

## ASSA Abloy Integration Guide



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 assumes no responsibility for incorrect or outdated information that may be contained in this publication.

DNA Fusion<sup>™</sup> and SSP<sup>™</sup> are trademarks of Open Options, LLC.

The DNA Fusion<sup>™</sup> Access Control Software and SSP<sup>™</sup> 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<sup>™</sup> Access Control Software and SSP<sup>™</sup> 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

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

#### Warranty

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



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

#### **Open Options Software License Agreement**

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

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

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

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

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

LIMITED WARRANTY: Open Options warrants that it has the sole right to license the Software to Licensee. Upon registration by the Licensee, Open Options further warrants that the media on which the Software is furnished will be free from defects in materials and workmanship under normal use for a period of twelve (12) months following the delivery of the Software to the Licensee. Open Options' entire liability and your exclusive remedy shall be the replacement of the Software if the media on which the Software is furnished proves to be defective. EXCEPT AS PROVIDED IN THIS SECTION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN PARTICULAR, EXCEPT AS PROVIDED IN THIS SECTION, WITH RESPECT TO ANY PARTICULAR APPLICATION, USE OR PURPOSE, LICENSOR DOES NOT WARRANT THAT THE PRODUCTS WILL MEET THE LICENSEE'S REQUIREMENTS, THAT THE PRODUCTS WILL OPERATE IN THE COMBINATIONS OF 3<sup>RD</sup> 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**

### Introduction

In this Guide	)-1
Integration Instructions	)-1
DNA Fusion/ASSA DSR	)-2
Minimum Requirements	)-2

### Step 1: Installing the DSR

DSR Overview1-
Wi-Fi Lock Considerations
PoE Considerations1-:
Network Considerations1-
ASSA DSR Installation
Installation and Configuration Steps1-
DSR Installation1-
Additional Information
Basic DSR Uninstall1-
Regedit Uninstall Process1-
SSL/TLS Encryption1-
Disabling Java Updates1-

### **Step 2: Installing the LCT and Configuring the Locksets**

ASSA Lockset Configuration Tool (LCT) Installation	2-1
Lock Configuration with the LCT	2-3
Network Setup	2-4
Reader Setup	2-5
Lock Configuration	2-5
Configuring a Lock	2-5
Upgrading Firmware	2-6
DNA DSR Utility	2-7
Configuring the DNA \ DSR Utility	2-8
DNA Fusion Service Permissions	2-9
COM+ Object	2-9
DNA Fusion Driver Service	2-10
DNA Fusion User Group	2-10

#### Step 3: Configuring the DSR and ASSA Locks in DNA Fusion

Adding the ASSA DSR to DNA Fusion	8-1
ASSA Driver Status	5-2
DSR Options	5-2
Adding the ASSA Locksets to DNA Fusion	3-3
Configuring the ASSA Doors	3-3
Setting Up ASSA in DNA Fusion	-5

Configuring Time Based Schedules	3-5
Day Periods	3-5
Holidays and Holiday Groups	3-6
Time Schedules	3-7
Creating ASSA Access Levels	
Creating a Legacy Access Level Group	3-9
Creating ASSA Access Modes	
ASSA Credential Information	

## **Aperio Integration**

Configuring the Aperio Hub in DNA Fusion	4-1
Wiring the Aperio Hub	4-1
LED Status	4-1
DIP Switch Settings	4-2
Aperio Hub Address Settings	4-2
Adding the Aperio Hub in DNA Fusion	4-3
Configuring the Aperio Programming Application	4-5
Installing the Aperio Programming Application	4-5
Configuring Aperio Locks in the Aperio Programming Application	4-7
Adding an Aperio Lockset to DNA Fusion	4-8

## 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.



### **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	Java Runtime Environment 1.8.0.51 (Installed with	
(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			

# Step1: 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.

🍘 About DNA	×	<
	anaFusion quatrix ou	
Soft Key ID	1FCCC17F-F8DE-4DD2-A23B-B49491B91 ^	
Warranty Expires On:	(N/A)	
Clients:	1/2	
Badging:	1/1	
Drivers:	1/6	
Sub-controllers:	4/10	
Web Users:	2	
ASSA Doors:	0/4	
Aperio Doors:	0/4	
Isonas Doors:	0/10	
Dormakaba Doors:	0/4	
EngageIP Doors:	0/4	
Handkey II Integration:	Yes	
BIOScrypt Integration:	Yes 🗸	
Refresh License	🖌 ОК	

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 Laccept 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.

Door Service Router 8.0.11.0			-		×
		PostgreSQL	Server Co	nfigura	ation
<ul> <li>Introduction</li> <li>License Agreement</li> <li>Choose Installation Folder</li> <li>Database Configuration</li> <li>Support Tool Configuration</li> <li>DSR Server Configuration</li> <li>Pre-Installation Summary</li> <li>Installing</li> <li>Install Complete</li> </ul>	Specify PostgreSQL Serv Host: Database: Username: Password: Confirm Password:	127.0.0.1 DSR postgres			
InstallAnywhere Cancel		1	<u>P</u> revious	<u>N</u> e)	t

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.

Door Service Router 8.0.11.0		– 🗆 X
		Support Tool Configuration
<ul> <li>Introduction</li> <li>License Agreement</li> <li>Choose Installation Folder</li> <li>Database Configuration</li> <li>Support Tool Configuration</li> <li>DSR Server Configuration</li> <li>Pre-Installation Summary</li> <li>Installing</li> <li>Install Complete</li> </ul>	Specify Support tool def Admin Name: Password: Confirm Password: User Name: Password: Confirm Password:	admin *********** ********** USer *********** ************************
InstallAnywhere Cancel		Previous Next

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.

Door Service Router 8.0.11.0		– 🗆 X
		Support Tool Configuration
<ul> <li>Introduction</li> <li>License Agreement</li> <li>Choose Installation Folder</li> <li>Database Configuration</li> <li>Support Tool Configuration</li> <li>DSR Server Configuration</li> <li>Pre-Installation Summary</li> <li>Install Complete</li> </ul>	Specify Support tool deta Admin Name: Password: Confirm Password: User Name: Password: Confirm Password:	ails       admin       ************       ************       user       ************       ************
InstallAnywhere		Previous Next

**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.

Door Service Router 8.0.11.0		– 🗆 X
		DSR Server Configuration
<ul> <li>Introduction</li> <li>License Agreement</li> <li>Choose Installation Folder</li> <li>Database Configuration</li> <li>Support Tool Configuration</li> <li>DSR Server Configuration</li> <li>Pre-Installation Summary</li> <li>Installing</li> <li>Install Complete</li> </ul>	Inadequate changes to th may render the system in support. Access Data Port. Lock Port: Security Valve: WS Encryption: TLS/SSL Security:	8080 2571 127.0.0.1 0:0:0:0:0:0.01 O true I alse O true I alse
InstallAnywhere Cancel		Previous <u>N</u> ext

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.

 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.

ASSA Edit DSR		×
Parameters		ך
ld:	1003	
Description:	ASSA Door	
Address:	127.0.0.1	
	Use SSL	
Port:	8443	
	OK Cancel	

#### **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.

Java Update - Warning	×
You have chosen to stop automatically checking for updates and will miss future security updates.	1
We strongly recommend letting Java periodically check for newer versions to ensi the most secure and fastest Java experience. Check Weekly	ure you have Do Not Check

- 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



- 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 Laccept 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.

New Configuration File		—	×
File Type*	Encrypted 🔹		
Site Name *	DNA ASSA	]	
Inactivity Timeout	300	onds (0 = off)	
Administrator Password *			
Confirm Password *			
	_	_	
* Mandatory Fields	_	Ok	Cancel

- 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**.

Lock C	onfigur	ation To	ol						- 0 X
2		B	- 13 -	?	- ID-			Site : DNA ASSA	Inactivity Timeout : 300 seconds 🧳
Lock F	Profile	Lo	k Config	guration	Diagnostics	Advanced Setup Ad	vanced Reader Configuration   Sys	tem User	
			Name			Description	Tags	Last Updated Date	Action
							No content in table		
									Create New Profile
ASS The glo	A AE	BLOY	,						LCT 4.0.52.0

5. **Click** the Create New Profile button.

The Lock Profile Details page opens.

			as DNA 655A I Institute Tensorie 200 records - A
	- Church Thurch Church	, 	te: Drok ASSA   Inecomy Inneoux: Sto seconds g
ock Profile Lock Configuration Diag	iostics Advanced Setup Advanced Reader Conf	figuration System User	
Name	Description	Tags	Last Updated Date
Door For DNA			
Details Network Setup Reader Set	up Cardholders Alarms Encryption		
Profile Name *	Door For DNA		
Profile Description			
Tags			
Set as default Privacy			
On Davies Failure			
On Power Failure			
🖲 Lock 🔘 Unlock			
* Mandatory Fields			
SSA ABLOY			Save Card
global leader in			LCT 4.0.52.0

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.

ock Configuration Tool			>
🔒 🖻 🕄 • 🛐 • 📭	+		Site : DNA ASSA   Inactivity Timeout : 300 seconds 🧳
ock Profile Lock Configuration Dia	nostics Advanced Setup Advanced Reader Confi	guration System User	
Namo	Deceintion	Tree	Last Undated Date
Deve Deve David		Taga	
DOOR FOR DINA			
Details Network Setup Reader S	etup Cardholders Alarms Encryption		
EAC Settings	WiFi Manager		Network Interface Device Settings
IP Address *	Preferred WiFi SSID	Select Reset	Default Wireless Rate
Host Name Ex. eacserver.domai	Security Type None		
Port * 2571			DIAC MIU Sze ( 5 to 1460) 536
Lock ID Sattings			POE MTU Size ( 512 to 1400) * 536
court settings			Use alternate PoE communication (required for S2 Security applications)
DHCP			
Static			
Static Addresses are assigned and saved during	n an		
* Mandatory Helds			
SSA ABLOY			Save Cancel
e global leader in			LCT 4.0.52.0

- 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.

WiFi Manager	
Preferred WiFi SSID	oollc Select Reset
Security Type	WPA2-Personal(TKIP)
Key *	
	✓ Hide Characters
Note: Use WPA-2-Tkip i same SSID. This networ group broadcasts. A lo network that is in migr WPA2 network when usi	node on a network that supports WPA2 and WPA onthe k is in migration mode and must use TKIP encryptionfor ckcset using WPA2-Personal mode will not work on a tion model. <sup>1</sup> you have trouble connecting a lockset to ang a WPA2-Personal mode.Try WPA2-TKIP instead.

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

Lock Configuration Tool			- • ×
C. 🚔 🗎 🕄 • 🖬 •		Site :	DNA ASSA 👔 Inactivity Timeout : 300 seconds 🧳
Lock Profile Lock Configuration Diagn			
Name	Description	Tags	Last Updated Date
Door For DNA			09-15-2020 08:41:38
Details Network Setup Reader Setu	P Cardholders Alarms Encryption		
Reader multiCLASS Reader			
# Card Type	Data Type Application		
0 HID Prox			
1 ICLASS/ICLASS SE			
2 Disable Entro			
< Disable Entry>			
3 KLASS/ICLASS SE			
HID Pres			
MIFARE Classic 1K			
MEARE Plus S			
Seos*			
MFARE Classic 4K			
MFARE Ultralight			
MFARE Plus X Ma	ndatory Fields		
1001 10101			Save Cancel
ASSA ABLOY The stabal leader in			LCT 4.0.52.0

- 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.

Lock Configuration Tool							- 🗆 X
C. 🚔 💾 🕄 • 🖬 • 🕪					Site :	DNA ASSA   Inactivity Timeo	#: 300 seconds 🧳
Lock Profile Lock Configuration Diagnostics	Advanced Setup	Advanced Reader	Configuration	System User			
Lock Name S/N	Profile	F/W Version	Conn.Type	Configured	Status	Last Configured Date	Action
Factory Default PC031D0455SA47CA		3_0p09_cx_v3532	Serial (COM4)	No	•		0 0
ASSA ABLOY The global leader in							LCT 4.0.52.0

#### **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.

. 🚔 🖻 🕄	· Ø· 📴					Site : Di	oors for ASSA   Inactivity Timeor	t: 300 seconds
ock Profile Lock Confi	iguration Diagnostic	s Advanced Setu	D Advanced Reade	r Configuration	System User			
Look Name	chi	Des Els	Children law	Come Trans	Conflormed	Challen .	Last Conferred Date	A self-re-
LOCK Rainie	syn	Prome	ry w version	Connerape	comgurea	Status	tast configured bate	Action
OE Office - Back Entrance	PC031D0455SA47CA	Doors for ASSA	3_0p09_cx_v3532	Serial (COM6)	Yes	•	09-21-2020 09:29:23	0
								0.0

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.

e Lo	ik Configur	ation Too	al III											-	- x
C.	<b>a</b>	8	₿•	? -	Ð						5	Re i DNA ASS	A   Inectivit	y Timeout i 300	seconds 🥒
	k Profile	Lock	Configu	ration	Diagnostics	Advanced S	ietup 🗍 Advance	d Reader C	onfiguration :	system User					
		Factory	Default		P0031D045	55A47CA			3_0p09_ox_v3532	Serial	(COMI)	No	•		
			P	11		where Cateron	De Co Provinci				_	_	_	_	
	onngur	ation	Firmware	i Upgrac	ie   Senarikun	mber setup	Radio Hirmwar	e upgrade							
	ock Deta	ita													
b	ck.Name 1							Lock Profile	De	er For DNA					
	WVenico														
1															
L	ock Seria	Numb	oer Details					Lock IP C	onfiguration						
	veration M	ode						10.4444							
								IF ADDIES							
le le	ternal S/N				A61CS			Subnet Mas	k*						
6	mpatibility	S/N	PO					Gateway *							
1.1	Mandatory	Fields													
														Configure	Bok
A	SSA AL	BLOY													CT 4.0.52.0
doc	coregioz	olitions	_									_			

- 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.

Lock Configuration Tool								- 🗆 🗙
C. 🖨 🖰 民	• ?• 🗗					Site : Do	oors for ASSA   Inactivity Timeo	ut: 300 seconds 🛛 🧳
Lock Profile Lock Conf	iguration Diagnostic	s Advanced Setup	Advanced Reade	r Configuration	System User			
Lock Name			F/W Version					
PoE Office - Back Entrance	PC031D0455SA47CA	Doors for ASSA	3_0p09_cx_v3532	Serial (COM6)	Yes	•	09-21-2020 09:29:23	o 👩
WiFi Office Front Entrance	PC034D0054SF06AA	Doors for ASSA	3_0p07_cx_v3511	N/A	Yes	•	09-21-2020 08:41:07	0

#### **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.



- 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

C DNA/DSR Utility		-		×	¢
DSR Parameters DSR Address				1.9.0.5	
127.0.0.1 (ASSA Door)	<b>Y</b>	🖉 Conne	ect		
DSR Functions V Regenerate User GUIDs					

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.

DSR Parameters  DSR Address  Iz7.00.1 (ASSA Door)  Version 8.0.11.0.  DSR Functions  Regenerate User GUIDs  Access point 943d6772-18a6-4c0e-91a0-8e1b747a60ac matches for serial number PC031D0455SA47CA. No actio  Successfully initialized access point Auto Add-PC031D0455SA47CA (PC031D0455SA47CA) DSR (127.00.1) (DNA/DSR Utility  Naking Orphan Day Periods Unking Orphan Day Exception Committing Pending User Committing Pending User Committing Pending User Committing Pending Day Periods Committing Pending Day Periods Committing Users Committing Versions Committing Versions Committing Versions Committing Versions Committing Versions Committing Versions Committing Users Committing Versions Committing Ve	DSR Parameters  DSR Address  Iz7.0.0.1 (ASSA Door) Version: 8.0.11.0.  DSR Functions  Connect  Connet  Connect  Connect  Connect  Connet  Connect  Connect  Connect	DNA/DSR Utility		
DSR Address  127.0.0.1 (ASSA Door)  Version: 8.0.11.0.  DSR Functions  Regenerate User GUIDs  Access point 943d6772-18a6-4c0e-91a0-8e1b747a60ac matches for serial number PC031D0455SA47CA. No actio  Successfully initialized access point: Auto Add-PC031D045SSA47CA (PC031D045SSA47CA) DSR (127.0.0.1) connected successfully DSR (127.0.0.1) connected successfully DSR Version: 8.0.11.0.  Linking Orphan Day Exception DNA/DSR Utility  DNA/DSR Utility  DNA/DSR Utility  DNA/DSR Utility  Committing Pending User  Committing Pending User Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules Committing Users Committing	130         DSR Address         127.0.0.1 (ASSA Door)         Version: 8.0.11.0.         Image: DSR Functions         DSR (27.0.0.1) connected successfully         DNA/DSR Utility         Image: DSR (20.0.0.0.0.0.0.0.0.0.0.0.0.0	DSR Parameters		
127.0.0.1 (ASSA Door)       Connect         Version: 8.0.11.0.       Connect         DSR Functions       Regenerate User GUIDs         Access point 943d6772-18a6-4c0e-91a0-8e1b747a60ac matches for serial number PC031D045SSA47CA. No actio         Successfully initialized access point: Auto Add-PC031D045SSA47CA (PC031D045SSA47CA)         DSR (127.0.0.1) connected successfully         DSR Version: 8.0.11.0.         Linking Orphan Day Exception         Linking Orphan Day Exception         Linking Orphan Day Exception         Linking Orphan Authorization         Committing Pending User         Committing Pending Day Periods         Committing Pending Day Exceptions         Committing Time Schedules         Committing Time Schedules         Committing Users         Committing Versions         Committing Versions         Committing Versions         Committing Time Schedules         Committing Versions         Committing	127.0.0.1 (ASSA Door) <ul> <li>Version: 8.0.11.0.</li> <li>DSR Functions</li> <li>Regenerate User GUIDs</li> </ul> Access point 943d6772-18a6-4c0e-91a0-8e1b747a60ac matches for serial number PC031D0455SA47CA. No actio         Successfully initialized access point: Auto Add-PC031D045SSA47CA (PC031D045SSA47CA)         DSR (127.00.1) connected successfully         DSR Version: 8.0.11.0.         Linking Orphan Day Exceptilizing Orphan Day Exceptilizing Orphan Day Exceptilizing Orphan Day Exceptilized access Point Modes to DSR.         Committing Pending User       OK         Committing Pending User       OK         Committing Pending User       OK         Committing Pending User Committing Pending User       OK         Committing Pending User       OK         Committing Pending User Committing Pending User Committing Pending User Committing Pending User Committing Pending Day Periods         Committing Pending Day Exceptions       Committing Pending Day Exceptions         Committing Pending Day Exceptions       Committing Time Schedules	DSR Address		1.9.0
Version: 8.0.11.0.	Version: 8.0.11.0.	127.0.0.1 (ASSA Door)		✓ <i>P</i> Connect
DSR Functions       Regenerate User GUIDs         Access point 943d6772-18a6-4c0e-91a0-8e1b747a60ac matches for serial number PC031D0455SA47CA. No actio         Successfully initialized access point: Auto Add-PC031D045SSA47CA (PC031D045SSA47CA)         DSR (127.0.0.1) connected successfully         DSR Version: 8.0.11.0.         Linking Orphan Day Periods         Unking Orphan Day Except         Linking Orphan Authorization         Committing Pending User         Committing Pending Day Exceptions         Committing Time Schedules         Committing Time Schedules         Committing Users         Committing Users         Committing Version         Committing Authorizations <td>DSR Functions       Regenerate User GUIDs         Access point 943d6772-18a6-4c0e-91a0-8e1b747a60ac matches for serial number PC031D0455SA47CA. No actio         Successfully initialized access point: Auto Add-PC031D0455SA47CA (PC031D045SSA47CA)         DSR (172.0.1) connected successfully         DSR Version: 8.011.0.         Linking Orphan Day Periods         Linking Orphan Day Excepti         DNA/DSR Utility         Linking Orphan Day Excepti         DNA Database has been refreshed to the DSR         Committing Pending User Access Point Modes to DSR         Committing Pending Day Periods         Committing Pending Day Periods</td> <td>Version: 8.0.11.0.</td> <td></td> <td></td>	DSR Functions       Regenerate User GUIDs         Access point 943d6772-18a6-4c0e-91a0-8e1b747a60ac matches for serial number PC031D0455SA47CA. No actio         Successfully initialized access point: Auto Add-PC031D0455SA47CA (PC031D045SSA47CA)         DSR (172.0.1) connected successfully         DSR Version: 8.011.0.         Linking Orphan Day Periods         Linking Orphan Day Excepti         DNA/DSR Utility         Linking Orphan Day Excepti         DNA Database has been refreshed to the DSR         Committing Pending User Access Point Modes to DSR         Committing Pending Day Periods	Version: 8.0.11.0.		
Access point 943d6772-18a6-4c0e-91a0-8e1b747a60ac matches for serial number PC031D0455SA47CA. No actio Successfully initialized access point: Auto Add-PC031D0455SA47CA (PC031D0455SA47CA) DSR (127.0.1) connected successfully DSR Version: 8.0.11.0 Linking Orphan Day Exception Linking Orphan Day Exception Linking Orphan Time Sched Linking Orphan Authorization Committing Pending User A Linking Orphan Authorization Linking Orphan Authorization Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules Committing Time Schedules Committing Time Schedules Committing Authorizations Committing Authorizations Committing Authorizations Committing Access Point Modes Committing Access Point Modes Committing Authorizations Committing Authorizations Committing Access Point Modes Committing Access Point Modes Committing Authorizations Committing Access Point Modes Committing Access Point Modes Committing Authorizations Committing Authorizations Committing Access Point Modes Committing Access Point Modes Committing Access Point Modes Committing Authorizations Committing Authorizations Committing Access Point Modes Committing Access Point	Access point 943d6772-18a6-4c0e-91a0-8e1b747a60ac matches for serial number PC031D0455SA47CA. No actio Successfully initialized access point: Auto Add-PC031D045SSA47CA (PC031D045SSA47CA) DSR (127.0.0.1) connected successfully DSR Version: 8.0.11.0. Linking Orphan Day Excepti Linking Orphan Authorizatic Linking Orphan Authorizatic Linking Orphan Authorizatic Committing Pending Day Periods Committing Pending Day Periods Committing Pending Day Exceptions Committing Pending Day Exceptions Committing Pending Day Exceptions	DSR Functions	V Regenerate User GUIDs	
Access point 3-5000 Control backet of backet o	Access point -F300 - F100 - FC00 - FC	Access point 943d6772-18a	5.4c0e.91a0.8e1h747a60ac matches for serial n	umber PC031D04555A47CA No actio
DSR (127.00.1) connected successfully DSR Version: 8.0.11.0. Linking Orphan Day Excepti Linking Orphan Day Excepti Linking Orphan Day Excepti Linking Orphan Time Sched Linking Orphan Authorization Committing Pending User A Committing Pending User A Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules Committing Time Schedules Committing Versions Committing Users Committing Users Committing Versions Committing Users Committing Authorizations Committing Authorizations Committing Authorizations	DSR (127.00.1) connected successfully DSR Version: 8.0.11.0. Linking Orphan Day Periods Linking Orphan Day Excepti Linking Orphan Time Sched Linking Orphan Authorizatik Committing Pending User Committing Pending Day Periods Committing Pending Day Periods Committing Pending Day Periods Committing Pending Day Periods Committing Pending Day Exceptions Committing Pending Day Exceptions Committing Pending Day Exceptions Committing Pending Day Exceptions Committing Pending Day Exceptions	Successfully initialized acce	s point: Auto Add PC031D04555A47CA (PC031D	04555447CA)
DNA /DSR Version: 8.0.11.0. Linking Orphan Day Periods Linking Orphan Day Exception Linking Orphan Day Exception Linking Orphan Time Schede Linking Orphan Authorization Committing Pending User Committing Pending Day Periods Committing Pending Day Exceptions Committing Users Committing Authorizations Committing Users Committing Users Commit	DNA/DSR Version: 80.11.0. Linking Orphan Day Periods Linking Orphan Day Excepti Linking User A Committing Pending User A Committing Pending User A Committing Pending Day Periods Committing Pending Day Exceptions Committing Pending Day Exceptions Committing Pending Day Exceptions Committing Pending Day Exceptions Committing Pending Day Exceptions	DSP (127.0.0.1) connected s	rescfully	, , , , , , , , , , , , , , , , , , ,
DNA/DSR Utility X Unking Orphan Day Excepti Linking Orphan Day Excepti Linking Orphan Day Excepti Linking Orphan Time Sched Linking Orphan Authorizatio Committing Pending User Committing Pending User Committing Pending Day Periods Committing Time Schedules Committing Time Schedules Committing Authorizations Committing Authorizations	DNA/DSR Utility X Unking Orphan Day Periods Unking Orphan Day Excepti Unking Orphan Day Excepti Unking Orphan Day Excepti Unking Orphan Authorizatit Unking Orphan Authorizatit Unking Orphan Authorizatit Unking Orphan Authorizatit Committing Pending Day Periods Committing Pending Day Periods Committing Pending Day Periods Committing Pending Day Exceptions Committing Pending Day Exceptions Committing Pending Day Exceptions	DSR (127.0.0.1) connected 3	ccessiony	
Linking Orphan Day Except Linking Orphan Day Except Linking Orphan Day Except Linking Orphan Time Sched Linking Orphan Time Sched Linking Orphan Authorizatic Linking Orphan Authorizatic Linking Orphan Access Point Modes to DSR Committing Pending Day Exceptions Committing Time Schedules Committing Time Schedules Committing Authorizations Committing Authorizations	Linking Orphan Day Excepti Linking Orphan Day Excepti Linking Orphan Day Excepti Linking Orphan Time Sched Linking Verset o DSR Committing Pending User Committing Pending User Committing Pending Day Periods Committing Pending Day Periods Committing Pending Day Exceptions Committing Pending Day Exceptions Committing Pending Day Exceptions	Linking Ornhan Day Periods	DNA/DSR Utility	×
Linking Orphan Day Except Linking Orphan Day Except Linking Orphan Time Sched Linking Orphan Athorization Linking Orphan Authorization Linking Orphan Authorization Committing Pending Day Exceptions Committing Time Schedules Committing Time Schedules Committing Authorizations Committing Authorizations Committing Authorizations Committing Authorizations Committing Authorizations Committing Authorizations Committing Authorizations	Linking Orphan Day Except Linking Orphan Day Except Linking Orphan Time Sched Linking Users to DSR Committing Pending User Committing Pending User Committing Pending Day Periods Committing Pending Day Periods Committing Pending Day Exceptions Committing Pending Day Exceptions	Linking Orphan Day Excenti		
Linking Orphan Time Sched Linking Users to DSR Committing Pending User Committing Pending User Linking Orphan Authorization Linking Orphan Access Point Modes to DSR Committing Pending Day Periods Committing Pending Day Exceptions Committing Users Committing Users Committing Users Committing Authorizations Committing Authorizations Committing Authorizations Committing Authorizations Committing Authorizations Committing Authorizations Committing Access Point Modes	Linking Orphan Time Sched Linking Users to DSR Committing Pending User Linking Orphan Authorizatia Linking Orphan Access Point Modes to DSR Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules	Linking Orphan Day Excepti		
Linking Users to DSR Committing Pending User Committing Pending User Linking Orphan Access Point Modes to DSR Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules Committing Users Committing Authorizations Committing Access Point Modes Committing Access Point Modes	Linking Users to DSR Committing Pending User Committing Pending User Linking Orphan Authorizatin Committing Pending Day Periods Committing Pending Day Exceptions Committing Pendules	Linking Orphan Time Sched	DNA Database has been refreshed	to the DSR
Committing Pending User A Committing Pending User A Linking Orphan Authorizatia Committing Pending Day Periods Committing Pending Day Exceptions Committing Pending Day Exceptions Committing Time Schedules Committing Authorizations Committing Authorizations Committing Authorizations Committing Access Point Modes Conversion Complete.	Committing Pending User A Committing Pending User C Linking Orphan Authorizatik Linking Orphan Access Point Modes to DSR Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules	Linking Users to DSR		
Committing Pending User COK Linking Orphan Authorizatic Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules Committing Jusers Committing Authorizations Committing Authorizations Committing Access Point Modes Conversion Complete.	Committing Pending User OK Linking Orphan Authorizatic Linking Orphan Access Point Modes to DSR Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules	Committing Pending User /		
Linking Orphan Authorizatie	Linking Orphan Authorizatic Linking Orphan Access Point Modes to DSR Linking Orphan Access Point Modes to DSR Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules	Committing Pending User (		OK
Linking Orphan Access Point Modes to DSR Committing Pending Day Periods Committing Time Schedules Committing Users Committing Authorizations Committing Access Point Modes Conversion Complete.	Linking Orphan Access Point Modes to DSR Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules	Linking Orphan Authorizatio		Luna and Luna
Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules Committing Users Committing Authorizations Committing Access Point Modes Conversion Complete.	Committing Pending Day Periods Committing Pending Day Exceptions Committing Time Schedules	Linking Orphan Access Poin	Modes to DSR	
Committing Pending Day Exceptions Committing Time Schedules Committing Users Committing Authorizations Committing Access Point Modes Conversion Complete.	Committing Pending Day Exceptions Committing Time Schedules	Committing Pending Day P	eriods	
Committing Time Schedules Committing Users Committing Authorizations Committing Access Point Modes Conversion Complete.	Committing Time Schedules	Committing Pending Day E	ceptions	
Committing Users Committing Authorizations Committing Access Point Modes Conversion Complete.		Committing Time Schedule	5	
Committing Authorizations Committing Access Point Modes Conversion Complete.	Committing Users	Committing Users		
Committing Access Point Modes Conversion Complete.	Committing Authorizations	Committing Authorizations		
Conversion Complete.	Committing Access Point Modes	Committing Access Point N	odes	
	Conversion Complete.	Conversion 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.

Dump         Pooling           Security         Identity         Activation           tion will run under the following account.         Identity         Identity           Account:         Identity         Identity         Identity           Isocount:         Identity         Identity         Identity           Isocount:         Identity         Identity         Identity           Isocount:         Identity         Identity         Identity           Isocount:         Identity         Identity         Identity	& Recycling Queuing	ASSA ABLOY Door Servic	ce Router Properties (Lo
Security Identity Activation dion will run under the following account. In Account: teractive user - The current logged on user incal Service - Built-in service account.	Queuing	ASSA ABLOY Door Servic	ice Router Properties (Lo
tion will run under the following account. n Account: teractive user - The current logged on user ical Service - Built-in service account.		General Log On Recov	
gwork Service - Built-in service account with netw vcal System - Complete access to local machine eer: OO \munoz	rork access Browse	Log on as: Cocal System account Alow service to int @ This account; Password: Confirm password;	Internet with desktop
rd:			
password:			
ver applications cannot run under system service a about <u>setting these properties</u> .	accounts.		

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.

DNADrvr32 Prope	rties (Local	Computer)			×
General Log On	Recovery	Dependencies			
Log on as:					
○ Local System	account				
Allo <u>w</u> serv	ice to interac	t with desktop			
This account	00	\jmunoz		Browse	
Password:	••	•••••			
<u>C</u> onfirm pass	vord:	•••••			
					=
		OK	Cancel	Apply	

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.
- 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.

6	ASSA Add DSR		×
	Parameters		
	ld:	Add	
	Description:	ASSA Doors	
	Address:		
		Use SSL	
	Port:	8082	
		OK	

- 4. Enter a Description for the DSR.
- 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 analyze 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.

 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.



- 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.

ASSA Door Propertie	5	Х
Properties	Access Point Properties	
Alarm Config	Access Point Information (ID - 1)	
	Access Point Information (ID - 1)         Confined:       Yes         Door Type:       Supp. Powend         Derocipion:       2007 AddEC0310/04555A4726         Senial Number:       PC031004555A4726         Battery Pct:       nr/a         Security Level:       Nonai         Host Macco:       'None'         Device Settings       Daby Battery Oneck Hour:         Daby Battery Oneck Hour:       12:00 an *       Schedule Type:         Strike Duration (Seconds):       5       Awake (seconds):       0         Strike Duration (Seconds):       10 *       Asleep (mnutes):       0         Strip Sectionel Bit       Miscelianeous       Sync Satus:       Monund         Immware:       Las Seen:       0/16/201334.37	
	Door State: Last Error: 09/17/20 12:04:54	
	OK Cano	el

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

Properties	<b>R</b> Ċ	Advanced Alarm Configuration	
Alarm Config			
	- 	Advanced Alarm Configuration	
		Exclude From Nam Processing	
		Alternate Priority:	
		1 •	
		Alarm Text	

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.

🍘 Assa Day Pe	eriod		×
ID:	Add		
Description	1:		
Time Pe	riods —		]
<mark>.</mark> ∭ond	ay	Start Time	End Time
<b></b> ∏ <u>u</u> es	day		
<mark>. ∭</mark> edr	nesday		
V <u>T</u> hurs	day		
V <u>F</u> rida	y		
Satur	day		
Sund:	ау		
		Add Time Period	<u>R</u> emove Time Period
			OK Cancel

- 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.

88	SSA Holiday	/			×
ונ D D	D: Description: Date: Time Perio	Add 08 /23/2017 💌 ds (not required) —			
	Start Ti	me	End	Time	
	Add Time	e Period		Remove Time Period	
				OK Cancel	

- 2. **Enter** a Description for the holiday.
- 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.

- 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.

🏽 🚳	ssa Holi	day Group			×
ld:		Add			
Des	cription	:			
	Туре		Selected	Holiday	
Ξ	🕑 Day I	Exceptio			
	F			Christmas 2017	
				Labor Day	
				Thanksgiving 2017	
				ОК	Cancel

- 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.

ld: Descriptior	Add .:		
Туре		Selected	Name
😑 🕑 Peri	ods		
•			24x7 Personnel
			Business Hours (8a-5p M-F)
			Cleaning (8p-11:59p M-F)
			Main Entrance Schedule (8:30a-4:30p)
			Weekends x 24
😑 🕑 Holi	day Grou		
			All Holidays
			City Hall Holidays
			City Library Holidays

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.

🏽 Assa Autho	orization	0	2	×
ld:	Add		2	
Description:				
Type:	Access			
Schedule:	Always			
Doors Me	mbers			
Selec	ted	Туре	Name	
			Auto Add-PC506E0008PA06CA	
•			Auto Add-PC50/D0033SF06AA	
			OK X Cancel	

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.

Group Properties				X
Group Properties	Group Properties			
	Group Type:	Access Level Group		
	Group Name:			
	Description:			
		Group Acc	ess Level Memb	ers
	Access Level	S		
- Ok				
X Cancel				
			- 20	Remove Level Modify Levels
- Help				
[				

- 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.

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.

Assa Acces	Assa Access Point Modes			
	Add			
1 <b>a</b> :	Auu			
Description:				
Schedule:	Always			
Type:	Unlock		•	
Туре		Selected	Name	
😑 🕑 Acces	s Points			
- F			Auto Add-PC506E0008PA06CA	
			Auto Add-PC507D0033SF06AA	

- 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.

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

Events	/ II Events/ III Durham, Josh				
🌡 Employee Inf	🛓 Engloyee Mo 🚯 Engloyee Mo (Page 2) 🧱 ID Badging 🔟 Card: 6001				
Employee					
Unique ID:	8 Type: NORMAL V				
Rist:	Josh				
Middle:		😻 Manage User Groups			
Last:	Durham				
E-Mail:		E-Mail Employee			
Employment					
Location:	Carroliton ~	Company: ND Custodial Needs V V Edit			
Department:	Operations V	Address: 4579 NW Road			
Ste:	Main Office V				
Title:	Associate V	Cky: Carroliton			
Work Phone:		State/Prov: TX - Texas			
Hire Date:	11/22/2019	Country: United States of Amer Zp:			
- Employee Ph	ofos				
Derator:	Last Updated Operator: Admin Oreated: 11/22/19.11:55:29 Updated: 09:02/20.09:34:25				

- 2. Enter the desired information in the Employee Info tabs.
- 3. Select the Card tab.

The card information is displayed.

🌲 Employee Info 🔮+ Employee Info (Page 2) 🖪 ID Badging 📧 Card: 6001	🛓 Employee Info 🔮 - Employee Info (Page 2) 🧕 ID Badging 🔟 Card: 6001				
Mode: Auto 🔹 🎯 Enroll 🔍	Trace History - Has Access To Mere Situations				
Card Format: None F/C: 0					
Card: 6001 Issue: 0 💌	Last Used	Date Stamps			
Hot Stamp: 0	Date/Time: 09/02/20 09:38:42	Created: 11/22/19 11:55:29			
PIN: 1234	Location: 1.3 D1 Lohby Door/ Warehouse	Updated: 09/02/20 09:41:47 Printed: N/A			
Card Type: Normal -	Operator: Admin				
Activation: 11/22/2019					
Deactivation: 11/22/2020 📴 00:00:00 🔄	ASSA Credential Format: None *				
Vacation Start: 9/24/2020 Vacation Start: ODay(s) +	ASSA Facility Code: 0				
Non-Use 1/ 1/2000					
Advanced Access Control	Access Levels				
Use Limit: Unlimited  APB Location: 0	Access Levels				
Activate Card	Access Level Groups				
PIN Exempt Card Auto Deactivate Card					
VIP (APB Exempt) Time/Attendance Card					
Always Download ADA Mode					
Override Card V1 Free APB Pass					
Host Macro: *None*   Edit					
Times Coder					
Code 11 *None*					
Code 2: Allene A					
Code 3: "None"					
Code 4: "None"					
Code 5: *None*					
Code 6: "None"					
Code 7: "None"					

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.

- 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
В	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 add	dress 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.

🍘 About DNA		Х
	ena Fusion Ana Fusion	
Licensed To:		^
USID:	DLR-00067	
Build Number:	7.8.0.5	
Soft Key ID	1FCCC17F-F8DE-4DD2-A23B-B49491B91	
Warranty Expires On:	(N/A)	
Clients:	0/2	
Badging:	0/1	
Drivers:	1/6	
Sub-controllers:	4/10	
Web Users:	2	
ASSA Doors:	1//	
Aperio Doors:	0/4	
Isonas Doors:	0710	
Dormakaba Doors:	0/4	¥
Refresh License	I OF	<

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

Downstream Ports				
Port 2 Baud Rate:	38400	<ul> <li>Port 3 Baud Rate:</li> </ul>	38400	-
PIV Authentication	1			
None		HID PIV	<ul> <li>Entry Point</li> </ul>	

- 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.

Hardware Properties: Sub-con     Sub-controller	ntroller 1.3.3 Sub-controller	×
···· Advanced	Site: Sub-controller (SIO): Description: Home Page:	Site 1: OO-TRNG-WX-JM2     SSP: 1.3: Storage Facility       SIO: 3 · Image: Site in the image: Sit
	Attributes Physical Address: Reply Channel: Send Channel: 4-Wre Configuration IP Addr: MAC Addr:	S     •       Port 2     •       Port 2     •       Inputs:     24       Outputs:     8       Readers:     8
Cancel Cancel Help	Mode: Cont	

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 | 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.
- 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.
- Double-click on the Aperio desktop icon.
   The New Installation dialog will appear.

Aperio® Programming Application		- 🗆 🗙
File Installation Help		
ONLINE OFFLINE	USB CABLE	
	A #	aperio
Quick scan Scan Refresh Connect	Disconnect Detect	
	© New Installation X	
	An installation represents a competer Apenode system.     The comparations of the installation Ammonum of 6 disactors with     upper activity of the installation Ammonum of 6 disactors with     upper activity of the installation Ammonum of 6 disactors with     upper activity of the installation Ammonum of 6 disactors with     upper activity of the installation Ammonum of 6 disactors with     upper activity of the installation Ammonum of 6 disactors with     upper activity of the installation ammonum     or disactors and within the ofference installations     members within the installation ammonum     preserve         extension         extension	
R USB radio dongle not connected		

- 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.

🤤 New Installat	ion X	<				
Installation An installation represents a complete Aperio® system. The password is used to securely encrypt all settings and configurations for the installation. A minimum of 8 characters with uppercase, lowercase, and numbers is required. The installation name can not be used as password. The key file contains unique keys that are used to secure the radio communication and prevent unauthorized reconfiguration of the system. Do <i>not</i> use the same key file for different installations.						
Installation Name	New Aperio Hub					
Password	•••••					
Confirm Password						
Key File	rio\Open Options-Open Options Test Bed-23549407.xml	]				
Import	Create Cancel					

- 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.

left Scan for communication hub(s)					
Select the communication hub(s) to retrieve information from Check the boxes for each Communication Hub and press "Show Details" to retrieve information. To select all, select the checkbox in the title row, or press Ctrl + "A" or Ctrl + "+". UHF Link is the signal quality between the USB radio dongle and the					
communication nub.			~		
Communication Hub	Radio Channels	UHF Link			
3ED9	11, 16, 25	al I	8		
3ED7	11, 16, 25		8		
F3D2	11, 16, 25	•••			
Rescan		Show Details	Cancel		

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.

		1.3	.3.08	3				
	8 📄	1. <u>3.3.R1</u>						
	8 📗	1.3	0-	Properties				
	8 📗	1.3	_	Deventeed				
	8 📗	1.3	$\overline{}$	Download				
	8 📗	1.3		Add Door	•		Create Aperio Door	
	8	1.3		Journal	+	-	Create Aperio Door (via Template)	
	-8	1.3		Defaults				
sor	nas Do	ors		Templates				
Eng	ite 1: E	NG		Homepage				
Sten	tofon		_					

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

- Door Objects	Common Propert	ies	
- Advanced - Macros - Auto Unlock - Notes	Address Site: Controller: Door Number:	Site 1: OO-TRNG-WX-JM2 1.3: Storage Facility ACM 2 Door Type: Normal	verner Stuations
	Other		
	Description:	Aperio Lockset	
	Home Page:		
	- Point Alarm Pro	nerties	
	Alternate Priority:	0   Security Level: Normal	•
		Do Not Load Home Page on Alam	
	Alam Media File:		
	Alarm Text:		
🖌 Ok			
	Camera:	"None"	<u> </u>
X Cancel	Templates	Shane S	
	Description:	None	
() Help	Application Notes:		

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

Global Access Level	4			
Name:	Warehouse Activation D			ate:
Default Time Schedule:	TS 001: Always	•	Deactivation Date:	
Access Level Category:	Access Level	•	Credential Function:	
Escort Requirements:	Not an Escort (def	Not an Escort (default)  Note: Creden		
Assigned 🔹 A	ddress 🖵 1	Description	•	Time Scheduk
1.	.1.D1	ACM 1		*Default
1.	.1.D2	ACM 2		*Default
🚽 1.	.3.D1	Lobby Door/ Warehouse		*Default
) 🔶 🔶 1.	.3.D2	Aperio Lockset		*Default

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



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