Schindler Integration Manual

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

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

Publish Date: November 21, 2019
Manual Number: BSH 1.0

Warranty

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

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

Open Options Software License Agreement

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

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

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

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

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

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

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

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

Table of Contents

This Page Intentionally Left Blank

Introduction 1

In This Chapter
√ Requirements √ Supported Panel Models

This section is designed to introduce you to DNA Fusion™ and the Schindler Destination Interface integration.

How This Section is Organized

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

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

Chapter 2, "Fusion/Schindler Integration and Installation," covers the Schindler integration installation and integration steps.

Chapter 3, "DNA Fusion Configuration," provides information on configuring Schindler settings in the DNA Fusion application.

Chapter 4, "Schindler in DNA Fusion," covers the various features available.

Icons and Conventions Used in This Manual

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

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

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

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

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

This Page Intentionally Left Blank

DNA Fusion/Schindler Overview

Open Options has partnered with Schindler to provide an integration designed to allow DNA Fusion to work with Schindler PORT Technology. DNA Fusion is a fully integrated component of the PORT Technology System. Each PORT terminal comes equipped with a radio frequency identification (RFID) sensor. When a passenger scans a pre-programmed RFID card at the PORT terminal, the system can verify that passenger's credentials through DNA Fusion and automatically call an elevator to transport that person to an authorized floor.

The DNA Fusion/Schindler integration interfaces with DNA Fusion version 7.5.0.33. It gives users the ability to manage their elevator dispatch control through the user-friendly DNA Fusion platform. Schindler's Destination Interface is a proven technology used in buildings around the world. DNA Fusion communicates with the Schindler third-party database and provides the ability to manage the cardholders access through Fusion. The integration creates a solution that allows both building and elevator access to be configured within DNA Fusion.

All access information is set up within the Schindler Port Technology system, and DNA Fusion allows the operator to set up special access levels that reference those Port Technology profiles. This allows cardholder, credential, and access information to be transferred in real-time to the Schindler Port Technology system.

Schindler

Minimum Requirements

The DNA Fusion driver and DNA Fusion/Schindler driver must be loaded on the same server.

Parameter	Minimum Software Requirements
Server Operating System	Windows 10, Windows 2012/2016/2019 Server
Client Operating System	Win 10, Win 2012/16/19 Server
DNA Fusion Version	7.0.0.1 or higher
Schindler Products	Schindler 5500 and 7000 Series Elevators
• Requires the Open Options Schindler Integration license	

NOTES:

DNA Fusion-Schindler Integration

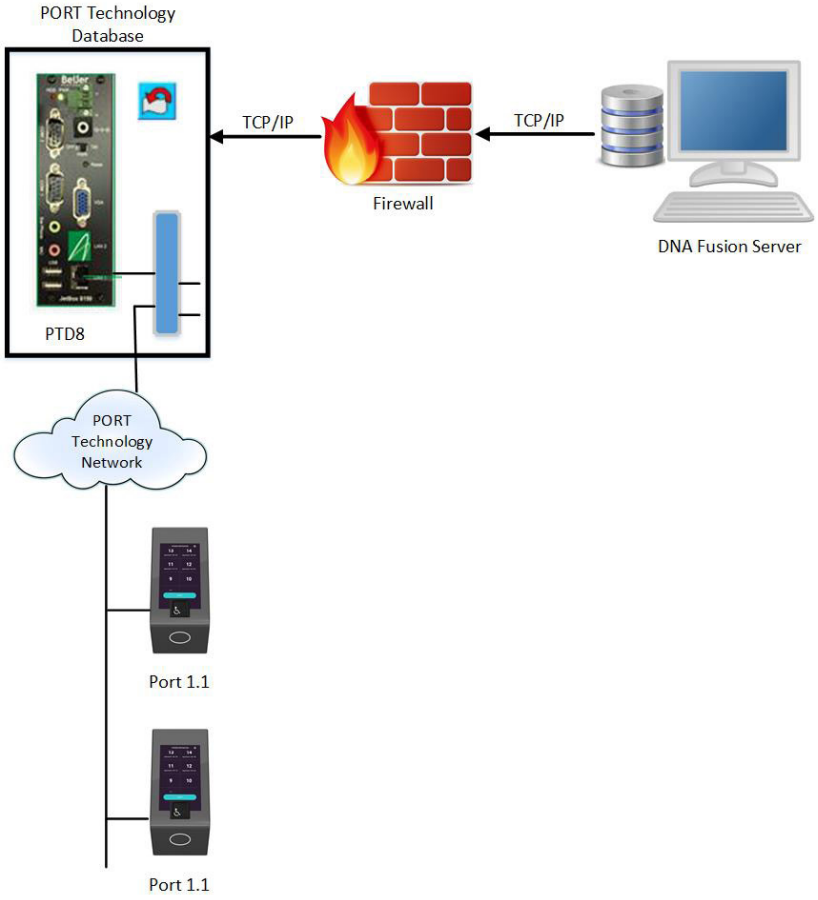
2

In This Section
√ Schindler Integration Installation √ Service Permissions

The Schindler integration is supported by DNA Fusion version 7.5.0.33 or higher. The integration requires the proper licensing to be in place prior to the installation of the integration software.

DNA Fusion™ interfaces with the Schindler PORT technology allowing for the interaction with both access control and elevator access from a single, common user interface. This is accomplished by integrating the Schindler third-party database with DNA Fusion. Unlike typical elevator integrations, DNA does not actively control the Schindler elevators and floors. The Schindler interface is a simple database synchronization mechanism.

When a cardholder is assigned a special Global Access Level that are linked to Schindler profiles, they are automatically synchronized with the Schindler system. Access transactions are blended seamlessly into DNA Fusion, becoming part of the standard Fusion system.



The site should only be licensed for Schindler elevators. If multiple elevator integrations are required, contact Open Options Technical Support.

Features and Functionality

The DNA Fusion / Schindler integration provides for a unified platform to configure access across both the DNA Fusion system and the Schindler PORT technology. The integration supports a number of features including:

- Automatic synchronization of cardholder data created in DNA Fusion
- Elevator activity is displayed in the Events grid
- Restrict floor entry based on the assigned Master Group (Access Level)

> *All elevator floor mapping and elevator access schedules are created in the Schindler system. DNAFusion does not obtain any programming information from the system. The Schindler system also controls the elevator reader modes.*

This chapter covers the installation and configuration of the DNA Fusion/Schindler driver as well Schindler configuration within DNA Fusion.

The following steps should be performed to complete the integration:

1. **Compile** a list of the Schindler Master Group and Profile names from the Schindler PORT system.
2. **Verify** the Schindler PORT system is configured to use the Generic Wiegand (38) format.
3. **Note** the specific card formats in the Schindler system, i.e., HID 26 Bit, Corporate Card, etc.

   DNA is preconfigured with eight (8) card formats. If not included, contact Open Options Technical Support.
4. **Run** the DNA Fusion-Schindler Integration application.
5. **Configure** the Schindler settings in DNA Fusion.

   See Chapter 3: DNA Configuration of more information.
6. **Create** the Master Groups.

   Each card is assigned a Master Group. Only one Master Group can be applied to a card. The Master Group must have the same naming convention as the Schindler PORT system.
7. **Manage** Profiles.

   A profile is basically an access level in DNA Fusion. The profile determines which floors a cardholder can access. The Profile must have the same naming scheme as Schindler's PORT Profile.

Schindler Installation and Configuration

DNA-Schindler Integration Installation

The integration installation process is very straightforward and can be performed without any knowledge of the software.

1. **Obtain** the dnaFusion Schindler Install application from the Open Options website or contact Technical Support.

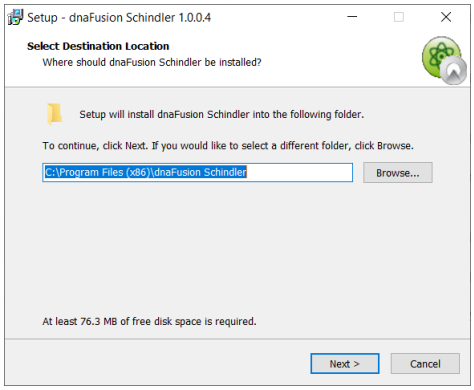
2. **Verify** the DNA Fusion DNADrvr32 Service Permissions.

   The DNA driver and the Schindler 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.

> ***The Schindler integration must be installed on the computer that hosts the DNA Fusion driver** (DNAdrvr32). **Contact Open Options Technical Support to obtain the Schindler installation file.***

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

   The Destination Location dialog appears.

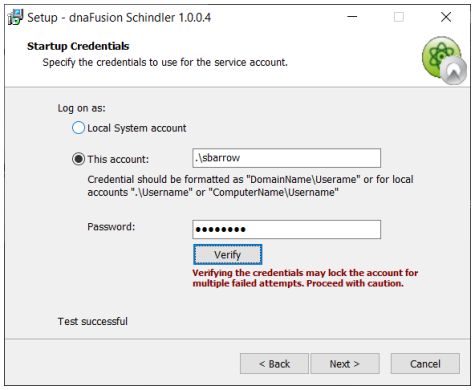


4. **Click** the Next button to continue the installation or **select** the Browse button and specify a different location.

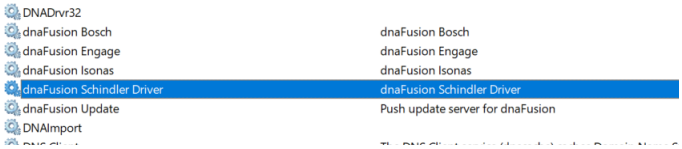
   The default location is C:\Program Files (x86)\dnaFusion Schindler.

   The Startup Credentials screen appears.

5. **Select** This Account, **enter** the credentials obtained in step 2, and **click** Next.



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



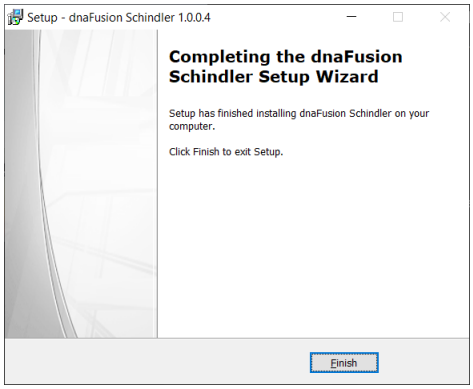
> ***Open Options recommends using the same account for both the DNA Fusion driver** (DNAdrvr32) and the DNA Fusion Bosch driver. **See page 2-7 for more information on the DNA Fusion driver service.***

The Ready to Install screen appears.

6. **Click** the Install button to start the process.

   When the installation is complete, the Install Complete screen opens.

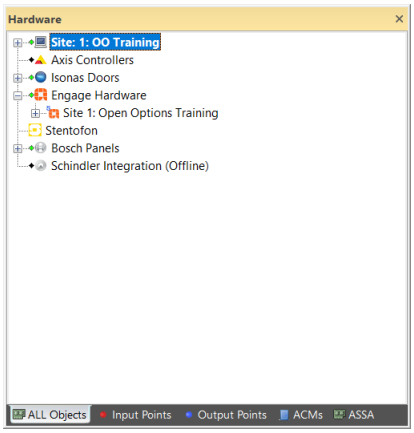
7. **Click** the Finish button to complete the installation.

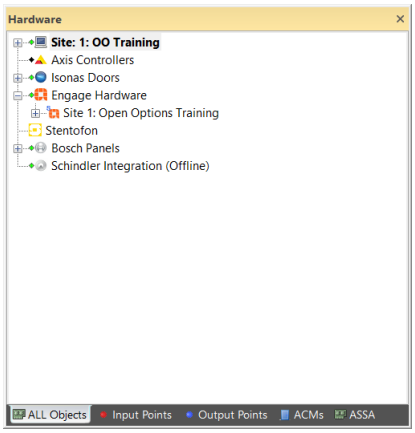


8. **Configure** the Schindler within the DNA Fusion application.

   See Chapter 3: DNA Configuration for more information.

   Once the integration is completed, the DNAFusion Schindler service will start. In the DNA Fusion Hardware Browser, the diamond next to the Schindler node will turn green. See page 3-1 for driver status color indicators.





The status will show "Offline" until the settings have been configured 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.

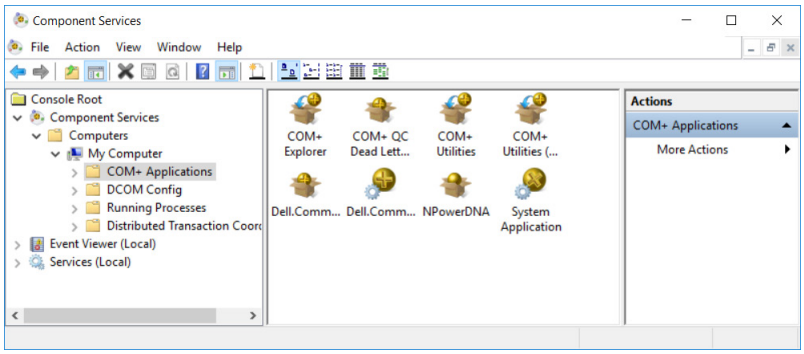
   To access Component Services, **type** the name in the Windows Start Search Bar and **select** the Component Services option from the list.

   The Component Services window opens.

2. **Double-click** the Computers item.

3. **Double-click** the My Computer icon and **open** the COM+ Applications 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 DNA Fusion Bosch service will require the same information. This also applies to the DNA Driver (DNAdrvr32) service.

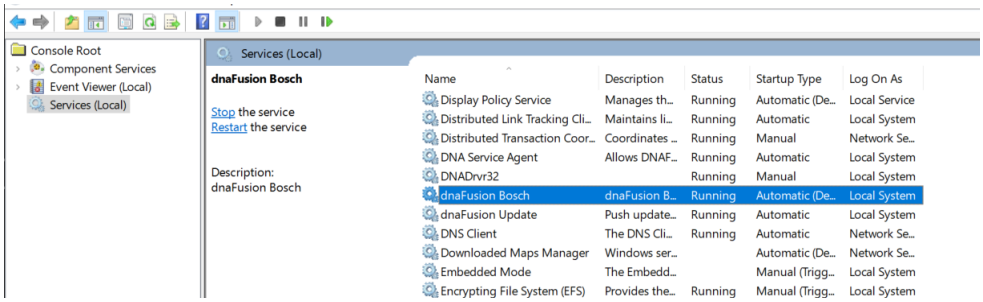
6. **Click** the OK button.

DNA Fusion Driver Service

1. From the Component Services dialog, **select** the Services option or **open** the Services window.

   The Services dialog will populate.

2. **Locate** the DNADrvr32 service.

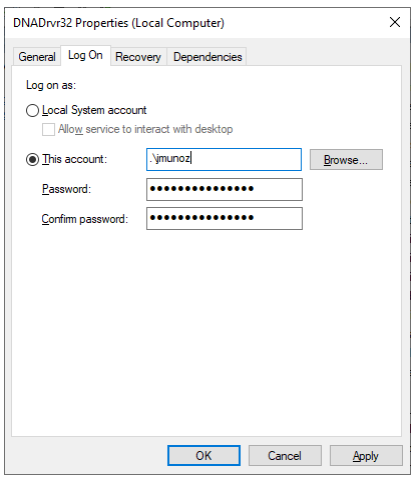


3. **Right-click** on the DNADrvr32 service and **select** the Properties option.

   The DNADrvr32 Properties dialog will open.

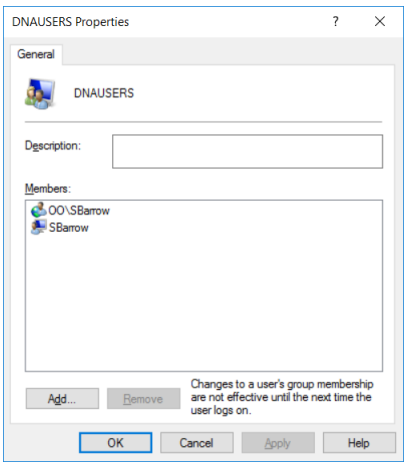
4. **Select** the Log On tab and **verify** the user configuration.

   Keep in mind this must be the same account used to run the NPowerDNA COM+ Object as well as the DNAFusion Bosch service which is configured on page 2-3.



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 option.
3. **Select** the Groups folder and **right-click** on the DNAUSERS group.
4. **Select** Add to Group from the menu.
   The DNAUSERS Properties dialog appears.
5. **Verify** the service account is listed in the dialog.
   If the account is not listed, **click** the Add button and **enter** the account's information.



6. **Click** the OK button to save any changes and close the dialog.

> *It is important that the account running the DNA Driver and Schindler Driver are in DNAUSERS group.*

DNA Fusion Configuration 3

In This Section
√ Adding the Schindler PORT to DNAFusion √ Configuring Doors √ Access Level Creation

The DNAFusion/Schindler PORT integration coordinates the Schindler elevator system with DNAFusion to ensure smooth and efficient passenger transportation. The brain behind The PORT Technology is a powerful software system that uses information to guide and transport people quickly and safely to their individual destinations, communicating with them through a simple yet elegant device called the PORT (Personal Occupant Requirement Terminal).

Once the Schindler integration has been installed, the PORT information can be added to DNA Fusion. The Schindler integration requires the correct licensing to be in place prior to adding the hardware to the DNA Fusion software.

> *DNAFusion provides Schindler specific operator permissions. The Admin profile inherently receives access to the permissions however other profiles may need to be edited to provide the create profile permissions. See chapter 4 in the User Manual for more information.*

To configure the Schindler PORT within the DNA Fusion application complete the following steps:

1. **Add** the Schindler PORT settings to DNA Fusion.
2. **Create** the Master Groups.

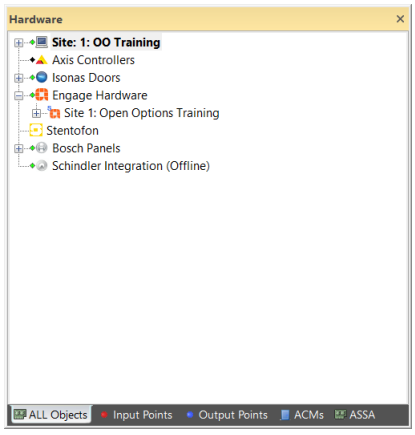
   Each card is assigned a Master Group. Only one Master Group can be applied to a card. The Master Group must have the same naming convention as the Schindler PORT system.
3. **Manage** Profiles.

   A profile is basically an access level in DNA Fusion. The profile determines which floors a cardholder can access. The Profile must have the same naming scheme as Schindler's PORT Profile.
4. **Configure** the Card Format(s).

Adding the Schindler PORT to DNA Fusion

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

   The Hardware Browser opens.



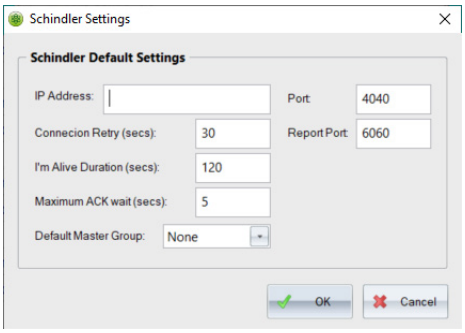
   The "Offline" status will display until the settings have been configured.

Status Indicators:

- Green Diamond - The DNAFusion Schindler driver is running and all systems are good.
- Black Diamond - The DNAFusion Schindler driver is inactive. Verify the DNADrvr32 and DNAFusion Schindler services are running under the correct identity. See page 2-7 for more information on service accounts.
- Yellow Diamond - The driver is running but unable to open the connection used to communicate status to DNA.
- Red Diamond - The driver is running but unable to open the connection used to communicate status to DNA.
- Purple Diamond - The Schindler driver is running but unable to open either the events or status connections to DNA.

2. **Right click** on the Schindler node and **select** Settings.

   The Schindler Settings dialog opens.



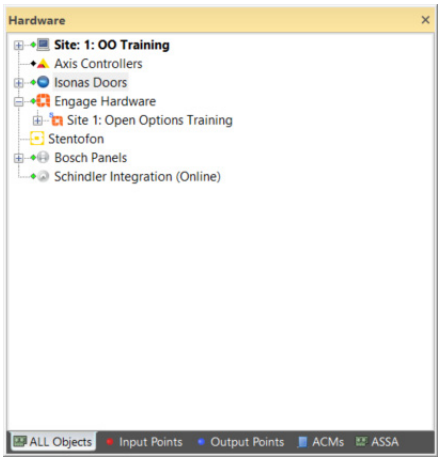
3. **Enter** the IP Address for the Schindler PORT system.

   This information will typically be obtained from the Schindler Job Site Engineer. It is important that the correct IP address be configured.

   Port assignments should only be changed if instructed by Schindler engineers. The Report Port is used for sites running the "Live Reporting Interface". The default Port is 4040 and the Report Port is 6060.

4. **Click** the Ok button to save the settings.

   The Schindler PORT will begin communication and "Online" will be displayed next to the Schindler node in the Hardware Browser.



   There is no physical hardware to bring online. Continue to Configuring Master Groups on page 3-3.

Configuring Master Groups

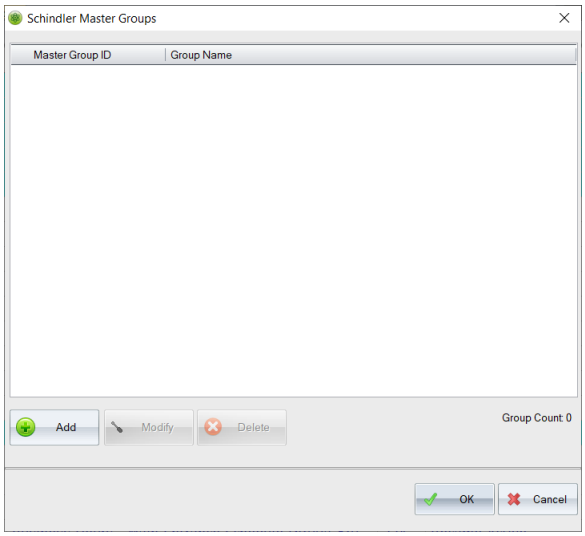
Master Groups must be created to match the Schindler groups. It is critical that the names match exactly including character case, spaces, and spelling.

The card must be assigned to a Master Group before it will be loaded into the Schindler PORT system. Each card can only be associated with one (1) Master Group.

To create the Master Group:

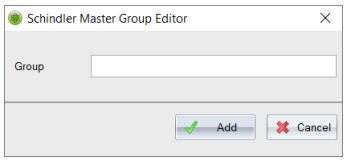
1. **Right-click** on the Schindler node in the Hardware Browser.

   The Schindler Master Groups dialog opens.



2. **Click** the Add button.

   The Schindler Master Group Editor opens.

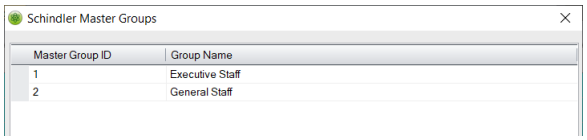


3. **Enter** the Master Group Name.

   This must match the Schindler Group name exactly including character case and spaces. It is critical for the information to be consistent. If this is inaccurate, the cardholder will not be downloaded to the Schindler PORT system.

4. **Click** the Add button to save the name.

   The Master Group appears in the list.



   If the Master Group is edited, all associated cardholders will be updated in the Schindler system. If a Master Group is deleted, DNA Fusion will send the Schindler system a command to delete the records**.**

5. **Repeat** steps 2 through 4 until all Master Groups have been configured.

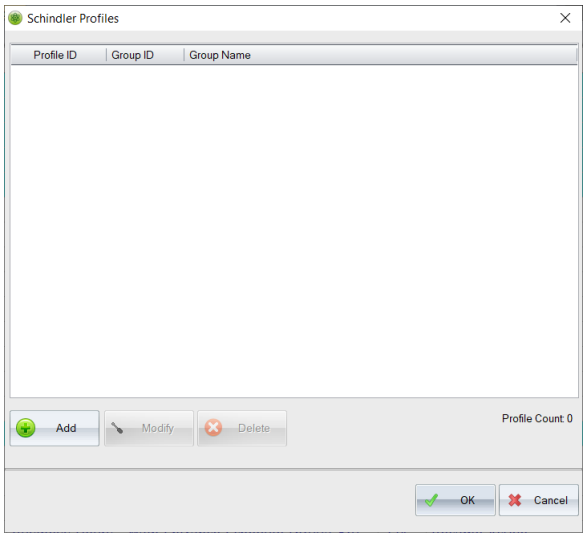
> Remember DNA does not actively control the Schindler elevators and floors. All elevator floor mapping and elevator access schedules are created and maintained in the Schindler system through master groups and profiles.

Creating Profiles

A Schindler Profile is equivalent to an Access Level in DNA Fusion. It defines the floor control in the Schindler PORT system and contains the information required by Schindler to determine the floors the cardholder can access. The profile in DNA Fusion must match the profile in Schindler exactly. This includes any capitalized letters, punctuation and spaces. Once the profile is created, DNA Fusion generates a Global Access Level Group that aligns with the Profile.

1. From the Hardware Browser, **right-click** on Schindler node and **select** Manage Profiles from the resulting menu.

   The Schindler Profiles dialog opens.



2. **Click** the Add button.

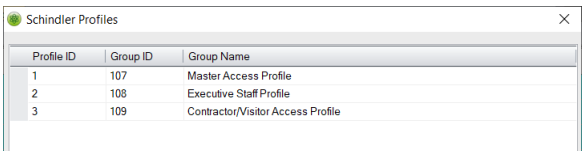
   The Schindler Profile Editor opens.

3. **Enter** the Profile Name.

   This must match the Schindler Profile name exactly including character case and spaces. It is critical for the information to be consistent. If this is inaccurate, the cardholder will not be downloaded to the Schindler PORT system.

4. **Click** the Add button to save the name.

   The new Profile appears in the list.



   DNA Fusion creates a Global Access Level that corresponds with the Schindler profile. The access level appears with a green icon on the levels folder. The Global Access Level does not contain any doors and is an access level that can assigned to a cardholder.

5. **Repeat** steps 2 through 4 until all Profiles have been added to DNA Fusion.

> Remember DNA does not actively control the Schindler elevators and floors. All elevator floor mapping and elevator access schedules are created and maintained in the Schindler system through master groups and profiles.

Adding Card Formats

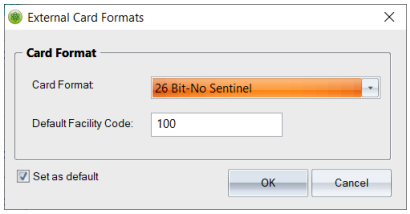
In order for the card to be synchronized with the Schindler PORT system, the credentials must be encoded to match the Schindler card reader's special formats. Each card must have a card format assigned to it for the cardholder to be synced with Schindler. There are eight (8) predefined card formats in DNA Fusion 7.5.0.30.

To simplify the process, a default card format can be configured. This will automatically populate on the cardholder record. If needed, the format can be changed in the record.

To create the card format:

1. From the Hardware Browser, **right-click** on Schindler node and **select** Card Formats from the context menu.

   The External Card Formats dialog opens.



2. **Select** the desired Card Format from the drop down menu.

   There are eight (8) predefined card formats in DNA Fusion 7.5.0.30. If additional formats are needed, please contact Open Options Technical Support.

3. **Enter** the Default Facility Code.

   Each format can assigned a Default Facility Code. When assigning a card format to a cardholder the default facility code will automatically be assigned to the card. If needed, the operator can manually change the facility code in the card record.

4. If desired, **select** the Set a Default checkbox.

   Only one format may be designated as the 'Default' format. When adding a new card, the designated format will automatically be assigned to the card. This can be overridden at the card level as needed.

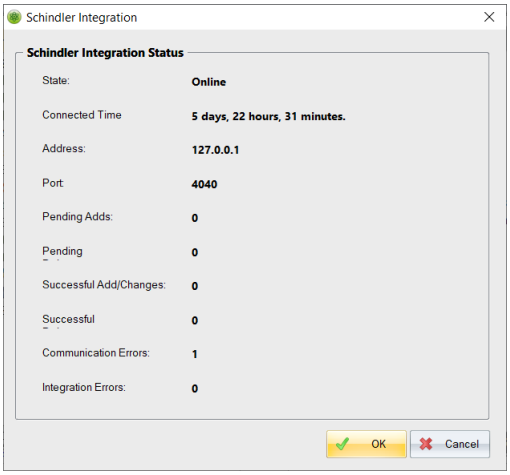
5. **Click** the Ok button to save the changes.

Schindler Integration Status

DNA Fusion provides a quick status screen the displays the state of the Schindler integration including any communication and synchronization errors.

1. From the Hardware Browser, **right-click** on Schindler node and **select** Status from the menu.

   The Schindler Integration Status dialog opens.



   The connection status and time along with port information and pending changes is displayed. The dialog provides information on communication and integration errors.

This Page Intentionally Left Blank

Schindler in DNA Fusion 4

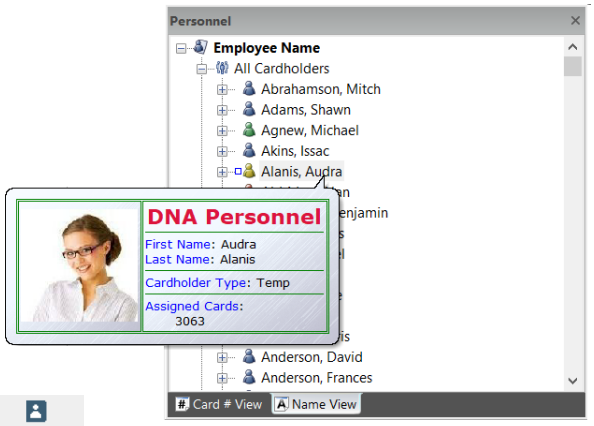
In This Chapter
√ Assigning Schindler Access to a Cardholder √ Generating Reports

The DNA Fusion/Schindler integration allows the operator to add the Schindler access level (profile) to the cardholder. There are reporting features that allow the operator to access information on the fly.

The Personnel Browser

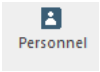
The Personnel Browser is an explorer window that contains essential information about system cardholders, including their names, card numbers, and personnel groups. The browser tree uses the following color-coded icons to represent personnel and card types:

- Blue - Normal
- Green - Visitor
- Yellow - Temporary
- Red - Disabled
- Purple - Contractor
- Orange - Vendor
- White (1-5) - Custom Types



To open the Personnel Browser:

1. **Click** the Personnel button on the Standard Toolbar.



OR

Select View / Explorers / Personnel from the Main Menu.

The Personnel Browser opens.

The browser contains two default tabs (located at the bottom): Name View and Card # View.

Managing Personnel

DNA Fusion offers a variety of personnel management features. For more information on cardholders, see Chapter 3: Personnel in the DNA Fusion User Manual.

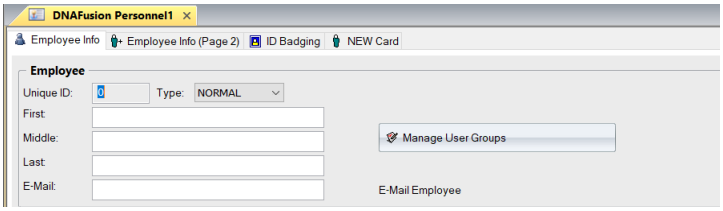
Adding Cardholders

1. **Right-click** inside the Personnel Browser and **select** Add New Cardholder.

   OR

   Select Add Cardholder from the Personnel Toolbar.

   A blank Personnel Record opens.



2. Continue to page 4-3 for managing cardholders.

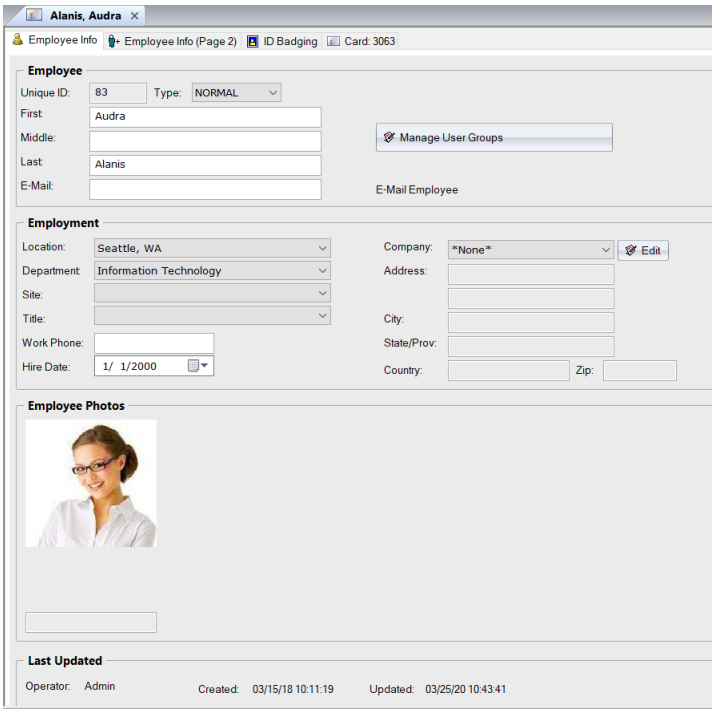
Opening Existing Cardholder Records

1. **Right-click** on the Cardholder Record and **select** Properties.

   OR

   Double click on the desired Cardholder from the Personnel Browser.

   The Personnel Record opens.



2. **Continue** to page 4-3 for managing cardholders.

Required Fields

In order for the cardholder record to be synchronized with the Schindler PORT system, there are a number of fields that must be properly configured.

Element	Required	Match Schindler Value	Notes
Person ID	Yes		Used by DNA Fusion
First Name	Yes		Personnel First Name
Last Name	Yes		Personnel Last Name
Department	No		Personnel Department
Start Date	Yes		Personnel Start Date
Stop Date	Yes		Personnel Stop Date
Credential Number	Yes		Specific encoded value. Requires the correct card format and credential number.
Master Group	**Yes**	**Yes**	This value must exist with the exact name in the PORT system. See page 3-3 for more information.
Profile	**Yes**	**Yes**	This value must exist with the exact name in the PORT system. See page 3-4 for more information.

Managing Cardholders

For detailed information on personnel, see Chapter 7: Personnel in DNA Fusion User Manual.

1. **Complete** the desired fields in each tab.

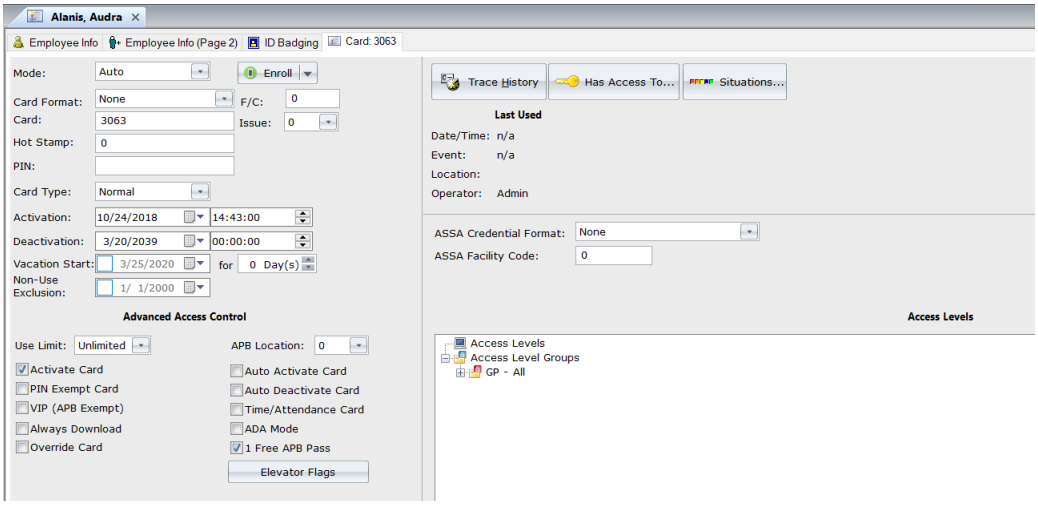
   See pages 7-7 through 7-12 in the DNA User Manual for a description of each field.

2. **Select** the New Card tab.

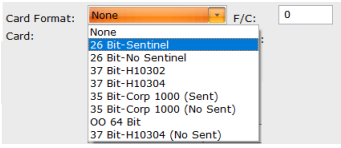
   OR

   Select the desired Card Number tab.

   The Card record opens.

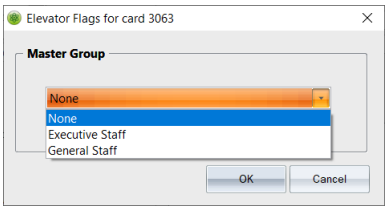


3. If needed, **select** the Card Format from the drop down list and **enter** the Facility Code (F/C). This will only be required for locations with multiple F/C.



4. **Select** the Elevator Flags button.

   The Elevator Flags/Master Group dialog opens.



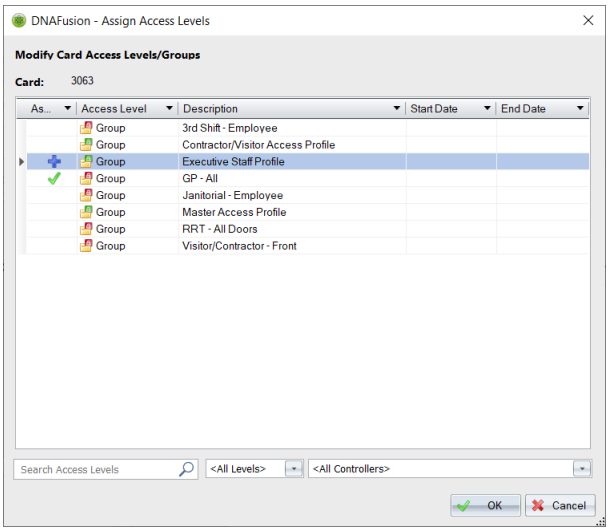
   The card must be assigned to a Master Group. This is a required component for Schindler PORT access. Each card can only be associated with one (1) Master Group.

5. **Click** the OK button.

6. **Right-click** in the Personnel Record and **select** Update.

7. **Right-click** in the Access Levels section and **select** Add/Remove/Modify Access from the menu.

   The Assign Access Levels dialog opens.



8. **Select** the appropriate Profile and/or Access Levels.

   Schindler profiles can be identified by the green icon on the access level folder. Assigning a profile can be accomplished in a number of different manners including drag and drop however the card can only be assigned one (1) profile. This is a required PORT component.

   For more information on assigning access levels, see page 7-13 in the DNA Fusion User manual.

9. To save the record, **click** Update Cardholder on the Personnel Toolbar or **right-click** in the Personnel Record and **select** Update.

NOTES:

Schindler InfoReady Reports

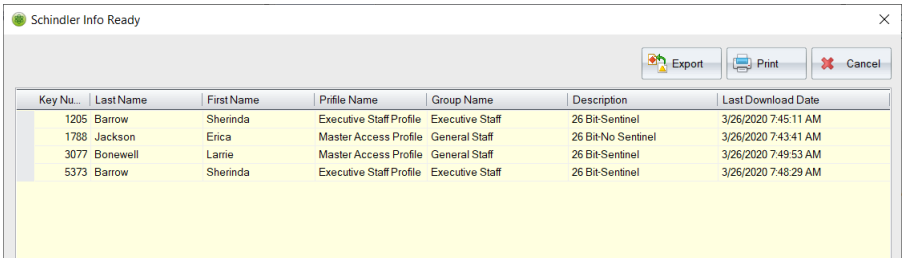
There are a number of quick and easy InfoReady reports available for the Schindler integration. For instance, you can see who has access to a specific access level.

Schindler Hardware InfoReady Report

This feature allows you to generate an immediate report that details who has access to the Schindler PORT system through DNA Fusion.

1. **Right-click** on the Schindler node and **select** Info Ready from the menu.

   The Schindler Info Ready dialog appears. It displays the cardholders that have access along with the profile and group assigned to the cardholder.



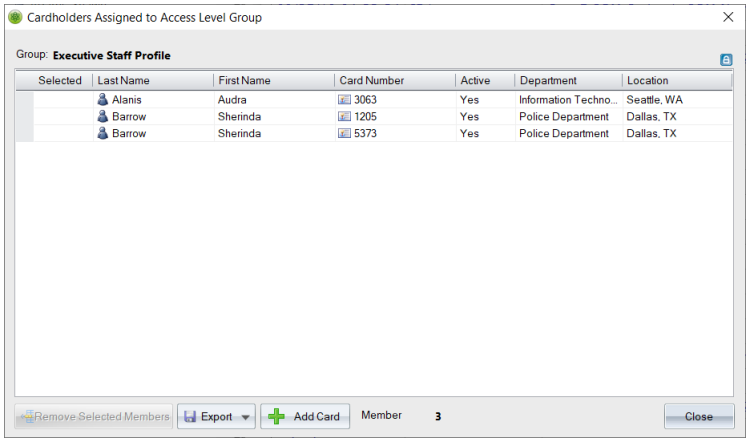
   The results can be exported, printed or e-mailed by selecting the appropriate button.

Access Level Assigned To InfoReady Report

The Assigned To feature is an InfoReady report that allows the operator to audit the cardholders assigned to a global access level group as well as Schindler Profile levels. It can also be used to add and remove the access level group from selected cards.

1. **Right-click** on the Access Level Group in the Access Levels Browser and **select** Assigned To.

   The Cardholders Assigned to Access Level Group dialog opens.



   To remove the access level group from a card: **select** the desired card(s) in the Selected column and **click** the Remove Selected Members button.

   A confirmation dialog will appear; **click** Yes to remove the access level group.

   The results can be printed or exported to a CSV file (.csv) by **selecting** the Print or Export button.

2. If needed, **click** the Export button and select the desired format:
   - Export Grid to CSV File - Exports the report to a CSV file (.csv).
   - Export Grid to Clipboard - Exports the report to the operator's clipboard.
3. **Click** Close to close the dialog.


OPEN OPTIONS®
ACCESS TECHNOLOGY