



OPEN OPTIONS®
— ACCESS TECHNOLOGY —



dna**Fusion**™

Technical Installation Manual



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 Open Options, LLC assumes no responsibility for incorrect or outdated information that may be contained in this publication.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™ and SSP™ are trademarks of Open Options, LLC.

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.

This manual has been written for DNA Fusion™ version 7.7 or higher.

Publish Date: June 25, 2020

Manual Number: TM-7.0

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

Warranty

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



16650 Westgrove Dr | Suite 150

Addison, TX 75001

Phone: (972) 818-7001

Fax (972) 818-7003

www.ooaccess.com

Open Options 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 UNINTERRUPTED 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

Chapter 1: Introduction

How This Manual Is Organized.....	1-1
Icons and Conventions Used in This Manual	1-1

Chapter 2: Installation

Installation Types	2-1
Computer Specifications	2-3
Server Specifications	2-3
Corporate Server w/SQL Express Database (< 20 doors / <5 clients).....	2-3
Enterprise Server PC w/SQL Server Database	2-3
Client Specifications.....	2-5
Client Workstation w/Photo ID	2-5
Server / Client Requirements	2-7
Network Requirements	2-7
Services Account Credentials	2-7
User Group Setup.....	2-8
Domain User Group Setup (DNA_Global).....	2-8
Server Installation & Configuration	2-9
Server Installation.....	2-9
Server Configuration.....	2-13
Adding Users to the DNAUSERS Group.....	2-13
Testing the Settings	2-14
Database Permissions	2-15
Client Installation	2-17
Firewall Configuration	2-19
Configuring ODBC Data Sources	2-20
Configuring the Windows Server	2-21
Windows 2008 Server	2-21
Windows 2012 Server	2-23
Windows 2016 Server	2-25
Windows 2019 Server	2-27
Migrating DNA Fusion to a New Server	2-29
Migrating with Server/Client Components on the Same Workstation	2-29
Migrating with Server and Client Components on Separate Workstations	2-30

Chapter 3: Hardware Configuration

Configuring Hardware	3-1
Hardware Browser.....	3-1
Configuring the Browser	3-1
Hardware Toolbar	3-2
Adding Hardware	3-3
Creating and Linking a Site	3-3

Creating a Site	3-3
Linking to a Site	3-4
Adding a Controller (SSP)	3-5
Adding a Channel	3-7
Ethernet (TCP/IP) Channel	3-9
IP Client - Remote (TCP/IP).....	3-9
Serial Channel.....	3-10
Modem Channel.....	3-10
Controller Properties	3-11
Controller Properties	3-11
Channels	3-11
Attributes	3-11
Controller Time Parameters.....	3-12
Connection	3-12
Downstream Ports	3-12
Stored Quantities	3-13
Controller Memory	3-13
Offline Transaction Capacity	3-13
Controller Flags	3-13
Quantities.....	3-14
Elevator Control	3-14
PIN and Duress Options.....	3-14
Cards & Dual Comm	3-15
Card Formats (Assets).....	3-15
Alternate Ports	3-15
Batch Processing	3-15
Adding Subcontrollers	3-17
Subcontroller Properties	3-19
Sub-controller.....	3-19
Address.....	3-19
Attributes	3-19
Advanced	3-21
Advanced Properties.....	3-21
Continuations.....	3-21
Identification.....	3-21
Updating Subcontroller Firmware.....	3-21
Adding Doors	3-23
Adding a Single Door	3-23
Adding an In and Out Door	3-24
Adding a Turnstile.....	3-25
Adding a Door From a Reader	3-26
Door Properties	3-27
Common Properties	3-27
Address.....	3-27
Other	3-27
Point Alarm Properties.....	3-28
Templates.....	3-28
Door Objects	3-29

Door Parameters	3-29
Reader	3-29
Contact	3-30
Request to Exit (REX)	3-30
Out Reader	3-30
Strike	3-30
ADA Settings	3-30
Advanced	3-31
Anti-Pass Back (APB) Settings	3-31
Door Parameters	3-32
Logging Based on Deny Violations	3-33
Secondary Request to Exit (REX)	3-33
Secondary Reader	3-33
Macros	3-33
Door Sounder	3-33
Alarm Conditions	3-34
Normal Conditions	3-34
Auto Unlock	3-35
Follows Schedule	3-35
First Person Unlock	3-35
Adding Elevators	3-37
Elevator Properties	3-39
Common Properties	3-39
Address	3-39
Other	3-39
Point Alarm Properties	3-40
Templates	3-40
Elevator Objects	3-41
Elevator Parameters	3-41
Reader	3-41
Inputs and Outputs	3-41
Floor Groups	3-41
Secondary (Biometric) Reader	3-41
Elevator Parameters	3-43
Attributes	3-43
Anti-Passback (APB)	3-43
Elevator Functions	3-44
Advanced Functions	3-44
Auto Unlock	3-45
Configuring Readers	3-46
Reader Properties	3-46
Common Properties	3-46
Address	3-46
Distribution / Other	3-46
Templates	3-46
Reader Properties	3-47
Reader Properties	3-47
Card Data Format	3-47

Advanced Properties.....	3-47
OSDP	3-47
Configuring Input Points	3-49
Input Properties	3-49
Common Properties	3-49
Address.....	3-49
Distribution / Other.....	3-49
Alarm Properties.....	3-49
Templates.....	3-50
Input Properties	3-51
Input Point Properties.....	3-51
Advanced Features.....	3-52
Configuring Output Points	3-53
Output Properties	3-53
Common Properties	3-53
Address.....	3-53
Distribution / Other.....	3-53
Alarm Properties.....	3-53
Templates.....	3-54
Output Properties	3-54
Output Properties	3-54
Advanced Properties	3-54
Adding NVR/DVRs	3-55
Installing the NVR/DVR Integration	3-55
Configuring the NVR/DVR	3-56
Adding the Cameras	3-57
Associating a DVR Camera with a Door.....	3-58
Card Formats	3-59
Configuring Card Formats	3-59
Creating a New Card Format	3-59
Copying a Card Format.....	3-59
Editing a Card Format	3-59
Gathering Card Format Information	3-60
Assigning a Card Format to the SSP	3-60
Corporate Mode Card Format	3-61
Multiple Facility Code Card Formats.....	3-62
Chapter 4: Upgrading DNA	
Software Upgrades	4-1
DNA Fusion Full Upgrade	4-1
Fusion Client Upgrades.....	4-3
Fusion Service Pack	4-3
NPower DNA to DNA Fusion 5.0 and above.....	4-4
License Updates	4-5
Chapter 5: Additional Apps	
Controller Connection Utility	5-3
Table Purger Tool	5-5
DNA Batch Download Settings Utility	5-6

DNA LED Control Application	5-6
DNA AutoExpire Tool	5-7
Running the Configuration Mode	5-7
Running the Silent Mode.....	5-7
DNA Event History Report Utility	5-9
Installation	5-9
E-Mail Authentication	5-9
Configuring the Event History Report Parameters	5-10
Scheduling a Report.....	5-11
Edit a Scheduled Report.....	5-11
Delete a Scheduled Report	5-11
DNA Time and Attendance Report	5-13
Installing the Time & Attendance Report	5-13
Setting up the Time & Attendance Report	5-14
HBMacro SQL Statement.....	5-16
Generating a Time & Attendance Report	5-17
DNA Import Tool	5-19
Running the Import Tool.....	5-19
Permissions Issues	5-20
Batch Printer	5-21
Opening the Batch Printer.....	5-21
Batch Printer Toolbar	5-21
Adding a New Batch.....	5-22
Modifying a Batch.....	5-22
Removing a Batch	5-23
Printing Batches	5-23
Exporting a Batch	5-23
DNA Diagnostics	5-25
Submitting Diagnostics.....	5-26
Saving Diagnostics	5-26
Browsing to a Log File.....	5-27
Starting and Stopping a Service	5-27
Downloading the License File	5-28

Appendix A: Troubleshooting

Locating the DNA Driver Version	A-1
COM Surrogate Errors	A-2
Starting and Stopping the Services	A-2
Driver	A-2
SQL Server.....	A-2
Client-to-Server Troubleshooting	A-3

Appendix B: Process Diagrams

Server Installation	B-1
Client Installation	B-3
Server/Client Setup	B-4
Adding Hardware Guide	B-5
Adding a Controller and Bringing it Online	B-6
Bringing a Door Online	B-7
Configuring Card Formats	B-8

This Page Intentionally Left Blank

Introduction

1

In This Chapter

✓ Manual Overview

This manual is designed to introduce you to DNA Fusion™ and explain the installation and hardware setup.

How This Manual Is Organized

This manual is divided into five chapters and four appendixes:

Chapter 1, "Introduction," provides an overview of the Technical Installation Manual.

Chapter 2, "Installation," covers the software installation for server and client workstations as well as the requirements and specifications for each configuration type.

Chapter 3, "Hardware Configuration," instructs the user how to add and set up hardware in DNA Fusion.

Chapter 4, "DNA Upgrades," provides information about upgrading the DNA Fusion system.

Chapter 5, "Additional Apps," provides information about additional applications that supplement the DNA Fusion system.

Appendix A, "Troubleshooting," covers troubleshooting steps for Serial and Ethernet installations.




Appendix B, "Process Diagrams," includes a series of flowcharts to illustrate key installation procedures.

Appendix C, "Command Line Parameters," includes a list of available command line parameters.

Appendix D, "Index," provides an alphabetized list of terms and concepts used in this manual, as well as corresponding page references.

Icons and Conventions Used in This Manual

The following icons call attention to useful or important information:

	This icon highlights time-saving hints, useful tips, and helpful shortcuts.
	This icon designates information that is important enough to keep filed in an easily accessible portion of your gray matter.
	If an action could damage the system, cost big bucks, lock the operator out of the system, or otherwise bring an end to civilization as we know it, it will be marked by this icon.

In addition to the icons above, this guide uses several typeface conventions to improve readability:

- **Special:** Indicates a menu item, toolbar selection, button, or system message.
- **Boldface:** Indicates a specific instruction or user action; usually appears in numbered steps.

This Page Intentionally Left Blank

Installation

2

In This Chapter

- ✓ DNA Fusion Requirements & Specifications
- ✓ Server Installation & Configuration
- ✓ Client Installation
- ✓ Firewall Configuration
- ✓ Configuring a Windows 2008/2012/2016/2019 Server
- ✓ ODBC Configuration
- ✓ Migrating DNA Fusion to a New Server

The DNA Fusion installation process is very straightforward and can be performed without any knowledge of the software. Before installing the application, verify that the computer meets the minimum requirements outlined on pages 2-3 through 2-5.

This chapter addresses the installation of the DNA Fusion software on both server and client machines.

Installation Types

This chapter covers two types of installation:

- Server - The computer that hosts the DNA Fusion database and runs the DNA driver.
 - ▣ The server's role may be separated into a Database Server and an Application Server.
- Client - A computer that connects to the DNA system via the Local Area Network (LAN) and Wide Area Network (WAN) but retrieves and saves data to and from the DNA Fusion database.

The DNA Fusion 7.0 setup includes both installations for SQL Server 2012 R2 Express. Each installation has its own requirements, specifications, and tasks.



The setup procedure for both the Database Server and the Client machines must be performed with an administrator logon.

The setup procedure must be performed for the Database Server prior to any Client machines.



If DNA Fusion is being installed on a Windows 2008, 2012, 2016, or 2019 Server, follow the configuration steps that begin on page 2-21. The Application Server role should be configured prior to installing DNA Fusion.



The setup procedure described in this manual is a typical installation. If the database and driver need to reside on separate servers, contact Open Options Technical Support for documentation.

This Page Intentionally Left Blank

Computer Specifications

These specifications are intended to serve as a baseline and do not take into account all the variables of each unique system. They are subject to change without notice.

DNA Fusion is not supported on home or mobile versions of Windows operating systems.

Server Specifications

The following specifications are configuration guidelines for your DNA server. In this instance, the DNA server refers to the PC that will host your DNA database.

Corporate Server w/SQL Express Database (< 20 doors / <5 clients)

PARAMETER	RECOMMENDED SPECIFICATION
Processor Speed	Intel Core i5 2.8 GHz + (or equivalent)
System Memory (RAM)	4 GB
Network Card	10/100 Ethernet Network Card
Hard Drive Size	250 GB
Graphics Card	VGA Support for 1024 x 768 resolution or higher
Video Memory (VRAM)	256 MB
Backup Device	YES
CD-RW Drive	YES
Operating System	Windows 2008 R2/2012 Server R2, Windows Server 2016 Windows 7, Windows 8, Windows 10 (32 and 64 bit support), Windows Server 2019
Optional	UPS (Uninterrupted Power Supply)
<ul style="list-style-type: none"> This specification is ideal for systems with less than 20 doors, 200 cardholders, or 1,000 transactions per day. DNA ships with a Microsoft Server 2012 SQL Express has a database size limit of 10 GB. 	



DNA Fusion is not supported on Home or Mobile versions of Windows OS.



If needed, SQL 2008 Express is available as a free download at the Microsoft website. <https://www.microsoft.com/en-us/download/details.aspx?id=1695>.

Enterprise Server PC w/SQL Server Database

PARAMETER	RECOMMENDED SPECIFICATION
Processor Speed	Intel Core i5 2.8 GHz + (or equivalent, multi-core)
Dual Processor	YES
System Memory (RAM)	8 GB +
Network Card	10/100 Ethernet Network Card
Hard Drive Size	500 GB
Graphics Card	VGA Support for 1024 x 768 resolution or higher
Video Memory (VRAM)	512 MB
Backup Device	YES
CD-RW Drive	YES
Operating System	Windows 2008 R2/2012 R2 Server, Windows Server 2016, Windows Server 2019
Database	Microsoft SQL 2005 through SQL 2016

PARAMETER	RECOMMENDED SPECIFICATION
Optional	Separate Database & Application Servers* UPS (Uninterrupted Power Supply) Isolated Database Server/Application Server Multi-Processor
<ul style="list-style-type: none">• This specification is designed for high-traffic (transaction) systems and systems that require multiple client database connections.• Microsoft SQL Server must be installed on the PC prior to installing DNA Fusion. <p>* Microsoft SQL Server may be installed on another (dedicated) computer prior to the DNA Fusion installation and identified during the DNA Fusion installation.</p>	



DNA Fusion is not supported on Home or Mobile versions of Windows OS. For Windows 8 installations, Enterprise is the only supported version.



If DNA Fusion is being installed on a Windows 2008, 2012, 2016, 2019 Server, follow the configuration steps that begin on page 2-21. Configure the Application Server role prior to installing DNA Fusion.



DNA Fusion will run on the following SQL Server Editions: 2000, 2005, 2008, 2008 R2, and 2012.



RAID hardware configuration and backup medium recommended for Enterprise servers.

Client Specifications

The following specifications are configuration guidelines for your DNA client workstation(s). A client workstation is a PC that is connected to the DNA system via LAN/WAN but retrieves and saves data to and from the DNA Fusion database.

Client Workstation w/Photo ID

PARAMETER	RECOMMENDED SPECIFICATION
Processor Speed	Intel Core i3 2.4 GHz + (or equivalent)
System Memory (RAM)	4 GB
Network Card	10/100 Ethernet Network Card
Hard Drive Size	250 GB
Graphics Card	VGA Support for 1024 x 768 resolution or higher
Video Memory (VRAM)	512 MB
Video Capture Device	YES (TWAIN Compliant)
USB Port	YES (if using USB capture device)
Backup Device	NO
CD-ROM Drive	YES
Operating System	Windows 7 Pro and Windows 8/8.1, Windows 10 (32-bit and 64-bit support)
Monitor	17-inch color (capable of 1024 x 768)
Optional	UPS (Uninterrupted Power Supply)
<ul style="list-style-type: none"> • If the Photo ID Client will be installed on a laptop, ensure that the unit is equipped with a minimum of one printer port and one serial port. • Additional USB and/or COM ports may be required when using badge printers with smart chip technology. See printer documentation for more information. • TWAIN devices must be compliant with Microsoft DirectX 9. 	

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Server / Client Requirements

DNA Fusion uses the network to support communication among software objects on different computers. The very nature of an access control software platform demands that a certain amount of network security is inherent in the application.

The following server and client requirements are intended to serve as a baseline and do not take into account all the variables of a system. They are subject to change without notice.

Network Requirements

DNA Fusion must meet certain network requirements in a client/server environment. The following network scenarios are acceptable for this operation:

- All DNA computers (servers and client workstations) are members of the same Windows domain regardless of what other applications are operating on the domain.
- DNA computers are members on different Windows domains, but each domain has an established bi-directional trust in place.
- DNA computers are members on different Windows domains, but each domain is managed under the Windows Active Directory Service or a master domain.

For security and authentication reasons, Open Options strongly recommends configuring DNA Fusion to operate in a Windows domain environment. However, if configuring to operate in a workgroup, all computers running DNA Fusion must be members of a single dedicated workgroup.

A few things to consider with this option:

- This method does NOT provide the same level of security as a domain environment.
- The absence of domain authentication requires that all passwords and users are managed at each individual PC in the DNA workgroup.
- If SQL Server is being used for data storage, all passwords will be required to be managed at the SQL Server level.
- Open Options offers limited support for this option (support limited to furnishing documentation).

Open Options is committed to your security and makes every effort to ensure the success of each DNA Fusion installation. However, Open Options cannot be held responsible for system failure due to non-compliance with the above network requirements.



A domain is a subnetwork comprised of a group of clients and servers under the control of one central security database. Within a domain, users only authenticate once to a centralized server (known as a domain controller) instead of repeatedly authenticating to individual servers and services. Individual servers and services accept the user based on the approval of the domain controller.

Services Account Credentials

During installation, a dialog will appear and request a local machine administrative login to run the DNA driver and COM+ services. This information will need to be obtained from the system user.

Open Options recommends setting the account password without an expiration date.

The services are used as follows:

- DNAdvr32 Service - Communicates with the controllers.
- COM+ Services - Reads and writes information to the DNA Fusion database.

User Group Setup

In order to grant permission to the DNA Fusion database, Open Options recommends configuring a User Group on the network to simplify permissions for the DNA Fusion operators. However, this step is optional. The following setup instructions are typically completed by the system administrator:

Domain User Group Setup (DNA_Global)

Open Options recommends that a Domain User Group be created prior to installing the DNA Fusion software.

1. **Create** a global Domain User Group labeled DNA_Global.
2. After the installation of DNA Fusion on the server machine is complete, **add** the domain group (DNA_Global) to the DNAUSERS group.
See page 2-13 for more information.
3. Add the DNA Fusion operator(s) to the DNA_Global Domain Group.
This step must be completed prior to adding the operator(s) in DNA Fusion.



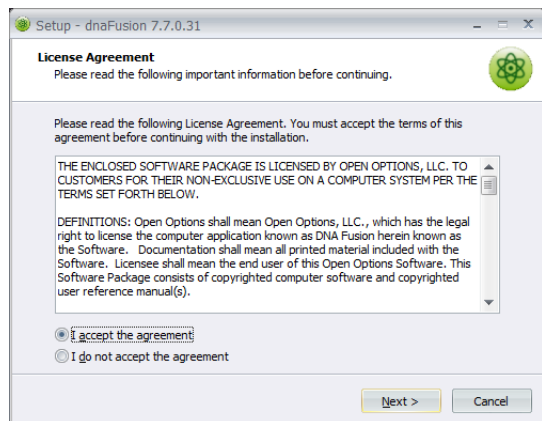
For more information on adding operators to the DNAUSERS and Distributed COM Users groups, see page 2-13.

Server Installation & Configuration

The following instructions are for Windows XP Professional/2008, 2012/R2 Server/Windows 8/Windows 10 (32-bit and 64-bit OS). If using SQL Server, it must be installed prior to the installation of DNA Fusion. Open Options also recommends that the Application Server role be configured prior to installing DNA Fusion. For more information, see pages 2-21 through 2-28.

Server Installation

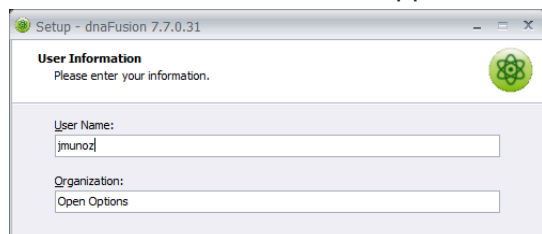
1. **Download** DNA Fusion through the link provided in the License e-mail or from the Open Options website. The License Agreement screen appears.



2. **Read** the License Agreement, **select** the I Accept the Agreement radio button, and **click** Next to continue.

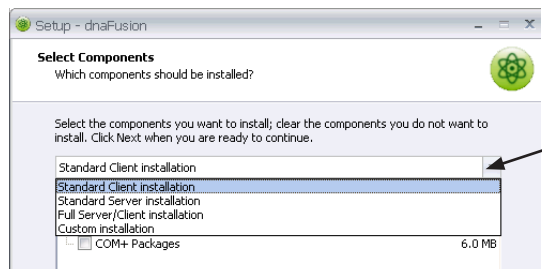
If I Do Not Accept the Agreement is selected, Cancel will be the only available option.

The User Information screen appears.



3. If desired, **change** the User Name and/or Organization and **click** Next. The Select Destination Location screen appears.
4. **Click** Next to accept the default location or **click** Browse to specify a different location. The default location is C:\Program Files (x86)\DNAFusion a for 64-bit OS.

The Select Components screen appears.

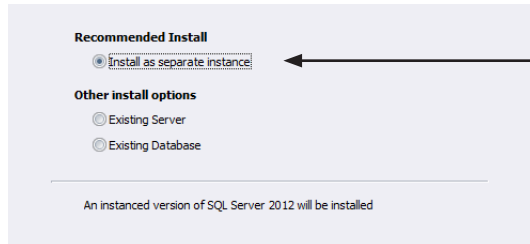


Select the Installation Type *from the drop-down list.*

5. **Select** the appropriate Installation Type from the drop-down list and **click** Next.
 - Full Server/Client Installation - Installs the objects to support server/client communication.
 - Standard Server Installation - Installs the components for a standalone server. Client components will not be installed, and a client GUI will not be installed.

The Database Server Options screen appears.

6. **Select** the radio button next to the appropriate Database Server Configuration option and **click** Next.
- Install as Separate Instance - Installs SQL Server Express 2012 and creates the DNA Fusion database. Continue to step 7.
 - Existing Server - Creates the DNA Fusion database only; requires an existing version of SQL Server to be installed prior to installing DNA Fusion. Continue to step A.
 - Existing Database - Uses an existing DNA database on an existing SQL Server. Both components must be in place prior to installing DNA Fusion. Continue to step A.



Select the radio button next to the correct Database Server Configuration option.

- a. From the Instance Name drop-down list, **select** the SQL Server Instance where the database will be created and **select** the radio button next to the correct Authentication Mode.

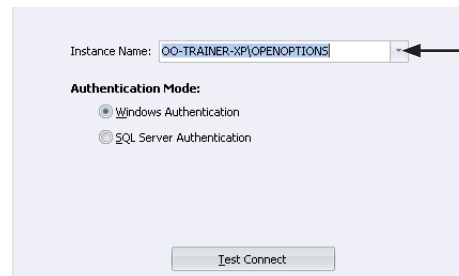


If using an Existing Server, it is crucial that the right instance is selected.

Click the Test Connect button to verify the connection to the SQL Server. **Click** the Next button to continue the installation.

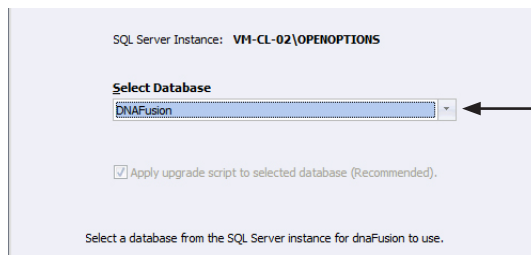
If Existing Server was selected, the Start Menu Folder screen will appear. Continue to step 7.

If Existing Database was selected, the Select Database dialog will appear. Continue to step B.



Select the SQL Server Instance from the drop-down list.

- b. From the Select Database drop-down list, **select** the DNAFusion database and **click** Next.
Recommended: Leave the Apply upgrade script to selected database box checked. This will upgrade the existing database and write any new fields that are included in the version.



Select the DNAFusion database from the drop-down list.

7. **Click** the Next button and **select** the Licensing option to generate a unique system ID number. The License screen appears.

- HASP Key - **Verify** that the DNA HASP key is inserted in a USB port on the server running the driver.
- Soft Key - **Enter** the Username and Password provided by Open Options. Requires an Internet connection.

- License File - **Install** the License File provided by Open Options prior to installation. No internet connection required.

License
How do you wish to license dnaFusion?

☐ Hasp Key

☒ Soft Key

Username

Password

Unable to locate the license file.
63F23B65-9549-485F-9892-BB8C24EC6F36

Enter the Soft Key information provided by Open Options.

8. **Click** the Next button.
The Startup Credentials screen appears.

Setup - dnaFusion

Startup Credentials
Specify the credentials to use for the service account and COM objects.

Log on as:

☒ Local System account

☐ This account:

Credential should be formatted as "DomainName\Username" or for local accounts ".\Username" or "ComputerName\Username"

Password:

Verify

Verifying the credentials may lock the account for multiple failed attempts. Proceed with caution.

< Back Next > Cancel

9. **Click** the This Account radio button.
10. **Enter** the Credentials and **click** the Verify button.

A local machine administrator login must be entered to run the DNA driver and COM+ services. This information will need to be obtained from the System User.

Open Options recommends setting the password without an expiration date. See page 2-8 for more information on the Services account.

Log on as:

☐ Local System account

☒ This account: student

Credential should be formatted as "DomainName\Username" or for local accounts ".\Username" or "ComputerName\Username"

Password: oobtraining

Verify

Verifying the credentials may lock the account for multiple failed attempts. Proceed with caution.

Test successful

11. If the login verification is successful, **click** Next button to continue the installation.
The Select Additional Tasks dialog appears.

Select the additional tasks you would like Setup to perform while installing dnaFusion, then click Next.

Additional icons:

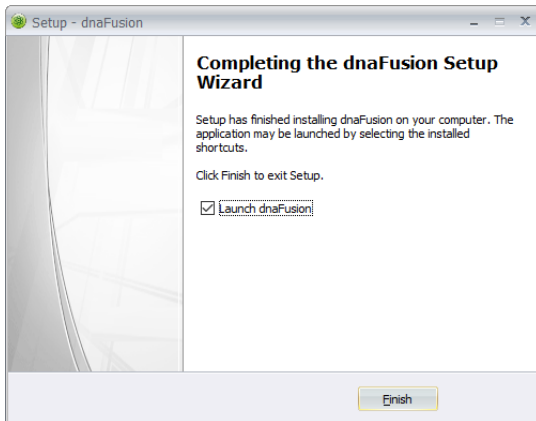
☒ Create a desktop icon

Windows Firewall

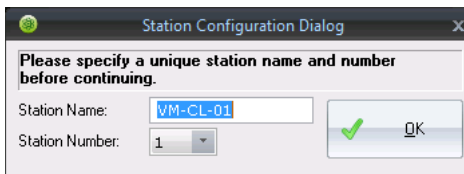
☒ Create Firewall Exclusions

12. If desired, **check** Create a Desktop Icon to add a shortcut icon the computer's desktop.
13. If desired, **check** Create Firewall Exclusions to set the firewall exclusions for Microsoft Windows Firewall.
Other software security packages may require further configuration. See page 2-19 for more information on ports used by DNA Fusion.
The Ready to Install screen appears with a summary of the installation.
14. **Click** the Install button to start the installation.

15. When the DNA installation is complete, a dialog will appear; **click** Finish to complete the setup. The DNA Fusion icon is added to the desktop.



The Station Configuration Dialog and DNA Fusion Login screen appear.



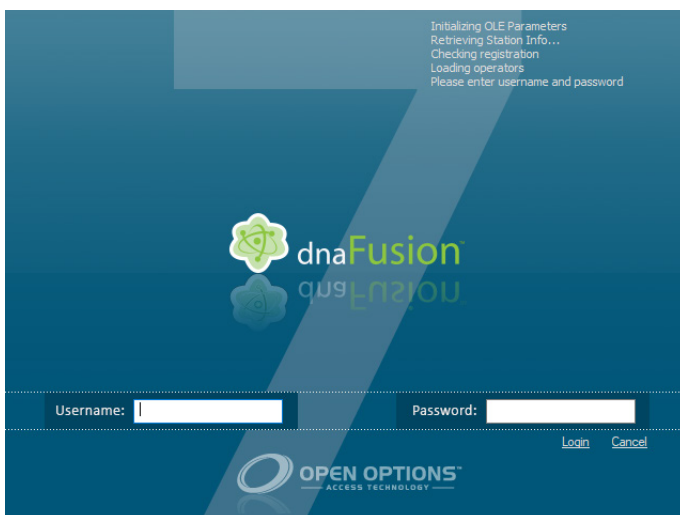
*The Station Configuration Dialog **only** appears the first time the DNA Fusion application is opened.*

16. If needed, **select** a different Station Number from the drop-down list and **click** OK. The Station Name auto-populates with the Windows Computer Name. This information appears in the DNA Properties dialog as well as on the Status Bar.



*The Station Name and Station Number **must be unique to the workstation**; no other machine should have the same name and number.*

17. In the DNA Fusion Login screen, **enter** the Username and Password and **click** Login. The default operator username is Admin without a password.



18. **Configure** the DNA Server. See page 2-13 for more information.
19. **Create** a Site and **link** the Station to the Site. See page 3-3 for information on configuring a site.
20. **Configure** the remaining hardware. For more information, see Chapter 3: Hardware Configuration.
21. If needed, **install** DNA Fusion on the client machine(s). See page 2-17 for instructions on Client Installation.

Server Configuration

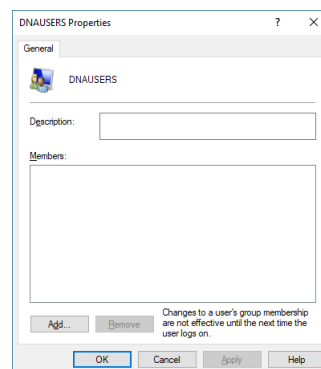
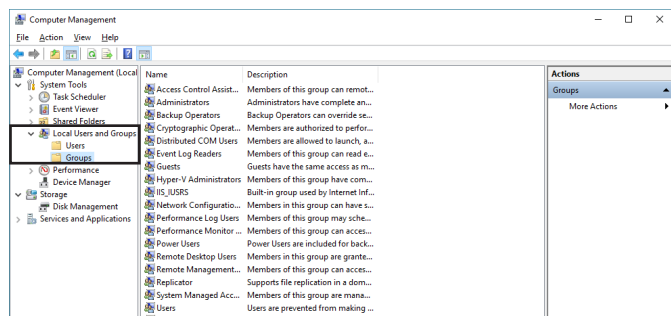
Adding Users to the DNAUSERS Group

The DNAUSERS group determines the DNA operator permissions to the COM+ application that communicates to the DNA Fusion database.

1. In the Computer Management dialog, **expand** the Local Users and Groups option.



To access to Computer Management *dialog*, **open the** Control Panel *and select* System and Security / Administrative Tools / Computer Management.



2. **Double-click** on the Groups folder and **right-click** on the DNAUSERS group.

3. **Select** Add to Group from the context menu.

The DNAUSERS Properties dialog appears.

4. **Click** the Add button.

The Select Users, Computers, Service Accounts or Groups dialog opens.

5. **Enter** the DNA_Global group and **click** Check Names to verify the entry.*

See page 2-8 for more information on the DNA_Global group.

It is recommended that the customer create and maintain a global DNAUSERS group on the domain (DNA_Global).

* If not using the recommended DNA_Global domain group, add the Windows logons for every user that will be authorized to run DNA Fusion.

6. **Enter** the Account Name that is configured to run COM+ and DNA driver (step 5) and **click** Check Names to verify the entry.

If the accounts are located, the configured information will appear in the name field.

7. **Click** OK to save the users.

8. **Right-click** on the Distributed COM Users group.

If the server was set up as a domain member, this group will be located under the Groups folder. If it was set up as a domain server, this group may be found in the BuiltIn folder or under Active Directory / Users & Computers.

9. **Select** Add to Group from the context menu.

The Distributed COM Users Properties dialog opens.

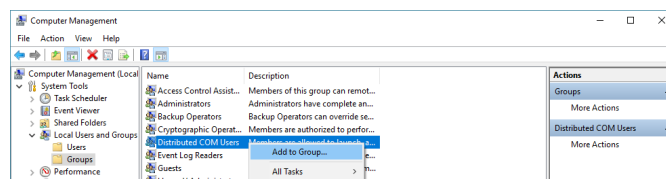
10. **Enter** the DNA_Global group and the Account Name that is running the COM+ and DNA driver services.

11. **Click** the Check Names button to verify the entry.

If the accounts are located, the configured information will appear in the name field.

12. **Click** OK.

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



Testing the Settings

To test the settings:

1. In the Component Services dialog, **right-click** on the DNA Fusion COM+ object and **select** Shut Down from the resulting menu.
2. **Right-click** on the DNA Fusion COM+ object and **select** Start.

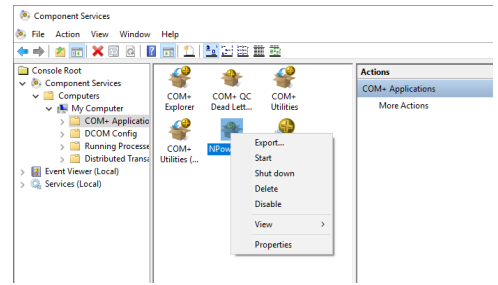
If the COM+ object starts and does not error out, it is properly configured. Proceed to step 3.

If an error is received, ensure that the configured account running the COM+ object is a Local Machine Administrator and that the user name and password are entered correctly.

3. If the COM+ object started, continue to **log in** to DNA Fusion.

If an error was received, **verify** that the COM+ account is a Local Machine Administrator.

To verify that the account has local machine administrative rights, **right-click** on My Computer (or This PC) and **select** Manage. **Expand** the Local Users and Groups option and **select** Groups. The account will appear in the Administrator group if it has local machine administrative rights.



Database Permissions

The account used to run the COM+ objects, the DNA Driver service, and the DNAUSERS group needs permission to access the DNA Fusion database.

If needed, install the SQL Server Management Studio application that comes with the DNA Fusion installation in the following location: CD-DNAvX.XX/CD Extras/SQL Server/SQL Server Management Studio Express (32-bit). If the 64-bit version is required, it can be downloaded from the Microsoft website.

1. **Open** SQL Server Management Studio and **log in**.
2. **Expand** the Security option and **right-click** on the Logins subfolder.
3. **Select** the New Login option from the context menu.

The Login - New dialog appears.

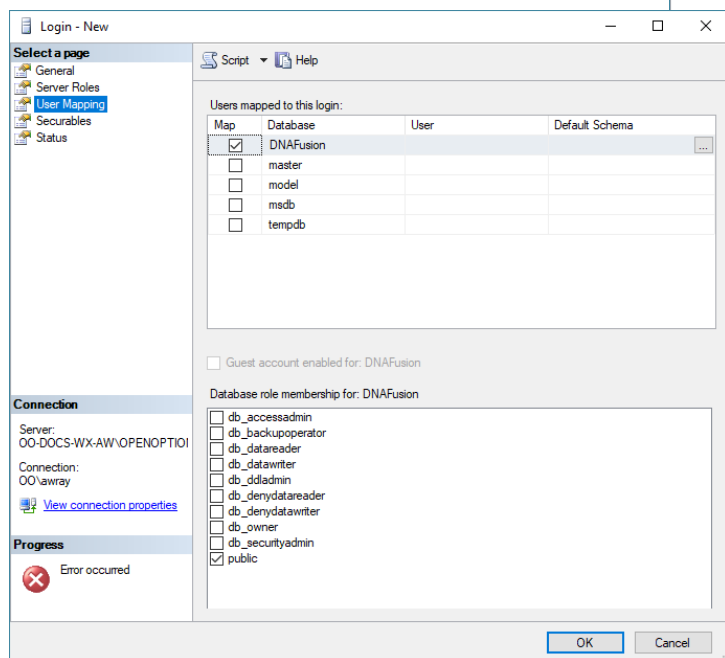
4. **Click** the Search button.
5. **Enter** the Service Account Login that is used to run the DNA Driver and **click** OK.

The user is added to the Login - New dialog.

6. **Select** the User Mapping option from the dialog menu on the left.

The User Mapping section opens.

7. **Select** the DNA Fusion database.

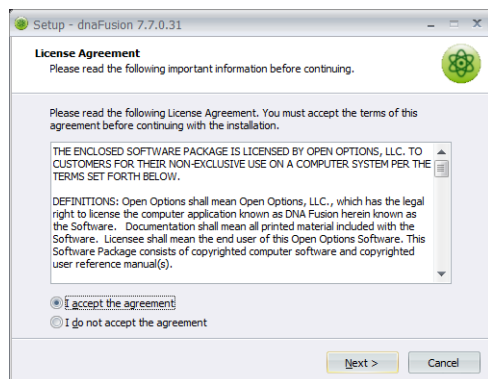


8. **Check** the following permissions for the user.
 - db_datareader
 - db_datawriter
 - db_ddladmin
9. **Click** OK to save the settings.
10. **Repeat** steps 3 through 9 for the user accounts of the DNA Fusion operators and grant them access to the db_datareader option.
 - If a database administrator will be responsible for future upgrades, their login will need to be added with access to the db_datareader, db_datawriter and db_ddladmin options.

[illegible]

Client Installation

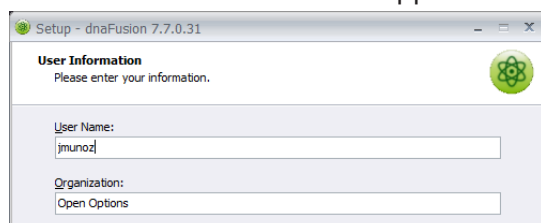
1. **Download** DNA Fusion through the link provided in the License e-mail or from the Open Options website. The License Agreement screen appears.



2. **Read** the License Agreement, **select** the I Accept the Agreement radio button, and **click** Next to continue.

If I Do Not Accept the Agreement is selected, Cancel will be the only available option.

The User Information screen appears.



3. If desired, **change** the User Name or Organization and **click** Next.

The Select Destination Location screen displays.

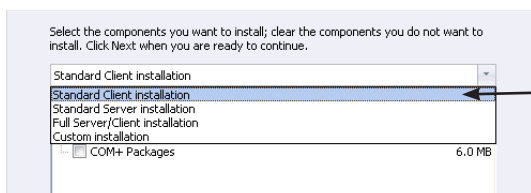
4. **Click** Next to accept the default location or **click** Browse to specify a different location.

The default location is C:\Program Files\DNAFusion for 32-bit OS and C:\Program Files (x86)\DNAFusion for 64-bit OS.

The Select Components screen appears.

5. **Select** the Standard Client Installation from the drop down and **click** Next.

- Standard Client Installation - Installs the client components necessary to support server/client communication.



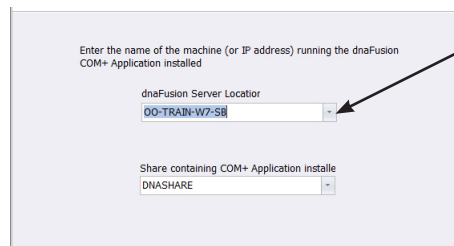
Select the Standard Client Installation from the drop-down list.

If the station will be used for badging, **select** the Enabled Badging checkbox.

The Client Setup screen appears.

6. **Enter** the Station Name or IP Address of the DNA Server or the machine running the DNA COM+ Application and **click** the Next button.

The DNAShare folder contains the COM+ Proxy installation and is populated with the correct information. By default, this folder is shared; however, permissions to the folder may need to be assigned.



Enter the Station Name or IP Address of the DNA Server running the DNA COM+ driver.

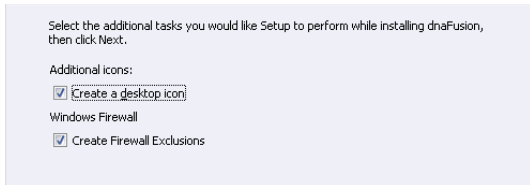


Do not change this field unless instructed by Open Options Technical Support.

7. **Click** the Next button to create the default shortcut in the Start Menu or **click** the Browse button to select another folder.

The Select Additional Tasks dialog appears.

8. If desired, **select** the Create a Desktop Icon checkbox to add a shortcut icon the computer's desktop.



The Create Firewall Exclusions checkbox is selected by default. This allows the DNA Fusion installation to set the firewall exclusions for Microsoft Windows Firewall.

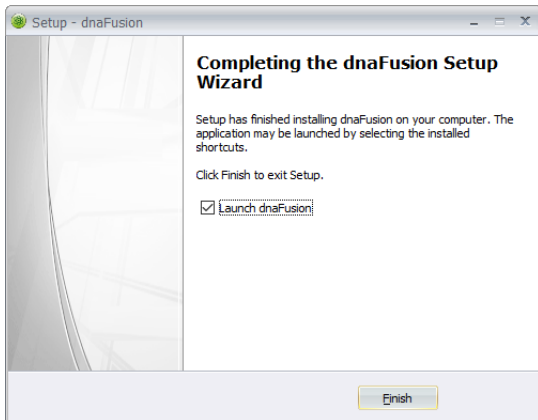
Other software security packages may require further configuration. See page 2-19 for more information on ports used by DNA Fusion.

9. **Click** Next.

The Ready to Install screen displays a summary of the installation.

10. **Click** the Install button to start the client installation.

11. When the installation is complete, a dialog appears; **click** Finish to complete the setup.



The DNA Fusion icon is added to the desktop.

12. **Log in** to DNA Fusion.

The default operator username is Admin without a password.



Firewall Configuration

If a firewall will be enabled, it will need to be configured to allow communication between the server, client(s), and the controller, if connected via Ethernet.

TCP Port 135 is used for authentication and TCP Ports 3555 and 3557 are used for driver communication. If the driver is not running when the clients connect and they need the ability to start the driver, Port 3556 will need to be added as well. TCP Port 3556 enables communication to the DNA Service Agent (dnaagent.exe). Ports 3558 and 3559 are used by the DNA Fusion Update application. The ODBC System DSN DNA Reports uses SQL Server Port 1433 to generate reports. Port 3560 is used for DMP and Flex API connections.

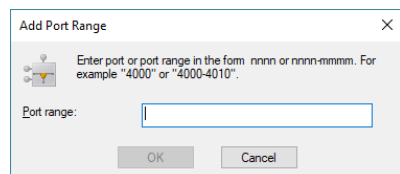
By default, DCOM is free to use any port between 1024 and 65535 when it dynamically selects a port for an application. Open Options recommends configuring DCOM to use a 500 port range on the server and each client PC that will connect to the DNA Database Server (Example: 1087 to 1587).

DNA Fusion also uses port 3001 for TCP communication between the server and the SSP(s) in the field connected via Ethernet.

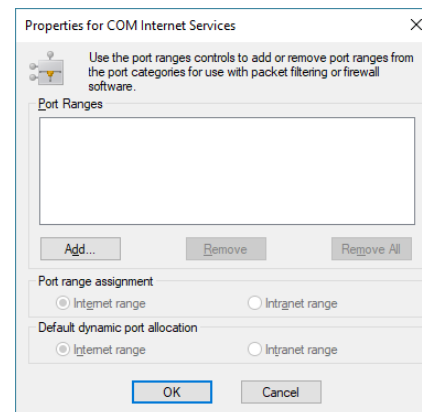
To share a folder or file, create an exception for File and Printer Sharing by opening ports 139 and 445 for TCP connections and ports 137 and 138 for UDP connections.

1. From the Control Panel, **open** the Administrative Tools.
The Administrative Tools dialog opens.
2. **Double-click** Component Services and **expand** the Component Services and Computers.
3. **Right-click** My Computer and **select** Properties.
The My Computer Properties dialog opens.
4. **Select** the Default Protocols tab.
5. **Highlight** the Connection-Oriented TCP/IP object and **click** the Properties button.
The Properties for COM Internet Services dialog opens.

6. **Click** the Add button.
The Add Port Range dialog appears.



7. **Enter** the Port Range and **click** OK.
8. **Click** OK to save the settings.
9. **Click** OK to close the dialog.
10. **Reboot** the PC.
Repeat steps 1 through 10 on the server and all client workstations.
11. **Open** Windows Firewall and **create** Exceptions for the following ports.
 - Port 135
 - ☐ Permit Incoming Traffic on the Server
 - ☐ Permit Incoming & Outgoing Traffic on the Clients
 - Ports 3555, 3556, 3557, 3558, 3559 and 3560
 - Port 1433
 - Port 3001
 - Server / Client Ports - 500 Port Range: 1087 - 1587 (from example above)
 - Ports 137, 138, 139 & 445
12. **Click** OK to save the setting.
13. **Click** OK to close the dialog.



Configuring ODBC Data Sources

The Open Database Connectivity (ODBC) interface is used to connect the client workstation to the Microsoft SQL Server running the DNA database.

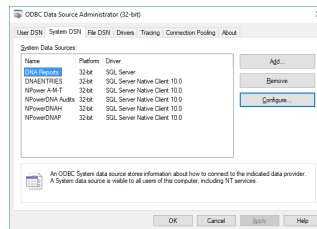
The ODBCs will also need to be configured at the Application Server if the Database resides on a separate server.



*For 64-bit systems, the DSNs may be accessed by running the following application:
C:\Windows\SysWOW64\odbcad32.exe*

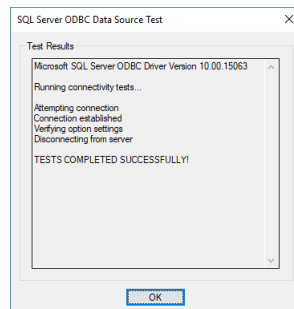
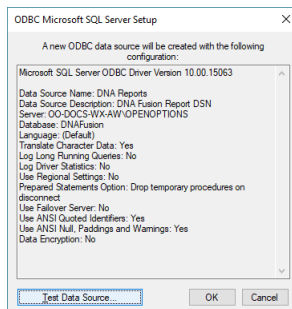
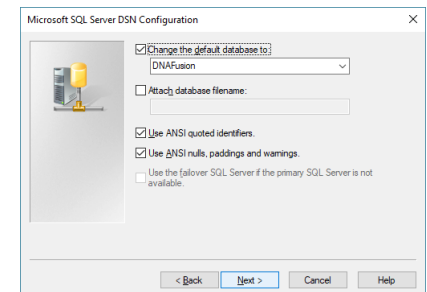
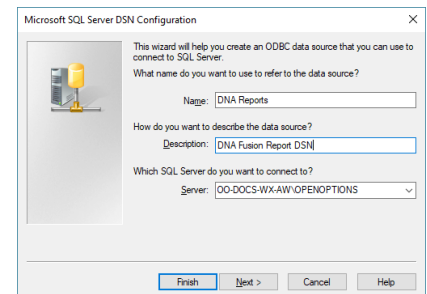
- From the Control Panel, **select** Administrative Tools / Data Sources (ODBC).
The ODBC Data Source Administrator dialog opens.
- Select** the System DSN tab.
 - On the server, reconfigure the following ODBC data sources to communicate with the DNA database:

- ☐ DNA Reports
- ☐ DNAENTRIES
- ☐ NPower A-M-T
- ☐ NPowerDNA Audits
- ☐ NPower DNAH
- ☐ NPower DNAP



- On a client, reconfigure the following ODBC data sources to communicate with the DNA database:
- ☐ DNA Reports
 - ☐ DNAENTRIES

- Select** the DNA Reports data source and **click** the Configure button.
The Microsoft SQL Server DSN Configuration dialog appears.
- Enter** a Name and Description for the data source.
- Select** the Server Name from the drop-down list and **click** the Next button.
- Verify** that the With Windows NT Authentication... and Connect to SQL Server to Obtain Default Settings... options are selected and **click** Next.
- Verify** that the Change the Default Database To: option is checked and the DNA Fusion database is selected from the drop-down list.
- Verify** that both of the Use ANSI options are checked and **click** the Next button.
- Click** the Finish button to complete the setup.



- Click** the Test Data Source button.
The SQL Server ODBC Data Source Test dialog appears.
- If the test was successful, **configure** the remaining DSNs from step 2.

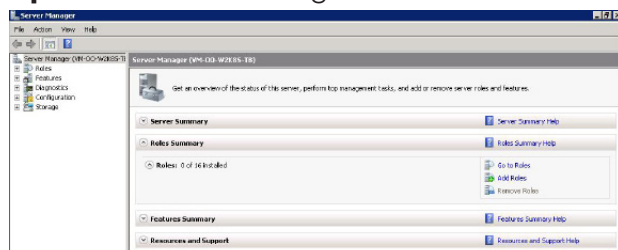
Configuring the Windows Server

If DNA Fusion is being installed on a Windows 2008, 2012, 2016, or 2019 Server, follow the configuration steps below. Configure the Application Server role prior to installing DNA Fusion.

Windows 2008 Server

The Windows 2008 Server must be configured as an Application Server in order to connect client machines to DNA Fusion. Verify that the active Windows user has administrative rights to access the server.

1. **Open** the Server Manager.



2. **Click** the Add Roles option under the Roles Summary option.

The Add Roles Wizard - Before You Begin dialog opens.

3. **Click** Next.

The Select Server Roles screen appears.



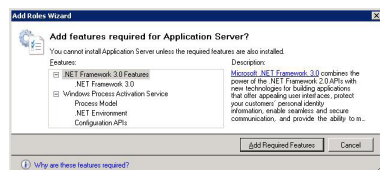
4. **Verify** that the Application Server option is selected.

If it is, **click** Cancel. The configuration process is complete.

If it is not, **select** the Application Server checkbox.

The Add Roles Wizard screen appears. Continue to step 5.

5. **Click** the Add Required Features button.

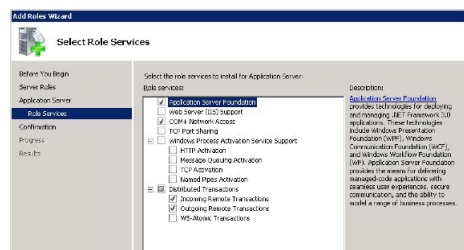


6. **Click** Next when the Application Server - Introduction to Application Server screen is displayed.

The Role Services dialog appears.

7. **Select** the following Role Services and **click** Next.

- Application Server Foundation
- COM+ Network Access
- Incoming Remote Transactions
- Outgoing Remote Transactions



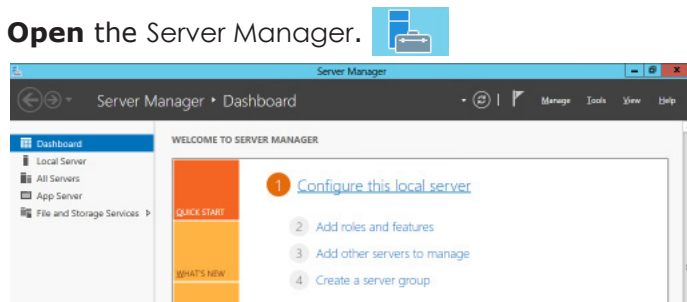
-

If the installation fails, it may be useful to acquire the Installation Disks for Server 2008 before attempting the process again.

Windows 2012 Server

The Windows 2012 Server must be configured as an Application Server in order to connect client machines to DNA Fusion. Verify that the active Windows user has administrative rights to access the server.

1. **Open** the Server Manager.

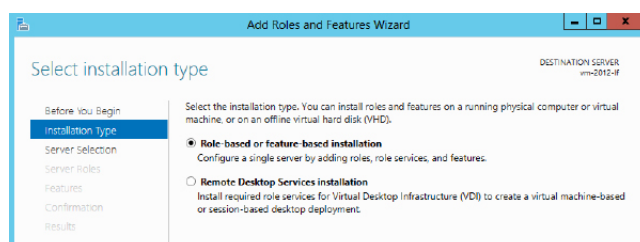


2. **Click** the Add Roles option under the Dashboard Quick Start option.

The Add Roles Wizard - Before You Begin dialog opens.

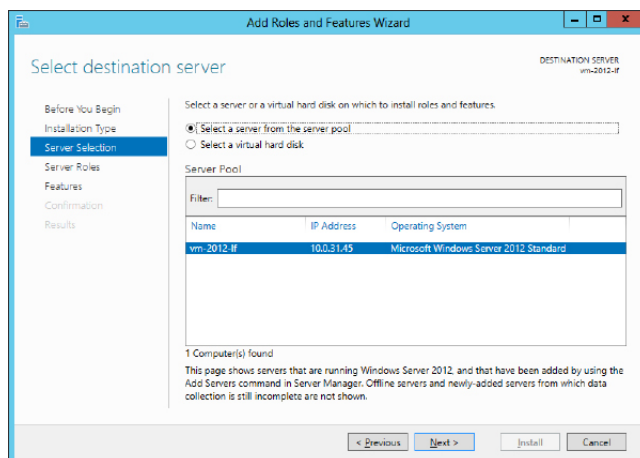
3. **Click** Next.

The Installation Type screen appears.



4. **Verify** that the Role-Based or feature-based installation option is selected and **click** Next.

The Server Selection screen appears.



5. **Select** the desired Server from the list and **click** Next.

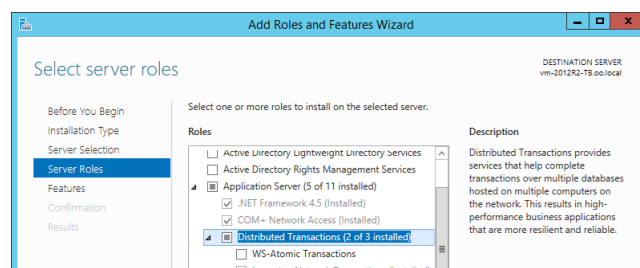
The Server Roles screen opens.

6. **Verify** that the Application Server option is installed.

If it is, **click** Cancel. The configuration process is complete.

If it is not, **select** the Application Server checkbox.

The Features dialog appears.



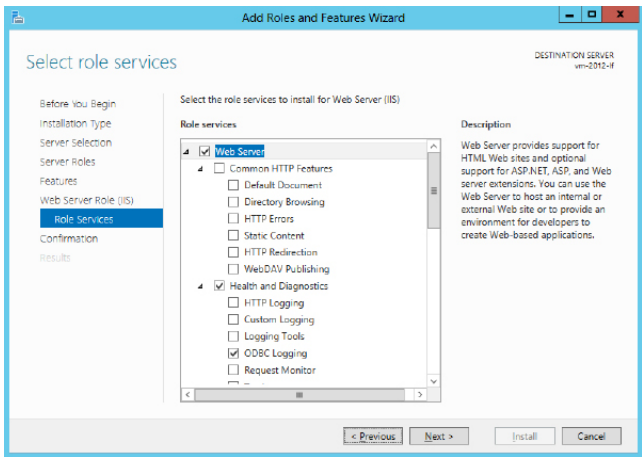
7. **Verify** that the .NET Framework Feature (3.5 & 4.5) options are installed.

If it is, **click** Cancel. The configuration process is complete.

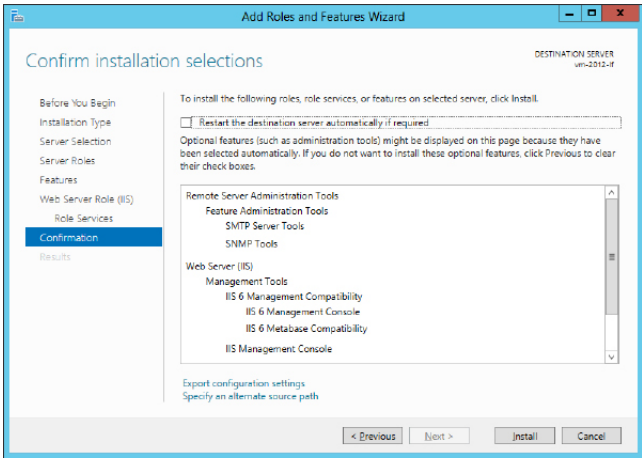
If it is not, **select** the .NET Framework Feature (3.5 & 4.5) checkbox.

8. If prompted, **click** Add Features when the Add Roles and Features Wizard screen is displayed.

9. **Click** the Next button to continue the installation.
The Web Server Role (IIS) dialog will appear.
10. **Click** the Next button to continue to the Roles Services dialog.




11. **Click** the Next button to continue the installation.
12. When the Confirmation dialog appears, **select** Install.



The Installation Results screen displays the results of the installation.

13. If the Installation was successful, **click** Close.
If the Installation fails, **verify** that the Windows user has the proper rights.

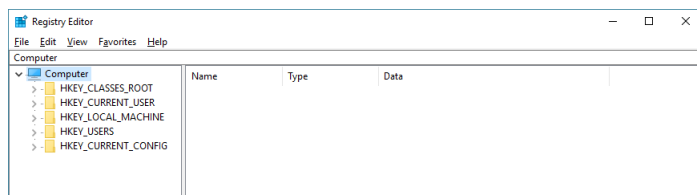
 *If the installation fails, it may be useful to acquire the Installation Disks for Server 2012 before attempting the process again.*

Windows 2016 Server

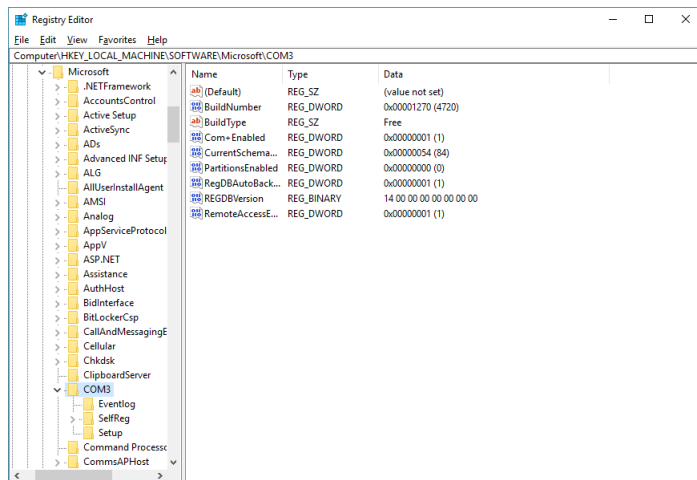
The Application Server role is not available in Windows 2016 Server. Because the COM+ Network Access feature belongs to the Application Server role, it cannot be enabled in the Windows 2016 Server.

Use the Windows Registry to manually configure the server:

1. **Open** the Registry Editor tool.

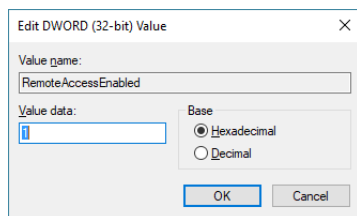


2. **Expand** the HKEY_LOCAL_MACHINE folder and **select** SOFTWARE / Microsoft / COM3.



3. **Double-click** on RemoteAccessEnabled.

The Edit DWORD (32-bit) Value dialog appears.



4. **Set** the Value Data field to 1.
5. **Click** OK to save the registry value.
6. **Close** the Registry Editor tool.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

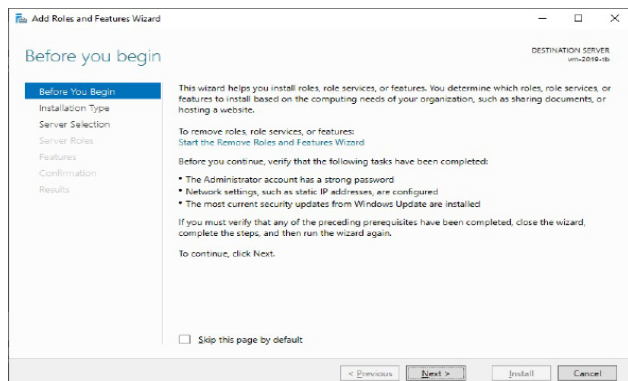
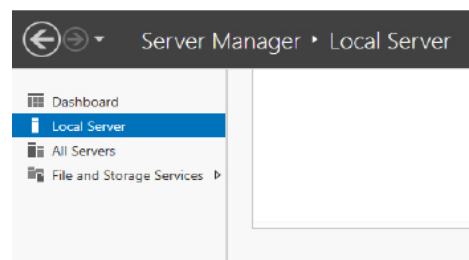
Windows 2019 Server

Before installing DNA Fusion, server configuration is required to prevent installation failure of DNA Fusion. Follow the steps below to configure an Windows Server 2019.

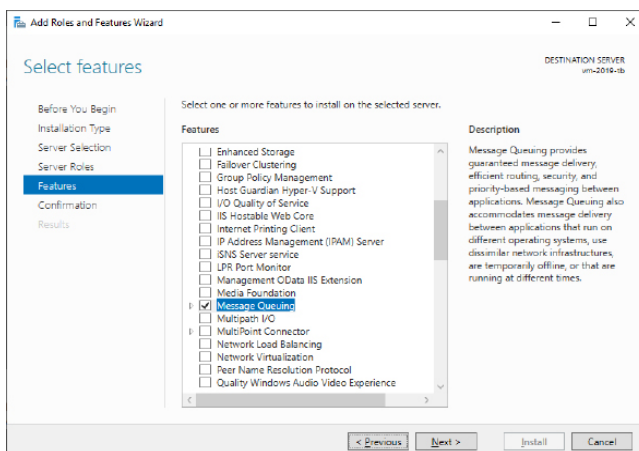
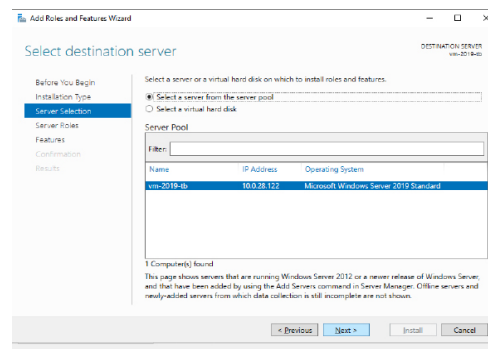
1. **Open** Server Manager.
2. **Select** Local Server.
3. **Scroll down** to Roles and Features.
4. **Select** the Add a Role option from the Tasks drop-down menu.

The Add Roles and Features Wizard opens.

Verify that tasks in Before you begin section are completed before continuing.



5. After verifying, **click** Next to advance to Installation Type.
6. **Select** Role-based or feature-based installation and **click** Next to advance to Server Selection.
7. In the Server Selection dialog, **verify** that the Select a server from the server pool option is selected.
8. **Ensure** Windows Server 2019 is selected and **click** Next to advance to Servers Roles.
9. Under Server Roles, **select** File and Storage Services and **click** Next to advance to Features.
10. In the Features section, **select** .Net Framework 3.5 Features.
11. **Expand** .Net Framework 3.5 Features and **select** .Net Framework 3.5 (includes .Net 2.0 and 3.0) installation.
12. In the Features section, **select** Message Queuing and **click** Next to advance to Confirmation.



13. In the Confirmation section, **select** Specify an alternate source path.



Open Options recommends to run the server as an Administrator.

14. On the Specify Alternate Source Path window, **enter** D:\source\sxs in the Path text box.
15. **Click** OK when the path is entered to proceed to install.

Migrating DNA Fusion to a New Server



If DNA Fusion will be installed as the Application Server on new workstation, turn OFF the User Access Control and reboot.



If you are installing DNA Fusion on a Windows 2008, 2012, 2016, or 2019 Server, follow the configuration steps described on pages 2-21 through 2-28.

Migrating with Server/Client Components on the Same Workstation

Follow the instructions below if the DNA Fusion server application (DNA Driver) and database will be installed on a new server.+

1. **Determine** the Licensing requirement:
 - Soft Key – If the system is using a soft key, contact Open Options Technical Support and request that the System Soft Key ID be reset. The request should be made on the day of the installation during Open Options' normal business hours.
 - HASP Key – Remove the HASP Key from the old server and place it in a free USB port on the new server.
 - If converting from a HASP Key to a Soft Key (moving to a virtual machine): Contact Open Options' Order Entry Department prior to the installation date and arrange for the HASP Key to be returned. This will require an advance replacement purchase order (PO) for the new system.
2. **Shut down** all DNA Fusion client machines.
3. **Stop** the DNA Driver (DNAdrvr32.exe) service on the old Application Server.
4. If using the OpenDX application, **stop** the OpenDX service.
5. **Verify** that SQL Server 2005 or 2008 is installed on the new Server.
6. **Back up** the DNAFusion (or NPowerDNA) Database and **restore** it with the same name on the new Server.
7. **Install** the DNA Fusion Server as described on page 2-9.
8. In the Select Components screen, **select** Client / Server Components and **click** Next.
9. **Select** Existing Database from the Database Server Options page and **click** Next.
See page 2-10 for information on Database Server Options.
10. From the Instance Name drop-down list, **select** the SQL Server Instance where the database resides and **select** the radio button next to the correct Authentication Mode.
11. From the Select Database drop-down, **select** the DNAFusion (or NPowerDNA) database and **click** Next.
12. **Complete** the installation as described on pages 2-10 through 2-12.
13. **Verify** the database permissions.
 - a. The account(s) running the COM+ objects and DNAdrvr32 service need(s) to have db_datareader, db_datawriter and db_ddladmin rights.
 - b. The user accounts for DNAFusion operators need to have db_datareader rights.
 - c. If a database administrator will be responsible for future upgrades, their account should have db_datareader, db_datawriter and db_ddladmin rights.
14. **Run** the Tablepurger.exe application to remove the old server name from the DNA Fusion database.
See page 5-5 for information on the Table Purger.
15. **Launch** DNA Fusion and **link** the Station to the Site.
16. On each client workstation, **edit** the DNA Reports ODBC System DSN to point to the new database server.
See page 2-20 for more information.
17. If the new Application Server's name is different, **run** the DNA Database Setup Package on each client.
Default location on the server:
 - ❑ 32-bit OS – C:\Program Files\DNAFusion\DNAShare or nPowerDNA\DNAShare
 - ❑ 64-bit OS – C:\Program Files (x86)\DNAFusion\DNA Share or nPowerDNA\DNAShare

This will point the clients COM+ objects to the new server.
Other items may need to be updated, such as photo paths, badge templates, etc.

Migrating with Server and Client Components on Separate Workstations

Follow the instructions below if the DNA Fusion server application (DNA Driver) will remain on the existing server and a new database will be installed on a new server.

1. **Shut down** all DNA Fusion client machines.
2. **Stop** the DNA Driver (DNADrvr32.exe) service on the Application Server.
3. If using the OpenDX application, **stop** the OpenDX service.
4. **Verify** that SQL Server 2005 or 2008 is installed on the new Server.
5. **Back up** the DNAFusion (or NPowerDNA) Database and **restore** it with the same name on the new Server.
6. **Install** the DNA Fusion Server as described on page 2-9.
In order to force a new server installation, run the setup with the Setup.exe /forcenew switch to update the settings and connect to the database on the new server.
7. On the Select Components screen, **select** Server Components and **click** Next.
8. **Select** Existing Database from the Database Server Options page and **click** Next.
See page 2-10 for information on Database Server Options.
9. From the Instance Name drop-down list, **select** the SQL Server Instance where the database resides and **select** the radio button next to the correct Authentication Mode.
10. From the Select Database drop-down, **select** the DNAFusion (or NPowerDNA) database and **click** Next.
11. **Complete** the installation as described on pages 2-10 through 2-12.
12. **Verify** the database permissions.
 - a. The account(s) running the COM+ objects and DNADrvr32 service need(s) to have db_datareader, db_datawriter and db_ddladmin rights.
 - b. The user accounts for DNAFusion operators need to have db_datareader rights.
 - c. If a database administrator will be responsible for future upgrades, their account should have db_datareader, db_datawriter and db_ddladmin rights.
13. **Run** the Tablepurger.exe application to remove the old server name from the DNA Fusion database.
See page 5-5 for information on the Table Purger.
14. **Launch** DNA Fusion and **link** the Station to the Site.
15. On each client workstation, **edit** the DNA Reports ODBC System DSN to point to the new database server.
See page 2-20 for more information.
16. If the new Application Server's name is different, **run** the DNA Database Setup Package on each client.
Default location on the server:
 - ❑ 32-bit OS – C:\Program Files\DNAFusion\DNAShare or nPowerDNA\DNAShare
 - ❑ 64-bit OS – C:\Program Files (x86)\DNAFusion\DNAShare or nPowerDNA\DNAShareThis will point the clients COM+ objects to the new server.
Other items may need to be updated, such as photo paths, badge templates, graphic maps, and the Universal Driver.

Hardware Configuration

3

In This Chapter

- ✓ Hardware Browser & Overview
- ✓ Adding Hardware to the System
- ✓ Hardware Properties
- ✓ Card Formats

In addition to setting up the hardware field devices for the access control system, the hardware properties must be configured in DNA Fusion so that the software can communicate with the field devices. This chapter explains how to add hardware to the system and configure the required hardware properties. It also provides instructions for creating and assigning card formats.

Configuring Hardware

Add the hardware in the following order:

1. Site - The collection of channels and controllers that communicates with a common driver.
2. Channel - The virtual pathway of communication from the host to one or more SSP controllers.
3. Controller - The data-gathering panel that makes local access decisions and stores information such as access levels, time schedules, triggers, and macros.
4. Subcontroller - One of a series of circuit boards that communicates information about field devices like readers, contacts, and motion detectors upstream to the controller.
5. Access Control Model (ACM) - A group of objects that, when associated together, form an entry point that is commonly associated with a door or elevator.

Hardware Browser

All hardware objects are added through the Hardware Browser. The Hardware Browser is an explorer window that contains a hierarchical “tree” of field devices that comprise the system.

To open the Hardware Browser:

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



Or

Select View / Explorers / Hardware from the Main Menu.

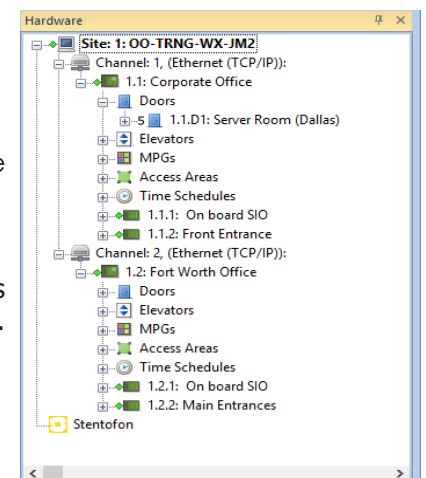
The Hardware Browser appears.

For information on status indicators and object colors in the Hardware Browser, see Chapter 8 in the DNA Fusion User Manual.

Configuring the Browser

















The Hardware Browser can be customized to display various tabs as well as objects in the hardware tree. The tree can be sorted by description or address.

1. **Right-click** in the white area at the bottom of the Hardware Browser.
2. **Select** Tree Properties from the context menu.
The Hardware Tree Behavior dialog opens.
3. **Configure** the settings.
See page 3-25 in the DNA Fusion User Manual for more information.



Hardware Toolbar

DNA Fusion provides many useful commands and shortcuts to help the operator control the hardware. These commands are available from the Hardware Toolbar.

Icon	Description
	Download Icon - Displays the Download Manager dialog to download the database information to the controller.
	Control Icon - Displays the Direct Control Dialog for the selected hardware object.
	Hardware Properties Icon - Displays the Hardware Properties for the selected hardware object. For more information, see pages 8-47 through 8-80 in the DNA Fusion User Manual.
	Add Hardware Icon - Click the arrow to display a drop-down menu of hardware objects. Select an option to display the Add dialog for the object.
	Remove Icon - Displays a confirmation dialog to delete the selected hardware object.
	Status Icon - Displays the Status dialog for the selected hardware object, if applicable.
	Default Template Icon - Applies the default template to the selected hardware object.
	Templates Icon - Displays the Template Manager dialog. See page 8-83 in the DNA Fusion User Manual for more information.
	Watch Item Icon - Adds the selected hardware object to an existing Watch Window. The Watch Window must be open in order for this option to be available. See Chapter 15 in the DNA Fusion User Manual for more information.
	Refresh Tree Icon - Updates the Hardware Browser tree.
	Homepage Icon - Launches the Home Page associated with the selected hardware object.
	Disable High Icon - Disables the IP Video Window from opening automatically on a High Priority alarm.
	Disable Normal Icon - Disables the IP Video Window from opening automatically on a Normal Priority alarm.
	Disable Low Icon - Disables the IP Video Window from opening automatically on a Low Priority alarm.
	Disable Custom Icon - Disables the IP Video Window from opening automatically on a Custom Priority alarm.
	Use Template Icon - Opens the Door Templates dialog for the selected hardware object. See page 8-83 in the DNA Fusion User Manual for more information.

Adding Hardware

Creating and Linking a Site

A Site is a collection of channels and controllers that communicates with a common driver (DNADrvr32). A site is the driver that communicates with the hardware of a given system. The system can have a maximum of 63 sites, and each site can have a maximum of 255 channels.



Most installations will only have one site with multiple channels. Each site is essentially a separate driver that communicates to the controllers on the designated channel.

Creating a Site

The first step in adding hardware is to create a site or establish communication with the driver. The hardware uses the driver to communicate with the database. This step must be performed from the DNA Fusion server.



A Site will be automatically added if the DNA Driver (DNADrvr32) service is started on the server after installation. The server station will need to be linked to the site. See page 3-4 for more information.

1. **Open** the Hardware Browser and **right-click** inside the browser.
2. **Select** New Site from the context menu.

The Add Site dialog appears.

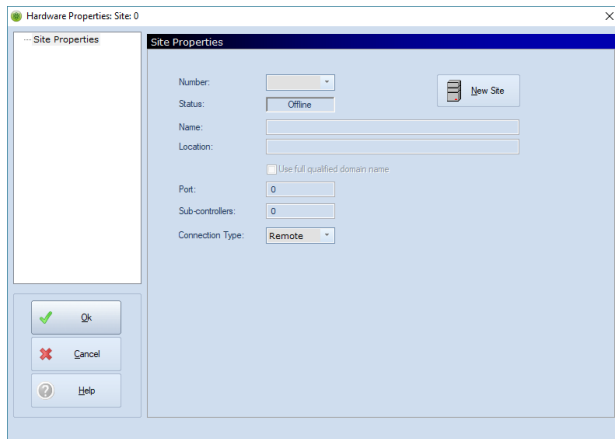
3. **Select** a Number for the site from the drop-down menu.
The dialog will auto-populate with the next available Number.
4. **Enter** a Name for the site.
5. If desired, **enter** a Description to help identify the site.
6. **Click** the Local button to add the workstation's location information to the Location field.
This provides the computer's name on which the site's driver resides. This step must be done on a server station, not on a client station.
7. **Click** OK.
The Site is added to the Hardware Browser.

Linking to a Site

The site must be linked to the server workstation to create the communication path for the driver. Client workstations will automatically link to the site.

1. **Right-click** in the Hardware Browser and **select** Link Station to Site.

The Site Properties dialog opens.



2. **Select** the Site Number entered in step 3 on page 3-3.

The site information automatically populates the dialog.

- Number - The site identification number.
- Status - The online or offline status.
- Name - The user-defined site name.
- Location - The name of the computer on which a given site's DNADrvr32 resides.
- Port - The driver machine TCP/IP port that is used to establish communication with the site's driver. (Default = 3555)
- Subcontrollers - The number of subcontrollers actively connected (online) to the site.
- Connection Type - The type of connection to the site.
 - ☐ Local - Server workstation
 - ☐ Remote - Client workstation

3. **Click** OK to save the settings.

The site is added to the Hardware Browser.



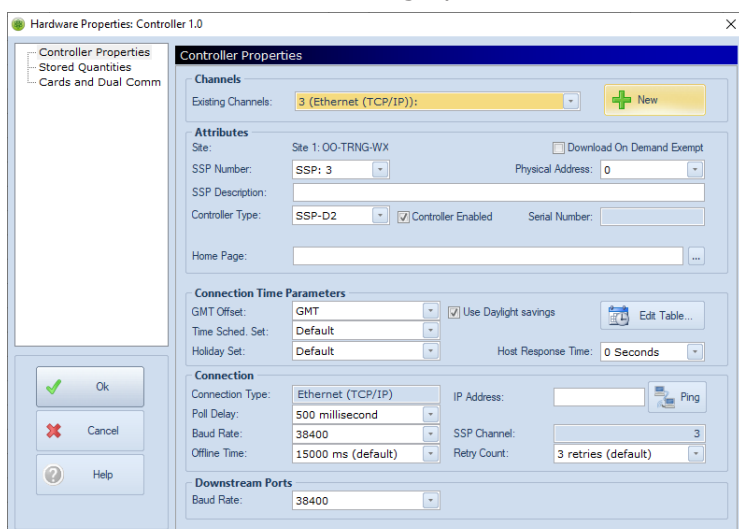
Click the New Site *button in the Site Properties dialog to add a new site; the Add Site dialog will appear. See page 3-3 for more information.*

Adding a Controller (SSP)

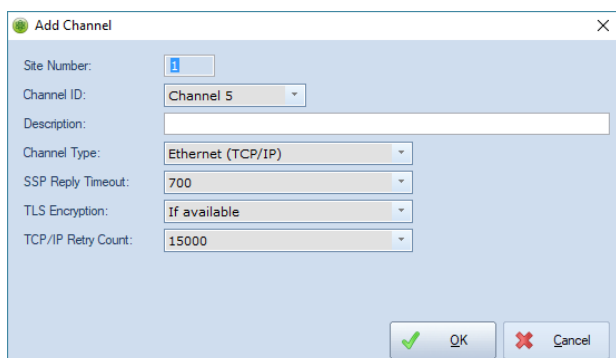
The controller is the data-gathering panel that makes local access decisions and stores information such as access levels, time schedules, and triggers and macros. Each setting is discussed in detail below.

1. In the Hardware Browser, **right-click** on a Site or Channel object and **select** Add SSP.

The Controller Properties dialog opens.



2. **Select** an Existing Channel from the drop-down or **click** the New button to configure a new channel. The Add Channel window opens.



3. **Configure** dialog fields.
See page 3-7 for information on setting up the various channel types.
 - Site Number - The location of the hardware. (Auto-populated)
 - Channel ID - The channel identification number.
 - Description - The user-defined channel description.
 - Channel Type - The method of communication connection. See pages 3-7 through 3-10 for more information.
4. If desired, **check** Download On Demand Exempt to override the Download on Personnel Demand setting in the DNA Site (Driver) Configuration dialog.
See page 20-3 in the DNA Fusion User Manual for more information.
5. If using a Serial connection, **select** the controller's Physical Address from the drop-down.
6. **Enter** a Description (typically location- or function-related).
7. **Select** the Controller Type from the drop-down list.
8. If desired, **toggle** the Controller Enabled checkbox to enable or disable the controller.
Disabled controllers appear gray in the Hardware Browser and do not communicate with the DNA driver.

9. **Select** the GMT Offset from the drop-down list. (Default GMT = 0)

This setting determines the panel's time zone. If not set correctly, the system will not open properly. See page 3-12 for more information on GMT settings.

10. If desired, select a Time Schedule Set or Holiday Set to associate with the controller.

For more information, see Chapter 5 in the DNA Fusion User Manual.

11. If needed, **uncheck** the Use Daylight Savings checkbox. This option is selected by default, and automatically adjusts the controller for daylight saving time.

12. **Enter** the channel information.

- If Ethernet (TCP/IP) Channel, **enter** the IP Address.

IP Address



Configure the controllers with the desired IP address prior to setting them up in DNA Fusion. For more information on configuring a controller's IP address, see Chapter 2 in the Hardware Manual.

- If IP Client - Remote (TCP/IP) Channel, **enter** the MAC Address.
- If Serial Channel, no information is required; however, the Physical Address will need to be set to a unique value on each controller.
- If Modem Channel, **enter** the Phone Number. The phone number should not contain any dashes, spaces or parentheses. A comma creates a pause.

MAC Address

Phone Number:

13. **Select** Stored Quantities from the dialog menu.

See page 3-13 for more information on Stored Quantities.

14. **Select** any desired Controller Flags and adjust any Quantities as needed.

15. **Click** the OK button to save the settings.



If a new Controller is added to DNA Fusion that is not network ready, use the Controller Connection Utility to disable them in the database. See page 5-3 for more information.

Adding a Channel

A channel is a virtual pathway that determines a communication route from the DNA Fusion server to one or more SSP controllers. DNA Fusion can communicate with the controllers via Ethernet, Serial or Modem connections. Controllers that are connected via Ethernet (TCP/IP) or Modem can have one channel per SSP, while controllers that communicate via Serial channels can have multiple SSPs per channel. New or existing channels can be added when configuring a new SSP.



*By default, Channel objects are hidden in the Hardware Browser. To view the available channels, **check** Channels under "All Objects" Tree Items *in the* Hardware Tree Behavior dialog. See page 3-25 in the DNA Fusion User Manual for more information.*

See page 3-5 for information on adding a channel through the Controller Properties window.

1. In the Hardware Browser, **right-click** on the desired Site.
2. **Select** Add Channel from the context menu.

The Add Channel dialog appears.

3. **Configure** the dialog fields.

See page 3-9 for information on setting up the various channel types.

- Site Number - The location of hardware. (Auto-populated)
- Channel ID - The channel identification number.
- Description - The user-defined channel description.
- Channel Type - The method of communication connection. See page 3-9 for more information.
 - ☐ Ethernet (TCP/IP) - If desired, the following options can be changed: SSP Reply Timeout, TLS Encryption, and TCP/IP Retry Count. Enter the IP Address in the Controller Properties dialog. See page 8-46 in the DNA Fusion User Manual for more information. The majority of channels use an Ethernet (TCP/IP) connection.
 - ☐ Serial - Select the COM Port from the drop-down list.
 - ☐ Dial In/Out - Select the Modem Name from the drop-down list.
 - ☐ IP Client - Remote TCP/IP - Provides the ability for panels to connect to the driver rather than the normal method of the driver connecting to the panel. Used in situations where the panels are behind a Hosted/Managed firewall. Only one per site can be used.

The following options are determined by the operator's Channel Type selection:

- COM Port - Identifies the COM Port for serial connections to the controller. (Serial configuration only)
- TLS Encryption - Determines whether the TLS Encryption is always required or only required if available. (TCP/IP configurations only)
- SSP Reply Timeout - SSP timeout in milliseconds. Recommended settings are 200-400 milliseconds for Serial channels, 600-800 milliseconds for TCP/IP channels.
- TCP/IP Retry Count - Number of times the driver will re-attempt communication between the host and a controller after an unsuccessful attempt. Recommended setting is 10,000-20,000 seconds. (TCP/IP configurations only)
- Baud Rate - Rate of transmission to the SSP. (Serial configuration only)

- Modem Name - Modem designation in the Control Panel. (Dial In/Out configurations only)
- RTS Mode - On/Toggle/Off/CTS-RTS Handshake (Serial configuration only)
 - ❑ On - Fixes the state of the RTS pin to ON. This setting is used with RS-232 with Hardware Handshake.
 - ❑ Toggle - Tells the port handler to set the RTS output to ON when data is being sent. This setting is used when the COM port is used in half-duplex mode, such as 2-wire RS-485 connection.
 - ❑ Off - Fixes the state of the RTS pin to OFF. For instance, setting 0 is used with RS-232 without Hardware Handshake.
 - ❑ CTS/RTS Handshake - Regulates communication based on the amount of traffic. This setting selects full hardware flow control. Hardware handshake is required if data transfer must be paused momentarily. Connections to the modems, terminal emulators (Lantronix), or connections at baud rates above 38,400 baud will require hardware flow control.
- Listening Port - Identifies the port on the server that remote panels will use for communication. Open Options recommends Port 3001. Only one per controller can be used. (Remote TCP/IP only)

Ethernet (TCP/IP) Channel

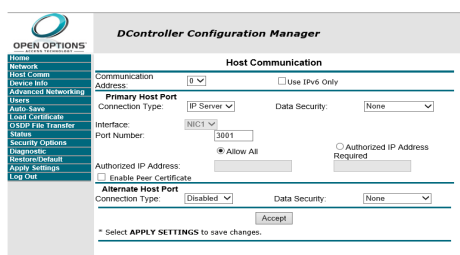
The Ethernet (TCP/IP) channel is the most commonly used channel type to communicate with IP-based controllers.

1. **Enter** a Description for the channel.
2. **Select** Ethernet (TCP/IP) from the Channel Type drop-down menu.
3. **Select** the SSP Reply Timeout from the drop-down menu.
The recommended setting for TCP/IP channels is 600-800 milliseconds.
4. **Select** the TLS Encryption option from the drop-down menu: If Available or Required.
5. **Select** the TCP/IP Retry Count from the drop-down menu.
The recommended setting is 10,000-20,000 seconds.
6. **Click** OK to save changes.
7. **Enter** the IP Address in the SSP Properties dialog.

IP Client - Remote (TCP/IP)

The IP Client - Remote (TCP/IP) option provides the ability for panels to connect to the DNA Driver rather than the normal method of the driver connecting to the panel. This type of channel is used in situations where the panel is located behind a firewall (Hosted/Managed). Only one IP Client - Remote channel can be created per site.

1. **Configure** the Controller using the Web Interface.
See page 2-2 in the System Hardware Manual for information on the Web Interface.
Use the following settings:
 - Host Communication Address: 0
 - Primary Host Port Connection Type: IP Client
 - Host IP: **Enter** the host IP address or the host name
 - Port Number: **Enter** the same port as the Listening Port specified when the channel was created.
 - Connection Mode: Continuous



The screenshot shows the 'DController Configuration Manager' web interface. On the left is a sidebar with 'OPEN OPTIONS' and a list of menu items: Home, Network, Host Comm, Device Info, Advanced Networking, Users, Auto Save, Load Certificate, Open and Transfer, Status, Security Options, Diagnostic, Restore Default, Apply Settings, and Log Out. The main content area is titled 'Host Communication' and contains the following settings:

- Communication Address:** 0 (dropdown menu)
- Use IPv6 only:** (checkbox, unchecked)
- Primary Host Port:**
 - Connection Type:** IP Server (dropdown menu)
 - Data Security:** None (dropdown menu)
- Interface:** NIC1 (dropdown menu)
- Port Number:** 3001 (text input)
- Authorized IP Address:**
 - ☒ Allow All
 - ☐ Authorized IP Address Required
- Alternate Host Port:**
 - ☐ Enable Peer Certificate
 - Connection Type:** Disabled (dropdown menu)
 - Data Security:** None (dropdown menu)

At the bottom, there is an 'Accept' button and a note: '* Select APPLY SETTINGS to save changes.'

2. **Enter** a Description for the channel.
3. **Select** IP Client - Remote (TCP/IP) from the Channel Type drop-down.
4. **Select** the SSP Reply Timeout from the drop-down menu.
The recommended setting for TCP/IP channels is 600-800 milliseconds.
5. **Select** the TLS Encryption option from the drop-down menu: If Available or Required.
6. **Enter** the Listening Port number.
Open Options recommends using Port 3001.
7. **Click** OK to save changes.
8. **Restart** the DNADrvr32 driver.
9. **Enter** the MAC Address in the SSP Properties dialog.
The MAC Address can be entered with or without the standard ':' symbol separating the six sections of the address. Enter all twelve hex digits that make up the MAC address.

Serial Channel

1. **Enter** a Description for the channel.
2. **Select** Serial from the Channel Type drop-down.
3. **Select** the SSP Reply Timeout from the drop-down.
The recommended setting for Serial channels is 200-400 milliseconds.
4. **Verify** that the Baud Rate is set to 38400.
5. **Select** the COM Port from the drop-down list.
6. **Set** the RTS Mode to OFF.
7. **Click** OK to save the changes.

Modem Channel

1. **Enter** a Description for the channel.
2. **Select** Dial (out), Dial (in) or Dial (out/in) from the Channel Type drop-down.
For information on configuring DNA Fusion to dial the controller or the controller to dial the host, see Chapter 10 in the DNA Fusion User Manual.
 - Dial (out) - Only allows DNA Fusion to initiate the connection to the controller.
 - Dial (in) - Only accepts incoming calls from the controller.
 - Dial (out/in) - Allows the driver to initiate the connection to the controller as well as accept incoming calls from the controller. This is the most frequently used setting.
3. **Set** the SSP Reply Timeout to 300.
4. **Verify** that the Baud Rate is set to 38400.
5. **Select** the COM Port from the drop-down.
6. **Set** the RTS Mode to CTS/RTS Handshake.
7. **Select** the Modem Name from the drop-down list.
8. **Click** OK to save changes.
9. **Enter** the Phone Number in the Controller Properties dialog.



Open Options recommends using the Multitech MultiModem ZBA modem at both the host and the controller. It is also recommended that both ends use a POTS line. For more information, see the Legacy Hardware Manual.



*The modem will attempt to connect when the settings are downloaded and when the operator Starts or Resets the driver. To manually establish a connection, **right-click** on the Controller and **select** Controller Commands / Connect or Disconnect.*

Controller Properties

Controller Properties

Channels

- SSP Channel - Indicates the controller's channel number and type.
- New or Properties - If selected, opens the Add or Edit Channel dialog to add a new channel or edit the existing SSP Channel's properties.

Attributes

- Site - Location of hardware (Auto-populated).
- SSP Number - Number designation for the controller.
- SSP Description - User-defined description of the controller; typically location- or function-related.
- Controller Type - Select the controller type from the drop-down list:
 - ☐ SSP-D2 - When adding an SSP-D2, the on-board RSC-D2 subcontroller is added automatically.
 - ☐ SSP-EP
 - ☐ DController - When adding an DController, the on-board DCont Subcontroller is added automatically.
 - ☐ SSP-LX
 - ☐ SSP (Standard)
 - ☐ SSP/C
 - ☐ SSP/E
 - ☐ PIM400-1501

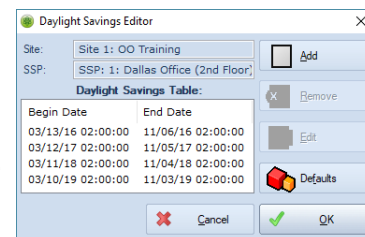


It is important to select the correct Controller Type when configuring the controller. Some boards have on-board subcontrollers that are added automatically when the controller is configured.

- Controller Enabled - Toggle checkbox to enable/disable the controller. Disabled controllers will appear gray in the Hardware Browser and do not communicate with the DNA driver.
- Home Page - A file associated with the controller that will open when the object goes into alarm.
- Download on Demand Exempt - If the driver has been configured to download personnel when they badge at a reader (Download Personnel on Demand), selecting this checkbox will override the setting and personnel will be downloaded normally.
- Physical Address - Physical address defined by the controller's DIP switch settings. This option should only be set on controllers with a serial connection.

Controller Time Parameters

- GMT Offset - Number of hours offset from Greenwich Mean Time. Determines the controller's time zone.
 - ☐ -5 = Eastern Time
 - ☐ -6 = Central Time
 - ☐ -7 = Mountain Time
 - ☐ -7 = Arizona
 - ☐ -8 = Pacific Time
 - ☐ -9 = Alaska
 - ☐ -10 = Hawaii
- Time Schedule Set - Selected Time Schedule Set for the SSP. See page 5-7 in the DNA Fusion User Manual for more information.
- Holiday Set - Selected Holiday Set for the SSP. See page 5-11 in the DNA Fusion User Manual for more information.
- Use Daylight Savings - Check to automatically adjust for daylight saving time. If this option is not selected, a message will appear when closing the Controller Properties dialog.
- Edit Table - Opens the Daylight Savings Editor.
 - ☐ Add - Opens the Daylight Savings Date Editor to define a Start and End Date/Time.
 - ☐ Remove - Removes the selected Daylight Savings entry.
 - ☐ Edit - Opens the Daylight Savings Date Editor to edit the selected date pair.
 - ☐ Defaults - Restores the default Daylight Savings information.
- Host Response Time - If Host Verification is enabled in the Door Properties / Advanced dialog (page 3-31), the SSP will report to the host computer for access confirmation. The Host Response Time is a timeout value for that decision. If the delay exceeds the value, the SSP will complete the access granted cycle.



Connection

- Connection Type - Connection type defined in the channel properties. (Auto-populated)
 - ☐ If Ethernet (TCP/IP) Channel, **enter** the IP Address.
 - ☐ If IP Client - Remote (TCP/IP) Channel, **enter** the MAC Address.
 - ☐ If Serial Channel, no information is required; however, the Physical Address will need to be set to a unique value.
 - ☐ If Modem Channel, **enter** the Phone Number. The phone number should not contain any dashes, spaces or parentheses. A comma creates a pause.
- Poll Delay - Time between each poll from the tree host to the SSP. (Auto-populated)
- Baud Rate - Speed at which the SSP communicates with the subcontrollers. (DIP switches 6 and 7)



A Baud Rate is the rate at which information is transferred in a serial communication channel. It is expressed in units of bits per second (bps, b/s). For example, a serial port with a baud rate of 9600 can transfer a maximum of 9600 bits per second.

- SSP Channel - Displays the channel number associated with the controller. (Auto-populated)
- Retry Count - Number of times a poll can fail before a panel is determined to be offline. (Default = 3)
- Offline Time - The time between messages from the host prior to SSP offline condition. For dialup connections, this allows the SSP to hang up after the host breaks the connection.

Downstream Ports

The following fields are determined by the Controller Type selection:

- Port 1 Baud Rate - Baud rate for Port 1. (SSP-D2, DController, SSP-LX, and PIM400-1501 only)
- Port(s) 2-5 Baud Rate - Baud rate for Ports 2-5; redundant ports. (SSP-EP, SSP-LX, and SSP/E only)
- Downstream Baud Rate - Baud rate for downstream ports.

Stored Quantities

Hardware Properties: Controller 1.1

Controller Properties
Stored Quantities
Cards and Dual Comm

Panel Memory: 6 MB Offline Transaction Capacity: 50000 Calculate

Controller Flags

- ☐ Store Issue codes
- ☐ Store APB Location
- ☒ Store Activation Date
- ☒ Store Deactivation Date
- ☐ Support Timed Anti-Pass Back
- ☐ Store Vacation date
- ☐ Store Temporary upgrade date
- ☐ Store Trigger Code
- ☐ Store Use limit

Quantities

Access Levels Per Card: 32
Large Card Size (bytes): *None*
Precision Access Levels: *None*
Access Levels: 255
Triggers: 125
Macros: 125

Time Schedules: 255
Holidays: 255
Cards: 3000
Secured Areas: 32
Unreported Transactions: 4000

Elevator Control

Max Floor: 3
Max per Cab: 1
Floor Groups: 2
Edit Floor Names

PIN and Duress Options

PIN digits to store: 6
Card ID Size: 32 Bit
Duress Digit: 0
Duress PIN Mode: *None*

Ok Cancel Help

Controller Memory

- Panel Memory - The amount of memory on the panel.
 - The SSP-EP defaults to 15 MB, but can be expanded with a memory module.
 - The SSP-D2, DController and PIM400-1501 default to 6 MB. Memory is expandable on the SSP-D2.
 - The SSP/C, default to 512 KB.
 - The SSP, SSP/E default to 1 MB, but can be expanded with a memory module.
 - The SSP-LX defaults to 16 MB, but can be expanded with a memory module.

Offline Transaction Capacity

- Offline Transaction Capacity - The number of transactions held in memory before the controller discards first-in/first-out transactions.
- Calculate - Automatically calculates the maximum Offline Transaction Capacity number based on current flags and quantity amounts set below. This figure should be less than the available memory.

Controller Flags

If a feature is used, it must be stored in the controller in order for it to work properly.

- Store Issue Codes - Stores Issue Codes for cards. The Issue Code number is used with magstripe cards and indicates the number of times a card has been issued to the cardholder (e.g. replacing a lost card). It is an internal number that is programmed on the card. See page 3-59 for more information on card formats.
- Store APB Location - If selected, stores the Anti-Pass Back (APB) locations when using APB.
- Store Activation Date - Stores the activation date and prevents access prior to the date set. (Default)
- Store Deactivation Date - Stores the deactivation date and prevents access after the date set. (Default)
- Support Timed Anti-Pass Back - Stores time of last entry to use with Anti-Pass Back. This option must be selected in order to use Timed Anti-Pass Back. For more information, see Chapter 11 in the DNA Fusion User Manual.
- Store Vacation Date - Stores the dates set for the vacation feature. See page 7-6 in the DNA Fusion User Manual for more information.
- Store Temporary Upgrade Date - Stores the temporary access level. See page 7-17 in the DNA Fusion User Manual for more information.
- Store Trigger Code - Stores trigger codes for card events on trigger and macro events. See page 10-11 in the DNA Fusion User Manual for more information.
- Store Use Limit - If selected, a card's Use Limit will be stored in the controller. See page 7-35 in the DNA Fusion User Manual for more information.

Quantities

- Access Levels Per Card - Number of access levels that can be assigned per card for the selected SSP. For more information, see Chapter 6 in the DNA Fusion User Manual.
- Large Card Size (bytes) - Provides support for large card sizes for PIV, PIV-I and TWIC cards.
- Precision Access Levels - The maximum number of precision access levels that can be assigned. See page 6-17 in the DNA Fusion User Manual for more information.
- Access Levels - The maximum number of access levels that can be stored in the controller. (Max. 255)
- Triggers - Indicates the maximum number of triggers to store. (Default = 125)
- Macros - Indicates the maximum number of macros to store. (Default = 125)
- Time Schedules - Each controller is able to store 255 time schedules. (Auto-populated)
- Holidays - Each controller is able to store 255 holidays. (Auto-populated)
- Cards - Indicates the maximum number of cards that can be stored in the controller. Cardholders must have an access level associated with the controller.



This number must be greater than the number of cardholders assigned access to the selected controller. If not, the additional cardholders will receive an Access Denied: Not in Card File event when they request access at a reader.

- Secured Areas - The maximum number of secured areas that can be created in the controller.
- Unreported Transactions - Number of unreported transactions before an event is logged. An event will occur when this number is exceeded. This event can be used to trigger the SSP to dial back and report transactions in modem configurations.

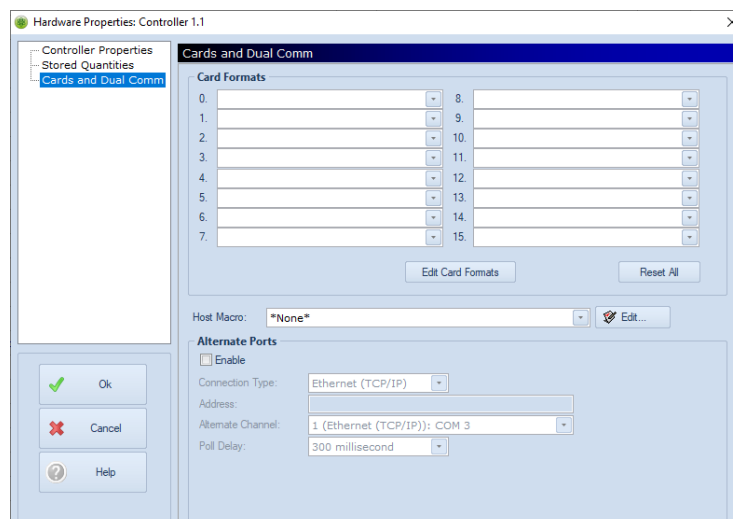
Elevator Control

- Max Floor - Indicates the maximum number of floors in the building.
- Max per Cab - Select the maximum number of floors per cab. The number entered must be less than or equal to the Max Floor quantity.
- Floor Groups - Maximum number of elevator access levels per floor group.
- Edit Floor Names - Opens the Edit Floor Names dialog to enter floor names. The number of Floor Names that can be edited is determined by the Max Floor setting. See page 8-52 in the DNA Fusion User Manual for more information on the dialog.

PIN and Duress Options

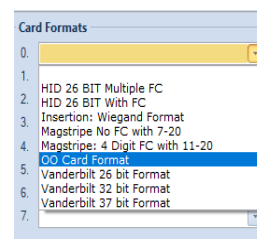
- PIN Digits to Store - Number of PIN digits to store in the controller. Used with a keypad reader.
- Card ID Size - Identifies the card size and sets the card format.
- Duress Digit - Specifies the duress digit (0 through 9) used to initiate a Duress event. Setting the Duress Digit to 0 indicates that the Duress feature is not used.
- Duress PIN Mode - Select the duress mode:
 - ☐ Add - If selected, the duress would be issued when the cardholder adds the specified Duress Digit to their original PIN. Only the last number of the PIN code will be changed.
 - ✦ Example: If the PIN Number is 1234 and the Duress Digit is set to 1, then the cardholder's Duress PIN would be 1235 – cardholder's original PIN 1234 + 1 = 1235.
 - If the Duress Digit is set to 6, then the cardholder's duress PIN would be 1230 – cardholder's original PIN 1234 + 6 = 1230.
 - ✦ If the Add option is selected, verify that duress PIN codes do not overlap with another cardholder's PIN number.
 - ☐ Append - If selected, the duress would be issued when the cardholder inserts the Duress Digit at the end of the cardholder's original PIN code.
 - ✦ Example: If the PIN Number is 1234 and the Duress Digit is set to 1, then the cardholder's Duress PIN would be 12341 – cardholder's original PIN 1234 with 1 inserted at the end = 12341.

Cards & Dual Comm



Card Formats (Assets)

- Card Formats 0-15 - Select a card format from the drop-down list. See page 3-59 for more information on creating card formats.
- Edit Card Formats - Opens the Card Formats Dialog to add, copy, edit, or remove card formats. See page 3-59 for more information.
- Host Macro - Select the Host Based Macro to execute from the list or click the Edit button.
 - ❑ Edit - Opens the Host Based Macro (Global I/O) dialog. See page 10-13 in the DNA Fusion User Manual for more information on Host Based Macros.



Alternate Ports

This section will only be available for SSP-EP and SSP-E controllers.

- Enable - If checked, enables the alternate ports when the communication is lost on the primary port. The remaining fields in the Alternate Ports section become available.
- Connection Type - Alternate port connection type.
- Phone Number - If the modem is selected, identifies the phone number to dial.
- Alternate Channel - Communication channel for the alternate port.
- Poll Delay - Time between polls on the alternate port. (Max. 3000 milliseconds)

Batch Processing

The Batch Processing feature allows command files to be sent to a controller. A command file is a text file that is formatted with commands and parameters. For instance, a batch process can be used to load an LED Mode table to a reader so that the LED lights behave in a manner other than the default setting.

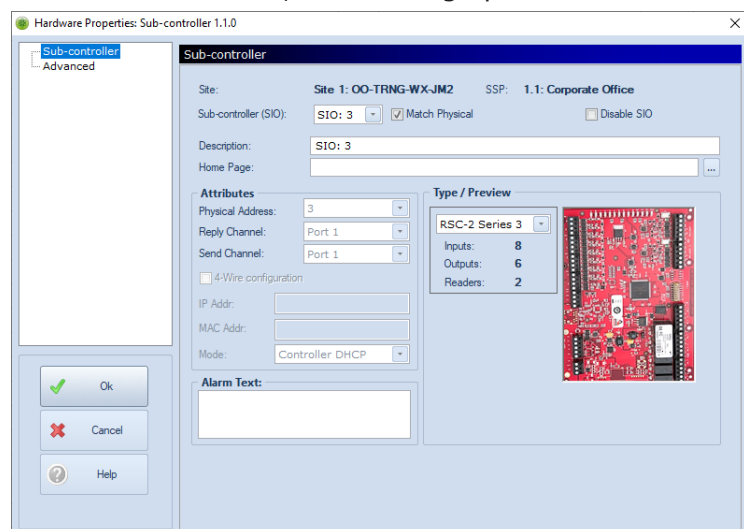
There are two ways to download a batch file to a controller:

- DNA / Administrative / Batch Processing. See page 20-14 in the DNA Fusion User Manual for more information.
- DNA Batch Download Settings Utility. See page 5-6 for more information.

Technical Installation Manual

Adding Subcontrollers

1. In the Hardware Browser, **right-click** on an existing Controller object and **select** Add/ Add Subcontroller. The Subcontroller Properties dialog opens.



2. **Enter** a Description for the subcontroller.
3. If desired, **check** Match Physical; the SSP will attempt to communicate with the subcontroller number that matches the predefined address settings. This address must match the DIP switch setting on the board.

Or

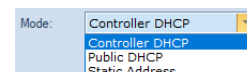
If Match Physical is unchecked, **select** a Physical Address.

4. If desired, **click** the Browse button to associate a Home Page with the subcontroller.
5. **Select** the Type of subcontroller from the drop-down list.

A preview of the board displays in the Type / Preview panel.

- If the NSC-100 subcontroller is selected, continue to step A.
- If GTWY, PIM400-485, or AD 300 is selected, see Chapter 7 in the System Hardware Manual.
- If Virtual SIO, Salto Router or Aperio Hub is selected, see Chapter 9 in the System Hardware Manual.
- For all other subcontrollers, continue to step 6.

- a. If NSC-100 is selected from the Type drop-down, **select** the Mode.

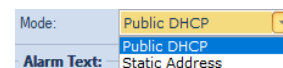


- ☐ **Controller DHCP** - The NSC-100's MAC address is automatically assigned an IP address from the controller, and the embedded DHCP server loads the IP address into the NSC-100.
- ☐ **Public DHCP** - The NSC-100's MAC address is automatically assigned an IP address from the public DHCP server, and the embedded DHCP server loads the IP address into the NSC-100.
- ☐ **Static Address** - The NSC-100 will be manually assigned a static IP address using the MR51e Address Tool.



Both Controller DHCP and Static Address methods require that the NSC-100 and the controller be in the same subnet and not isolated by network switches.

- b. **Enter** the IP Address for the NSC-100.
- c. **Enter** the MAC Address found on the NSC-100's on-board RJ-45 socket.
- d. If NSC-200 is selected from the Type drop-down, select the Mode.



- ☐ **Public DHCP** - The NSC-200's MAC address is automatically assigned an IP address from the public DHCP server, and the embedded DHCP server loads the IP address into the NSC-200.
- ☐ **Static DHCP** - Enter the NSC-200's IP address configured on the NSC-200 Configuration Managers. See page 3-41 in the System Hardware Manual for more information.

6. If desired, **enter** Alarm Text.
7. If desired, **select** the Advanced menu option to configure the advanced settings.
See page 3-21 for more information.
8. **Click** OK to save the settings.
The subcontroller appears in the Hardware Browser.

Subcontroller Properties

Sub-controller

The screenshot shows a software window titled "Hardware Properties: Subcontroller 1.1.0". Inside, there's a "Sub-controller" tab. The "Site" is "Site 1: OO Training" and "SSP" is "1.1: Dallas Office (2nd Floor)". "Subcontroller (SIO)" is set to "SIO: 3" with the "Match Physical" checkbox checked. "Description" is "SIO: 3" and "Home Page" is empty. Under "Attributes", "Physical Address" is "3", "4-Wire configuration" is unchecked, "SSP Reply Channel" is "Port 1", and "SSP Send Channel" is "Port 1". "IP Addr", "MAC", and "Mode" (set to "Controller DHCP") are also present. An "Alarm Text" field is at the bottom. A "Type / Preview" section shows "RSC-2" with "Inputs: 8", "Outputs: 6", and "Readers: 2", accompanied by a circuit board image. Navigation buttons (Ok, Cancel, Help) are at the bottom left.

Address

- Site - Identifies the site name defined in the Site Properties dialog. (Auto-populated)
- SSP - Name of the SSP controller attached to the subcontroller. (Auto-populated)
- Subcontroller (SIO) - Subcontroller identification in the software.
 - ❑ Match Physical - Matches the physical address in the software with the dipswitch settings on the board. When selected, the SSP will attempt to communicate with the subcontroller number that matches the dipswitch settings. For example, SIO 2 will communicate with the subcontroller that has a Physical Address of 2. See the System Hardware Manual for dipswitch settings.
- Disable SIO - If checked, disables the subcontroller and stops communication with the SSP controller.
- Description - User-defined description of the subcontroller; typically location- or function-related.
- Home Page - The homepage associated with the subcontroller.

Attributes

- Physical Address - Physical address as set on the DIP switches. This option will be grayed out when the Match Physical option is selected and will automatically increase as subcontrollers are added to the system. See the System Hardware Manual for more information on DIP switch settings.
- 4-Wire Configuration - If checked, indicates the 4-Wire RS-485 communication is ON. (Legacy hardware only)
- SSP Reply Channel - Identifies the SSP port that the subcontroller will use when communicating with the controller.
- SSP Send Channel - Reflects the SSP Reply Channel. (Auto-populated)
- IP Addr - When the NSC-100 or NSC-200 subcontroller is selected, the IP Addr field identifies the IP address assigned to the subcontroller.
- MAC - If the NSC-100 subcontroller is selected, the MAC field identifies the subcontroller's default MAC address.
- Mode - When the NSC-100 or NSC-200 subcontroller is selected, use the Mode drop-down to define the addressing method: Controller DHCP, Public DHCP or Static Address. See page 3-17 for more information.

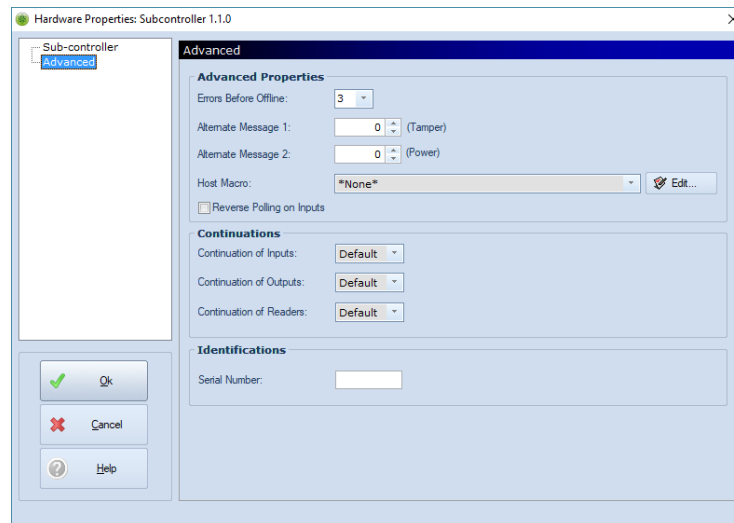
Type/Preview

- Type - Drop-down list to select the type of subcontroller.
- Inputs - Number of inputs on the selected subcontroller. (Auto-populated)
- Outputs - Number of outputs on the selected subcontroller. (Auto-populated)
- Readers - Number of readers on the selected subcontroller. (Auto-populated)

Alarm Text

- Point-specific alarm text that is displayed in the Alarm Grid when an alarm occurs.

Advanced



Advanced Properties

- Errors Before Offline - Number of consecutive communication errors before the subcontroller is determined to be offline.
- Alternate Message 1 (Tamper) - Changes the alarm priority for the cabinet tamper from the event-specific priority to the user-determined priority.
- Alternate Message 2 (Power) - Changes the alarm priority for the power tamper from the event-specific priority to the user determined priority.
- Host Macro - Select the Host Based Macro to execute.
 - ❑ Edit - Opens the Host Based Macro (Global I/O) dialog. See page 10-13 in the DNA Fusion User Manual for more information on Host Based Macros.
- Reverse Polling on Inputs - Changes the order by which the system processes inputs. If selected, inputs will be processed from higher number to lower number.

Continuations

The following options are advanced features and should not be modified unless the operator has a thorough understanding of the ramifications.

- Continuation of Inputs (Elevator Setting) - If the number of floors selected exceeds the available inputs for a single controller, inputs will be taken from the next consecutive subcontroller. This allows you to jump/skip subcontrollers with continuation.
- Continuation of Outputs (Elevator Setting) - If the number of floors selected exceeds the available outputs for a single controller, outputs will be taken from the next consecutive subcontroller. This allows you to jump/skip subcontrollers with continuation.
- Continuation of Readers (Elevator Setting) - If the number of floors selected exceeds the available readers for a single controller, readers will be taken from the next consecutive subcontroller. This allows you to jump/skip subcontrollers with continuation by identifying the subcontroller 1-64 that will be used.

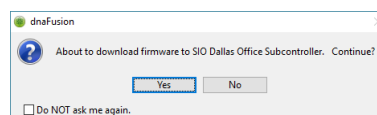
Identification

- Serial Number - Reference field only; stores the subcontroller serial number for future reference.

Updating Subcontroller Firmware

The subcontroller's (RSC-1/RSC-2/RSC-DT/ISC-16/OSC-16/NSC-100/NSC-200) firmware can be updated from the Hardware Browser.

1. **Right-click** on the desired Subcontroller and **select** Reload Firmware from the menu.
A confirmation dialog appears.
2. **Click** Yes to confirm.
The subcontroller's firmware is reloaded.



Technical Installation Manual

Adding Doors

A door, also referred to as an Access Control Model (ACM), performs two functions: it validates access requests, and it manages and monitors the access point. It is possible to configure a door without a physical reader, if only door monitoring functions are required.

DNA Fusion supports three types of doors: Single, In & Out, and Turnstile.

Adding a Single Door

1. In the Hardware Browser, **right-click** on the Door under the Controller and **select** Add Door / Use Default.
Or
Right-click on the Controller and **select** Add / Add Door / Use Default.
The New Door dialog opens.



Doors can also be added through a specific reader. See page 3-26 for more information.

2. If needed, **select** the appropriate Door Type from the drop-down menu.
3. **Enter** a Description for the door (typically location-related).
4. If desired, **click** the Browse button to associate a Home Page with the door.
See page 3-27 for more information on the remaining Common Properties.
5. **Select** Door Objects option from the dialog menu.
6. **Select** Single from the Type drop-down.
7. **Set** the remaining Door Properties.
If this is a PIM or AD door, specify the Extension (Ext.) Mode.
8. **Select** the Reader from the address drop-down list.
9. **Select** the Contact and Request to Exit objects to configure the door settings.
10. **Select** the Strike from the drop-down list.
See page 3-29 for more information on each Door Object.
The Edit buttons will become available as each hardware object is selected.
11. If desired, **set** the Strike Time and Held Time under the ADA Settings.
These settings only apply if the ADA Mode flag is checked in the Cardholder's Record.
12. If desired, **configure** the Advanced dialog per the descriptions on page 3-31.
13. If desired, **configure** the Macros dialog. See page 3-33 for more information.
14. If desired, **select** the Auto Unlock option from the dialog menu and **configure** the door to follow a designated time schedule. See page 3-35 for more information.
15. **Click** OK to save the settings.
The door is added to the Hardware Browser.

Adding an In and Out Door

1. In the Hardware Browser, **right-click** on the Door under the Controller and **select** Add Door / Use Default Or
Right-click on the Controller and **select** Add / Add Door / Use Default.
The New Door dialog opens.



Doors can also be added through a specific reader. See page 3-26 for more information.

2. If needed, **select** the appropriate Door Type from the drop-down menu.
3. **Enter** a Description for the door (typically location-related).
4. If desired, **click** the Browse button to associate a Home Page with the door.
See page 3-27 for more information on the other Common Properties.
5. **Select** Door Objects from the dialog menu.

6. **Select** In and Out from the Type drop-down.
The Out Reader section appears.
7. If needed, **select** the In Reader from the drop-down list.
The Edit buttons will become available as each hardware object is selected.
8. **Select** the Contact from the drop-down.
9. **Select** the Out Reader from the drop-down list and **verify** the Pair Door: selection.
10. **Select** the Strike and continue to configure the door settings.
See page 3-29 for more information on each Door Object.
11. If desired, **configure** the Advanced dialog per the descriptions on page 3-31.
12. If desired, **configure** the Macros dialog. See page 3-33 for more information.
13. If desired, **select** the Auto Unlock option from the dialog menu and **configure** the door to follow a designated time schedule. See page 3-35 for more information.
14. **Click** OK to save the settings.
The door is added to the Hardware Browser.

Adding a Turnstile

1. In the Hardware Browser, **right-click** on the Door under the Controller and **select** Add Door / Use Default.
Or

Right-click on the Controller and **select** Add / Add Door / Use Default.

The New Door dialog opens.



Doors can also be added through a specific reader. See page 3-26 for more information.

2. If needed, **select** the appropriate Door Type from the drop-down menu.
3. **Enter** a Description for the door (typically location-related).
4. If desired, **click** the Browse button to associate a Home Page with the door.
See page 3-27 for more information on the other Common Properties.
5. **Select** Door Objects from the dialog menu.

6. **Select** Turnstile from the Type drop-down.
The Strike Mode field will appear under the Door Properties section.
7. **Select** the desired Strike Mode from the drop-down:
 - Pulse on Grant - Pulses the turnstile when access is granted.
 - Pulse on Door Cycle - Pulses the turnstile when the arm is cycled.
8. If needed, **select** the Reader from the drop-down list.
The Edit buttons will become available as each hardware object is selected.
9. **Select** the Contact from the drop-down.
10. **Select** the Request to Exit (REX) from the drop-down list.
11. **Select** the Strike and continue to configure the door settings.
See page 3-29 for more information on each Door Object.
12. If desired, **configure** the Advanced dialog per the descriptions on page 3-31.
13. If desired, **configure** the Macros dialog. See page 3-33 for more information.
14. If desired, **select** the Auto Unlock option from the dialog menu and **configure** the door to follow a designated time schedule. See page 3-35 for more information.
15. **Click** OK to save the settings.
The door is added to the Hardware Browser.

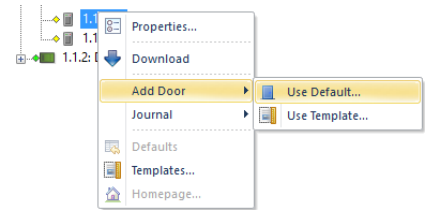
Adding a Door From a Reader

This shortcut allows the door to be created from the associated reader.

1. In the Hardware Browser, **expand** the Subcontroller and **right-click** on the desired Reader object.
2. **Select** Add Door / Use Default from the context menu.

The New Door dialog opens.

3. **Enter** a Description for the door (typically location-related).
4. If desired, **configure** the other options in the Common Properties dialog per the descriptions on page 3-27.
5. **Select** the Door Objects option from the dialog menu.



The Door Objects auto-populate with the reader address as well as the addresses for the next set of available points. See page 3-29 for more information on Door Objects.

Hardware Properties: NEW Door

- Common Properties**
 - Door Objects
 - Advanced
 - Macros
 - Auto Unlock
 - Notes
- Door Objects**
 - Door Properties**
 - Type: **Single** (LED Mode: No Change) [Edit...]
 - Pre-Alarm: 0 sec (Held Time: 10 sec)
 - Ext. Mode: None
 - Reader**
 - Address: *None* [Edit...]
 - Default Mode: Card Only (Type: Normal)
 - Offline Mode: Facility Code
 - Contact**
 - Address: *None* [Edit...]
 - Request To Exit (REX)**
 - Address: *None* [Edit...]
 - Strike**
 - Address: *None* [Edit...]
 - Activation: 3 sec (Mode: No impact on strike)
 - ADA Settings**
 - Strike Time: 56 sec (Held Time: 0 sec)

Buttons: Ok, Cancel, Help

6. If desired, **configure** the Advanced dialog per the descriptions on page 3-31.
7. If desired, **configure** the Macros dialog per the descriptions on page 3-33.
8. If desired, **select** the Auto Unlock option from the dialog menu and **configure** the door to follow a designated time schedule. See page 3-35 for more information.
9. **Click** OK to save the settings.

The door is added to the Hardware Browser.

Door Properties

Common Properties

Address

- Site - Identifies the site associated with the door. (Auto-populated)
- Controller - Identifies the controller associated with the door. (Auto-populated)
- Door Number - Drop-down field to select the ACM number.
- Door Type - Determines how the door will function.
 - ☐ Normal - Door will operate as a regular access control door.
 - ☐ Muster - Door will operate as both a muster point and a regular access control door. See the Muster Report Manual for more information.
 - ☐ Auto Activate - Door will operate as a regular access control door, but if a badge is presented that has been designated an Auto Activate card, the badge will be activated. See page 7-12 in the DNA Fusion User Manual for more information.
 - ☐ Auto Deactivate - Door will operate as a regular access control door, but if a badge is presented that has been designated an Auto Deactivate card, the badge will be deactivated. See page 7-12 in the DNA Fusion User Manual for more information.
 - ☐ Time and Attendance In - Door will operate as a regular access control door, but if a badge is presented that has been designated a Time & Attendance card, the data will be collected and stored in a separate table as the In Time. See page 7-12 in the DNA Fusion User Manual for more information.
 - ☐ Time and Attendance Out - Door will operate as a regular access control door, but if a badge is presented that has been designated a Time & Attendance card, the data will be collected and stored in a separate table as the Out Time. See page 7-12 DNA Fusion User Manual for more information.



See page 5-13 for information on generating a DNA Time and Attendance Report.

- Situations... - Opens the Situation Level Manager Settings dialog for the associated door. See Chapter 9 in the DNA Fusion User Manual for more information.

Other

- Description - User-defined description of the door that appears in the browser; typically location-related.
- Home Page - Home page that will open when the door goes into alarm.

Point Alarm Properties

- Alternate Priority - If selected, overrides the default event-specific Alarm Priority set in DNA / Administrative / Alarms and Events / Logging. The alternate ID will be displayed in the Alarm Grid. See page 14-25 in the DNA Fusion User Manual for more information.
- Security Level - Category designation. Allows administrator to restrict operator use. See page 4-8 in the DNA Fusion User Manual for more information.
- Do Not Load Home Page on Alarm - If the associated door goes into alarm, the Home Page will not load.
- Alarm Media File - Audio file to be played when the associated door goes into alarm.
- Alarm Text - Additional text to be displayed with the alarm reason when the associated door goes into alarm.
- Camera - Drop-down list of available cameras to associate with the door. If selected, enables the Launch Camera and Show Archived Video options in the Events and Alarm Grid context menus. Selecting a menu option will populate the camera in the Video View Manager.

Templates

The operator should create templates before applying them to hardware objects. See page 8-83 in the DNA Fusion User Manual for more information on templates.

- Template Name - Select a template to configure the door.
- Description - Auto-populated by the template.
- Application Notes - Auto-populated by the template.

Door Objects

Door Parameters

- Type - Specifies the type of door.
 - ☐ Single - Select this option to configure a single door with one reader.
 - ☐ In and Out - Select this option when using Access Areas or Anti-Pass Back; two readers will be assigned to the door.
 - ☐ Turnstile - Select this option to configure a turnstile door; the Strike Mode drop-down list will appear.
- Pre-Alarm - Number of seconds before the selected door reports a Door Held Pre-Alarm event/alarm, causing an event to be generated prior to a Door Held alarm.
- Ext. Mode - Sets the door's exterior mode. Only available for Schlage AD doors. See the System Hardware Manual for more information.
- LED Mode - Defines the LED operation of the reader.
 - ☐ Edit - Opens the LED Function Configuration dialog to configure the LED settings for custom values.
- Held Time - Length of time an input will be ignored when it goes active during an Access Granted event. Indicates the number of seconds before the door reports a Door Held event/alarm. This only applies to inputs that are specified as the Door Contact.

Reader

- Address - Specifies the reader's address.
 - ☐ Edit - Opens the Reader Properties dialog. See page 3-46 for more information.
- Default Mode - Defines the normal state of the reader.
 - ☐ None - A reader is not associated with the door and all door hardware is inoperable.
 - ☐ Disabled - Disables the reader; the door remains locked with no REX capability.
 - ☐ Unlocked - Allows unlimited access to the door without the need for an access level.
 - ☐ Locked - Access is not allowed, but the door can be used from the inside by using the REX button.
 - ☐ Facility Code - Only the facility code is checked for access authorization.
 - ☐ Card Only - Checks the card number for access authorization.
 - ☐ PIN Only - Verifies the PIN code for access authorization.
 - ☐ Card and PIN - Checks the card and PIN numbers for access authorization.
 - ☐ PIN or Card - Either the PIN or card number is checked for access authorization.
- Offline Mode - Defines the offline mode of the reader.
 - ☐ None - The door is not associated with a reader nor any additional door hardware.
 - ☐ Disabled - Disables the reader; the door remains locked with no REX capability.
 - ☐ Unlocked - Allows unlimited access to the door without the need for an access level.

- ☐ Locked - Access is not allowed, but the door can be used from the inside by using the REX button.
- ☐ Facility Code - Only the facility code is checked for access authorization.
- Type - Specifies type of reader.
 - ☐ Normal - Standard card reader.
 - ☐ Keypad - A reader with a numeric keypad.
 - ☐ Text Keypad - A reader with both a numeric keypad and text display.

Contact

- Address - Specifies the address of the door contact.
 - ☐ Edit - Opens the Input Properties dialog for the door contact. See page 3-49 for more information.

Request to Exit (REX)

This section appears if Type is set to Single or Turnstile.

- Address - Specifies the address of the REX.
 - ☐ Edit - Opens the Input Properties dialog for the REX input. See page 3-49 for more information.

Out Reader

This section appears if Type is set to In and Out. It is used in conjunction with Anti-Pass Back (APB) settings. See Chapter 11 in the DNA Fusion User Manual for more information.

- Address - Specifies the address of the Out Reader; both readers must be wired to the door.
 - ☐ Edit - Opens the Reader Properties dialog for the reader. See page 3-46 for more information.
- Pair Door - Drop-down field to select a Door to pair with the Out Reader.

Strike

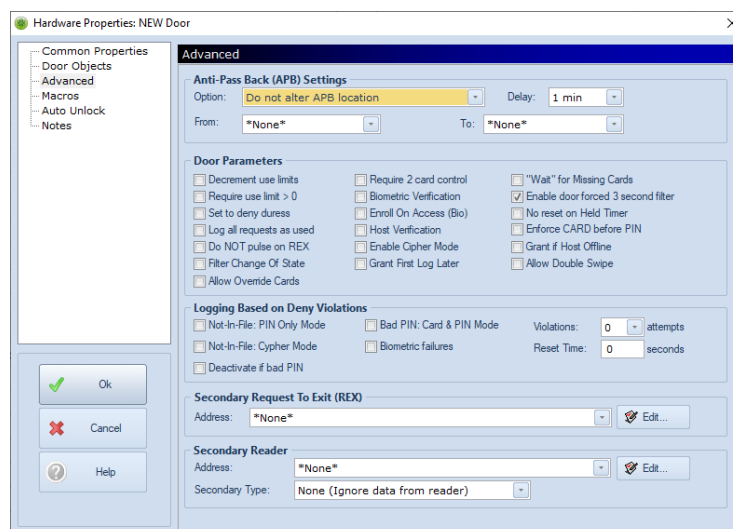
- Address - Specifies the address of the door strike.
 - ☐ Edit - Opens the Output Properties dialog for the strike. See page 3-53 for more information.
- Activation - Maximum number of seconds the door will be unlocked when an Access Granted event is received. Check code for your area.
- Mode - Defines how the door strike will behave when the door is opened.
 - ☐ No impact on strike - Opening the door or closing the door does not affect the activation timer.
 - ☐ Cut Short On Open - Strike activation timer is canceled and the strike is re-energized when the door is opened.
 - ☐ Cut Short On Close - Strike activation timer is canceled and the strike is re-energized when the door is closed after being opened. Primarily used for magnetic doors.
 - ☐ Tailgate: Short On Open - Strike activation timer is canceled and the strike is re-energized when the door is opened. In addition, the adjacent relay is pulsed for one (1) second.
 - ✦ Example: If the strike is assigned to 1.1.1.O1 then 1.1.1.O2 would be pulsed for one (1) second.
 - ☐ Tailgate: Short On Close - Strike activation timer is canceled and the Strike is re-energized when the door is closed after being opened. In addition, the adjacent relay is pulsed for one (1) second.
 - ✦ Example: If the strike is assigned to 1.1.1.O1 then 1.1.1.O2 would be pulsed for one (1) second.

ADA Settings

The following options are invoked for cardholders when ADA Mode is flagged in the Card Tab of the Cardholder's Record. See page 7-12 in the DNA Fusion User Manual for more information.

- Strike Time - Number of seconds the strike will unlock if card is flagged as ADA.
- Held Time - Number of seconds before the door reports a Door Held alarm/event if card is flagged as ADA.

Advanced



Anti-Pass Back (APB) Settings

See Chapter 11 in the DNA Fusion User Manual for information on configuring Anti-Pass Back.

- Option - Drop-down field to select the type of anti-pass back.
 - ☐ Do not alter APB location - Anti-pass back is not in use.
 - ☐ Accept any location, change on entry - Accept any new location, change the user's location to the current reader, and generate an anti-pass back violation for an invalid entry. (Area-based Soft APB)
 - ☐ Check location, change on entry - Check user location; if a valid entry is made, change the user's location to the new location. If an invalid entry is attempted, do not grant access. (Area-based Hard APB)
 - ☐ Check last valid user - References the user's card number and will not allow access to the same card number until either a different card is presented at the reader or the APB delay expires. Requires Support Timed Anti-Pass Back to be enabled in the Controller Properties / Stored Quantities dialog. See page 3-13 for more information. (Reader-based APB using the reader's last user)
 - ☐ Check last ACR used, no location change - Does not allow a cardholder to present his or her card to the same reader twice in a row. Once access is granted at the reader, the user will not be granted access at the same reader again until the user presents his card at another reader in the system or until the APB delay expires. Requires Support Timed Anti-Pass Back to be enabled in the Controller Properties / Stored Quantities dialog. See page 3-13 for more information. (Reader-based APB using the cardholder's access history)
 - ☐ Check current location, change on entry - Similar to option #2, except that the APB delay will reset the user's area after the specified time. Requires Support Timed Anti-Pass Back to be enabled in the Controller Properties / Stored Quantities dialog. See page 3-13 for more information. (Area-based APB)
- Delay - The number of minutes before APB resets. Only used in conjunction with APB options #3-5. (Max. delay = 1092 minutes)
- From - The Access Area that the cardholder comes from.
- To - The Access Area that the cardholder enters.

Door Parameters

- Decrement Use Limits - The selected door will decrement Use Limits associated with cards.
- Require Use Limit > Zero - If a card's Use Limit reaches 0, do not grant access.
- Set to Deny Duress - Denies access when the controller receives a duress signal at the selected door. (PIN & Card Only)
- Log All Requests as Used - Assumes that the door was used and logs all access requests as Door Used when the request is granted. Do not use with Anti-Pass Back.
- Do NOT pulse on REX - Prohibits pulsing the door strike during the REX cycle. Used for a quiet exit.
- Filter Change of State - Filters all state changes and displays only Opened or Closed events.
- Allow Override Cards - Allows cardholders with Override Card credentials to bypass any door parameter and allow access to the door.



After mass editing door parameters, reset controllers to enable changes.

- Require 2 Card Control - Requires two (2) valid access credentials to be presented for access to be granted.
- Biometric Verification - Select if biometric hardware is being supported. This is an advanced feature and should be avoided unless the operator has an understanding of the ramifications.
- Enroll on Access (Bio) - Select if biometric hardware is being supported; the system will record the a person's biometric signature on the first presentation. This information will be used as the future reference.
- Host Verification - Host verification must be obtained prior to granting access. See Host Response Time on page 3-12 to set the timeout parameter. If selected, access at this door will be dependent on communication with the DNA server.
- Enable Cipher Mode - Allows the user to enter the card number through a keypad.
- Grant First Log Later - Grants access to the door and then logs the event; allows instant access to the door. Door Used/Not Used events are not logged until door is actually opened or timeout expires. Applies to Access Granted events only.
- "Wait" for Missing Cards - If an access request is denied due to a Card Not in File event, the reader is put into the wait state and waits for a host response from the DNA server.
- Enable Door Forced 3 Second Filter - If selected, a Door Forced event will NOT be reported if the door is reopened within three (3) seconds of closing after an Access Granted event. (Default setting)
- No Reset on Held Timer - If the selected door is opened after an Access Granted event, and a subsequent card read occurs, the Held Time set in the Common Properties dialog will not start over.
- Enforce CARD before PIN - Requires the cardholder to badge before entering their PIN number.
- Grant If Host Offline - Access will be granted if the host is offline. Works in conjunction with Host Verification.
- Allow Double Swipe - Enables the double swipe feature for the door. If selected, the user can write a trigger and macro combination to execute programmed commands. See page 10-9 in the DNA Fusion User Manual for more information.

Logging Based on Deny Violations

- Not-In-File: PIN Only Mode - Logs an event when an incorrect PIN is entered and the cardholder does not have an access level on this controller.
- Not-In-File: Cypher Mode - Logs an additional event when an incorrect PIN (card number) is entered.
- Deactivate if Bad PIN - Deactivates the card if the number of attempts exceeds the stated quantity.
- Bad PIN: Card & PIN Mode - An additional event will be logged when an incorrect PIN is entered for a valid card read.
- Biometric Failures - An additional event will be logged when a biometric failure occurs.
- Violations - Number of violations to allow before deactivating a card when an incorrect PIN is entered.
- Reset Time - The amount of time before the count resets pin violations. After the time has expired, the cardholder may attempt to reenter the PIN.

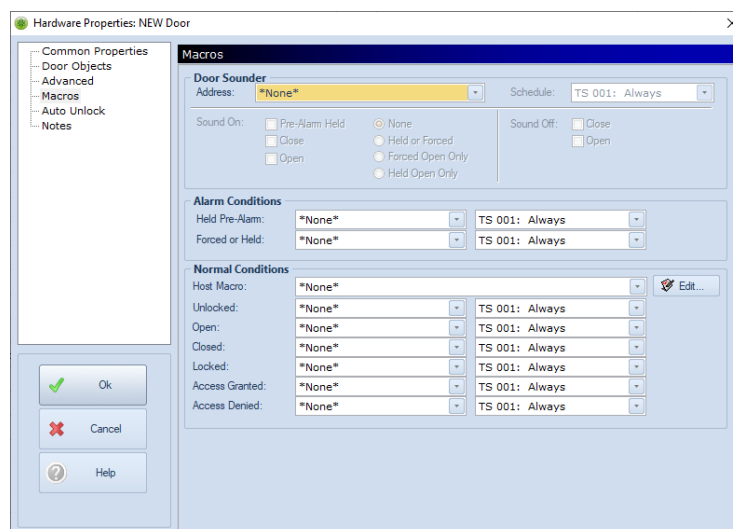
Secondary Request to Exit (REX)

- Address - Address of the secondary REX.
 - ☐ Edit - Opens the Output Properties dialog for the secondary REX. See page 8-77 in the DNA Fusion User Manual for more information.

Secondary Reader

- Address - Drop-down list of readers to select for Reader 2.
 - ☐ Edit - Opens the Reader Properties dialog for this object. See page 8-71 in the DNA Fusion User Manual for more information.
- Secondary Type - Drop-down list of reader types to select for Reader 2.

Macros



Door Sounder

Configuring this section creates a trigger and macro based on the selections.

- Address - Address of door sounder that will be affected.
- Schedule - Drop-down list of the available time schedules.
- Sound On - Condition(s) required to activate the door sounder. If the selected event occurs, the output listed above will be activated.
 - ☐ Pre-Alarm Held ☐ Held or Forced
 - ☐ Close ☐ Forced Open Only
 - ☐ Open ☐ Hold Open Only
- Sound Off - Condition(s) required to deactivate the door sounder. If the selected event occurs, the output listed above will be deactivated.

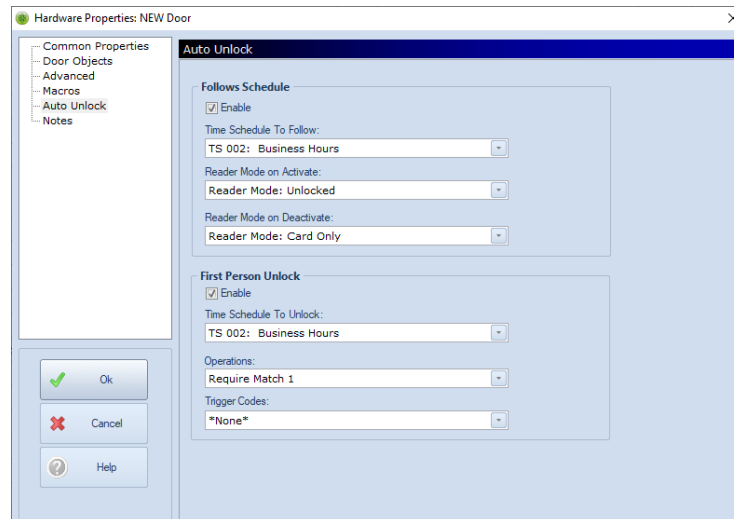
Alarm Conditions

- Held Pre-Alarm - Drop-down list of macros to activate when a Door Held Pre-Alarm message is received along with a drop-down list of available time schedules.
- Forced or Held - Drop-down list of macros to activate when a Forced or Held message is received along with a drop-down list of available time schedules.

Normal Conditions

- Host Macro - Select the Host Based Macro to execute.
 - ▣ Edit - Opens the Host Based Macro (Global I/O) dialog. See page 10-13 in the DNA Fusion User Manual for more information.
- Unlocked - Drop-down list of macros to activate when a Door Unlocked message is received along with a drop-down list of available time schedules.
- Open - Drop-down list of macros to activate when a Door Open message is received along with a drop-down list of available time schedules.
- Closed - Drop-down list of macros to activate when a Door Closed message is received along with a drop-down list of available time schedules.
- Locked - Drop-down list of macros to activate when a Door Locked message is received along with a drop-down list of available time schedules.
- Access Granted - Drop-down list of macros to activate when an Access Granted message is received along with a drop-down list of available time schedules.
- Access Denied - Drop-down list of macros to activate when an Access Denied message is received along with a drop-down list of available time schedules.

Auto Unlock



Follows Schedule

The Follows Schedule feature is used to set up a door to adhere to a specified time schedule and designated reader modes. See page 8-9 in the DNA Fusion User Manual for more information.

- Enable - If checked, activates the fields in the Follows Schedule section.
 - ❑ Time Schedule to Follow - Select the desired Time Schedule from the drop-down list.
 - ❑ Reader Mode on Activate - Select the Reader Mode for the door when the specified time schedule becomes active.
 - ❑ Reader Mode on Deactivate - Select the Reader Mode for the door when the specified time schedule becomes inactive.

First Person Unlock

The First Person Unlock feature can be used to configure a door to unlock when the first cardholder is granted access to the door during a specified time schedule. See page 8-9 in the DNA Fusion User Manual for more information.

- Enable - If checked, activates the fields in the First Person Unlock section.
 - ❑ Time Schedule to Follow - Select the desired Time Schedule from the drop-down list.
 - ❑ Operations - Select an Operation for the trigger code from the drop-down list. See page 10-11 in the DNA Fusion User Manual for more information. This field is only required if trigger codes are used.
 - ❑ Trigger Codes - Select the desired Trigger Code from the drop-down list. See page 10-11 in the DNA Fusion User Manual for more information.

Technical Installation Manual

Adding Elevators

Elevators fall into two categories:

- Non-Feedback - The elevator does not have tracking capability.
 - ☐ Requires an output for each floor (x per cab)
 - ☐ Requires a reader inside each cab
- Floor Selectors - The elevator is capable of tracking movement.
 - ☐ Requires an output for each floor (x per cab)
 - ☐ Requires a reader inside each cab
 - ☐ Requires an input for each floor (x per cab)



Before an elevator can be added, the elevator parameters must be configured in the Controller Properties / Stored Quantities dialog. See page 3-13 for more information.

1. In the Hardware Browser, **right-click** on the Elevator object under the Controller and **select** Add Elevator.

Or

Right-click on the Controller and **select** Add / Add Elevator.

The New Elevator dialog opens.



*The Elevators object must be checked in the Hardware Tree Properties for the object to be visible in the tree. **Right-click** in the white space of the Hardware Browser, **select** Tree Properties from the menu, and **check** Elevators under the "All Objects" Tree Items heading.*

2. **Enter** a Description (typically location-related).
See page 3-39 for more information on the other Common Properties.
3. **Select** Elevator Objects from the dialog menu.
See page 3-41 for more information on each Elevator Object.
4. **Select** Elevator Type from the drop-down list.
5. **Enter** the Floor Quantity from the drop-down list.
6. **Select** the Reader to pair with the elevator.
The Edit button will become available when the reader is selected.
7. If Elevator Type was set to Elevator Reader (Floor Selectors), **select** the First Input from the drop-down list.
8. **Select** the First Relay from the drop-down list.
9. If Elevator Type was set to Elevator Reader (Floor Selectors), **select** the Selection Delay time from the drop-down list.

10. **Select** the Relay Duration from the drop-down list.
11. **Configure** the Floor Groups section. See page 3-41 for more information.
12. If desired, **configure** the Elevator Parameters dialog.
See page 3-43 for information on Elevator Parameters.
13. If desired, **select** Auto Unlock from the dialog menu and **configure** the elevator to follow a time schedule.
See page 3-45 for more information on the Auto Unlock dialog.
14. **Click** OK to save the settings.
The elevator is added to the Hardware Browser.

Elevator Properties

Common Properties

Address

- Site - Identifies the site associated with the elevator. (Auto-populated)
- Controller - Identifies the controller associated with the elevator. (Auto-populated)
- Elevator Number - Drop-down field to select the ACM number.
- Door Type - Determines how the door will function.
 - ☐ Normal - Door will operate as a regular access control door.
 - ☐ Muster - Door will operate as both a muster point and a regular access control door. See the Muster Report Manual for more information.
 - ☐ Auto Activate - Door will operate as a regular access control door, but if a badge is presented that has been designated an Auto Activate card, the badge will be activated. See page 7-12 in the DNA Fusion User Manual for more information.
 - ☐ Auto Deactivate - Door will operate as a regular access control door, but if a badge is presented that has been designated an Auto Deactivate card, the badge will be deactivated. See page 7-12 in the DNA Fusion User Manual for more information.
 - ☐ Time and Attendance In - Door will operate as a regular access control door, but if a badge is presented that has been designated a Time & Attendance card, the data will be collected and stored in a separate table as the In Time. See page 7-12 in the DNA Fusion User Manual for more information.
 - ☐ Time and Attendance Out - Door will operate as a regular access control door, but if a badge is presented that has been designated a Time & Attendance card, the data will be collected and stored in a separate table as the Out Time. See page 7-12 in the DNA Fusion User Manual for more information.



See page 5-13 for information on generating a DNA Time and Attendance Report.

- Situations... - Opens the Situation Level Manager Settings dialog for the associated elevator. See Chapter 9 in the DNA Fusion User Manual for more information.

Other

- Description - User-defined description of the elevator that appears in the browser; typically location-related.
- Home Page - Home page associated with the elevator that will open when the elevator goes into alarm.

Point Alarm Properties

- Alternate Priority - If selected, overrides the default event-specific Alarm Priority set in DNA / Administrative / Alarms and Events / Logging. See page 14-25 in the DNA Fusion User Manual for more information.
- Security Level - Category designation. Allows administrator to restrict operator use.
- Do Not Load Home Page on Alarm - If the associated elevator goes into alarm, the Home Page will not load.
- Alarm Media File - Audio file to be played when the associated elevator goes into alarm.
- Alarm Text - Additional text to be displayed with the alarm reason when the associated elevator goes into alarm.
- Camera - Drop-down list of available cameras to associate with the elevator. If selected, enables the Launch Camera and Show Archived Video options in the Events and Alarm Grid context menus. For more information, see pages 14-7 and 14-23 in the DNA Fusion User Manual.

Templates

Templates are covered on page 8-83 in the DNA Fusion User Manual.

- Template Name - Select a template to configure the elevator.
- Description - Auto-populated by the template.
- Application Notes - Auto-populated by the template.

Elevator Objects

Elevator Parameters

- Elevator Type - Specifies the type of elevator.
 - ☐ Elevator Reader (No Feedback) - Floor selection information will not be sent to the SSP. Requires outputs to be available for each floor per cab.
 - ☐ Elevator Reader (Floor Selectors) - Floor selection information will be sent to the SSP. Requires inputs and outputs to be available for each floor per cab.
- Floor Quantity - Number of floors being controlled for this elevator. Elevator banks will require the user to configure more than one (1) elevator.

Reader

- Reader - Specifies the elevator reader's address.
 - ☐ Edit - Opens the Reader Properties dialog. See page 3-46 for more information.
- Default Mode - Defines the normal state for the elevator.
- Offline Mode - Defines the offline mode for the elevator.

Inputs and Outputs

- First Input - Address of the first input for the floor selectors. Grayed out if No Feedback is selected.
- First Relay - Address of the first relay for the elevator relays.
- Selection Delay - The amount of time a cardholder has to select a floor(s).

Floor Groups

See page 6-7 in the DNA Fusion User Manual for more information on Floor Groups.

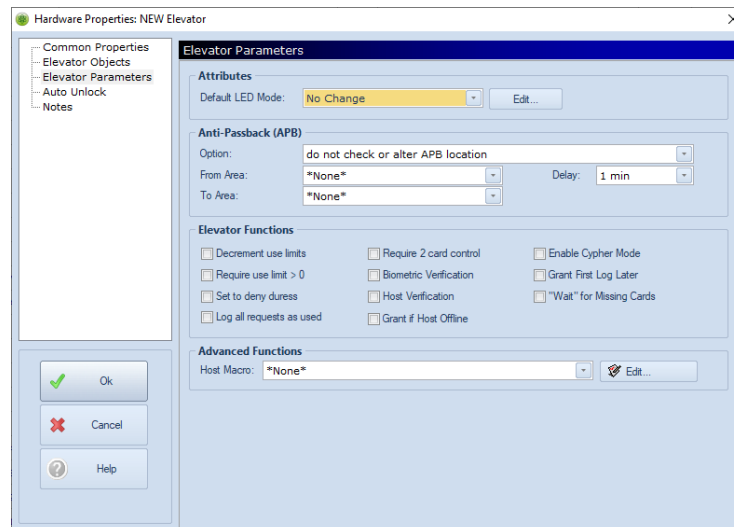
- Override Mode - Used to unlock certain floors during a selected time schedule. When the time schedule is inactive, the floors will return to their default mode.
- Facility Code Mode - Indicates which floors will be available if the elevator is set to Facility Code Mode. This may be useful when commissioning a system and access levels have not been created and assigned to cardholders.
- Off-line Mode - Specifies the floors that will be unlocked if the controller loses communication with the reader subcontroller for the elevator. The subcontroller that holds the floor selector relays must stay online for this mode to activate.

Secondary (Biometric) Reader

- Reader 2 - Drop-down list of reader addresses to select for Reader 2.
 - ☐ Edit - Opens the Reader Properties dialog for this object. See page 3-46 for more information.
- Reader Type - Drop-down list of reader types to select for Reader 2.

Technical Installation Manual

Elevator Parameters



Attributes

- Default LED Mode - Drop-down list of LED Modes to select for default.
 - ❑ Edit - Opens the LED Function Configuration dialog to configure the LED settings.

Anti-Passback (APB)

See Chapter 11 in the DNA Fusion User Manual for information on configuring Anti-Pass Back.

- Option - Drop-down field to select the type of anti-pass back.
 - ❑ Do not check or alter APB location - Anti-pass back is not in use.
 - ❑ Accept any location, change on entry - Accept any new location, change the user's location to the current reader, and generate an anti-pass back violation for an invalid entry. (Area-based Soft APB)
 - ❑ Check location, change on entry - Check user location; if a valid entry is made, change the user's location to the new location. If an invalid entry is attempted, do not grant access. (Area-based Hard APB)
 - ❑ Check this reader's last valid user - References the user's card number and will not allow access to the same card number until either a different card is presented at the reader or the APB delay expires. Requires Support Timed Anti-Pass Back to be enabled in the Controller Properties / Stored Quantities dialog. See page 3-13 for more information. (Reader-based APB using the reader's last user)
 - ❑ Check user's last ACR used, no location change - Does not allow a cardholder to present his or her card to the same reader twice in a row. Once access is granted at the reader, the user will not be granted access at the same reader again until the user presents his card at another reader in the system or until the APB delay expires. Requires Support Timed Anti-Pass Back to be enabled in the Controller Properties / Stored Quantities dialog. See page 3-13 for more information. (Reader-based APB using the cardholder's access history)
 - ❑ Check user's current location, change on entry - Similar to option #2, except that the APB delay will reset the user's area after the specified time. Requires Support Timed Anti-Pass Back be enabled in the Controller Properties / Stored Quantities dialog. See page 3-13 for more information. (Area-based APB)
- Delay - The number of minutes before APB resets. Only used in conjunction with APB options #3-5. (Max. delay = 255 minutes)
- From - The Access Area that the cardholder comes from.
- To - The Access Area that the cardholder enters.

Elevator Functions

- Decrement Use Limits - The selected elevator will decrement Use Limits associated with cards.
- Require Use Limit > Zero - If a card's Use Limit reaches 0, do not grant access.
- Set to Deny Duress - Denies access when the controller receives a duress signal at the selected elevator. (PIN & Card Mode Only)
- Log All Requests as Used - Assumes that the door was used and logs all access requests as Door Used when the request is granted. Note: Do not use with Anti-Pass Back.
- Require 2 Card Control - Requires two (2) valid access credentials to be presented for access to be granted.
- Biometric Verification - Select if biometric hardware is being supported. This is an advanced feature and should be avoided unless the operator has an understanding of the ramifications.
- Host Verification - Host verification must be obtained prior to granting access. See page 8-50 in the DNA Fusion User Manual for information on Host Response Time to set the timeout parameter. If selected, access at this elevator will be dependent on communication with the DNA server.
- Grant If Host Offline - Access will be granted if the host is offline. Works in conjunction with Host Verification.
- Enable Cypher Mode - Allows the user to enter the card number through a keypad.
- Grant First Log Later - Grants access to the elevator and then logs the event; allows instant access to the elevator. Door Used/Not Used is not logged until the elevator is actually opened or the timeout expires. Applies to Access Granted events only.
- "Wait" for Missing Cards - If an access request is denied due to the reason Card Not in File, the reader is put into the wait state and waits for a host response.

Advanced Functions

- Host Macro - Select the Host Based Macro to execute.
 - ❑ Edit - Opens the Host Based Macro (Global I/O) dialog. See page 10-13 in the DNA Fusion User Manual for more information on Host Based Macros.

Auto Unlock

The Follows Schedule feature is used to set up an elevator to adhere to a specified time schedule and designated reader modes. See page 8-16 in the DNA Fusion User Manual for more information.

- Enable - If checked, activates the fields in the Follows Schedule section.
 - ❑ Time Schedule to Follow - Select the desired Time Schedule from the drop-down list.
 - ❑ Reader Mode on Activate - Select the Reader Mode for the elevator when the specified time schedule becomes active.
 - ❑ Reader Mode on Deactivate - Select the Reader Mode for the elevator when the specified time schedule becomes inactive.



The First Person Unlock feature is not supported by elevators.

Configuring Readers

Readers can be configured as Proximity, Wiegand Insertion, or Magstripe; with or without a keypad; or as a specific reader model. The configuration in the Reader Properties dialog defines how the controller expects the data to be formatted. It also provides additional settings when configuring an OSDP reader.



Incorrectly identifying the Reader Type may cause Invalid Data errors during card reads.

To configure a reader:

1. In the Hardware Browser, **right-click** on the desired Reader under the Subcontroller object and **select** Properties.
The Reader Properties dialog opens.
2. **Populate** the appropriate fields using the Reader Properties descriptions on pages 3-46 and 3-47.
3. **Click** OK to save the settings.

Reader Properties

Common Properties

The screenshot shows the 'Hardware Properties: Reader 1.1.2.R1' dialog box with the 'Common Properties' tab selected. The left sidebar contains a tree view with 'Common Properties', 'Reader Properties', and 'Notes'. The main area contains the following fields:

- Address:**
 - Site: OO-TRNG-WX-JM2
 - Controller: 1.1: Corporate Office
 - Sub-Controller: 1.1.2: Main Entrance
 - Point/Reader #: 1 Type: Reader ACM Number: 0
- Distribution / Other:**
 - Description: ACM 2 - Reader
 - Home Page: (empty field with a browse button '...')
- Templates:**
 - Template Name: *None*
 - Description: (empty field)
 - Application Notes: (empty field)

At the bottom left are three buttons: 'Ok' (with a green checkmark), 'Cancel' (with a red X), and 'Help' (with a question mark).

Address

- Site - Site location for the selected reader. (Auto-populated)
- Controller - Controller for the selected reader. (Auto-populated)
- Sub-Controller - Subcontroller for the selected reader. (Auto-populated)
- Point/Reader # - Point or reader number. (Auto-populated)
- Type - Type of point. (Auto-populated)
- ACM Number - Identifies which ACM is associated with the reader. The number "0" indicates that the reader has not been associated with a door. (Auto-populated)

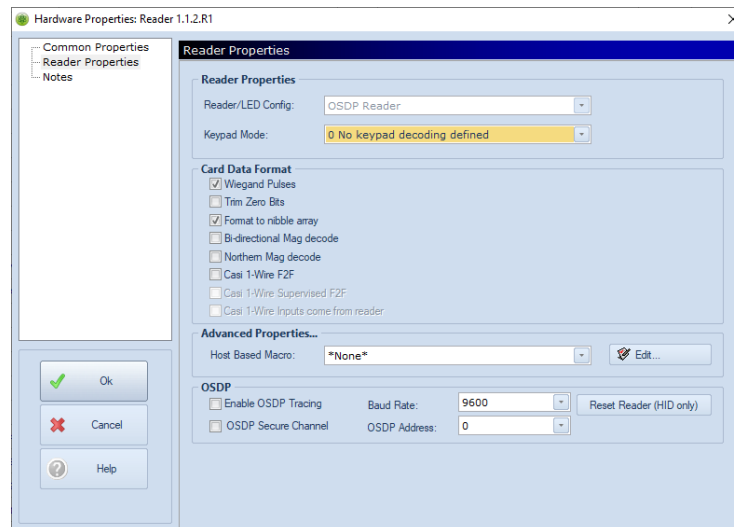
Distribution / Other

- Description - User-defined description of the reader; typically location-related.
- Home Page - Home page associated with the reader.

Templates

- Template Name - Select a template to configure the reader.
- Description - Auto-populated by the template.
- Application Notes - Auto-populated by the template.

Reader Properties



Reader Properties

- Reader/LED Config - Drop-down menu of the LED configurations.



A batch file can be used to load an LED Mode table to a reader to make the LED lights behave in a manner other than the default settings. See page 5-6 for more information on Batch Processing and using the DNA LED Control Application.

- Keypad Mode - Drop-down menu of the keypad modes.

Card Data Format

- Wiegand Pulses - Used with Proximity Readers.
- Trim Zero Bits - Used with most readers except Sensor Insertion or Dorado Readers. Trims the leading 0 bits from the card number.
- Format to nibble array - Used with Keypad Readers.
- Bi-directional Mag decode - Used with Keypad Readers.
- Northern Mag decode - Used with Keypad Readers.
- Casi 1-Wire F2F - If checked, flags the reader as using Casi F2F output format.
- Casi 1-Wire Supervised F2F - Only available if Casi 1-Wire F2F is selected; if checked, flags the reader as using Casi Supervised F2F protocol.
- Casi 1-Wire Inputs come from reader - Only available if Casi 1-Wire Supervised F2F is selected; if checked, flags the reader as using CASI inputs for the output format.

Advanced Properties

- Host Based Macro - Select a Host Based Macro to associate with this reader.
 - ❑ Edit - Opens the Host Based Macro (Global I/O) dialog. See page 10-13 in the DNA Fusion User Manual for more information.

OSDP

The OSDP section will be grayed out unless the Reader/LED Config is set to OSDP Reader.

- Enable OSDP Tracing - Used for troubleshooting; if checked, enables the operator to view log files generated from the reader.
- OSDP Secure Channel - Encrypts the communication channel between the OSDP reader and the door controller.
- Baud Rate - Drop-down list to select the baud rate for the OSDP reader.
- OSDP Address - Drop-down list to select the address for the OSDP reader.
- Reset Reader (HID Only) - Resets configured HID OSDP reader.

Technical Installation Manual

Configuring Input Points

Input Points are connections on the subcontroller that sense whether a circuit is open or closed. They monitor door switches, request-to-exit (REX) buttons, and motion detector contacts. They can also be used to monitor dry contacts from fire alarm panels, temperature, pressure alarms, and other peripherals.

1. In the Hardware Browser, **right-click** on the Input Point under the Subcontroller object and **select** Properties.

The Input Point Properties dialog opens.

2. **Populate** the appropriate fields using the Input Properties descriptions on pages 3-49 through 3-52.
3. **Click** OK to save the settings.

Input Properties

Common Properties

Address

- Site - Site location for the selected input point. (Auto-populated)
- Controller - Controller for the selected input point. (Auto-populated)
- Sub-Controller - Subcontroller for the selected input point. (Auto-populated)
- Point/Reader # - Point or reader number. (Auto-populated)
- Type - Type of point. (Auto-populated)
- ACM Number - ACM number for the reader. The number "0" indicates that the input has not been associated with a door. (Auto-populated)
- Situations... - Opens the Situation Level Manager Settings dialog for the associated point. See Chapter 9 in the DNA Fusion User Manual for more information.

Distribution / Other

- Description - User-defined description of the input point; typically location-related.
- Home Page - Home page associated with the input point.
- Do Not Load Home Page on Alarm - If the associated input point goes into alarm, the Home Page will not load.

Alarm Properties

- Alarm Setting - Type of alarm setting for the input point.
 - ☐ Global Settings - If checked, uses the system default settings.
 - ☐ Local Settings - If checked, activates the Alarm States settings on the right.

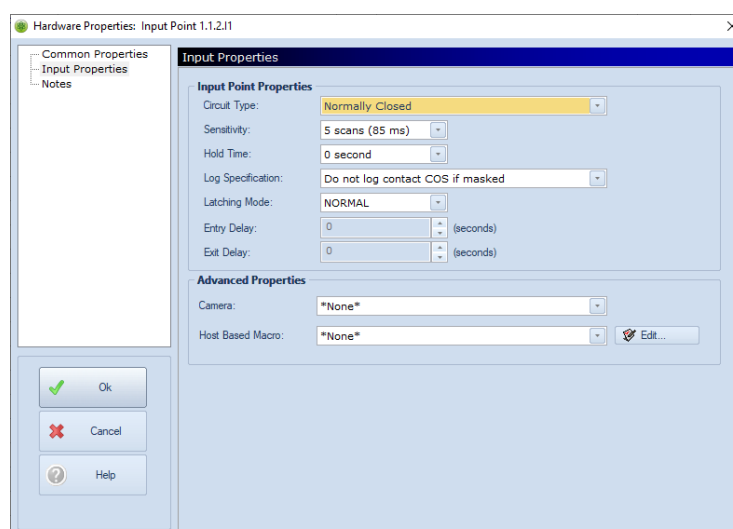
- ☐ Never an Alarm - If checked, a change in state will be reported only in the Event Log.
- Alarm States - If Local Settings was selected, check the states to report as an alarm.
 - ☐ Active - If checked, reports alarm if point is active.
 - ☐ Faults - If checked, reports alarm if point fault is reported.
 - ☐ Comm Loss - If checked, reports alarm if the subcontroller is offline.
- Alarm Priority - Selected Alarm Priority overrides the default event-specific priority set in DNA / Administrative / Events & Alarms / Logging. See page 14-25 in the DNA Fusion User Manual.
- Alarm Media File - Point-specific alarm file to be displayed when an alarm occurs.
- Alarm Text - Additional text to display with the alarm reason when the selected point goes into alarm.

Templates

Templates are covered on page 8-83 in the DNA Fusion User Manual.

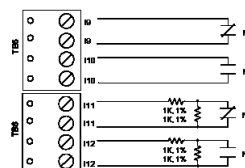
- Template Name - Select a template to configure the input point.
- Description - Auto-populated by the template.
- Application Notes - Auto-populated by the template.

Input Properties



Input Point Properties

- Circuit Type - Defines the circuit when in the normal state.
 - ☐ Normally Closed - No End of Line Termination (EOL)
 - ☐ Normally Open - No EOL
 - ☐ Normally Closed (1K Safe, 2K Alarm) - With EOL
 - ☐ Normally Open (2K Safe, 1K Alarm) - With EOL
 - ☐ Custom Table 1-4
- Sensitivity - Number of consecutive input scans before a change of state is reported. A low sensitivity setting (2) requires the system to receive two consecutive readings from an input prior to reporting a change of state. A high sensitivity setting (15) will require the input to report fifteen consecutive readings without deviation before the system will report an alarm.



Sensitivity is measured in units where each unit is reported to the SSP approximately every 17 milliseconds. Example: With a sensitivity setting of 4, the input will have to report the same status (open, close, fault, etc.) four times before a change of state will be reported.

● *Sensitivity values should never be set lower than 2 since noise and other factors may cause the system to report numerous changes in state.*

The recommended setting is 2 for REX outputs and 4-6 for standard inputs. Use higher numbers only if you are receiving noise-induced fault reports.

- Hold Time - Amount of time (in seconds) that an input will be ignored if activated, once reset. Generally used in association with a motion detector or other device capable of reporting many alarms per second. (Max. value = 15 seconds)
- Log Specification - Logging parameters specific to the point.
 - ☐ Log All Changes - Logs all change of state events.
 - ☐ Do not log contact COS (change of state) if masked - Fault-to-fault COS events will be logged but masked contact COS events will not.
 - ☐ No masked contact COS + no fault to fault COS - Masked contact COS events and fault-to-fault COS events will not be logged.
- Latching Mode - Type of latching mode. Only used when configuring entry and exit delays common with secured areas.
 - ☐ Normal - Select when no Entry or Exit Delay is used.
 - ☐ Non-Latching - Generates an alarm only if the point is still in alarm after the entry time has expired. If the door is opened and immediately closed (within the entry delay), the alarm would not be generated. An event will be generated when the change of state happens, but no alarm will be received. If selected, an Entry and Exit Delay should be set.

- ❑ Latching - The contact closure will generate an alarm unless the point is masked within the entry delay time. If the door is opened, regardless if the door is shut again, an alarm will be generated (unless the monitor point is masked). This is the recommended setting. If selected, an Entry and Exit Delay should be set.
- Entry Delay - Warning period to allow for disarming of system. If the system is not disarmed within the entry delay, an alarm will be generated. Available if Non-Latching or Latching is selected for the Latching Mode.
- Exit Delay - Amount of time to delay before removing the mask to allow for arming of the system. Once the exit delay has expired, the mask is removed and the point is considered armed. Available if Non-Latching or Latching is selected for the Latching Mode.

Advanced Features

- Camera - Drop-down list of available cameras to associate with the input point. If selected, enables the Launch Camera and Show Archived Video options in the Events and Alarm Grid context menus. Selecting a menu option will populate the camera in the Video View Manager.
- Host Based Macro - Select a Host Based Macro to associate with this reader.
 - ❑ Edit - Opens the Host Based Macro Edit (Global I/O) dialog. See page 10-13 in the DNA Fusion User Manual for more information.

Configuring Output Points

Output Points are connections on the subcontrollers that act as a switch controlled by the SSP. They are typically used to control door strikes (locks), but can also be used to control elevators, HVAC equipment, lighting, and other peripherals.

1. In the Hardware Browser, **right-click** on the Output Point under the Subcontroller object and **select** Properties.

The Output Point Properties dialog opens.

2. **Populate** the appropriate fields using the Output Properties descriptions on pages 3-53 and 3-54.
3. **Click** OK to save the settings.

Output Properties

Common Properties

The screenshot shows the 'Common Properties' dialog box for an Output Point. The title bar reads 'Hardware Properties: Output Point 1.1.2.01'. The dialog is organized into several sections:

- Address:** Includes fields for Site (Site 1: OO-TRNG-WX-JM2), Controller (1.1: Corporate Office), Sub-Controller (1.1.2: Main Entrance), Point/Reader # (1), Type (Control Point), and ACM Number (0). There is a 'Situations...' button.
- Distribution / Other:** Includes a Description field, a Home Page field with a browse button (...), and a checkbox for 'Do Not Load Home Page on Alarm'.
- Alarm Properties:** Includes 'Alarm Setting' with radio buttons for Global Settings (selected), Local Settings, and Never an Alarm; 'Alarm States' with checkboxes for Active, Faults, and Comm Loss; 'Alarm Priority' (set to 1), 'Alarm Media File' with a browse button (...), and an 'Alarm Text' field.
- Templates:** Includes a 'Template Name' dropdown menu (set to 'None'), a 'Description' field, and an 'Application Notes' field.

At the bottom left, there are three buttons: 'Ok' (with a green checkmark), 'Cancel' (with a red X), and 'Help' (with a question mark).

Address

- Site - Site location for the selected output point. (Auto-populated)
- Controller - Controller for the selected output point. (Auto-populated)
- Sub-Controller - Subcontroller for the selected output point. (Auto-populated)
- Point/Reader # - Point or reader number. (Auto-populated)
- Type - Type of point. (Auto-populated)
- ACM Number - ACM number for the reader. The number "0" indicates that the output has not been associated with a door. (Auto-populated)
- Situations... - Opens the Situation Level Manager Settings dialog for the associated point. See Chapter 9 in the DNA Fusion User Manual for more information.

Distribution / Other

- Description - User-defined description of the output point; typically location-related.
- Home Page - Home page associated with the output point.
- Do Not Load Home Page on Alarm - If the associated point goes into alarm, the Home Page will not load.

Alarm Properties

- Alarm Setting - Type of alarm setting for the output point.
 - ☐ Global Settings - If checked, uses the system default settings.
 - ☐ Local Settings - If checked, activates the Alarm States settings on the right.

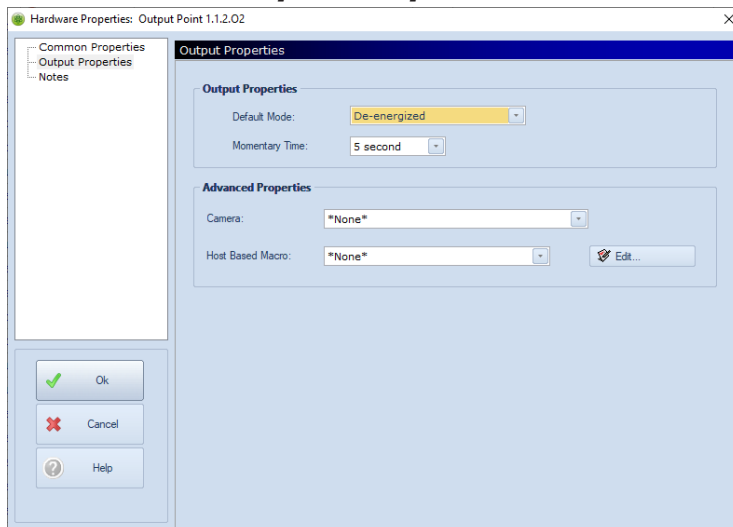
- ☐ Never an Alarm - If checked, a change in state will be reported only in the Event Log.
- Alarm States - If Local Settings was selected, check the states to report as an alarm.
 - ☐ Active - If checked, reports alarm if point is active.
 - ☐ Faults - If checked, reports alarm if point fault is reported.
 - ☐ Comm Loss - If checked, reports alarm if the subcontroller is offline.
- Alarm Priority - Selected Alarm Priority overrides the default event-specific priority set in DNA / Administrative / Events & Alarms / Logging. See page 14-25 in the DNA Fusion User Manual.
- Alarm Media File - Point-specific alarm file to be displayed when an alarm occurs.
- Alarm Text - Additional text to display with the alarm reason when the selected point goes into alarm.

Templates

Templates are covered on page 8-83 in the DNA Fusion User Manual.

- Template Name - Select a template to configure the output point.
- Description - Auto-populated by the template.
- Application Notes - Auto-populated by the template.

Output Properties



Output Properties

- Default Mode - Specify if the relay coil is Energized or De-energized in the normal state.
- Momentary Time - Amount of time that the relay will activate when given a momentary command. Check local code. (Max. = 255 seconds)

Advanced Properties

- Host Based Macro - Select a Host Based Macro to associate with the output point.
 - ☐ Edit - Opens the Host Based Macro (Global I/O) dialog. See page 10-13 in the DNA Fusion User Manual for more information.

Adding NVR/DVRs

NVR/DVR integration provides a seamless interface between DNA Fusion and the network/digital video recorder. The integration allows users to view live or recorded video on the network, providing quick access to video from alarms generated in the system. The NVR/DVR integration is a licensed feature.

For information on managing NVR/DVRs, see Chapter 8 in the DNA Fusion User Manual.

The following NVR/DVRs are compatible with the DNA Fusion system:

- 3xLogic
- Milestone
- Salient
- March Networks
- Bosch Video
- OnSSI
- Video Insight
- ACTi
- Verint
- Exacq Vision
- Instek
- HIK Central

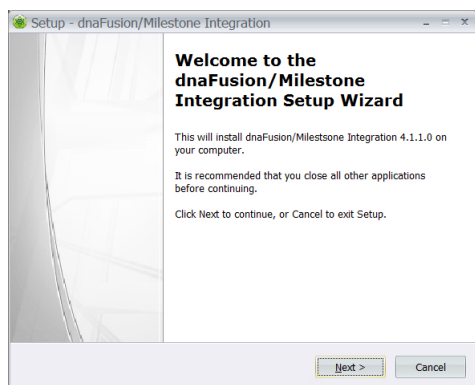
Integrating the NVR/DVR is a three-step process:

1. **Run** the NVR/DVR Integration installation.
2. **Configure** the NVR/DVR within the DNA Fusion system.
3. **Add** the camera(s) to the DNA Fusion system. For a more detailed integration process, follow the steps below.

Installing the NVR/DVR Integration

1. **Obtain** the correct NVR/DVR Integration installation from Open Options and extract the files to a common location.
2. **Open** the folder and **double-click** the .exe for the NVR/DVR Integration.
The Open File - Security Warning dialog appears.

3. **Click** Run to start the installation process.
The Integration Setup Wizard dialog opens.



Before installing the DVR Integration, Open Options recommends backing up the DNA Fusion database as well as closing all open programs. See page 20-7 in the DNA Fusion User Manual for more information.

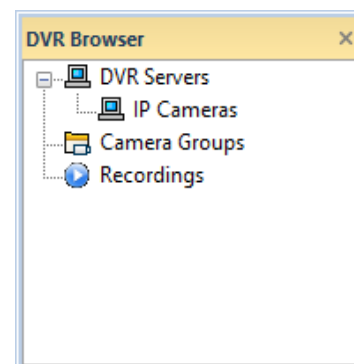
4. **Click** Next to continue the installation.
The File Location screen appears.
5. **Click** the Install button to start the installation.
The installation begins.
6. When the installation is complete, **click** Finish to complete the setup.

Configuring the NVR/DVR

1. **Open** DNA Fusion and **select** the DVR Manager icon from the Standard Toolbar.
Or
Select View / Explorers / DNA DVR from the Main Menu.
The DVR Browser opens.



2. **Right-click** on the DVR Servers object and **select** Add DVR Server.
The DVR Server dialog opens.



The DNAFusion-DVR Server dialog box contains the following fields and controls:

- DVR Type:** A drop-down menu currently showing "MileStone XProtect Enterprise".
- Description:** A text input field.
- Address:** A text input field.
- Authentication:** A drop-down menu currently showing "Basic".
- Pass Phrase:** A text input field.
- User Name:** A text input field.
- Password:** A text input field.
- Server GMT:** A drop-down menu currently showing "(UTC-06:00) Central Time (US & Canada)".
- Buttons:** "Ok" (with a green checkmark icon) and "Cancel" (with a red X icon).

3. **Select** the DVR Type from the drop-down list.

The DNAFusion-DVR Server dialog box is shown with the "DVR Type" dropdown menu open. The list of options includes:

- MileStone XProtect Enterprise (highlighted)
- MileStone XProtect Corporate/Expert
- MileStone XProtect Enterprise
- OnSSI Ocularis
- Salient
- Video Insight

4. **Enter** a Description for the DVR Server.
5. **Enter** the server's IP address in the IP Address field.
6. **Enter** the User Name and Password for the DVR.
7. **Select** the Authentication mode from the drop-down list.
The selection must match the Authentication mode setting on the DVR Server.



*For Milestone Enterprise systems, **select** Basic Authentication. For Milestone Corporate systems, **select** Windows Authentication.*

8. **Select** the Server GMT Offset from the drop-down list.
The Server Time appears below the drop-down.
9. **Click** OK to save the settings and add the DVR.
The DVR Server appears in the DVR Browser.

Adding the Cameras

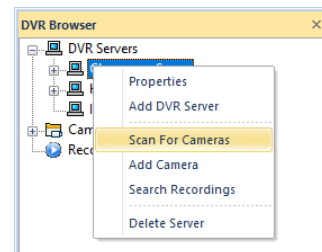
1. In the Hardware Browser, **right-click** on the desired DVR Server and **select** Scan for Cameras. A plus sign appears by the server and the cameras are automatically added to the system. Click the plus sign to expand the server and reveal the cameras.

For integrations that don't support scan for cameras:

If the integration does not support the Scan for Cameras capability, the cameras must be added manually:

- a. **Right-click** on the DVR Server and **select** Add Camera.

The DVR Camera dialog opens.



- b. **Enter** a Description for the camera and **configure** the remaining properties. See page 8-79 in the DNA Fusion User Manual for more information.
- c. **Click** the OK button to save the camera.
- d. **Repeat** until all required cameras have been added.

For IP camera integrations:

IP cameras allow the operator to monitor the camera from the system. See page 8-80 in the DNA Fusion User Manual for more information.

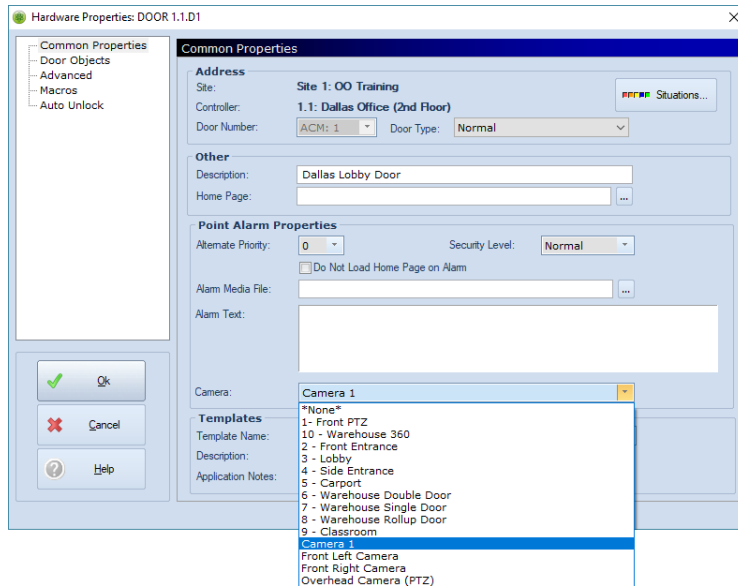
- a. **Right-click** on the IP Camera object and **select** Add Camera.

The IP Camera dialog opens.


- b. **Enter** a Description for the camera.
- c. **Enter** the URL or IP Address where the camera is located.
- d. **Click** the OK button to save the camera.
- e. **Repeat** until all required cameras have been added.

Associating a DVR Camera with a Door

1. In the Hardware Browser, **right-click** on the Door object and **select** Properties.
The Door Properties dialog opens.
2. In the Point Alarm Properties section, **select** the Camera from the drop-down list.



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

A camera icon  will appear next to events to notify the user that a camera is associated with the hardware object in the event. See page 14-7 in the DNA Fusion User Manual for more information on recalling archived video from the Events Grid. A Host Based Macro can also be created to automatically open the Video View Manager when a particular event occurs.



Card Formats

The Card Format dialog defines a format for the controller to take the raw card data and format it into fields for access request processing. Multiple formats allow the use of badges with different facility codes and/or data lengths.

DNA Fusion also offers Corporate Mode which uses the Facility Code and Card Number along with an offset number to create a unique credential number. The Multiple Facility Code mode can also be used. See page 3-61 and 3-62 for more information.

Configuring Card Formats

1. In the Hardware Browser, **double-click** on the Controller object

OR

Right-click on the Controller object and **select** Properties.

2. **Select** Cards and Dual Comm from the dialog menu.

The Cards and Dual Comm dialog appears.

3. **Click** the Edit Card Formats button.

The Card Formats Dialog opens.

4. **Select** an option: New, Copy, or Edit.
Use the instructions below to complete the process.

Creating a New Card Format

1. **Click** the New button.
2. **Enter** a Description for the new card format.
3. **Enter** the Facility Code.
4. **Select** the Card Format from the drop-down list.
5. **Enter** the desired values in the Card Format fields.
6. **Click** the Save button to save the configuration.
The new format is added to the Description drop-down.

Copying a Card Format

1. **Select** the Card Format from the Description drop-down and **click** the Copy button.
2. **Change** the name in the Description field.
3. **Enter** the correct Facility Code and/or change any desired values.
4. **Click** the Save button to save the configuration.
The new format is added to the Description drop-down.

Editing a Card Format

1. **Click** the Edit button.
2. **Edit** the desired values in the Card Format fields.
3. **Click** the Save button to save the changes.

Gathering Card Format Information

DNA Fusion allows the operator to easily identify the bit format and the facility code for an access credential.

1. **Present** the card to a reader.
2. **Open** the Events Grid and look at the Event Data for the Access Denied: Invalid Card Format event to determine the bit format.

Events										
ID	Event Time	Panel Time	Address	Description	Index	Event Description	Card #	First Name	Last Name	Event Data
1	04/22/14 13:54:46	04/22/14 13:54:46	1.4 D2	Kelsey Center Training Room Door (315)	50	Access Denied: Invalid Card Format	0			26 bits: 0186003d

3. **Assign** the generic card format that contains the same bit structure as the card to the controller.
See Assigning a Card Format to the SSP instructions below.
In the example above, the operator would **select** the HID 26 BIT With FC.
4. **Present** the same card to the reader a second time.
5. **Check** the Event Data for the Access Denied: Facility Code event to determine the Facility Code (FC).

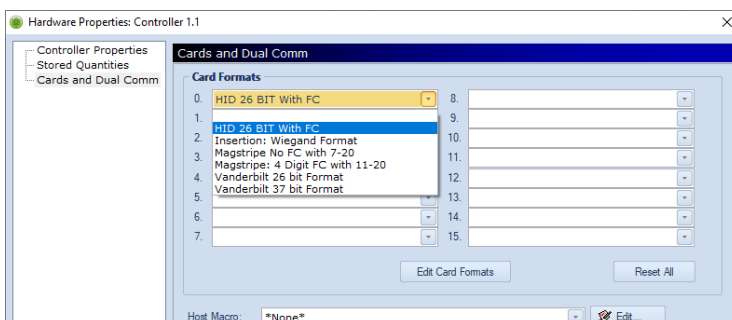
Events										
ID	Event Time	Panel Time	Address	Description	Index	Event Description	Card #	First Name	Last Name	Event Data
2	04/22/14 14:01:01	04/22/14 14:01:01	1.4 TS12	ICU Paddle (10a-2p & 5p-8p M-Sun w/H)	223	Became Inactive	0			
3	04/22/14 14:00:05	04/22/14 14:00:05	1.4 D2	Kelsey Center Training Room Door (315)	53	Access Denied: Facility Code	5003	???	???	Fmt: 0, FC: 75 Issue: -1

6. **Create** the card format by following the instructions on page 3-59 for Copying a Card Format.
7. **Assign** the newly created card format to the controller.
See Assigning a Card Format below.
Overwrite or delete the generic card format added in step 3.
8. **Download** the changes to the controller.

Assigning a Card Format to the SSP

Up to eight card formats (0-15) may be active simultaneously for each SSP controller. Multiple card formats allow the operator to use facility codes or different data lengths, as is frequently encountered in large corporate systems.

1. **Right-click** on the Controller in the Hardware Browser.
2. **Select** Properties from the context menu.
The Controller Properties dialog opens.
3. **Select** Cards and Dual Comm from the dialog menu.



4. **Select** the desired formats (0-15) from the Card Formats drop-down fields.
5. **Click** OK to save the formats to the controller.

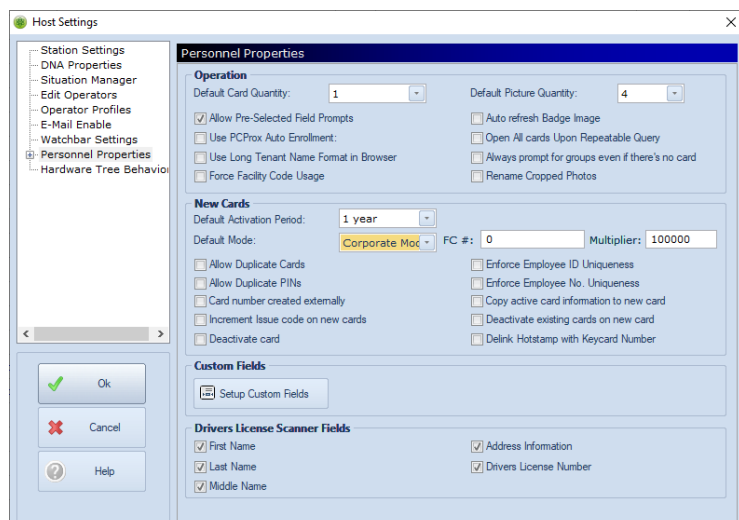
Corporate Mode Card Format

The Corporate Mode uses the Facility Code and Card Number along with an defined offset number to create a unique credential number. The Corporate Mode option allows the system to have as many facility codes as needed with only one card format (per bit structure).

When you set up a card format for the Corporate Mode ensure that the Card ID Offset matches the multiplier set up in Personnel Properties.

1. **Click** the DNA Properties button in the Standard Toolbar and **select** Personnel Properties from the dialog menu.

The Host Settings / Personnel Properties dialog appears.



2. In the New Cards section, **select** the Corporate Mode from the Default Mode drop-down.

The FC # and Multiplier fields appear.

Once the Default Mode is set to Corporate Mode, the workstation's new cards will populate with the configured Facility Code and will use the Multiplier to create a unique Credential.

3. **Enter** the Facility Code and, if needed, **change** the Multiplier (defaults to 100,000) for the system.

The Multiplier determines the digits needed to calculate the card number.

4. **Click** OK to save the settings.

5. **Create** a Card Format for the desired bit structure.

See page 3-59 for more information.

6. **Verify** that the Card ID Offset matches the Multiplier set in step 1.

7. **Set** the Card Flags value and **click** the Save button.

6 = Ignores the Facility Code. Will work for all facility codes formats. (Recommended)

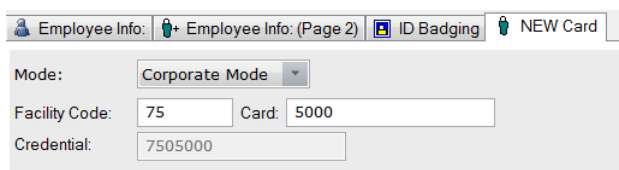
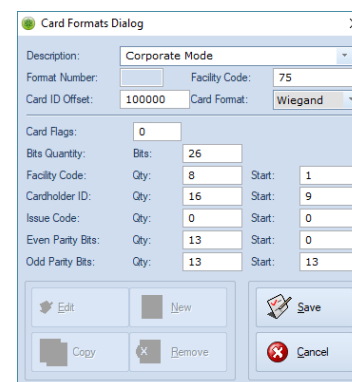
4 = Requires a Card Format per facility code; useful in some situations.

8. **Click** Close to close the dialog.

9. In the Controller Properties / Cards and Dual Comm dialog, **select** the new Card Format from the drop-down list and **click** OK.

10. **Add** a new cardholder.

When a new card is added to the Cardholder's Record, the Mode field in the Card Tab will default to Corporate Mode.

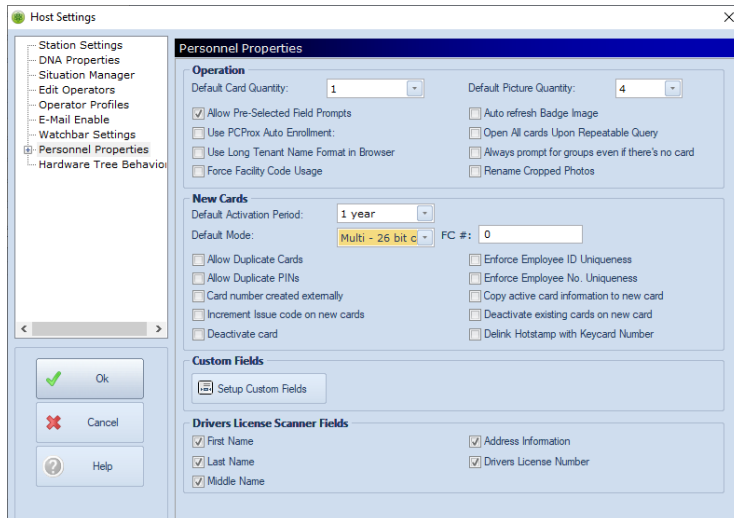


Multiple Facility Code Card Formats

Although there is a maximum of sixteen (16) card formats for each controller, the Multiple Facility Code option can be used to convert one or more of the card's facility codes to a unique card number.

1. **Click** the DNA Properties button in the Standard Toolbar and **select** Personnel Properties from the dialog menu.

The Host Settings / Personnel Properties dialog appears.



2. **Select** the desired Multi - XX Bit Card option from the Default Mode drop-down.

The FC # field appears.

If the Default Mode is set to Multi, the workstation's new cards will populate with the configured Facility Code and will use it along with the Card Number to create a unique Credential.

3. **Enter** the Facility Code and **click** OK to save the settings.

4. **Create** a Card Format for the desired bit structure.

See page 3-59 for more information.

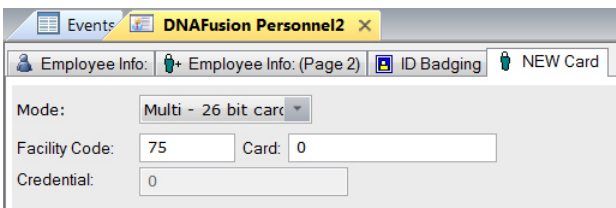
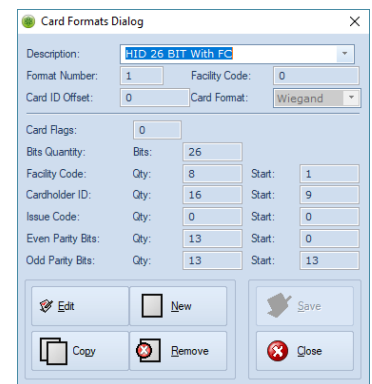
5. **Click** the Save button to save the configuration.

6. **Click** Close to close the dialog.

7. In the Controller Properties / Cards and Dual Comm dialog, **select** the new Card Format from the drop-down list and **click** OK.

8. **Add** a new cardholder.

When a new card is added to the Cardholder's Record, the Mode field in the Card Tab will default to the Multi - XX Bit Card mode set in the Personnel Properties dialog.



Upgrading DNA 4

In This Chapter

- ✓ Server Upgrades
- ✓ Client Upgrades
- ✓ License Updates

DNA Fusion operators can perform two types of upgrades: software upgrades and license updates. This chapter discusses both types.

Software Upgrades

DNA Fusion software upgrades do not require additional licenses; however, the Site must be under a current Software Maintenance Agreement in order to perform the upgrade.

Upgrading to version 7.0 or later requires the appropriate license(s) for any additional integrations.

Depending on which version of DNA Fusion the site is running prior to the upgrade, follow the applicable instructions below.

DNA Fusion Full Upgrade

When a version of DNA Fusion is released, only the DNA Server needs to be updated. All client workstations will check the Server for updates upon startup and will automatically synchronize with the server to ensure that the latest version is running across the entire system.

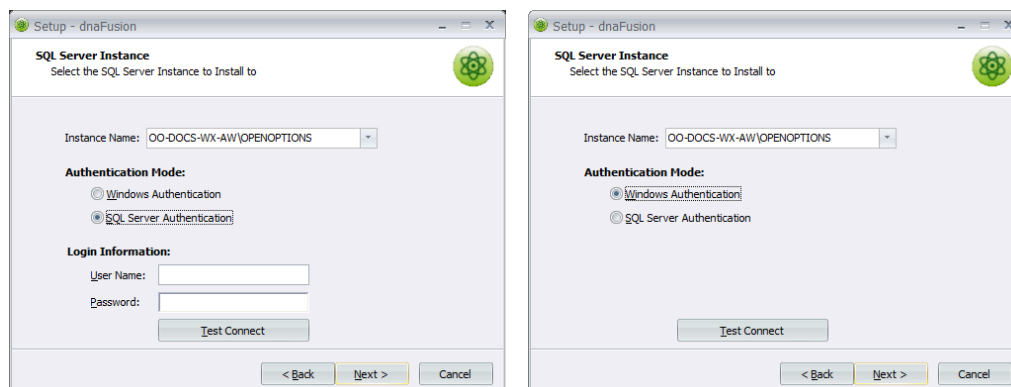
1. **Close** the DNA Fusion application.
2. **Backup** the DNA Fusion (or NPowerDNA) database.
3. **Download** the full version of DNA Fusion through the link included in the License e-mail or from the Open Options website.

The installation process starts automatically.

If the Service Pack is run, the option to Enable Client Push will not be available.

4. **Read** the License Agreement, **select** the I Accept the Agreement radio button, and **click** Next to continue.
5. **Verify** the User Information and **click** Next.

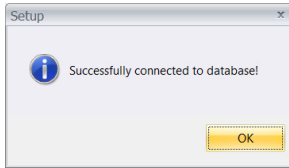
The SQL Server Instance screen appears.



6. **Verify** the Instance Name (or enter the IP address of the server), **select** the Authentication Mode, and, if needed, **enter** the Login Information.

7. **Click** the Test Connection button.

If the information is correct, a Successfully Connected dialog will appear. **Click** OK to continue.

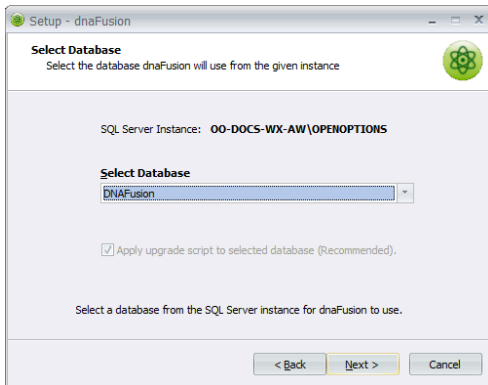


If the Instance Name is not correct, a Connection Failed dialog will appear. **Click** OK and **select** the correct Instance Name from the drop-down or **enter** the IP Address of the server.

8. **Click** Next.

The Select Database screen appears.

9. **Select** DNAFusion from the Select Database drop-down and **click** the Next button to continue.



The Select Additional Tasks dialog appears.

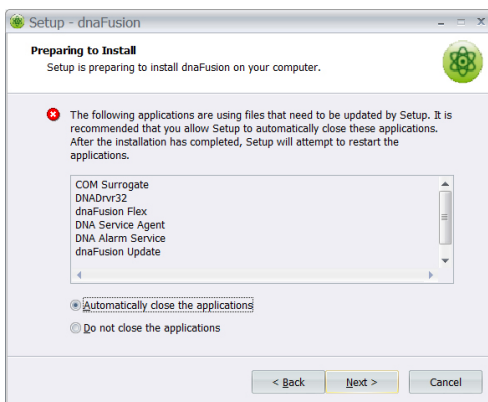
10. If desired, **check** Create a Desktop Icon to add a shortcut icon the computer's desktop.
11. If desired, **check** Create Firewall Exclusions to set the firewall exclusions for Microsoft Windows Firewall. Other software security packages may require further configuration. See page 2-19 for more information on ports used by DNA Fusion.

The Ready to Install screen appears with a summary of the installation.

12. **Click** the Install button to start the installation.

The upgrade process begins.

If any DNA-related applications or services are in use, a dialog will appear prompting the operator to close the applications.



13. **Click** Finish to complete the Server Upgrade.

Fusion Client Upgrades

After the DNA Fusion server is upgraded, the client workstations will check for updates upon startup and will automatically synchronize with the server to ensure that the newest version is running across the entire DNA Fusion system.



If the DNA system is being upgraded from NPower DNA to DNA Fusion, the upgrade will need to be performed at the server as well as at each client workstation. See page 4-4.

1. **Log in** to Windows with an Administrator or Local Administrator account.
If the Windows user does not have rights to install the software, DNA Fusion will not update.
2. **Launch** the DNA Fusion application.
The dnaLauncher dialog opens. The upgrade process will continue automatically.
If the update fails to install, run the upgrade from the DNA Fusion Installation file. See page 2-17 for information on client installations.
3. **Log in** to DNA Fusion.
The Client Upgrade is complete.

Fusion Service Pack

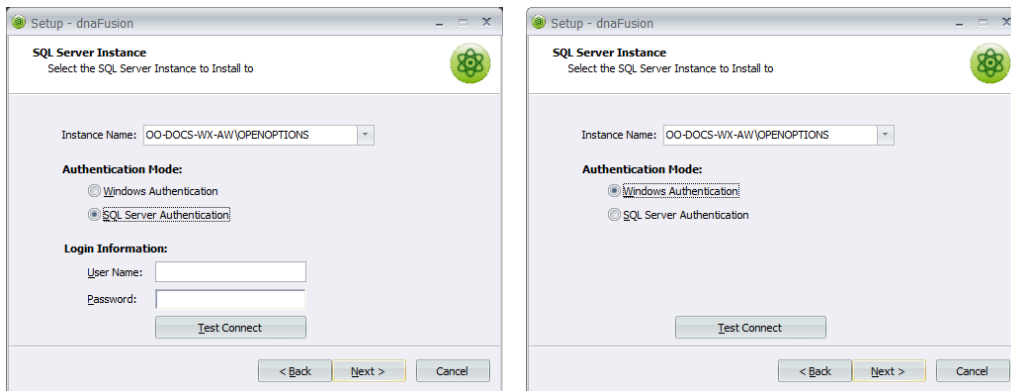
Service packs can be used to update the DNA Fusion Server only. The service pack does NOT automatically synchronize the clients' DNA Fusion application with the server.

1. **Close** DNA Fusion.
2. **Backup** the DNAFusion (or NPower DNA) database.
3. **Download** DNA Fusion through the link included in the License e-mail or from the Open Options website.
The installation process starts automatically.
4. **Read** the License Agreement, **select** the I Accept the Agreement radio button, and **click** Next to continue.
5. **Verify** the User Information and **click** Next.
The SQL Server Instance screen appears.
6. **Verify** the Instance Name (or enter the IP address of the server), **select** the Authentication Mode, and, if needed, **enter** the Login Information.
7. **Click** the Test Connection button.
If the information is correct, a Successfully Connected dialog will appear. **Click** OK to continue.
If the Instance Name is not correct, a Connection Failed dialog will appear. **Click** OK and **select** the correct Instance Name from the drop-down or **enter** the IP Address of the server.
8. **Click** Next, **verify** the Select Database field is set to DNAFusion, and **click** the Next button to continue the installation.
The Select Additional Tasks screen appears.
9. If desired, **check** Create a Desktop Icon to add a shortcut icon the computer's desktop.
10. If desired, **check** Create Firewall Exclusions to set the firewall exclusions for Microsoft Windows Firewall.
Other software security packages may require further configuration. See page 2-19 for more information on ports used by DNA Fusion.
The Ready to Install screen appears with a summary of the installation.
11. **Click** the Install button to start the installation.
The upgrade process begins.
If any DNA-related applications or services are in use, a dialog will appear prompting the operator to close the applications.
12. **Click** Finish to complete the Server Upgrade.

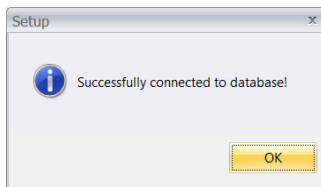
NPower DNA to DNA Fusion 5.0 and above

When upgrading from NPower DNA to DNA Fusion, the upgrade must be performed at the server prior to upgrading the client workstation(s).

1. **Close** NPowerDNA.
2. **Backup** the NPowerDNA database.
3. In the File Explorer, **locate** and **double-click** on the upgrade executable (.exe) file.
The License Agreement screen appears.
4. **Read** the License Agreement, **select** the I Accept the Agreement radio button, and **click** Next to continue.
5. **Verify** the User Information and **click** Next.
The SQL Server Instance screen appears.



6. **Verify** the Instance Name (or enter the IP address of the server), **select** the Authentication Mode, and, if needed, **enter** the Login Information.
7. **Click** the Test Connection button.
If the information is correct, a Successfully Connected dialog will appear. **Click** OK and continue.



If the Instance Name is not correct, a Connection Failed dialog will appear. **Click** OK and **select** the correct Instance Name from the drop-down or **enter** the IP Address of the server.

8. **Click** Next, **verify** the Database Selection and **click** the Next button to continue the installation.
9. **Follow** the resulting Install Wizard.
10. **Review** the Ready to Install dialog.
11. **Click** Install.
The upgrade process begins.
12. **Click** Finish to complete the Server Upgrade.
13. If needed, **update** the client workstation(s).

License Updates

Changes or additions to a DNA Fusion system's configuration may require additional licensing depending on the type of additions to the system. The process below is for DNA Fusion version 5.2 and above.

Older versions may require additional steps that are outlined in the License Update e-mail.

Three (3) licensing methods are currently available for DNA Fusion:

- Soft Key - The Soft Key licensing information was entered during the initial installation or when the system was converted from a HASP Key to a Soft Key. An internet connection is required for automatic updates.
- HASP Key - HASP Key licensing requires a free USB port on the DNA Fusion Server running the DNA Driver. An internet connection is required for automatic updates.
- License File - If an Internet connection is not available, Open Options Technical Support will provide a file that contains the updated Licensing information for the Site.

The following items require additional licensing from Open Options, LLC.:

- Client Workstations
- Universal Driver
- Sub-Controllers
- Photo Badging
- Active Directory Operator Plug-In
- Fusion Web
- Fusion Mobile
- OpenDX
- NVR/DVR Integrations
- PIM Door Integrations
- ASSA Door Integrations
- Aperio Door Integrations
- Salto Door Integrations
- Honeywell Integrations
- CASI/M5 Bridge Integrations
- Drivers for Alarm Panels & CCTV

To update a license:

1. **Determine** the updated Licensing requirement.
 - Soft Key: If the system is using a Soft Key and has an Internet connection, the updated licensing information will be automatically downloaded from the Open Options Licensing Server. If an Internet connection is not available, Open Options will provide a License File.
 - HASP Key: If the system is using a HASP Key and has an Internet connection, the updated licensing information will be automatically downloaded from the Open Options Licensing Server. If an Internet connection is not available, Open Options will provide a License File.
 - License File: Install the updated License File provided by Open Options. Contact Open Options Order Entry Department with the Soft Key ID prior to the upgrade date.



The Soft Key ID is located in the Help / About DNA dialog.

This Page Intentionally Left Blank

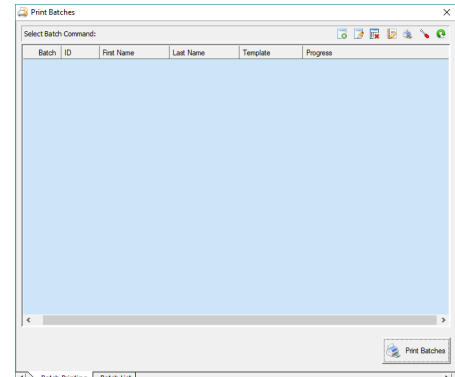
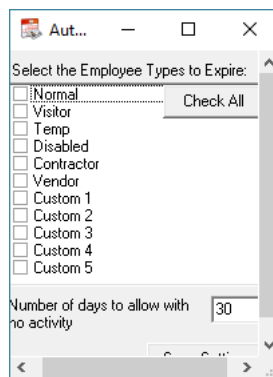
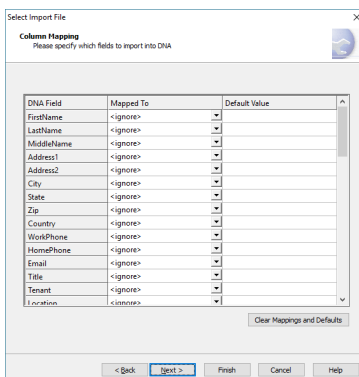
Additional Apps 5

In This Chapter

- ✓ Controller Connection Utility
- ✓ Table Purger Tool
- ✓ DNA Batch Download Settings Utility
- ✓ DNA LED Control Application
- ✓ Auto Expire Tool
- ✓ Event History Report Utility
- ✓ Time & Attendance Report
- ✓ DNA Import Tool
- ✓ Batch Printer
- ✓ DNA Diagnostics

This chapter covers the following DNA Fusion support tools:

- Controller Connection Utility - Opens an interface to disable controllers that are not network ready.
- Table Purger Tool - Deletes certain information from specific tables in the DNA Fusion (or NPowerDNA) database.
- DNA Batch Download Settings Utility - Allows batch files to automatically download to the desired controller. For instance, a batch file might load an LED Mode table.
- DNA LED Control Application - Allows the operator to customize the LED Mode of a door.
- Auto Expire Tool - Deactivates cards that do not have any usage history within the specified timeframe.
- Event History Report Utility - Generates custom Event History reports without the need for a DNA client.
- Time & Attendance Report - Generates a report that captures In and Out information about Time and Attendance cards.
- DNA Import Tool - Allows the operator to import personnel and card data from an exported CSV file (.csv) to the DNA Fusion database.
- Batch Printer - Allows the operator to print batches of cards based on specific criteria, such as Personnel Groups, Personnel or Card Type, Card Expiration, or Custom Fields.
- DNA Diagnostics - Allows the operator to submit diagnostic log files to Open Options, such as COM objects, services, database tables, installation and license information, etc.



This Page Intentionally Left Blank

Controller Connection Utility

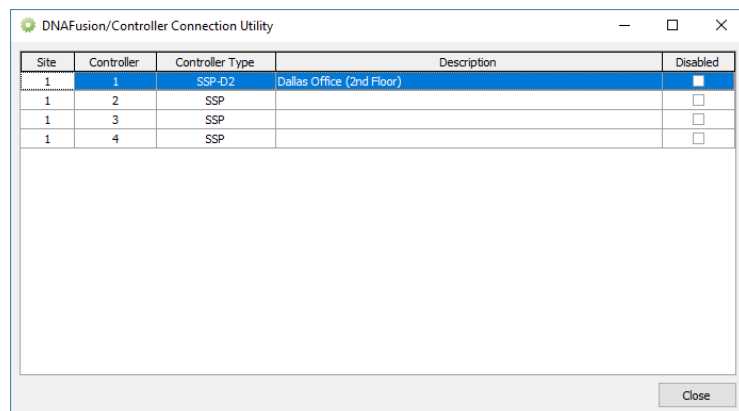
The Controller Connection Utility can be used to disable controllers and add them to DNA Fusion before they are network ready. This utility will stop the DNA Driver (DNAdrv32) from attempting to connect to the Controllers until they are configured.

The utility can also be used to reconnect the controllers to the driver once they are network ready. Contact Open Options Technical Support or visit the Open Options website to obtain the Controller Connection Utility.

To Disable the Controllers:

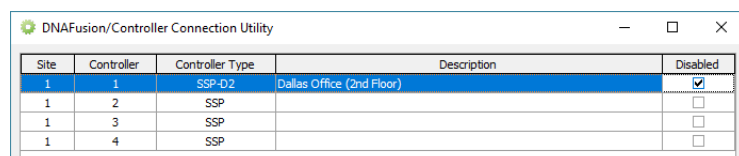
1. **Run** the DCUtil application.

The DNAFusion/Controller Connection Utility dialog opens.



2. **Check** the Disabled box(es) next to the desired controller(s).

If disabled, the DNA driver (DNAdrv32) will not attempt to automatically connect to the controller(s).

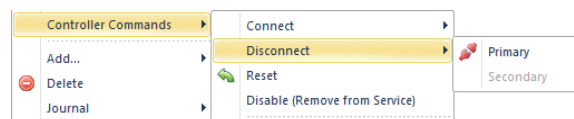


3. **Click** the Close button to save the changes.

Changes will also be saved when the operator selects a different row.

4. **Launch** DNA Fusion.

5. In the Hardware Browser, **right-click** on the disabled controller and **select** the Controller Commands / Disconnect / Primary option.



To Enable the Controllers:

1. **Run** the DCUtil application.

The DNAFusion/Controller Connection Utility dialog opens.

2. **Uncheck** the Disabled box(es) next to the desired controller(s).

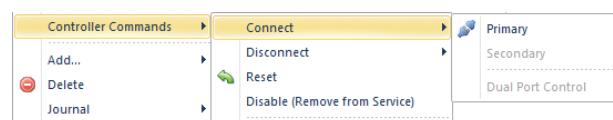
3. **Click** the Close button to save the changes.

The DNA Driver will automatically connect to the controller(s) again.

Changes will also be saved when the operator selects a different row.

4. **Launch** DNA Fusion.

5. In the Hardware Browser, **right-click** on the controller and **select** the Controller Commands / Connect / Primary option.



[illegible]

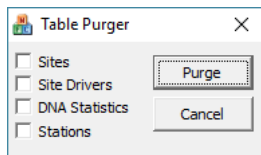
Table Purger Tool

The Table Purger application is an executable file (.exe) that resets key tables from the DNA Fusion (or NPowerDNA) database. It can be downloaded from the Open Options website.

To run the Table Purger:

1. **Close** the DNA Fusion Server and all DNA Fusion Clients.
2. **Double-click** the TablePurger.exe file.

The Table Purger dialog opens.



3. **Check** the desired option(s).
 - Sites - Purges the table that contains a record for every station/site combination.
 - Site Drivers - Removes information from the table that contains a record for each unique site in the system.
 - DNA Statistics - Removes the information from the table that is primarily used for licensing purposes, including client, badging and subcontroller licenses. There is also a record for each site as well as for each station.
 - Stations - Deletes the Unique Name and Station Number information for all DNA Fusion workstations from the database.
4. **Click** the Purge button.

The selected information will be removed from the SQL tables.



The purge is immediate; a confirmation message will NOT be displayed.

5. **Open** DNA Fusion on the Server, **verify** the Station Name and Number, and **click** OK.
The Station Name should be your computer name.
If the Site and Site Driver information was purged, the Hardware Browser will be empty.
6. **Log in** to the DNA Fusion Server.
If the station information was purged, the Station Configuration dialog will appear. See page 2-12 for more information.
7. **Right-click** in the Hardware Browser and **select** Link Station to Site.
8. **Repeat** steps 5 through 7 for all client workstations.

DNA Batch Download Settings Utility

The Batch Download Settings Utility provides the ability to automatically download a batch file to a specific controller. This allows the driver to load the designated batch file at startup and send it to the controller.

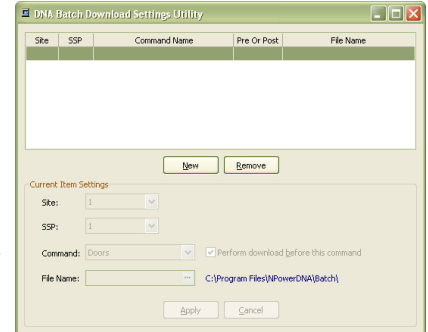


The DNA Batch Download Settings Utility is only for use with legacy software (NPowerDNA). Operators can perform batch processing manually in DNA Fusion. See page 20-14 in the DNA Fusion User Manual for more information.

1. **Locate** the DNABatchDownloadSettings.exe file and **double-click** on the icon to open the application.

Default location: C:\Program Files\NPowerDNA\Tools

The DNA Batch Download Settings Utility dialog opens.



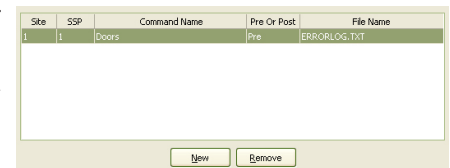
2. **Click** the New button to add a new command line.
3. **Select** the Site and SSP Number from the drop-down lists.
4. From the Command drop-down, **select** the desired Command Type for the batch file.

5. If desired, **uncheck** the Download Before this Command box.

If unchecked, the file will be downloaded prior to the DNA system downloading to the controller.

6. **Click** the Browse button next to the File Name field to select the text command file that will be downloaded.

The file must reside in the following location: C:\Program Files\NPowerDNA\Batch.



7. Once the parameters are configured, **click** Apply to add the file.

The command appears in the main window.

If desired, **double-click** the Command to edit the data or **select** the Command and **click** Remove to delete the command.

DNA LED Control Application

The DNA LED Control Application allows the operator to customize the LED Mode tables for a door.

1. **Locate** the dnaLedControl.exe file and **double-click** on the icon to open the application.

The default location is C:\Program Files\DNAFusion\Tools for 32-bit OS or C:\Program Files (x86)\DNAFusion\Tools for 64-bit OS.

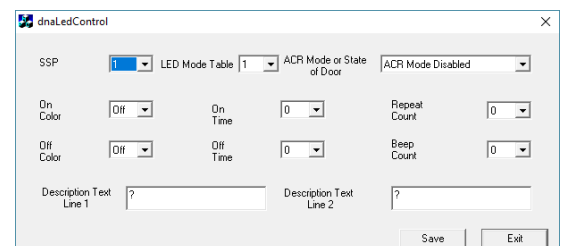
The dnaLedControl dialog opens.

2. **Select** the desired SSP number from the drop-down list.
3. **Select** the LED Mode Table to edit.

Doors have three (3) LED Modes; the LED Mode is specified in the Door Objects dialog. See page 3-27 for more information.

- 1 = Short Red Pulse
- 2 = Solid Red Short Pulse
- 3 = Solid Green Short Pulse

This setting determines which table will be edited.



4. **Select** the ACR Mode or State of Door from the drop-down list.

5. **Configure** the selected mode by **selecting** the On Color, On Time, Off Color, Off Time, Repeat Count, and Beep Count from the drop-down lists.

6. **Click** the Save button when finished.

The file is saved to C:\Program Files\DNAFusion\Batch for 32-bit OS or C:\Program Files (x86)\DNAFusion\Batch for 64-bit OS.

7. **Repeat** steps 3 through 6 until all desired states or modes are programmed.

DNA AutoExpire Tool

The AutoExpire Tool deactivates cards that do not have any usage history within a specified number of days. It has two operation modes: Configuration and Silent.

- Configuration Mode - Opens the AutoExpire dialog and allows the operator to select an Employee Type and specify a number of inactive days.
- Silent Mode - Marks cards as inactive if the card matches the selected Employee Type and has not been used in the identified amount of time.

Running the Configuration Mode

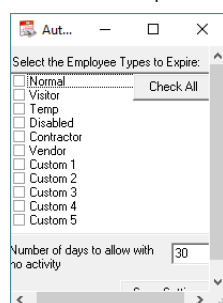
The AutoExpire Tool can be run on the DNA server or any DNA client.



The AutoExpire Tool requires NPowerDNA version 3.5 and higher or DNA Fusion to run.

1. **Double-click** the AutoExpire.exe icon to open the AutoExpire dialog.

The AutoExpire dialog opens.



2. **Select** the Employee Type to expire.

If the cardholder's Employee Type in DNA Fusion matches the selected Employee Type, the card will be eligible for deactivation.

3. **Enter** the Number of Days to Allow With No Activity.

If a card has not been used within the specified amount of time, the card will be eligible for deactivation.

4. **Click** the Save Settings button to save the changes.

When the application is run in Silent Mode and a card meets both requirements specified in steps 2 and 3, the card will be deactivated and the controllers will be updated.

Running the Silent Mode

In Silent Mode, the program will mark the cards as inactive if the card has not been used in the identified time frame and the selected Employee Type matches the cardholder's record.

To manually start the program:

1. **Type** the following in the Command Prompt or in a Batch File if the file is located in the C: root directory.
AutoExpire silent



To automatically run the AutoExpire Tool, a batch file must be created and scheduled via the Windows Scheduler.

To schedule:

1. From the Start Menu, **select** All Programs/Accessories and **select** the Notepad application. Notepad will open.
2. **Add** the following information to the text file if the file is located in the C: root directory.
AutoExpire silent
3. **Select** File / Save As and **enter** a Name.
The file should be saved in the same folder as the AutoExpire.exe file.
4. **Close** the Notepad application.

5. **Locate** the saved file from step 3.
6. **Change** the file extension to .BAT.
The file's icon will change.
7. From the Start Menu, **select** All Programs / Accessories / System Tools and **select** the Scheduled Tasks option.
The Scheduled Tasks window opens.
8. **Double-click** the Add Scheduled Task item.
The Scheduled Task Wizard opens.
9. **Follow** the Wizard to complete the setup.
The task will run the AutoExpire Tool based on the designated schedule.

DNA Event History Report Utility

The DNA Event History Report Utility allows the operator generate customized Event History reports without a DNA Fusion client. The reports are generated in standard PDF (.pdf) format and can be automatically e-mailed via SMTP protocol to one or multiple recipients. Type the link below to a URL or click on the link to begin the installation process.

Installation

1. **Click** on the link <http://license.ooinc.com/Download/DNAEventHistory>.
Setup.exe will begin to download.

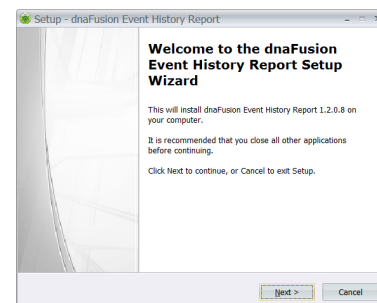


The Windows protected your "PC window will open." To bypass this window, click on "More info," and select "Run anyway."

2. After download is completed, **Double-click** Setup.exe to begin the installation.
The Welcome screen appears.
3. **Click** the Next button to continue.
The Destination Location screen displays.
4. **Click** the Next button or **select** the Browse button to specify a different location.
The Ready to Install window opens.
5. **Click** the Install button to start the installation.
The installation begins.
6. **Click** the Finish button to complete the installation.



The application is normally run as a Background Task in the Task Manager, so a program icon is not created.



E-Mail Setup

If reports will be scheduled and e-mailed to a recipient, the e-mail options will need to be set up.

1. Locate and open the DNAEventHistory.exe application.
Default Location: C:\Program Files (x86)\DNAFusion\Tools\DNAEventHistory
The DNA Event History Report dialog opens.

2. **Click** the E-mail Setup button.
The DNAEvent History Email Setup dialog opens.

3. **Enter** the Host Name and verify the Port number.
If configured, the mail server's name and outbound port information can be obtained by entering the following from the Windows Command Prompt.

Netsh diag connect mail

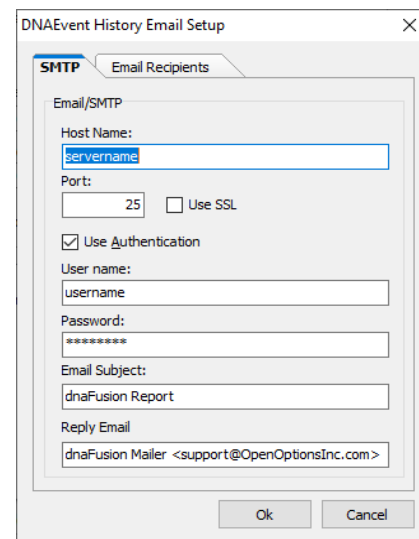
If successful, the e-mail configuration information will be returned.

Example:

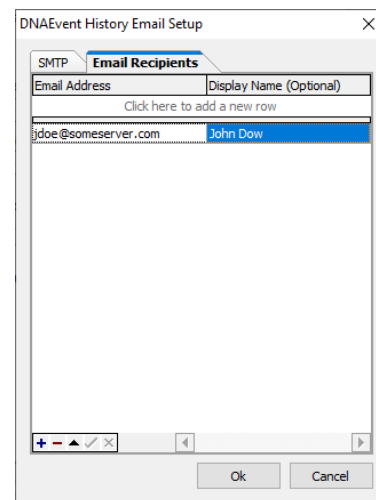
Mail Server Name

OutboundMailPort = 25

If no connection to port 25, see the system administrator and request that SMTP be enabled and/or modify any antivirus software to allow the DNAEventHistory.exe to e-mail third-party e-mail addresses.



4. If using SSL (Secure Socket Layer), **click** the Use SSL checkbox.
5. **Enter** the User Name and Password information.
6. If desired, **change** the Email Subject address.
7. **Enter** a valid Reply Email address.
8. Select the Email Recipients tab.
9. Select the Email Address field and enter the desired e-mail address.
10. If desired, enter a Display Name for the e-mail address.
11. Click the OK button to save the changes.

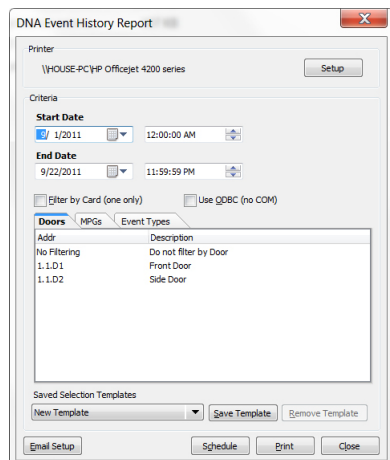


Configuring the Event History Report Parameters

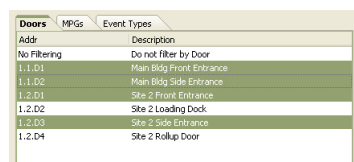
1. **Locate** and **open** the DNAEventHistory.exe application.

Default location: C:\Program Files\DNAFusion\Tools\DNAEventHistory

The DNA Event History Report dialog opens.



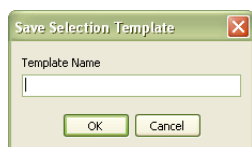
2. **Enter** a Start Date and Time.
3. **Enter** an End Date and Time.
4. **Select** the desired Door(s) from the list on the Doors tab.
Use the Shift or Control key to select multiple items.



5. If desired, **select** the MPG(s) from the MPGs tab.
If the system does not contain Monitor Point Groups, there will be nothing listed in the MPGs tab.
6. If needed, **select** the desired Events from the list on the Event Types tab.
Use the Shift or Control key to select multiple items.
7. If desired, **check** the Filter by Card checkbox and **select** the Card on the Cards tab.
Only one card can be selected.



8. **Select** the Save Template button to save the report configuration for future use.
The Save Selection Template dialog opens.



9. **Enter** a Template Name and **click** the OK button.
The Template is added to the Saved Selection Templates drop-down.
10. **Click** the Print button to generate the report.
The results open in the Report Viewer.



Scheduling a Report

1. **Click** the Schedule button from DNA Event History Report dialog to set the report on a schedule. The Schedule Report dialog appears.

2. **Enter** a unique Task Name.

3. In the PDF File to Save Report To: field, **click** the Browse button and **locate** the desired PDF (.pdf) file.

Prior to this step, a PDF document will need to be created if one does not already exist.

Default location: C:\Program Files\DNAFusion\Scheduled Reports.

4. **Select** the Selection Criteria Template from the drop-down list.

For information on creating templates, see step 8 on page 5-10.

5. If desired, **select** the Email PDF checkbox to e-mail the report to the specified recipients.

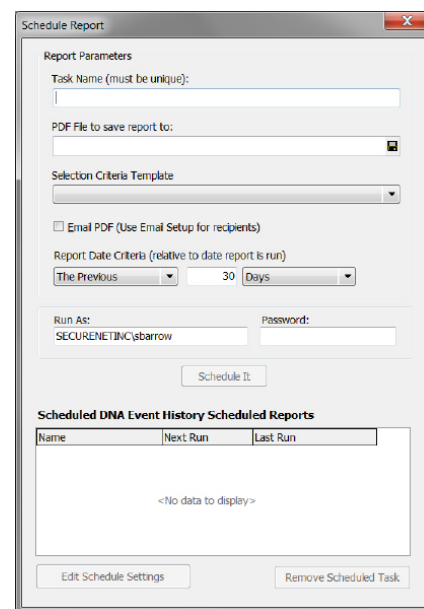
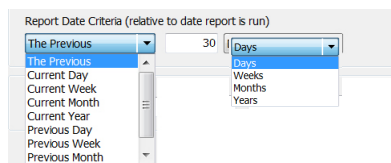
See page 5-9 for more information on e-mail setup.

6. **Set** the Report Date Criteria.

a. **Select** the Frequency.

b. **Enter** the desired Timeframe.

c. **Specify** the Units.

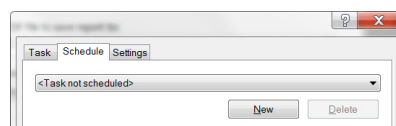


7. In the Run As section, **enter** the Password for the default user or **change** the User information and **enter** the Password for the specified user.

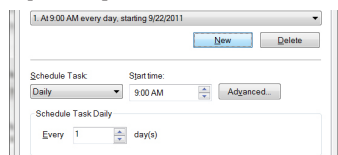
8. **Click** the Schedule It button.

The Scheduling dialog opens.

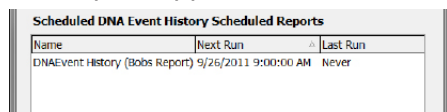
9. **Click** the New button.



10. **Specify** the desired Schedule and **click** OK.



The report appears in the Scheduled DNA Event History Scheduled Reports section.



Edit a Scheduled Report

1. **Select** the report from the Scheduled DNA Event History Scheduled Reports section.

2. **Click** the Edit Schedule Settings button.

The Schedule dialog opens.

3. **Edit** the Schedule and **click** OK.

Delete a Scheduled Report

1. **Select** the report from the Scheduled DNA Event History Scheduled Reports section.

2. **Click** the Remove Scheduled Task button.

DNA Time and Attendance Report

The DNA Time and Attendance Report captures In and Out information to simplify payroll. When a Time and Attendance card is presented at the specified door, the information is written to the DNATimeAttendanceRpt table in the database. This information includes the cardholder's name, whether the door used was an In or Out door, date and time, card number, card type, title, department, and the employee ID number.



DNA Fusion and SQL Server must be installed prior to configuring the Time and Attendance Report.

Installing the Time & Attendance Report

1. **Double-click** dnaTASetup.exe to begin the installation.

The Password screen appears.



2. **Enter** the Password and **click** Next.

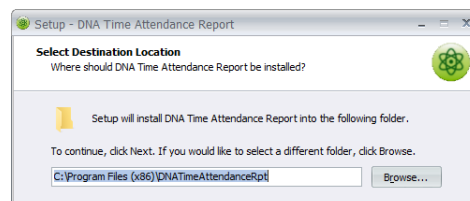
Contact Open Options Technical Support to obtain the password.

The Select Destination Location screen displays.

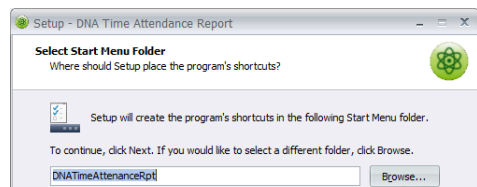
3. If desired, **browse** to a new file destination and **click** Next.

Default location:

- 32-bit OS – C:\Program Files\DNATimeAttendanceRpt
- 64-bit OS – C:\Program Files (x86)\DNATimeAttendanceRpt



The Select Start Menu Folder screen appears.

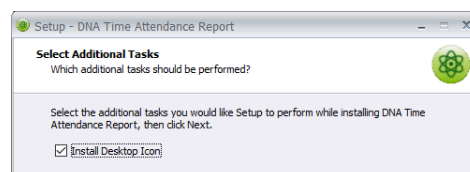


4. **Browse** to the desired Start Menu folder and **click** Next.

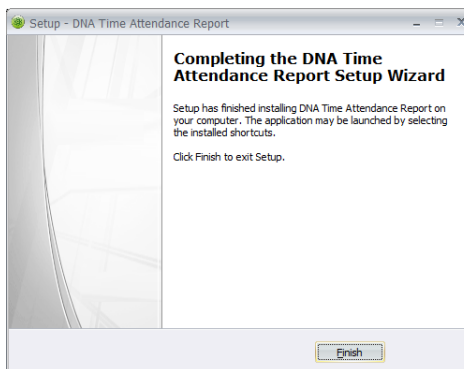
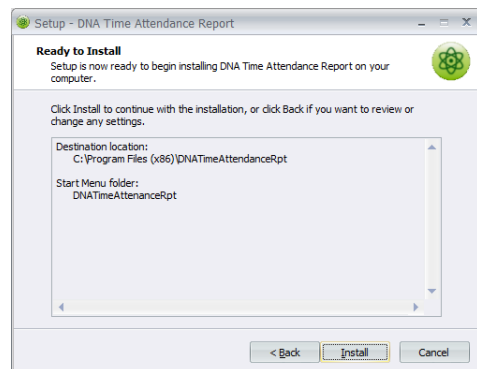
The default folder is DNATimeAttendanceRpt.

The Select Additional Tasks screen appears.

5. If desired, **select** the Install Desktop Icon checkbox and **click** Next.



The Ready to Install screen appears.



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

The installation begins.

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

Setting up the Time & Attendance Report

The first step is to prepare the DNA Fusion (or NPowerDNA) database for the project data as well as create the new Host Based Macros that will populate the database.

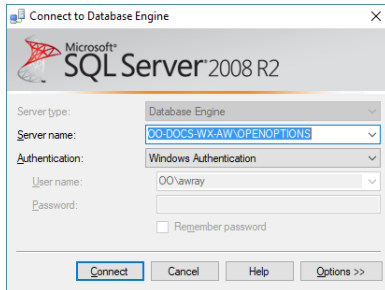
1. **Open** the DNATimeAttendanceRpt folder.

The default location is C:\Program Files\DNATimeAttendanceRpt for 32-bit OS or C:\Program Files (x86)\DNATimeAttendanceRpt for 64-bit OS.

2. **Double-click** on the DNATimeAttendanceRpt_Create.SQL query.  DNATimeAttendanceRpt_Create
Type: Microsoft SQL Server Query File

This SQL query creates the initial project table and the associated indexes.

The Connect to Database Engine dialog appears.



3. If required, **enter** the login information and **click** the Connect button.

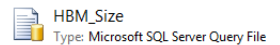
Microsoft SQL Server Management Studio opens.

4. **Select** the DNAFusion (or NPowerDNA) database option from the drop-down and **click** Execute.

The results will appear in the Message window.



5. If running DNAFusion 5.0.0.1135 or below, **execute** the HBM_Size.SQL query by **double-clicking** the file.



If running a later version, skip to step 8.

This query expands the size of the parameter fields in the Host Based Macro table.

The Connect to Server dialog opens.

6. If required, **enter** the login information and **click** the Connect button.

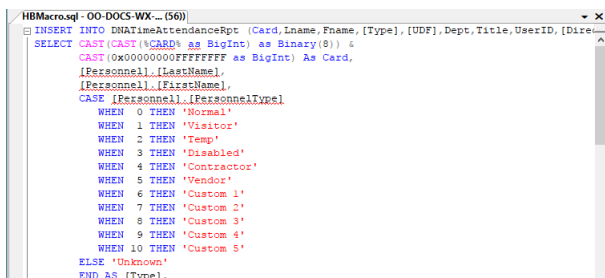
Microsoft SQL Server Management Studio opens.

7. **Select** the DNAFusion (or NPowerDNA) database option from the drop-down and **click** Execute.

The results will appear in the Message window.

8. **Double-click** the HBMacro.SQL query to open the file.  HBMacro
Type: Microsoft SQL Server Query File

Microsoft SQL Server Management Studio opens with the HBMacro query.



9. **Select** the text in the query and copy it to the clipboard.

10. **Open** DNAFusion and **select** the Triggers & Macros button on the Standard Toolbar.

The Triggers and Macros Browser opens.

11. **Select** the Host Based Macros browser tab.

12. **Right-click** on the desired Site object and **select** Add Host Macro.
The Host Based Macro (Global I/O) dialog opens.
13. **Enter** a name in the Macro Description field.
14. From the Local Object Type (Controlling Object) drop-down, **select** the Door option.
A list of door options appears in the Event ID drop-down lists.
15. **Select** the Door Event that will appear in the Events Grid when badging at Time & Attendance Doors.
Generally, this will be 072: Access Granted: Door Used.

The DNA driver (DNAdrvr32) will run the SQL query when the desired condition has been met (most likely Access Granted: Door Used). Certain parts of the SQL statement will be replaced with values from the current transactions; this includes the card number (%CARD%), door address (%ADDR%), current time (%PTIMEDATE%), as well as the cardholder's first and last names (%FIRSTNAME% and %LASTNAME%).

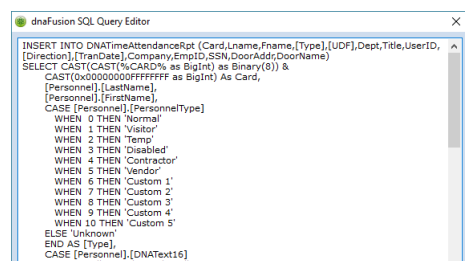
16. From the Remote Object (Controlled Object) drop-down, **select** the DBM: Add to Database With Events Server option.

A list of corresponding options appears in the Action drop-down lists.

17. **Click** the Build button under the Action 1 header. 

The SQL Query Editor dialog opens.

18. **Paste** the SQL query copied in step 10 into the SQL Query Editor window.



See page 5-16 for the complete HBMacro.SQL statement.

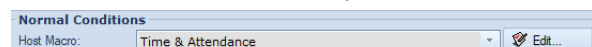
19. **Customize** the statement as needed:
 - If Custom Personnel Types are used in DNA Fusion, **modify** the Custom 1-5 (6-10) text strings under the Personnel Type section.
 - **Edit** the CASE '%ADDR%' statement to designate the doors that will be used as the Entry and Exit doors. A '1' indicates the entry door and a '0' identifies the exit door.

For instance, if door 1.1.D10 is the entrance door and 1.2.D1 is the exit, the SQL statement would be edited as follows:

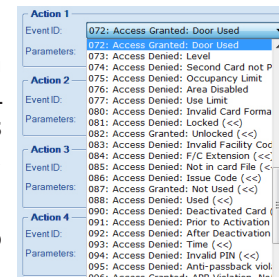
```
WHEN '1.1.D10' THEN 1
WHEN '1.2.D1' THEN 0
```

The operator can identify an unlimited number of entry and exit combinations.

20. **Click** OK to save the statement.
21. **Click** OK to save the Host Based Macro.
22. In the Hardware Browser, **right-click** on the first designated door and **select** Properties.
23. **Select** Macros from the dialog menu.
24. **Click** the Host Macro drop-down and **select** the Host Based Macro created in steps 10 through 20.



25. **Click** OK to save the changes.
26. Repeat steps 22 through 25 for all designated Entry/Exit doors.



HBMacro SQL Statement

Below is the complete HBMacro.SQL statement:

```

INSERT INTO DNATimeAttendanceRpt (Card,Lname,Fname,[Type],[UDF],Dept,Title,UserID,[Direction],[TranDate],C
ompany,EmpID,SSN,DoorAddr,DoorName)
SELECT CAST(CAST(%CARD% as BigInt) as Binary(8)) &
    CAST(0x00000000FFFFFFFF as BigInt) As Card,
    [Personnel].[LastName],
    [Personnel].[FirstName],
    CASE [Personnel].[PersonnelType]
        WHEN 0 THEN 'Normal'
        WHEN 1 THEN 'Visitor'
        WHEN 2 THEN 'Temp'
        WHEN 3 THEN 'Disabled'
        WHEN 4 THEN 'Contractor'
        WHEN 5 THEN 'Vendor'
        WHEN 6 THEN 'Custom 1'
        WHEN 7 THEN 'Custom 2'
        WHEN 8 THEN 'Custom 3'
        WHEN 9 THEN 'Custom 4'
        WHEN 10 THEN 'Custom 5'
    ELSE 'Unknown'
    END AS [Type],
    CASE [Personnel].[DNAText16]
        WHEN Null THEN 'Unassigned'
        WHEN '' THEN 'Unassigned'
    ELSE
        [Personnel].[DNAText16]
    END,
    CASE [Personnel].[Department]
        WHEN NULL THEN 'Unassigned'
        WHEN '' THEN 'Unassigned'
    ELSE
        [Personnel].[Department]
    END,
    [Personnel].[Title],
    [Personnel].[UserID],
    CASE '%ADDR%'
        WHEN '1.4.D1' THEN 1
        WHEN '1.4.D2' THEN 0
        WHEN '1.4.D3' THEN 0
        WHEN '1.4.D4' THEN 1
    ELSE 0
    END AS [Direction],
    '%PTIMEDATE%' AS [TranDate],
    [Company].[Company] ,
    [Personnel].[EmpID] ,
    [Personnel].[SSN],
    '%ADDR%' As DoorAddr,
    '%ADDRESS%' As DoorName
FROM [Keycards]
LEFT OUTER JOIN [Personnel] ON ([Keycards].[UserID] = [Personnel].[UserID])
LEFT OUTER JOIN [Company] ON ([Personnel].[Company] = [Company].[CompanyID])
WHERE [Keycards].[KeyNumber] = CAST(CAST(%CARD% as BigInt) as Binary(8)) & Cast(0x00000000FFFFFFFF as
BigInt)

```

Custom Text Strings

CASE '%ADDR%' Statement

Generating a Time & Attendance Report

1. **Open** the DNA Time & Attendance Report application.

This can be done from the Desktop icon or the Start Menu.

The DNA Time & Attendance Report dialog opens.

2. **Select** the desired Report Type from the drop-down list:

- Hours by Last Name - Alphabetizes the cardholders and provides the cardholder's total hours for each day as well as total hours for the report. Allows the operator to filter the report by a specific cardholder.
- Hours by Personnel Type - Groups cardholders by Personnel Type and provides the cardholder's total hours for each day as well displaying the total hours for each group. Allows the operator to filter the report by a specific Personnel Type.
- Summary Listing (By Name) - Alphabetizes the cardholders and provides the cardholder's total hours for the specified Date Parameters as well as the total hours for the report.
- Summary Listing (No Grouping) - Alphabetizes the cardholders and provides the total hours for the report.
- Hours by Department (Break on Dept) - Groups cardholders by Department and separates each department on a new page of the report. Provides the cardholder's total hours for each day as well as the cardholder's and department's total hours for the report. Allows the operator to filter the report by a specific Department.
- Hours by Department (Break on Person) - Groups cardholders by Department and separates each cardholder on a new page of the report. Provides the cardholder's total hours for each day as well as the cardholder's and department's total hours for the report. Allows the operator to filter the report by a specific Department.
- Hours by Department - Groups cardholders by Department and provides the cardholder's total hours for each day as well as the cardholder's and department's total hours for the report. Allows the operator to filter the report by a specific Department.

3. Depending on the Report Type selected above, **configure** the report parameters.

- Hours by Last Name - If desired, **select** the Cardholder from the Last/First drop-down list.
- Hours by Personnel Type - If desired, **select** the Personnel Type from the drop-down list.
- Hours by Department (Break on Dept) - If desired, **select** the Department from the drop-down list.
- Hours by Department (Break on Person) - If desired, **select** the Department from the drop-down list.
- Hours by Department - If desired, **select** the Department from the drop-down list.

4. **Select** the desired Identity Field to include in the report: Employee ID or Employee #.

These fields are located in the Employee Info: (Page 2) tab of the Cardholder's Record.

5. If needed, **edit** the Start and End dates and times.

The dates default to the first minute of the first day of the current month and the last minute of the last day of the current month.

6. **Select** the Duration Threshold to apply to the report. (Default = None; Max = 48 hours)
The Duration Threshold setting specifies the maximum amount of time that must expire between entry and exit transactions in case entries become orphaned.
7. If desired, **check** Round Duration to Nearest 5 Minute Interval to round Duration times in the report.
For example, if the duration between the Time In and Time Out is one hour and six minutes (01:06), the report will round this amount to one hour and five minutes (01:05).
8. **Select** the New Entry Threshold to apply to the report. (Default = 16 hours; Max = 24 hours)
9. **Click** the Print button.
The results will open in the Report Preview.
If Export is selected, the results will be saved to the specified location.

DNA Import Tool

The DNA Import Tool allows the operator to import data from an external data source into the DNA Fusion database tables. The Import Tool can add cards to the imported records as well as assign the cards to a personnel group at the time of the import. This simplifies the assignment of door access and creation of personnel groups.

Open Options recommends using a small file that contains just a couple of values to test the configuration before trying to import larger quantities.

Running the Import Tool

It is recommended that the Import Tool be run on the DNA database server.

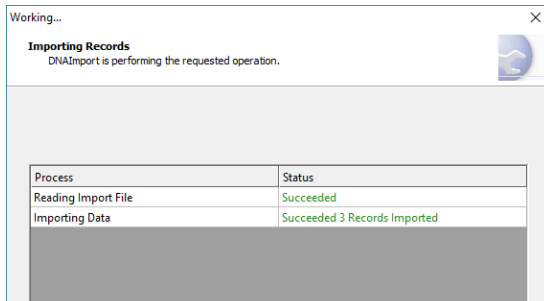
1. **Double-click** the DNAImport.exe file to open the DNA Import tool.
The Welcome dialog appears.
2. **Click** the Next button to continue.
The Select Import File dialog appears.
3. **Select** the Browse button to locate the desired import file.
The Open dialog appears.
4. **Locate** the desired file and **click** the Open button.
5. If the first row of the imported file contains column names, **check** the First Row Has Column Names box.
If checked, the first row will be available for mapping; however, it will be ignored during the import process.
6. If needed, **edit** the Row Delimiter field.
This entry specifies the end-of-row character. See table below.
7. If needed, **edit** the Column Delimiter field.
This entry separates the data items. See table below.

VALUE	DESCRIPTION
{CR}{LF}	Delimited by a carriage return-line feed combination.
{CR}	Delimited by a carriage return.
{LF}	Delimited by a line feed.
Semicolon {;}	Delimited by a semicolon.
Colon {:}	Delimited by a colon.
Comma {,}	Delimited by a comma.
Tab {\t}	Delimited by a tab.
Vertical bar { }	Delimited by a vertical bar.

8. If available, **select** a desired Template from the Use Template From Previous Import list.
9. **Click** the Next button.
The Column Mapping dialog opens.
10. **Select** the desired Mapped To field from the drop-down list for the corresponding DNA Field.
The Mapped To fields are pulled from the imported file. If the first row contained column names (step 5), they will be displayed in the drop-down.
11. If desired, **enter** a Default Value and **click** the Next button.
The Additional Settings dialog appears.
12. If desired, **select** the Save Settings For Future Import checkbox and **enter** a Template Name.

13. If desired, **select** the Create Personnel Group for Imported Personnel checkbox and **enter** the Group Name.
14. If desired, **uncheck** the Check For Duplicates boxes.
15. **Click** the Next button to start the import process.

The Importing Records dialog opens.



16. When complete, **click** the View Report button to view the import results or **click** the Close button to exit the application.

Permissions Issues

In order for the import to be successful, there are few permissions issues to consider:

- Permission to connect to the source and destination databases or file shares.
- Permission to read data from the source database or file. If using SQL Server, this requires SELECT permissions on the source tables and views.
- Permissions to write data to the destination database or file. In SQL Server, this requires INSERT permissions on the destination tables.

Batch Printer

The Batch Printer tool allows the operator to print batches of cards based on filtered criteria, including Personnel Group, Personnel Type, Card Type, Department, Company, Location, Title, Card Expiration, and Custom Fields. Each batch is associated with a specific badge template file (.bdg) and stored in a print queue until the operator is ready to print.

Opening the Batch Printer

To open the Batch Printer application:

1. **Double-click** on the BatchPrinter.exe file.

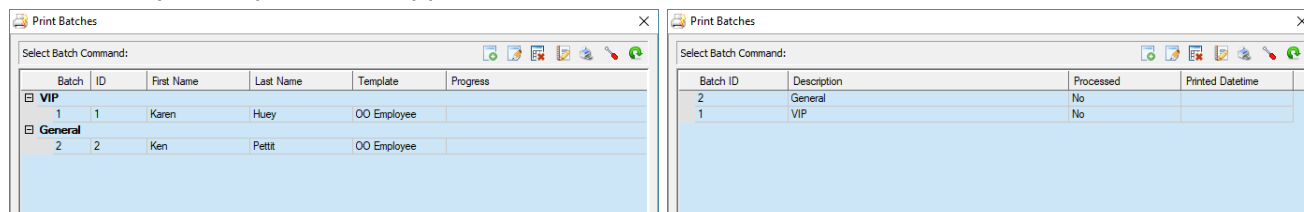
Default location:

- 32-bit OS – C:\Program Files\DNAFusion\Tools\BatchPrinter\BatchPrinter.exe
- 64-bit OS – C:\Program Files (x86)\DNAFusion\Tools\BatchPrinter\BatchPrinter.exe

The Print Batches dialog opens.








2. **Select** the desired tab:

- Batch Printing - Displays a print queue of batches and their print status. Expand an item to view the cards included in the batch.
- Batch List - Displays a list of batch commands configured by the operator as well as the date and time that they were printed, if applicable.



Batch Printer Toolbar

The Print Batches dialog contains a toolbar with the following commands:

	Add New Batch	Opens the Filter List dialog to create a new batch. See page 5-22.
	Edit Working Batch	Opens the Filter List dialog to edit an existing batch. See page 5-22.
	Delete Selected Items	Removes the selected batch from the print queue. See page 5-23.
	Create Batch Report	Displays a dialog with the number of the last batch printing entries.
	Print Batches	Opens the Page Setup dialog to configure the print settings and print the batch(es) in the queue. See page 5-23.
	Batch Print Configuration	Opens the Settings dialog to configure the Badge Template and Photos paths as well as select the printer. See page 5-22.
	Refresh	Refreshes the batch print queue.

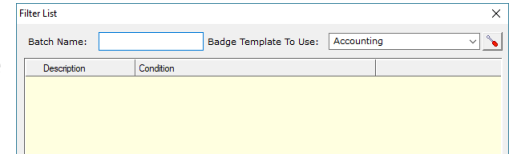
Adding a New Batch

1. In the Batch Printing or Batch List tab of the Print Batches dialog, **click** the Add New Batch icon. 

Or

Right-click in the dialog and **select** Add Batch to Print from the context menu.

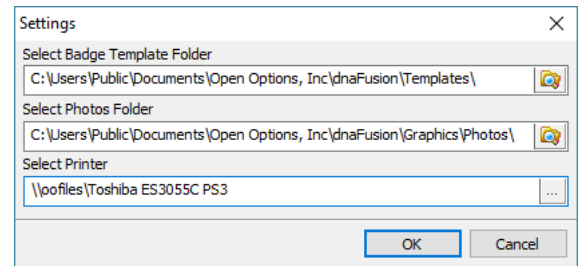
The Filter List dialog opens.



2. If needed, **click** the Batch Print Configuration icon to set up the template path. Otherwise, skip to step 5.

3. **Configure** the Settings dialog:

- Select Badge Template Folder - **Browse** to the desired badge template folder or **enter** the directory path. This is the folder location that will determine the Badge Template drop-down options.
- Select Photos Folder - **Browse** to the desired photos folder or **enter** the directory path.
- Select Printer - **Click** the Browse button to configure the Page Setup dialog and **select** the printer.



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

5. In the Filter List dialog, **enter** a Batch Name and **select** a Badge Template to Use from the drop-down. The drop-down options are determined by the Badge Template Folder path set in step 3.

6. **Click** the Add button to add a filter to the batch command.

The Select a Filter dialog appears.

7. **Select** a Type from the drop-down.

8. **Select** the desired filter option(s) from the list.

Press and **hold** the Ctrl or Shift key to select multiple options.

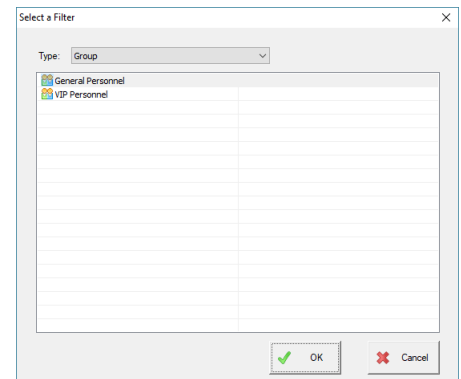
9. **Click** OK.

The filter(s) is/are added to the Filter List dialog.

10. **Repeat** steps 6-9 as needed to apply additional filters to the batch.

11. **Click** OK.


The batch appears in the Print Batches dialog.



If the filtered criteria does not match any personnel or card records in the DNA Fusion database, the batch will still appear in the Batch List tab; however, it will not be added to the print queue in the Batch Printing tab.

Modifying a Batch

To edit an existing batch command:

1. In the Batch Printing or Batch List tab of the Print Batches dialog, **select** an existing batch and **click** the Edit Working Batch icon. 

Or

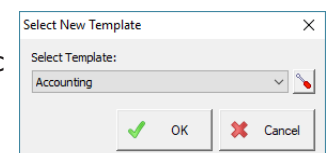
In the Batch List tab, **right-click** on the existing batch and **select** Modify Selected Batch.

The Filter List dialog appears.

2. **Edit** the batch as desired and **click** OK.

To change the Badge Template for specific batches or cardholders:

1. In the Batch Printing tab, **right-click** on the desired batch item(s) or specific cardholder(s) and **select** Change Badge Template.
2. **Select** a Template from the drop-down and **click** OK.



Removing a Batch

To remove a batch group:

1. In the Batch Print or Batch List tab of the Print Batches dialog, **select** the desired batch(es) and **click** the Delete Selected Items icon. 

Or

Right-click on the desired batch(es) and **select** Remove Group from Batch.

A confirmation dialog appears for each batch.

2. **Click** Yes to confirm.

The selected batch(es) are removed from the Print Batches dialog.

To remove one or more cardholders from the batch print queue:

1. In the Batch Printing tab, **expand** the batch item, **right-click** on the desired cardholder(s), and **select** Remove Person from Batch.

A confirmation dialog appears.

2. **Click** Yes to confirm.

The cardholder(s) is/are removed from the queue.



When the Remove Person from Batch option is used, the selected cardholder(s) will be deleted from ALL batches in the print queue.

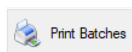
Printing Batches

To print batches in the queue:

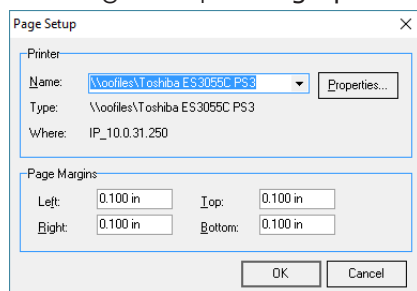
1. In the Batch Printing tab of the Print Batches dialog, **click** the Print Batches icon. 

Or

Click the Print Batches button.



The Page Setup dialog opens.



2. If needed, **select** a different printer from the Name drop-down and **configure** the Properties.
3. **Click** OK.

The batches will begin printing from the top of the queue and the Progress column will display the print status for each badge. A progress bar will also appear at the bottom of the dialog.

4. If needed, **click** the Stop Printing button to cancel the print queue. 



At least one badge template file (.bdg) must be present in the configured Badge Template Folder in order to print batches. The default folder path is C:\Users\Public\Documents\Open Options, Inc.\dnaFusion\Templates. See page 5-22 for more information.

Exporting a Batch

To export a batch to a CSV (.csv) file:

1. In the Batch Printing or Batch List tab of the Print Batches dialog, **right-click** on the desired batch and **select** Export Selected Batch.
2. **Browse** to the desired file location and **click** Save.

[illegible]

DNA Diagnostics

The DNA Diagnostics tool allows the operator to submit log files directly to Open Options Technical Support to quickly diagnose or troubleshoot a system error. Additionally, the operator can save diagnostics to an archive, browse to a specific log file, start and stop services on the workstation, view software license information, and/or download the DNA Fusion license file.

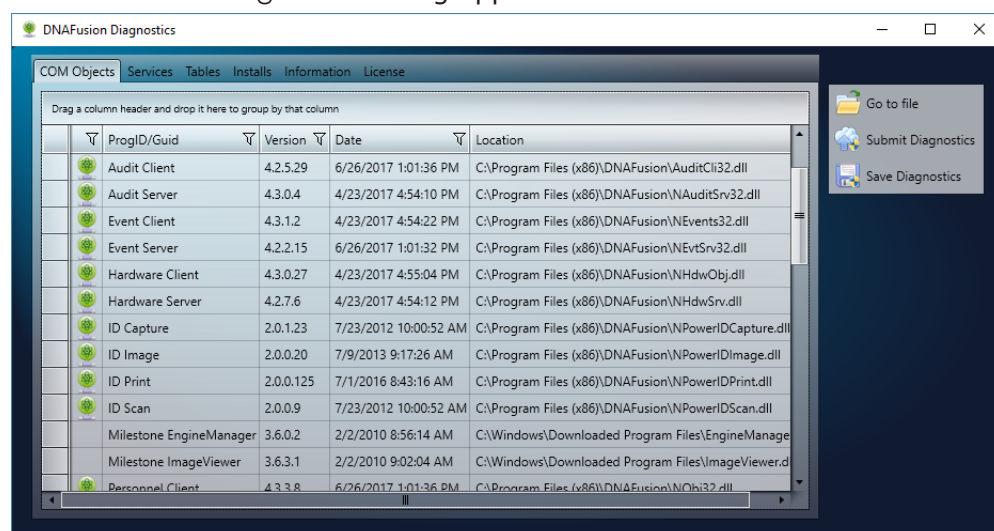
To open the DNA Diagnostics application:

1. **Double-click** on the DNADiagGui.exe file.

Default location:

- 32-bit OS – C:\Program Files\DNAFusion\Tools\Diagnostics\DNADiagGui
- 64-bit OS – C:\Program Files (x86)\DNAFusion\Tools\Diagnostics\DNADiagGui

The DNAFusion Diagnostics dialog appears.



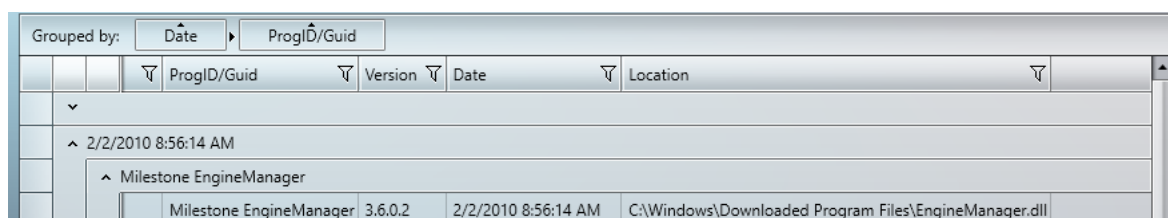
2. **Select** the desired tab to view the diagnostic parameters:

- COM Objects - Displays a grid of COM object information, including the active version and file location.
- Services - Displays a grid of DNA services and allows the operator to Start, Stop, Pause, or Restart the selected service.
- Tables - Displays a grid of database table information.
- Installs - Displays information about DNA Fusion installs, including the installation date, version, and application path. Expand an item to view additional information.
- Information - Displays key diagnostic information regarding the .NET Versions, Codecs, Environment Variables, Logical Drives, Processor, System, and Video.
- License - Provides a diagnostic overview of the station's licensing information.



*If desired, **drag and drop** a column header to the "Grouped By" box to group items in the grid by the selected column. **Add** additional column headers to create subgroups. See page 14-16 in the DNA Fusion User Manual for more information on this feature.*

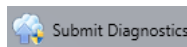
*To **remove** a column, **drag** the header away from the "Grouped By" box OR **hover** the mouse over the column header in the "Grouped By" box and **click** the X button.*



Submitting Diagnostics

The DNA Diagnostics tool allows the operator to submit their log files directly to Open Options Technical Support for the purpose of diagnosing or troubleshooting an error in the DNA Fusion software.

1. In the DNAFusion Diagnostics dialog, **click** the Submit Diagnostics button.



This action can be performed from any tab in the dialog.

The Submit Diagnostics - Welcome dialog opens.

2. If desired, **enter** any additional information to submit with the log files to Open Options.

3. **Click** Next to continue.

The Submit Diagnostics - Additional Files screen appears.

4. If desired, **click** the Add Files button to provide additional files that may be useful for troubleshooting.

To remove a file from the list, **click** the X button to the right of the list item.

To clear all files from the list, **click** the Clear button.

5. **Click** Next to continue.

The Submit Diagnostics - User Provided Data screen appears.

PROVIDE	NAME	EXPRESSION
<input checked="" type="checkbox"/>	AccessArea	
<input type="checkbox"/>	AccessLevelDescriptions	
<input type="checkbox"/>	AccessLevelGroup	
<input type="checkbox"/>	AccessLevels	
<input type="checkbox"/>	Acknowledgements	

6. If desired, **select** a specific database table(s) to provide to Open Options for troubleshooting.

Enter text in the Filter Tables field to filter the list of available tables.

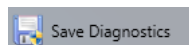
7. **Click** Submit.

The diagnostic data is sent to Open Options Technical Support.

Saving Diagnostics

DNA Diagnostics allows the operator to archive diagnostic log files in a compressed (.zip) folder.

1. In the DNAFusion Diagnostics dialog, **click** the Save Diagnostics button.



This action can be performed from any tab in the dialog.

The Save As dialog appears.

2. **Browse** to the desired file location, **edit** the File Name, and **click** Save.

The Save Diagnostics - Welcome dialog opens.

3. If desired, **enter** any additional information to provide to Open Options.

4. **Click** Next to continue.

The Save Diagnostics - Additional Files screen appears.

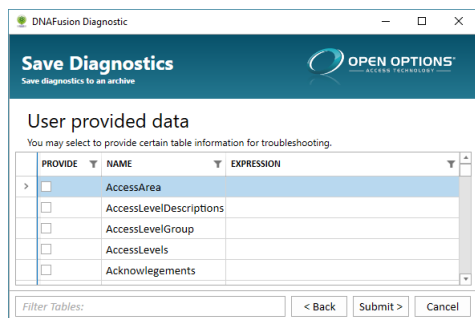
5. If desired, **click** the Add Files button to provide additional files that may be useful for troubleshooting.

To remove a file from the list, **click** the X button to the right of the list item.

To clear all files from the list, **click** the Clear button.

6. **Click** Next to continue.

The Save Diagnostics - User Provided Data screen appears.



7. If desired, **select** a specific database table(s) to provide to Open Options for troubleshooting. **Enter** text in the Filter Tables field to filter the list of available tables.

8. **Click** Submit.

The diagnostic data is archived to a compressed (.zip) folder.

9. **Click** Finish.

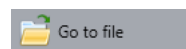
Browsing to a Log File

The DNA Diagnostics tool provides an option to quickly browse to a specific log file location.

1. In the DNAFusion Diagnostics dialog, **select** one of the following tabs:

- COM Objects
- Services
- Installs

2. **Select** an item from the grid and **click** the Go to File button.







The DNAFusion dialog appears with the selected file location.

Starting and Stopping a Service

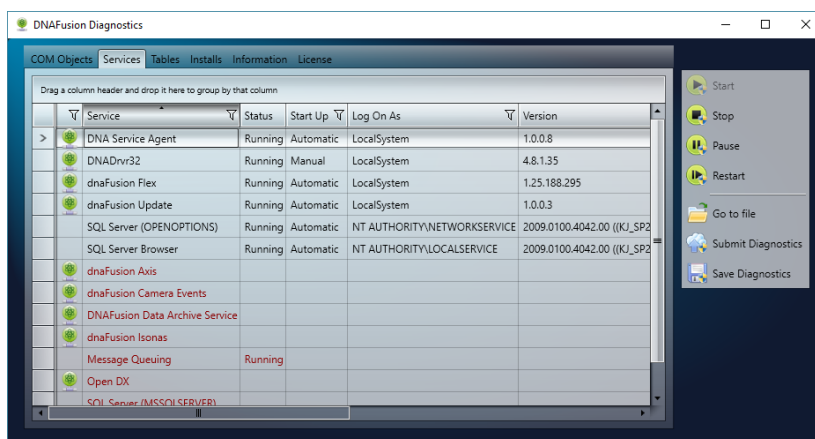
The operator can Start, Stop, Pause or Restart services directly from the DNA Diagnostics tool.

1. In the DNAFusion Diagnostics dialog, **select** the Services tab.

2. **Select** a Service from the grid and **click** one of the following options:

-  Start
-  Stop
-  Pause
-  Restart

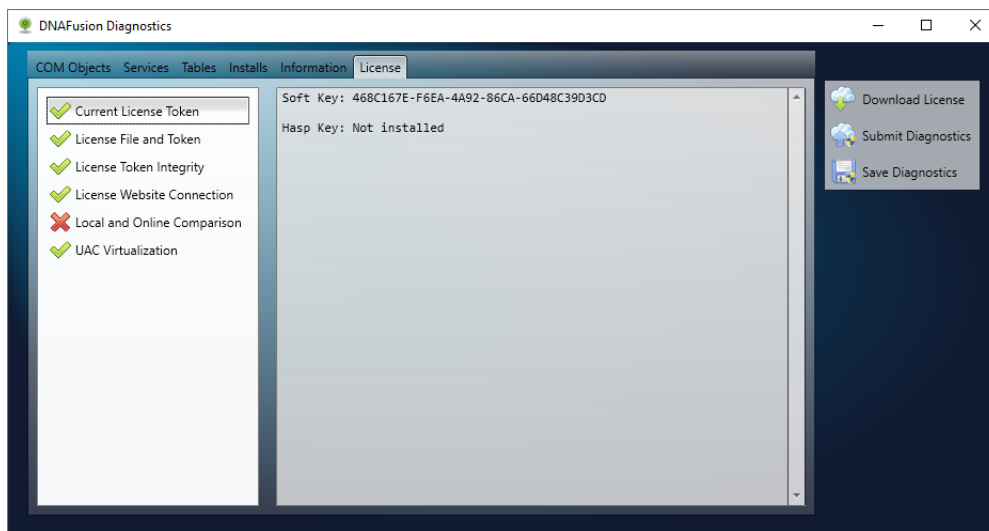
3. The Status column changes to reflect the updated service status.



Downloading the License File

The operator can download the DNA Fusion license install file directly from the DNA Diagnostics tool.

1. In the DNAFusion Diagnostics dialog, **select** the License tab.



2. **Click** the Download License button.  Download License

A link to the LicenseInstall.exe file appears in the operator's web browser.

Troubleshooting A

Locating the DNA Driver Version

The DNA Driver version (dnaDrv32.exe) can be obtained using the following procedure:

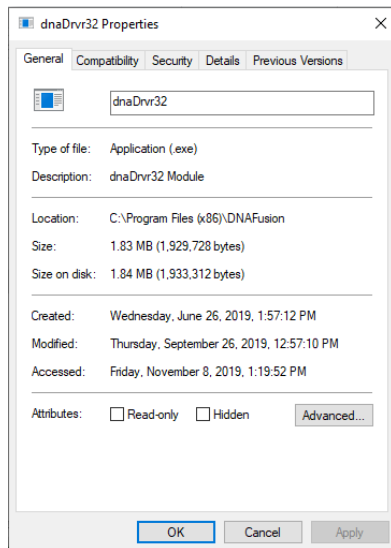
1. **Open** the DNAFusion folder.

Default location:

- 32-bit OS – C:\Program Files\DNAFusion
- 64-bit OS – C:\Program Files (x86)\DNAFusion

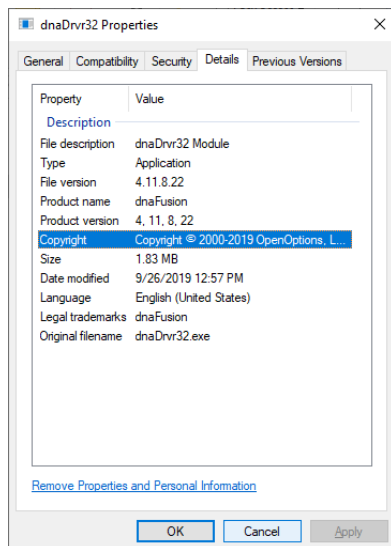
2. **Right-click** on the dnaDrv32 application and **select** Properties.

The dnaDrv32 Properties dialog opens.



3. **Select** the Details tab.

The driver version is specified in the Product Version field.



COM Surrogate Errors

If a COM Surrogate error appears when launching DNA Fusion, use the following information to troubleshoot the issue:

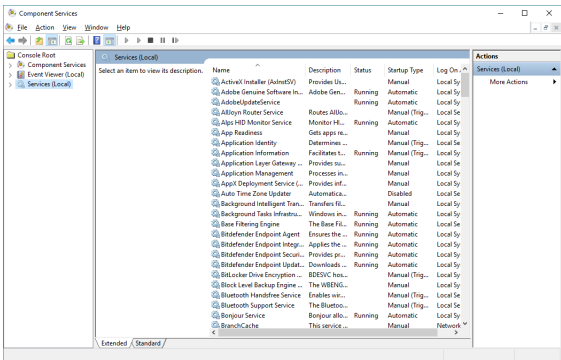
1. **Run** the DNABatchDownloadSettings.exe application.
Default location:
 - 32-bit OS – C:\Program Files\DNAFusion\Tools
 - 64-bit OS – C:\Program Files (x86)\DNAFusion\Tools
2. **Review** the error message.
 - Access Denied - The Windows login does not have rights to the COM Objects. See pages 2-8 and 2-15 for more information.
 - Configured Identity is Incorrect - The DNAFusion COM+ application needs to be configured to run under a Windows Local Administrator account. See page 2-8 for more information.
 - Oledb Error - Issue connecting to the DNA Fusion database and/or the DNAdrv32 driver service account does not have permission to connect to the database. See page 2-15 for database connection issues and page 2-8 for information on driver service account.
 - RPC Server Unavailable - Typically received from the client workstation. This error could indicate a number of problems, such as a firewall or unreachable network server. For more information on firewall configuration, see page 2-19.

Starting and Stopping the Services

Driver

To manually start or stop the driver service:

1. From the Control Panel, **open** the Component Services and **select** Services (Local) from the dialog menu.



2. **Right-click** on the DNADrv32 service and **select** Start or Stop.
3. If no other services are to be controlled at this time, **close** the dialog.
However, if the operator wishes to manually start SQL Server at this time, they may **right-click** SQL Server (OPENOPTIONS) in this dialog and **select** Start.

SQL Server

To manually start the SQL Server service:

1. From the Control Panel, **open** the Component Services and **select** Services (Local) from the dialog menu.
2. **Right-click** on the SQL Server (OPENOPTIONS).

This is the default server name. The actual system may have a different server name if a typical installation was not conducted.
3. **Select** Start.
4. If no other services are to be controlled at this time, **close** the dialog.

However, if the operator wishes to manually control the Driver at this time, they may **right-click** DNADrvr32 in this dialog and **select** Start or Stop.

Client-to-Server Troubleshooting

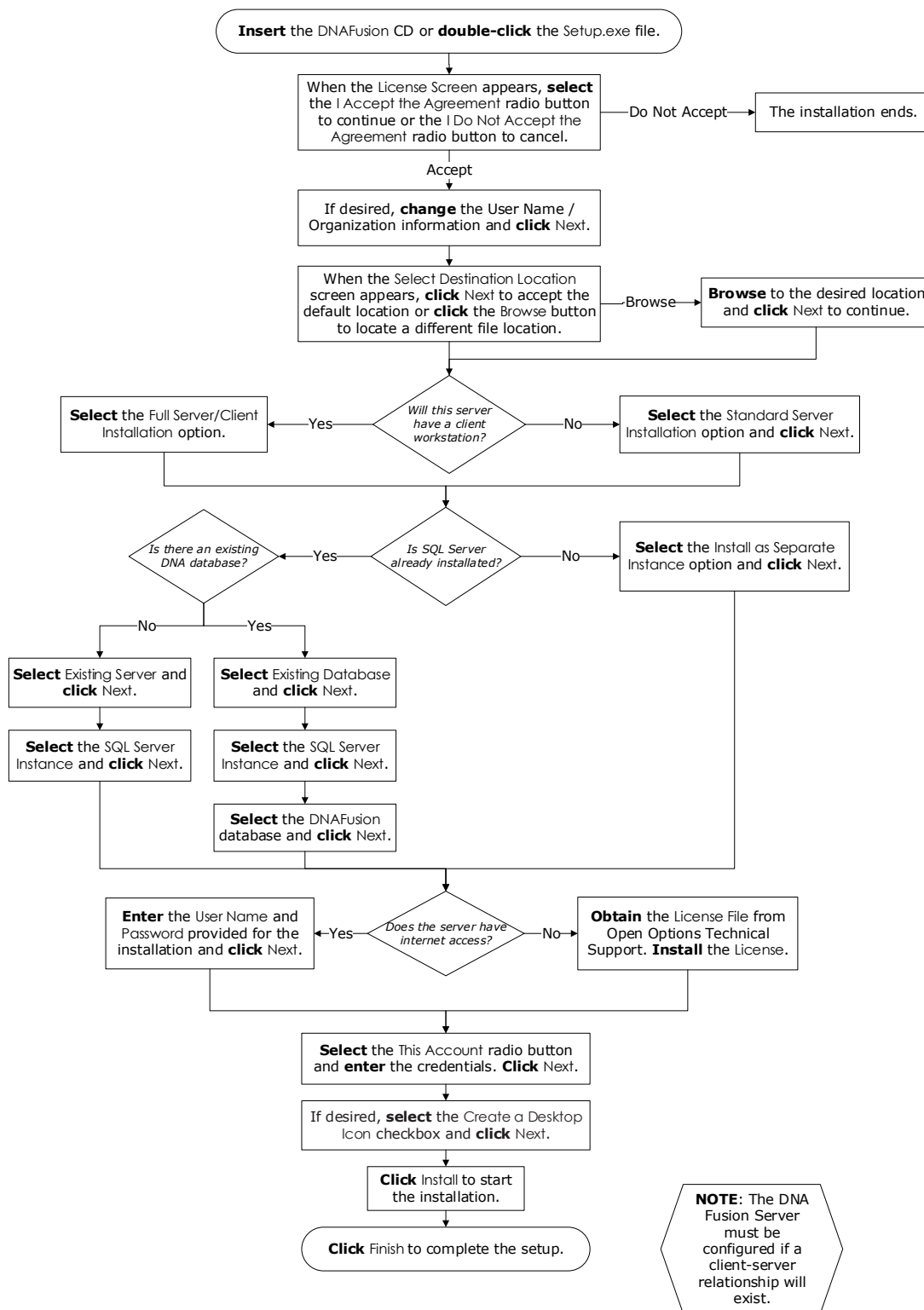
ERROR	ISSUE	RESOLUTION
COM Disabled Error when attempting to connect	A DNA Fusion client uses MSDTC to talk to the server, if the Application Server's Role is not configured correctly on the Server.	Configure the Application Server's Role.
General Access Denied Error	The Windows user has not been added to the server's Distributed COM Users group.	Add the Windows user to the Distributed COM Users group.
RPC Server Unavailable Error	Once MSDTC functionality is established, the client will authenticate to the Application Server using the client's current Windows credentials. This authentication happens on Port 135, so if the port is blocked, an error will occur.	Open Port 135 on the client.
RPC Server Unavailable Error	After Windows Authentication is successful, DCOM will then attempt to open a random high port to the server. If this connection fails, the operator will receive an error message.	MSDTC can be configured to use a specific port range, but both the client and the Application Server need to be configured for the same range.
Configured identity is incorrect, please check user name and password.	The windows account that is attempting to start the COM+ object on the Application Server is not a local machine administrator, or the configured user name and password is incorrect.	Configure the current identity correctly or change the login information running the COM+ object to a local machine administrator.
A Crystal Reports "Login Failed" Error	This error will be the result of a refused connection to the SQL server. To run a report, the active Windows user must have SQL permissions for a direct connection to the database. The default port for this SQL connection is Port 1433.	Add the Windows users to the DNAUSERS group on the Application Server.

This Page Intentionally Left Blank

Process Diagrams

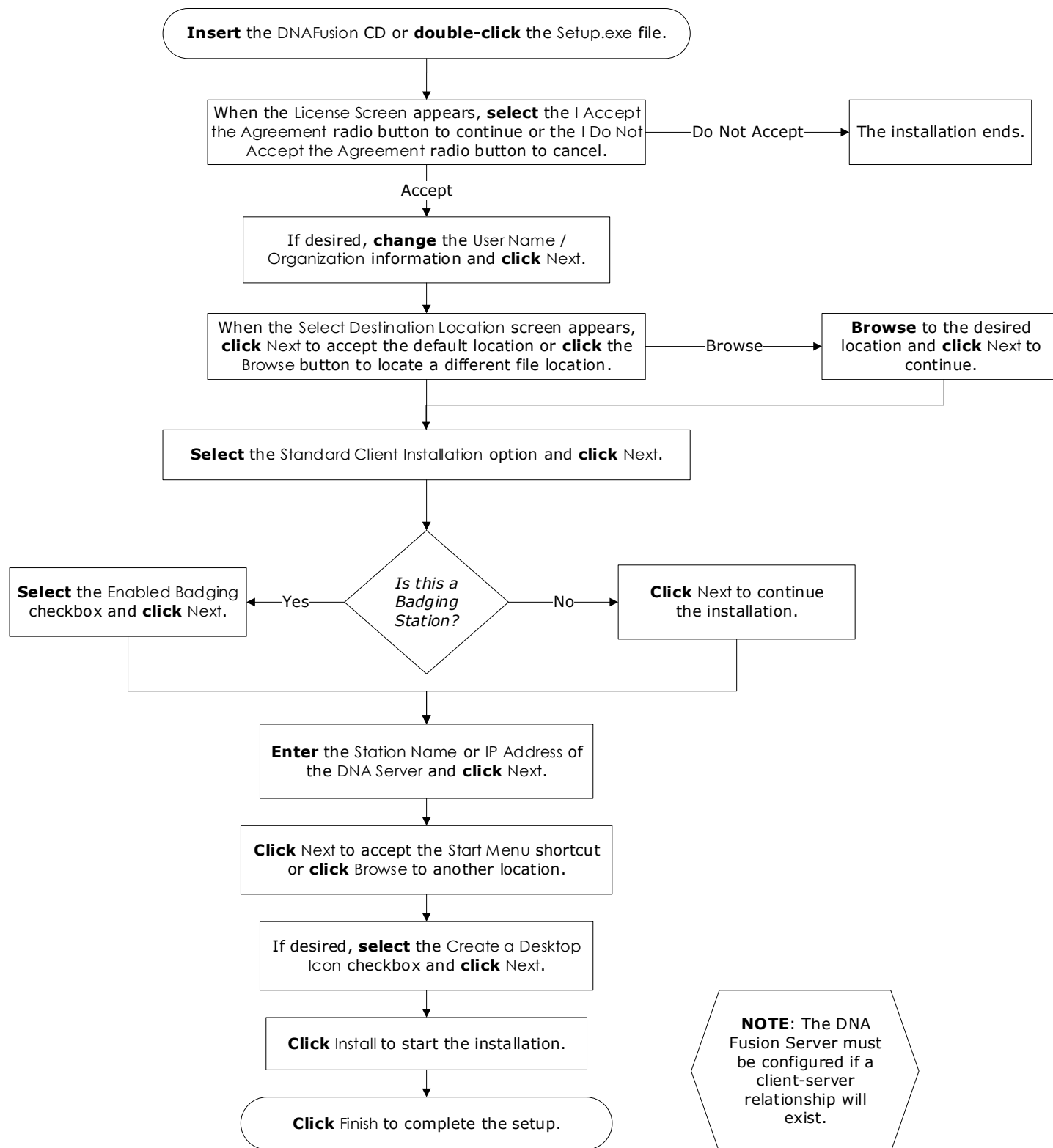
B

Server Installation

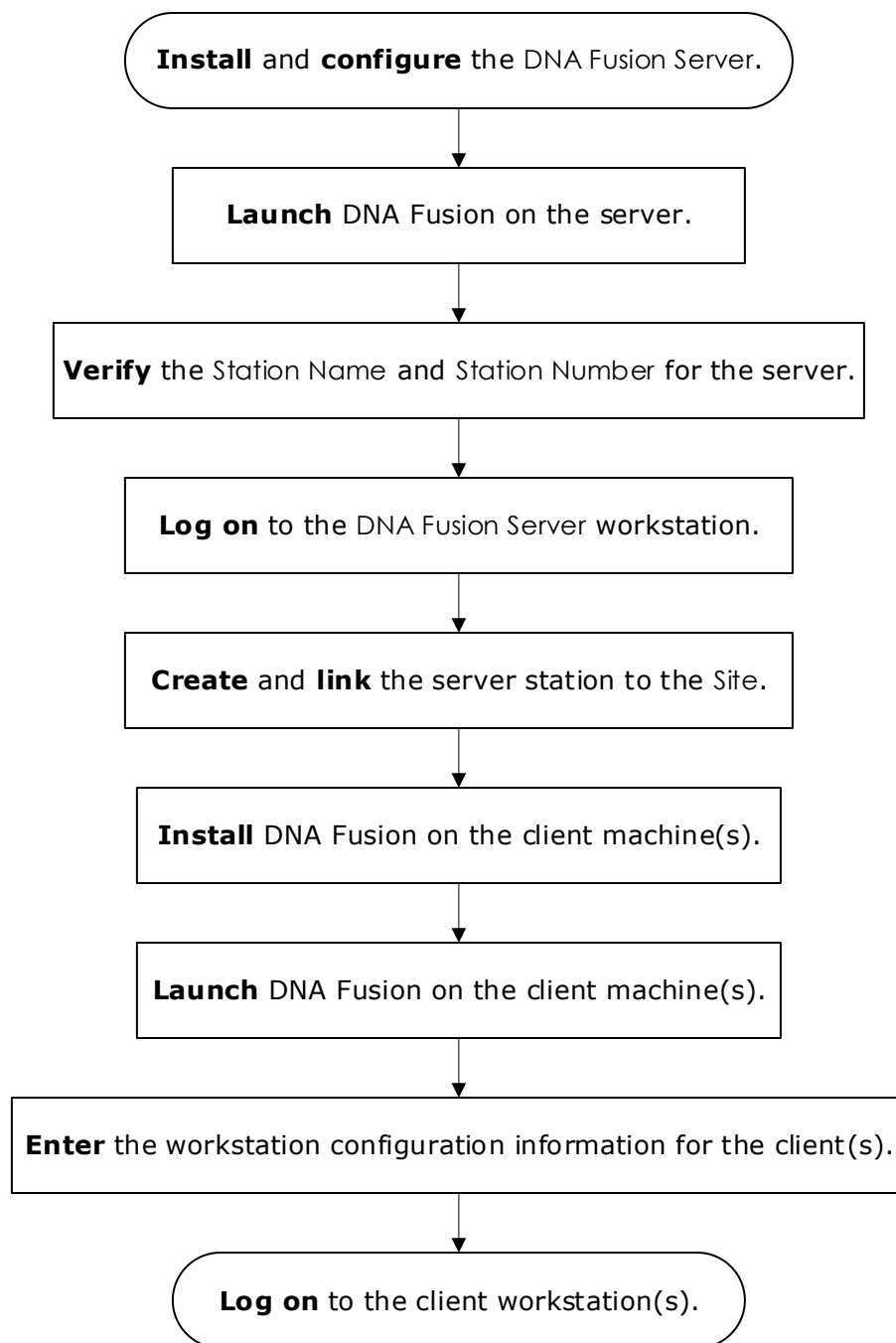


This Page Intentionally Left Blank

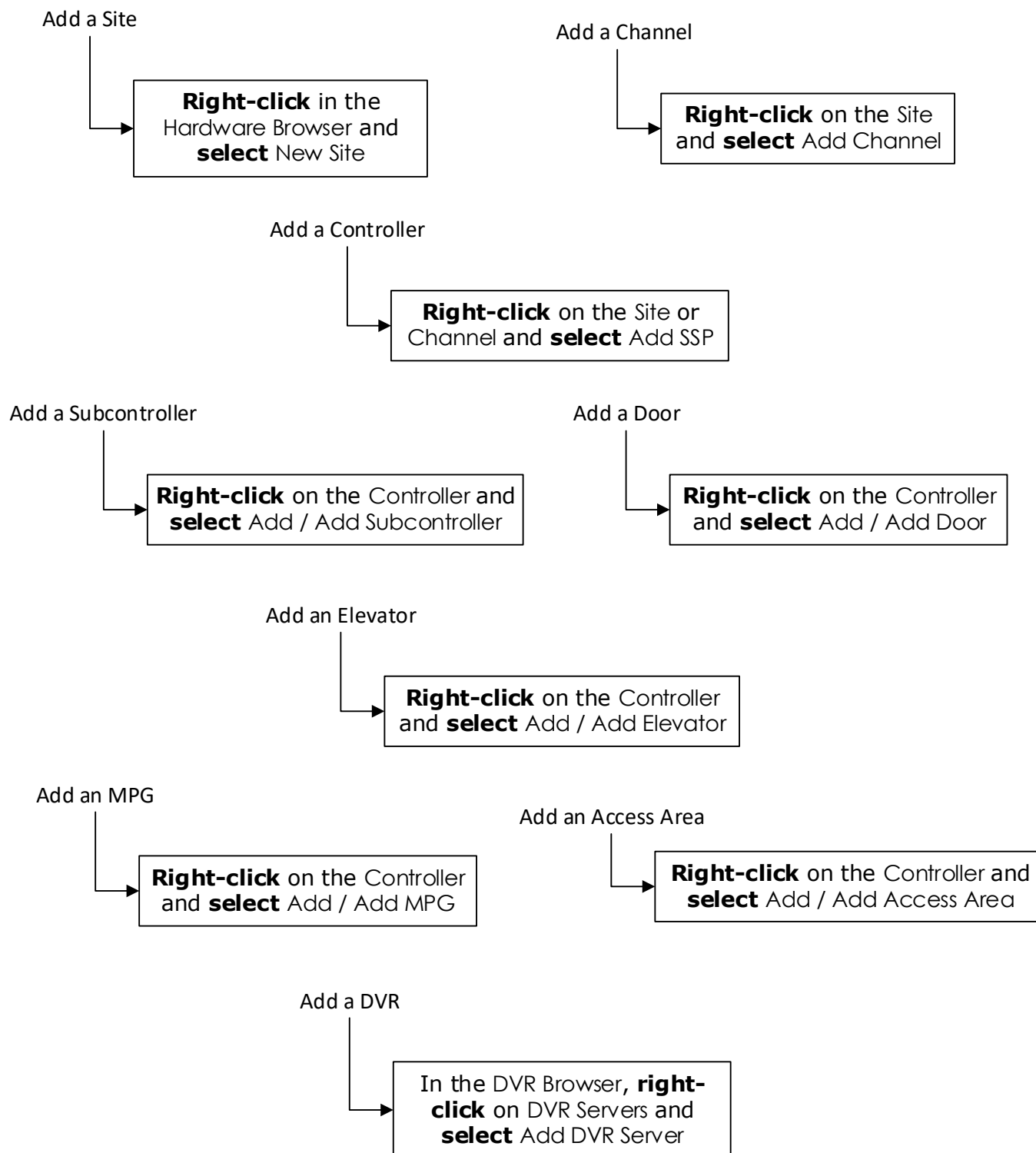
Client Installation



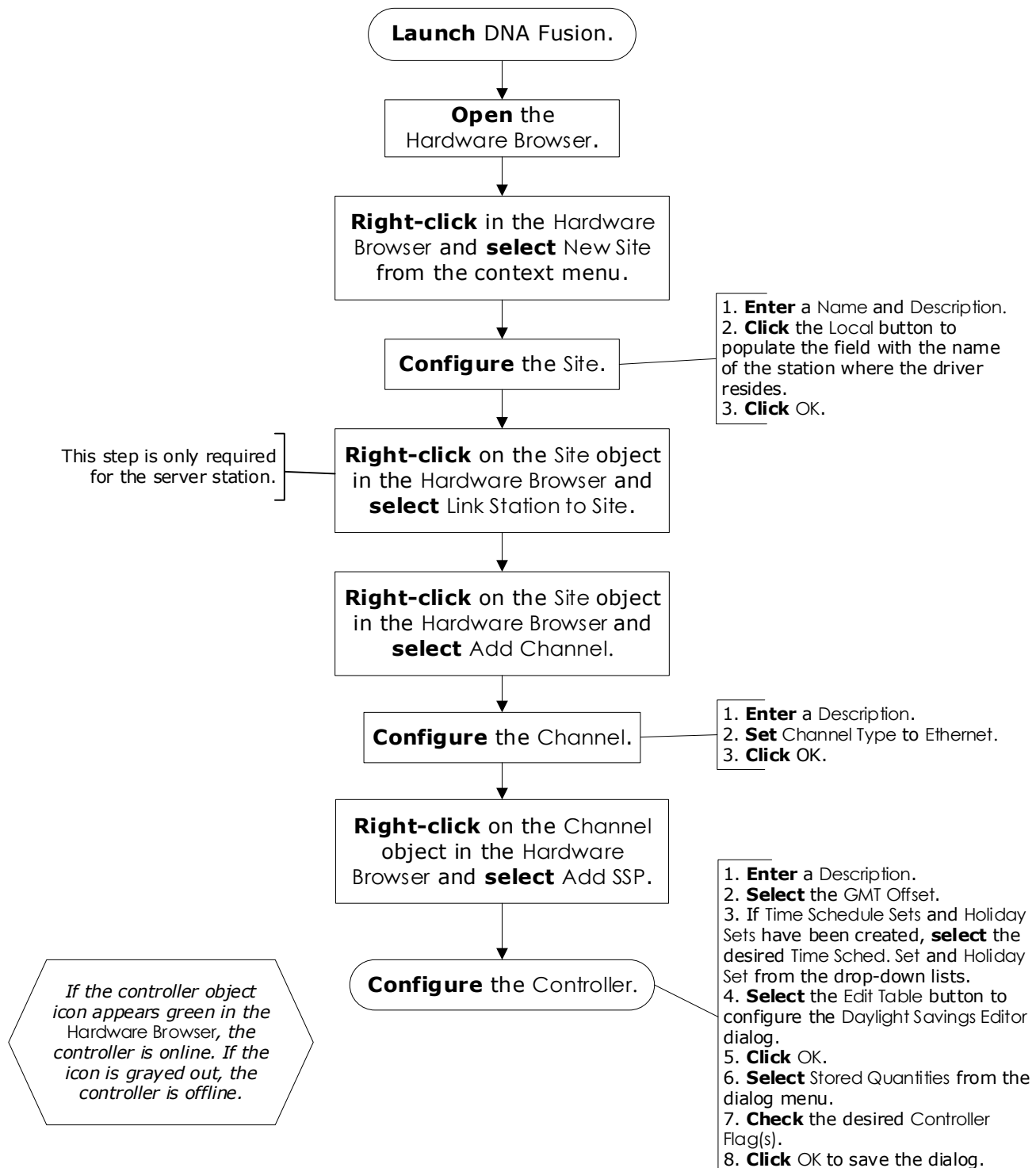
Server/Client Setup



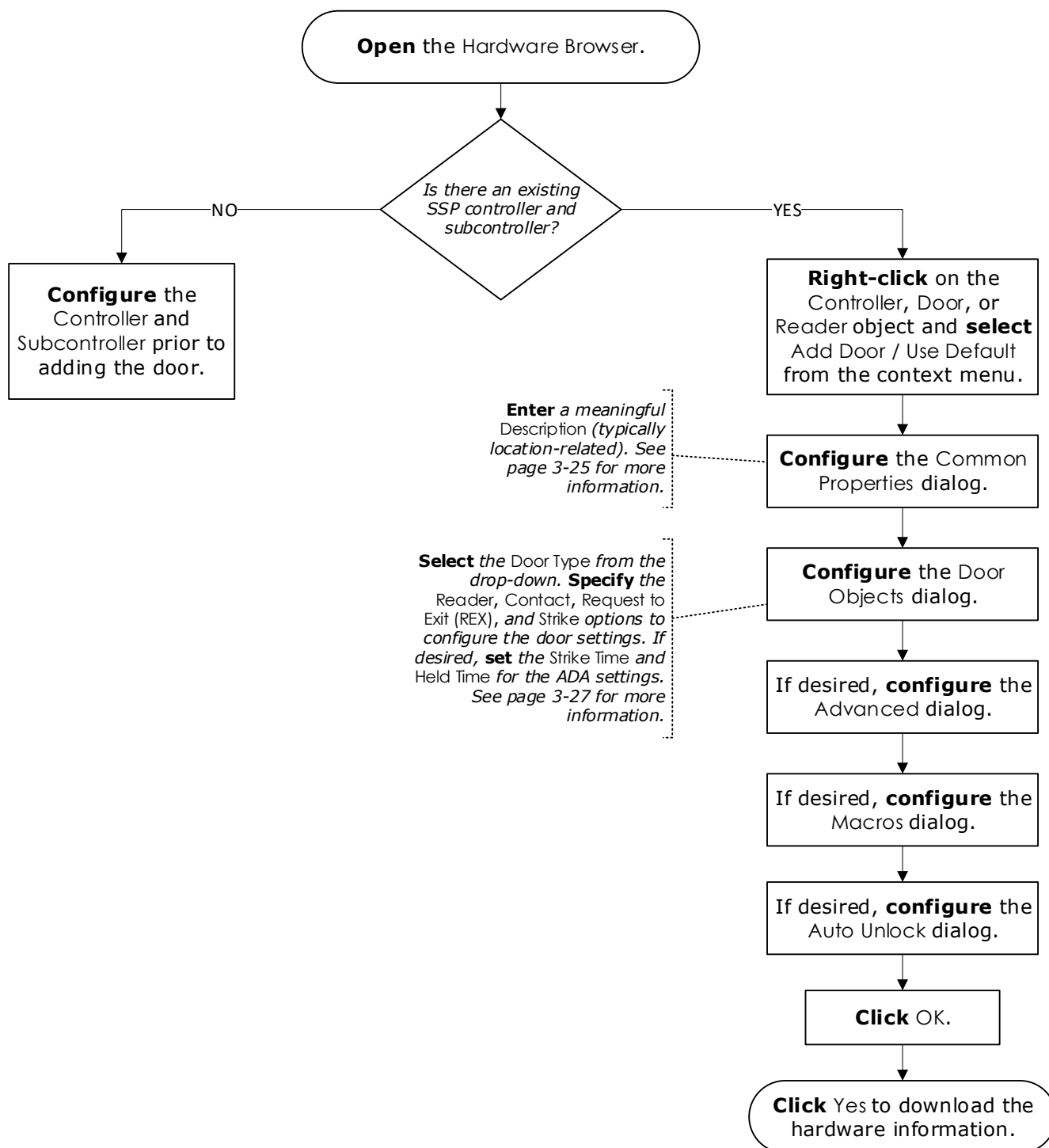
Adding Hardware Guide



Adding a Controller and Bringing it Online

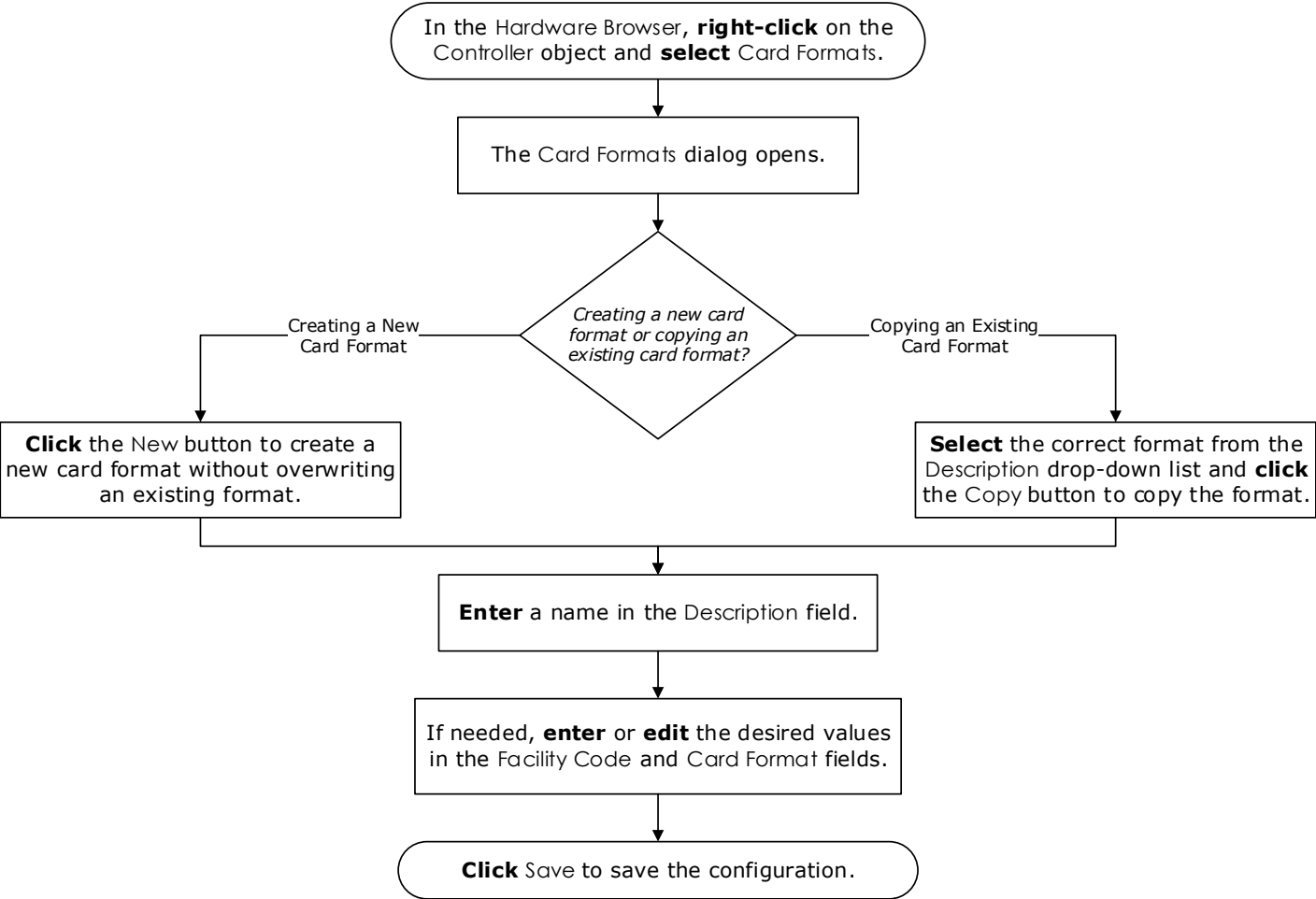


Bringing a Door Online

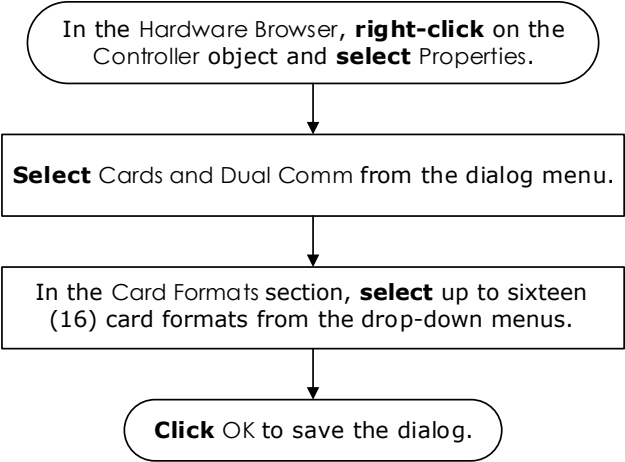


Configuring Card Formats

STEP #1: CREATE A CARD FORMAT



STEP #2: ASSIGN CARD FORMAT TO CONTROLLER



Command Line Parameters



PARAMETER	DESCRIPTION	DEFAULT
/FORCENEW	Forces the system to ignore existing settings and act like a new install.	
/FORCEDBU	Forces the DNAUpdates.sql to run on an upgrade.	
/NOHASP	Does not try to install the HASP drivers.	
/NOBONJOUR	Does not try to install the Bonjour service.	
/NONATIVE	Does not try to install the SQL Native Client. If this is present it uses old style SQL Server drivers.	
/INSTTYPE=xxxx	Full = Full Client; Client = Standard Client	
/SILENT	Shows the install progress dialog, but there is no interaction with the user except for the cancel button (unless you use /NOCANCEL).	
/VERYSILENT	No visual indicators and no interaction with user.	
/NOCANCEL	If using /SILENT, disables the cancel button so the user cannot stop the install.	
/PASSWORD=xxxxx	If the install is password protected, this allows you to specify the password for automated installs.	
Client Installations Only		
/SERVER=xxxx	Sets the name of the DNA Server.	
/SHARE=xxxx	Sets the name of the share on the DNA Server.	DNAShare
Server Installations Only		
/SQLINST=xxxxx	Sets the SQL Instance name to xxxxx, i.e. server-name\instancename or servername - On.	LocalMachineName\OpenOptions
/SQLDB=xxxxx	Sets the database name to xxxxx.	DNAFusion
/SQLMODE=x	0=New Instance, 1=Existing Server, 2=Existing DB	New Instance (0)
/SQLUSER=xxxxx	If using SQL Authentication, this is the username.	Use Windows Authentication
/SQLPWD=xxxxx	If using SQL Authentication, this is the password.	Use Windows Authentication
/PUSH	Enables push updates.	Not Enabled

Examples:

Install a client for an existing server (OO-DEV-XP-CL):

```
C:\>setup / INSTTYPE=CLIENT / SILENT / SERVER=OO-DEV-XP-CL / PASSWORD=6f6=m_kS / NOCANCEL
```

Install a new server that already has a SQL Server:

```
C:\>setup / INSTTYPE=FULL / VERYSILENT / SQLINST=OO-DEV-XP-CL / OpenOptions /  
SQLDB=DNAFusion / SQLMODE=1
```

This Page Intentionally Left Blank

Index



A

- Access Levels Per Card 3-14
- AD 300 3-17
- Alternate Priority 3-28, 3-40, 3-48, 3-52
- Anti-Pass Back Settings 3-31, 3-42
- Auto Activate 3-27, 3-39
- Auto Deactivate 3-27, 3-39
- AutoExpire Tool 5-1, 5-7
 - Configuration Mode 5-7
 - Silent Mode 5-7

B

- Batch Processing 3-15

C

- Cameras (IP Based)
 - Adding 3-57
- Card Formats 3-15, 3-57
 - Assigning 3-58
 - Copying 3-57
- Channel
 - Adding 3-5
 - Modem Channel 3-8
 - Serial Channel 3-8
 - TCP/IP Channel 3-7
- Client 2-1
- Client Installation 2-17
 - Standard Client Installation 2-17
- Client Specifications
 - DNA Client Workstation 2-5
 - DNA Client Workstation with Photo ID 2-5
- Computer Specifications
 - Client Specifications 2-5
 - Server Specifications 2-3
- Configuring Hardware 3-1
- Controller
 - Adding 3-9
 - GMT Offset 3-9
 - Holiday Set 3-12
 - Physical Address 3-9, 3-11
 - Properties
 - Cards & Dual Comm 3-15
 - Controller Properties 3-11
 - Stored Quantities 3-13
 - Time Schedule Set 3-12
 - Use Daylight Savings 3-9, 3-12
- Controller Flags 3-13
- Controller Memory 3-13

D

- Database Permissions 2-15
- Database Server Configuration 2-10
 - Existing Database 2-10
 - Existing Server 2-10
- Daylight Savings 3-9, 3-12
- Digital Video Recorder
 - Add Cameras 3-55
 - Adding 3-53
 - Authentication Mode 3-54
 - Configure 3-54
- DNA Batch Download Settings Utility 5-1, 5-6
- DNA Event History Report Utility 5-9
 - Email Setup 5-9
 - Parameters 5-10
 - Scheduling 5-11
- DNA Import Tool 5-1, 5-18
 - Permissions 5-20
 - Running 5-19
- DNA LED Control Application 5-1, 5-6
- DNA Time and Attendance Report 5-13
 - Generating 5-17
 - Installation 5-13
- DNA Users Group 2-13
- Domain User Group Setup 2-8
- Door
 - Adding 3-23
 - From a Reader 3-26
 - In & Out 3-24
 - Single Door 3-23
 - Properties
 - Advanced 3-31
 - Common Properties 3-27
 - Door Objects 3-29
 - Macros 3-33
- Doors
 - Alternate Priority 3-28, 3-40
 - Anti-Pass Back (APB) Settings 3-31
 - In & Out 3-24
 - Situation Level Manager 3-27
- Duress Digit 3-14
- Duress PIN Mode 3-14

E

- Elevator
 - Adding 3-37
 - Properties 3-39
 - Common Properties 3-39
 - Elevator Objects 3-41
- Elevator Control 3-14
- Elevators
 - Anti-Pass Back (APB) Settings 3-42
 - Floor Groups 3-41
 - Non-Feedback 3-37
- Event History Report Utility 5-1
- Existing Database 2-10
- Existing Server 2-10

F

Facility Code 3-57, 3-58
Firewall Configuration 2-19
Full Server / Client Installation 2-9

G

GMT Offset 3-9, 3-12
GTWY 3-17

H

Hardware
 Adding Hardware 3-3
 Site 3-3
Hardware Browser
 Configuring 3-1
 Opening 3-1
HASP Key 2-10, 4-5
Held Time 3-29
Holiday Set 3-12

I

Input Point
 Properties
 Common Properties 3-47
 Input Properties 3-48
Input Points
 Alternate Priority 3-48, 3-52
 Circuit Type 3-49
 Configuring 3-47
 Sensitivity 3-49
Installation
 Server 2-9
Installation Types 2-1
 Client 2-1
 Server 2-1
Instance Name 4-2, 4-3, 4-4

K

Keypad Mode 3-46

L

LED Control Application 5-6
License File 2-11, 4-5
License Updates 4-4
Licensing 2-10

M

Match Physical 3-19
Migrating 2-25
Migrating DNA Fusion 2-25
 Same Workstation 2-29
 Separate Workstations 2-30
Muster 3-27, 3-39

N

Network Requirements 2-7

Network Video Recorder (NVR). See Digital Video Recorder

New Server 2-29

NSC-100 3-17

O

ODBC Data Sources 2-20

Output Point

Properties

Common Properties 3-51

Output Properties 3-52

Output Points

Default Mode 3-52

Momentary Time 3-52

P

Physical Address 3-11, 3-19

PIM400-485 3-17

R

Reader

Properties

Common Properties 3-45

Reader Properties 3-46

Readers

Configuring 3-45

Reverse Polling on Inputs 3-21

S

Server 2-1

Server/Client Requirements 2-7

Network Requirements 2-8

User Group Setup 2-7

Server Configuration 2-13

Administrative Rights Account Assignment 2-13

Component Services 2-13

DNA Driver 2-13

Database Permissions 2-15

DNA Users Group 2-13

Windows 2003 Server 2-21

Windows 2008 Server 2-21

Server Installation 2-9

Existing Database 2-10

Existing Server 2-10

Full Server/Client Installation 2-9

Standard Server Installation 2-9

Server Specifications

DNA Server (Stand-Alone) with SQL Express Database 2-3

DNA Server with SQL Express Database 1 to 4 clients 2-3

Service Pack 4-1

Site

Creating 3-3

Linking 3-4

Situation Level Manager 3-27

SMTP Mailer 5-1

Soft Key 2-10, 4-5

Software Upgrades

Client 4-3

NPowerDNA 4-4

- Service Pack 4-1
- SQL Server Express 2-3
- SSP. *See* Controller
- Standard Server Installation 2-9
- Store Temporary Upgrade Date 3-13
- Store Vacation Date 3-13
- Strike Activation 3-30
- Subcontroller Firmware 3-21
 - Updating 3-21
- Subcontrollers
 - Adding 3-17
 - Physical Address 3-19
 - Properties
 - Advanced 3-21

T

- Table Purger Tool 5-1, 5-3
 - Run 5-5
- Time and Attendance In 3-27, 3-39
- Time and Attendance Out 3-27, 3-39
- Time & Attendance Report 5-1
 - Generating 5-17
 - Installing 5-13
 - Setting up 5-14
- Time Schedule Set 3-12
- Toolbars
 - Hardware 3-2

U

- Upgrades 4-1, 4-3
- User Group Setup
 - Domain User Group Setup 2-8
 - Local Domain Setup 2-8

W

- Windows 2008 Server 2-21

This Page Intentionally Left Blank

