DNA Fusion™ is a trademark of Open Options, Inc.

The DNA Fusion™ Access Control and Security Management System uses equipment that generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this installation manual, 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 the user’s expense.

The DNA Fusion™ Access Control and Security Management System 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 is proprietary information of Open Options, Inc.

Unauthorized reproduction or distribution of this manual is strictly forbidden without the written consent of Open Options, Inc.

The information contained within this manual is for informational purposes only and is subject to change at any time without notice.

Open Options, Inc. assumes no responsibility for incorrect or outdated information that may be contained in this publication.

This manual has been written for DNA Fusion™ version 5.4 or higher

Print Date: April 20, 2012
Manual Number: D-TI5.4.1

©Copyright 2002-2012 Open Options, Inc. 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.
Open Options, Inc. Software License Agreement and Warranty

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

DEFINITIONS: Open Options shall mean Open Options, Inc., 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, Inc., 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 and acceptance of the software package, 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. 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 ninety (90) days 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. This warranty is void if the media defect has resulted from accident, abuse, or misapplication. Open Options does not warrant that the Software will meet the end user customer requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTIES ARE THE ONLY WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. 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 & Conventions Used in this Manual ................................................ 1-1

Chapter 2: Installation
Installation Types .................................................................................. 2-1
Computer Specifications ......................................................................... 2-3
Server Specifications .............................................................................. 2-3
   DNA Server (Stand Alone) w/SQL Express Database .......................... 2-3
   DNA Server PC w/SQL Express Database 1 to 4 Clients* ................. 2-3
   DNA Enterprise Server PC w/SQL Server Database ....................... 2-4
Client Specifications .............................................................................. 2-5
   DNA Client Workstation .................................................................. 2-5
   DNA Client Workstation w/Photo ID .............................................. 2-5
Server / Client Requirements ............................................................... 2-6
Network Requirements .......................................................................... 2-6
User Group Setup ................................................................................. 2-6
   Domain User Group Setup (DNA_Global) ..................................... 2-6
   Local Domain Setup ...................................................................... 2-6
Server Installation & Configuration ....................................................... 2-7
Installation ......................................................................................... 2-7
Server Configuration ........................................................................... 2-11
   Administrative Rights Account Assignment .................................. 2-11
   Adding Users to the DNA Users Group ..................................... 2-12
   Component Services Default Permissions ................................... 2-13
   Testing the Settings ..................................................................... 2-13
   Database Permissions .................................................................. 2-14
Fusion Software Upgrades ................................................................... 2-14
Client Installation ................................................................................ 2-15
Installation ......................................................................................... 2-15
Firewall Configuration .......................................................................... 2-17
Configuring ODBC Data Sources .......................................................... 2-18
Installing DNAFusion on a 64-bit OS ...................................................... 2-19
Configuring a Windows 2003 Server ......................................................... 2-21
Configuring a Windows 2008 Server ......................................................... 2-22
Migrating DNA Fusion to a New Server .................................................. 2-24
   Migrating with Server/Client Components on the Same Workstation 2-24
   Migrating with Server and Client Components on the Separate Workstations 2-25

Chapter 3: Hardware Configuration
Configuring Hardware ......................................................................... 3-1
The Hardware Browser ......................................................................... 3-1
<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the Browser ........................................................................................................... 3-1</td>
</tr>
<tr>
<td>Hardware Toolbar ......................................................................................................................... 3-2</td>
</tr>
<tr>
<td>Adding Hardware .......................................................................................................................... 3-3</td>
</tr>
<tr>
<td>Creating and Linking a Site ......................................................................................................... 3-3</td>
</tr>
<tr>
<td>Creating a Site ............................................................................................................................. 3-3</td>
</tr>
<tr>
<td>Linking to a Site ......................................................................................................................... 3-4</td>
</tr>
<tr>
<td>Adding a Channel .......................................................................................................................... 3-5</td>
</tr>
<tr>
<td>Serial Channel ............................................................................................................................. 3-6</td>
</tr>
<tr>
<td>TCP/IP Channel ............................................................................................................................ 3-6</td>
</tr>
<tr>
<td>Modem Channel ............................................................................................................................ 3-6</td>
</tr>
<tr>
<td>Adding an SSP (Controller) .......................................................................................................... 3-7</td>
</tr>
<tr>
<td>Controller Properties .................................................................................................................... 3-9</td>
</tr>
<tr>
<td>Controller Properties .................................................................................................................... 3-9</td>
</tr>
<tr>
<td>Attributes .................................................................................................................................... 3-9</td>
</tr>
<tr>
<td>Controller Time Parameters ........................................................................................................ 3-9</td>
</tr>
<tr>
<td>Connection ................................................................................................................................... 3-10</td>
</tr>
<tr>
<td>Downstream Ports ....................................................................................................................... 3-10</td>
</tr>
<tr>
<td>Stored Quantities .......................................................................................................................... 3-11</td>
</tr>
<tr>
<td>Controller Memory ....................................................................................................................... 3-11</td>
</tr>
<tr>
<td>Offline Transaction Capacity ....................................................................................................... 3-11</td>
</tr>
<tr>
<td>Controller Flags .......................................................................................................................... 3-11</td>
</tr>
<tr>
<td>Quantities .................................................................................................................................... 3-11</td>
</tr>
<tr>
<td>Elevator Control ........................................................................................................................... 3-12</td>
</tr>
<tr>
<td>PIN and Duress Options ............................................................................................................... 3-12</td>
</tr>
<tr>
<td>Cards &amp; Dual Comm ....................................................................................................................... 3-13</td>
</tr>
<tr>
<td>Card Formats (Personnel) ............................................................................................................. 3-13</td>
</tr>
<tr>
<td>Alternate Ports ............................................................................................................................. 3-13</td>
</tr>
<tr>
<td>Batch Processing ......................................................................................................................... 3-13</td>
</tr>
<tr>
<td>Adding Subcontrollers ................................................................................................................. 3-14</td>
</tr>
<tr>
<td>Subcontroller Properties ............................................................................................................. 3-15</td>
</tr>
<tr>
<td>Sub-Controller .............................................................................................................................. 3-15</td>
</tr>
<tr>
<td>Address ....................................................................................................................................... 3-15</td>
</tr>
<tr>
<td>Attributes ..................................................................................................................................... 3-15</td>
</tr>
<tr>
<td>Type/Preview ............................................................................................................................... 3-15</td>
</tr>
<tr>
<td>Alarm Text ................................................................................................................................... 3-15</td>
</tr>
<tr>
<td>Advanced ..................................................................................................................................... 3-16</td>
</tr>
<tr>
<td>Advanced Properties .................................................................................................................... 3-16</td>
</tr>
<tr>
<td>Continuations ............................................................................................................................... 3-16</td>
</tr>
<tr>
<td>Identification ............................................................................................................................... 3-16</td>
</tr>
<tr>
<td>Updating Subcontroller Firmware ............................................................................................... 3-16</td>
</tr>
<tr>
<td>Adding Doors ............................................................................................................................... 3-17</td>
</tr>
<tr>
<td>Adding a Single Door .................................................................................................................... 3-17</td>
</tr>
<tr>
<td>Adding an In &amp; Out Door ............................................................................................................. 3-18</td>
</tr>
<tr>
<td>Adding a Door From a Reader ...................................................................................................... 3-19</td>
</tr>
<tr>
<td>Door Properties ............................................................................................................................ 3-21</td>
</tr>
<tr>
<td>Common Properties ...................................................................................................................... 3-21</td>
</tr>
<tr>
<td>Address ....................................................................................................................................... 3-21</td>
</tr>
<tr>
<td>Other .......................................................................................................................................... 3-21</td>
</tr>
</tbody>
</table>
Point Alarm Properties ................................................................. 3-22
Door Objects .................................................................................. 3-23
   Door Parameters ......................................................................... 3-23
   Reader ....................................................................................... 3-23
   Contact ....................................................................................... 3-24
   Request to Exit (REX) ................................................................. 3-24
   Strike ......................................................................................... 3-24
   ADA Settings ........................................................................... 3-24
Advanced ......................................................................................... 3-25
   Anti-Pass Back (APB) Settings ................................................... 3-25
   Door Parameters ......................................................................... 3-25
   Logging Based on Deny Violations ............................................. 3-26
   Secondary Request to Exit (REX) ................................................ 3-26
   Secondary (Biometric) Reader .................................................... 3-26
Macros ............................................................................................. 3-27
   Door Sounder ............................................................................ 3-27
   Alarm Conditions ...................................................................... 3-27
   Normal Conditions .................................................................... 3-27
Follows Schedule .......................................................................... 3-28
Adding Elevators ........................................................................... 3-29
Elevator Properties .......................................................................... 3-31
   Common Properties ...................................................................... 3-31
      Address .................................................................................. 3-31
      Other ..................................................................................... 3-31
      Point Alarm Properties .......................................................... 3-32
   Elevator Objects ......................................................................... 3-33
      Elevator Parameters ............................................................... 3-33
      Reader .................................................................................... 3-33
      Inputs & Outputs .................................................................... 3-33
      Floor Groups ......................................................................... 3-33
      Secondary (Biometric) Reader ................................................ 3-33
      Elevator Parameters ............................................................... 3-35
      Attributes ............................................................................... 3-35
      Anti-Pass Back (APB) ............................................................... 3-35
      Elevator Functions ................................................................. 3-35
   Follows Schedule ....................................................................... 3-36
Configuring Readers ....................................................................... 3-37
Reader Properties ........................................................................... 3-37
   Common Properties ...................................................................... 3-37
      Address .................................................................................. 3-37
      Distribution / Other ................................................................. 3-37
   Reader Properties ....................................................................... 3-38
      Reader Properties ..................................................................... 3-38
      Card Data Format .................................................................... 3-38
      Advanced Properties .............................................................. 3-38
      Templates ................................................................................ 3-38
Configuring Input Points ............................................................... 3-39
Input Properties ............................................................................. 3-39
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Properties ...........................................................................</td>
<td>3-39</td>
</tr>
<tr>
<td>Address</td>
<td>3-39</td>
</tr>
<tr>
<td>Distribution / Other</td>
<td>3-39</td>
</tr>
<tr>
<td>Alarm Properties</td>
<td>3-39</td>
</tr>
<tr>
<td>Input Properties</td>
<td>3-41</td>
</tr>
<tr>
<td>Input Point Properties</td>
<td>3-41</td>
</tr>
<tr>
<td>Advanced Features</td>
<td>3-42</td>
</tr>
<tr>
<td>Templates</td>
<td>3-42</td>
</tr>
<tr>
<td>Configuring Output Points</td>
<td>3-43</td>
</tr>
<tr>
<td>Output Properties</td>
<td>3-43</td>
</tr>
<tr>
<td>Common Properties</td>
<td>3-43</td>
</tr>
<tr>
<td>Address</td>
<td>3-43</td>
</tr>
<tr>
<td>Distribution / Other</td>
<td>3-43</td>
</tr>
<tr>
<td>Alarm Properties</td>
<td>3-43</td>
</tr>
<tr>
<td>Output Properties</td>
<td>3-44</td>
</tr>
<tr>
<td>Output Properties</td>
<td>3-44</td>
</tr>
<tr>
<td>Advanced Features</td>
<td>3-44</td>
</tr>
<tr>
<td>Adding DVRs</td>
<td>3-45</td>
</tr>
<tr>
<td>DVR Integration</td>
<td>3-45</td>
</tr>
<tr>
<td>Configure the DVR</td>
<td>3-46</td>
</tr>
<tr>
<td>Add the Cameras</td>
<td>3-47</td>
</tr>
<tr>
<td>Associating a DVR Camera to a Door</td>
<td>3-47</td>
</tr>
<tr>
<td>Adding Cameras</td>
<td>3-48</td>
</tr>
<tr>
<td>Associating a Camera to a Door</td>
<td>3-48</td>
</tr>
<tr>
<td>Card Formats</td>
<td>3-49</td>
</tr>
<tr>
<td>Creating a Card Format</td>
<td>3-49</td>
</tr>
<tr>
<td>Creating a New Card Format</td>
<td>3-49</td>
</tr>
<tr>
<td>Copying a Card Format</td>
<td>3-49</td>
</tr>
<tr>
<td>Editing a Card Format</td>
<td>3-49</td>
</tr>
<tr>
<td>Gathering Card Format Information</td>
<td>3-50</td>
</tr>
<tr>
<td>Assigning a Card Format to the SSP</td>
<td>3-50</td>
</tr>
</tbody>
</table>

**Chapter 4: Upgrading DNA**

Software Upgrades ................................................................. 4-1
NPower DNA to DNA Fusion 5.0 and above ................................ 4-1
DNA Fusion Service Pack ......................................................... 4-3
Fusion Client Upgrades ........................................................... 4-4
License Updates ........................................................................... 4-5

**Chapter 5: Additional Apps**

Table Purger Tool ........................................................................ 5-3
DNA Batch Download Settings Utility ........................................... 5-4
DNA LED Control Application ....................................................... 5-4
SMTP Mailer .................................................................................. 5-5
Installation .................................................................................... 5-5
Configuration ................................................................................ 5-5
Running the Program .................................................................... 5-6
Exiting the Program ....................................................................... 5-6
Remote Archive Utility .................................................................. 5-7
Table of Contents

Installation ............................................................................................................................ 5-7
Configuring the Remote Archive Utility ................................................................. 5-8
Running the Program ............................................................................................... 5-9
Scheduling the NPowrDNA Remote Archive Utility .............................................. 5-9
AutoExpire Tool ........................................................................................................ 5-11
                                          Running the Configuration Mode .................................................. 5-11
                                          Running the Silent Mode ........................................................................ 5-11
DNA Event History Report Utility ......................................................................... 5-13
Email Setup ................................................................................................................ 5-13
Configuring the Event History Report Parameters ........................................... 5-14
Scheduling a Report .................................................................................................. 5-15
   Edit a Scheduled Report ........................................................................................ 5-15
   Delete a Scheduled Report ..................................................................................... 5-15
DNA Time and Attendance Report ........................................................................ 5-17
Installing the Time & Attendance Report ............................................................. 5-17
Setting up the Time & Attendance Report ............................................................. 5-18
Generating a Time & Attendance Report ............................................................... 5-21
DNA Import Tool ...................................................................................................... 5-23
                                          Running the Import Tool ........................................................................ 5-23
Permissions Issues ..................................................................................................... 5-24

Appendix A: Troubleshooting
Testing Communication from SSP to Computer ..................................................... A-1
Unable to Bring SSP Controller Online - Ethernet Configuration ....................... A-3
Unable to Bring SSP Controller Online - Serial Configuration .............................. A-5
COM Surrogate Errors ............................................................................................. A-7
Starting and Stopping the Services ......................................................................... A-7
   Driver .................................................................................................................... A-7
   SQL Server .......................................................................................................... A-7

Appendix B: Process Diagrams
DNAFusion Server Installation ................................................................................. B-1
DNA Fusion Client Installation ............................................................................... B-3
Server/Client Setup ................................................................................................... B-4
Adding Hardware Guide ......................................................................................... B-5
Adding a Controller and Bringing it On-line ........................................................ B-6
Bringing a Door On-line ......................................................................................... B-7
Configuring Card Formats ...................................................................................... B-8
This Page Intentionally Left Blank
This section is designed to introduce you to DNA Fusion™ and explain the installation and hardware setup.

**HOW THIS SECTION IS ORGANIZED**

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


Chapter 2, “Installation,” covers the software side of the installation including both the server and client workstations as well as the configuration steps. This chapter also provides information about the requirements and specifications for each configuration type.

Chapter 3, “Hardware Configuration,” provides instruction on the hardware setup within the DNA Fusion software.

Chapter 4, “DNA Upgrades,” information on upgrading the DNA system.

Chapter 5, “Additional Apps” provides information on the additional applications that compliment the DNAFusion system.

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

Appendix B, ” Process Diagrams”

**ICONS AND CONVENTIONS USED IN THIS MANUAL**

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

- [ ] This icon highlights time-saving hints, helpful shortcuts, and advice that you’ll find especially helpful.

- [i] This icon marks information that is important enough for you to keep it filed in an easily accessible portion of your gray matter.

- [!] If something you’re doing could damage the system, end up costing big bucks, lock you out of the system, or otherwise bring an end to civilization as we know it, you’ll find it highlighted with the icon.

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

Small icons - such as [ ], [ ], etc.: These icons indicate buttons and/or symbols that you can select or click to make something happen.
A Special Font: Text that look like this indicates a menu item, toolbar selection, button, or a message from the system.

Boldface: Boldface text, which usually appears in numbered steps, tells you about specific actions that you should take.
The DNA Fusion™ installation process is very straightforward and can be performed without any knowledge of the software. Before installing please verify the computer meets the minimum requirements outlined on page 2-3 through 2-5 of this chapter.

This chapter addresses the installation of the DNA Fusion software on both Server and Client machines.

**Installation Types**

There are two types of installation covered in this chapter:

- **Server** - The PC that will host the DNA Fusion database and run the DNA driver.
  - The Servers role may be separated into: a Database Server & an Application Server.
- **Client** - A PC that is connected to the DNA system via the LAN/WAN but retrieves and saves data to and from the DNA server.

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 procedures must be performed for the Database Server prior to any Client machines being setup.**

**If you are installing DNA Fusion on a Windows 2003 or 2008 Server, follow the procedure described on page 2-21 for 2003 Server or 2-22 for 2008 Server configuration steps.**

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

DNAFusion is not supported on any Home version of Windows Operating Systems.

**Server Specifications**

The following configuration specifications are designed as guidelines for configuring your DNA server. The DNA server in this instance refers to the PC that will host your DNA database.

**DNA Server (Stand Alone) w/SQL Express Database**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Recommended Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Speed</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>System Memory (RAM)</td>
<td>2 GB</td>
</tr>
<tr>
<td>Network Card</td>
<td>10/100 Ethernet Network Card</td>
</tr>
<tr>
<td>Hard Drive Size</td>
<td>100 GB</td>
</tr>
<tr>
<td>Graphics Card</td>
<td>VGA Support for 1024x768 Resolution</td>
</tr>
<tr>
<td>Video Memory</td>
<td>128 MB</td>
</tr>
<tr>
<td>Backup Device</td>
<td>YES</td>
</tr>
<tr>
<td>CD-RW Drive</td>
<td>YES</td>
</tr>
<tr>
<td>Optional</td>
<td>UPS (Uninterrupted Power Supply)</td>
</tr>
</tbody>
</table>

- This specification is ideal for systems with less than 20 doors, 200 cardholders, or 1,000 transactions per day.
- DNA ships with a Microsoft SQL 2008 Express database for 32-bit systems. SQL Express has a limit of 10 GB database size.

**DNA Server PC w/SQL Express Database 1 to 4 Clients***

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Recommended Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Speed</td>
<td>3 GHz</td>
</tr>
<tr>
<td>System Memory (RAM)</td>
<td>4 GB</td>
</tr>
<tr>
<td>Network Card</td>
<td>10/100 Ethernet Network Card</td>
</tr>
<tr>
<td>Hard Drive Size</td>
<td>250 GB</td>
</tr>
<tr>
<td>Graphics Card</td>
<td>VGA Support for 1024x768 Resolution</td>
</tr>
<tr>
<td>Video Memory</td>
<td>128 MB</td>
</tr>
<tr>
<td>Backup Device</td>
<td>YES</td>
</tr>
<tr>
<td>CD-RW Drive</td>
<td>YES</td>
</tr>
<tr>
<td>Optional</td>
<td>Mirrored Hard Drives&lt;br&gt;Multi-Processor&lt;br&gt;UPS (Uninterrupted Power Supply)</td>
</tr>
</tbody>
</table>

- DNA ships with a Microsoft SQL 2008 Express database for 32-bit systems. SQL Express has a limit of 10 GB database size.

* Concurrent client workstations connected to the system at any given time.
**DNA Enterprise Server PC w/SQL Server Database**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Recommended Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Speed</td>
<td>3.4 GHz</td>
</tr>
<tr>
<td>Dual Processor</td>
<td>Yes</td>
</tr>
<tr>
<td>System Memory (RAM)</td>
<td>4 GB+</td>
</tr>
<tr>
<td>Network Card</td>
<td>10/100 Ethernet Network Card</td>
</tr>
<tr>
<td>Hard Drive Size</td>
<td>250 GB</td>
</tr>
<tr>
<td>Graphics Card</td>
<td>VGA Support for 1024x768 Resolution</td>
</tr>
<tr>
<td>Video Memory</td>
<td>128 MB</td>
</tr>
<tr>
<td>Backup Device</td>
<td>YES</td>
</tr>
<tr>
<td>CD-RW Drive</td>
<td>YES</td>
</tr>
<tr>
<td>Operating System</td>
<td>Microsoft Windows 2003 &amp; 2008 Server</td>
</tr>
</tbody>
</table>

**Optional**

- Separate Database & Application Servers*
- UPS (Uninterrupted Power Supply)
- Isolated DB Server/App Server
- Multi-Processor

- This specification is designed for high traffic (transaction) systems and systems requiring multiple client database connections.
- MS SQL Server is required to be installed on the PC prior to installing DNA Fusion.
*MS SQL Server may be installed on another (dedicated) computer prior to the installation of DNA Fusion and identified during the DNA Fusion install.

---

**Open Options does not distribute SQL 2008 Express for 64-bit Windows Operating systems. It is the customer’s responsibility to provide this component on 64-bit systems and install prior to installing DNA Fusion. SQL 2008 Express is available as a free download at the Microsoft website.**

**Client Specifications**

The following configuration specifications are designed as guidelines for configuring your DNA client workstations. A client workstation is defined as a PC that is connected to the DNA system via the LAN/WAN but retrieving and saving data to and from the DNA Server.

### DNA Client Workstation

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Recommended Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Speed</td>
<td>2 GHz</td>
</tr>
<tr>
<td>System Memory (RAM)</td>
<td>1 GB</td>
</tr>
<tr>
<td>Network Card</td>
<td>10/100 Ethernet Network Card</td>
</tr>
<tr>
<td>Hard Drive Size</td>
<td>60 GB</td>
</tr>
<tr>
<td>Graphics Card</td>
<td>VGA Support for 1024x768 Resolution</td>
</tr>
<tr>
<td>Video Memory</td>
<td>64 MB</td>
</tr>
<tr>
<td>Backup Device</td>
<td>NO</td>
</tr>
<tr>
<td>CD-ROM Drive</td>
<td>YES</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows XP Professional/Vista Business or Enterprise/Windows 7</td>
</tr>
<tr>
<td>Monitor</td>
<td>17 inch color (capable of 1024x768)</td>
</tr>
<tr>
<td>Optional</td>
<td>UPS (Uninterrupted Power Supply)</td>
</tr>
</tbody>
</table>

### DNA Client Workstation w/Photo ID

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Recommended Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor Speed</td>
<td>2 GHz</td>
</tr>
<tr>
<td>System Memory (RAM)</td>
<td>2 GB</td>
</tr>
<tr>
<td>Network Card</td>
<td>10/100 Ethernet Network Card</td>
</tr>
<tr>
<td>Hard Drive Size</td>
<td>60 GB</td>
</tr>
<tr>
<td>Graphics Card</td>
<td>VGA Support for 1024x768 Resolution</td>
</tr>
<tr>
<td>Video Memory</td>
<td>128 MB</td>
</tr>
<tr>
<td>Video Capture Device</td>
<td>YES (TWAIN Compliant)</td>
</tr>
<tr>
<td>USB Port</td>
<td>YES (if using USB capture device)</td>
</tr>
<tr>
<td>Backup Device</td>
<td>NO</td>
</tr>
<tr>
<td>CD-ROM Drive</td>
<td>YES</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows XP Professional/Vista Business or Enterprise/Windows 7 (Badge Production is not supported on Windows Server Operating Systems)</td>
</tr>
<tr>
<td>Monitor</td>
<td>17 inch color (capable of 1024x768)</td>
</tr>
<tr>
<td>Optional</td>
<td>UPS (Uninterrupted Power Supply)</td>
</tr>
</tbody>
</table>

NOTE: If Photo ID Client is to be installed on a LAPTOP computer, ensure 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 featuring smart chip technology. Please see printer documentation for more information.

- TWAIN devices must be complaint with DirectX 9.
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 / client requirements are meant 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 has certain network requirements that must be met for it to operate in a client/server environment. Any of the following network scenarios are acceptable for this operation:

- All DNA computers (servers and client workstations) MUST be members of the same Windows domain regardless of what other applications are operating on the domain.
- All DNA computers are members of a dedicated Windows domain.
- DNA computers can be members on different Windows domains, but each domain MUST have an established bi-directional trust in place.
- DNA computers can be members on different Windows domains, but each domain MUST be managed under Windows Active Directory Service or a master domain.
- All DNA computers are members of a single dedicated workgroup without a Windows domain.

A few things to consider with this option are:

- 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.

User Group Setup

The following steps are typically completed by the System Administrator.

Domain User Group Setup (DNA_Global)

Prior to installing the DNA Fusion software, a domain user group needs to be created.

1. Create a global domain user group and call it 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 2-12 for more information.

Local Domain Setup

Prior to a new DNA operator being added, they must be added to the DNA_Global Domain Group.

1. Create a Windows login for the new operator, if it does not already exist.
2. Add the operators login to the DNA_Global Domain Group by selecting My Network Places / Entire Network and then locate the server.
4. Add the user and configure their rights to allow access.
5. Add the operator to DNA Fusion.
   See Chapter 4: DNA Operators in the Users Manual for more information.

What is a domain? A domain is a subnetwork made up of a group of clients and servers under the control of one central security database. Within a domain, users authenticate once to a centralized server known as a domain controller, rather than repeatedly authenticating to individual servers and services. Individual servers and services accept the user based on the approval of the domain controller.
Server Installation & Configuration

The following instructions are for XP, Windows 2003/2008 Server, Vista (32-bit OS) and Windows 7. If the server has a 64-bit OS and will be installing SQL Express 2008, see page 2-19. If using SQL Server, it must be installed prior to the installation of DNA Fusion.

Installation

1. **Insert** the DNA Fusion CD into the computer or download the install from the Open Options website. The installation process will start automatically and the Welcome screen will be displayed.

2. When the Welcome Screen appears, **click** Next to begin the installation.

![Welcome Screen](image)

The License Agreement screen will appear.

3. **Read** the License Agreement and **select** the I accept the agreement radiobutton and **click** Next to continue.

   If the I do not accept the agreement radiobutton is selected, **Cancel** and **Back** will be the only available options.

   The User Information dialog box appears.

4. If desired, **change** the User Name/Organization Information and **click** Next.

   The File Location screen is displayed.

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

   Default Location: C:\Program Files\NPowerDNA

   The Component Selection screen appears.

6. **Select** the correct 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 stand alone server. No client components will be installed.

   ![Component Selection](image)

   The Database Server Options screen will appear.
7. **Select** the radiobutton next to the appropriate Database Server Configuration and **click** Next.
   - **Install Separate Instance** - Installs SQL Server Express 2005 and creates the Fusion database. Continue to step 8.

   ![Select the radiobutton next to the correct Database Server Configuration option.](image)

   - **Existing Server** - Creates the Fusion database only; requires an existing version of SQL Server be installed on the host computer prior to the DNA Fusion installation. Continue to step a.
   - **Existing Database** - **Select** if an existing DNA database will be used on an existing SQL Server. Both components must be in place prior to the Fusion install. Continue to step a.

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

   ![Select the SQL Server Instance from the list.](image)

   ![Click the Test Connect button to verify the connection to the SQL Server. Click the Next button to continue the installation.](image)

   If Existing Server was selected, the Start Menu Folder screen will appear. Continue to step 8.

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

   b. From the Select Database drop down list, **select** the nPowerDNA database and **click** Next. Open Options recommends the Apply upgrade script checkbox be left checked. This will upgrade the existing database and write any new fields that are included in the version.

   ![Select the nPowerDNA database from the drop down list.](image)

8. **Click** the Next button and select the Licensing option.
   A unique system ID number is generated.
   - **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. Internet connection required.
   - **License File** - **Install** the License File provided by Open Options prior to installation. No internet connection required.
9. **Click** the Next button to create the default shortcut in the Start Menu or **click** the Browse button **select** another folder.
   The Select Additional Tasks dialog appears.

![Select Additional Tasks](image1)

10. If desired, **select** the Create a desktop icon checkbox.
    The Windows Firewall 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; contact Open Options Technical Support for more information.
    The Ready to Install screen will appear with a summary of the installation.

![Ready to Install](image2)

11. **Click** the Install button to start the installation.
    Installation will begin.
    The SQL Server Setup screen will appear during installation.

12. When the DNA installation is complete a dialog box will appear, **press** Finish to complete the set up.
    The DNA Fusion icon will appear on the desktop.

13. Server installation is finished.
    - If this server will connect to clients, continue to step 14.
    - If this is a standalone server, continue to page 2-1 in the Users Manual for log on information or to 3-1 in the Tech Manual for hardware setup information.

14. If the Domain Users Group was utilized, work with the IT department to add the operators to the domain group (DNA_Global) and configure their rights. See page 2-6 for more information.

15. **Configure** the DNA Server. See page 2-11 for more information.

16. **Start** DNA Fusion and log in. See page 2-1 in the Users Manual for information on starting DNA Fusion.

17. **Create** a Site and **link** to the Site. See page 3-3 for information on configuring a site.

18. **Configure** the remaining hardware. See Chapter 3: Hardware Configuration for more information.

19. **Install** DNA Fusion on the client machines. See page 2-15 for Client Installation.
**Server Configuration**

**Administrative Rights Account Assignment**

**Component Services**

1. From the Control Panel, **double-click** Administrative Tools. The Administrative Tools dialog opens.
2. **Double-click** Component Services and **expand** the Component Services and Computers options in the tree.
3. **Double-click** My Computer and **expand** COM+ Applications. Component Services will open.

4. **Right-click** on the NPowerDNA icon and **select** Properties from the menu. The NPowerDNA Properties window will appear.
5. **Click** the Identity tab.
   Configure the COM+ object to run with an account that has local machine Administrator rights. Open Options recommends that the password for the account be set to not expire.
6. **Select** This User and **enter** the user’s name and password to run under a specific user.
   The account information will need to be obtained from the customer.
7. **Click** OK to save the settings.

**DNA Driver**

1. **Select** Services from the Console Menu on the left.

2. **Right-click** on the DNADrv32 service and **select** Properties.
3. **Select** the Log On tab.
4. **Select** This account and **enter** the user’s name and password used in step 6.
   Remember this account must have local machine Administrator rights.
5. **Click** OK to save the settings.
6. **Close** the open dialogs.
Adding Users to the DNA Users Group

1. From the Start menu, **right-click** on My Computer and **select** Manage from the menu. The Computer Management dialog appears.

2. **Expand** the Local Users and Groups option.

3. **Select** the Groups folder and **right-click** on the DNAUSERS group.

4. **Select** Add to Group from the menu. The DNAUsers Properties dialog appears.

5. **Click** the Add button. The Select Users, Computers, or Groups dialog opens.

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

   See page 2-6 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 Logon’s for every user that will be authorized to run DNA Fusion.

7. **Enter** the Account Name that is running the COM+ and DNA driver (steps 6 & 11) and **click** Check Names to verify the entry.

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

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

9. **Right-click** on the Servers Distributed COM+ users group.

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

10. **Select** Add to Group from the menu. The Servers Distributed COM+ Properties dialog opens.

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

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

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

13. **Click** OK.

14. **Click** OK to save the changes.
Component Services Default Permissions

1. From the Control Panel, double-click Administrative Tools. The Administrative Tools dialog opens.
2. Double-click Component Services and expand the Component Services and Computers options in the tree.
4. Select the COM Security tab.
6. Click the Add button. The Select Users or Groups dialog opens.
7. Click the Locations buttons, select the Local computer and click OK.
8. Type DNAUSERS in the Name field and click Check Names. After the name resolves, click OK.
9. Check the Allow option for Local and Remote Access in the Permissions box and click OK.
11. Click the Add button. The Select Users or Groups dialog opens.
12. Click the Locations buttons, select the Local computer and click OK.
13. Type DNAUSERS in the Name field and click Check Names. After the name resolves, click OK.
14. Check the Local Launch, Remote Launch, Local Activation, and Remote Activation in the Permissions box and click OK.
15. Click OK to save the users.
16. Click OK to save the changes.

Testing the Settings

Lets test the settings!
1. From the Component Services window, right-click on the NPowerDNA COM+ object and select Shut Down from the resulting menu.
2. Right-click on the NPowerDNA COM+ object and select Start. If the COM+ object starts and does not error out, it is properly configured.
   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, return to page 2-9 step 16.
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 and select Manage. **Expand** the Local User and Groups option and **select** Groups. The account will appear in the Administrator group if it has local machine administrative rights.

Server 2003 Only: Depending on the role of the 2003 Server, these local groups may be found in the BuiltIn folder under Groups or in the Active Directory / Users & Computers.

### Database Permissions

The account used to run the COM+ Objects and the DNA Driver service as well as the DNA User group need permission to the NPowerDNA database.

If needed, install the SQL Server Management Studio application that comes with the DNAFusion 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 sub-header.
3. **Select** the New Login option from the menu and **click** the Search button. The Login New dialog appears.
4. **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.
5. **Select** the User Mapping option from the menu on the left. The User Mapping section will open.
6. **Select** the NPowerDNA database.
7. **Check** the following permissions for the user.
   - db_datareader
   - db_datawriter
   - db_ddladmin
8. **Click** OK to save the settings.
9. **Repeat** steps 3 through 8 for the User accounts of the Fusion operators and provide them access to the datareader option.
   - If a database administrator will be responsible for future upgrades, their login will need to be added and access to the datareader, datawriter and ddladmin options.
Client Installation

**Installation**

1. **Insert** the DNA Fusion CD into the computer or **download** the install from the Open Options website. The installation process will start automatically and the Welcome screen will be displayed. If the Welcome screen does not appear, **double click** the Setup icon on the CD.

2. When the Welcome Screen appears, **click** Next to begin the installation.

   ![Welcome Screen](image1)

   The License Agreement screen will appear.

3. **Read** the License Agreement and **select** the I accept the agreement radiobutton and **click** Next to continue.

   If the I do not accept the agreement radiobutton is selected, Cancel and Back will be the only available options.

   The User Information dialog box appears.

4. If desired, **change** the User Name/Organization Information and **click** Next.

   The File Location screen is displayed.

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

   **Default Location:** `C:\Program Files\NPowerDNA`

   The Component Selection screen appears.

6. **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.

   ![Component Selection](image2)

   **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 will appear.

7. **Enter** the Workstation 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 but appropriate permissions to the folder may need to be assigned. Do not change this field unless instructed by Open Options Technical Support.

   ![Client Setup](image3)

   **Enter** the Work Station Name or IP Address of the DNA Server running the DNA COM+ driver.
8. **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.

9. If desired, **select** the Create a desktop icon checkbox.

   ![](image)

   The Windows Firewall 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; contact Open Options Technical Support for more information.

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

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

    Installation will begin.

11. When installation is complete a dialog box will appear, **press** Finish to complete the set up.

    The DNA icon will appear on the desktop.

12. Client installation is finished.

13. **Start** Fusion (see page 2-1 in the Users Manual) and **link** the station to the Site (see page 3-4: Linking to a Site for more information).

    The sites hardware will populate the Hardware Browser.

14. The Client setup is complete.

    Continue to page 2-1 in the Users Manual for system setup information.
Firewall Configuration

If a Firewall will be enabled, then it will need to be configured to allow communication between the server, clients and the controller if connected via Ethernet.

TCP Port 135 is for authentication and TCP Port 3555 and 3557 is 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 allows communication to the DNAAgent service (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.

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 connecting 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 & 445 for TCP connections and ports 137 & 138 for UDP connections.

1. From the Control Panel and **double-click** Administrative Tools. The Administrative Tools dialog will open.
2. **Double-click** Component Services and **expand** the Component Services and Computers options in the tree.
4. **Select** the Default Protocols tab.
5. **Highlight** the Connection-oriented TCP/IP object and **click** the Properties button. The Properties for the COM Internet Services dialog opens.
6. **Click** the Add button.
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 1-10 on the server and all client workstations.
11. **Open** the 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, and 3559
    - 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 for connecting the client workstation to the Microsoft SQL Server running the DNA database.

The ODBC's 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: C:\windows\syswow64\odbcad32.exe

1. From the Control Panel, open the Administrative Tools / Data Sources (ODBC) dialog.
2. Select the System DSN tab.
   - On the Server reconfigured the following ODBC sources to communicate with the DNA database:
     - DNA Reports
     - DNA Entries
     - NPower AMT
     - NPowerDNA Audits
     - NPower DNAH
     - NPower DNAP.
   - On a client, reconfigured the following ODBC sources to communicate with the DNA database:
     - DNA Reports
     - DNA Entries
3. Select the DNA Reports data source and click the Configure button.
   The Microsoft SQL Server DSN Configuration dialog appears.
4. Select the Server Name and Instance Name (if any) from the drop down list and click the Next button.
5. Verify that the With integrated Windows Authentication and Connect to SQL Server to obtain defaults options are selected and click Next.
6. Verify that the Change Default Database to: option is selected and the nPowerDNA database is listed. If the nPowerDNA database is not selected, click the drop down list and select the nPowerDNA database.
7. Verify that Use ANSI options are selected and click the Next button.
8. Click the Finish button to complete the setup.
9. When the Summary screen appears, click the Test Connection button.
10. If the test was successful, configure the remaining DSN's.
Installing DNAFusion on a 64-bit OS

This installation is for 64-bit systems using the SQL Express 2008 database engine.

1. If needed, **install** the .NET 3.5.
   This is a required pre-requisite for SQL Server 2008. The .NET 3.5 install can be found on the Open Options ftp site (dotnetfx35.exe).

2. If needed, **install** the Windows Update for Installer 4.5.
   The Installer 4.5 Update can also be found on the Open Options ftp site (Windows6.0-KB942288-v2-x64.msu).

3. **Install** SQL Server Express 2008A(x64).
   The SQL Server 2008 install can be found on the Open Options ftp site (SQLEXPR_x64_ENU.exe) or on the Microsoft website (http://www.microsoft.com/sqlserver/2005/en/us/express.aspx).
   a. When prompted for the Installation Type, **select** the New Installation.

   b. **Accept** all the defaults until the Feature Selection page is reached.
   c. When the Feature Selection screen is displayed, **check** the Database Engine Services option and **click** Next.

   d. On the Server Configuration Page, **enter** the default User Name: NT AUTHORITY LOCAL SERVER with no password.

   e. **Continue** accepting all the defaults until the Database Engine Configuration page is reached.
   On the Instance Configuration page, make note of the Instance Name. This is especially true if it is named anything other than SQLExpress. This information will be needed during the DNA Fusion installation.

   f. When the Database Engine screen appears, **select** the correct Authentication Mode and **add** any SQL Server Administrators.
   Open Options recommends using Mixed Mode Authentication and setting an SA password. This will allow someone to log into the SQL Server as an administrator under the SA account.
   **Click** Next to continue.

   g. **Continue** until the SQL Server installation is complete.

4. **Install** DNAFusion version 5.1 and above.
   See Server Installation instructions on page 2-7.
Installation

The DNAFusion install can be found on the Open Options ftp site (CD-DNAv5.X.zip).

a. When prompted for the SQL Server Instance, enter the Instance Name from step 3d (Default: `<MachineName>\SQLExpress`).

b. Continue with the DNAFusion installation as described on page 2-7.
Configuring a Windows 2003 Server

2. Click Next. The Preliminary Steps Screen will be displayed.

3. Click Next. The Server Role Screen will appear.
4. Confirm that the application server is configured. If it is, click Cancel. You are done.
   
   If it is not, click Next. The Application Server Options screen appears.
5. Verify that all the checkboxes are unchecked and click Next.

6. Click Next when the Summary of Selections screen is displayed.
7. Click Finish. The Wizard will automatically configure the server.
Configuring a Windows 2008 Server

The Windows 2008 Server will need to be configured as an Application Server in order for Fusion clients to achieve connectivity. Ensure that the Windows user that is logged in has Administrative access and rights to 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 will be displayed.

3. **Click** Next.
   The Select Server Roles screen will appear.

4. **Confirm** that the Application Server option is selected.
   If it is, **click** Cancel. You are done.
   If it is not, **select** the Application Server checkbox.
   The Add Roles Wizard screen appears.

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

8. When the Confirmation dialog appears, **select** Install.
   The Installation Results screen will be displayed with the results of the installation.

9. If the Installation was successful, **click** Close.
   If the Installation fails, **verify** that the Windows user has the proper rights.
   Acquiring the Installation Disks for Server 2008 maybe useful before reattempting the process again.
**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 2003 or 2008 Server, follow the procedure described on page 2-21 for 2003 Server or 2-22 for 2008 Server configuration steps.

**Migrating with Server/Client Components on the Same Workstation**

Follow the instructions below if the Fusion server application (DNA driver) & 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 during Open Options normal business hours the day of the installation.
   - **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 return of the HASP Key. This will require an advance replacement PO for the new system.

2. **Shut down** all Fusion clients.
3. **Stop** the DNA driver (DNAdvr32.exe) service on the old Application Server.
4. If utilizing the OpenDX application, **stop** the OpenDX service.
5. **Verify** that the new Server has SQL Server 2005 or 2008 installed.
6. **Back up** the NPowerDNA database and **restore** it with the same name on the new Server.
7. **Install** the DNA Fusion Server as described on page 2-7.
8. On the Component Selection screen, **select** Client / Server Components and **click** Next.
9. **Select** Existing Database from the Database Server Options page and **click** Next. See page 2-8 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 radiobutton next to the correct Authentication Mode.
11. From the Select Database drop down list, **select** the nPowerDNA database and **click** Next.
12. **Complete** the installation as described on pages 2-8 and 2-9.
13. **Verify** the database permissions.
   a. The account(s) running the com objects and DNADvr32 service needs to have datareader, datawriter and ddladmin rights.
   b. The user accounts for DNAFusion operators would need to have datareader rights.
   c. If there is a database administrator who would be responsible for future upgrades, their account should have datareader, datawriter and ddladmin rights.
14. **Run** the Tablepurger.exe application to remove the old server name from database. See page 5-3 for information on the Table Purger.
15. **Launch** Fusion and **link** the Station to Site.
16. On each client workstation, **edit** the DNA Reports ODBC System DSN to point to the new database server. See page 2-18 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: C:\Program Files\nPowerDNA\DNAShare
   This will point the clients COM+ objects on the client to the new server. There may be other items that need to be updated including Photo Paths, Badge Templates, etc.
**Migrating with Server and Client Components on the Separate Workstations**

Follow the instructions below if the 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 Fusion clients.
2. **Stop** the DNA driver (DNAdvr32.exe) service on the Application Server.
3. If utilizing the OpenDX application, **stop** the OpenDX service.
4. **Verify** that the new Server has SQL Server 2005 or 2008 installed.
5. **Back up** the NPowerDNA database and **restore** it with the same name on the new Server.
6. **Install** the DNA Fusion Server as described on page 2-7.
   
   In order to force a new server installation, run the setup with the `setup.exe /forcenew` switch to update the settings and connect the database on the new server.
7. On the Component Selection screen, **select** Server Components and **click** Next.
8. **Select** Existing Database from the Database Server Options page and **click** Next.
9. From the Instance Name drop down list, **select** the SQL Server Instance where the database will be created and **select** the radiobutton next to the correct Authentication Mode.
   
   See page 2-8 for information on Database Server Options.
10. From the Select Database drop down list, **select** the nPowerDNA database and **click** Next.
11. **Complete** the installation as described on pages 2-8 and 2-9.
12. **Verify** the database permissions.
   
   a. The account(s) running the com objects and DNADrvr32 service needs to have datareader, datawriter and ddladmin rights.
   
   b. The user accounts for DNAFusion operators would need to have datareader rights.
   
   c. If there is a database administrator who would be responsible for future upgrades, their account should have datareader, datawriter and ddladmin rights.
13. **Run** the Tablepurger.exe application on the server to remove on the old server name from database.
   
   See page 5-3 for information on the Table Purger.
14. **Point** the System DSNs on the Application Server to the new Database Server.
   
   See page 2-18 for information on configuring ODBC sources.
15. **Launch** Fusion and **link** the Station to Site.
16. On each client workstation, **edit** the DNA Reports ODBC System DSN to point to the new database server.
   
   See page 2-18 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: C:\Program Files\nPowerDNA\DNASHare
   
   This will point the clients COM+ objects on the client to the new server.
   
   There may be other items that need to be updated including Photo Paths, Badge Templates, Graphic Maps and the Universal Driver.
In addition to setting up the various field devices that make up the hardware components of the system, you must configure the settings in DNA Fusion so the software knows how to communicate with the various field devices. This chapter discusses the steps required to add hardware to the system and configure the settings for the different devices along with controlling various hardware objects.

Configuring Hardware

Hardware is created in the following order:
1. Site - Collection of channels and controllers that communicate with a common driver.
2. Channel - Virtual pathway of communication from the host to one or more SSPs.
3. Controller - Data gathering panel that makes local access decisions as well as stores all information such as access levels, time schedules, and triggers and macros.
4. Subcontroller - One of a series of circuit boards that communicates information about field devices like readers, contacts, motion detectors, etc., upstream to the SSP.
5. ACMs - A group of objects that when associated together form a point of entry that is normally associated with a door or elevator.

The Hardware Browser

All hardware is added through the Hardware Browser. The Hardware Browser is an explorer window that consists of a hierarchical layout of the field devices that make up 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 will open.

   For more information on the Hardware Browser, see Chapter 8 in the Users Manual.

Configuring the Browser

The Hardware Browser can be customized to display various tabs as well as objects in the Hardware tree. The hardware tree can also 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 list.
3. Configure the Settings. See page 3-22 in the User Manual for more information on Hardware Tree Settings.
**Hardware Toolbar**

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Download Manager Icon" /></td>
<td>Download Manager Icon - Displays the Download Manager dialog box for downloading the database information to the SSP.</td>
</tr>
<tr>
<td><img src="image" alt="Direct Control Icon" /></td>
<td>Direct Control Icon - Displays the Direct Control dialog for the selected hardware object.</td>
</tr>
<tr>
<td><img src="image" alt="Hardware Properties Icon" /></td>
<td>Hardware Properties Icon - Displays the Hardware Properties for the selected hardware object.</td>
</tr>
<tr>
<td><img src="image" alt="Add Hardware Icon" /></td>
<td>Add Hardware Icon - Click the arrow to display a drop-down menu of hardware objects. Selecting an item displays the Add dialog box for the selected object.</td>
</tr>
<tr>
<td><img src="image" alt="Delete Icon" /></td>
<td>Delete Icon - Displays the deleted item confirmation box.</td>
</tr>
<tr>
<td><img src="image" alt="Status Icon" /></td>
<td>Status Icon - Displays the status for the selected hardware object.</td>
</tr>
<tr>
<td><img src="image" alt="Default Template Icon" /></td>
<td>Default Template Icon - Applies the default template to the selected hardware object.</td>
</tr>
<tr>
<td><img src="image" alt="Template Manager Icon" /></td>
<td>Template Manager Icon - Displays the Template Manager dialog box.</td>
</tr>
<tr>
<td><img src="image" alt="Watch Window Icon" /></td>
<td>Watch Window Icon - Adds the selected hardware object to an existing Watch Window.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh Tree Icon" /></td>
<td>Refresh Tree Icon - Updates the Hardware Explorer tree.</td>
</tr>
<tr>
<td><img src="image" alt="Home Page Icon" /></td>
<td>Home Page Icon - Launches the home page associated with the selected hardware object.</td>
</tr>
<tr>
<td><img src="image" alt="Disable High Icon" /></td>
<td>Disable High Icon - Disables the IP Video Window from opening automatically on a High Priority alarm.</td>
</tr>
<tr>
<td><img src="image" alt="Disable Normal Icon" /></td>
<td>Disable Normal Icon - Disables the IP Video Window from opening automatically on a Normal Priority alarm.</td>
</tr>
<tr>
<td><img src="image" alt="Disable Low Icon" /></td>
<td>Disable Low Icon - Disables the IP Video Window from opening automatically on a Low Priority alarm.</td>
</tr>
<tr>
<td><img src="image" alt="Disable Custom Icon" /></td>
<td>Disable Custom Icon - Disables the IP Video Window from opening automatically on a Custom Priority alarm.</td>
</tr>
</tbody>
</table>
Adding Hardware

Creating and Linking a Site

A site is defined as a collection of channels and controllers that communicate with a common driver. Think of a site as the location of the communicating hardware for a section or all of a given system. Each site can have a maximum of 128 channels and the system can have a maximum of 63 sites.

Most installations will have only one site with multiple channels. Each site is basically a separate driver that communicates to the various channels and controllers.

Creating a Site

A Site will automatically be created if the DNA Driver (DNADrvr32) service is started on the server after installation. The Station will need to be linked to the newly created site. See page 3-4.

The first step in adding hardware is creating a site or establishing a common driver for the hardware to use for communicating to the database.

1. **Open** the Hardware Browser and **right-click** inside the browser.
2. **Select** Sites/New Site from the menu.
   
The Add Site Driver dialog box will appear.

3. **Select** the Site Number from the Number drop down.
4. **Click** the Local button to add the workstations location information to the Location field. This provides the computers name on which the site’s driver will residing.
5. **Enter** a site name in the Name field.
6. The Port field will automatically default to port 3555. This is the TCP/IP port used by the station to establish communication with the site’s driver.
7. If desired, **enter** a Description for identification.
8. **Click** OK.
**Linking to a Site**

Site must be linked within the Hardware Browser to create the communication path for the driver.

1. **Right-click** inside the Hardware Browser and **select** Sites/Link Station to Site. The Site Properties dialog box will open.

2. **Select** the Site Number entered in step 3 above under Creating a Site. The site information will automatically populate the dialog box.
   - Number - Identification for the site.
   - Status - Indicates online or offline status.
   - Name - Site name.
   - Location - Name of computer on which a given site's DNADrvr32 driver is residing.
   - Port - Driver machine TCP/IP port used to establish communication with the site’s driver.
   - Subcontrollers - Number of sub-controllers actively connected (online) for the site.
   - Connection Type - Indicates the connection type to the site.
   - New Site - Opens the Add Site Driver dialog box.

3. The **Connection Type** will default to the correct setting.
   - Local - Server Workstation
   - Remote - Client Workstation

4. **Click** OK to save the settings.
   The site will appear in the Hardware Browser.

---

*A new site can be added by pressing the New Site button in the Site Properties dialog box; the Add Site Driver dialog will appear. See page 3-3 for more information.*
Adding a Channel

A channel is a defined virtual pathway determining a route of communication from the host to one or more SSPs. DNA Fusion can communicate with the controllers using either: Serial, Ethernet, or Modem communications. SSPs that communicate using serial channels may have multiple SSPs for a channel. While SSPs that are connected via modems or Ethernet have one channel per SSP.

1. With the Hardware Browser open, **right-click** on the desired Site.

2. **Select** Add Channel from the drop-down menu.
   
The Add Channel dialog box will appear.

3. **Populate** the fields to configure the correct channel settings.
   
   See page 3-6 for information on setting up the various channel types.
   
   - **Site Number** - Location of hardware (auto-populated).
   - **Channel ID** - Designation for the channel.
   - **Description** - Label for the channel.
   - **Channel Type** - Method of communication connection. See page 3-6 for more information.
     - **Serial** - Select COM Port from the drop down list.
     - **Dial In/Out** - Select the Modem Name from the drop down list.
     - **Ethernet/Remote TCP/IP** - If desired, change the TCP/IP Retry Count.
   - **COM/Receiving Port** - COM Port for serial connections/Receiving Port for Remote TCP/IP.
   - **Baud Rate** - Rate of transmission to SSP.
   - **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 an SSP after an unsuccessful attempt. TCP/IP Configurations only.
   - **Modem Name** - Modem designation in the Control Panel. Dial In/Out Configurations only.
   - **RTS Mode** - On/Toggle/Off/CTS-RTS Handshake
     - **On** - Fixes the state of the RTS pin to ON. RS-232 with Hardware Handshake.
     - **Toggle** - Tells the port handler to set the RTS output to ON when data is being sent. Used when the COM port is set to half-duplex mode, such as 2-wire RS-485.
     - **Off** - Fixes the state of the RTS pin to OFF. 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.
Hardware Configuration

**Serial Channel**
1. Enter a Description for the channel.
2. Select Serial from the Channel Type drop down.
3. Select the COM Port from the drop down list.
4. Verify that the Baud Rate is set to 38,400.
5. Set the SSP Reply Timeout to 300.
6. Set the RTS Mode to OFF.
7. Click OK to save changes.

**TCP/IP Channel**
1. Enter a Description for the channel.
2. Select Ethernet (TCP/IP) from the Channel Type drop down.
3. Verify that the Baud Rate is set to 38,400.
4. Verify the RTS Mode is set to CTS/RTS Handshake.
5. Click OK to save changes.
6. Enter the IP Address in the SSP Properties dialog.
   See page 3-7.

**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 to dial the controller or the controller to dial the host, see Chapter 10: Triggers & Macros in the User Manual.
   - Dial (out) - Only allows DNA to initiate the connection to the SSP.
   - Dial (in) - Only accepts incoming calls from the SSP.
   - Dial (out/in) - Allows the driver to initiate the connection to the SSP as well as accepts calls initiated by the SSP. Most common setting.
3. Verify that the Baud Rate is set to 38,400.
4. Set the SSP Reply Timeout to 300.
5. Select the Modem from the Modem Name drop down list.
6. Set the RTS Mode to CTS/RTS Handshake.
7. Click OK to save changes.
8. Enter the Phone Number in the SSP Properties dialog.
   See page 3-7.

Open Options recommends using the Multitech MultiModem ZBA modem at both the host and the SSP. It is also recommended that both ends utilize a POTS line. For more information see Chapter 9 in the Hardware Manual.
Adding an SSP (Controller)

The controller is the data gathering panel that makes local access decisions. The SSP also stores all information such as access levels, time schedules, and triggers and macros. Each setting is discussed in detail on the following pages.

1. **Right-click** an existing Channel object from the tree in the Hardware Browser.
2. **Select** Add SSP from the menu.
   The Controller Properties dialog box opens.

3. **Select** the Controller’s Physical Address from the drop down list.
4. **Enter** a user defined Description (typically location or function related).
5. **Select** the Controller Type from the drop down list.
6. If desired, **select** a Download Priority.
7. **Select** the GMT Offset from the drop down list.
   See page 3-9 for more information on GMT.
8. **Check** the Use Daylight Savings checkbox to automatically adjust for daylight saving time.
9. **Enter** the channel information.
   - If Ethernet (TCP/IP) Channel, **enter** the IP Address.
   - If Modem Channel, **enter** the Phone Number. The phone number should not contain any dashes, spaces or parenthesis. A comma creates a pause.

   The modem will attempt to connect when the setting are downloaded and anytime the driver is started or reset. To manually establish a connection right-click on the SSP and selecting Controller Commands/Connect or Disconnect.

   - If Serial Channel, no information is required.
10. **Click** the Stored Quantities option on the menu.
    See page 3-11 for more information on Stored Quantities.
11. **Select** any Controller Flags that will used and adjust any Quantities as needed.
12. **Click** the OK button to save the settings.
Controller Properties

Attributes

- **Site** - Location of hardware (auto populated).
- **SSP Number** - Designation for the SSP.
- **SSP Description** - User defined description of the SSP-typically location or function related.
- **Controller Type** - Select the SSP type from the drop-down list.
  - SSP (Standard)
  - SSP-C
  - SSP-E
  - SSP-EP
  - SSP-D2 - When adding an SSP-D2, the on-board RSC-D2 subcontroller is added automatically.
- **Use Encryption** - If selected, data will be encrypted from the server to the SSP.
  NOTE: Using encryption will cause the system to run about 30% slower.
- **Home Page** - A file associated with the controller that will open when the object goes into alarm.
- **Download on Demand Exempt** - If this checkbox is enabled, cardholder data will be downloaded as a group to the SSP.
- **Physical Address** - Physical address defined by the SSP’s dipswitch settings.

Controller Time Parameters

- **GMT Offset** - Number of hours offset from Greenwich Mean Time.
  - -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 this SSP. See page 5-5 in the Fusion User Manual.
- **Holiday Set** - Selected holiday set for this SSP. See page 5-9 in the Fusion User Manual.
● Use Daylight Savings - Check to automatically adjust for Daylight Savings Time.
● Edit Table - Opens the Daylight Savings Editor.
  □ Add - Opens the Daylight Savings Date Editor. Up to 20 date pairs can be added in chronological order.
  □ Remove - Removes the selected Daylight Savings entry.
  □ Edit - Opens the Daylight Savings Date Editor.
  □ Defaults - Loads the default Daylight Savings information.
● Host Response Time - If Host Verification is enabled in the Door/Advanced dialog (page 3-26), the SSP will report to the Host for access confirmation. This value 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).
  □ Serial Channel - If Serial Channel, no further information is needed.
  □ Dial In / Out Channel - If Dial In/Out Channel, enter the Phone Number. Remember to include any leading digits. A comma creates a pause.
  □ TCP/IP Channel - If IP Channel, enter the IP Address.
● 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. (Dipswitches 6 & 7)
● Password - Sets a password in the SSP to permit communication. (Dipswitch 8)
● SSP Channel - Channel that the SSP is attached to on the Hardware Tree. (auto populated)
● Retry Count - Number of times a poll can fail before a panel is determined to be offline.
● 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
● Port 1 Baud - Baud rate for downstream port: physically Port 2 on the board.
● Port 2 Baud - Baud rate for downstream port: physically Port 3 on the board. (SSP-EP only)
**Controller Memory**
- Panel Memory - The amount of memory on the panel.
  - The SSP-EP defaults to 15 Meg.
  - The SSP-D2 defaults to 6 Meg.

**Offline Transaction Capacity**
- Current Setting - The number of transactions held in memory before the controller discards first-come/first-served transactions.
- Calculate - Automatically calculates the Current Settings number based on current flags and quantity amounts set below.

**Controller Flags**
If a feature is used, it must be stored in the controller in order for it to work.
- Store Issue Codes - Stores re-issue codes for cards. Indicates how many times a card with the same card number has been issued.
- Store APB Location - Stores the Anti-Pass Back locations.
- Store Activation Date - Stores the activation date. Prevents access prior to date set.
- Store Deactivation Date - Stores the deactivation date. Prevents access after set date.
- Support Timed Anti-Pass Back - Stores time of last entry for use with Anti-Pass Back. All Readers must be set up for Timed APB.
- Store Vacation Date - Stores dates for vacation. See page 7-9 in the DNA User Manual.
- Store Temporary Upgrade Date - Stores temporary access level. See page 7-9 in the DNA User Manual.
- Store Trigger Code - Stores trigger codes for a card.
- Store Use Limit - Stores use limit for a card. See page 7-10 in the DNA User Manual.
- Store Asset Code - Stores an asset code for a card.

**Quantities**
- Access Levels Per Card - Number of access levels that can be assigned per card for the selected SSP. See Chapter 6: Access Levels for more information.
- Precision Access Levels - Number of precision access levels. See page 6-17 in the DNA Users Manual for more information on Precision Access Levels.
- Access Levels - Number of access levels. Max. 255
- **Triggers** - Number of triggers to store. Default=128
- **Macros** - Number of macros to store. Default=128
- **Time Schedules** - Number of time schedules to store. (auto-populated)
- **Holidays** - Number of holidays to store. (auto-populated)
- **Cards** - Number of cards allowed in the controller.
- **Secured Areas** - Number of secured areas allowed in the controller.
- **Unreported Transactions** - Number of unreported transactions to log event. There will be an Event entry made when this number is exceeded. Can be used to trigger the SSP to dial back and report transactions.

### Elevator Control
- **Max Floors** - Number of floors in the building.
- **Max. per Cab** - Maximum number of floors per cab. The number entered must be less than or equal to the Building Max.
- **Floor Group Quantity** - Set maximum number of elevator access levels per floor group.
- **Edit Floor Names** - Opens SSP Floors Setup dialog box, allowing names to be entered.

### PIN and Duress Options
- **PIN Digits to Store** - Number of PIN digits to store. Used with a keypad reader.
- **Card ID Size** - Set card format.
- **Duress Digit** - Indicate the duress digit 0 through 9. Setting the Duress Digit to 0 indicates that the Duress feature is not used.
- **Duress PIN Mode** - Add or Append the original PIN.

- **Add** - If Add is 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 = 1234.
    
    If the Duress Digit is set to 6, then the cardholder’s duress PIN would be 1236 - cardholder’s original PIN 1234 + 6 = 1230.
    
    If the Duress Digit is set to 2, then the cardholder’s duress PIN would be 1236 - cardholder’s original PIN 1234 + 7 = 1231.

- If the Add option is selected, care should be taken so that PIN codes do not overlap.

- **Append** - If Append is 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.
    
    If the PIN Number is 1234 and the Duress Digit is set to 6, then the cardholder’s Duress PIN would be 12346 - cardholder’s original PIN 1234 with 6 inserted at the end = 12346.
Cards & Dual Comm

Card Formats (Personnel)
- Card Formats 0-7 - Select a card format from the library. See page 3-49 for more information on setting up card formats.
- Host Macro - Select the Host Based Macro to execute.
- Edit - Opens the Host Based Macro edit dialog. See page 10-13 in the Users Manual for more information on Host Based Macros.

Alternate Ports
This section will be available only with the SSP-E.
- Enable - Enables the alternate ports when the communication is lost on the primary port.
- Connection Type - Alternate port connection type.
- Phone # - Phone number to dial if the alternate port is connected to a machine.
- Alternate Channel - Communication channel for the alternate port.
- Poll Delay - Time between polls on the alternate port.

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

There are 2 means of downloading a batch file to an SSP:
- DNA/Administrative/Batch Processing. See page 20-14 for more information.
- DNA Batch Download Settings application. See page 5-4 for more information.
Adding Subcontrollers

1. **Right-click** an existing Controller object from the tree in the Hardware Browser.

2. **Select** Add from the menu and **select** Add Subcontroller. The Subcontroller Properties dialog box opens.

3. **Enter** a user defined Description of the subcontroller.

4. If Match Physical is checked, a Physical Address is not required. The system will match the boards dipswitch settings for the physical address. If Match Physical is unchecked, a Physical Address will need to be selected.

5. If desired, set a Home Page by **clicking** the Browse button.

6. **Select** the Type of subcontroller from the drop down list. A preview of the board will be displayed as the various boards are selected.
   - If the NSC-100 subcontroller was selected, continue to step a.
   - If GTWY, PIM400-485 or AD 300 is selected, see Chapter 11: Schlage Locks in the Hardware Manual.
   - All other subcontrollers, continue to step 7.
   a. If NSC-100 is selected from the Type drop down, **enter** an available IP Address that resides on the same subnet as the controller.
      
      ![IP Address Entry]

   b. **Enter** the MAC Address found on the NSC-100s on-board RJ-45 socket. The controller has a built-in DHCP service that will handle the registration of the IP address for the NSC-100.

7. If desired, **enter** Alarm Text.

8. If needed, **select** the Send and Receive Channels from the drop down list.

9. If desired, **select** the Advanced menu option to configure the advanced settings. See page 3-15 for more information.

10. **Click** OK to save the settings.
Subcontroller Properties

Address
- Site - Name of site defined in site properties. (auto-populated)
- SSP - Name of SSP attached to subcontroller. (auto-populated)
- Subcontroller (SIO) - Subcontroller address.
- Match Physical - Matches the physical address in the software with the dipswitch settings on the board. When selected, the SSP will attempt to communicate to the subcontroller on the next available address. See the Hardware Manual for dipswitch settings.
- Disable SIO - If checked, the subcontroller will be disabled.
- Description - User-defined description of the subcontroller; typically location or function related.
- Home Page - Home page to associate with the subcontroller.

Attributes
- Physical Address - Physical address as set on the dipswitches. This option will be greyed out when the Match Physical option is selected and will automatically increase as subcontrollers are added to the system. See the Hardware Manual for dipswitch settings.
- 4-Wire Configuration - If checked, the 4-Wire RS-485 communications is ON.
- SSP Relay Channel - Indicates the port on that the subcontroller is using to communicate to the controller.
- SSP Send Channel - Reflects the SSP Reply Channel. (auto-populated)
- IP Addr - When the NSC-100 subcontroller is selected, the IP Addr field identifies the IP address that the subcontroller is assigned.
- MAC Addr - When the NSC-100 subcontroller is selected, the MAC Addr field identifies the subcontroller’s default MAC address.

Type/Preview
- Type - Drop-down list featuring different subcontrollers.
- 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 Properties

- Errors Before Offline - Number of consecutive communication errors before the subcontroller is determined to be offline.
- Alternate Message 1 - Change the alarm information for the cabinet tamper to a different message, allowing the utilization of the hardware point for another purpose.
- Alternate Message 2 - Change the alarm information for the power tamper to a different message, allowing the utilization of the hardware point for another purpose.
- Host Macro - Select the Host Based Macro to execute.
- Edit - Opens the Host Based Macro edit dialog. See page 10-13 for more information on Host Based Macros.
- Reverse Polling on Inputs - Changes the order in which inputs are processed by the system. If selected, inputs will be processed from higher number to the lower number.

Continuations

- 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 SIO. This allows you to jump/skip SIOs with continuation.
  This is an advanced feature and modification should be avoided unless the operator has a through understanding of the ramifications.
- 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 SIO. This allows you to jump/skip SIOs with continuation.
  This is an advanced feature and modification should be avoided unless the operator has a through understanding of the ramifications.

Identification

- Serial Number - Reference Field Only: Stores the subcontroller serial number for future reference.

Updating Subcontroller Firmware

The Subcontrollers (RSC1/RSC2/RSC-DT/ISC16/OSC16/NSC-100) firmware can be updated from the Hardware Browser.

1. **Right-click** on the Subcontroller and select **Reload Firmware** from the menu.
   Depending on the subcontroller, a dialog will appear.
2. **Follow** the directions on the screen.
   The subcontrollers firmware is reloaded.
Adding Doors

Access Control Models (ACMs) perform two functions: it validates access requests and it manages and monitors the access point. It is possible to configure a system without a physical reader, if only door monitoring functions are required.

There are two types of doors: Single and In & Out.

NOTE: Doors can also be added through a reader. See page 3-19 for more information.

Adding a Single Door

1. **Right-click** the Door object under the SSP object from the tree in the Hardware Browser.
2. **Select** Add Door from the menu.
   The New Door dialog box opens.

3. **Enter** a user defined Description; typically location or geographical in nature.
4. If needed, **select** the correct Door Type for the application.
5. If desired, set a Home Page by **clicking** the Browse button.
   See page 3-21 for more information on the other Common Properties.
6. **Click** the Door Objects link on the menu.
7. **Select** Single in the Type drop down.
8. **Select** the Reader from the 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 3-23 for more information on each Door Object.
    The Edit button will become available as each hardware object is selected.
11. If desired, **set** the Strike and Held Time for the ADA Settings.
    These settings only apply to cardholders with the ADA Flag set in their record.
12. If desired, **configure** the Advanced dialog per the descriptions on page 3-25 and 3-26.
13. If desired, **configure** the Macros dialog. See page 3-27 for more information.
14. If desired, **select** the Follows Schedule link on the menu and configure the door to follow a designated time schedule. See page 3-28 for more information.
15. **Click** OK to save the settings.
    The door is added to the Hardware Tree Browser.
## Adding an In & Out Door

1. **Right-click** the Door object under the SSP object in the Hardware Browser.
2. **Select** Add Door from the menu.
   The New Door dialog box opens.
3. **Enter** a user defined Description; typically location or geographical in nature.
4. If desired, set a Home Page by **clicking** the Browse button.
   See page 3-21 for more information on the other Common Properties.
5. **Click** the Door Objects link on the menu.
   The Door Objects page opens.

### Hardware Properties

6. **Select** In and Out in the Type drop down.
   **Select** the In Reader from the drop down list.
   See page 3-23 for more information on each Door Object.
   The Edit button will become available as each hardware object is selected.
7. **Select** the DSM and Request to Exit Contacts.
8. **Select** the Out Reader from the drop down list and verify the Pair Door: selection.
9. **Select** the Strike Output and continue to configure the door settings.
10. If desired, **configure** the Advanced dialog per the descriptions on page 3-25 and 3-26.
11. If desired, **configure** the Macros dialog. See page 3-27 for more information.
12. If desired, **select** the Follows Schedule link on the menu and configure the door to follow a designated time schedule. See page 3-28 for more information.
13. **Click** OK to save the settings.
   The door is added to the Hardware Tree Browser.
**Adding a Door From a Reader**

1. **Expand** the Subcontroller to locate a reader and **right-click** on the Reader.
2. **Select** Add Door from the menu.
   The New Door dialog opens.
3. **Enter** a Description.
4. If desired, **configure** the other options in the Common Properties dialog per the descriptions on page 3-21.
5. **Select** the Door Objects link.
   The Door Objects are prepopulated with the reader address as well as the addresses for the next set of available points. See page 3-23 and 3-24 for more information on Door Objects.

6. If desired, **configure** the Advanced dialog per the descriptions on page 3-25 and 3-26.
7. If desired, **configure** the Macros dialog.
   See page 3-27 for more information.
8. **Click** OK when finished.
   The door is added to the Hardware Tree.
Door Properties

**Common Properties**

**Address**
- Site - Site number. (auto-populated)
- Controller - Name of controller defined in controller properties. (auto-populated)
- Door Number - Access Control Model #
- Door Type - Determines how the door function.
  - Normal - Door will operate as a regular access control door.
  - Muster - Door will operate as a muster point in addition to 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 a Auto Activate badge, the badge will be activated. See page 7-10 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 a Auto Deactivate badge, the badge will be deactivated. See page 7-10 in the DNA Fusion User 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 a Auto Activate badge, the badge will be activated. See page 7-10 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 badge, the data will be collected and stored in a separate table as the In Time. See page 5-17 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 badge, the data will be collected and stored in a separate table as the Out Time. See page 5-17 for more information.
  - InfoReader - Works in conjunction with the InfoReader hardware.
- Situations - Opens the Situation Level Manager Settings dialog for the associated door. See Chapter 9 in the Users Manual for more information on Situation Manager.

**Other**
- Description - User defined description of the door that appears in the browser; typically location related.
- Home Page - Home page associated with the door that will open when the door goes into alarm.
Point Alarm Properties

- **Alternate Priority** - Selected Alarm Priority overrides the default Event specific priority set in DNA / Administrative / Events & Alarms / Logging. See page 14-23.

- **Security Level** - Category designation. Allows administrator to restrict operator use.

- **Do Not Load Home Page on Alarm** - If associated door goes into alarm, the Home Page will not load.

- **Alarm Media File** - Door specific alarm file to be displayed when an alarm occurs.

- **Alarm Text** - Point specific alarm text to be displayed when an alarm occurs in addition to the alarm reason.

- **Camera** - Camera associated with the door; allowing it to be recalled in the Event Grid as well as in the Alarm Grid.
Door Objects

Door Parameters

- **Type** - Specifies type of door.
  - In & Out Door - Select this option when using Access Areas or Anti Passback. When selected, two readers will be assigned to the door.
  - Single Door - Assigns one reader to the door.

- **Pre-Alarm Held** - Number of seconds before door reports Door Held Pre-Alarm event/alarm causing an event to be generated prior to a Door Held alarm.

- **LED Mode** - LED operation.

- **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 door reports a Door Held event/alarm. This only applies to inputs that are specified as the Door Contact.

Reader

- **Address** - Specifies the reader address.
- **Edit** - Opens the Reader Properties dialog box. See page 3-37.
- **Default Mode** - Defines the normal state of the reader.
  - None - No reader is associated with the door.
  - Disabled - Disables the reader and the door remains locked with no REX capability.
  - Unlocked - Unlimited access mode.
  - Locked - No access is allowed but the door can be used from the inside, using the REX button.
  - Facility Code - Only the facility code is checked, for access authorization.
  - Card Only - Only the card number is checked, for access authorization.
  - PIN Code - Only the PIN code is checked, for access authorization.
  - Card and PIN - Both the card and PIN numbers are checked, for access authorization.
  - Card or PIN - Either the card or PIN numbers are checked, for access authorization.
- **Offline Mode** - Defines offline mode of the reader. Uses same settings as the Default Mode.
  - None - No reader is associated with the door.
  - Disabled - Disables the reader and the door remains locked with no REX capability.
  - Unlocked - Unlimited access mode.
  - Locked - No access is allowed but the door can be used from the inside, using the REX button.
  - Facility Code - Only the facility code is checked, for access authorization.
Hardware Configuration

- Type - Specifies type of reader.
  - Normal
  - Keypad
  - Text Keypad

Contact
- Address - Specifies the address of the door contact.
- Edit - Opens the Edit dialog for this object. See page 3-39.

Request to Exit (REX)
- Address - Specifies the address of the REX.
- Edit - Opens the Edit dialog for this object. See page 3-39.

Strike
- Address - Specifies the address of the door strike.
- Edit - Opens the Edit dialog for this object. See page 3-43.
- Activation - Maximum seconds door will be unlocked when an Access Granted is received. Check code for your area.
- Mode - Defines how the door strike will act when door is opened.
  - No Impact on Strike - Opening the door or closing the door does not effect the Activation Timer.
  - Cut Short On Open - Strike Activation Timer is canceled and the Strike is re-engergized when the door is opened.
  - Cut Short On Close - Strike Activation Timer is canceled and the Strike is re-engergized when the door is closed after it has been opened.
  - Tailgate: Short When Opens - Strike activation timer is canceled and the Strike is re-engergized when the door is opened. In addition, the adjacent relay is pulsed for 1 second. Example: If the strike is assigned to 1.1.1.O1 then 1.1.1.O2 would be pulsed for one second.
  - Tailgate: Short When Closes - Strike activation timer is canceled and the Strike is re-engergized when the door is closed after it has been opened. In addition, the adjacent relay is pulsed for 1 second. Example: If the strike is assigned to 1.1.1.O1 then 1.1.1.O2 would be pulsed for one second.

ADA Settings
The following options are invoked for cardholders with the ADA Flag set in the Cardholder record. See page 7-10 in the Users 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.
Anti-Pass Back (APB) Settings
See Chapter 11 in the Users Manual for information on configuring Anti-Pass Back.

- Option - 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 be enabled in the SSP Properties / Stored Quantities dialog. (Reader-based APB using the readers last user)
  - Check last ACR used, no location change - Disallows a cardholder to present his card to the same reader twice in a row. Once access is granted at the reader, the user will not be granted access at this same reader again until the user presents his card at another reader in the system or APB delay has expired. Requires Support Timed Anti-Pass Back be enabled in the SSP Properties / Stored Quantities dialog. (Reader-based APB using the cardholders access history)
  - Check current location, change on entry - Similar to option #2, except that the APB delay will reset user’s area after the specified time. Requires Support Timed Anti-Pass Back be enabled in the SSP Properties/ Stored Quantities dialog. (Area-based APB)

- Delay - Number of minutes before APB resets. Only used in conjunction with APB options 3-5. Max. delay = 255 minutes
- From - The area number the user comes from.
- To - The area number the user enters.

Door Parameters
- Decrement Use Limit - This door decrements Use Limit associated with card.
- Require Use Limit > 0 - If use limit reaches 0, do not allow access.
- Set to Deny Druess - Denies access upon receiving a duress signal. PIN & Card only
- Log All Requests as Used - Assumes that the door was used and log all access requests as used Door Used as soon as the request is granted. Not for use with Anti-Pass Back.
- Do NOT pulse on REX - Prohibits pulsing the door strike on REX cycle. Used for quiet exit.
- Filter Change of State - Filters all changes of state and displays only Open or Closed events.
- Require 2 Card Control - Requires two access credentials to be presented.
- Biometric Verification - Biometric hardware is being supported. This is an advanced feature and should be avoided unless the operator has a understanding of the ramifications.
- Enroll on Access - Biometric hardware is being supported and the system should record the biometric signature on the first presentation. This information will be used as the future reference.
- Grant If Host Offline - Access will be granted in the event the Host is not available. Works in conjunction with Host Verification.
- Host Verification - Host verification must be obtained prior to granting access. See page 3-10 Host Response Time to set the timeout parameter.
- Enable Cypher Mode - Allows 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. Access Granted events only.
- Wait for Missing Card - If an access request is denied due to “card not in file,” the reader is put into the wait state and waits for host response.
- Enable Door Forced 3 Second Filter - If selected, a Door Forced event will not be reported if the door is reopened within 3 seconds of closing after an Access Granted event.
- No Reset on Held Timer - If checked and an Access Granted is received and the door is opened and then a subsequent card read happens, the shunt time will not be started over.
- Enforce CARD before PIN - Requires the cardholder to badge before entering their PIN number.

Logging Based on Deny Violations
- Not in File: PIN only Mode - An event will be logged when an incorrect PIN is entered.
- Not in File: Cypher Mode - An event will be logged 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.
- Biometric Failures - An additional event will be logged when an biometric failure occurs.
- Violations - Number of violations to allow before event is logged.
- Reset Time - The amount of time before the count resets.

Secondary Request to Exit (REX)
- Address - Address of secondary REX.
- Edit - Opens the Edit dialog for this object.

Secondary (Biometric) Reader
- Address - Drop-down list of readers to select for Reader 2.
- Edit - Opens the Edit dialog for this object.
- ReaderType - Drop-down list of reader types to select for Reader 2.
**Macros**

![Image of Macros interface]

**Door Sounder**
This option creates a trigger and macro based upon the selections.

- **Address** - Address of door sounder.
- **Schedule** - Drop-down list of the available time schedules.
- **Sound On** - Condition to activate the sounder.
  - Pre-Alarm Held
  - Held or Forced
  - Close
  - Open
- **Sound Off** - Conditions to deactivate the sounder.

**Alarm Conditions**

- **Held Pre-Alarm / Schedule** - Drop-down list of macros to activate when a Door Held Pre-Alarm message is received along with a drop-down list of 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 time schedules.

**Normal Conditions**

- **Host Macro** - Select the Host Based Macro to execute.
- **Edit** - Opens the Host Based Macro edit dialog. See page 10-13 in the Users Manual for more information on Host Based Macros.
- **Unlocked / Schedule** - Drop-down list of macros to activate when a Door Unlocked message is received along with a drop-down list of time schedules.
- **Open / Schedule** - Drop-down list of macros to activate when a Door Open message is received along with a drop-down list of time schedules.
- **Closed / Schedule** - Drop-down list of macros to activate when a Door Closed message is received along with a drop-down list of the available time schedules.
- **Locked / Schedule** - Drop-down list of macros to activate when a Door Locked message is received along with a drop-down list of the available time schedules.
- **Access Granted / Schedule** - Drop-down list of macros to activate when an Access Granted message is received along with a drop-down list of the available time schedules.
- **Access Denied / Schedule** - Drop-down list of macros to activate when an Access Denied message is received along with a drop-down list of the available time schedules.
The Follows Schedule option provides a quick way to set up a door(s) to adhere to a specified time schedule and designated ACM modes. For more information, see page 8-7 in the Users Manual for more information.

- **Enable Door Follows Time Schedule for this door** - Check the box to implement the Follow Time Schedule feature.
  - **Time Schedule to Follow** - Select the desired Time Schedule from the drop down list.
  - **Reader Mode on Activate** - Select the ACM Mode for the door when the specified time schedule becomes active.
  - **Reader Mode on Deactivate** - Select the ACM Mode for the door when the specified time schedule becomes inactive.
Adding Elevators

There are two options when setting up an elevator:

- Non-Feedback - No tracking capability
  - Requires output for each floor (x per cab)
  - Requires reader inside each cab
- Feedback - Ability to track movement
  - All requirements above
  - Requires input for each cab (x per cab)

Before an elevator can be added, you must indicate the elevator parameters in the SSP Properties/Stored Quantities dialog box. See page 3-12.

1. **Right-click** the Elevator object under the SSP object from the tree in the Hardware Browser.

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 Tree select Tree Properties from the menu and check Elevators under the “All Objects Tree Items” heading.

2. **Select** Add Elevator from the menu.
   The New Elevator dialog box opens.

3. **Enter** a user defined Description; typically location or geographical in nature.
   See page 3-31 for more information on the other Common Properties.

4. **Click** the Elevator Objects link on the menu.
   See page 3-33 for more information on each Elevator Object.

5. **Select** Elevator Type from the drop down list.

6. **Enter** the Floor Quantity and the Starting Floor for this elevator.

7. **Select** the Reader options.
   The Edit button will become available when the reader is selected.

8. Feedback Only: **Select** the First Input from the drop down list.

9. **Select** the First Relay from the drop down list.

10. **Enter** the Selection Delay time.
    See page 3-33 for more information on Floor Groups. Floor Groups are covered on page 6-5 in the DNA User Manual.
11. If desired, **configure** the Elevator Parameters dialog per the descriptions on page 3-33.

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

   The elevator is added to the Hardware Tree Browser.

   ![Elevator Tree](image)
Elevator Properties

Common Properties

Address
- Site - Site number for the elevator (auto-populated)
- Controller - Controller for the elevator (auto-populated)
- Elevator Number - Number designation for the elevator.
- Door Type - Determines how the door function.
  - Normal - Door will operate as a regular access control door.
  - Muster - Door will operate as a muster point in addition to 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 a Auto Activate badge, the badge will be activated. See page 7-10 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 a Auto Deactivate badge, the badge will be deactivated. See page 7-10 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 badge, the data will be collected and stored in a separate table as the In Time. See page 5-17 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 badge, the data will be collected and stored in a separate table as the Out Time. See page 5-17 for more information.
  - InfoReader - Works in conjunction with the InfoReader hardware.
- Situations... - Opens the Situation Level Manager Settings dialog for the associated elevator. See Chapter 9 in the Users Manual for more information on Situation Manager.

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 - Selected Alarm Priority overrides the default Event specific priority set in DNA / Administrative / Events & Alarms / Logging. See page 14-23.
- **Security Level** - Category designation. Allows administrator to restrict operator use.
- **Do Not Load Home Page on Alarm** - If associated elevator goes into alarm, the Home Page will not load.
- **Alarm Media File** - Elevator specific alarm file to be displayed when an alarm occurs.
- **Alarm Text** - Point specific alarm text to be displayed in the Alarm Grid when an alarm occurs in addition to the alarm reason.
- **Camera** - Camera associated with the elevator; allowing it to be recalled in the Event Grid as well as in the Alarm Grid.
Elevator Parameters

- Type - Specifies type of elevator.
  - Elevator Reader (No Feedback) - No floor selection information is passed to the SSP.
  - Elevator Reader (Floor Selectors) - Floor selection information will be sent to the SSP.
- Floor Quantity - Number of floors being controlled.
- Starting Floor - The starting floor for the elevator.

Reader

- Reader - Specifies the reader address.
- Edit - Opens the Reader Properties dialog box. See page 3-33.
- Default Mode - Defines the normal state of the reader.
- Offline Mode - Defines offline mode of the reader.

Inputs & Outputs

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

Floor Groups

See page 6-5 in the Users 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 the floors that will available if the elevator enters Facility Code Mode. This may be useful when commissioning a system and access levels have not been created/assigned.
- Off-line Mode - Specifies the floors that will be unlocked if the SSP (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 readers to select for Reader 2.
- Edit - Opens the Edit dialog for this object.
- Reader Type - Drop-down list of reader types to select for Reader 2.
**Elevator Parameters**

![Elevator Parameters screenshot]

**Attributes**
- Default LED Mode - Drop-down list of LED Modes to select for default.

**Anti-Pass Back (APB) Settings**
See Chapter 11 in the Users Manual for information on configuring Anti-Pass Back.
- Option - 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. (Area-based Soft)
  - 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)
  - 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 be enabled in the SSP Properties / Stored Quantities dialog. (Reader-based using the readers last user)
  - Check last ACR used, no location change - Disallows a cardholder from presenting his 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 card is presented at another reader in the system or APB delay has expired. Requires Support Timed Anti-Pass Back be enabled in the SSP Properties / Stored Quantities dialog. (Reader-based using the cardholders access history)
  - Check current location, change on entry - Similar to option #2, except the APB delay will reset user’s area after the specified time. Requires Support Timed Anti-Pass Back be enabled in the SSP Properties / Stored Quantities dialog. (Area-based)
- Delay - Number of minutes before APB resets. Only used in conjunction with APB options 3-5. Max. delay = 255 minutes
- From Area - The area number the user comes from.
- To Area - The area number the user enters.

**Elevator Functions**
- Decrement Use Limits - This door decrements Use Limit associated with card.
- Require Use Limit > Zero - If use limit reaches 0, do not allow access.
- Set to Deny Duress - Denies access upon receiving a duress signal. PIN & Card Mode only.
● Log All Access Requests as Used - Assume that the door was used and log all access requests as used Door Used as soon as the request is granted. Not for use with Anti-Pass Back.

● Require 2 Card Control - Requires two access credentials to be presented.

● Biometric Verification - Biometric hardware is being supported. This is an advanced feature and should be avoided unless the operator has a understanding of the ramifications.

● Enroll on Access - Biometric hardware is being supported and the system should record the 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 page 3-10 Host Response Time to set the timeout parameter.

● Grant If Host Offline - Access will be granted in the event the Host is not available. Works in conjunction with Host Verification.

● Enable Cypher Mode - Allows 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 is not logged until door is actually opened or timeout expires. Access Granted events only.

● Wait for Missing Card - If an access request is denied due to “card not in file,” the reader is put into the wait state and waits for host response.

**Follows Schedule**

The Follows Schedule option provides a quick way to set up a door(s) to adhere to a specified time schedule and designated ACM modes. See page 8-12 in the Users Manual for more information.

● Enable Door Follows Time Schedule for this door - Check the box to implement the Follow Time Schedule feature.
  - Time Schedule to Follow - Select the desired Time Schedule from the drop down list.
  - Reader Mode on Activate - Select the ACM Mode for the door when the specified time schedule becomes active.
  - Reader Mode on Deactivate - Select the ACM Mode for the door when the specified time schedule becomes inactive.
Configuring Readers

Readers can be configured as Proximity, Wiegand Insertion or Magstripe; with or without a keypad; or as a specific model of reader. How the reader is configured in the device properties defines how the SSP expects the data to be formatted. Incorrectly identifying the reader type can cause Invalid Data errors during card reads.

1. **Right-click** the Reader object under the Subcontroller object from the tree in the Hardware Browser.
2. **Select** Properties from the menu.
   
The Reader Properties dialog box opens.

3. **Populate** the appropriate fields to configure the reader settings.

Reader Properties

*Common Properties*

**Address**
- Site - Site location for this reader. (auto-populated)
- Controller - Controller for this reader. (auto-populated)
- Sub-Controller - Sub-Controller for this reader. (auto-populated)
- Point/Reader - Point or reader number. (auto-populated)
- Type - Type of point. (auto-populated)
- Door ID - Door associated with the reader. 0 indicates that the reader has not been associated with a door. (auto populate)

**Distribution / Other**
- Description - User-defined description of the door; typically location related.
- Home Page - Home page associated with the reader.
Reader Properties

- **LED Configuration** - Drop-down menu of the LED configurations.

  *A batch file can be used to load a LED Mode table to a reader to make the LED lights behave in a manner other than default. See page 5-4 for more information on Batch Processing or page 5-4 for more information on LED Control.*

- **Keypad Mode** - Drop-down menu of the keypad modes.
- **Reader Type** - Drop-down menu of the reader types.

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** - Used with Keypad Readers.
- **CASI 1-Wire F2F** - If checked, flags the reader as using CASI F2F output format.

Advanced Properties

- **Host Based Macro** - Select a Host Based Macro to associate with this reader.
- **Edit** - Opens the Host Based Macro Edit dialog box. See page 10-13 in the User Manual for more information.

Templates

- **Template Name** - Select a template to configure the reader.
- **Description** - Auto populated by the template.
- **Application Notes** - Auto populated by the template.
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 (RXE) buttons and motion detector contracts. They can also be used to monitor dry contacts from fire alarm panels, temperature and pressure alarms, etc.

1. **Right-click** the Input Point object under the Subcontroller object from the tree in the Hardware Browser.
2. **Select** Properties from the menu.
   
   The Input Point Properties dialog box opens.

3. **Populate** the appropriate fields to configure the input point settings.

**Input Properties**

*Common Properties*

**Address**

- Site - Site location for this input point. (auto-populated)
- Controller - Controller for this input point. (auto-populated)
- Sub-Controller - Sub-Controller for this 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. 0 indicates that the input has not been associated with a door. (auto populate)
- Situations - Opens the Situation Level Manager Settings dialog for the associated point. See Chapter 9 in the Users Manual for more information on Situation Manager.

**Distribution / Other**

- Description - User defined description of the input point; typically location related.
- Home Page - Home page associated with the reader.
- Do Not Load Home Page on Alarm - If associated 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 Setting 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.

● **Alternate Priority** - Selected Alarm Priority overrides the default Event specific priority set in DNA / Administrative / Events & Alarms / Logging. See page 14-23.

● **Alarm Media File** - Output specific alarm file to be displayed when an alarm occurs.

● **Alarm Text** - Point specific alarm text to be displayed when an alarm occurs in addition to the alarm reason.
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 1-3

- Sensitivity - Number of consecutive input scans before a change of state is reported. A low sensitivity setting (2) requires the system to receive this number of consecutive readings from an input prior to reporting a change of state. A high sensitivity setting (15) will require the input to report 15 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.) 4 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.

- 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 change of state events will be logged but change of state events will not be logged if they are masked.
  - No masked contact COS + no fault to fault COS - Contact change of state will not be logged if masked and no fault to fault changes.

- Latching Mode - Type of latching mode. Only used with configuring entry and exit delays common with secured areas.
  - Normal - Select Normal 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. A event will be generated when the change of state happens, but no alarm would be received. If selected, an Entry and Exit should be set.
Hardware Configuration

- **Latch** - 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 preferred setting. If selected, an Entry and Exit 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** - Enables camera menu item in Event/Alarm grid context menus. When enabled, the operator may click a menu item to display camera view browser.

- **Host Based Macro** - Select a Host Based Macro to associate with this reader.

- **Edit** - Opens the Host Based Macro Edit dialog box. See page 10-13 in the Users Manual for more information.

**Templates**

- **Template Name** - Select a template to configure the reader.

- **Description** - Auto-populated by the template.

- **Application Notes** - Auto-populated by the template.
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, etc.

1. **Right-click** the Output Point object under the Subcontroller object from the tree in the Hardware Browser.
2. **Select** Properties from the menu.
   The Output Point Properties dialog box opens.

3. **Populate** the appropriate fields to configure the output point settings.

## Output Properties

### Common Properties

#### Address
- **Site** - Site location for this input point. (auto-populated)
- **Controller** - Controller for this input point. (auto-populated)
- **Sub-Controller** - Sub-Controller for this input point. (auto-populated)
- **Point/Reader** - Point or reader number. (auto-populated)
- **Type** - Type of point. (auto-populated)
- **ACM Number** - Access Control Model number for the reader. 0 indicates that the output has not been associated with a door. (auto populate)
- **Situations...** - Opens the Situation Level Manager Settings dialog for the associated point. See Chapter 9 in the Users Manual for more information on Situation Manager.

#### Distribution / Other
- **Description** - User defined description of the input point; typically location related.
- **Home Page** - Home page associated with the reader.
- **Do Not Load Home Page on Alarm** - If associated 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.
Hardware Configuration

- **Alarm States** - If Local Setting 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.

- **Alternate Priority** - Selected Alarm Priority overrides the default Event specific priority set in DNA / Administrative / Events & Alarms / Logging. See page 14-23.

- **Alarm Media File** - Output specific alarm file to be displayed when an alarm occurs.

- **Alarm Text** - Point specific alarm text to be displayed when an alarm occurs in addition to the alarm reason.

**Output Properties**

![Output Properties](image)

- **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.

**Advanced Features**

- **Host Based Macro** - Select a Host Based Macro to associate with this reader.
- **Edit** - Opens the Host Based Macro Edit dialog box. See page 10-13 in the Users 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 Fusion User Manual.

There are numerous NVR/DVRs that are compatible with the DNA Fusion system.

- Milestone
- Dedicated Micros
- Instek
- Pelco
- Pelco Endura
- Salient
- General Solutions
- Cathexis
- Integral
- ONSSI
- 3x Logic
- Aviligon
- Panasonic
- Intervid
- Exacq Vision

Setting up the NVR/DVR integration is a three step process:

1. Run the NVR/DVR Integration installation.
2. Configure the NVR/DVR within the DNA system.
3. Add the cameras to the Fusion system.

NVR/DVR Integration

For Milestone integrations, run the Milestone Remote Client installation on the desired workstations.

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 DVR.
   The Open File - Security Warning dialog will appear.
3. Click Run to start the installation process.
   The InstallAware Wizard dialog will open.

Before installing the DVR Integration, Open Options recommends backing up the DNA Fusion database as well as closing all open programs.

4. Click Next to continue the installation.
   The file location screen is displayed.
5. Click Next to accept the default location (Default: C:Program Files\DNA Fusion) or click the Browse button to specify a different location.
   The Installation screen will appear.
6. Click the Next button to start the installation.
   Installation will begin.
7. When installation is complete, click Finish to complete the setup.
Configure the NVR/DVR

1. **Open** DNA Fusion and **select** the DVR Browser icon from the Standard Toolbar.
   The DVR Browser opens.

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

3. **Enter** a Description for the DVR server.

4. **Enter** the DVR’s address in the IP Address field.

5. **Enter** the User Name and Password for the DVR.

6. **Select** the Authentication Mode from the drop down list.
   This must match the Authentication Mode setting on the DVR server.
   
   ![For Milestone Enterprise systems, select Basic Authentication. For Milestone Corporate systems, select Windows Authentication.](image)

7. **Select** the Server GMT Offset from the drop down list.
   For Instek Integrations only: **Select** the Casablanca setting from the list; all of Instek’s time is stored on the server. For all other types, **select** the correct GMT offset for the server.
   Once selected, the Server Time will appear to the right of the drop down.

8. **Select** the DVR Type from the drop down list.
   For Cathexis Integrations, **select** the Intervid option.

9. **Click** OK to save the settings and add the DVR.
   The DVR server appears in the DVR Browser.
Add the Cameras

1. **Right-click** on the DVR Server Node in the Hardware Browser and **select** Scan for Cameras.

   A plus sign appears by the server and the cameras are automatically added to the system. Clicking the plus sign reveals the cameras.

   **For Integrations that don’t support scan for cameras:**

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

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

   The Camera Properties dialog opens.

   b. **Enter** a Description and Camera Number for the camera.

   c. **Click** the OK button to save the camera.

   d. **Repeat** until all required cameras have been added.

Associating a DVR Camera to a Door

1. **Right click** on the ACM point and **select** Properties.

2. From the Common Properties page, **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 archived video is available for that particular event. See pages 14-7 and 14-18 in the DNA User Manual for more information on recalling archived video. A Host Based Macro can also be created to automatically open the Video Window when a particular event occurs.
Adding Cameras

IP cameras may be added to Fusion; allowing the operator to monitor the camera from the system.

1. **Right-click** the Site object from the tree in the Hardware Browser.

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

2. **Select** Add Camera from the menu.
   The Camera Properties dialog box opens.

3. **Enter** a Name and if desired a Description for the camera.
4. **Select** IP Camera from the Camera Type drop down list.
5. In the URL or IP Address field, **enter** the URL or IP Address where the camera is located.
6. **Assign** a Priority setting for the camera.
   This setting ties to the Video Window setting. See page 3-25 in the User Manual.
7. **Click** OK to save the settings.
   The camera is added to the camera list in the Hardware Browser.

   **Associating a Camera to a Door**

1. **Right click** on the ACM point and **select** Properties.
2. From the Common Properties page, **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 video is available for that particular event. See pages 14-7 and 14-18 in the DNA User Manual for more information on recalling archived video. A Host Based Macro can also be created to automatically open the Video Window when an event occurs.
Card Formats

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

Creating a Card Format

1. **Right-click** on the SSP in the Hardware Browser.
2. **Select** Card Formats from the menu. The Card Formats Dialog box opens.
3. **Select** the option below and continue.
   - New Card Format
   - Edit Card Format
   - Copy Card Format

Creating a New Card Format

1. **Click** the New button.
2. **Enter** a name in the Description field.
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 Format from the 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 allows you to easily identify the bit format and the facility code for an access credential.

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Event Description</th>
<th>Card #</th>
<th>Last Name</th>
<th>First Name</th>
<th>Event Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Side Door</td>
<td>Access Denied: Invalid Card Format</td>
<td>0</td>
<td>?????</td>
<td>?????</td>
<td>26 bits: 99700200</td>
</tr>
</tbody>
</table>

3. **Assign** the generic card format that contains the same bit structure as the card to the SSP.
   
   See Assigning a Card Format above.

   In our example, we would **select** the HID 26 bit with Facility Code.

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).

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Event Description</th>
<th>Card #</th>
<th>Last Name</th>
<th>First Name</th>
<th>Event Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Side Door</td>
<td>Access Denied: Facility Code</td>
<td>91</td>
<td>???</td>
<td>???</td>
<td>Part: 0, FC: 47 Issue: -1</td>
</tr>
</tbody>
</table>

6. **Create** the card format by following the instructions on page 3-49 for Copying a Card Format.
7. **Assign** the newly created card format to the SSP.
   
   See Assigning a Card Format below.
   
   Be sure to overwrite or delete the generic card format added in step 3.

8. **Download** the changes to the SSP.

**Assigning a Card Format to the SSP**

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

1. **Right-click** on the SSP in the Hardware Browser.
2. **Select** Properties from the menu.
   
   The Controller Properties dialog box opens.

3. **Select** the Cards and Dual Comm tab from the menu.

4. **Select** the formats (0-7) from the Card Formats drop-down.
5. **Click** OK to save the formats to the controller.
Upgrading DNA

In This Chapter

| ✓ | Server Upgrades |
| ✓ | Client Upgrades |
| ✓ | Fusion License Updates |

There are two types of upgrades that can be performed: software upgrades and license updates. Both types will be discussed in this section.

**Software Upgrades**

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

Depending on the version of DNA the site is running prior to the upgrade, follow the instructions below for the correct version instructions.

**NPower DNA to DNA Fusion 5.0 and above**

When upgrading from NPower DNA to DNA Fusion, the upgrade will need to be performed at the server prior to upgrading each client workstation.

1. Close NPowerDNA.
2. Backup the NPowerDNA database.
3. In Windows Explorer, double-click the upgrade executable file.
   - The Upgrade Welcome Screen will appear.
4. Click Next.
5. Read the License Agreement and select the I accept the agreement radiobutton and click Next to continue.
6. Verify the User Information and click Next.
   - The SQL Server Instance dialog will open.
7. Verify the Instance Name and click the Test Connection button.
   - If the Instance Name 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.
    - If any information on this screen is incorrect, click the Cancel button. The upgrade will need be performed in a different manner.
Upgrading DNA

a. **Click** Start and **select** Run.
b. **Type** cmd and **click** OK.
c. **Type** cd and the location of the setup file to change the location of the prompt.
   Example: cd desktop
d. **Type** setup forcenew.
   A new installation will begin. Follow the instructions on page 2-7 for a server or 2-15 for a client.

11. **Click** Install.

   The upgrade process will begin.

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

---

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.
**DNA Fusion Service Pack**

When a new service pack or version is released, only the DNA Server needs to be updated. All client workstations will check the Server for updates upon start up and will automatically synch with the server to ensure the latest version is running across the entire system.

1. **Close** DNA Fusion.
2. **Backup** the NPowerDNA database and if needed,
3. In Windows Explorer, **double-click** the upgrade executable file.
   The Upgrade Welcome Screen will appear.
4. **Click** Next.
5. **Read** the License Agreement and **select** the I accept the agreement radiobutton and **click** Next to continue.
6. **Verify** the User Information and **click** Next.
   The SQL Server Instance dialog will open.
7. **Verify** the Instance Name and **click** the Test Connection button.
   If the Instance Name 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.

If any information on this screen is incorrect, **click** the Cancel button. The upgrade will need be performed in a different manner.

a. **Click** Start and **select** Run.

b. **Type** cmd and **click** OK.

c. **Type** cd and the location of the setup file to change the location of the prompt.
   Example: cd desktop

d. **Type** setup forcenew.

   A new installation will begin. Follow the instructions on page 2-7 for a server or 2-15 for a client.

11. **Click** Install.
   The upgrade process will begin.
12. **Click** Finish to complete the Server Upgrade.
Fusion Client Upgrades

After the upgrade is performed on the Fusion Server, all client workstations will check for updates upon start up and will automatically synchronize with the server to ensure the latest version is running across the entire Fusion system.

1. **Log in** to Windows with an Administrator Account or an Account that is a Local Administrator.
   
   If the Windows user does not have rights to install software, Fusion will not update.

2. **Launch** the DNAFusion application.
   
   The dnaLauncher dialog will open.

   The upgrade process will continue automatically.

   If the update fails to install, run the upgrade from the DNAFusion Installation Application. See page 2-15 for information on Client Installations.

3. **Log in** to Fusion.

   The Client Upgrade is complete.
License Updates

Changes or additions to a Fusion systems configuration may require additional licensing depending upon the type additions to the system. The process below is for DNAFusion version 5.2 and above.

Older versions may require additional steps that are outlined in the License Update email.

There are currently three (3) methods of licensing Fusion.

- **Soft Key** - The Soft Key licensing information was entered upon 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 Fusion Server running the DNA Driver. An internet connection is required for automatic updates.
- **License File** - If no Internet connection is available, a file will be provided by Open Options Technical Support that contains the updated Licensing information for the Site.

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

- Client Workstations
- Universal Driver
- Sub-Controllers
- Drivers for Alarm Panels & CCTV
- Photo Badging
- Active Directory Operator Plug-In
- Fusion Web
- OpenDX

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 automatically be downloaded from the Open Options Licensing Server. If there is no Internet connection, see the License File information below.
   - **HASP Key**: If the system is using a HASP Key and has an internet connection, the updated licensing information will automatically be downloaded from the Open Options Licensing Server. If there is no Internet connection available, a license file will be provided by Open Options.
   - **License File**: Install the updated License File provided by Open Options. Contact Open Options Order Entry Department with the Soft Key ID (Help / About DNA) prior to the upgrade date.
There are numerous support tools that are available for use with DNA. This chapter will cover the following tools:

- **Table Purger Tool** - Deletes certain information in specific fields from the NPowerDNA database.
- **DNA Batch Download Settings Utility** - Allows batch files to automatically be downloaded to the desired controller. For instance, a batch files might load an LED Mode table.
- **DNA LED Control Application** - Allows customization of the LED Mode for a door.
- **SMTP Mailer** - Monitors a defined set of folders for new files. Any files matching the defined file specification are emailed as an attachment to the specified recipients.
- **Remote Archive Utility** - Reoccurring archive tool that allows the Alarms, Audits and Transactions tables to be archived on different schedules.
- **Auto Expire Tool** - Deactivates card that do not any usage history within the specified timeframe.
- **Event History Report Utility** - Allows customized Event History reports to be generated without the need for a DNA client.
- **Time & Attendance Report** - Provides a simple way to utilize the DNAFusion system to gather time in/out information.
- **DNA Import Tool** - The Import tool is a simple manual method to copy data from a source to the DNA Fusion database.
This Page Intentionally Left Blank
**Table Purger Tool**

The Table Purger application is an executable file that deletes certain information from the NPowerDNA database. It can be downloaded from the openoptionsinc.com ftp site.

**To run the Table Purger:**

1. **Close** the DNA Fusion Server and all Fusion Clients.
2. **Double click** the Table Purger.exe file.
   - The Table Purger 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 Subcontrollers licensing. There is also a record for each site as well as for each station.
   - **Stations** - Deletes the Unique Name and Number Station Information for all Fusion workstations from the database.
4. **Click** the Purge button.
   - The selected information will be removed from the SQL tables.
   - The purge is immediate, and a confirmation message will not be displayed.
5. **Open** DNA Fusion on the Server, **verify** the Station Name and Number information 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 Fusion Server.
7. **Right click** in the Hardware Browser and **select** Site / 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 start up and send it to the controller.

1. **Locate** the DNABatchDownloadSetting.exe file and **double click** the icon to open the application.
   
   Default Location: `C:\ Program Files\ NPowerDNA\ Tools`
   
   The DNA Batch Download Settings dialog will open.

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 Fusion system downloading to the controller.

6. **Click** the Browse button next to the File Name field to identify the text command file to be downloaded.
   
   The file must reside in the following location: `C:\ Program Files\ NPowerDNA\ Batch`

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

The command will appear in the main window.

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

---

**DNA LED Control Application**

The DNA LED Control Application allows for the customization of the LED Mode tables for a door.

1. **Locate** the dnaLEDControl.exe file and **double click** the icon to open the application.
   
   Default Location: `C:\ Program Files\ NPowerDNA\ Tools`
   
   The dnaLEDControl dialog will open.

2. **Select** the desired SSP number from the drop down list.

3. **Select** the LED Mode table to edit.
   
   There are three (3) LED Modes for a door; the LED Mode is specified during door configuration. See page 3-23 for more information.
   
   - **1** = Door Object Short Red Pulse
   - **2** = Solid Red Short Pulse
   - **3** = Solid Green Short Pulse

   This setting will determine which table is edited.

4. **Select** the ACR Mode or Door State 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\ NPowerDNA\ Batch`

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

---

*Batch processing can also be performed manually from within the DNAFusion application. See page 20-14 for more information.*

---

*Additional Apps*
SMTP Mailer

The SMTP Mailer program monitors a defined set of folders for new files. Any files matching the defined file specifications are emailed as an attachment to the specified recipients. The SMTP Mailer runs as a Task Tray application.

Installation

1. **Double click** Setup.exe to begin the installation.  
The Welcome screen appears.
2. **Click** the Next button to continue.  
The Destination Location screen is displayed.
3. **Click** the Next button or select the Browse button to specify a different location.  
The Additional Tasks screen appears.
4. If desired, **click** the Create a desktop icon checkbox and **click** Next.  
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.  
If desired, uncheck the Launch Open Options SMTP Mailer checkbox.  
If the Launch Open Options SMTP Mailer checkbox is checked, the application icon will appear in the Task Tray.

While the application may be accessed from the Start Menu or via the Desktop shortcut, the install will create an icon in the Startup folder. This allows the application to be started every time a user logs in.

Configuration

The application is configuration of through the OOSMTPMailer.INI file which is located in the SMTP application directory.

1. **Open** the OOSMTPMailer.INI file.  
Default Location: C:Program Files\NPowerDNA\Tools\OOSMTP

The INI file includes all the settings for the SMTP Mailer application. The following settings are available:

- **SMTP Settings** - The SMTP connection information is setup in this section. This includes the SMTP Server name, the server port, type of Authentication, User Name and Password as well as if SSL (Secure Sockets Layer) is used.
- **Directory 1-10 Configuration** - Allows different watched directories and separate email address to be identified.
- **Email Settings** - Contains the email addresses for the selected recipients.
2. **Enter** the SMTP information for each field.
   - **Host** - Enter the SMTP Server name.
   - **UserName** - Enter the User Name and Password for authentication.
   - **Authentication** - Enter 0 for User Name/Password or enter 1 for Password.
   - **UseSSL** - Enter 0 if not using SSL or enter 1 if using SSL.
   - **Port** - Enter the port for the Server.

   Leave the SMTP section empty if there is no existing SMTP server. The application will use a default SMTP serving utilizing SSL.

3. **Edit** the Dir1 settings.
   - **WatchDirectory** - If desired, specify a different monitored folder.
   - **WatchFileSpec** - Indicates the type of file to send to the email recipients. The asterisk allows any file with the specified extension to be sent.
   - **To** - Enter the email address for the recipients in either Standard format (username@domain.com) or Display Name format (Display Name <username@domain.com). Multiple email addresses must be separated with a semicolon.

4. If desired, **configure** additional Directories to watch different directories and send the reports to different email addresses.

   The program supports up to 10 separate email directories (in the format Dir1, Dir2, Dir10) with each one allowing individualized email settings. Any email items that are common between watched directories may alternatively be defined in an Email section using the same format.

   Leaving the To: item out of a Directories configuration (Dir1-Dir10) will cause the default value from the Email section below to be used.

5. **Enter** the Email information.
   - **From** - If desired, edit the From address for the emails.
   - **To** - Enter the email address for the recipients in either Standard format (username@domain.com) or Display Name format (Display Name <username@domain.com). Multiple email addresses must be separated with a semicolon.

To automate this process, reports can be scheduled in the DNAFusion application. The report can then be exported to the specified Watch Directory in the indicated format. See Chapter 19: Scheduling for more information.

### Running the Program

The OOSMTP Mailer runs as a Task Tray application. An icon will appear in the Task Tray.

#### To view the status of the Mailer:

1. **Right-click** on the Task Tray icon.
2. **Select** Show Log Window from the menu.

   A report will open that includes every report that has been emailed since startup.

   Closing the report will not shut down the program; the icon will return to the Task Tray.

### Exiting the Program

#### To shut down the program:

1. **Right-click** on the Task Tray icon.
2. **Select** Exit Program from the menu.

   The program will startup again when the computer is restarted.
Remote Archive Utility

The Open Options Remote Archive Utility is a recurring archive program. Archiving allows the database to create space for new transactions. After installation, a batch file will need to be created to execute the Archive Tool; the batch file will be scheduled via the Windows Task Scheduler.

Installation

The Archive Utility must be installed on the DNA server.

1. **Double click** DNA Archive Setup.exe to begin the installation.
   
The Welcome screen appears.

2. **Click** the Next button to continue.
   
The Destination Location screen is displayed.

3. **Click** Next button or **select** the Browse button to specify a different location.

4. **Select** the Components that will be installed and **click** Next.
   
   - **Server and Client Tools** - **Select** the Server and Client Tools option to install the DNA Archive Service and the configuration interface. The DNA Archive Service is the service that runs in the background and completes the archiving task.
   
   - **Only Client Tools** - **Select** the Only Client Tools option to install the Remote Utility interface. The interface allows the user to execute archive operations against the database. The client tool can be run from anywhere on the network as long as the server machine can be accessed and the needed ports are not blocked by a firewall.

   The **Select** Data Directory dialog is displayed.

5. **Click** the Browse button to locate the desired archive folder.

6. When the path is displayed in the field, **click** the Next button to continue the installation.

7. **Click** Next to accept the default folder or **click** the Browse button to specify a different location.

   The Ready to Install window opens.

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

   The installation begins.

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

   During the installation, the NPowerDNA Data Archive Service is created and started. To verify that the service is running, **right click** on the My Computer icon in the Start Menu and **select** Manage. Open the Services and Applications tree item and **select** the Services option. Locate the NPowerDNA Data Archive Service in the list; **select** the service to see the status.
1. **Open** the Remote Archive Utility.
   Default location: C:\ Program Files\ NPowerDNA\ Archive Tools
   The DNA Remote Archive Utility dialog opens.

   ![DNA Remote Archive Utility dialog](image)

2. **Select** Connect To Server.
   The Connection Options dialog appears.

3. **Enter** the computer name of the DNA Server and **click** OK.

   ![Connection Options dialog](image)
   If needed, **edit** the port number.
   The connection status will appear in the DNA Remote Archive Utility window.
   If the connection was successful, continue to step 4.
   If the connection was unsuccessful, return to step 2.

4. **Specify** the number of Days To Keep In Database.
   This setting determines the amount of data that will be left in the database; i.e. if 30 is entered, the DNA database will contain the last 30 days of information. Any data that is more than 31 days will be archived out when the tool is run.
   During the installation, the DNA Data Archive Service is created and started. To verify that the service is running, **right click** on the My Computer icon in the Start Menu and **select** Manage. **Open** the Services and Applications tree item and **select** the Services option. Locate the DNA Data Archive Service in the list; **select** the service to see the status.
   If needed, configure any firewalls to allow communication on the following ports: Server TCP port is 22953 and the Client TCP port is 22954.

5. If needed, **select** the Set Data Path option to indicate the destination folder.
   The destination folder is originally set during installation.
Running the Program

The NPowerDNA Remote Archive Utility provides an easy interface to archive specific table types.

To manually archive data:

1. **Open** the DNA Remote Archive Utility.
   - Default location: C:\Program Files\NPowerDNA Archive Tools
   - The DNA Remote Archive Utility dialog opens.

2. **Select** the type of archive to execute.
   - Archive Transactions - Select to archive Event History only.
   - Archive Alarms - Select to archive Alarms only.
   - Archive Audits - Select to archive Operator Actions only.
   - Archive All - Select to archive Event History, Alarms and Operator Actions.
   - The selected item(s) will be archived and placed in the designated location in XML format.

3. **Close** the DNA Remote Archive Utility application.

Scheduling the NPowerDNA Remote Archive Utility

To automatically execute the Remote Archive Utility, a batch file will need to be created and then scheduled via the Windows Scheduler.

1. From the **Start Menu**, **select** All Programs/Accessories and **select** the Notepad application.
   - The Notepad will open.

2. **Add** the following information to the text file.
   - The following example is based on the default installation paths.
   - "C:\Program Files\npowerdna archive tools\ArchiveScheduler.exe" DAYS -Table Types
   - DAYS - Specify the number of days to keep in the database. For example, if 30 is entered the DNA database will contain the last 30 days of information. Any data that is more than 31 days will be archived out when the schedule is run.
   - Table Types - **Enter** one or any combination of the following values.
     - -T = Archives Event History only
     - -A = Archives Alarms only
     - -AD = Archives Operator Actions only
     - -ALL = Archives Event History, Alarms and Operator Actions
   - **EXAMPLES**:
     - "C:\Program Files\npowerdna archive tools\ArchiveScheduler.exe" 180 -ALL
     - The example above would backup all transactions and retain 180 days of information in the database.
     - "C:\Program Files\npowerdna archive tools\ArchiveScheduler.exe" 45 -T
     - The example above would backup the Event History only and retain 45 days of information in the database.
     - "C:\Program Files\npowerdna archive tools\ArchiveScheduler.exe" 30 -T-A
     - The example above would backup the Event History and Alarms only and retain 30 days of information in the database.

3. **Select** File / Save As and **enter** a name.
   - The file should be saved in the DNA Archive Tools folder.

4. **Close** the Notepad application.

5. **Open** Windows Explorer and **locate** the saved file from step 3.

6. **Change** the file extension to .BAT.
   - The files 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 archive the database based on the designated schedule.
AutoExpire Tool

The Open Options AutoExpire Tool will deactivate cards that do not have any usage history within a specified number of days. The AutoExpire tool has two modes of operation: Configuration and Silent.

- **Configuration Mode** - Opens the AutoExpire dialog and allows an Employee Type to be selected and the number of inactive days to be specified.
- **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 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 the Silent Mode and a card meets both requirements specified above, 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 at 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 will be created and scheduled via the Windows Scheduler.**

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 files 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 customized Event History reports to be generated without a DNA client. The reports are generated in standard pdf format and can be automatically emailed via the SMTP protocol to one or multiple recipients.

Installation

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

**The application is normally run as a Background Task in the Task Manager so no program icon is created.**

**Email Setup**

If reports will be scheduled and emailed to a recipient, the email options will need to be setup.

1. **Locate** and **open** the DNAEventHistory.exe application.
   Default Location: C:\ Program Files\ NPowerDNA\ Tools\ DNAEventHistory
   The DNA Event History Report dialog opens.
2. **Click** the Email 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 email configuration information will be returned.
   **Example:**
   Mailer Server Name
   OutboundMailPort = 25
   If no connection to port 25, see the system administrator and request that SMTP be enabled and /or modify any anti-virus software to allow the DNAEventHistory.exe to email 3rd party emails.
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 field.
7. **Enter** a valid Reply Email address.
8. **Select** the Email Recipients tab.
9. **Select** the Email Address field and **enter** the desired email address.
   A Displayed Name may also be entered for the recipient.
10. **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\NPowerDNA\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 keys 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 MPG section.
6. If needed, **select** the desired Events from the list on the Events tab.
   Use the Shift or Control keys to select multiple items.
7. If desired, **check** the Filter by Card checkbox and **select** the card(s) 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 will open.

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 will 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 **navigate** to the desired pdf file location. Prior to this step a pdf document will need to be created if it does not already exist. Default Location: C:\Program Files\NPowernDNA\Scheduled Reports.
4. **Select** the Selection Criteria Template from the drop down list. For information on creating Templates, see page 5-14 step 8.
5. If desired, **select** the Email PDF checkbox to email the report to the specified recipients. See page 5-13 for more information on setting up email.
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 will open.
9. **Click** the New button.
10. **Specify** the desired Schedule and **click** OK.

The report will appear 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 will open.
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 & Attendance Report captures In and Out information to simplify payroll. When a Time & Attendance card is presented at the specified door the information is written to the DNATimeAttendanceRpt table in the database. This information includes the cardholder name, whether the door used was a In or Out door, date and time, card number, card type, title, department and the Employee ID number.

Some form of SQL Server Management software must be installed prior to starting the setup procedure. If needed, the SQL Server Management Studio Express installation can be downloaded and installed.

**Installing the Time & Attendance Report**

1. **Double click** dnaTASetup.exe to begin the installation.
   The Welcome screen appears.

2. **Click** the Next button to continue.
   The Password dialog appears.

3. **Enter** the Open Options supplied Password and **click** Next.
   The password can be obtained contacting Open Options Technical Support.
   The Destination Location screen is displayed.

4. **Click** the Next button or **select** the Browse button to specify a different location.
   The Start Menu screen is displayed.

5. **Click** the Next button to continue or **select** the Browse button to specify a different folder.
   The Additional Tasks screen appears.

6. If desired, **click** the Install Desktop icon checkbox and **click** Next.
   The Ready to Install window opens.

7. **Click** the Install button to start the installation.
   The installation begins.

8. **Click** the Finish button to complete the installation.
Setting up the Time & Attendance Report

The first step is to prepare the NPowerDNA database for the project data as well as creating the new Host Based Macros that will populate the database.

1. **Open** the DNA Time and Attendance Report folder.
   
   Default Location: C:\ Program Files\ DNATimeAttendanceRpt

2. **Double click** the DNATimeAttendanceRpt_Create.SQL query.
   
   This SQL query creates the initial project table and the associated indexes.
   
   The SQL Server log in dialog appears.

3. If required, **enter** the log in information and **click** the Connect button.
   
   SQL Server Management Studio will open.

4. **Select** the NPowerDNA database option from the drop down and **click** the Execute button.
   
   The results will appear in the Message Window.

5. If running DNAFusion 5.0.0.1135 and 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.
   
   SQL Server log in dialog will open.

6. If required, **enter** the log in information and **click** the Connect button.
   
   SQL Server Management Studio will open.

7. **Select** the NPowerDNA database option from the drop down and **click** the Execute button.
   
   The results will appear in the Message Window.

8. **Double click** the HBMacro.SQL query to open the file.
   
   SQL Server log in dialog will open.

9. **Click** the Cancel button.
   
   SQL Server Management Studio will open with the HBMacro query.

10. **Select** the text in the query and copy it to the clipboard.
11. **Open** DNAFusion and **select** the Triggers & Macros button on the Standard Toolbar.
   The Triggers & Macros Browser will open.

12. **Select** the Host Based Macro tab.

13. **Right click** on the Host Based Macros header and **select** Add Host Macro.
    The Host Based Macros dialog opens.

14. From the Local Object Type (Controlling Object) drop down, **select** the Door option.
    A resulting list of options will appear in the Event ID drop down.

15. **Select** the desired Door Event that appears in the Event Grid when badging at the Time & Attendance Doors.
    Generally this will be Event ID: 072: Access Granted: Door Used.
    The SQL will be run from the DNA driver 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%), and current time (%PTIMEDATE%) as well as the cardholder first and last name.

16. From the Remote Object Type (Controlling Object) drop down, **select** the Add to Database with Events Server option.
    A resulting list of options will appear in the Event ID drop down.

17. **Click** the Build button under the Action 1 header.
    The NPower DNA SQL Query Editor opens.

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

19. **Customize** the following as needed.
    - If Custom Personnel Types are used in Fusion, modify the Custom 1-5 (6-10) text strings under the Personnel Type section.
    - Edit the Door (%ADDR%) case statement to designate the doors which will be used as the Entry and Exit doors. A ‘1’ indicates an entry door and a ‘0’ identifies the exit door.
    For instance, if door 1.1.D10 is the entrance door and 1.2.D1 the exit. The SQL statement would be edited as follows
      WHEN ‘1.1.D10’ THEN 1
      WHEN ‘1.2.D1’ THEN 0
    There is no limit on the number of entry/exit door combinations that can be identified.

20. **Click** OK to save the statement.

21. **Click** OK to save the Host Based Macro.

22. **Locate** the designated doors in the Hardware Browser, **right-click** on the first door and **select** Properties.

23. **Select** the Macros link from the menu on the left side.

24. **Click** the Host Based Macro drop down and **select** the Host Based Macro created in step 11.

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

26. Repeat steps 22-25 for the other designated Entry/Exit doors.
Below is the complete HBMacro.SQL statement:

```sql
INSERT INTO DNATimeAttendanceRpt
(Card,Lname,Fname,[Type],[UDF],Dept,Title,UserID,[Direction],[TranDate],Company,EmpID,SSN)
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 'Teacher'
WHEN 7 THEN 'Admin Staff'
WHEN 8 THEN 'Sub'
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 '1.2.D3' THEN 1
WHEN '1.2.D5' THEN 0
ELSE 0
END AS [Direction],
'%%TIMEDATE%%' AS [TranDate],
[Company].[Company],
[Personnel].[EmpID],
[Personnel].[SSN]
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)
```

Generating a Time & Attendance Report

1. Open the DNA Time & Attendance Report application.
   This can be accomplished from the Desktop icon or through the Start Menu.
   The DNA Time & Attendance Report application opens.

   ![DNA Time & Attendance Report Application]

2. Select the desired Report Type from the drop down list.
   There are two types of reports that can be generated:
   - Hours by Last Name - Alphabetizes the cardholders and provides the cardholder’s total hour for each
     day as well as total hours for the report. Allows for selection of specific cardholders.
   - 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 for selection of a specific
     personnel type.
   - Export Data to Excel - Exports the report data to an XLS file. If selected, the Print button will change
     to Export.

3. Depending on the report type selected above, configure the report.
   - 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.
   - Export Data to Excel - The Save As dialog will open. Enter a file name or verify the existing location
     and click Save. The Export Field's dialog appears. Check the desired DNA Fields and click the Ok
     button.

4. From the Identity Field, select the desired field to include in the report.

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.
   The Duration Threshold setting specifies the maximum amount of time that must expire between entry
   and exit transactions in case entries become orphaned.

7. Click the Print or Export button to generate the report.
   If print is selected, the results will open in the Report Viewer.
   If export is selected, the results will be saved to the specified location.
**DNA Import Tool**

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

Open Options recommends that a small file containing just a couple of values is used to test the configuration, before trying to import thousands of entries.

**Running the Import Tool**

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

1. **Double click** the dnaimport.exe icon to open the DNA Import dialog.
   
   The DNA Import dialog opens.

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 selected, the first row will be ignored during the import process.

6. If needed, **edit** the Header Row Delimiter field.
   
   This entry specifies the end of the row character. See the table below.

7. If needed, **edit** the Column Delimiter field.
   
   This entry separates the data items. See the table below.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\r\n</td>
<td>Delimited by a carriage return-line feed combination.</td>
</tr>
<tr>
<td>\r</td>
<td>Delimited by a carriage return.</td>
</tr>
<tr>
<td>\n</td>
<td>Delimited by a line feed.</td>
</tr>
<tr>
<td>;</td>
<td>Delimited by a semicolon.</td>
</tr>
<tr>
<td>:</td>
<td>Delimited by a colon.</td>
</tr>
<tr>
<td>,</td>
<td>Delimited by a comma.</td>
</tr>
<tr>
<td>\t</td>
<td>Delimited by a tab.</td>
</tr>
<tr>
<td>|</td>
<td>Delimited by a vertical bar.</td>
</tr>
</tbody>
</table>

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.

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.

![Create Personnel Group for Imported Personnel](image)

14. If desired, **uncheck** the Check For Duplicates boxes.

15. **Click** the Next button to start the import process. The Importing Records dialog opens.

![Importing Records](image)

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 to have a success import, 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.
Testing Communication from SSP to Computer

The following test can help identify where problems might be occurring.

1. **Stop** the DNA driver (DNADrvr32).
   See page A-7 for information on stopping the DNA driver.

2. **Start** a HyperTerminal Session and **connect** through whatever COM port that the SSP is connected to that needs to be tested.
   Use the following settings:
   - Bits per Second = 38400
   - Data Bits = 8
   - Parity = None
   - Stop Bits = 1
   - Flow Control = None (Set to Flow Control=Hardware if the SSP dip switch number 5 is on).

3. After connecting to the SSP, the “+++ATZ” characters will be returned through the HyperTerminal window within 30 seconds.
   If the “+++ATZ” command is displayed, this indicates communication is getting through to the SSP. Proceed to step 4.
   If the “+++ATZ” isn’t returned, then there is a break in the communication somewhere between the computer and the SSP. In the case of the latter situation, first check cabling; then perform a loopback test on the COM port. After checking cabling, proceed to step 4.

4. **Test** the COM Port for loop back.
   This test confirms that data can be sent to the SSP.
   On the SSP, twist together the wires attached to PINs 1 and 2.

5. With HyperTerminal open and connected to the COM port, **type** A on the keyboard.
   The letter A should appear on the HyperTerminal screen.
   If the A is not displayed, a loop back test will need to be performed on the computer’s COM port.

6. **Test** the computer’s COM port for loopback.
   This can be accomplished in two ways: Use a loop back tester or paper clip jumpers DB9 PINs 2 and 3.

7. With HyperTerminal open and connected to the COM port, **type** A on the keyboard.
   The letter A should appear on the HyperTerminal screen.
   If the A is not displayed, the COM port on the computer is bad.
Locating the DNA Driver Version

The DNA Driver version (dnadrvr32.exe) can be obtained using the following procedure.

1. **Open** the NPower DNA folder.
   Default Location: C:\Program Files\NPowerDNA

2. **Right-click** on the dnaDrvr32 application and **select** Properties.
   The dnaDrvr32 Properties dialog will open.

3. **Select** the Details tab.
   The Driver version is located in the Product Version field.
Unable to Bring SSP Controller Online – Ethernet Configuration

Symptoms:
- Unable to bring SSP online over Ethernet via external Lantronix Micro Serial Server or Micro Serial Server Lite (MSS Lite is only applicable to the SSP-E.)
- SSP indicator in Hardware Browser tree is grayed out.
- SSP Status Dialog displays Offline.
- The message balloon Com Status is Offline.
- Messages in either the Event or Alarm Manager state that an SSP is offline.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| Unable to ping Lantronix IP address from the computer running the SSP driver. | Common resolution when pinging a Lantronix Micro Serial Server fails:  
  a. Verify that power is being supplied to the Lantronix.  
  b. Check to see if the Lantronix has the correct IP Address, Subnet Mask, and Default Gateway. This can be done by opening a telnet session to the Lantronix.  
    i. Click on the Windows Start button / Run.  
    ii. Type telnet and click OK. This will start telnet. Note: telnet.exe is installed with the TCP/IP protocol.  
    iii. After telnet starts, click Connect / Remote System, then enter in the IP address in the Host Name box and click Connect.  
    iv. Type Open in the User Name and press the return key. Then type Show Server at the Local Prompt and press the return key.  
    v. If changes need to be made, see Chapter: Ethernet Connection in the Technical Installation Hardware Manual for instructions on programming the Lantronix.  
  c. Ping the IP address of the application server locally to verify computer’s network configuration is functional.  
  d. Verify that the Default Gateway is configured for the server if there are one or more Routers between the Lantronix and the computer.  
  e. Make sure the Default Gateway is programmed into the Lantronix. Check this by following steps above. Change the default gateway if needed. Example: CHANGE GATEWAY 192.0.1.66 |
| Baud rate configured by the SSP dipswitches may not match the baud rate in the Lantronix Micro Serial Server. | Verify that the baud rate selected by the SSP dipswitches matches what was programmed into the Lantronix. To check this you will need to connect to the Lantronix via telnet (see above). |
| IP address in the Controller Properties does not match the IP address assigned to the Lantronix. | Check to see if the IP address in the Controller Properties is the same as the one assigned to the Lantronix. Verify that the IP addresses match by gaining access into the Lantronix. |
| The 232/485 jumpers are set for 485 communications. | In order to get an SSP online over Ethernet, the SSP 232/485 jumpers must be set for 232. Note: Here are the jumper numbers for the different types of SSP(s):  
  - SSP - J9-J13  
  - SSP/C - J3-J9  
  - SSP/E - J13-J19 |
<p>| SSP is configured to share channels with other SSP(s). | SSP(s) over Ethernet cannot be multi-dropped or share channels with other controllers. |</p>
<table>
<thead>
<tr>
<th><strong>Cause</strong></th>
<th><strong>Resolution</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Control setting for the Lantronix may not match the settings for the SSP.</td>
<td>Verify that the Lantronix flow control is set to RTS\CTS and that SSP dipswitch 5 is turned on. If a Lantronix MSS1 or MSS100 is used, make sure that the correct pins are shorted together at the Lantronix Micro Serial Server. If using a DB-25, short pins 20, 6 and 5 together. If a DB-9 is being used, short pins 4, 6 and 8. See page 8-9 in the Technical Installation Hardware Manual for more information.</td>
</tr>
</tbody>
</table>
Unable to Bring SSP Controller Online – Serial Configuration

Symptoms:
- Unable to bring SSP online.
- SSP indicator in Hardware Browser tree is grayed out.
- SSP Status Dialog displays Offline.
- The message balloon Com Status is Offline.
- Messages in either the Event or Alarm Manager state that an SSP is offline.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No power to the SSP.</td>
<td>Check to see if power is being supplied to the SSP.</td>
</tr>
<tr>
<td>Wrong voltage applied to the SSP.</td>
<td>Verify that the voltage applied to the SSP is 12Vdc or 12Vac and that it is connected correctly at the SSP. The AC/DC and GND positions should be used on the power port. See Chapter 2: Controllers in the Technical Installation Hardware Manual.</td>
</tr>
<tr>
<td>Settings in the Channel Properties configured incorrectly.</td>
<td>Make sure the Channel Type in the Channel Properties is set for the media used, i.e. Serial, Ethernet, Dial-Up (Dial Out), Dial-Up (Accept Incoming), Dial-up (Dial Out and Accept Incoming), SSP.</td>
</tr>
<tr>
<td>Connection properties in the Controller Properties are incorrect.</td>
<td>Check the Channel Setting in the Controller Properties, and make sure the baud rate setting in the Channel window matches the baud rate set in the SSP. This should be set to 38400. Also make sure that the downstream ports baud rate is set to 38400.</td>
</tr>
<tr>
<td>Incorrect value in the Physical Address in the Controller Properties.</td>
<td>Verify that Physical Address in Controller Properties matches the address on the SSP. If there is an incorrect value or a null value in this window, the SSP will not come online. For instructions on how to physically address an SSP, see Chapter 2 in the Technical Installation Hardware Manual.</td>
</tr>
<tr>
<td>The 232/485 jumpers on the right side of the SSP are set incorrectly.</td>
<td>Make sure that jumpers J9-J14 on SSP are set for 232 or 485 depending on which type of communication protocol that is being used. If these are incorrect, it will prevent the SSP from coming online.</td>
</tr>
<tr>
<td>DNA Driver (DnaDrvr32.exe) not running.</td>
<td>Verify that the DNA driver is running. This can be done by right-clicking on the Site in the Hardware Browser tree and selecting Connection / Ping Driver from the menu. If the driver is running a message box will display indicating that it is running. If the driver is not online, then a message box will give the operator the option to reconnect to site driver.</td>
</tr>
<tr>
<td>Wiring from the computer to the SSP is incorrect.</td>
<td>Check wiring from SSP to computer. See hardware manual for correct wiring scheme and alter if needed. Wiring instructions can be found on page 2-7 and 2-8 in the Technical Installation Hardware Manual. Also make sure there is no break in the communication chain from the computer to the SSP.</td>
</tr>
<tr>
<td>SSP not initialized after adding it to the database.</td>
<td>This commonly occurs when you add your first SSP. After adding the first SSP you must then perform a Download All.</td>
</tr>
<tr>
<td>SSP may have hardware faults.</td>
<td>While hardware faults are uncommon, the possibility should not be ignored.</td>
</tr>
</tbody>
</table>
COM Surrogate Errors

If upon opening DNAFusion a COM Surrogate error is received, use the following information to assist in troubleshooting the issue.

1. Run the DNABatchDownloadSettings.exe application.
   Default Location: C:\Program Files\NPowerDNA\Tools\DNABatchDownloadSettings.exe

2. Review the error message that was received.
   - Access Denied - The Windows login does not have rights to the COM Objects. See page 2-11 and 2-13 for more information.
   - Configured Identity is Incorrect - The NPowerDNA COM+ application needs to be configured to run under a Windows Local Administrator Account. See page 2-11 for more information.
   - OleDb Error - Issue connecting to the NPowerDNA database and/or the DNAdrvr32 driver service account does not have permission to connect to the database. See page 2-18 for database connection issues and page 2-11 for information on driver service account.
   - RPC Server Unavailable - Typically received from the client workstation. This error could be a number of issues including a firewall or the client cannot find the server on the network. For more information on firewall configuration see page 2-17.

Starting and Stopping the Services

Driver

To manually start or stop the Driver service:
1. From the Control Panel, select Administrative Tools \ Computer Management \ Services.

2. In the Services dialog, select the file named DNADrv32.

3. Click Start or Stop.

4. If no other services are to be controlled at this time, close the dialog.

   However, if the operator wishes to start SQL Server manually at this time, they may select MSSQLSERVERAGENT in this dialog and click Start.

SQL Server

To manually start the SQL Server service:
1. From the Control Panel, select Administrative Tools \ Computer Management \ Services.

2. In the Services dialog, select the file named SQL Server\Open Options.

   This is the default server name. The actual system may have a different server name if a typical installation was not conducted.

3. Click Start.

4. If no other services are to be started at this time, close the dialog.

   However, if the operator wishes to control the Driver manually at this time, they may select DNADrv32 in this dialog and click Start or Stop.
This Page Intentionally Left Blank
When the Welcome Screen appears, click the **Next** button to continue the installation.

When the License Screen appears, select the **I accept agreement** radiobutton or the **I do not accept** radiobutton to Cancel and click **Next**.

Insert the DNAFusion CD or double-click the **Setup.exe** file.

Will this server be a client workstation?

Select the **Full/Server Client** Installation option and click **Next**.

Is this a Badging station?

Select the **Enabled** Badging checkbox and click **Next**.

Click **Next** to continue the installation.

Click **Ready to Install** to start the installation.

Click **Finish** to complete the set up.

NOTE: The Fusion Server must be configured if a client server relationship will exist.

Select the **User Name/Organization** information and click **Next**.

When the File Location Screen appears, click **Next** to accept the default location or click the **Browse** button.

No

Yes

Enter the **User Name** and **Password** provided for the installation and click **Next**.

Does the DNAfusion Server have internet access?

Obtain the License File executable from Open Options Technical Support. Install the License.

Does the installation already have a NPowerDNA database?

No

Yes

If desired, select the **Create a desktop icon** checkbox and click **Next**.

Select Existing Server and click **Next**.

Select Existing Database and click **Next**.

Select the SQL Server Instance and click **Next**.

Select the SQL Server Instance and click **Next**.

Select the NPowerDNA database and click **Next**.

Select the Install as a Separate Instance option and click **Next**.

Select the Standard Server Installation option and click **Next**.

Select the Full/Server Client Installation option and click **Next**.

Click **Next** to accept the default program group or select another group.
This Page Intentionally Left Blank
DNAFusion Client Installation

1. Insert the DNAFusion CD or double-click the Setup.exe file.

2. When the Welcome Screen appears, click the Next button to continue the installation.

3. When the License Screen appears, select the I accept agreement radiobutton or the I do not accept radiobutton to Cancel and click Next.

4. Accept

5. If desired, change the User Name/Organization information and click Next.

6. When the File Location Screen appears, click Next to accept the default location or click the Browse button.

7. Select the Standard Client Installation option and click Next.

8. Select the Enabled Badging checkbox and click Next.

9. Is this a Badging station?
   - Yes: Click Next to continue the installation.
   - No: Proceed to the next step.

10. Enter the Server’s Name or IP Address and click Next.

11. Click Next to accept the default program group or select another group.

12. If desired, select the Create a desktop icon checkbox and click Next.

13. Click Ready to Install to start the installation.

14. Click Finish to complete the setup.

NOTE: The Fusion Server must be configured if a client server relationship will exist.
Server/Client Setup

Install and configure the Fusion server.

Launch DNAFusion on the Server.

Verify the workstation name and number for the server.

Log on to the Fusion Server workstation.

Create and link the station to a Site.

Install Fusion on the client machines.

Launch DNAFusion on the client machine.

Enter the workstation configuration information for the client.

Log on to the client workstation.

Right click in the Hardware Browser and link the Station to the Site.
Adding Hardware Guide

Add a Site
- RIGHT-CLICK in the Hardware Browser

Add a Channel
- RIGHT-CLICK on the Site

Add an SSP
- RIGHT-CLICK on a Channel

Add a Subcontroller
- RIGHT-CLICK on an SSP

Add a Door
- RIGHT-CLICK on the SSP, Door header or a free Reader

Add an Elevator
- RIGHT-CLICK on the SSP or Elevator header

Add a DVR
- RIGHT-CLICK on the DVR Servers

Add an IP Camera
- RIGHT-CLICK on the Site
Adding a Controller and Bringing it On-line

1. Open Fusion
2. Open the Hardware Browser.
3. RIGHT-CLICK in the Hardware browser. Select Add Site from the context menu.
4. Configure the Site. Enter a Name and click the Location button to populate the field with the name of the station where the driver resides. Click OK.
5. RIGHT-CLICK on the Site object and select Add Channel from the context menu.
6. Configure the Channel. Enter a meaningful description. Select the Channel Type. Configure the channel based upon the type selected. (See page 3-6 for channel information).
7. RIGHT-CLICK on the channel object in the Hardware browser. Select Add SSP... from the context menu.
8. Configure the Controller. RIGHT-CLICK on the controller object in the Hardware browser. Select Status from the context menu. In the SSP Status dialog, select the Reload button. Wait a few moments while the application downloads the firmware. Click OK.
9. Ensure that the Physical Address is correct. Type in a meaningful description. Select the correct Controller Type. Set the GMT Offset. Check the Use Daylight Savings Time checkbox if the location utilizes daylight saving time. If IP channel, enter the IP address. Select the Stored Quantities object in the Controller tree. If desired, select the desired Controller Flag checkboxes and adjust the Quantities. Click OK.
10. If the controller text appears green, the controller is online. If the controller text is grayed out, the controller is offline.

If desired, select the desired Controller Flag checkboxes and adjust the Quantities. Click OK.
Bringing a Door On-line

Open the Hardware Browser.

Is there an existing SSP and subcontroller?

NO

An SSP and a subcontroller must be added to the system prior to the addition of a door.

YES

RIGHT-CLICK on the SSP, Door header or a free reader under a subcontroller.

Select Add Door from the context menu.

Configure the Common Properties dialog.

Select the Door Type from the drop down. Specify the Reader, Contact, Request to Exit and Strike options to configure the door settings. If desired, set the Strike and Held Time for the ADA Settings.

Configure the Door Objects dialog

If desired, configure the Advanced dialog.

If desired, configure the Macros dialog.

If desired, configure the Follows Schedule dialog.

CLICK OK.

Click Yes to download the hardware information.
**Configuring Card Formats**

**STEP #1:**
CREATE A CARD FORMAT

RIGHT-CLICK on the SSP and select **Card Formats** from the context menu.

The Card Formats dialog will display.

Are you creating a new card format or editing an existing card format?

New Card Format

Select the **New** button to create a new card format without overwriting an existing format.

Enter a name in the Description field.

If needed, enter or edit the desired values in the card format fields.

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

Existing Card Format

Select the correct format from the Description drop down list and click the **Copy** button to copy the format.

**STEP #2:**
ASSIGN CARD FORMAT TO THE CONTROLLER

In the Hardware browser, right-click the SSP and select **Properties** from the context menu.

Select the **Card and Dual Comm** link from the dialog tree.

In the resulting dialog, select up to 8 card formats in the drop-down menus.

**CLICK OK.**
## Command Line Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>/FORCENEW</td>
<td>Forces system to ignore existing settings and act like a new install.</td>
<td></td>
</tr>
<tr>
<td>/FORCENDBU</td>
<td>Forces the DNAUpdates.SQL to run on an upgrade.</td>
<td></td>
</tr>
<tr>
<td>/NOHASP</td>
<td>Does not try to install the HASP drivers.</td>
<td></td>
</tr>
<tr>
<td>/NOBONJOUR</td>
<td>Does not try to install the Bonjour service.</td>
<td></td>
</tr>
<tr>
<td>/NONATIVE</td>
<td>Do not try to install the SQL Native Client. If this is present it uses old style SQL Server drivers.</td>
<td></td>
</tr>
<tr>
<td>/INSTTYPE=xxxx</td>
<td>Full = Full Client, Client = Standard Client</td>
<td></td>
</tr>
<tr>
<td>/SILENT</td>
<td>Shows the install progress dialog, but there is no interaction with the user except for the cancel button (unless you use /NOCANCEL).</td>
<td></td>
</tr>
<tr>
<td>/VERYSILENT</td>
<td>No visual indicators and no interaction with user.</td>
<td></td>
</tr>
<tr>
<td>/NOCANCEL</td>
<td>If using /SILENT this disables the Cancel button so user cannot stop the install.</td>
<td></td>
</tr>
<tr>
<td>/PASSWORD=xxxxxx</td>
<td>If the install is password protected this allows you to specify the password for automated installs.</td>
<td></td>
</tr>
</tbody>
</table>

Only Used for Client Based Installs

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>/SERVER=xxxx</td>
<td>Sets the name of the DNA Server.</td>
<td></td>
</tr>
<tr>
<td>/SHARE=xxxx</td>
<td>Sets the name of the share on the DNA Server.</td>
<td>DNAShare</td>
</tr>
</tbody>
</table>

Only Used for Server Based Installs

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>/SQLINST=xxxxxx</td>
<td>Sets the SQL Instance name to xxxx, i.e. server-name\instancename or servername - On.</td>
<td>LocalMachineName\OpenOptions</td>
</tr>
<tr>
<td>/SQLDB=xxxxxx</td>
<td>Sets the database name to xxxx.</td>
<td>NPowerDNA</td>
</tr>
<tr>
<td>/SQLMODE=x</td>
<td>0=New Instance, 1=Existing Server, 2=Existing DB</td>
<td>New Instance (0)</td>
</tr>
<tr>
<td>/SQLUSER=xxxxxx</td>
<td>If using SQL Authentication, this is the username.</td>
<td>Use Windows Authentication</td>
</tr>
<tr>
<td>/SQLPWD=xxxxxx</td>
<td>If using SQL Authentication, this is the password.</td>
<td>Use Windows Authentication</td>
</tr>
<tr>
<td>/PUSH</td>
<td>Enable Push Updates</td>
<td>Not Enabled</td>
</tr>
</tbody>
</table>

### 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=NPowerDNA2 /SQLMODE=1
```
This Page Intentionally Left Blank
Index

**A**
- Access Levels Per Card 3-11
- Activation Date 3-11
- AD 300 3-14
- ADA Settings 3-24
- Alternate Priority 3-22, 3-31, 3-40, 3-44
- Anti-Pass Back Settings 3-25, 3-35
- APB Location 3-11
- Auto Activate 3-21, 3-31
- Auto Deactivate 3-21, 3-31
- AutoExpire Tool 5-1, 5-11
  - Configuration Mode 5-11
  - Silent Mode 5-11

**B**
- Batch Processing 3-13

**C**
- Cameras (IP Based)
  - Adding 3-48
- Card Formats 3-13, 3-49
  - Assigning 3-50
  - Copying 3-49
  - Creating 3-49
  - Editing 3-49
- Channel
  - Adding 3-5
    - Modem Channel 3-6
    - Serial Channel 3-6
    - TCP/IP Channel 3-6
- Client 2-1
- Client Installation 2-15
  - Standard Client Installation 2-15
- Client Specifications
  - DNA Client Workstation 2-5
  - DNA Client Workstation with Photo ID 2-5
- COM+ Object 2-11
- Component Services 2-11
- Component Services Default Permissions 2-13
- Component Services Permissions 2-13
- Computer Specifications
  - Client Specifications 2-5
  - Server Specifications 2-3
- Configuring Hardware 3-1
- Controller
  - Adding 3-7
Index

GMT Offset 3-7
Holiday Set 3-9
Physical Address 3-7, 3-9
Properties
  Cards & Dual Comm 3-13
  Controller Properties 3-9
  Stored Quantities 3-11
  Time Schedule Set 3-9
  Use Daylight Savings 3-7, 3-10
Controller Flags 3-11
Controller Memory 3-11
Create Firewall Exclusions 2-9, 2-16

D

Database Permissions 2-14
Database Server Configuration 2-8
  Existing Database 2-8
  Existing Server 2-8
Daylight Savings 3-7, 3-10
Deactivation Date 3-11
Digital Video Recorder
  Add Cameras 3-47
  Adding 3-45
  Authentication Mode 3-46
  Configure 3-46
  Integration 3-45
DNA Batch Download Settings Utility 5-1, 5-4
DNA Driver 2-11
DNA Event History Report Utility 5-13
  Email Setup 5-13
  Parameters 5-14
  Scheduling 5-15
DNA Import Tool 5-1, 5-23
  Permissions 5-24
  Running 5-23
DNA LED Control Application 5-1, 5-4
DNA Time and Attendance Report 5-17
  Generating 5-21
  Installation 5-17
  Setting up 5-18
DNA Users Group 2-12
Domain User Group Setup 2-6
Door
  Adding 3-17
    From a Reader 3-19
    In & Out 3-18
    Single Door 3-17
  Properties
    Advanced 3-25
    Common Properties 3-21
    Door Objects 3-23
    Follows Schedule 3-28
    Macros 3-27
Doors
  ADA Settings 3-24
  Alternate Priority 3-22
  Anti-Pass Back (APB) Settings 3-25
  Follows Schedule 3-28
Index

In & Out  3-18
Situation Level Manager  3-21
Duress Digit  3-12
Duress PIN Mode  3-12

E

Elevator
  Adding  3-29
  Properties  3-31
    Common Properties  3-31
    Elevator Objects  3-33
Elevator Control  3-12
Elevators
  Alternate Priority  3-31
  Anti-Pass Back (APB) Settings  3-35
  Feedback  3-29
  Floor Groups  3-33
  Follows Schedule  3-36
  Non-Feedback  3-29
Event History Report Utility  5-1
Existing Database  2-8
Existing Server  2-8

F

Facility Code  3-49, 3-50
Firewall Configuration  2-17
Follows Schedule  3-36
Full Server / Client Installation  2-7

G

GMT Offset  3-7, 3-9
GTWY  3-14

H

Hardware
  Adding Hardware  3-3
    Site  3-3
Hardware Browser  3-1
  Configuring  3-1
  Opening  3-1
HASP Key  2-8, 4-5
Held Time  3-23
Holiday Set  3-9

I

Input Point
  Properties
    Common Properties  3-39
    Input Properties  3-41
Input Points
  Alternate Priority  3-40
  Circuit Type  3-41
  Configuring  3-39
  Sensitivity  3-41
Index

Installation
  64-bit OS 2-19
  Client 2-15
  Server 2-7
Installation Types 2-1
  Client 2-1
  Server 2-1
Instance Name 4-3
Issue Codes 3-11

J

K
Keypad Mode 3-38

L
LED Configuration 3-38
LED Control Application 5-4
License File 2-8, 4-5
License Updates 4-5
Licensing 2-8
Local Domain Setup 2-6

M
Match Physical 3-15
Migrating 2-24
Migrating DNA Fusion 2-24
  Same Workstation 2-24
  Separate Workstations 2-25
Muster 3-21, 3-31

N
Network Requirements 2-6
Network Video Recorder (NVR). See Digital Video Recorder
New Server 2-24
NSC-100 3-14

O
ODBC Data Sources 2-18
Output Point
  Properties
    Common Properties 3-43
    Output Properties 3-44
Output Points
  Alternate Priority 3-44
  Default Mode 3-44
  Momentary Time 3-44

P
Physical Address 3-9, 3-15
PIM400-485 3-14
Index

Q

R
Reader
  Properties
    Common Properties  3-37
    Reader Properties  3-38
Readers
  Configuring  3-37
Remote Archive Utility  5-1, 5-7
  Configuring  5-8
  Executing  5-9
  Scheduling  5-9
Reverse Polling on Inputs  3-16

S
Server  2-1
Server/Client Requirements  2-6
  Network Requirements  2-6
  User Group Setup  2-6
Server Configuration  2-11
  Administrative Rights Account Assignment  2-11
    Component Services  2-11
    DNA Driver  2-11
  Component Services  2-11
  Component Services Default Permissions  2-13
  Database Permissions  2-14
  DNA Driver  2-11
  DNA Users Group  2-12
  Windows 2003 Server  2-21
  Windows 2008 Server  2-22
Server Installation  2-7
  64-bit OS  2-19
  Existing Database  2-8
  Existing Server  2-8
  Full Server/Client Installation  2-7
  Standard Server Installation  2-7
Server Specifications
  DNA Enterprise Server with SQL Server Database  2-4
  DNA Server (Stand-Alone) with SQL Express Database  2-3
  DNA Server with SQL Express Database 1 to 4 clients  2-3
Service Pack  4-3
Site
  Creating  3-3
  Linking  3-4
SMTP Mailer  5-1, 5-5
  Configuration  5-5
  Executing  5-6
Soft Key  2-8, 4-5
Software Upgrades
  Client  4-4
  NPowerDNA  4-1
  Service Pack  4-3
SQL Server Express  2-3, 2-4, 2-19
SSP.  See Controller
Standard Server Installation  2-7
Index

Store Temporary Upgrade Date  3-11
Store Vacation Date  3-11
Strike Activation  3-24
Subcontroller Firmware  3-16
  Updating  3-16
Subcontrollers
  Adding  3-14
  Physical Address  3-15
Properties
  Advanced  3-16

T

Table Purger Tool  5-1, 5-3
  Run  5-3
Temporary Upgrade Date  3-11
Time and Attendance In  3-21
Time and Attendance Out  3-21
Time & Attendance Report  5-1
  Generating  5-21
  Installing  5-17
  Setting up  5-18
Timed Anti-Pass Back  3-11
Time Schedule Set  3-9
Toolbars
  Hardware  3-2
Trigger Code  3-11

U

Upgrades  4-1, 4-4
User Group Setup  2-6
  Domain User Group Setup  2-6
  Local Domain Setup  2-6

V

Vacation Date  3-11

W

Windows 2003 Server  2-21
Windows 2008 Server  2-22

X

Y

Z