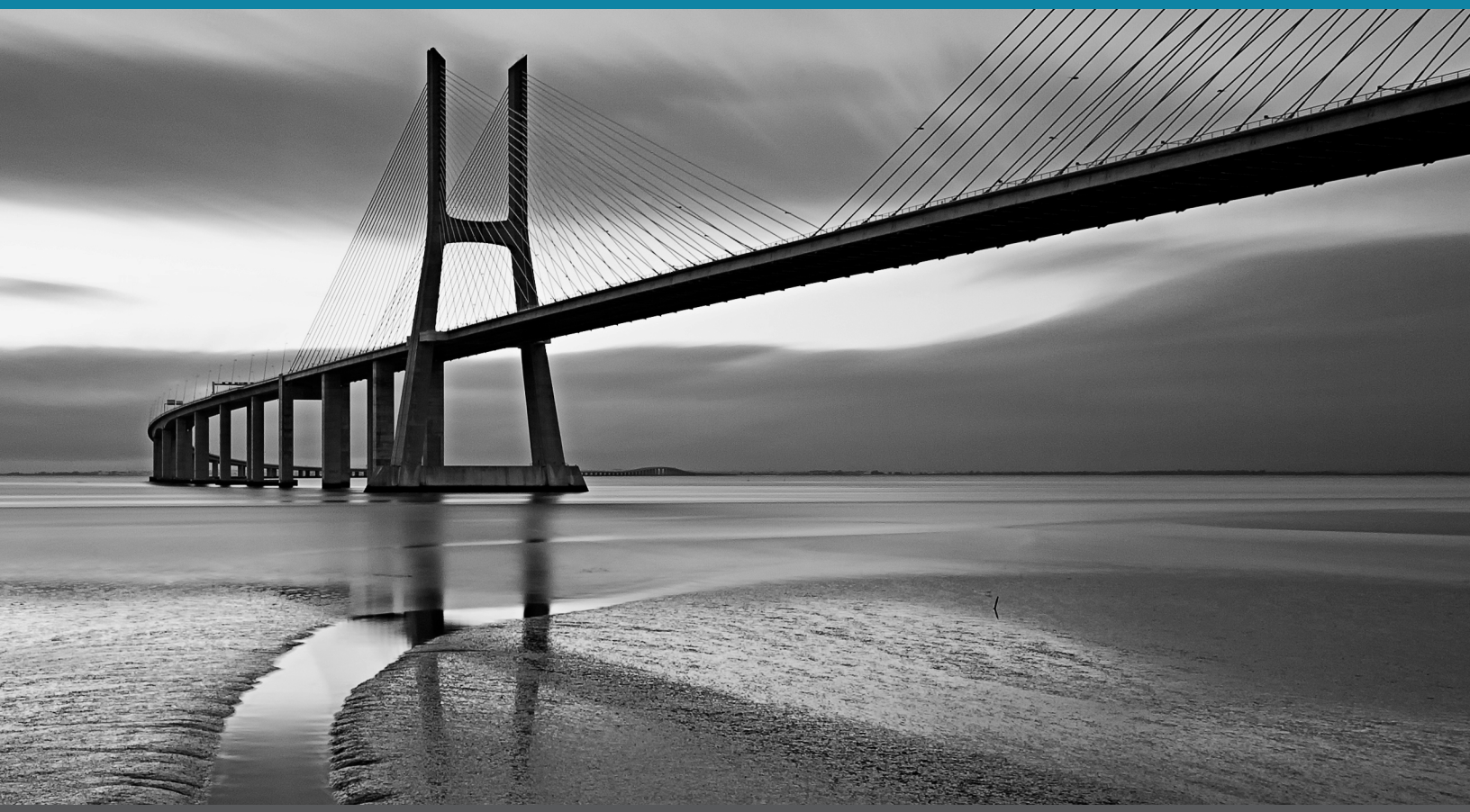
3. **Uncheck** the Check for Updates Automatically box.
   A Java Update - Warning opens.



4. **Select** Do Not Check.
5. **Click** Apply, then **select** Ok.

This Page Intentionally Left Blank

Step 2: Installing the LCT and Configuring the Locks



In This Section:

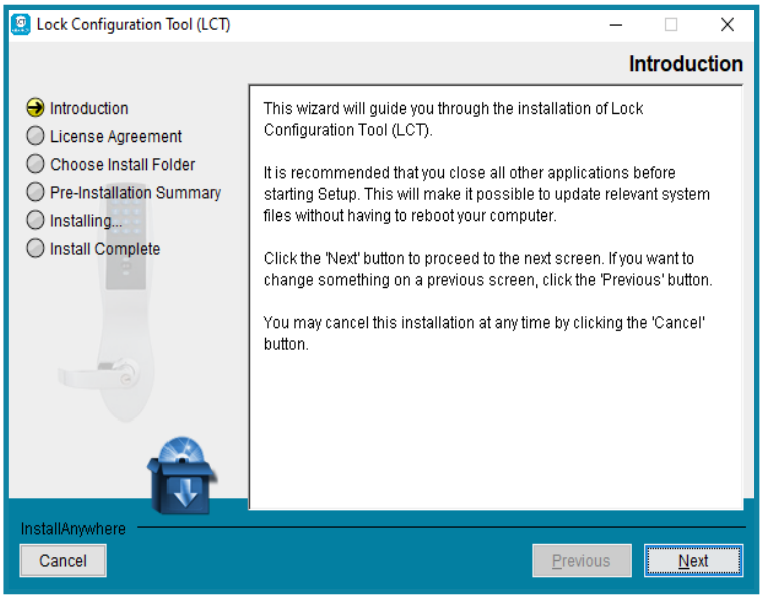
- LCT Installation
- Lock Configuration in the DSR
- DNA\DSR Utility
- DNA Fusion Service Permissions

ASSA Lockset Configuration Tool (LCT) Installation

Once the DSR installation is complete, the ASSA LCT software must be used to configure the locks. This software can be obtained from www.ooaccess.com.

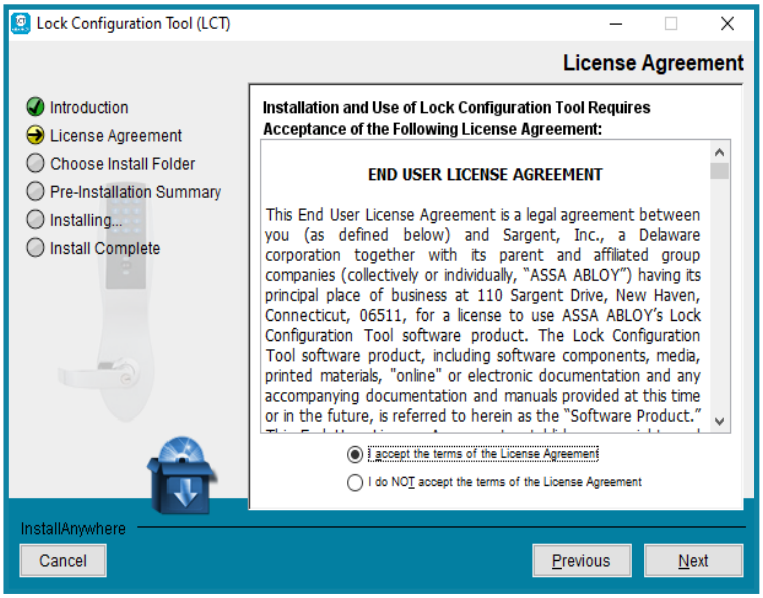
1. **Run** the Lock Configuration Tool (LCT).

   The Introduction screen will open.



2. **Click** the Next button.

   The License Agreement screen appears.



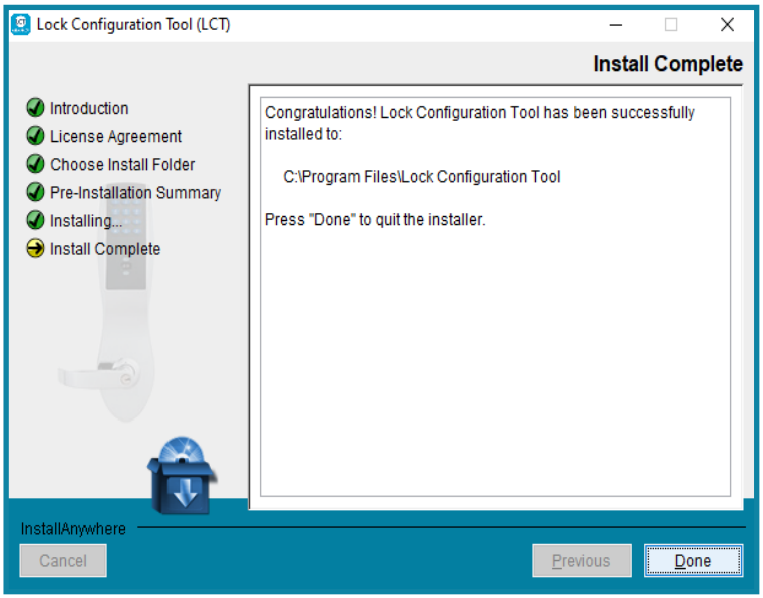
3. **Select** the I accept radio button and **click** the Next button.

   The Installation Folder dialog appears.

   The default location is C:\Programs Files\Lock Configuration Tool.

   The Pre-installation Summary appears.

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



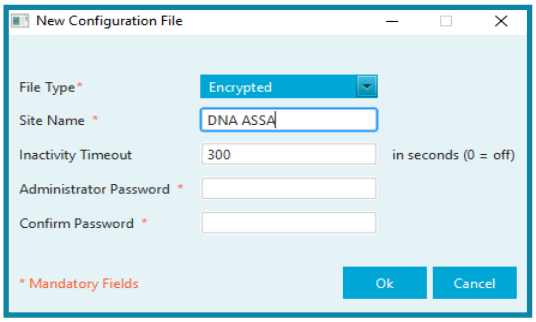
5. **Click** the Done button to complete the LCT installation.
   The installation is finalized.

Lock Configuration with the LCT

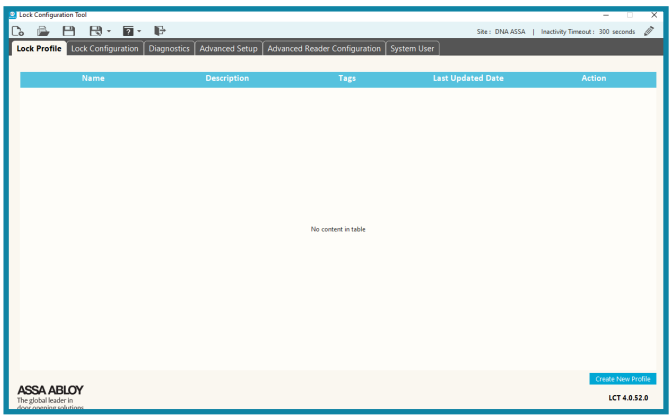
The network and locks must be configured using the ASSA ABLOY Lock Configuration Tool (LCT) software before they can be added to the DSR Support Tool.

Once this step is completed, the IT Administrator may need to take additional steps to allow the locks to communicate on the network. For more information, see the Lock Configuration Tool User Manual.

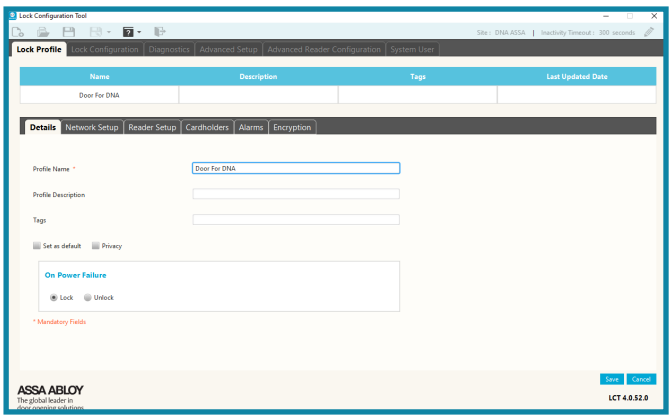
1. **Open** the LCT software .
   The Select Option dialog appears.
2. **Click** the Create button to add a new configuration file.
   The New Configuration File dialog opens.



3. **Enter** the Site Name and Administrator Password.
   Use the Password that was set in the DSR installation for the Admin.
4. **Re-Enter** the password and **click** the Ok button to create the configuration file.
   The Lock Profile opens.



5. **Click** the Create New Profile button.
   The Lock Profile Details page opens.



A lock profile consists of common configuration items that apply to a set of locks.

6. **Enter** a Profile Name, and if desired, a Profile Description for reference.
7. If needed, **check** the Set as Default option.

   If multiple profiles exist, the default profile will automatically be selected when configuring locks. If only one (1) profile exists, the system will automatically assign the default flag.
8. If desired, **check** the Privacy box to enable support for the Privacy button.

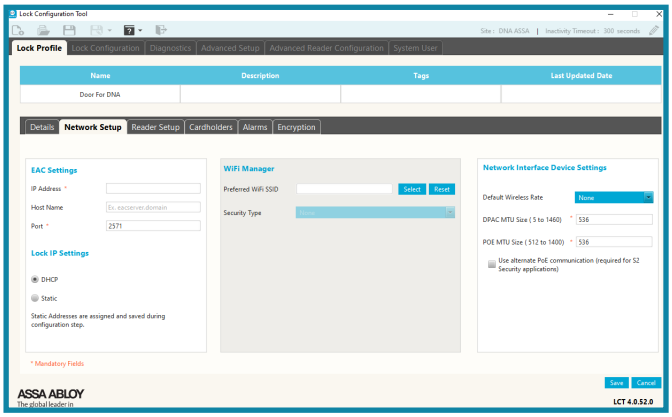
   If enabled, and a user presses the privacy button on the door, the door will only grant access to users with an access level that has been designated with the Deadbolt Override option. Pressing the privacy button on the door will end any passage mode, and secure the opening.
9. **Select** the Power Failure option: Lock or Unlock.

   The lock defaults to the selected state when power failure occurs.

Network Setup

1. **Select** the Network Setup tab.

   The Network Setup dialog appears.



2. In the EAC Settings section, **enter** the IP Address of the DSR server.

   The locks will use port 2571 to communicate with DNA Fusion.
3. In the Lock IP Settings section, **select** either the DHCP or Static.

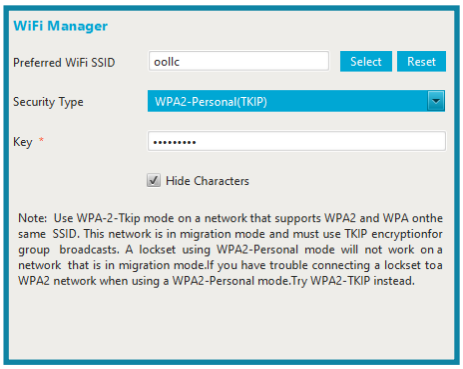
   This setting will determine how locks are assigned an IP address. If the Static option is selected, the locks IP address will be assigned and saved during the lock configuration.

For Wi-Fi Locks

4. **Click** the Select button, under the WiFi Manager section, to configure the network.

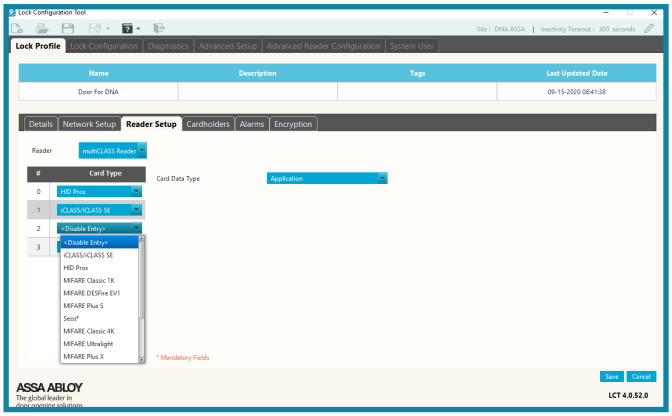
   The Select WiFi Network dialog opens.
5. **Select** the desired network from the list and **click** the OK button.

   The network appears in the Preferred WiFi SSID field.



Reader Setup

1. **Select** the Reader Setup tab.
2. **Select** the Reader Type from the drop-down menu.
   If multiCLASS is selected, up to four (4) Card Types can be selected.



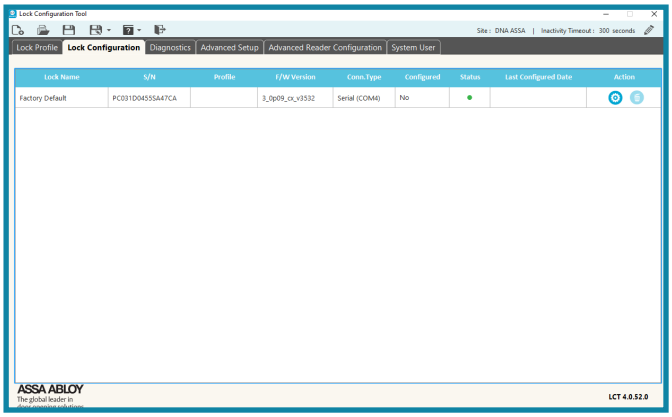
3. **Click** the **Save** button to save the profile.
   A Profile Saved confirmation dialog appears.
4. **Click** OK to continue.
   The Profile is saved.

Lock Configuration

Once a Lock Profile has been created, the locksets will need to be configured.

To access the Lock Configuration screen:

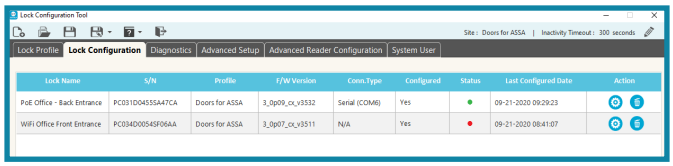
1. From the LCT main screen, **select** the Lock Configuration tab.
   The Lock Configuration page appears.



Configuring a Lock

The LCT main screen provides detailed information for both configured and unconfigured connected locks. The LCT scans the USB ports every 10 seconds, and automatically detects connected locks as well as displaying disconnected locks from the last scan.

Unconfigured locks are located at the top of the list for ease of navigation. Once a lock has been configured, the LCT maintains the configuration file in the list of locks.



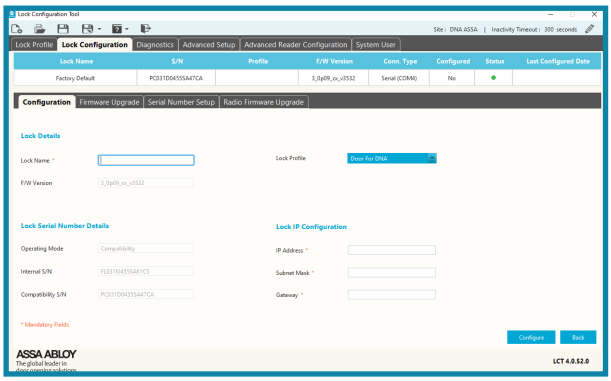
To access the configuration screen:

1. **Connect** the lockset to the computer via USB cable.

   The LCT will auto discover the lockset and populate the Lock Configuration dialog. A green circle will appear in the Status column.

2. **Select** the Lock Configuration icon.

   The Lock Configuration screen opens.

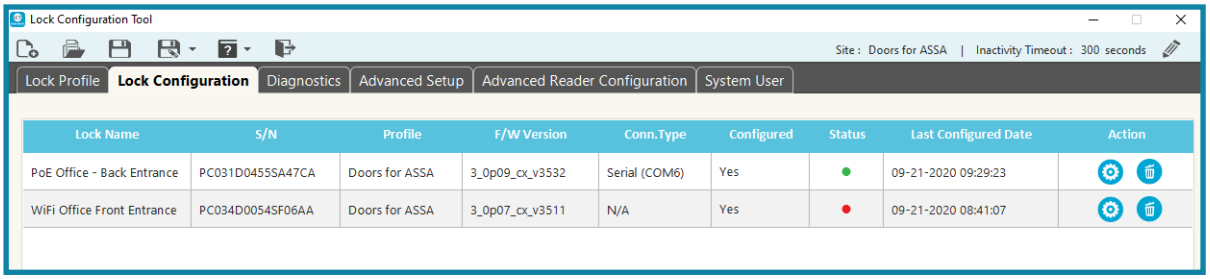


3. **Enter** a Lock Name.
4. If multiple profiles exist, **select** the desired Profile from the drop-down menu.
5. **Click** the Configure button to start the configuration process.

   When the configuration process is complete, a dialog will open confirming the success.

6. **Click** the Ok button to continue.

   The Main Configuration page is displayed and the lock's configuration status has been updated. The Last Configured Date column will reflect the date and time of the last successful configuration.



Upgrading Firmware

To upgrade the lock's firmware:

1. **Connect** the lock using the USB cable and open the Configuration page.

   The Lock Configuration dialog will appear.

2. **Select** the Firmware Upgrade tab.

   The Firmware section opens.

3. If needed select the Firmware version from the drop-down.
4. **Click** the Upload Firmware button.

   A confirmation dialog will appear.

5. **Click** the Ok button to continue.

   The firmware will be uploaded and a dialog will open confirming Success.

6. **Click** the Ok button to close the dialog.

> **Note**: *If DNA Fusion was recently upgraded, Open Options recommends updating the DSR version, as well as the Firmware.*

DNA DSR Utility

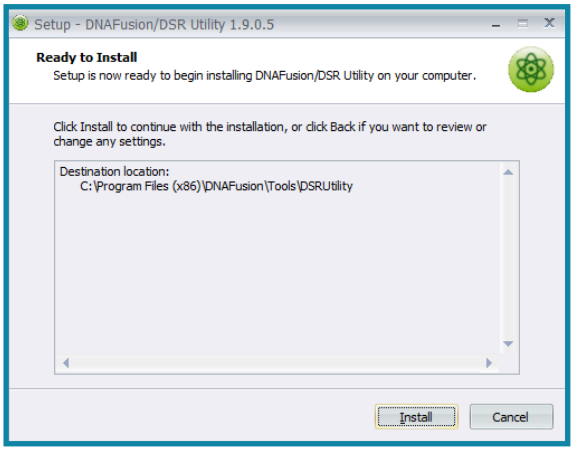
The DNA\DSR Utility is used to connect and synchronize the DSR. The most common function for this utility will be to Refresh the DSR after an upgrade and the data base type has been changed, moved to a new machine, or re-installed due to hardware failure. In all of those cases the DSR database is empty an the user needs to synchronize DNA Fusion with the DSR. This process will ensure the settings in DNA Fusion are updated in the DSR database.

Installation Prerequisites:

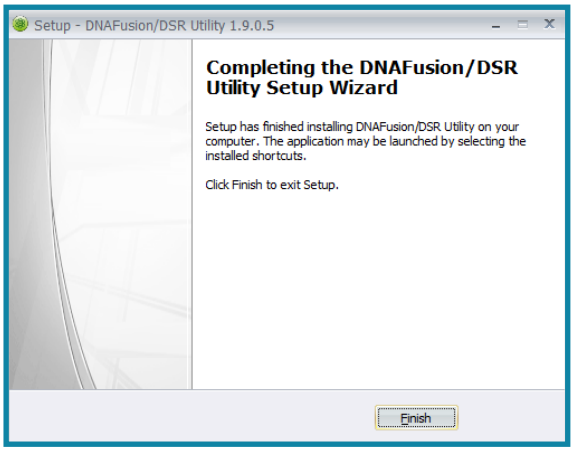
- Windows 10 Pro or higher
- .Net 4.5.2
- Must be installed on the DNA Server.

To install the DNA\DSR Utility:

1. **Locate** the DNA\DSR Utility installation file.
   The default location is C:\Program Files (x86)\DNA Fusion\Tools.
2. **Right-click** on the DNADsrUtilSetup file and **select** Run as administrator.
   The DNA\DSR Utility Installation will open.



3. **Click** the Install button to begin the installation.
   When the installation is done, a dialog will appear.
4. **Click** the Finish button to complete the installation.



An icon will appear on the desktop.

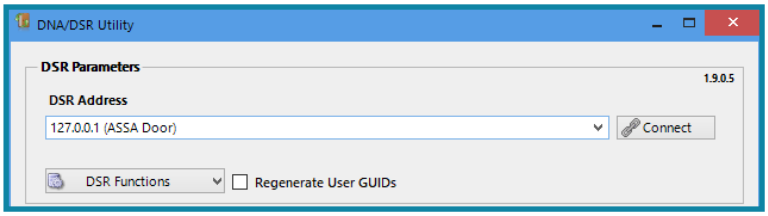
Configuring the DNA \ DSR Utility

1. **Locate** the DSR Utility application file.

   The default location is C:\Programs Files (x86)\DNA Fusion\Tools\DSRUtility.

2. **Right-click** on the DNADsrUtility file and **select** Run as administrator.

   The DNA\DSR Utility will open



3. **Click** the Connect button.

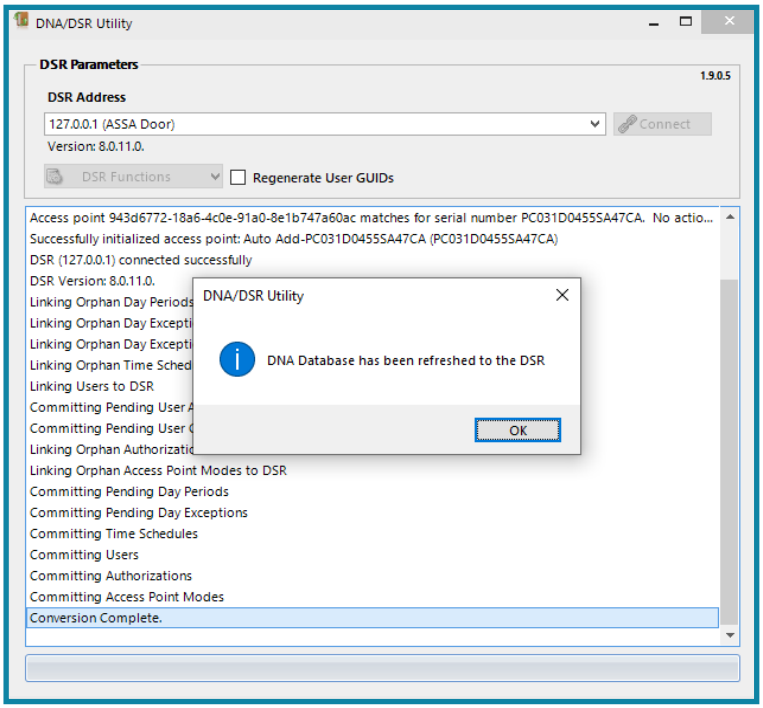
   A dialog will appear if the DNADrvr32 service is running. The service will need to be stopped to connect to the DSR.

4. **Select** Yes to continue.

   The DNA Driver is stopped and the DNA\DSR Utility is connected to the DSR.

5. From the DSR Functions drop-down, **select** Refresh DSR.

   The DSR will be refreshed; activity will be visible in the Utility window and a confirmation dialog will appear when complete.



6. **Click** the Ok button.

7. **Close** the DNA\DSR Utility.

   A dialog will appear with the status of the DNADrvr32 service. The service will need to be started to connect to the DSR.

8. **Click** Yes to restart the driver.

Follow the next step for ASSA configuration in DNA Fusion.

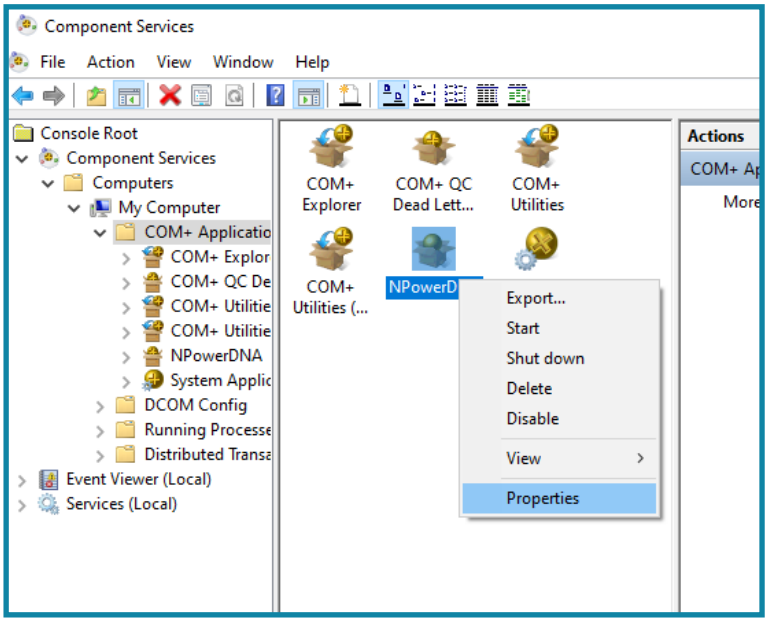
DNA Fusion Service Permissions

In order for the integration to function properly, the DNA Driver and COM+ objects, as well as the DNA User Group must be configured properly. This is imperative to the success of the integration.

COM+ Object

1. **Open** the Component Services menu on the server.
2. **Double-click** the Computer item.
3. **Double-click** the My Computer icon and **open** the COM+ Application folder.

   The COM+ Objects dialog appears.



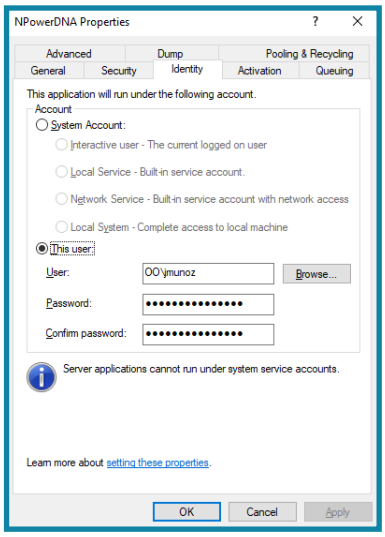
4. **Right-click** on the NPowerDNA object and **select** Properties.

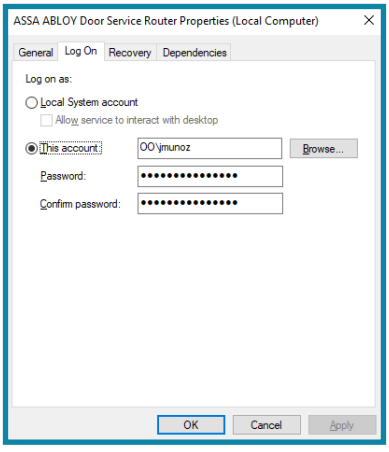
   The NPowerDNA Properties dialog opens.

5. **Select** the Identity tab, **verify** This user is selected and the User and Password fields are completed.

   If the objects permissions have not been configured, **enter** a local machine Administrative login information and **click** the Ok button.

   The ASSA ABLOY Door Service Router service will require the same information. This also applies to the DNA Driver (DNADrvr32) service.

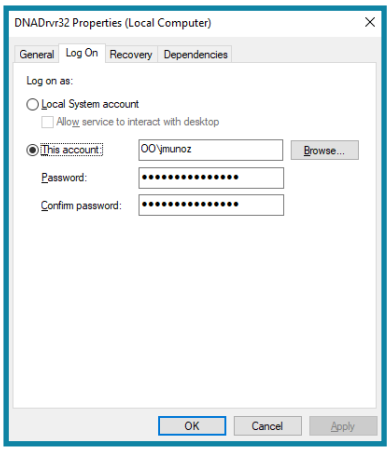




6. **Click** the Ok button.

DNA Fusion Driver Service

1. From the Component Services dialog, select the Services option or open the Services window.
   The Service dialog will populate.
2. **Locate** the DNADrvr32 service.
3. **Right-click** on the DNADrvr32 service and **select** the Properties option.
   The DNADrvr32 Properties dialog will open.



4. **Select** the Log On tab and **verify** the user configuration.

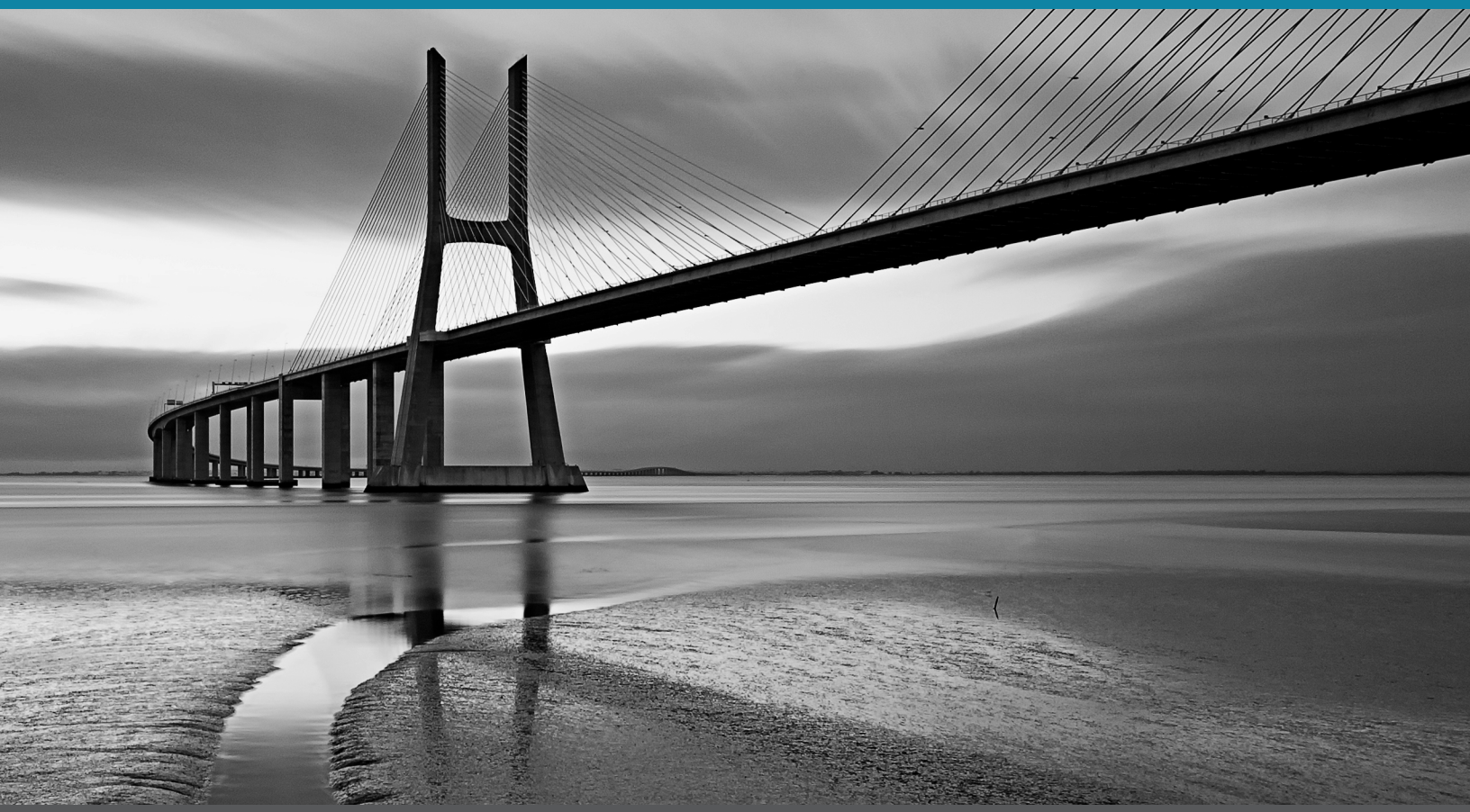
> **Note**: *The DNADrvr32 account must match the account used to operate the NPowerDNA COM+ Object as well as the ASSA ABLOY Door Service Router service.*

DNA Fusion User Group

1. **Right-click** on My Computer or This PC and **select** Manage from the menu.
   The Computer Management dialog appears.
2. **Expand** the Local Users and Groups options.
3. **Select** the Groups folder and **right-click** on the DNAUSERS group.
4. **Select** Add to Group from the menu.
   The DNAUSERS Properties dialog opens.
5. **Verify** the Service account is listed in the dialog.
   If the account is not listed, **click** the Add button and enter the account's information.
6. **Click** the Ok button to save any changes and close the dialog.

Step 3:

Configuring the DSR and ASSA Locks in DNA Fusion



In This Section:

- Configuring the DSR in DNA Fusion
- Adding ASSA Locks to DNA Fusion
- Configuring ASSA Locks in DNA Fusion

Adding the ASSA DSR to DNA Fusion

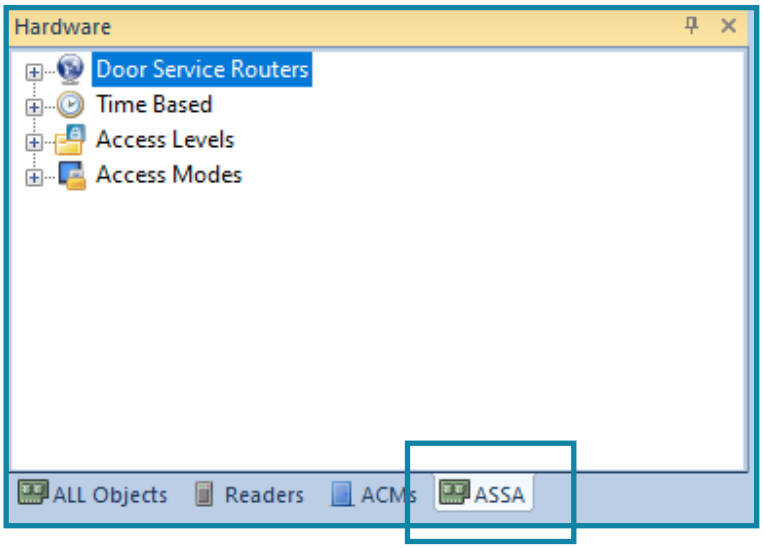
DNA Fusion communicates with a wide range of ASSA ABLOY Wi-Fi and PoE locking devices. Once the integration installation has been completed, connect the ASSA hardware to the network and configure the locksets within the DNA Fusion software.

Once the ASSA DSR has been configured, the DSR will need to be added to DNA Fusion.

1. With DNA open, **select** the Hardware browser button on the toolbar.

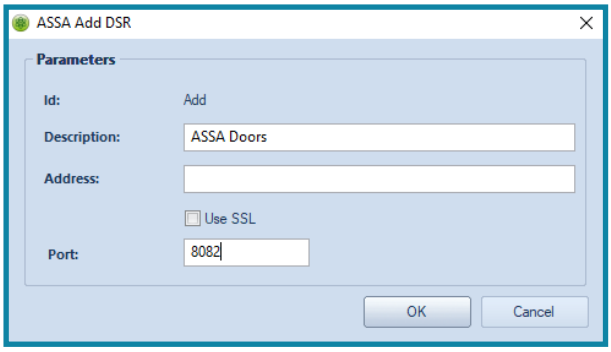
   The Hardware browser opens.

2. **Select** the ASSA tab at the bottom of the browser.



3. **Right-click** on the Door Service Routers option and **select** Add DSR from the menu.

   The ASSA Add DSR dialog will open.



4. **Enter** a Description for the DSR.
5. **Enter** the IP Address of the DSR Server.

   This information was obtained during the DSR installation. See page 1-5.

6. If needed, **check** the Use SSL checkbox to enable SSL.

   If enabled, SSL requires port 8443 to be configured for communication. See page 1-7 for more information.

7. **Click** the Ok button.

   The DSR is added to the Hardware browser.

8. **Verify** the driver status. See page 3-2 for more information.

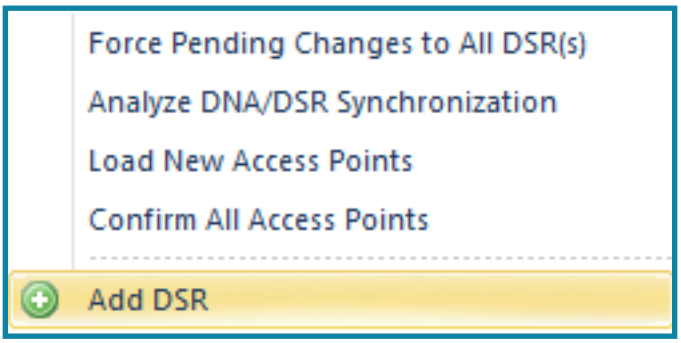
ASSA Driver Status

The ASSA driver is reflected by the color of the diamond in the 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 ASSA DSR services are running under the correct identity.

DSR Options

There are a number of options available for the DSR including the ability to analzye the data between DNA Fusion and the DSR.



To access these options:

1. **Right-click** on the Door Service Routers header in DNA Fusion.
   The DSR context menu appears.
2. **Select** the desired options.
   - Force Pending Changes to All DSR(s) - Pushes any pending changes to all Door Service Routers (DSRs).
   - Analyze DNA/DSR Synchronization - This tool analyzes the users, access levels, and access points to determine if there are any "out of sync" issues. If selected, the ASSA DSR Analyzer opens. This dialog provides an option that will attempt to repair any detected issues. A severity warning will be displayed to indicate the level of the issue that was repaired. View the tooltips contained within the log files. Once complete, a Force pending Changes to All DSRs should be performed.
   - Load New Access Points - Forces new locks to be displayed in the Hardware browser.
   - Confirm All Access Points - Allows for the confirmation of all locks instead of confirming on an individual lock basis.

Adding the ASSA Locksets to DNA Fusion

ASSA locksets will automatically be detected when they are connected to the network. The locks will communicate with the DSR during the LCT configuration, and will automatically be detected by DNA Fusion. Once the devices have been discovered, they will need to be confirmed in DNA Fusion to configure the door properties.

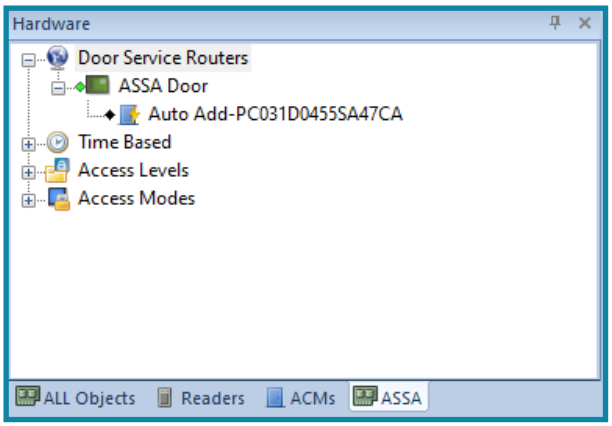
1. With the Hardware browser open, **select** the ASSA tab at the bottom of the browser.

   The ASSA tab opens.

2. **Connect** the ASSA lockset to the network (PoE or Wi-Fi) that will communicate with the DNA Fusion server.

   When an ASSA Abloy Lockset is connected to the network, DNA will automatically add the device to the Hardware browser. The service uses a UDP broadcast service to connect to devices.
   They appear in the Hardware browser with the MAC Address and Auto Add as the description.

   The devices will need to be confirmed to start communicating with the lock.



3. **Right-click** on the door and **select** Confirm.

   The door state and the diamond color will change. The color represents the door status.

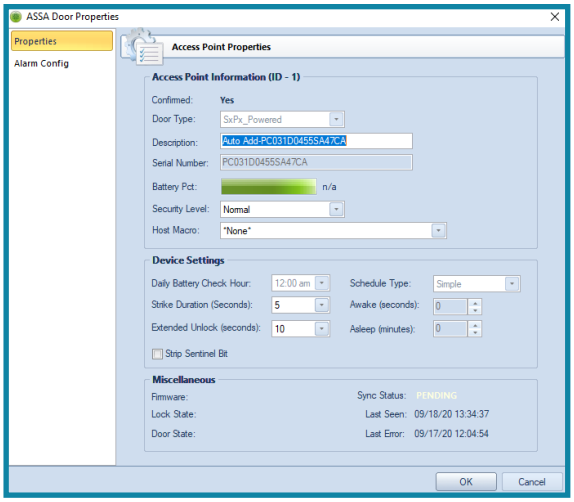
4. **Continue** to confirm the remaining ASSA doors.

   Once the door has been confirmed, the properties may be edited.

Configuring the ASSA Doors

Once the lockset has been confirmed in DNA Fusion, the door settings can be configured.

1. From the ASSA tab in the Hardware browser, **right-click** on the ASSA Door and **select** Properties from the menu.



   Depending on the lockset, Wi-Fi, or PoE, the properties dialog will vary slightly.

2. **Enter** a Description for the door.

   The default name is the Serial Number of the device. This name will appear in the Events Grid as well as, be used in any references to the door. The description is auto-populated when the device is auto-added.

3. **Select** the correct Security Level from the drop-down list.

   Category designation. All administrator to restrict operator use in the Operator Profiles.

4. If configured, **select** a Host Based Macro from the drop-down list or **click** the Edit button.

   If the Edit option is selected, the Host Based Macro Editor will open.

5. For Wi-Fi locks, **select** the Daily Battery Check Hour and the Schedule Type.

   Wi-Fi locks communicate on a schedule since they are not generally always communicating with the DSR.

   Simple - If selected, **set** the Awake (Seconds) and Asleep Time (Minutes). This will define the period of communication (Awake) as well as the interval between communication (Asleep). The Asleep period is determined from the last lock online event time. This is the default setting for most installations.

   Always On - The lock will communicate continuously. If the lock is battery powered, this setting will drain the batteries quickly (typically in one (1) day).

   Always Off - If selected, the lock will not communicate with the DSR. No event will trigger communication to start.

   COMM User Only - A COMM User is a cardholder that has been assigned an ASSA Access Level that has been designated as a Wakeup/COMM Access Level Type. Only a COMM User will trigger the lock to establish communication. If selected, an access level must be created, and assigned to a cardholder for the purpose of "waking up" the lock to begin communication.

6. **Configure** the Strike Duration (0-255 Seconds).

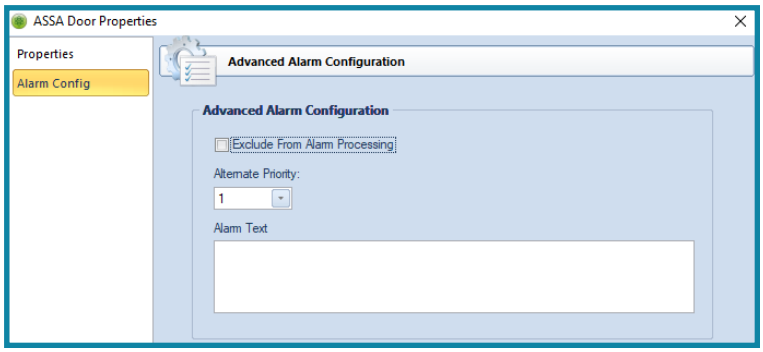
   The number of seconds the door will remain unlocked when a valid credential is presented.

7. **Set** the Extended Unlock (Seconds) Time.

   Determines the amount of time for cards that have been flagged with ADA.

8. **Select** the Alarm Config tab.

   The ASSA Advanced Alarm Configuration dialog opens.



9. If desired, **select** the Exclude From Alarm Processing checkbox

10. If desired, **select** an Alternate Priority and **enter** Alarm Text.

    If Alternate Priority is configured, it will override the default event specific Alarm Priority set in DNA / Administrative / Alarms and Events / Logging. The alternate ID will be displayed in the Alarm Grid.

11. **Select** the WiFi Triggers tab.

    The Access Point WiFi Triggers dialog appears.

12. **Check** the desired WiFi Trigger options.

    These options determine what conditions trigger the WiFi lock to wake up and report status to DNA Fusion as well as download changes.

12. **Click** the OK button to save the changes to the DNA Fusion system.

    The door will appear in the Hardware browser. If the door appears grayed out, it has not been confirmed.

13. To confirm the door, right-click on the door and **select** the Confirm option. If the door appears yellow, **right-click** on the door and **select** Initialize Device.

    Doors must be confirmed before the ASSA service will start to communicate with them.

Setting Up ASSA in DNA Fusion

There several of items that must be configured in the DNA Fusion system that are specific to the ASSA DSR integration. This includes the following items:

- Time Based Schedules
  - Day Periods
  - Holidays
  - Holiday Groups
  - Time Schedules
- Access Levels
- Access Modes

Configuring Time Based Schedules

Time based schedules are used to create access levels for cardholders as well as access modes for ASSA doors. These schedules include Day Periods, Holidays, Holiday Groups, and Time Schedules.

Day Periods

A day period is defined as time periods and associated days of the week. Once created, these Day Periods are combined with holidays to create Time Schedules. Time Schedules are associated with Access Levels and Access Modes.

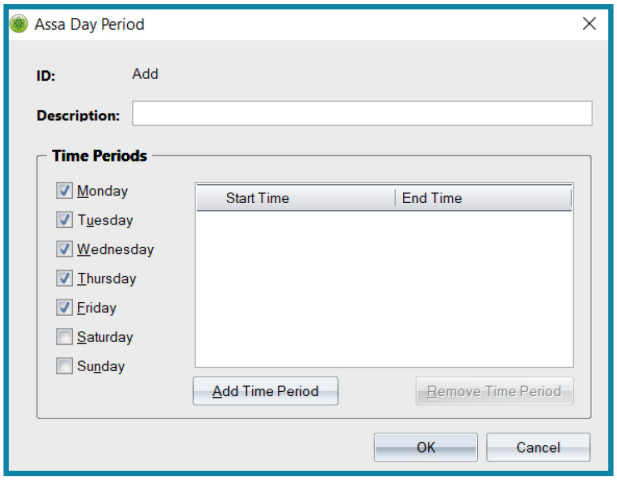
To add a Day Period:

1. From the ASSA hardware tab in the Hardware browser, **expand** the Time Based header by clicking the plus sign (+).

   The Time Based categories are displayed.

2. **Right-click** on the Day Periods header and **select** Add Day Period.

   The Assa Day Period dialog opens.



3. **Enter** a Description for the Day Period.
4. If needed, **check** or **uncheck** days of the week. Monday through Friday are selected by default.
5. **Click** the Add Time Period button.

   A time interval field is added.

6. **Enter** the Start and End Time periods for the schedule.
7. If needed, **configure** additional time periods.
8. **Click** the OK button to save the Day Period schedule.

   The Day Period is added to the ASSA hardware tab.

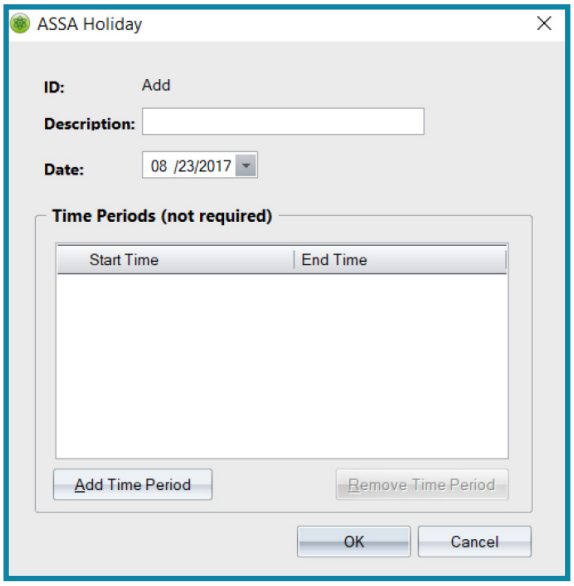
Holidays and Holiday Groups

Holidays for ASSA DSR locks are building blocks for Holiday Groups. A holiday must be created prior to the inclusion in a Holiday Group.

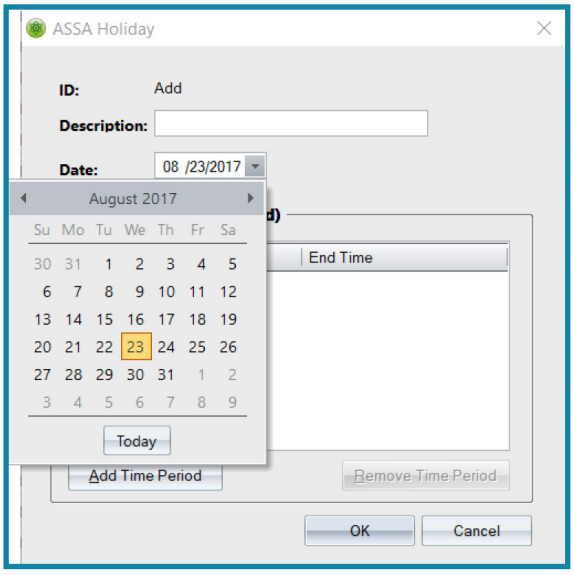
Time periods can be associated with holidays to limit the hours, and create partial days. When a day is specified as a holiday, it is treated differently by the system than a regular day (M-Su). Holidays are defined by the date and, if needed, the duration time for the holiday.

To create a Holiday:

1. From the ASSA tab in the Hardware browser, **right-click** on the Holidays header and **select** Add Holiday.
   The ASSA Holiday dialog opens.



2. **Enter** a Description for the holiday.
3. **Click** the down arrow in the Date field.
   A calendar appears.



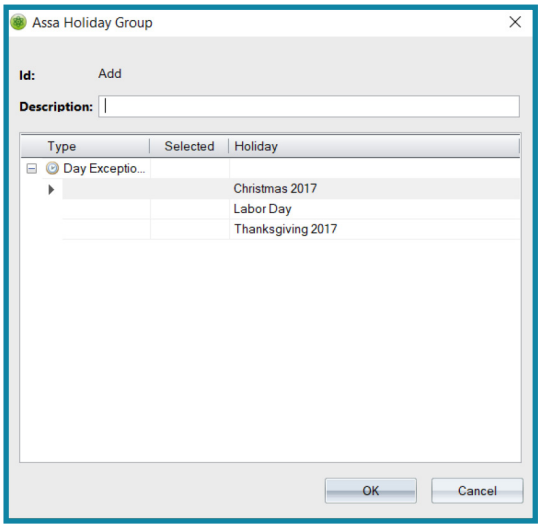
4. **Select** the date from the calendar.
   The date is populated in the Date field.
5. If needed, **click** the Add Time Periods button to define a time for the holiday and **enter** a Start and End Time.
   If no time period is specified, the holiday will cover the entire 24 hours of the selected date.

6. **Click** the OK button to save the holiday.
   The holiday is added to the Holidays subheader in the Hardware browser.
7. **Associate** the holiday with a Holiday Group.

To create a Holiday Group:

Holiday groups are part of a Time Schedule and must be defined to configure the time schedules.

1. **Right-click** on the Holiday Group header and **select** Add Holiday Group.
   The ASSA Holiday Groups dialog opens.

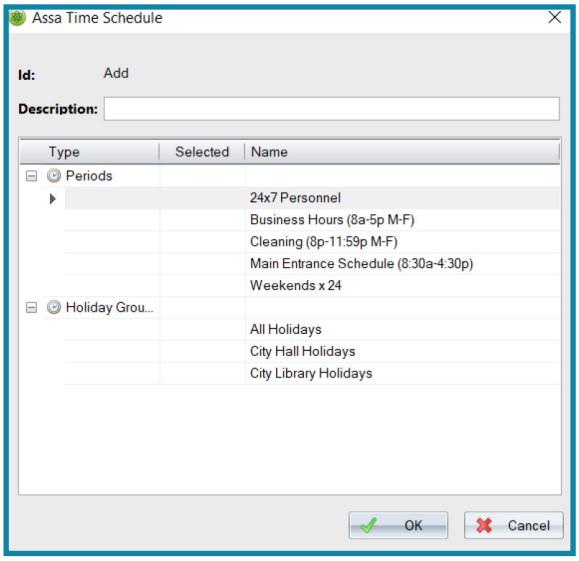


2. **Enter** a Description for the group.
3. **Check** the Selected column for the desired holidays.
4. **Click** the OK button to save the Holiday Group.
   The new holiday group is added to the Holiday Groups subheader.

Time Schedules

Time schedules are defined day periods and, if needed, associated holiday groups. Once created, time schedules are used to create Access Levels for cardholders, and Access Modes for doors.

1. From the ASSA tab in the Hardware browser, **right-click** on the Time Schedules header and **select** Add Time Schedule.
   The ASSA Time Schedules dialog opens.



2. **Enter** a Description for the time schedule.
3. **Select** the desired Day Period by checking the Selected column.
4. If needed, **check** the Holiday Group to associate with the Time Schedule.

   This creates a relationship between the day and time (Day Period: Monday-Friday) and the holiday dates (Holiday Groups: specific date).
5. **Click** the OK button to save the Time Schedule.

   The Time Schedule is added to the Hardware browser.

Creating ASSA Access Levels

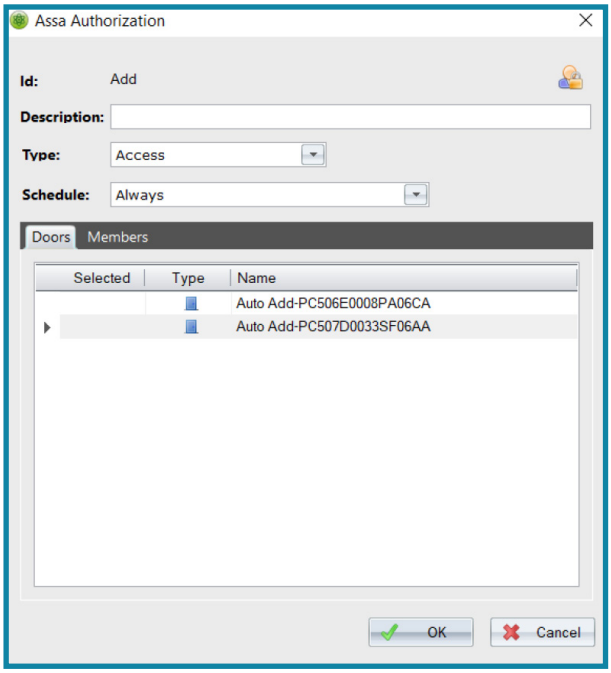
An Access Level consists of an ASSA door and an associated time schedule. When the access level is added to a card record, it determines where and when the cardholder has access within the system.

Access Levels can be grouped together for ease of distribution. Access Level Groups can be added to individual cards or groups of cards in the system. This section covers how to create and modify ASSA access levels as well as creating Legacy Access Level Groups.

To create an ASSA Access Level:

1. From the ASSA tab in the Hardware browser, **right-click** on the Access Levels header and **select** Add ASSA Access Level.

   The ASSA Authorization dialog opens.



2. **Enter** a Description for the access level.
3. If desired, **select** the access Type from the drop-down list.
   - Access (Default) - Standard access
   - Wakeup/COMM - Used for WiFi locks to initiate communication to the DSR and does not grant access to the selected locks. This can be used to push changes to the lock since WiFi locks are not online all the time. Typically WiFi locks "wake up" on a schedule that is set in the Door Properties.
   - Access - Override Deadbolt - Credentials assigned an Override access level will have access to the door in Lockdown mode as well as if the deadbolt has been engaged from the secure side of the entry.
   - Double Swipe - Provides the functionality to toggle the door from a Locked state to an Unlocked state or vice versa with the double swipe of a credential. Any user assigned an access level defined as Double Swipe will have the ability to change the state of the door.

If the lock type is a px, the door will remain in the toggled state until the associated Time Schedule deactivates. For IN 120 locks running in px compatibility mode, the door will return to the locked state at the end of the time schedule. However, sx lock types do not automatically return to the locked state when the associated time schedule deactivates.

Note: *While DNA Fusion and the DSR support a wide array of Locksets (Sargent, Corbin, Russwin), this feature is not available in all locksets.*

4. **Select** the Time Schedule from the drop-down list.

   Time schedules will need to be created prior to adding the access level. Open Options recommends time schedules be programmed for hardware and personnel separately.

5. **Check** the Selected column to add a door(s) to the access level.

   The Members tab will display the cardholders that have been assigned the selected access level.

   Once ASSA Access Levels have been created, Legacy Access Level Groups can be created to group access levels for ease of distribution to cardholders.

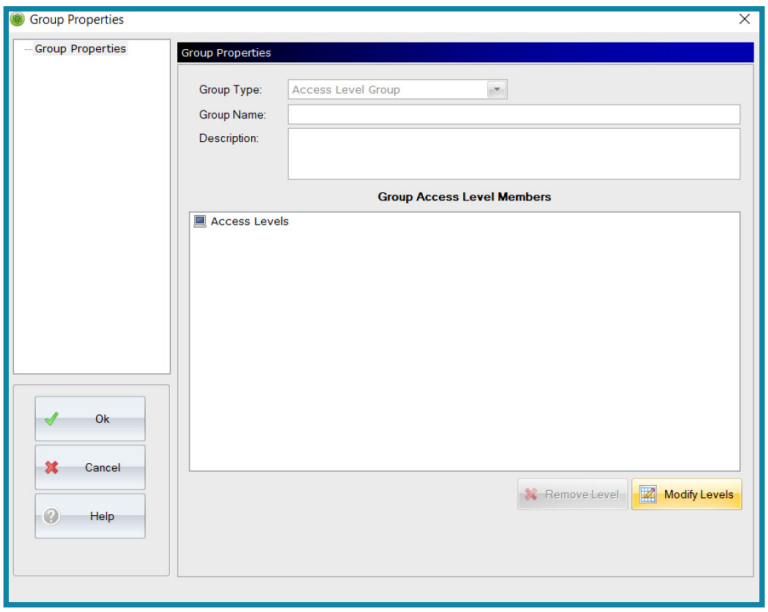
   For more information on access levels, see Chapter 6 in the DNA Fusion User Manual.

Creating a Legacy Access Level Group

A Legacy Access Level Group provides an easy way for legacy access levels and ASSA access levels to be grouped together in a common access level. This will allow a cardholder to have access to doors on multiple controllers and ASSA locks with a single legacy access level group.

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

   The Legacy Access Level dialog opens.



2. **Enter** a Group Name for the legacy access level group.
3. **Click** the Modify Levels button.

   The DNA Fusion - Assign Access Levels dialog opens.

   The ASSA access levels are identified by the distinct icon.

4. **Select** the Assigned column for the desired ASSA Access Levels and Legacy Access Levels.

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

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

5. **Click** OK to save the Legacy Access Level dialog.

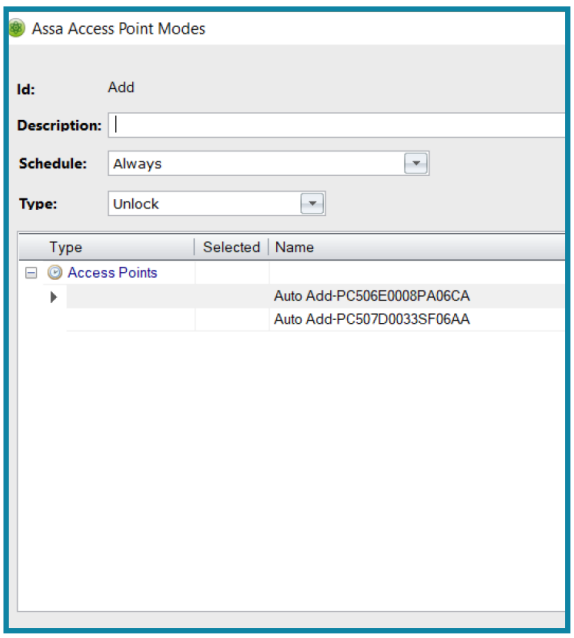
   The Legacy Access Level Group will appear in the browser and is ready for distribution to cardholders.

Creating ASSA Access Modes

Access modes are configured to specify a reader mode change based on an event, including unlocking the reader on a schedule as well as a first person unlock option. Once enabled, the door will either unlock based on the associated schedule or when the first person accesses the door within the specified time schedule.

1. From the ASSA tab in the Hardware browser, **right-click** on the Access Modes header and **select** Add Access Mode.

   The ASSA Access Point Modes dialog opens.



2. **Enter** a Description for the access mode.
3. **Select** a Time Schedule from the drop-down menu.

   Time Schedules should be created before configuring Access Modes.
4. If desired, **select** the Access Mode Type from the drop-down list.
   - Unlock (Default) - The reader will automatically change modes, and Unlock the door if the specified schedule is active when the cardholder badges. The door will return to the secure state at the end of the time schedule.
   - First Person Through - If the selected Time Schedule is active, the first person to badge will unlock the door. The door will remain in the unlocked state until the time schedule deactivates.
   - Primary - Requires the cardholder to have a PIN associated with their personnel record.
   - Primary THEN Secondary - Once configured, cardholders assigned this level would be required to present a valid card and enter a PIN.

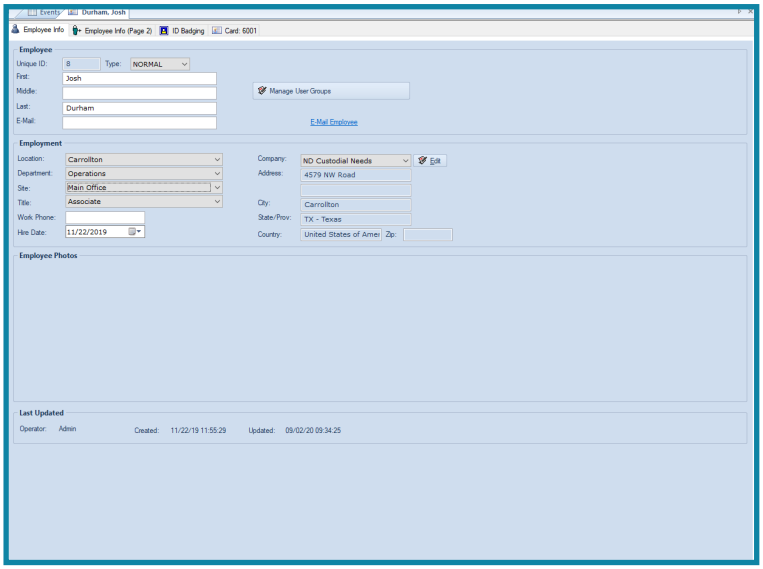
> **CAUTION**: *This setting defines the cardholders access instead of the locksets mode. The lockset will NOT accept a cardholder if either the Primary or Primary THEN Secondary mode is selected and a PIN is not associated with cardholders. The lockset operates in a mode where the cardholder is required to present credentials based on this setting. This requires some cardholders to enter both factors while other cardholders present a card.*

5. **Check** the Selected column to add a door(s) to the access mode.
6. **Click** the OK button to add the access mode.

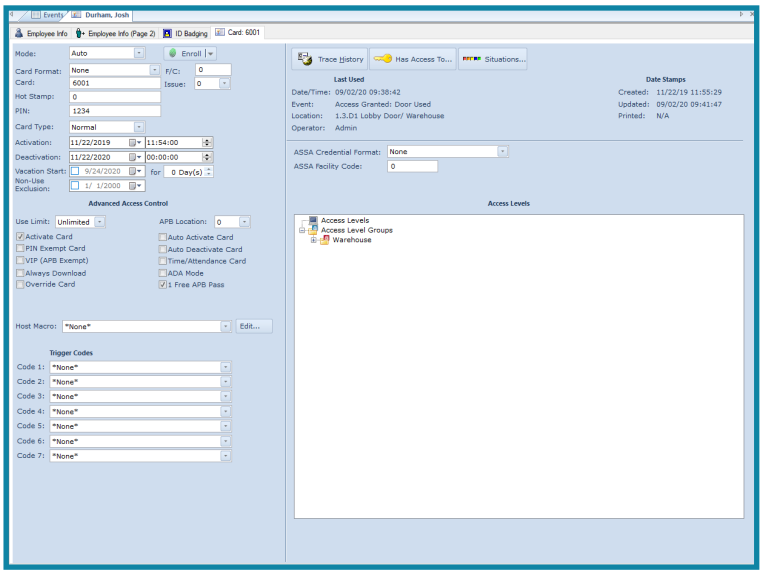
ASSA Credential Information

This section explains how to assign card information to a Personnel Profile.

1. From the Personnel browser, **add** a new cardholder or **open** an existing cardholder's record.
   The cardholder's record opens.



2. **Enter** the desired information in the Employee Info tabs.
3. **Select** the Card tab.
   The card information is displayed.

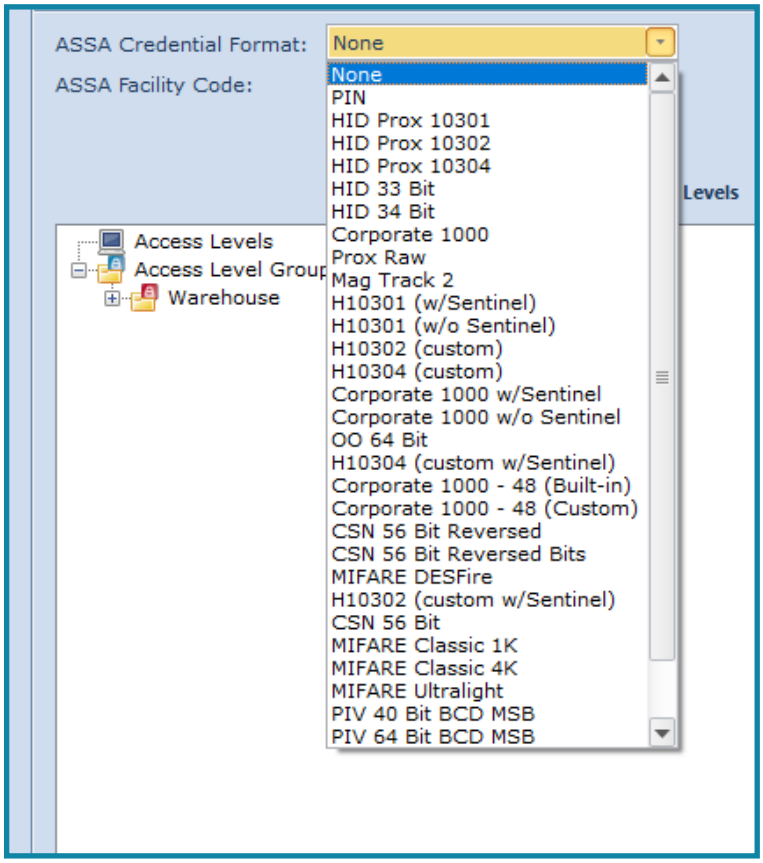


4. For new cards, **enter** the Card number and complete any other fields.

> **Note**: *Two cards will need to be issued if the installation is utilization multiple hardware platforms. One card would use the standard card format programmed in the Open Options controller. The second card would have the ASSA format and the facility code information.*

5. If needed, **right-click** in the record and **select** the Add New Card option.
   The Card number dialog appears.
6. **Enter** the Card number and **click** the Set button.

7. **Right-click** in the record and **select** the Update option.
   The record is saved and updated.
8. **Select** a card format from ASSA Credential Format drop-down list.
   If PIN is selected, a PIN must be entered in the card record. PINs must be six (6) digits in length.



9. **Enter** the Facility Code for the credential.
10. **Update** the cardholder's record.
11. If desired, **add** an access level to the cardholder.

Aperio Integration

In This Section:

- Configuring the Aperio Hub in DNA Fusion
- Installing the Aperio Programming Application
- Configuring the Aperio Locks

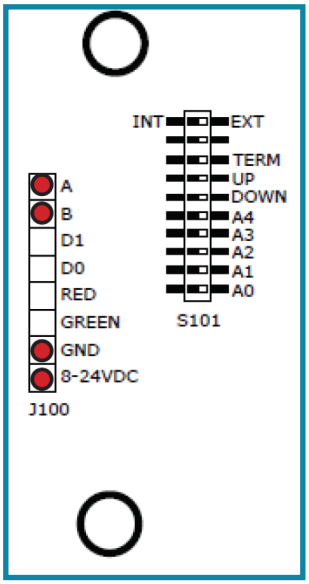
Configuring the Aperio Hub in DNA Fusion

The Aperio Hub must be model AH30 and be setup for Open Options (should be indicated by a sticker).

Wiring the Aperio Hub

The Aperio Hub (AH30) is wired to a controller's RS-485 port. The required connections are shown in the table below.

Aperio Hub Wire Terminals	Description
A	RS-485 Data A
B	RS-485 Data B
DATA 1	Wiegand Data 1 signal. Used to transmit credential information
DATA 0	Wiegand Data 0 signal. Used to transmit credential information.
RED	Used for access decision. Leave unconnected if DIP switch 1 (A0) is in the OFF position.
GREEN	Wiegand green signal. Used for access decision.
GND	GND = signal ground.
8-24 Vdc	Power supply limit. The power supply shall be a Limited Power Source (LPS) according to EN 60950-1. The power supply shall be 3A over current protected. Wire requirements are 16 to 22 AWG



Ensure that the Aperio Hub (AH30) is wired correctly. See the table and the diagram above to verify the wiring connections.

From the RS-485 port:

1. **Wire** the TR+ to A terminal on the Aperio Hub.
2. **Wire** the TR- to B terminal on the Aperio Hub.
3. **Wire** the GND (LSP or Panel) to the GND terminal on the Aperio Hub.
4. **Wire** the Power to the 8-24 Vdc terminal.

LED Status

LED Frequency	Description
Solid GREEN	Aperio Hub is Online
Solid GREEN, one short RED flash	Aperio Lock is Offline
Solid GREEN, two short RED flashes	EAC Offline
Solid GREEN, three short RED flashes	Aperio Lock and EAC Offline
Yellow, Flashing	UHF Communication
Solid Yellow	Pairing Active

DIP Switch Settings

A0-A3 (1-56) is used to set physical address of the Aperio Hub (AH30).

Label	DIP Switch Number	Description
A0-A4	DS1-5	Controls physical addressing of the AH30.
DOWN	DS6	Controls the use of the RS-485 pull down resistor.
UP	DS7	Controls the use of the RS-485 pull up resistor.
TERM	DS8	Controls the use of termination between A and B.
	DS9	Not Used.
INT/EXT	DS10	Controls the use of the external antenna.

Aperio Hub Address Settings

Address	A0 (DS1)	A1 (DS2)	A2 (DS3)	A3 (DS4)	A4 (DS5)
0	Do NOT use address 0				
1	**ON**	OFF	OFF	OFF	OFF
2	OFF	**ON**	OFF	OFF	OFF
3	**ON**	**ON**	OFF	OFF	OFF
4	OFF	OFF	**ON**	OFF	OFF
5	**ON**	OFF	**ON**	OFF	OFF
6	OFF	**ON**	**ON**	OFF	OFF
7	**ON**	**ON**	**ON**	OFF	OFF
8	OFF	OFF	OFF	**ON**	OFF
9	**ON**	OFF	OFF	**ON**	OFF
10	OFF	**ON**	OFF	**ON**	OFF
11	**ON**	**ON**	OFF	**ON**	OFF
12	OFF	OFF	**ON**	**ON**	OFF
13	**ON**	OFF	**ON**	**ON**	OFF
14	OFF	**ON**	**ON**	**ON**	OFF
15	**ON**	**ON**	**ON**	**ON**	OFF

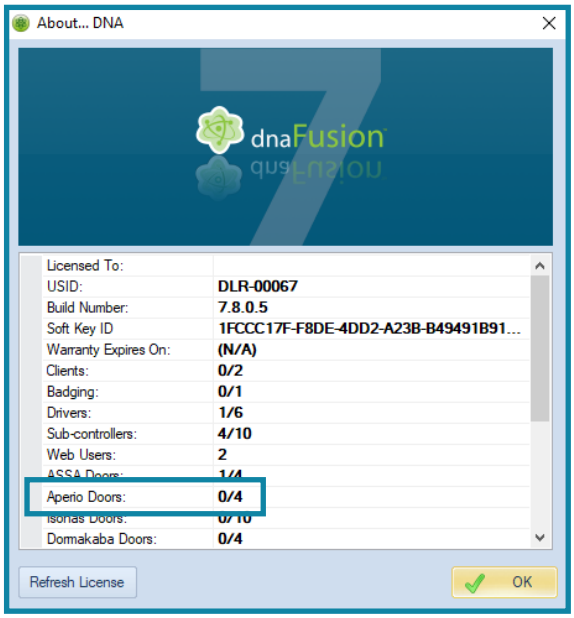
Note: *Physical address is not read on fly. The user must power down and up for each DIP switch change, otherwise the Aperio Hub will operate on the same physical address.*

Note: *If the Aperio Programming Application is used to set the RS-485 addresses, the application will override the address set by the DIP switch.*

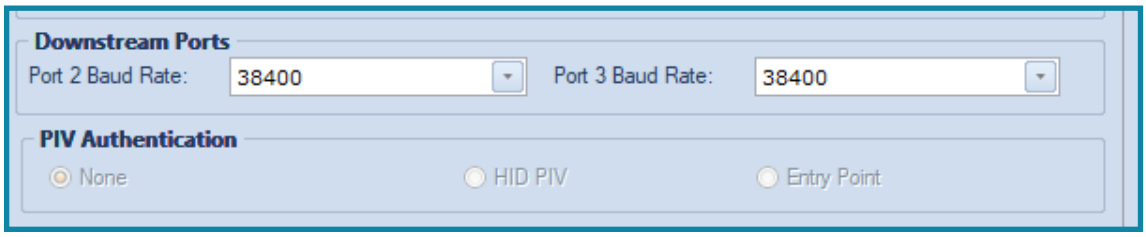
Adding the Aperio Hub in DNA Fusion

Before adding the AH30:

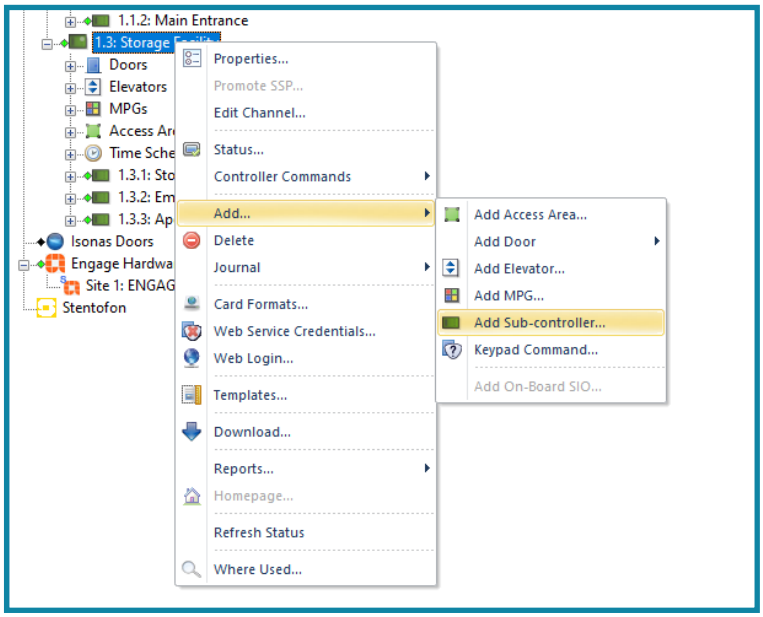
1. **Ensure** that Aperio Doors license has been added to the DNA Fusion system.



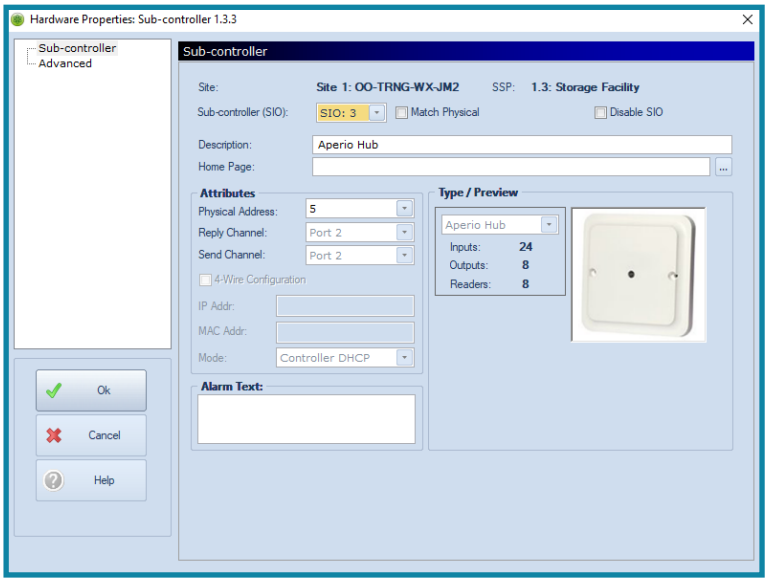
2. **Ensure** that the Baud Rate for the controller is set to 38400.



3. Once the prerequisites are met, **right-click** on the controller with the Aperio Hub attached.
4. **Select** Add > Add Sub-controller.



5. In the Type / Preview drop-down menu, **select** Aperio Hub.
6. **Add** a Description for the Aperio Hub.
7. **Ensure** the Physical Address matches what the DIP switches were set to on the Aperio Hub when power was applied.



8. **Select** Ok to download the settings.

   If needed, **reset** the controller to bring the Aperio Hub online.

   The Aperio Hub must be online before configuring the Aperio Programming Application.

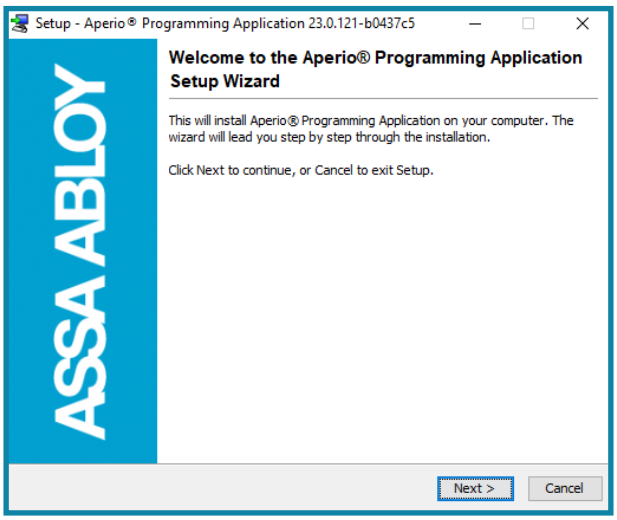
Configuring the Aperio Programming Application

The Aperio Programming Application is available in the Aperio Kit and is needed to complete the Aperio integration. Follow the steps below for installation and configuration instructions.

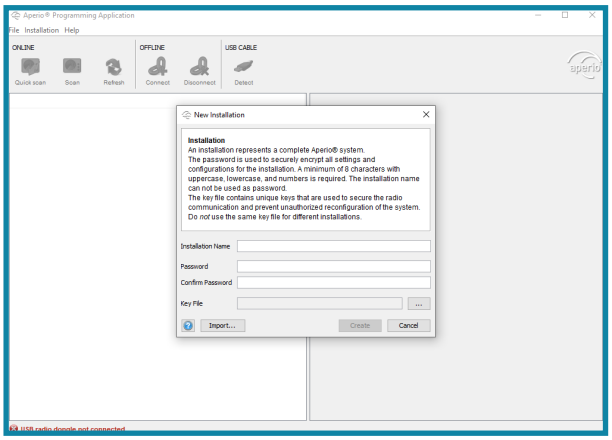
Installing the Aperio Programming Application

To install the Aperio Programming Application:

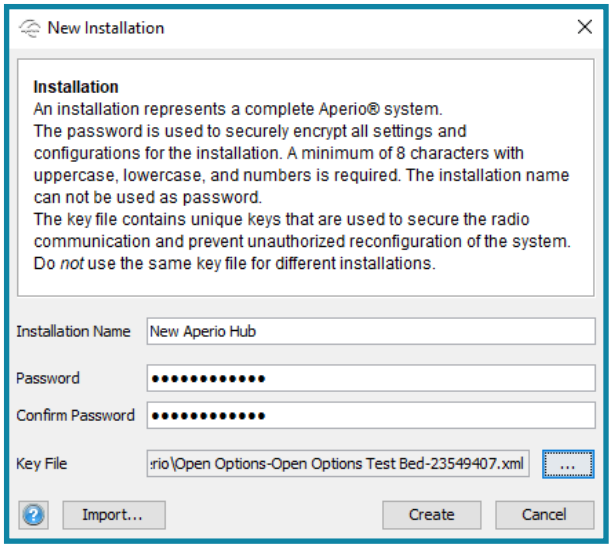
1. **Locate** setup.progapp application.
2. **Double-click** on the application.
3. **Click** Run.
   The Setup dialog opens.



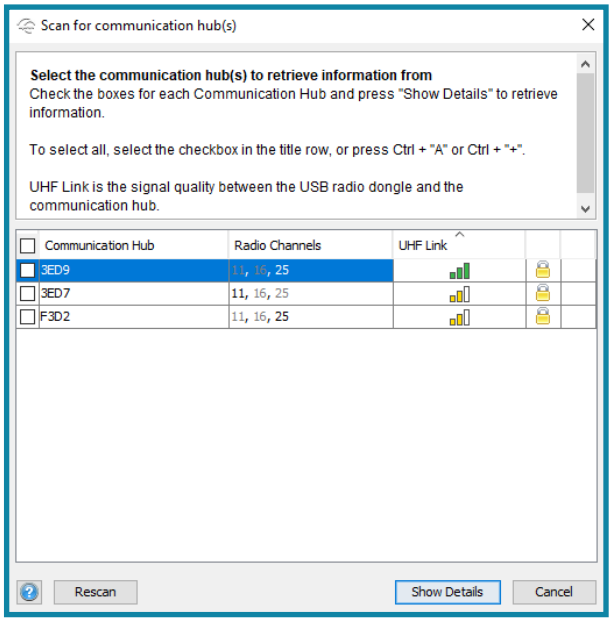
4. **Click** Next.
   The License Agreement appears.
5. **Select** I accept.
6. **Select** the where to download the application or **select** Next to accept the default path.
   Default Path: C:\Program Files (x86)\Assa Abloy\ Aperio Programming Application.
7. Once the install is complete, **click** on the Finish button.
   An Aperio Icon should appear on the desktop.
8. **Double-click** on the Aperio desktop icon.
   The New Installation dialog will appear.



9. **Enter** a Installation Name and Password
10. Re-enter the Password.
11. **Locate** and **open** the Key File by selecting the browse (...) button.
    The file type is .xml.

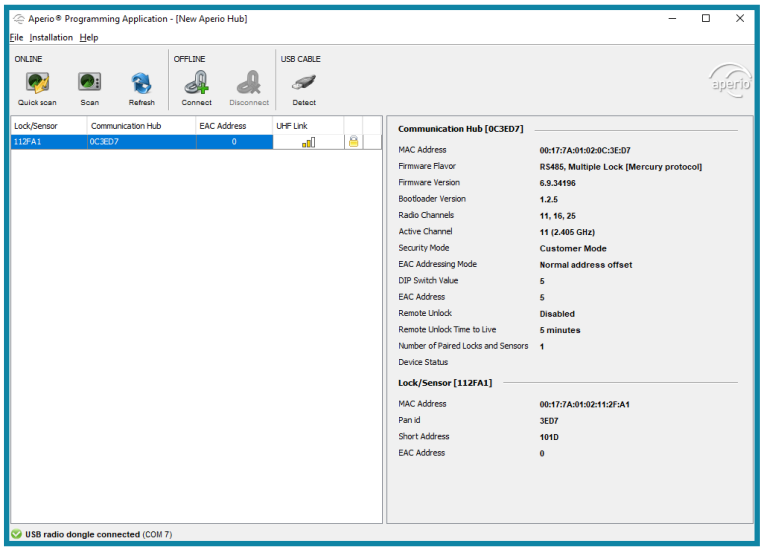


12. **Click** on the Create button.
13. **Insert** the Wi-Fi dongle into the Host Machine
    The USB stick is labeled Aperio Wireless Lock Technology.
14. **Select** Quick Scan.
    Aperio Hubs (Communication Hubs) in range will appear in the Quick Scan dialog.



15. **Select** the desired Aperio Hub.
    The correct Aperio Hub can be identified by the MAC Address.
16. **Click** on Show Details.
    The Aperio Hub will be displayed on the dashboard.

17. To switch to Customer Mode, **right-click** on the Aperio Hub and **select** Switch to Customer Mode.
    This action will remove the customer mode caution.

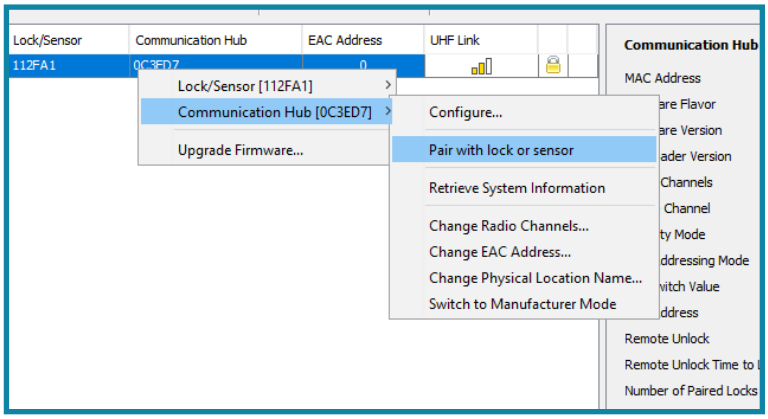


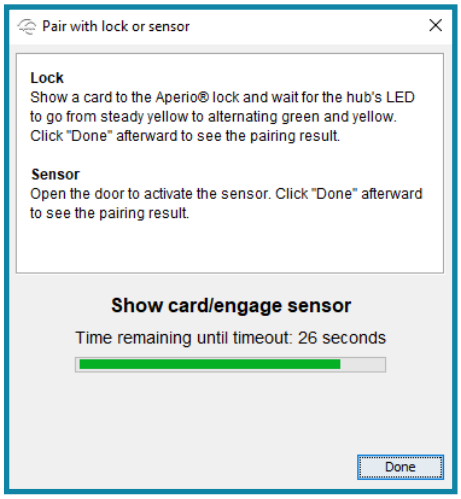
Configuring Aperio Locks in the Aperio Programming Application

Ensure that the Aperio doors are powered on. The batteries must be installed correctly and at the correct voltage. Ensure that the cover is placed properly. The Lockset cannot be paired with the Aperio Hub if the battery cover is not placed properly.

> **Note**: *The POST test should complete with one (1) red LED flash followed quickly by one flash of the green LED and a beep. If the batteries are not installed correctly the lockset will flash red ten (10) times.*

1. In the Aperio Programming Application dashboard, right-click on the Aperio Hub.
2. **Select** Communication Hub > Pair with lock or sensor.
   Follow the instructions in the image below.

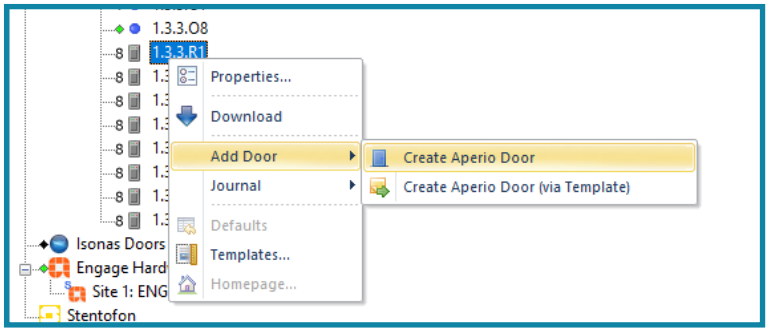




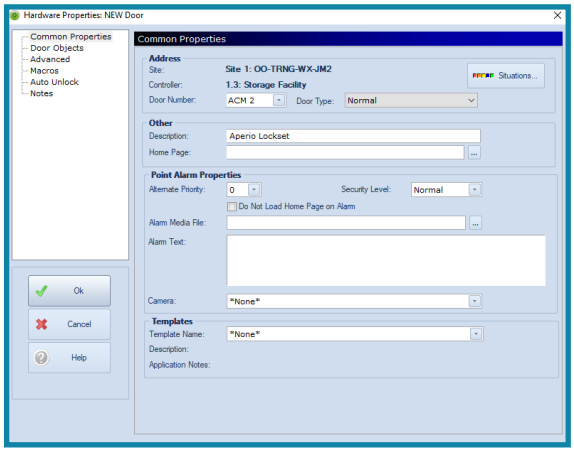
   The Aperio lockset and the Aperio Hub are now paired.
3. If a Security mode conflict error is shown after the pairing, **switch** to Customer Mode. See step 17, page 4-7.

Adding an Aperio Lockset to DNA Fusion

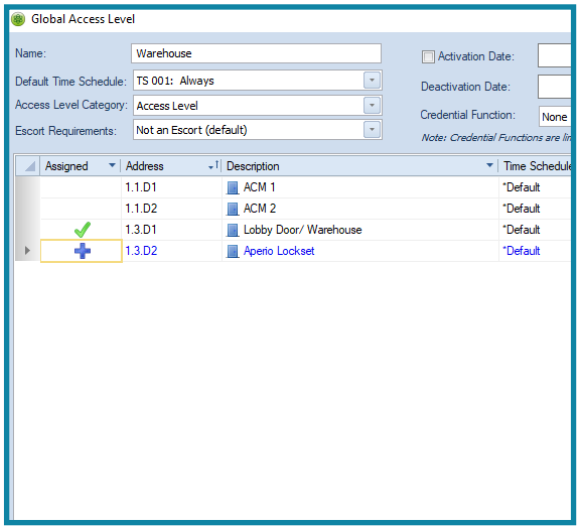
1. **Locate** the Aperio Hub in DNA Fusion.
2. **Expand** the Aperio Hub's hardware tree.
3. **Right-click** on a reader icon.
4. **Select** Add Door > Create Aperio Door.



5. In the Hardware Properties: NEW door dialog, **add** a Description to the door.



6. **Click** Ok to download.
7. **Open** the Access Level browser and **add** the Aperio Door to a desired Access Level Group.



8. If needed, **add** card formats to the controller.

OPEN OPTIONS®
ACCESS TECHNOLOGY

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

Publish Date | September 28, 2020
DNA Fusion Version | 7.8 or Greater
Manual Number | AIG 1.0

www.ooaccess.com