OPEN OPTIONS®
ACCESS TECHNOLOGY

dnaFusion™

DNA Fusion User Manual

dnaFusion™

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

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

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

Publish Date: August 25, 2020
Manual Number: - UM 7.7

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™
ACCESS TECHNOLOGY

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

Open Options Software License Agreement

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

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

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

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

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

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

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

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

Table of Contents

Chapter 1: Introduction

Chapter 2: Getting Started

Chapter 3: DNA Properties

Chapter 4: Operators

Chapter 5: Time & Holiday Schedules

Chapter 6: Access Levels

Chapter 7: Personnel

Chapter 8: Hardware Features

Chapter 9: Situation Manager

Chapter 10: Triggers & Macros

Chapter 11: Access Areas & Anti-Pass Back

Chapter 12: Secured Areas

Chapter 13: Tenants

Chapter 14: Events & Alarms

Chapter 15: Watch Window

Chapter 16: HTML Viewer

Chapter 17: Reports

Chapter 18: Graphic Maps

Chapter 19: Scheduling

Chapter 20: System Settings & Maintenance

Chapter 21: ID Badging

Appendix A: Menu Structures

Appendix B: Process Diagrams

Appendix C: Shortcut Keys

Appendix D: Replacement Text

Appendix E: Glossary

This Page Intentionally Left Blank

Introduction 1

In This Chapter

- √ Manual Overview
- √ Introduction to DNA Fusion
- √ System Specifications
- √ Open Options Resources

This manual is designed to introduce the DNA Fusion software and explain how to configure and set up the access control system.

How This Manual is Organized

This manual contains seven parts:

Part One: Introduction & Overview

Chapter 1, "Introduction," provides an overview of the manual and system requirements.

Chapter 2, "Getting Started," provides an overview of the DNA Fusion software.

Part Two: DNA Configuration

Chapter 3, "DNA Properties," covers setup information for the DNA Fusion software.

Chapter 4, "Operators," provides instructions for adding & configuring operators in the system.

Chapter 5, "Time & Holiday Schedules," provides instructions for adding time and holiday schedules.

Chapter 6, "Access Levels," explains how to configure and assign access levels.

Chapter 7, "Personnel," provides instructions for adding, editing, managing, and deleting cardholders.

Chapter 8, "Hardware Features," covers the configure and control of hardware within the DNA Fusion software.

Part Three: System Management

Chapter 9, "Situation Manager," covers how to enable and configure situation levels.

Chapter 10, "Triggers & Macros," explains the process of creating triggers and macros.

Chapter 11, "Access Areas & Anti-Pass Back," provides basic setup instructions for access areas and anti-pass back options.

Chapter 12, "Secured Areas," covers setting up secured areas.

Chapter 13, "Tenants," covers configuring the tenants feature.

Part Four: System Monitoring

Chapter 14, "Events & Alarms," explains how to view and manage system events and alarms.

Chapter 15, "Watch Windows," provides an overview of watch windows and their function.

Chapter 16, "HTML Viewer," covers setting up custom HTML pages.

Chapter 17, "Reports," lists the various reports available in DNA and instructions for creating custom reports.

Chapter 18, "Graphic Maps," provides information on creating and monitoring graphic maps.

Part Five: Data Management

Chapter 19, “Scheduling,” explains how to schedule automated tasks.

Chapter 20, “System Settings and Maintenance,” provides instructions for archiving information and performing a system backup.

Part Six: Badging

Chapter 21, “ID Badging,” covers designing badging templates and badge management.

Part Seven: Appendixes

Appendix A - Menu Structure

Appendix B - Process Diagrams

Appendix C - Shortcut Keys

Appendix D - Replacement Text

Appendix E - Glossary

Icons and Conventions Used in This Manual

The following icons call attention to useful or important information:

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

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

- Special: Indicates a menu item, toolbar selection, button, or dialog in the system.
- **Boldface**: Indicates an instruction or user action; bold text usually appears in numbered steps.

Introduction to DNA Fusion

DNA Fusion™ is built from the latest software development technology by Microsoft®. It is designed with Distributed Network Architecture, which offers a scalable, efficient, and reliable solution for both small and large-scale enterprises. DNA Fusion continues to revolutionize the access control industry by reducing many of the limitations inherent in the deployment of enterprise-based access control applications.

DNA Fusion is also designed with 100% InfoReady™ architecture. With this model, information is always readily accessible, eliminating the need to run a report (or multiple reports) to retrieve the necessary data.

What is DNA Fusion?

- DNA Fusion is a Windows 32/64-bit application built on Microsoft's Distributed Network Architecture platform to deliver enterprise-wide access control solutions.
- DNA Fusion provides TCP/IP network communication between clients and SSP controllers; server and client applications are intranet- and Internet-enabled.
- DNA Fusion offers an advanced graphical user interface (GUI) using standard Windows conventions. Customization features, such as dockable toolbars and adjustable windows, allow users to configure the software environment and tailor the workstation to their individual needs.
- DNA Fusion works in conjunction with a common access control processor and delivers seamless integration to a variety of DVR/NVR systems and third-party devices.

DNA Advantages

- Multi-Document Interface - DNA Fusion allows the operator to open and adjust multiple data windows, browsers, and toolbars simultaneously.
- Drag & Drop Functionality - The multi-document interface enables drag-and-drop functionality to simplify and improve operability.
- Personnel Groups - Create logical personnel groups to easily assign default access levels.
- Dynamic Event Filters - Filter events by specific criteria and quickly toggle back to all events.
- Advanced Alarm Handling - DNA streamlines the alarm management process by providing a counter on multiple alarms from the same point. Operators can acknowledge and clear alarms multiple alarms with a single keystroke.

System Configuration Overview

DNA Fusion is developed using Windows standards and tools. It utilizes Distributed Component Object Model (DCOM) to support communication between software objects on networked computers, as well as TCP/IP to support communication between the driver and the host. The nature of an access control software platform demands that a certain amount of network security is inherent in the application and, as a result, specific network requirements must be met to successfully deploy DNA Fusion on the customer's network.

DCOM

DNA Fusion uses a Microsoft-based architecture known as DCOM to serve as the primary communication infrastructure for the client-server environment. The DCOM model improves network bandwidth usage, enables communication across multiple network protocols, and provides a Windows NT extensible security framework.

Event data collected by the field controllers are stored in the database via the DNA Fusion COM objects. The data is also transmitted to each subscribed client, allowing the client to display real-time event data. Clients can view the configuration data and send changes to the driver to be transmitted to the appropriate field hardware (assuming that the requesting DNA operator possesses the necessary privileges).

TCP/IP

TCP/IP is a network protocol that supports communication between the driver and the host. TCP/IP uses the client/server model of communication. It is the most common method of communication with controllers.

Services

After DNA Fusion has been installed, certain utility programs, known as services, are necessary for the application to operate successfully. Typically, these services are only installed on the server workstation. However, it is possible for each service to reside on a separate server.

DNA Fusion typically uses three services:

- DNA Driver — The driver service is run by the DNADrvr32.exe application. It runs as a Windows service and is the communications hub for the DNA Fusion software. The driver communicates with field controllers to collect event data and transmit configuration data regarding system personnel and hardware.
- DNA Service Agent — The service agent starts when a client opens. If the driver service is not running, the DNA Service Agent will automatically start the driver service.
- SQL Server — The SQL Server service communicates to the DNA Fusion database. There is one SQL Server service for each instance of SQL Server running on the computer.

Requirements & Specifications

The following requirements and specifications 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.

Installation Types

This chapter covers two types of installation:

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

Each installation has its own requirements, specifications, and tasks.

Network Requirements

DNA Fusion has certain network requirements that must be met for successful deployment in the client/server environment. Any of the following network scenarios are acceptable:

- 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. (Recommended)
- DNA computers can be members on different Windows domains, but bi-directional trust MUST be established for each domain.
- 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. This configuration is less secure than a domain.
    - □ 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 must be managed at the SQL Server level.

Server Specifications

In this instance, the server refers to the PC that will host the DNA Fusion database.

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

Parameter	Recommended Specification
Processor Speed	Intel Core i5 2.8 GHz + (or equivalent, multicore)
System Memory (RAM)	4 GB
Network Card	10/100 Ethernet
Hard Drive Size	250 GB
Graphics Card	VGA Support for 1024 x 768 resolution or higher
Video Memory (VRAM)	256 MB
Backup Device	YES
CD-RW Drive	YES
Operating System	Windows 2012 Server R2, Windows Server 2016, Windows 10 (32 and 64 bit support), Windows Server 2019
Optional	UPS (Uninterrupted Power Supply)
• This specification is ideal for systems with less than 20 doors, 200 cardholders, or 1,000 transactions per day. • DNA ships with a Microsoft Server SQL Server Express 2012 has a database size limit of 10 GB.	

Enterprise Server PC /SQL Server Database (> 20 doors / > 5 clients)

Parameter	Recommended Specification
Processor Speed	Intel Core i5 2.8 GHz + (or equivalent, multi-core)
Dual Processor	YES
System Memory (RAM)	8 GB
Network Card	10/100 Ethernet
Hard Drive Size	500 GB
Graphics Card	VGA Support for 1024 x 768 resolution or higher
Video Memory (VRAM)	512 MB
Backup Device	YES
CD-RW Drive	YES
Operating System	Windows 2012 R2 Server, Windows Server 2016, Windows Server 2019
Database	Microsoft SQL Server 2012 through 2016 (recommended Microsoft SQL Server 2012 R2 or higher)
Optional	Separate Database & Application Servers* UPS (Uninterrupted Power Supply) Isolated Database Server/Application Server Multi-Processor

- This specification is designed for high-traffic (transaction) systems and systems that require multiple client database connections.
- Microsoft SQL Server must be installed on the PC prior to installing DNA Fusion.

* Microsoft SQL Server may be installed on another (dedicated) computer prior to the DNA Fusion installation and identified during the DNA Fusion installation.

! *DNA Fusion is not supported on* Home *or* Mobile *versions of Windows OS or Windows 10 S.*

ⓘ *RAID hardware configuration and backup medium recommended for Enterprise servers.*

Client Specifications

A client workstation is defined as a PC that is connected to the DNA system via LAN/WAN but retrieves and saves data to and from the DNA server.

Client Workstation w/Photo ID

Parameter	Recommended Specification
Processor Speed	Intel Core i3 2.4 GHz + (or equivalent)
System Memory (RAM)	4 GB
Network Card	10/100 Ethernet
Hard Drive Size	250 GB
Graphics Card	VGA Support for 1024x768 resolution or higher/512 MB VRAM
Video Memory (VRAM)	512 MB
Video Capture Device	YES (TWAIN Compliant)
USB Port	YES (if using USB capture device)
Backup Device	NO
CD-ROM Drive	YES
Operating System	Windows 10 (32-bit and 64-bit support)
Monitor	17-inch color (capable of 1024 x 768)
Optional	UPS (Uninterrupted Power Supply)

- If the Photo ID Client will be installed on a laptop, ensure that the unit is equipped with at least one printer port and one serial port.
- Additional USB and/or COM ports may be required when using badge printers featuring smart chip technology. See printer documentation for more information.
- TWAIN devices must be compliant with DirectX 9.

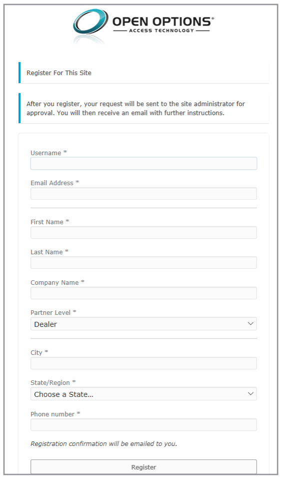
NOTES:

Open Options Resources

The Open Options website is www.ooaccess.com. The site contains resources that are not available to the general public, but offered to customers and partners with a registered web account. To access the partner portal, click Login and sign in with a valid Username and Password.

To create and register a new account, use one of the following methods:

- **Click** Login / View Your Account and **enter** the required information on the My Account page.
- **Click** the Login button, **select** Register, and **enter** the required information in the registration form.



OPEN OPTIONS ACCESS TECHNOLOGY

Register For This Site

After you register, your request will be sent to the site administrator for approval. You will then receive an email with further instructions.

Username *

Email Address *

First Name *

Last Name *

Company Name *

Partner Level *
Dealer

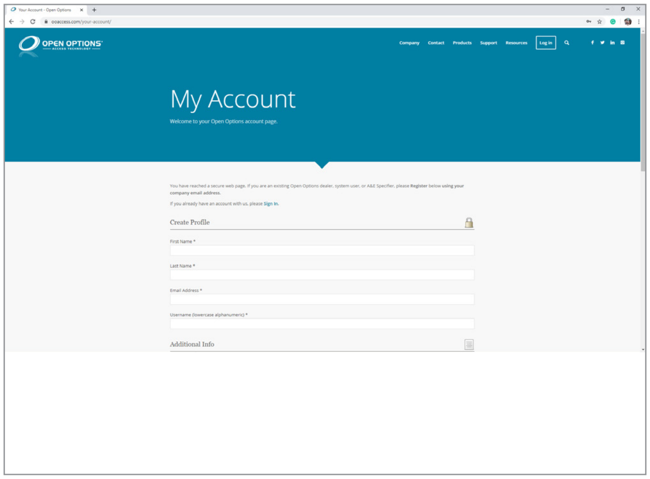
City *

State/Region *
Choose a State...

Phone number *

Registration confirmation will be emailed to you.

Register



Your Account - Open Options

ooaccess.com/your-account/

OPEN OPTIONS ACCESS TECHNOLOGY

Company Contact Products Support Resources Log in

My Account

Welcome to your Open Options account page.

You have reached a secure web page. If you are an existing Open Options dealer, system user, or A&E Specifier, please **Register** below **using your company email address.**

If you already have an account with us, please **Sign In.**

Create Profile

First Name *

Last Name *

Email Address *

Username (lowercase alphanumeric) *

Additional Info

> *A temporary password will be sent to the registered e-mail address after the webmaster approves the account. Use an e-mail address associated with an employee or dealer.*

Training Videos

The Training Videos page provides links to video tutorials that demonstrate how to perform various operations in the DNA Fusion software. The following videos are available:

- How to Add a Cardholder in DNA Fusion
- Working with Personnel Groups
- Simple Reporting with InfoReady™
- Global Access Levels
- Legacy Access Levels and Groups
- Removing Access Levels in DNA Fusion
- How to Deactivate Cards
- How to Use Auto-Expiring Access Levels

Knowledge Base

The Knowledge Base provides links to support-related articles and technical bulletins. It is designed to answer frequently-asked questions about Open Options' software and hardware products as well as resolve common troubleshooting issues.

Support Forum

The Support Forum allows registered web users to search for answers to specific technical issues or post their own topic to obtain timely feedback from Open Options technical support professionals.

Downloads

The Download Center allows registered web users to download the latest versions of software, manuals, and supplementary tools.

This Page Intentionally Left Blank

Getting Started 2

In This Chapter

Starting DNA Fusion

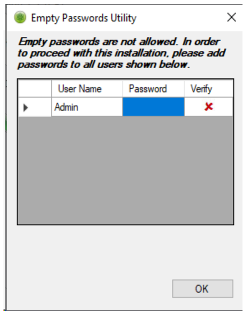
1. After installing DNA Fusion, **double-click** on the dnaFusion desktop icon.

   OR

   Locate the application in the following default location:

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

   The Empty Password Utility dialog opens.



Empty Passwords Utility

Empty passwords are not allowed. In order to proceed with this installation, please add passwords to all users shown below.

	User Name	Password	Verify
▸	Admin		✗

2. Add passwords for the Admin and, or all operators in DNA Fusion.

   The Login screen appears.

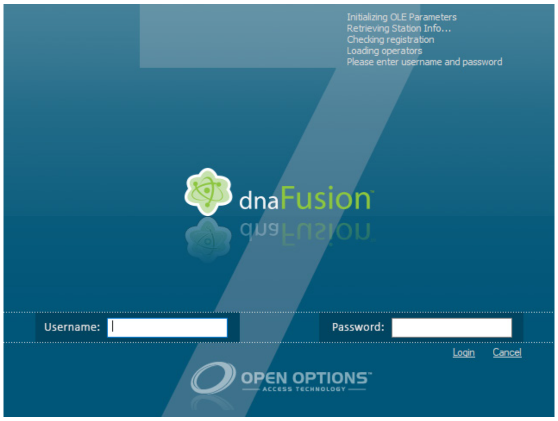
Logging In

When the DNA Fusion application starts, the Login screen will appear.

DNA uses operator credentials for several purposes:

- The Username and Password tell DNA which desktop configuration to use.
- DNA matches the operator against an Operator Profile.
  - □ The operator can assign Operator Privileges to certain users depending on their Operator Profile.

1. From the Login screen, **enter** the Username and Password.



Initializing OLE Parameters
Retrieving Station Info...
Checking registration
Loading operators
Please enter username and password

The default operator is Admin *without a password.*

2. **Click** the Login button.

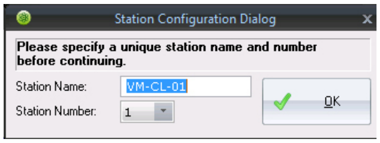
Initial Workstation Login

The first time an operator launches DNA Fusion, they will be prompted to configure the workstation.

1. **Open** DNA Fusion.

   The Station Configuration Dialog appears.

   The Station Name auto-populates with the Windows Computer Name. This information appears in the DNA Properties dialog as well as the Status Bar.

   Station Configuration Dialog

   Please specify a unique station name and number before continuing.

   Station Name: VM-CL-01

   Station Number: 1

2. **Select** a unique Station Number from the drop-down list and **click** OK.

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

   The Login screen appears.

3. **Continue** to log in as described on page 2-1.

Changing Operators

DNA Fusion tracks each operator's actions, so it is important to log out each time an operator has completed a session.

To change operators:

1. **Select** File / Log Out from the Main Menu.

   OR

   Double-click on the Operator field in the Status Bar. See page 2-7 for more information.

2. **Enter** the new Username and Password and **click** Login.

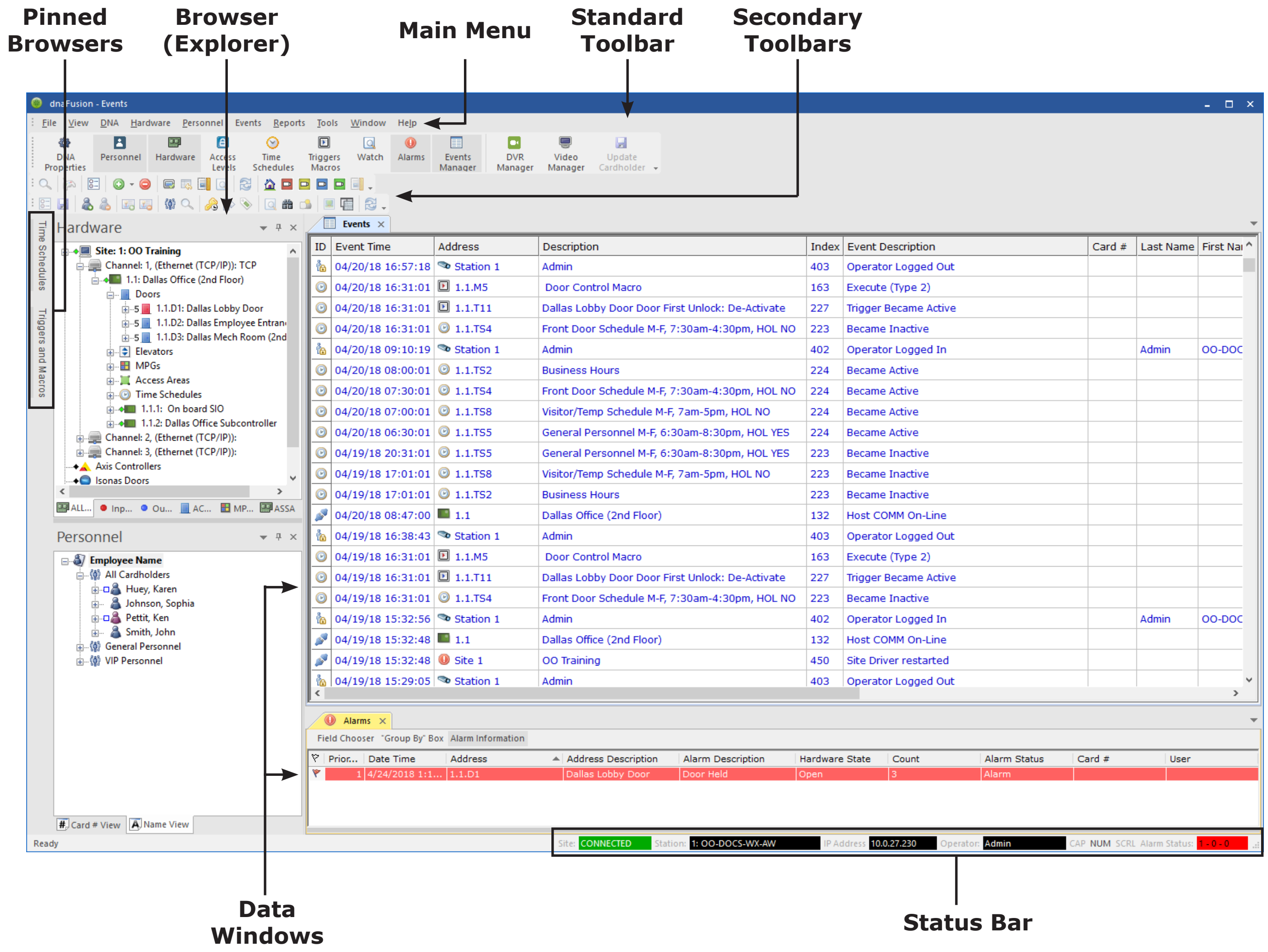
DNA Fusion Environment

The DNA Fusion software is designed with a simple, user-friendly interface that provides a considerable amount of navigation and flexibility to the operator.

While it is possible to perform the same action using multiple pathways, the user never leaves the main screen. Consequently, the operator is only required to learn a few operations, most of which are fairly intuitive and follow standard Windows conventions.

The main screen consists of seven (7) principal elements:

- Main Menu
- Standard Toolbar
- Secondary Toolbars
- Browsers (Explorers)
- Pinned Browsers
- Data Windows
- Status Bar



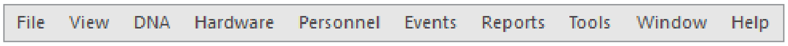
ID	Event Time	Address	Description	Index	Event Description	Card #	Last Name	First Na
	04/20/18 16:57:18	Station 1	Admin	403	Operator Logged Out			
	04/20/18 16:31:01	1.1.M5	Door Control Macro	163	Execute (Type 2)			
	04/20/18 16:31:01	1.1.T11	Dallas Lobby Door Door First Unlock: De-Activate	227	Trigger Became Active			
	04/20/18 16:31:01	1.1.TS4	Front Door Schedule M-F, 7:30am-4:30pm, HOL NO	223	Became Inactive			
	04/20/18 09:10:19	Station 1	Admin	402	Operator Logged In		Admin	OO-DOC
	04/20/18 08:00:01	1.1.TS2	Business Hours	224	Became Active			
	04/20/18 07:30:01	1.1.TS4	Front Door Schedule M-F, 7:30am-4:30pm, HOL NO	224	Became Active			
	04/20/18 07:00:01	1.1.TS8	Visitor/Temp Schedule M-F, 7am-5pm, HOL NO	224	Became Active			
	04/20/18 06:30:01	1.1.TS5	General Personnel M-F, 6:30am-8:30pm, HOL YES	224	Became Active			
	04/19/18 20:31:01	1.1.TS5	General Personnel M-F, 6:30am-8:30pm, HOL YES	223	Became Inactive			
	04/19/18 17:01:01	1.1.TS8	Visitor/Temp Schedule M-F, 7am-5pm, HOL NO	223	Became Inactive			
	04/19/18 17:01:01	1.1.TS2	Business Hours	223	Became Inactive			
	04/20/18 08:47:00	1.1	Dallas Office (2nd Floor)	132	Host COMM On-Line			
	04/19/18 16:38:43	Station 1	Admin	403	Operator Logged Out			
	04/19/18 16:31:01	1.1.M5	Door Control Macro	163	Execute (Type 2)			
	04/19/18 16:31:01	1.1.T11	Dallas Lobby Door Door First Unlock: De-Activate	227	Trigger Became Active			
	04/19/18 16:31:01	1.1.TS4	Front Door Schedule M-F, 7:30am-4:30pm, HOL NO	223	Became Inactive			
	04/19/18 15:32:56	Station 1	Admin	402	Operator Logged In		Admin	OO-DOC
	04/19/18 15:32:48	1.1	Dallas Office (2nd Floor)	132	Host COMM On-Line			
	04/19/18 15:32:48	Site 1	OO Training	450	Site Driver restarted			
	04/19/18 15:29:05	Station 1	Admin	403	Operator Logged Out			

Prior...	Date Time	Address	Address Description	Alarm Description	Hardware State	Count	Alarm Status	Card #	User
1	4/24/2018 1:1...	1.1.D1	Dallas Lobby Door	Door Held	Open	3	Alarm		

Site: CONNECTED Station: 1: OO-DOCS-WX-AW IP Address 10.0.27.230 Operator: Admin CAP NUM SCRL Alarm Status: 1 - 0 - 0

Main Menu

The Main Menu is an initial launch point for navigating to a task. Each menu item contains a drop-down list of related options.



Items that are inapplicable to the current configuration or selection are known as "ghost items" and will appear gray in the context menu.

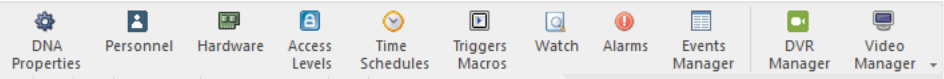
If an arrow appears next to the menu option, hover the mouse to expand its contents and view a sub-menu of related items.

Toolbars

Toolbars provide a convenient way to open browsers or perform tasks that normally require the operator to navigate the Main Menu. DNA Fusion consists of a primary toolbar, known as the Standard Toolbar, and various secondary toolbars associated with the application's browsers and data windows.

Standard Toolbar

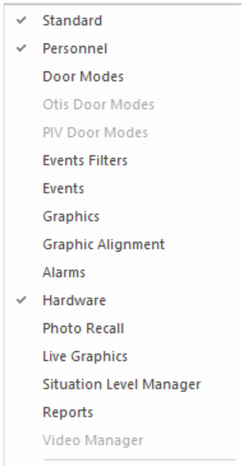
The Standard Toolbar is a series of buttons located at the top of the main screen just below the Main Menu. It provides quick access to some of the program's most-used features.



The Alarms and Events Manager buttons populate data windows in the main screen, while the remaining buttons open browsers that allow the operator to perform tasks related to specific information.

DNA Properties	DNA Properties Icon	Opens the Host Settings dialog.
Personnel	Personnel Icon	Toggles the Personnel Browser.
Hardware	Hardware Icon	Toggles the Hardware Browser.
Access Levels	Access Levels Icon	Toggles the Access Levels Browser.
Time Schedules	Time Schedules Icon	Toggles the Time Schedules Browser.
Triggers Macros	Triggers & Macros Icon	Toggles the Trigger & Macros Browser.
Watch	Watch Icon	Toggles the Watch Window.
Alarms	Alarms Icon	Opens the Alarm Grid in a data window.
Events Manager	Events Manager Icon	Opens the Events Grid in a data window.
DVR Manager	DVR Manager Icon	Toggles the DVR Browser.
Video Manager	Video Manager Icon	Toggles the Video View Manager window.

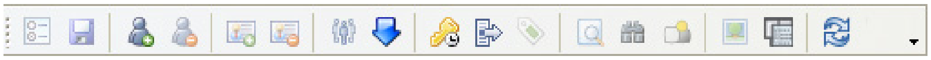
Secondary Toolbars



Secondary Toolbars are launch points to perform specific tasks. Each secondary toolbar will be discussed in a later section.

1. To display the list of toolbars, **right-click** in the Main Menu / Standard Toolbar area.
2. To display a given toolbar, **select** the desired toolbar option.

   Active buttons have colored icons; inactive buttons that are not applicable to the current configuration will appear grayed out.

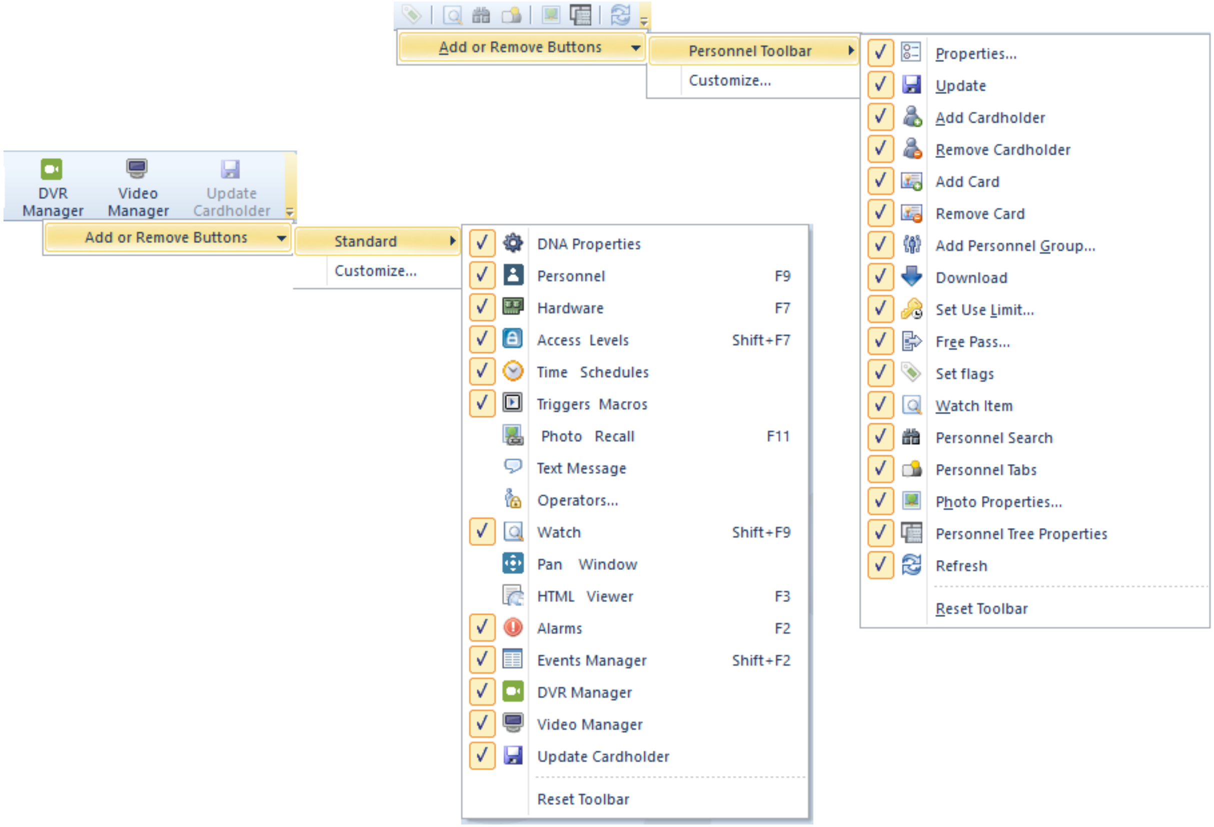


3. To hide a toolbar, **deselect** the menu item.

Adding and Removing Toolbar Buttons

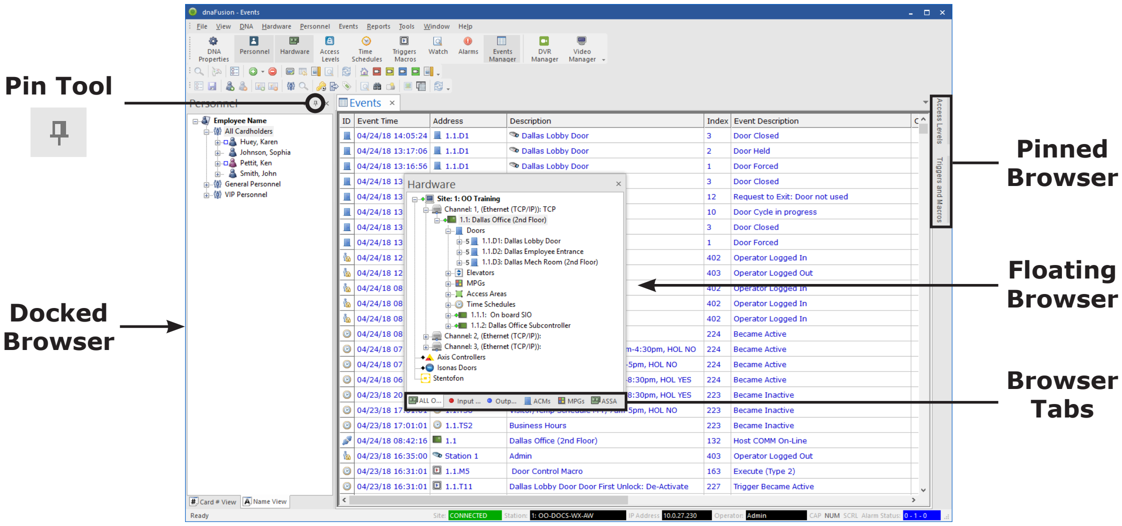
1. **Click** on the down-arrow to the right of the Secondary Toolbar and **select** Add or Remove Buttons / Toolbar.

   A list of toolbar items appears.
2. **Configure** the toolbar buttons:
   - **Check** an item to add it to the toolbar.
   - **Uncheck** an item to remove it from the toolbar.
   - **Click** Reset Toolbar to return the toolbar to its original settings and ignore any changes.



Browsers (Explorers)

Browsers, also referred to as explorers, are adjustable windows that populate when the operator selects certain buttons from the Standard Toolbar or the View / Explorers drop-down in the Main Menu. Browser information is organized in a hierarchical "tree" view, where tree objects represent nodes that can be expanded to view subgroups of related information. Some browsers also contain tabs at the bottom of the window. For example, the Hardware Browser contains tabs that, when selected, filter the tree by specific hardware types.



- Employee Name
  - All Cardholders
    - Huey, Karen
    - Johnson, Sophia
    - Pettit, Ken
    - Smith, John
  - General Personnel
  - VIP Personnel

- Site: 1: OO Training
  - Channel: 1, (Ethernet (TCP/IP)): TCP
    - 1.1: Dallas Office (2nd Floor)
      - Doors
        - 5 1.1.D1: Dallas Lobby Door
        - 5 1.1.D2: Dallas Employee Entrance
        - 5 1.1.D3: Dallas Mech Room (2nd Floor)
      - Elevators
      - MPGs
      - Access Areas
      - Time Schedules
      - 1.1.1: On board SIO
      - 1.1.2: Dallas Office Subcontroller
  - Channel: 2, (Ethernet (TCP/IP)):
  - Channel: 3, (Ethernet (TCP/IP)):
- Axis Controllers
- Isonas Doors
- Stentofon

ID	Event Time	Address	Description	Index	Event Description
	04/24/18 14:05:24	1.1.D1	Dallas Lobby Door	3	Door Closed
	04/24/18 13:17:06	1.1.D1	Dallas Lobby Door	2	Door Held
	04/24/18 13:16:56	1.1.D1	Dallas Lobby Door	1	Door Forced
	04/24/18 13			3	Door Closed
	04/24/18 13			12	Request to Exit: Door not used
	04/24/18 13			10	Door Cycle in progress
	04/24/18 13			3	Door Closed
	04/24/18 13			1	Door Forced
	04/24/18 12			402	Operator Logged In
	04/24/18 12			403	Operator Logged Out
	04/24/18 08			402	Operator Logged In
	04/24/18 08			402	Operator Logged In
	04/24/18 08			402	Operator Logged In
	04/24/18 08			224	Became Active
	04/24/18 07		m-4:30pm, HOL NO	224	Became Active
	04/24/18 07		-5pm, HOL NO	224	Became Active
	04/24/18 06		-8:30pm, HOL YES	224	Became Active
	04/23/18 20		8:30pm, HOL YES	223	Became Inactive
	04/23/18 17		5pm, HOL NO	223	Became Inactive
	04/23/18 17:01:01	1.1.TS2	Business Hours	223	Became Inactive
	04/24/18 08:42:16	1.1	Dallas Office (2nd Floor)	132	Host COMM On-Line
	04/23/18 16:35:00	Station 1	Admin	403	Operator Logged Out
	04/23/18 16:31:01	1.1.M5	Door Control Macro	163	Execute (Type 2)
	04/23/18 16:31:01	1.1.T11	Dallas Lobby Door Door First Unlock: De-Activate	227	Trigger Became Active

Ready Site: CONNECTED Station: 1: OO-DOCS-WX-AW IP Address 10.0.27.230 Operator: Admin CAP NUM SCRL Alarm Status: 0 - 1 - 0

By default, browsers are docked on the left or right side of the main screen. However, operators can drag them to any desired location by left-clicking the browser heading. Use the blue guidelines to dock a floating browser on the left, right, top, or bottom of the screen.

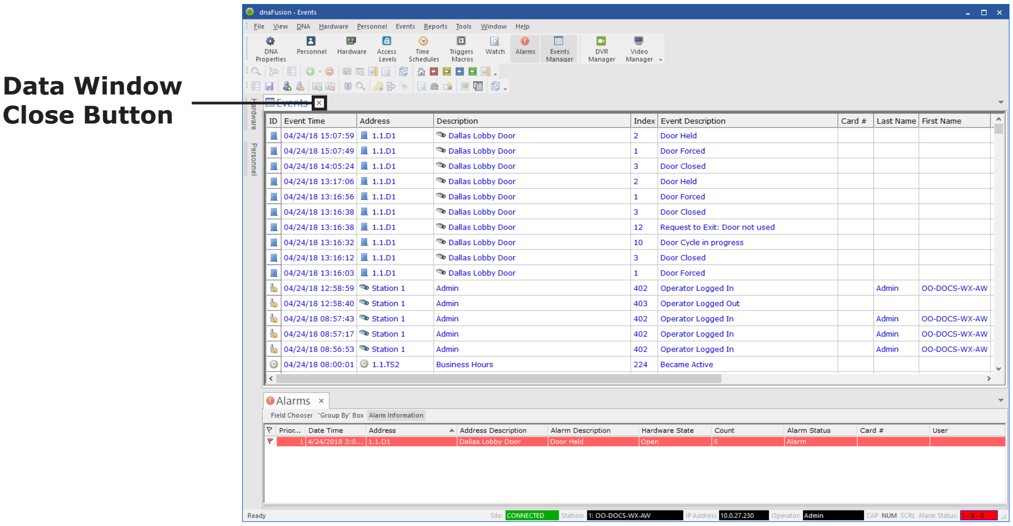
Alternatively, operators can select the Pin Tool to hide the browser in the form of a document tab. To recall the browser, hover the mouse cursor over the pinned tab; the browser will automatically hide when cursor moves outside of the browser's edge. Toggle the Pin Tool to dock the browser again.

Items in the browser tree have a parent-child relationship. The parent, or tree, object can be expanded to reveal subitems, known as child objects, by clicking the plus (+) sign. To collapse an expanded item in the browser tree, click the minus (-) sign.

Data Windows

Data windows are adjustable windows that populate when the operator selects the Alarms or Events Manager buttons from the Standard Toolbar. Typically, these windows are system-generated spreadsheets or dialog boxes populated partially by the operator.

Unlike browsers, data windows cannot be closed by clicking the same button that opened them. Instead, the Data Window must be closed by clicking the X located on the data window tab.



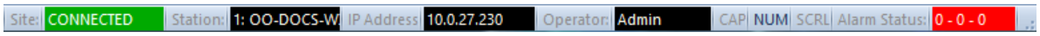
ID	Event Time	Address	Description	Index	Event Description	Card #	Last Name	First Name
	04/24/18 15:07:59	1.1.D1	Dallas Lobby Door	2	Door Held			
	04/24/18 15:07:49	1.1.D1	Dallas Lobby Door	1	Door Forced			
	04/24/18 14:05:24	1.1.D1	Dallas Lobby Door	3	Door Closed			
	04/24/18 13:17:06	1.1.D1	Dallas Lobby Door	2	Door Held			
	04/24/18 13:16:56	1.1.D1	Dallas Lobby Door	1	Door Forced			
	04/24/18 13:16:38	1.1.D1	Dallas Lobby Door	3	Door Closed			
	04/24/18 13:16:38	1.1.D1	Dallas Lobby Door	12	Request to Exit: Door not used			
	04/24/18 13:16:32	1.1.D1	Dallas Lobby Door	10	Door Cycle in progress			
	04/24/18 13:16:12	1.1.D1	Dallas Lobby Door	3	Door Closed			
	04/24/18 13:16:03	1.1.D1	Dallas Lobby Door	1	Door Forced			
	04/24/18 12:58:59	Station 1	Admin	402	Operator Logged In		Admin	OO-DOCS-WX-AW
	04/24/18 12:58:40	Station 1	Admin	403	Operator Logged Out			
	04/24/18 08:57:43	Station 1	Admin	402	Operator Logged In		Admin	OO-DOCS-WX-AW
	04/24/18 08:57:17	Station 1	Admin	402	Operator Logged In		Admin	OO-DOCS-WX-AW
	04/24/18 08:56:53	Station 1	Admin	402	Operator Logged In		Admin	OO-DOCS-WX-AW
	04/24/18 08:00:01	1.1.TS2	Business Hours	224	Became Active			

Prior...	Date Time	Address	Address Description	Alarm Description	Hardware State	Count	Alarm Status	Card #	User
1	4/24/2018 3:0...	1.1.D1	Dallas Lobby Door	Door Held	Open	5	Alarm		

Ready Site: CONNECTED Station: 1: OO-DOCS-WX-AW IP Address 10.0.27.230 Operator: Admin CAP NUM SCRL Alarm Status: 1 - 0 - 0

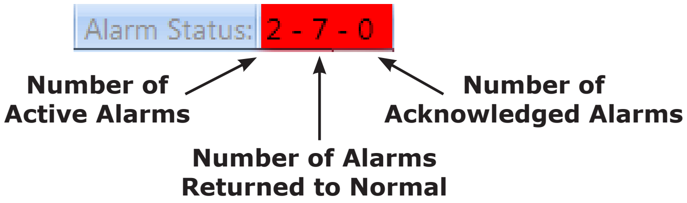
Status Bar

The Status Bar is located at the bottom of the application interface. It provides useful information about the workstation, including the site status, station name, IP address, active operator, and alarm status.



Site: CONNECTED Station: 1: OO-DOCS-W IP Address 10.0.27.230 Operator: Admin CAP NUM SCRL Alarm Status: 0 - 0 - 0

- Site – Displays the site status. If Connected, the DNA Driver (DNADrvr32) is running. If Disconnected, the DNA Driver is not communicating with the application.
- Station – Shows the Station Identification (client) information that was entered when the workstation was initially brought online. This information also appears in the Host Settings / Station Settings dialog.
- IP Address – Identifies the workstation's IP Address.
- Operator – Displays the username of the Operator currently logged in at the workstation.
- CAP/NUM/SCRL – Indicates whether the caps lock, num lock, and/or scroll lock is on or off for the workstation's keyboard. (Black text = ON).
- Alarm Status – Displays the current alarm counts in the Alarm Grid. The field's background color changes depending on the state of the alarms:
  - □ Red = Active alarms
  - □ Blue = Returned to normal
  - □ Black = No active alarms



Alarm Status: 2 - 7 - 0

Number of Active Alarms

Number of Alarms Returned to Normal

Number of Acknowledged Alarms

The Status Bar also includes a couple of interactive features:

- Change Operators - **Double-click** on the Operator field.
- Open the Alarm Grid - **Double-click** on the Alarm Status field.

NOTES:

Customize Dialog

In addition to selecting which toolbars to display and hide, toolbars can be customized to provide greater efficiency or to create a profile for other users with specific buttons. New toolbars may even be created and customized according to the desires of the operator.

1. To display the Customize dialog, **click** on the small down-arrow to the right of the Standard Toolbar and **select** Add or Remove Buttons / Customize OR **select** View / Toolbars / Customize from the Main Menu.

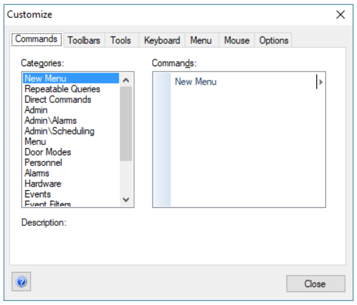
   The Customize dialog opens.

   The following tabs are available:

   - Commands - Displays all commands and allows the operator to customize commands.
   - Toolbars - Displays all toolbars and allows the operator to add and customize toolbars.
   - Tools - Displays all the available tools and allows the operator to configure new tools.
   - Keyboard - Displays the shortcut key for the selected command and allows the operator to configure new shortcut keys.
   - Menu - Allows the operator to reset a selected menu and add commands to context menus.
   - Mouse - Allows the operator to customize mouse controls.
   - Options - Allows the operator to configure the view settings for menus and toolbars.
2. After customizing DNA Fusion, **close** the application to save the settings.

Commands

1. **Select** the Commands tab.



Categories:
New Menu
Repeatable Queries
Direct Commands
Admin
Admin\Alarms
Admin\Scheduling
Menu
Door Modes
Personnel
Alarms
Hardware
Events
Event Filters

Commands:
New Menu

2. **Select** a Category from the list.
3. **Drag** the desired command to an active toolbar. See page 2-13 for more information.

   The command appears on the toolbar.
4. **Click** Close to close the dialog.

Toolbars

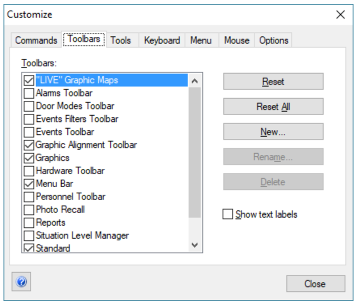
1. **Select** the Toolbars tab.
2. **Click** the New button.

   The Toolbar Name dialog appears.
3. **Enter** a Name for the new toolbar and **click** OK.

   The toolbar is added to the list.
4. **Check** the new Toolbar item to enable it in the main screen.
5. **Click** the Commands tab.
6. **Drag** the desired commands from the list in the Commands tab to the new toolbar.

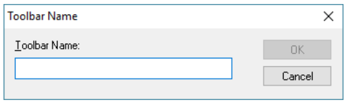
   OR

   Drag buttons from active toolbars to the new toolbar.
7. **Close** the Customize dialog.



Toolbars:
☑ "LIVE" Graphic Maps
□ Alarms Toolbar
□ Door Modes Toolbar
□ Events Filters Toolbar
□ Events Toolbar
☑ Graphic Alignment Toolbar
☑ Graphics
□ Hardware Toolbar
☑ Menu Bar
□ Personnel Toolbar
□ Photo Recall
□ Reports
□ Situation Level Manager
☑ Standard

□ Show text labels

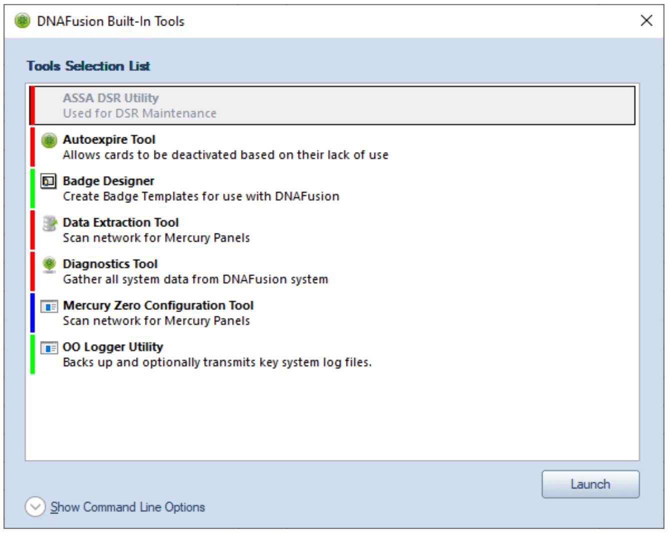


Toolbar Name:

Tools

The Tools option in the Main Menu contains a list of built-in tools. The operator/administrator can select a tool from the Tool Selection List and will launch the desired application. See page 20-15 for more information.

1. **Select** Tools from the Main Menu.



DNAFusion Built-In Tools

Tools Selection List

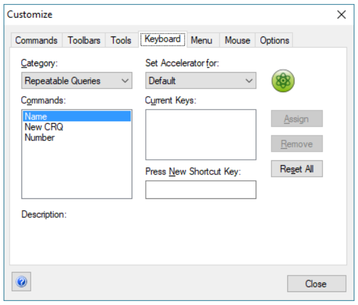
- ASSA DSR Utility
  Used for DSR Maintenance
- Autoexpire Tool
  Allows cards to be deactivated based on their lack of use
- Badge Designer
  Create Badge Templates for use with DNAFusion
- Data Extraction Tool
  Scan network for Mercury Panels
- Diagnostics Tool
  Gather all system data from DNAFusion system
- Mercury Zero Configuration Tool
  Scan network for Mercury Panels
- OO Logger Utility
  Backs up and optionally transmits key system log files.

2. **Select** a tool from the Tools Selection List.
3. **Click** Launch.

Keyboard

Keyboard shortcuts can be created to save time when performing operations in DNA Fusion. See Appendix C for a list of default shortcut keys.

1. **Select** the Keyboard tab.



Customize

Category: Repeatable Queries

Set Accelerator for: Default

Commands:
Name
New CRQ
Number

Current Keys:

Press New Shortcut Key:

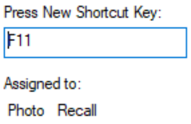
Description:

2. **Select** the Category from the drop-down list.
3. **Select** the Command from the list.

   If a shortcut key is already assigned to the command, it will appear in the Current Keys field.

4. **Place** the cursor in the Press New Shortcut Key field and **press** the new shortcut key or key combination that will be assigned to the selected command.

   The combination appears in the field. If the shortcut has already been assigned to another command, it will appear below the Press New Shortcut Key field.



Press New Shortcut Key: F11

Assigned to: Photo Recall

5. **Click** Assign to assign the shortcut to the selected command.

   This action will override the shortcut key if it is already assigned to another command.

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

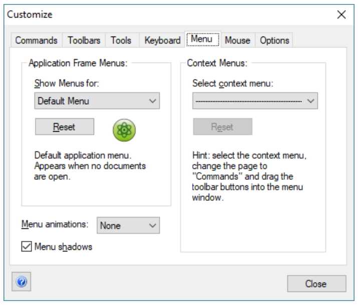
Menu

1. **Select** the Menu tab.

   Two menu types are configurable:

   - Application Frame Menus - Items located in the Main Menu.
   - Context Menus - Context-specific menus that result from right-clicking on a point or object.

Application Frame Menus



Application Frame Menus:

Show Menus for: Default Menu

Default application menu. Appears when no documents are open.

Menu animations: None

☑ Menu shadows

Context Menus:

Select context menu: ------------------------------

Hint: select the context menu, change the page to "Commands" and drag the toolbar buttons into the menu window.

2. **Select** the Menu from the drop-down list.

   The Main Menu will appear as if the window was active.

3. **Select** the Commands tab and move the item(s) to the desired menu location.
4. **Click** Close to save and close the dialog.

Context Menus

2. **Select** the Context Menu from the drop-down list.

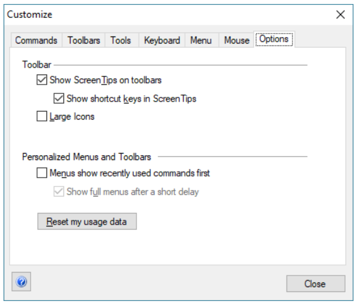
   The Context Menu will appear in a new dialog.

3. **Select** the Commands tab and move the item(s) to configure the context menu.
4. **Click** Close to save and close the dialog.

> **Click** Reset *to restore the selected menu to the original settings; all changes will be lost.*

Options

1. **Select** the Options tab.



Toolbar

☑ Show ScreenTips on toolbars

☑ Show shortcut keys in ScreenTips

□ Large Icons

Personalized Menus and Toolbars

□ Menus show recently used commands first

☑ Show full menus after a short delay

- Show ScreenTips on Toolbars - Shows each toolbar icon’s function on mouse hover.
  - □ Show Shortcut Keys in ScreenTips - Displays assigned shortcut keys in the toolbar’s ScreenTips.
- Large Icons - Increases the size of the toolbar icons.
- Menus Show Recently Used Commands First - Displays recently used menu items first and collapses the remaining items into a separate drop-down.
  - □ Show Full Menus After a Short Delay - Reveals all collapsed menu items after a short delay.
- Reset My Usage Data - Clears recently used commands.

2. **Select** Close to save and close the dialog.

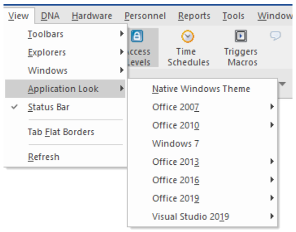
NOTES:

Customizing the DNA Environment

Changing the Desktop Appearance

1. **Select** View / Application Look from the Main Menu.
2. **Select** the desired setting from the context menu.

   The DNA Fusion interface changes to reflect the setting selected.



Changing the Data Window Appearance

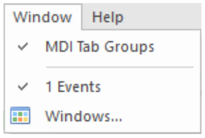
1. **Select** Window from the Main Menu.

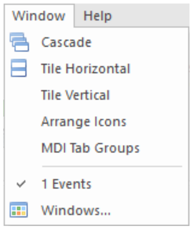
   If MDI Tab Groups is checked, the active windows are nested together in the Data Window.

   To tile the windows, **drag** the tab of the desired window to the left, right, top, or bottom of the Data Window until a blue guideline appears in the window, then **drop** the tab.

   If the MDI Tab Groups is unselected, the menu options change and the windows become detached from the Data Window. To arrange the windows, **select** the desired option from the Window menu on the Main Menu.
2. **Select** the desired setting from the resulting list.

   The Data Window changes to reflect the selected setting.

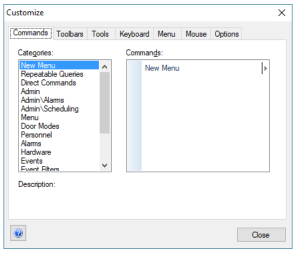




Hiding a Main Menu Item

1. With the Customize dialog open, **click** on the menu heading to be hidden.
2. **Drag** and **drop** it off the Main Menu and onto any other panel or section of the screen.

   An X will appear next to the button icon when the menu item is in a delete location. The menu heading will be hidden from view and no part of the menu will be visible.



Adding Toolbar Buttons

1. **Click** on the small down-arrow to the right of the Standard Toolbar and **select** Customize.

   The Customize dialog opens.
2. In the Commands tab, locate the Command and **drag** and **drop** it onto the desired Toolbar.

   OR

   Locate the desired item on the menu or toolbar and **drag** and **drop** it onto the desired Toolbar.

   A black line will appear on the toolbar to identify the location. If an X appears, the selected location is not valid.

   The Command will appear on the Toolbar.

Hiding Toolbar Buttons

1. With the Customize dialog open, **click** on the toolbar button to be hidden.
2. **Drag** and **drop** it away from the toolbar and onto any other area of the screen.

   An X will appear next to the button icon when the button is in a delete location. The toolbar will be hidden from view and its function will not be accessible.

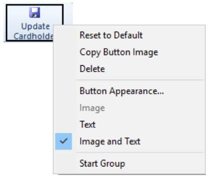
> ! *Buttons are moved from one toolbar to another; they are not copied. When a button is moved to a custom toolbar, it is removed from the original toolbar. To copy a button,* ***press*** *and* ***hold*** *the* Ctrl *key while moving the button.*

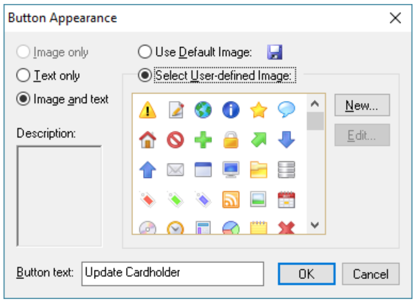
Modifying Toolbar Buttons

All toolbar buttons and icons can be modified.

1. With the Customize dialog open, **right-click** on the button you wish to modify.
2. **Select** Button Appearance from the context menu.

   The Button Appearance dialog opens.





Button text: Update Cardholder

3. **Select** the Select User-Defined Image checkbox.

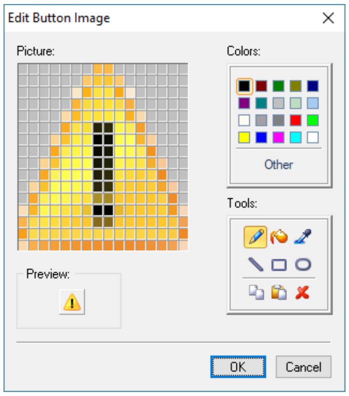
   The default images become active in the panel below.
4. **Select** an Icon from the panel and, if desired, **select** the Edit button to edit the current selection.

   Or

   Select the New button to create a new icon.

   The Edit Button Image dialog appears.

   Use the simple drawing interface to create or modify an icon. A live Preview appears below the drawing.



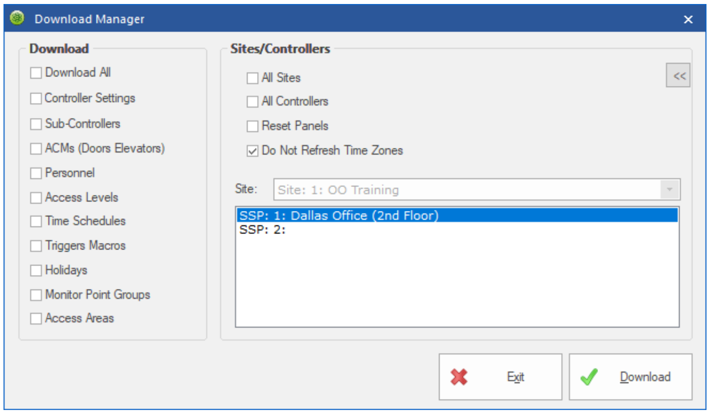
5. **Select** Colors and Tools from the palette.
6. **Click** OK to save the icon and return to the Button Appearance dialog.
7. If desired, **enter** a new description in the Button Text field.
8. **Click** OK to save the changes and return to the Customize dialog.
9. **Click** Close to exit the Customize dialog.

Downloading

Records must be downloaded to the controller before they can be added to the panel. Open Options recommends performing a full download when entering or changing large amounts of information.

1. Depending on the object, there are numerous ways to perform a download.
   - From the Hardware Browser, **right-click** on the Site and **select** Download OR **select** Hardware / Download from the Main Menu.
   - From the Personnel Browser, **right-click** on the desired Cardholder or Card object and **select** Download OR **select** Personnel / Download from the Main Menu.
   - For individual downloads, **right-click** on the desired object and **select** Download.

   Unless the operator is performing an individual download, the Download Manager dialog appears.



☐ Download All
☐ Controller Settings
☐ Sub-Controllers
☐ ACMs (Doors Elevators)
☐ Personnel
☐ Access Levels
☐ Time Schedules
☐ Triggers Macros
☐ Holidays
☐ Monitor Point Groups
☐ Access Areas

☐ All Sites
☐ All Controllers
☐ Reset Panels
☑ Do Not Refresh Time Zones

Site: Site: 1: OO Training

SSP: 1: Dallas Office (2nd Floor)
SSP: 2:

2. **Select** the Download All checkbox to download all information to the controller(s).

   OR

   Select individual download options.
3. **Select** the desired Site(s)/Controller(s).
4. **Click** OK.

   A status bar will indicate the download’s progress. **Click** the Exit button at any time to close the window without affecting the download.

> *The download status of a controller can also be viewed by* **right-clicking** *on the controller and* **selecting** *the* Status / Download Status *option. See page 8-31 for more information.*

This Page Intentionally Left Blank

DNA Properties 3

In This Chapter

√ Station Settings
√ DNA Properties
√ Situation Manager
√ E-Mail Enable
√ Personnel Properties
√ Hardware Tree Settings

DNA Fusion is designed to adapt to a variety of system and user needs. To that end, the operator can use the Host Settings to configure the application's appearance and behavior on their individual workstation.

The Host Settings are parameters that determine the display and operational preferences as well as the manner in which the application will perform a given task. Most of the Host Settings are workstation-specific; however, a number of options are applied globally.

Host Settings Dialog

The DNA Properties are configured using a series of dialogs in the Host Settings. Changes to these properties only affect the host workstation.

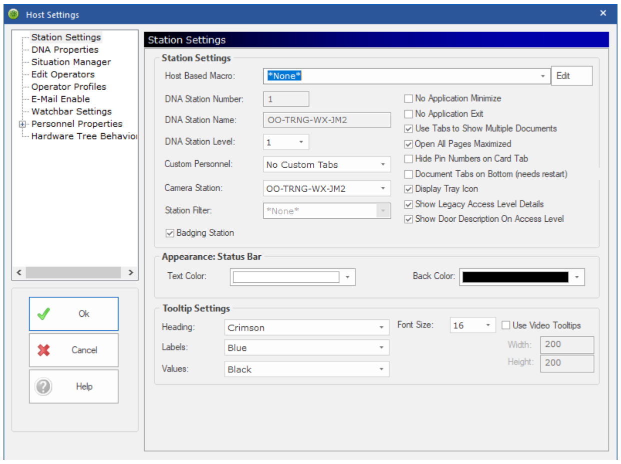
To open the Host Settings:

1. **Click** the DNA Properties button on the Standard Toolbar.

   OR

   Select DNA / Administrative / Properties from the Main Menu.

   The Host Settings dialog appears.



Station Settings

Station Settings

Host Based Macro: *None*

DNA Station Number: 1

DNA Station Name: OO-TRNG-WX-JM2

DNA Station Level: 1

Custom Personnel: No Custom Tabs

Camera Station: OO-TRNG-WX-JM2

Station Filter: *None*

☑ Badging Station

☐ No Application Minimize
☐ No Application Exit
☑ Use Tabs to Show Multiple Documents
☑ Open All Pages Maximized
☐ Hide Pin Numbers on Card Tab
☐ Document Tabs on Bottom (needs restart)
☑ Display Tray Icon
☑ Show Legacy Access Level Details
☑ Show Door Description On Access Level

Appearance: Status Bar

Text Color: □ Back Color: ■

Tooltip Settings

Heading: Crimson

Labels: Blue

Values: Black

Font Size: 16

☐ Use Video Tooltips

Width: 200

Height: 200

2. **Select** a Category from the dialog menu.

   The associated dialog opens. See pages 3-3 through 3-29 for information about each dialog.

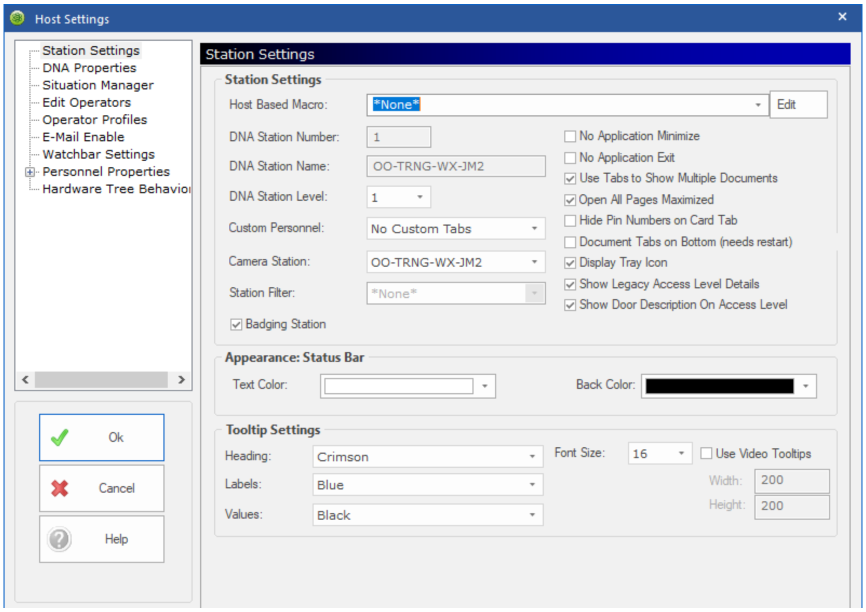
3. Depending on the selection, **perform** one or more of the following actions:

   - **Enter** data in the fields.
   - **Use** the drop-down menus and link browser buttons.
   - **Select** the desired radio buttons and checkboxes.

This Page Intentionally Left Blank

Station Settings

The Station Settings dialog is used to configure the workstation's settings to determine how DNA will behave.



Station Settings

Host Based Macro: *None* Edit

DNA Station Number: 1

DNA Station Name: OO-TRNG-WX-JM2

DNA Station Level: 1

Custom Personnel: No Custom Tabs

Camera Station: OO-TRNG-WX-JM2

Station Filter: *None*

☑ Badging Station

☐ No Application Minimize

☐ No Application Exit

☑ Use Tabs to Show Multiple Documents

☑ Open All Pages Maximized

☐ Hide Pin Numbers on Card Tab

☐ Document Tabs on Bottom (needs restart)

☑ Display Tray Icon

☑ Show Legacy Access Level Details

☑ Show Door Description On Access Level

Appearance: Status Bar

Text Color: □ Back Color: ■

Tooltip Settings

Heading: Crimson

Labels: Blue

Values: Black

Font Size: 16

☐ Use Video Tooltips

Width: 200

Height: 200

Station Settings

- Host Based Macro - Select the Host Based Macro to associate to the workstation or click Edit to open the Host Based Macro (Global I/O) dialog.
- DNA Station Number - Displays the local station number. (Read-only)
- DNA Station Name - Displays the local station name. (Read-only)
- DNA Station Level - Designates the workstation's level (1-32) to determine which operators can log in at the station based on their operator profile settings. See page 4-8 for more information.
- Custom Personnel - Select an option below.
    - □ No Custom Tabs - If selected, uses only the default Custom Fields found on the Employee Info (Page 2) tab of the Personnel Record. Does not include items from the Custom Fields tab. See page 3-26 for setup information.
    - □ 1 to 1 Linkage (Legacy) - If selected, personnel records will include a separate tab labeled Custom Fields. The fields in this tab are configured in the Personnel Custom Fields Setup dialog. Allows the operator to identify up to 50 fields. See page 3-17 for more information.
    - □ 1 to Many Linkage - If selected, the predefined Custom Fields located in the Custom Fields tab of the Personnel Record will be used. Allows the operator to identify up to 50 alphanumeric fields and places the data into a grid. These fields can only be edited through the Custom Fields Editor tool. Contact Open Options Technical Support for more information on this tool.
- Camera Station - Select a workstation from the drop-down to import the camera (IP-based) settings from the selected workstation to the current workstation.
- Station Filter - Determines which Event Filter or Alarm Escalation Filter to apply to the DNA workstation. This option will be grayed out unless the Filters feature is configured. See page 14-29 for more information.
- Badging Station - Check if this machine will be used as a badging station. Must be licensed for badging functionality. If selected, two features are added to the workstation: the ID Badging tab in the Personnel Record and the Photo ID dialog in the Personnel Properties. See Chapter 21 for more information.
- No Application Minimize - Removes the minimize button; the application must restart to take effect.
- No Application Exit - Removes the exit function.
- Use Tabs to Show Multiple Documents - Enables tabs to display multiple documents.
- Open All Pages Maximized - All pages will display maximized when opened.

- Use Embedded Video Windows - Select if using a DVR integration.
- Hide pin numbers on card tab (needs restart) - If checked, PIN numbers will be masked on the cardholder's record.
- Show Document Tabs on Bottom - If checked, data window tabs will appear at the bottom of the window instead of the top. Requires an application restart to take effect.
- Display Tray Icon - The DNA Fusion icon will appear in the Windows Tray when the application is running. The icon will also convey important system information (e.g. driver connection status) in the form of a balloon.
- Show Legacy Access Level Details - If checked, the Add Legacy Access Level Group option will be available from the Access Levels Browser when the operator right-clicks on the Access Level Groups header.
- Show Door Description on Access Level - If checked, the Door Description will appear in the Access Levels Browser for door objects under the Access Level Groups header.

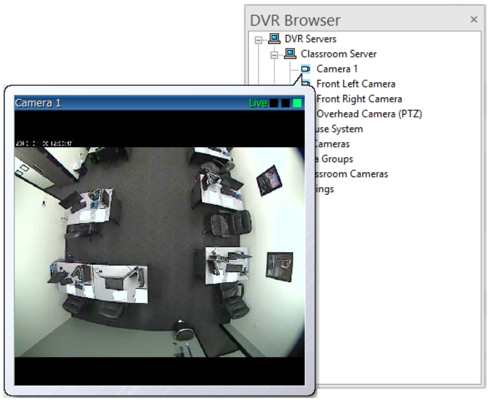
Appearance: Status Bar

- Text Color - Changes the text color on the Status Bar.
- Back Color - Changes the background color on the Status Bar.

> *Color changes on the* Status Bar *will not take effect until DNA Fusion restarts.*

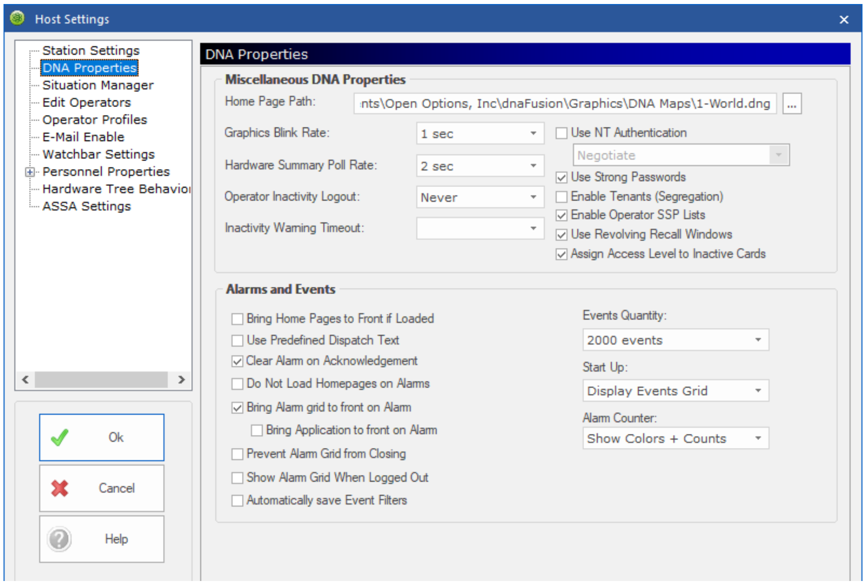
Tooltip Settings

- Heading - Changes the heading color on tooltips. (Default = Crimson)
- Labels - Changes the label color on tooltips. (Default = Blue)
- Values - Changes the value color on tooltips. (Default = Black)
- Font Size - Changes the heading font size on tooltips.
- Use Video Tooltips - If checked, hovering the cursor over a camera in the DVR Browser will display a live video tooltip.
  - □ Width - Sets the width for the tooltip video window.
  - □ Height - Sets the height for the tooltip video window.



DNA Properties

The DNA Properties dialog configures many of the common properties that affect how the application behaves.



DNA Properties

Miscellaneous DNA Properties

Home Page Path: nts\Open Options, Inc\dnaFusion\Graphics\DNA Maps\1-World.dng

Graphics Blink Rate: 1 sec

Hardware Summary Poll Rate: 2 sec

Operator Inactivity Logout: Never

Inactivity Warning Timeout:

□ Use NT Authentication

Negotiate

☑ Use Strong Passwords

□ Enable Tenants (Segregation)

☑ Enable Operator SSP Lists

☑ Use Revolving Recall Windows

☑ Assign Access Level to Inactive Cards

Alarms and Events

□ Bring Home Pages to Front if Loaded

□ Use Predefined Dispatch Text

☑ Clear Alarm on Acknowledgement

□ Do Not Load Homepages on Alarms

☑ Bring Alarm grid to front on Alarm

□ Bring Application to front on Alarm

□ Prevent Alarm Grid from Closing

□ Show Alarm Grid When Logged Out

□ Automatically save Event Filters

Events Quantity: 2000 events

Start Up: Display Events Grid

Alarm Counter: Show Colors + Counts

Miscellaneous DNA Properties

- Home Page Path - Main graphic page. Often used as a starting point to link other graphic pages in the system. The Home Page is accessed through the Main Menu (File / DNA Homepage).
- Graphics Blink Rate - The rate at which an object on a graphic page will blink in the event of an alarm.
- Hardware Summary Poll Rate - The amount of time between hardware status updates.
- Operator Inactivity Logout - Logs out the operator after the selected length of inactivity.
- Inactivity Warning Timeout - Determines the number of seconds prior to inactivity logout that a warning will appear.
- Use NT Authentication - If checked, DNA Fusion uses Windows NT Authentication; select the desired authentication protocol from the drop-down.
  - Negotiate - Automatically selects between Kerberos and NTLM based on network compatibility.
  - NTLM - Uses an encrypted challenge/response mechanism to authenticate the user.
  - Kerberos - Protocol of choice; supports mutual authentication between the client and server before establishing a secure network connection. Adds greater security than NTLM to network systems.

> ❗ *NT Authentication requires an operator with admin privileges that uses the same username as the NT network logon. See page 4-1 for information on adding operators.*

- Use Strong Passwords - Enforces strong passwords for DNA operators. When enabled, passwords must contain both lowercase and uppercase letters, a punctuation character, a numerical character, and meet a minimum 8-character length requirement. This field is only available if Use NT Authentication is not selected.
- Enable Tenants (Segregation) - Activates the tenants feature (see Chapter 13) to restrict multi-tenant viewing for certain operators and enables fields in the Personnel Properties / Tenant Settings dialog. Enabling this feature results in changes to both the hardware and personnel settings. If enabled/disabled on the database server, it also prompts the operator to sync indexes via the DNA Indexing Utility.
- Enable Operator SSP Lists - Enables the Profile SSP List button in the Operator Profiles dialog, allowing operators to control specific SSP controllers. This is a global setting that affects system hardware at the controller level. See page 4-27 for more information.
- Use Revolving Recall Windows - Allows the operator to assign specific doors to the Photo Recall Windows. See page 7-43 for more information.
- Assign Access Level to Inactive Cards - Provides the ability to assign an access level to an inactive card.

Alarms and Events

- Bring Home Pages to Front if Loaded - If a Home Page is associated with an alarm point, the home page is brought to the front of the application when the object goes into alarm.
- Use Predefined Dispatch Text - Requires the operator to use predefined dispatch text to clear an alarm. See page 14-25 for more information.
- Clear Alarm on Acknowledgement - Allows the operator to clear alarms on acknowledgement if the object has returned to its normal state.

> ❗ *Keep in mind that these settings are workstation-specific; if alarms will be monitored on multiple stations,* Clear Alarm on Acknowledgement *should NOT be selected on any station.*

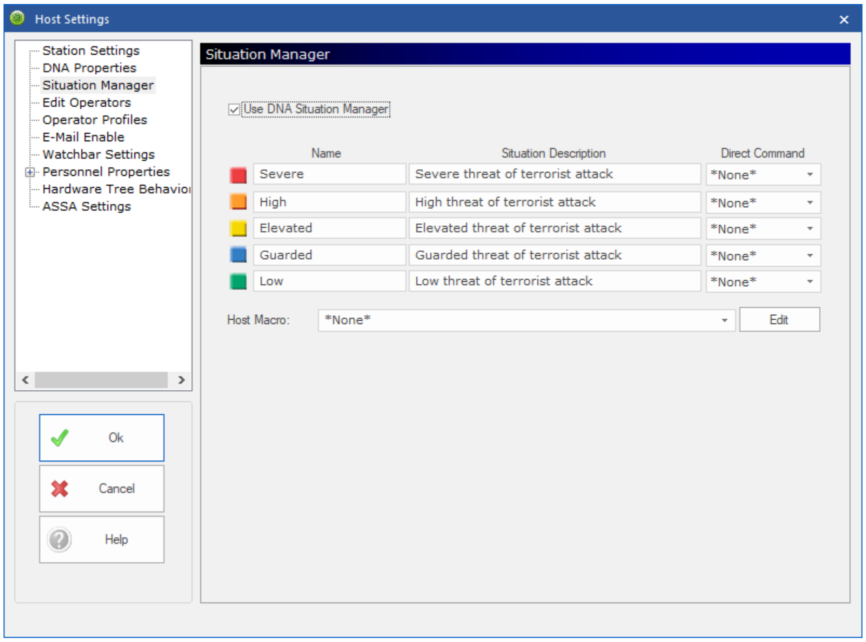
- Do Not Load Homepages on Alarms - If selected, and homepages have been specified for hardware objects, they will not be loaded on this workstation in the event of an alarm.
- Bring Alarm Grid to Front on Alarm - If selected, the Alarm Grid will automatically move to the front when an alarm is generated, and the Bring Application to Front on Alarm checkbox will become available.
- Bring Application to Front on Alarm - If selected, the DNA Fusion application will automatically move to the front when an alarm is generated. This option is only available if Bring Alarm Grid to Front on Alarm is checked.
- Prevent Alarm Grid from Closing - If selected, the Alarm Grid cannot be closed on the workstation after it is opened.
- Show Alarm Grid When Logged Out - If selected, the Alarm Grid will be visible when the operator is logged out of DNA. Operators will be required to log in to respond to alarms.
- Automatically Save Event Filters - If selected, all Event Filters applied to the Events Grid will be saved when the grid is closed and reapplied when the grid is opened again.

> ⓘ *If* Automatically Save Event Filters *is checked, DNA Fusion will save the event filters applied to the* Events Grid *in the* Default.evt *file. The DNA operator will need basic read/write privileges to the folder and file. Default location:*
>
> - 64-bit OS — C:\Program Files (x86)\DNAFusion
> - 32-bit OS — C:\Program Files\DNAFusion

- Events Quantity - Maximum number of events displayed in the Events Grid.
- Start Up - Specifies which page will appear during application startup.
- Alarm Counter - Allows the administrator to select the format for the Alarm Status Bar at the bottom of the DNA window.

Situation Manager

The Situation Manager dialog is used to configure Situation Levels. See Chapter 9 for more information.



Situation Manager

☑ Use DNA Situation Manager

	Name	Situation Description	Direct Command
🟥	Severe	Severe threat of terrorist attack	*None*
🟧	High	High threat of terrorist attack	*None*
🟨	Elevated	Elevated threat of terrorist attack	*None*
🟦	Guarded	Guarded threat of terrorist attack	*None*
🟩	Low	Low threat of terrorist attack	*None*

Host Macro: *None*

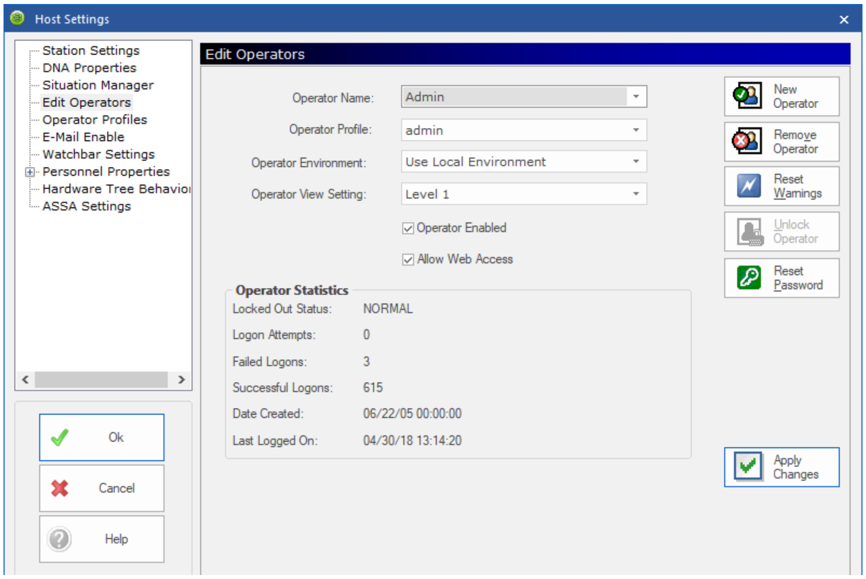
Situation Manager Settings

- Use DNA Situation Manager - Enables the Situation Manager, which allows the operator to configure situation levels.
- Situations - Enter the Name and Description for each color-coded situation. Direct commands can also be linked to the situation by selecting a command from the drop-down. See page 8-29 for more information.
- Host Macro - If desired, select a Host Macro from the drop-down. See page 10-13 for more information.

NOTES:

Edit Operators

The Edit Operators dialog allows you to add operators and assign operator profiles to the selected operator. See Chapter 4 for more information.



Edit Operators

Operator Name: Admin

Operator Profile: admin

Operator Environment: Use Local Environment

Operator View Setting: Level 1

☑ Operator Enabled

☑ Allow Web Access

Operator Statistics

Locked Out Status:	NORMAL
Logon Attempts:	0
Failed Logons:	3
Successful Logons:	615
Date Created:	06/22/05 00:00:00
Last Logged On:	04/30/18 13:14:20

- Operator Name - Select the operator name to edit or remove.
- Operator Profile - Select the profile to assign to the selected operator.
- Operator Environment - If configured, select the database desktop view that the operator will see upon logging in. The default setting is Use Local Environment. See page 4-21 for more information.
- Operator View Setting - Select which local environment desktop view the operator will see upon login. See page 4-21 for more information on setting up the operator environment from the local registry.
- Operator Enabled - If unchecked, the operator will not be able to log in to DNA Fusion.
- Allow Web Access - If checked, the selected operator will be able to log in to Fusion Web. See the Fusion Web Manual for more information.

Operator Statistics

- Locked Out Status - Displays the lockout status for the selected operator.
- Logon Attempts - Number of times the selected operator has attempted to log in to DNA.
- Failed Logons - Number of times the selected operator has attempted to log in to DNA but failed.
- Successful Logons - Number of times the selected operator has successfully logged in to DNA.
- Date Created - Date the operator was created.
- Last Logged On - Date the operator last logged in to DNA.

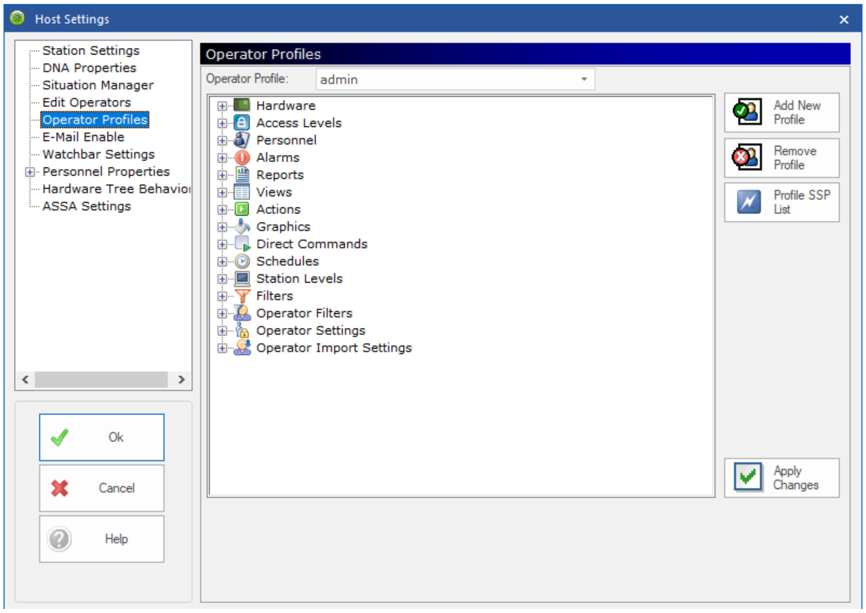
Options

- New Operator - Opens the Password Verification dialog to create a new operator.
- Remove Operator - Deletes the selected operator.
- Reset Warnings - Restores warning dialogs that have been disabled by the selected operator.
- Unlock Operator - Unlocks the selected operator’s account. This option will be available if the selected operator is currently in a locked out status.
- Reset Password - Opens the Password Verification dialog to change the selected operator's password.
- Apply Changes - Saves the current configuration.

> ! *The* Apply Changes *button must be selected in order to save changes to the dialog. Otherwise, all changes will be lost when selecting another operator or closing the dialog.*

Operator Profiles

The Operator Profiles dialog is used to configure rights and privileges for DNA Fusion operators. See Chapter 4 for more information.



Operator Profile: admin

- Operator Profile - Select the operator profile to edit or remove.
- Privileges - Expand categories and check the boxes to select or deselect the desired privileges.

  □ Hardware
  □ Access Levels
  □ Personnel
  □ Alarms
  □ Reports
  □ Views
  □ Actions
  □ Graphics
  □ Direct Commands
  □ Schedules
  □ Tenants
  □ Station Levels
  □ Filters
  □ Operator Filters
  □ Operator Settings
  □ Operator Import Settings

> *The* Tenants *privileges are only available when* Enable Tenants (Segregation) *is checked in the* DNA Properties *dialog.*

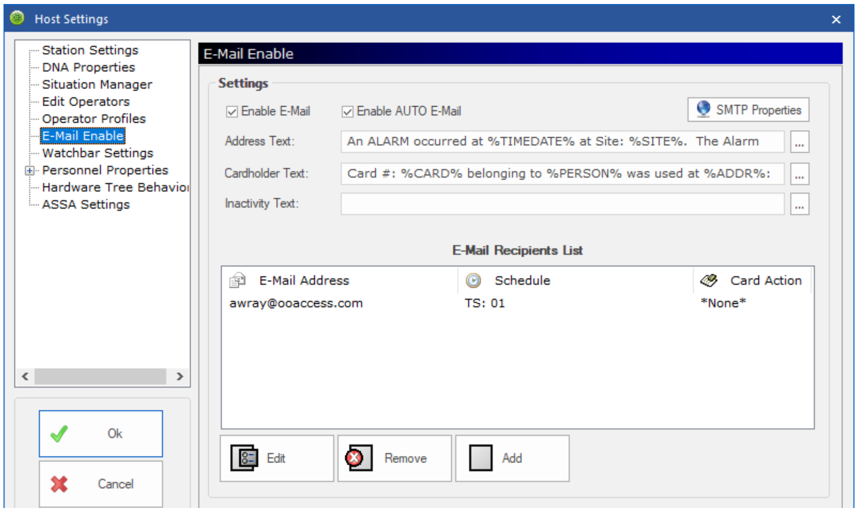
Options

- Add New Profile - Adds a new operator profile; opens the Add DNA Operator Profile dialog.
- Remove Profile - Deletes the selected operator profile.
- Profile SSP List - Opens the Operator Controller Selection dialog to grant or restrict operator access to specific SSPs. To use this feature, select the Enable Operator SSP Lists checkbox in the Host Settings / DNA Properties dialog. See page 4-27 for more information.
- Apply Changes - Saves the dialog's current configuration.

> *The* Apply Changes *button must be selected in order to save changes to the dialog. Otherwise, all changes will be lost when selecting another operator profile or closing the dialog.*

E-Mail Enable

The E-Mail Enable dialog is used to activate the AUTO E-Mail feature after the SMTP Properties have been configured. E-mail events can also be set up as Host Based Macros in the Email Authentication section of the Driver Setup dialog. See page 20-3 to set up e-mail authentication.



☑ Enable E-Mail ☑ Enable AUTO E-Mail

Address Text: An ALARM occurred at %TIMEDATE% at Site: %SITE%. The Alarm

Cardholder Text: Card #: %CARD% belonging to %PERSON% was used at %ADDR%:

Inactivity Text:

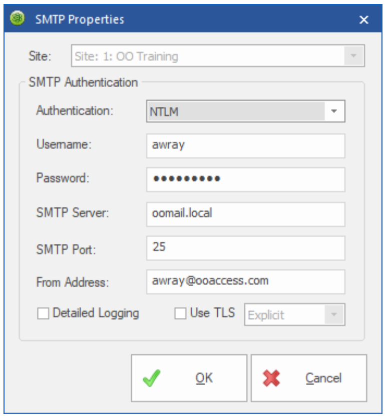
E-Mail Address	Schedule	Card Action
awray@ooaccess.com	TS: 01	*None*

Settings

- Enable E-Mail - Enables the e-mail function. Must be selected to activate the remaining dialog fields.
- Enable AUTO E-Mail - Enables the AUTO e-mail function; the Address Text and Cardholder Text fields.
  - ◻ Address Text - (AUTO) Event text sent with an alarm/event. Enter the desired text using the Replacement Text described in Appendix D.
  - ◻ Cardholder Text - (AUTO) Event text sent with a cardholder event. Enter the desired text using the Replacement Text described in Appendix D.
  - ◻ Inactivity Text - (AUTO) Event text sent with an operator inactivity event. **Enter** the desired text using the Replacement Text described in Appendix D.
- SMTP Properties - Opens the SMTP Properties dialog. See below.

SMTP Properties

The SMTP Properties dialog must be configured to receive automatic e-mails using the SMTP feature. If there is no connection to port 25, see the system administrator and request that SMTP be enabled and/or modify any anti-virus software to allow DNA Fusion (dnafusion.exe) to e-mail third-party addresses.



Site: Site: 1: OO Training

Authentication: NTLM

Username: awray

Password: •••••••••

SMTP Server: oomail.local

SMTP Port: 25

From Address: awray@ooaccess.com

☐ Detailed Logging ☐ Use TLS Explicit

- Authentication - Type of authentication.
- Username - User’s SMTP name.
- Password - User’s SMTP password.
- SMTP Server - E-mail server’s name.
  If configured, the mail server’s name and outbound port information should be obtained from the Information Technology department.
- SMTP Port - Default is 25. If needed, change the port number.
- From Address - E-mail address that will appear in the From: field.
- Detailed Logging - If selected, enables a high level of logging used to troubleshoot e-mail failures. Do NOT enable this option unless advised by Open Options Technical Support.
- Use TLS - Enforces Transport Layer Security (TLS) encryption. All TLS modes are equally secure but have different port requirements.
  - ◻ Automatic - Selects the best encryption method.
  - ◻ Implicit - Encryption is switched on as soon as the channel is established.
  - ◻ Explicit - Client requests TLS encryption to be enabled.

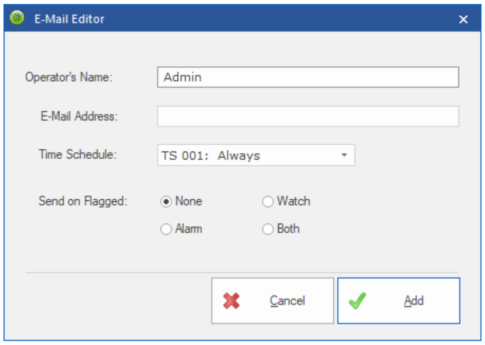
E-Mail Recipients List

The E-Mail Recipients List contains a list of e-mail recipients as well as any time schedules or card flags associated with the e-mail event.

- Edit - Edits the selected recipient record; opens the E-mail Editor dialog.
- Remove - Removes the selected recipient.
- Add - Adds a new recipient; opens the E-Mail Editor dialog.

E-Mail Editor

- Operator's Name - Recipient's name.
- E-Mail Address - Recipient's e-mail address.
- Time Schedule - E-mails will be sent during the specified time schedule.
- Send on Flagged - Select the condition under which a cardholder event will be e-mailed. Selecting Both will notify the recipient(s) of cardholder events that have been marked as Alarm and Watch cards.



E-Mail Editor

Operator's Name: Admin

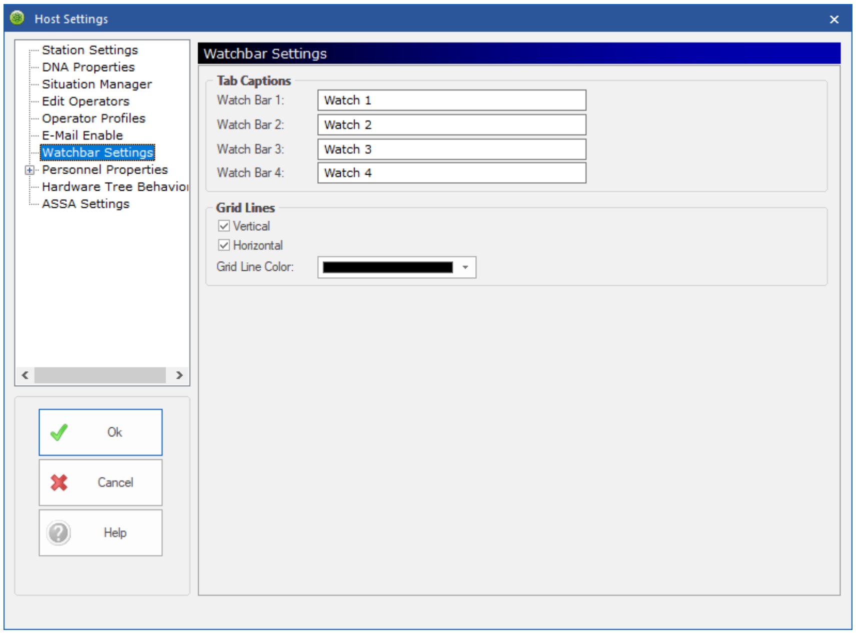
E-Mail Address:

Time Schedule: TS 001: Always

Send on Flagged: ● None ○ Watch ○ Alarm ○ Both

Watchbar Settings

The Watchbar Settings dialog is used to configure the Watch Windows. See Chapter 15 for more information.



Tab Captions

Watch Bar 1: Watch 1

Watch Bar 2: Watch 2

Watch Bar 3: Watch 3

Watch Bar 4: Watch 4

Grid Lines

☑ Vertical

☑ Horizontal

Grid Line Color: ■

Tab Captions

- Watch Bar 1 - Caption for Tab 1 on the Watch Window.
- Watch Bar 2 - Caption for Tab 2 on the Watch Window.
- Watch Bar 3 - Caption for Tab 3 on the Watch Window.
- Watch Bar 4 - Caption for Tab 4 on the Watch Window.

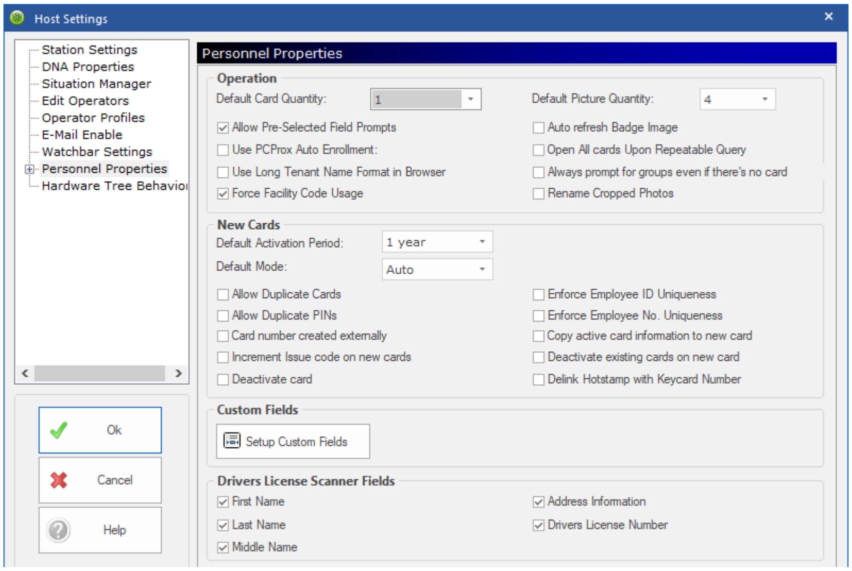
Grid Lines

- Vertical - Displays vertical grid lines in the Watch Window.
- Horizontal - Displays horizontal grid lines in the Watch Window.
- Grid Line Color - Determines the color of the grid lines in the Watch Window.

NOTES:

Personnel Properties

The Personnel Properties dialog is used to configure properties for cardholders, personnel records, ID badges, objects in the Personnel Browser, and tenants (if applicable).



Host Settings

- Station Settings
- DNA Properties
- Situation Manager
- Edit Operators
- Operator Profiles
- E-Mail Enable
- Watchbar Settings
- Personnel Properties
- Hardware Tree Behavio

Personnel Properties

Operation

Default Card Quantity: 1 | Default Picture Quantity: 4

☑ Allow Pre-Selected Field Prompts | □ Auto refresh Badge Image
□ Use PCProx Auto Enrollment: | □ Open All cards Upon Repeatable Query
□ Use Long Tenant Name Format in Browser | □ Always prompt for groups even if there's no card
☑ Force Facility Code Usage | □ Rename Cropped Photos

New Cards

Default Activation Period: 1 year
Default Mode: Auto

□ Allow Duplicate Cards | □ Enforce Employee ID Uniqueness
□ Allow Duplicate PINs | □ Enforce Employee No. Uniqueness
□ Card number created externally | □ Copy active card information to new card
□ Increment Issue code on new cards | □ Deactivate existing cards on new card
□ Deactivate card | □ Delink Hotstamp with Keycard Number

Custom Fields

Drivers License Scanner Fields

☑ First Name | ☑ Address Information
☑ Last Name | ☑ Drivers License Number
☑ Middle Name

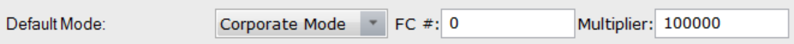
Operation

- Default Card Quantity - Determines the number of cards loaded to a new cardholder. (Default = 1)
- Default Picture Quantity - Determines the number of photos allowed per cardholder record. (Default = 4)
- Allow Pre-Selected Field Prompts - Allows the operator to create predefined text for some personnel fields. Fields are configured by right-clicking on the field and selecting Add Text. See page 7-8.
- Use PCProx Auto Enrollment - Select if a PCProx Enrollment Reader will be used to assign cards to a personnel record. The enrollment reader must be connected.
- Use Long Tenant Name Format in Browser - Extends the names of tenant objects in the Personnel Browser.
- Force Facility Code Usage - If selected, Card Number and Facility Code populate as required fields in the Personnel Record.
- Auto Refresh Badge Image - If selected, the Badge Template image in the ID Badging tab of the Personnel Record refreshes automatically.
- Open All Cards Upon Repeatable Query - If selected, and a personnel record is opened using a repeatable query for an individual card number, all of the cardholder's Card tabs will appear in the record. See page 7-31 for more information on repeatable queries.
- Always prompt for groups even if there's no card - If selected, DNA Fusion will prompt the operator to add the cardholder to a personnel group even if the cardholder does not have a card.
- Rename Cropped Photos - If selected, automatically saves cropped photos under a new file name.

New Cards

- Default Activation Period - Sets the default activation period for new cards. (Default = 1 year)
- Default Mode - Sets the default Mode for new cards. The default Auto mode uses the controller-stored card formats.

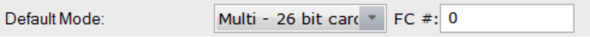
  If Corporate Mode is selected, **enter** the facility code (FC#) and the Multiplier.

  Default Mode: Corporate Mode FC #: 0 Multiplier: 100000

  The Corporate Mode allows the system to have multiple facility codes under one card format (per bit structure). When the card format for the Corporate Mode is created, ensure that the Card ID Offset matches the multiplier set up in the Personnel Properties. See page 8-81 for more information on configuring card formats, and see page 7-11 for more information on cardholders. [Example: Multiplier * FC# + Card# = Credential >> 1,000,000,000 x 6 = 6,000,000,000 + 449,166,208 = 6,449,166,208]

  If Multi - X bit card is selected, **enter** the Facility Code for the desired card format.

  Default Mode: Multi - 26 bit carc FC #: 0
- Allow Duplicate Cards - Check to allow duplicate card numbers.
- Allow Duplicate PINs - Check to allow duplicate PIN numbers between cardholders.
- Card Number Created Externally - Check to prevent operators from manually assigning a card number to a new card. The card number is read from the database.

- Increment Issue Code on New Cards - If the Issue Code function is used, select this option to automatically increase the Issue Code by one digit when a new card is issued. See page 8-53 for details.
- Deactivate Card - If checked, all new cards are automatically deactivated when added to the Personnel Record. The Activate checkbox must be selected before the card will grant access. See page 7-12 for more information on activating cards.
- Enforce Employee ID Uniqueness - Check to disable duplicate Employee ID entries in the Personnel Record.
- Enforce Employee No. Uniqueness - Check to disable duplicate Employee No. entries in the Personnel Record.
- Copy Active Card Information to New Card - When selected, access level information from the original card will be automatically copied to the new card upon Update. See page 7-16 for more information.
- Deactivate Existing Cards on New Card - If checked, and a new card is added to a personnel record, the existing card(s) will be automatically disabled upon Update. See page 7-21 for more information.
- Delink Hotstamp with Keycard Number - If selected, the Card and Hot Stamp fields will have separate values.

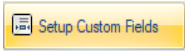
Custom Fields

If the Custom Personnel option on the Station Settings dialog is set to 1 to 1 Linkage (Legacy), the Custom Fields must be configured before saving the information in a personnel record.

> ! *The* Custom Fields Quantity *must be specified on all client workstations in order to view the* Custom Fields*.*

- Setup Custom Fields - Opens the Personnel Custom Fields Setup dialog to configure custom fields.

Personnel Custom Fields Setup

1. **Select** the Setup Custom Fields button. 

   The Personnel Custom Fields Setup dialog opens.

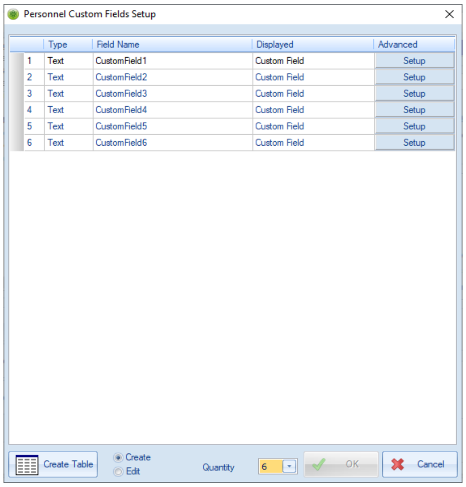
- Create - Allows the creation of a new custom fields table.
- Edit - Allow edits to custom field table.

2. **Click** the Quantity drop-down menu to set the desired amount of fields (Max. of 49 fields).

- Quantity - Determines the number of custom fields that appear in the Personnel Custom Fields Setup.

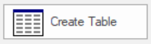
3. Configure the fields in the dialog

- Type - **Select** the type of field (text, numeric, etc.).
- Field Name - Database field name.
- Displayed - Label that appears in the Personnel Record.
- Advanced Setup - Opens the Advanced Properties dialog.



	Type	Field Name	Displayed	Advanced
1	Text	CustomField1	Custom Field	Setup
2	Text	CustomField2	Custom Field	Setup
3	Text	CustomField3	Custom Field	Setup
4	Text	CustomField4	Custom Field	Setup
5	Text	CustomField5	Custom Field	Setup
6	Text	CustomField6	Custom Field	Setup

● Create
○ Edit
Quantity 6

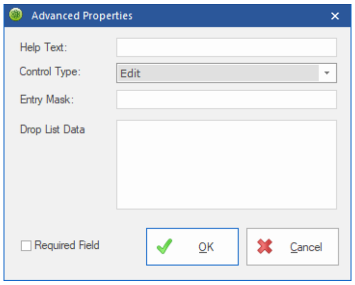
4. **Click** on the Create Table button. 

- Create Table - Must click to create the table in the database. Failure to do so will result in an error when closing a personnel record. (Behind-the-scenes operation)

> *It is important to create a unique name for each field. The* Field Name *and* Displayed Name *do not have to be identical, but it is recommended that they bear some relationship to each other. The* Field Name *is limited to 32 characters without punctuation or spaces. The* Displayed Name *does not have these restrictions.*

Advanced Properties

- Help Text - Context-sensitive help text that displays when the cursor hovers over the field.
- Control Type - Determines the field type:
  - □ Edit - Allows the operator to enter and/or edit original text in the field. Max. 50 characters.
  - □ Drop List - Allows the operator to select a predefined option from a drop-down menu. Drop-down items are configured in the Drop List Data field.
  - □ ComboBox - Allows the operator to enter original text or select a predefined option from a drop-down menu. Drop-down items are configured in the Drop List Data field.
- Entry Mask - A text mask that appears over Edit field types to specify a template, e.g. SSN: ###-##-#### or Phone: ###-###-####.



Help Text:
Control Type: Edit
Entry Mask:
Drop List Data
□ Required Field

- Drop List Data - List of items for either the Drop List or ComboBox field. (Hint: **type** an item and **press** Ctrl+Enter to go to the next line.)
- Required Field - If checked, designates a required field.

Drivers License Scanner Fields

This section determines the fields that will be imported when a driver's license is scanned into the DNA Fusion system; check all that apply. See page 7-3 for more information.

NOTES:

Photo Recall

The Photo Recall dialog sets the parameters for the Photo Recall windows. See page 7-43 for more information.

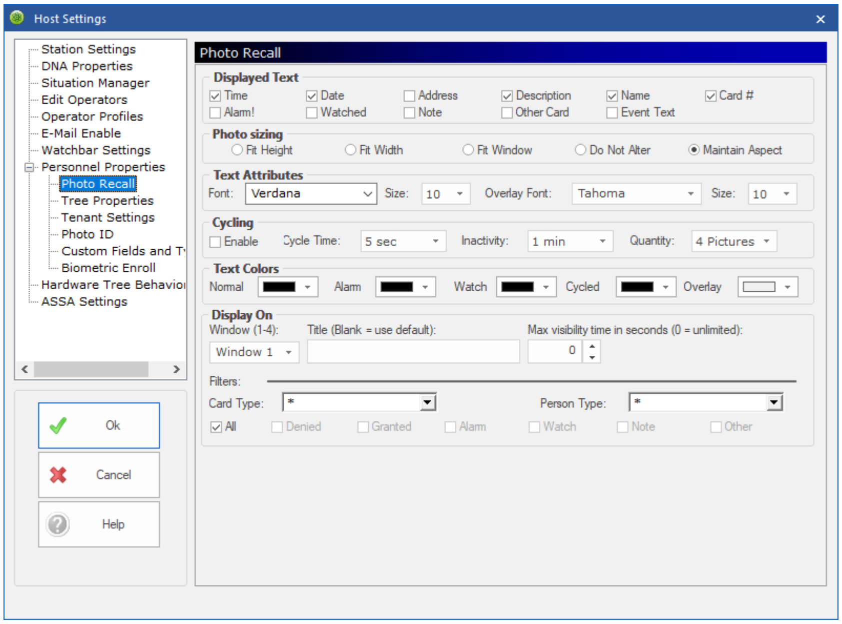


Photo Recall

Displayed Text
☑ Time ☑ Date □ Address ☑ Description ☑ Name ☑ Card #
□ Alarm! □ Watched □ Note □ Other Card □ Event Text

Photo sizing
○ Fit Height ○ Fit Width ○ Fit Window ○ Do Not Alter ● Maintain Aspect

Text Attributes
Font: Verdana Size: 10 Overlay Font: Tahoma Size: 10

Cycling
□ Enable Cycle Time: 5 sec Inactivity: 1 min Quantity: 4 Pictures

Text Colors
Normal ■ Alarm ■ Watch ■ Cycled ■ Overlay □

Display On
Window (1-4): Window 1
Title (Blank = use default):
Max visibility time in seconds (0 = unlimited): 0

Filters:
Card Type: * Person Type: *
☑ All □ Denied □ Granted □ Alarm □ Watch □ Note □ Other

Displayed Text

- Time - Displays the event time with the photo.
- Date - Displays the event date with the photo.
- Address - Displays the door/elevator address with the photo.
- Description - Displays the door/elevator description with the photo.
- Name - Displays the cardholder's name with the photo.
- Card # - Displays the card number with the photo.
- Alarm! - If an Alarm Card Flag was set, Alarm! Card will be displayed. Any associated data will be displayed along with the photo.
- Watched - If a Watch Card Flag was set, Watched Card will be displayed. Any associated data will be displayed along with the photo.
- Note - If a Note Card Flag was set, Note will be displayed. Any associated data will be displayed along with the photo.
- Other Card - If an Other... Card Flag was set, Other will be displayed. Any associated data will be displayed along with the photo.
- Event Text - Displays the event description in the Photo Recall window.

Photo Sizing

- Fit Height - Stretches the photo to fit the window's height; maintains aspect.
- Fit Width - Stretches the photo to fit the window's width; maintains aspect.
- Fit Window - Stretches picture to fit the window; may not maintain aspect.
- Do Not Alter - Retains the original size of the photo.
- Maintain Aspect - Fits height and width to closest match while maintaining aspect.

Text Attributes

- Font - Changes the displayed font.
- Font Size Size - Changes the font size.
- Overlay Font - Defines the font of the overlay text for items such as note text, personnel type, etc.
- Overlay Size - Changes the overlay font size.

Cycling

- Enable - If checked, cycles multiple photos in the Photo Recall window.
- Cycle Time - Sets the cycle time between photos. (Default = 5 sec.)
- Inactivity - The amount of time a cardholder’s photo will display in the recall window before resuming the photo cycle.
- Quantity - The number of photos in the cycle/rotation set.

Text Colors

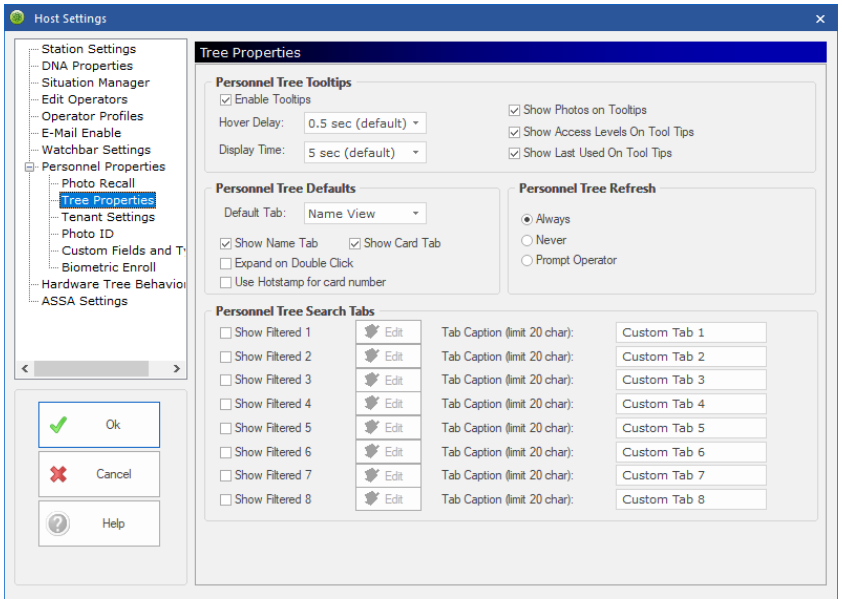
- Normal - Sets the text color for normal events.
- Alarm - Sets the text color for alarm events.
- Watch - Sets the text color for watch events.
- Cycled - Sets the text color for photo cycling.
- Overlay - Sets the color for any overlay text, such as note text, personnel type, etc.

Display On

- Window (1-4) - Applies the Display On settings to the selected window.
- Title - Enter a name for the window. (If blank, the window uses the default title.)
- Max visibility time in seconds - Enter the amount of time (in seconds) to display the last badged photo. The window will become blank after the set time expires. (0 = Unlimited)
- Filters - A condition must be selected for the system to display the designated photo(s).
  - □ Card Type - Displays photos for the designated card type.
  - □ Person Type - Displays photos for the designated personnel type.
  - □ All - Displays photos on all card reads.
  - □ Denied - Displays photos if access is denied.
  - □ Granted - Displays photos if access is granted.
  - □ Alarm - Displays photos on cards flagged as Alarm cards.
  - □ Watch - Displays photos on cards flagged as Watch cards.
  - □ Note - Displays photos on cards flagged as Note cards.
  - □ Other - Displays photos on cards flagged as Other cards.

Tree Properties

The Tree Properties dialog is used to set the tree properties in the Personnel Browser, such as tooltip options and search tabs for each workstation. These settings can also be accessed by right-click in the Personnel Browser and selecting Personnel Tree Properties.



Personnel Tree Tooltips

☑ Enable Tooltips

Hover Delay: 0.5 sec (default)

Display Time: 5 sec (default)

☑ Show Photos on Tooltips

☑ Show Access Levels On Tool Tips

☑ Show Last Used On Tool Tips

Personnel Tree Defaults

Default Tab: Name View

☑ Show Name Tab ☑ Show Card Tab

□ Expand on Double Click

□ Use Hotstamp for card number

Personnel Tree Refresh

● Always

○ Never

○ Prompt Operator

Personnel Tree Search Tabs

□ Show Filtered 1	Edit	Tab Caption (limit 20 char):	Custom Tab 1
□ Show Filtered 2	Edit	Tab Caption (limit 20 char):	Custom Tab 2
□ Show Filtered 3	Edit	Tab Caption (limit 20 char):	Custom Tab 3
□ Show Filtered 4	Edit	Tab Caption (limit 20 char):	Custom Tab 4
□ Show Filtered 5	Edit	Tab Caption (limit 20 char):	Custom Tab 5
□ Show Filtered 6	Edit	Tab Caption (limit 20 char):	Custom Tab 6
□ Show Filtered 7	Edit	Tab Caption (limit 20 char):	Custom Tab 7
□ Show Filtered 8	Edit	Tab Caption (limit 20 char):	Custom Tab 8

Personnel Tree Tooltips

- Enable Tooltips - If checked, enables tooltips for tree objects in the Personnel Browser.
- Hover Delay - Length of time the cursor must hover before the tooltip appears. (Default = 0.5 seconds)
- Display Time - Length of time the tooltip displays. (Default = 5 seconds)
- Show Photos on Tooltips - Displays the cardholder’s photo in the tooltip.
- Show Access Levels on Tooltips - Displays the card’s access level(s) in the card tooltip.
- Show Last Used on Tooltips - Displays the card's last used information (i.e., date, time, location, and event) in the card tooltip.

Personnel Tree Defaults

- Default Tab - Tab shown at start up: Name View or Card View.
- Show Name Tab - Displays the Name View tab.
- Show Card Tab - Displays the Card # View tab.
- Expand on Double Click - If selected, double-clicking on an employee or personnel group in the Personnel Browser will expand the tree instead of opening a new Personnel Record.
- Use Hotstamp for Card Number - If selected, the Hot Stamp number will be displayed as the card number in the Personnel Browser and Events Grid.

Personnel Tree Refresh

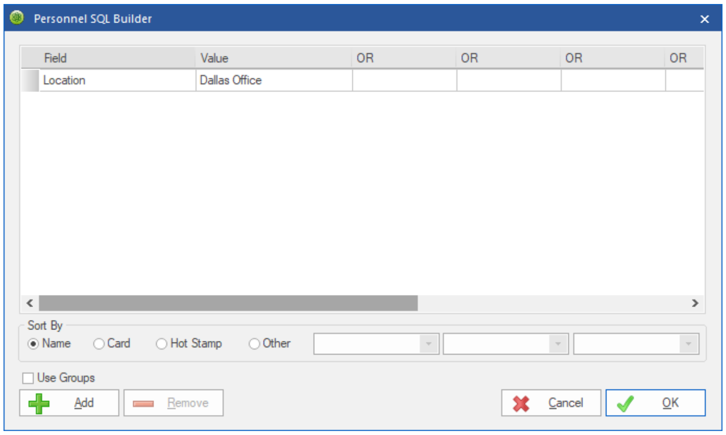
- Always - Refreshes the Personnel Browser automatically when an update is available.
- Never - Does not refresh the Personnel Browser automatically.
- Prompt Operator - Prompts the operator to refresh the Personnel Browser when an update is available.

Personnel Tree Search Tabs

- Show Filtered 1-8 - If checked, displays a custom tab with filtered search results in the Personnel Browser.
- Edit - Opens the Personnel SQL Builder dialog. See page 3-22 for more information.
- Tab Caption - Description for the custom tab. (Max. 20 characters)

Personnel SQL Builder

Allows the system administrator to build custom search tabs that automatically filter the Personnel Browser by the criteria set in the Personnel SQL Builder. See page 7-32 for more information.



Field	Value	OR	OR	OR	OR
Location	Dallas Office				

Sort By
● Name ○ Card ○ Hot Stamp ○ Other

□ Use Groups

Filters

- Field - Select the field type from the drop-down.
- Value - Enter the search criteria, or, if applicable, select a predefined field from the drop-down.
- OR - Enter the additional search criteria, or, if applicable, select a predefined field from the drop-down.

Sort By

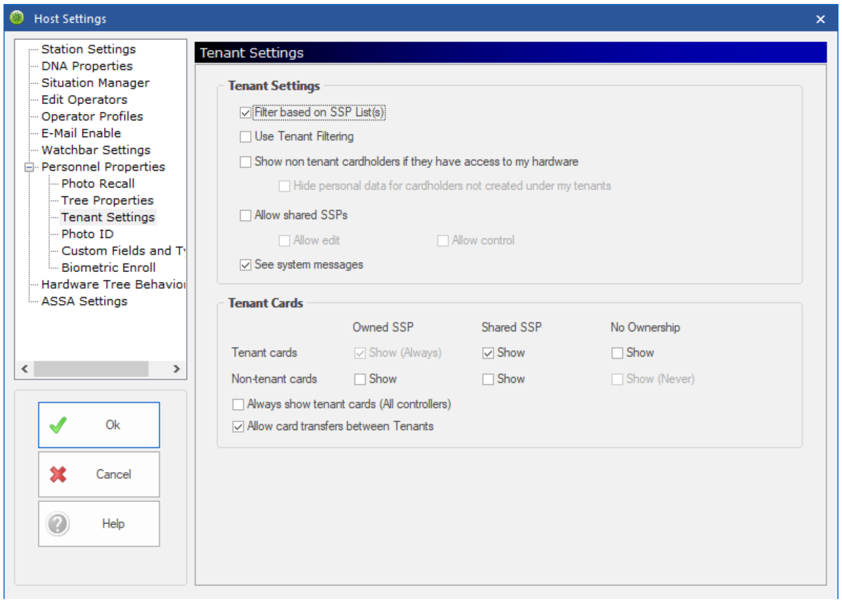
- Name - Sorts the browser tab by name.
- Card - Sorts the browser tab by card number.
- Hot Stamp - Sorts the browser tab by hot stamp number.
- Other - Select the browser tab sort criteria from the drop-down list(s).

Options

- Add - Adds another filter row to the grid.
- Remove - Removes the selected filter row from the grid.

Tenant Settings

The Tenants feature is used to visually separate SSP controllers and personnel. For more information, see Chapter 13.



Tenant Settings

Tenant Settings

☑ Filter based on SSP List(s)

☐ Use Tenant Filtering

☐ Show non tenant cardholders if they have access to my hardware

☐ Hide personal data for cardholders not created under my tenants

☐ Allow shared SSPs

☐ Allow edit ☐ Allow control

☑ See system messages

Tenant Cards

	Owned SSP	Shared SSP	No Ownership
Tenant cards	☑ Show (Always)	☑ Show	☐ Show
Non-tenant cards	☐ Show	☐ Show	☐ Show (Never)

☐ Always show tenant cards (All controllers)

☑ Allow card transfers between Tenants

> Enable Tenants (Segregation) *must be checked in the* DNA Properties *dialog to edit the* Tenant Settings*.*

- Filter based on SSP List(s) - Filter the events and hardware by SSP for the current tenant checked.
- Use Tenant Filtering - Check if Alarm Escalation and Event Routing will be used in combination with tenants. See page 14-31 for more information.
- Show non tenant cardholders if they have access to my hardware - Displays non-tenant activity in the Events Grid.
  - Hide personal data for cardholders not created under my tenants - Hides the cardholder's first and last names; only the card number will be visible.
- Allow Shared SSPs - Allows tenants to share SSP controllers. This allows the system owner to share SSPs and/or control of the SSPs with this client.
  - Allow Edit - Allows the operator to edit configurable settings on shared SSPs.
  - Allow Control - Allows the operator to control hardware on shared SSPs.
- See System Messages - Displays system messages for the operator on this workstation.
- Tenant Cards
  - Owned SSP: Show (Always) - Displays tenant cards on tenant SSPs. (Read-only; always enabled)
  - Shared SSP: Show - Displays tenant cards on shared SSPs.
  - No Ownership: Show - Displays tenant cards on SSPs other than tenants.
- Non-Tenant Cards
  - Owned SSP: Show - Displays non-tenant cards on tenant SSPs.
  - Shared SSP: Show - Displays non-tenant cards on shared SSPs.
  - No Ownership: Show (Never) - Displays non-tenant cards on SSPs other than tenants. (Read-only; always disabled)
- Always Show Tenant Cards (All Controllers) - Override button; enables all checkboxes on the Tenant Cards row regardless of their configuration.
- Allow Card Transfers between Tenants - Allows a card to be assigned to another tenant on the system.

NOTES:

Photo ID

The Photo ID dialog allows the operator to set the naming convention for photos taken at a badging station as well as configure additional Photo ID settings.

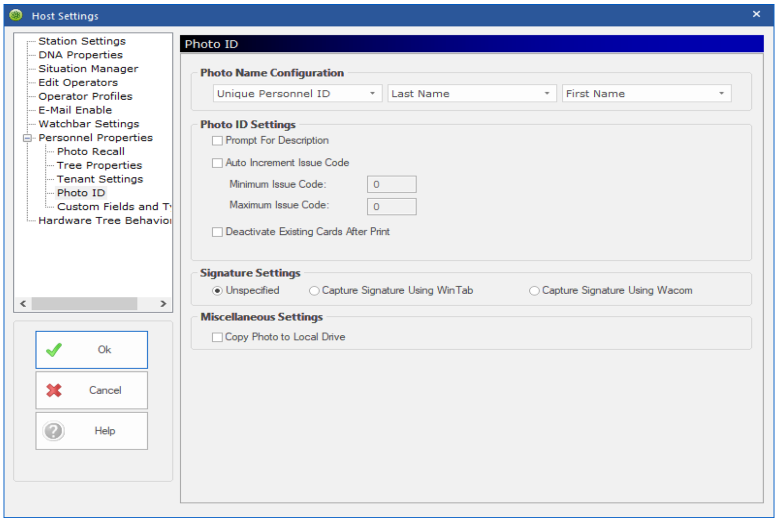


Photo ID

Photo Name Configuration

Unique Personnel ID | Last Name | First Name

Photo ID Settings

□ Prompt For Description

□ Auto Increment Issue Code

Minimum Issue Code: 0

Maximum Issue Code: 0

□ Deactivate Existing Cards After Print

Signature Settings

● Unspecified ○ Capture Signature Using WinTab ○ Capture Signature Using Wacom

Miscellaneous Settings

□ Copy Photo to Local Drive

Badging Station *must be checked in the* Station Settings *to view and manage the* Photo ID *dialog. If not, it will be hidden from the dialog menu.*

Photo Name Configuration

Select from the following drop-down options to configure the naming convention for photos:

- Date of Photo
- Employee Number
- First Name
- Last Name
- Time of Photo
- Unique Personnel ID
- Employee ID

Photo ID Settings

- Prompt for Description - Prompts the operator to enter a description for the photo.
- Auto Increment Issue Code - If the Store Issue Codes checkbox is selected in the Controller Properties / Stored Quantities dialog (see page 8-53), selecting this option will automatically increase the Issue Code by one digit when a new badge is printed. This feature requires the badge template to reference the Keycards_IssueCode database field in the Badge Designer. See page 21-8 for more information.
  - Minimum Issue Code - Sets the minimum accepted Issue Code.
  - Maximum Issue Code - Sets the maximum accepted Issue Code.
- Deactivate Existing Cards After Print - Automatically deactivates any existing cards associated with the cardholder's record after printing a new badge.

Signature Settings

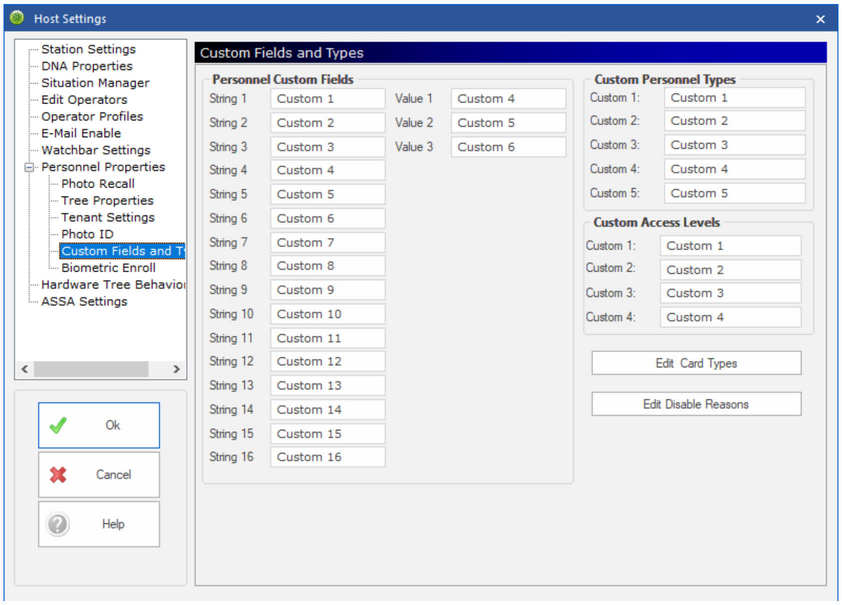
- Capture signature using WinTab - Select to use a WinTab interface to capture signatures. The WinTab driver must be installed.
- Capture Signature using Wacom - Select to use a Wacom interface to capture signatures. The Wacom driver must be installed.

Miscellaneous Settings

- Copy Photo to Local Drive - Saves a copy of the photo in the local drive (C:).

Custom Fields and Types

The Custom Fields and Types dialog is used to configure the custom text fields that appear in the Personnel Record, as well as the custom fields for personnel types, card types, access levels, and disable reasons.



Custom Fields and Types

Personnel Custom Fields			
String 1	Custom 1	Value 1	Custom 4
String 2	Custom 2	Value 2	Custom 5
String 3	Custom 3	Value 3	Custom 6
String 4	Custom 4		
String 5	Custom 5		
String 6	Custom 6		
String 7	Custom 7		
String 8	Custom 8		
String 9	Custom 9		
String 10	Custom 10		
String 11	Custom 11		
String 12	Custom 12		
String 13	Custom 13		
String 14	Custom 14		
String 15	Custom 15		
String 16	Custom 16		

Custom Personnel Types	
Custom 1:	Custom 1
Custom 2:	Custom 2
Custom 3:	Custom 3
Custom 4:	Custom 4
Custom 5:	Custom 5

Custom Access Levels	
Custom 1:	Custom 1
Custom 2:	Custom 2
Custom 3:	Custom 3
Custom 4:	Custom 4

Personnel Custom Fields

- Custom String 1-16 - Label for custom text fields in the DNA Custom Fields section of the Personnel Record.
- Custom Value 1-3 - Label for custom value fields in the DNA Custom Fields section of the Personnel Record.

Custom Personnel Types

- Custom 1-5 - Label for custom personnel categories. Appears as a list item in the Type drop-down menu, which is located in the Employee Info tab of the Personnel Record.

Custom Access Levels

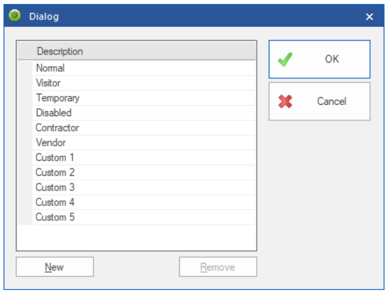
- Custom 1-4 - Label for custom access level groups or categories. Appears as a list item in the Access Level Category drop-down menu of the Access Levels Maintenance Dialog. See page 6-5.

Edit Card Types

The Edit Card Types dialog is used to define up to 255 custom Card Types.

1. **Select** the Edit Card Types button.
2. **Click** the New button.

   The <New Card Type> field appears.
3. **Enter** a name for the Card Type.
4. **Click** OK to save the settings.



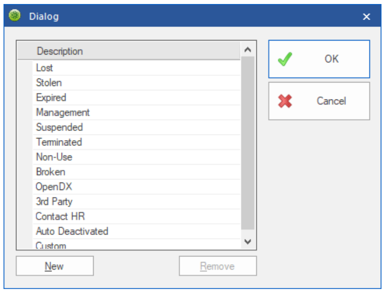
Description
Normal
Visitor
Temporary
Disabled
Contractor
Vendor
Custom 1
Custom 2
Custom 3
Custom 4
Custom 5

Edit Disable Reasons

The Edit Disable Reasons dialog is used to define up to 255 custom Disable Reasons.

1. **Select** the Edit Disable Reasons button.
2. **Click** the New button.

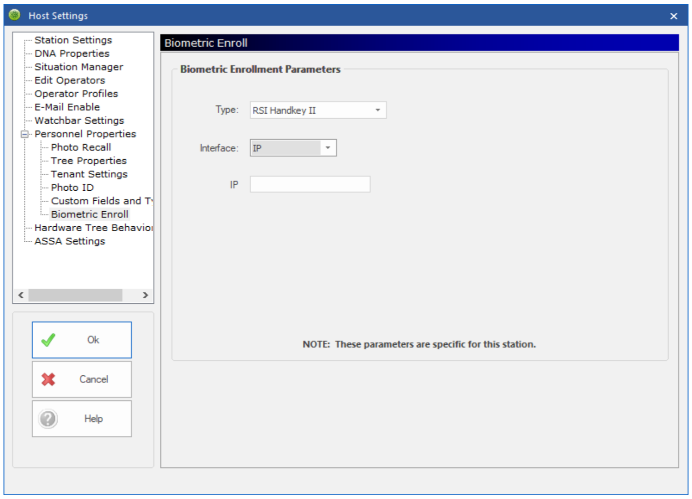
   The <New Disable Reason> field appears.
3. **Enter** a name for the Disable Reason.
4. **Click** OK to save the settings.



Description
Lost
Stolen
Expired
Management
Suspended
Terminated
Non-Use
Broken
OpenDX
3rd Party
Contact HR
Auto Deactivated
Custom

Biometric Enroll

The Biometric Enroll dialog sets the parameters for RSI and Bioscrypt biometric enrollment devices. The site must be licensed for the biometric device and the installation must be complete before the option becomes visible. The parameters are specific to the workstation.



Biometric Enroll

Biometric Enrollment Parameters

Type: RSI Handkey II

Interface: IP

IP

NOTE: These parameters are specific for this station.

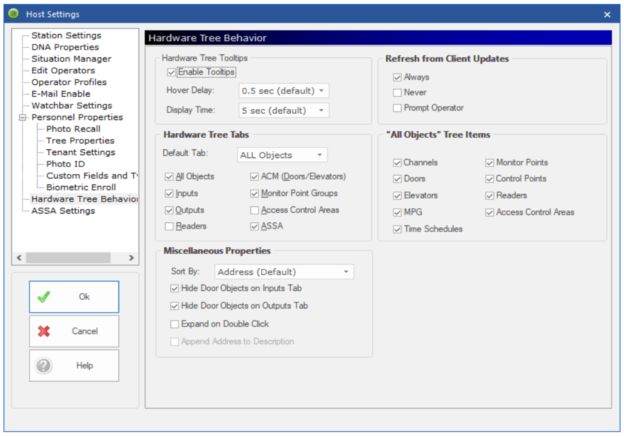
Biometric Enrollment Parameters

- Type - **Select** the type of biometric enrollment reader.
- Interface - **Select** the type of reader connection: IP or Serial. The remaining parameters change depending on the selection.
  - ☐ IP - Enter the IP address. (IP)
  - ☐ COM Port - Select the reader's serial port. (Serial)
  - ☐ Baud Rate - Select the communication baud rate; the default rate is 9600. (Serial)
  - ☐ Device ID - Enter the reader's identification number. (Serial; Bioscrypt only)

> ⓘ For more information on the Biometric Enroll, see the Biometric Manual.

Hardware Tree Behavior

The Hardware Tree Behavior dialog is used to configure the Hardware Tree. These settings can also be accessed by right-clicking in the Hardware Browser and selecting Tree Properties.



Hardware Tree Behavior

Hardware Tree Tooltips

☑ Enable Tooltips

Hover Delay: 0.5 sec (default)

Display Time: 5 sec (default)

Refresh from Client Updates

☑ Always

☐ Never

☐ Prompt Operator

Hardware Tree Tabs

Default Tab: ALL Objects

☑ All Objects ☑ ACM (Doors/Elevators)

☑ Inputs ☑ Monitor Point Groups

☑ Outputs ☐ Access Control Areas

☐ Readers ☑ ASSA

"All Objects" Tree Items

☑ Channels ☑ Monitor Points

☑ Doors ☑ Control Points

☑ Elevators ☑ Readers

☑ MPG ☑ Access Control Areas

☑ Time Schedules

Miscellaneous Properties

Sort By: Address (Default)

☑ Hide Door Objects on Inputs Tab

☑ Hide Door Objects on Outputs Tab

☐ Expand on Double Click

☐ Append Address to Description

Hardware Tree Tooltips

- Enable Tooltips - If checked, enables tooltips for tree objects in the Hardware Browser.
- Hover Delay - Length of time the cursor must hover to display the tooltip. (Default = 0.5 seconds)
- Display Time - Length of time the tooltip will display. (Default = 5 seconds)

Hardware Tree Tabs

- Default Tab - Sets the default active tab.
- All Objects - If selected, displays the All Objects tab on the Hardware Browser.
- Inputs - If selected, displays the Inputs tab on the Hardware Browser.
- Outputs - If selected, displays the Outputs tab on the Hardware Browser.
- Readers - If selected, displays the Readers tab on the Hardware Browser.
- ACM (Doors/Elevators) - If selected, displays the ACM tab on the Hardware Browser.
- Monitor Point Groups - If selected, displays the MPGs tab on the Hardware Browser.
- ASSA - Only available if licensed for ASSA integration. Displays the ASSA tab on the Hardware Browser.
- Access Control Areas - If selected, displays the Access Control Areas tab on the Hardware Browser.

"All Objects" Tree Items

Determines the hardware tree objects that will be visible in the ALL Objects tab of the Hardware Browser.

- Channels - If selected, displays Channels in the ALL Objects tree.
- Doors - If selected, Doors will be displayed in the ALL Objects tree.
- Elevators - If selected, displays Elevators in the ALL Objects tree.
- MPG - If selected, MPGs will be included in the ALL Objects tree.
- Time Schedules - If selected, Time Schedules will be displayed in the ALL Objects tree.
- Monitor Points - If selected, displays Monitor Points in the ALL Objects tree.
- Control Points - If selected, displays Control Points in the ALL Objects tree.
- Readers - If selected, displays Readers in the ALL Objects tree.
- Access Control Areas - If selected, Access Control Areas will be included in the ALL Objects tree.

Refresh from Client Updates

- Always - Refreshes the Hardware Browser automatically when an update is available.
- Never - Does not refresh the Hardware Browser automatically.
- Prompt Operator - Prompts the operator to refresh the Hardware Browser when an update is available.

Miscellaneous Properties

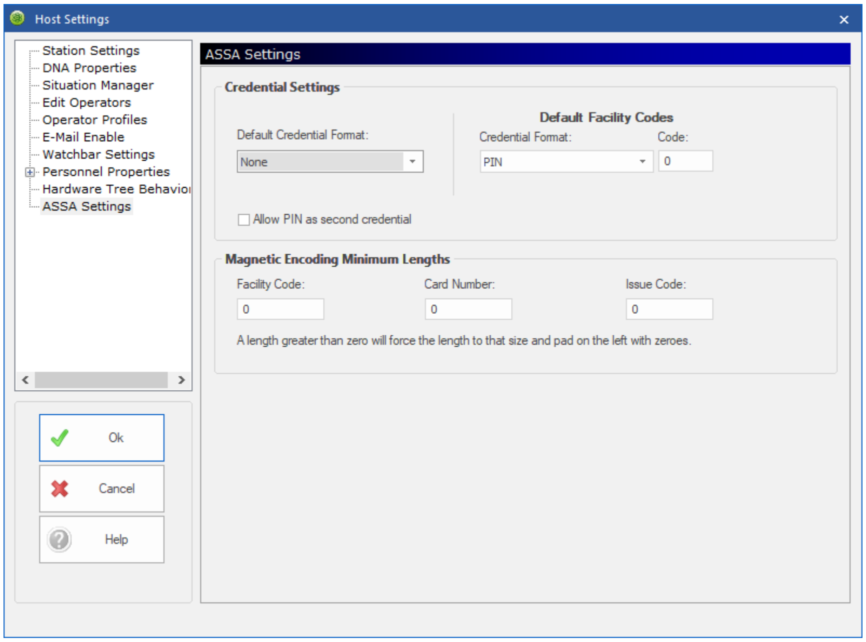
- Sort By - Defines the sort order of the Hardware Tree. Drop-down options include:
  - Address (Default) - Sorts hardware objects by address in ascending order.
  - Address -DESCENDING - Sorts hardware objects by address in descending order.
  - Description - Sorts hardware objects by description in ascending alphabetical order.
  - Description -DESCENDING - Sorts hardware objects by description in descending alphabetical order.

> If Description or Description (DESCENDING) is selected, the address will disappear from the hardware object in the Hardware Browser. To include the address, select Append Address to Description.

- Hide Door Objects on Inputs Tab - Hides input objects on the Inputs tab if they are associated with a door.
- Hide Door Objects on Outputs Tab -Hides output objects on the Outputs tab if they are associated with a door.
- Expand on Double Click - If selected, double-clicking on a hardware object will expand the tree instead of opening the Properties for the hardware object.
- Append Address to Description - Only available if the Sort By drop-down is set to Description or Description -DESCENDING. If selected, the address for each hardware object appears at the end of the description.

ASSA Settings

The ASSA Settings dialog is only available if the site is licensed for ASSA doors.



ASSA Settings

Credential Settings

Default Credential Format: None

Default Facility Codes

Credential Format: PIN Code: 0

□ Allow PIN as second credential

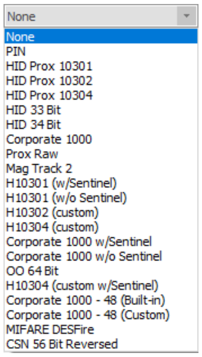
Magnetic Encoding Minimum Lengths

Facility Code: 0 Card Number: 0 Issue Code: 0

A length greater than zero will force the length to that size and pad on the left with zeroes.

Credential Settings

- Default Credential Format - Select the credential format from the drop-down list.
- Default Facility Codes - Select the Credential Format from the drop down-list and enter the Facility Code for each selected credential type.
- Allow PIN as second credential - If checked, allows the cardholder to use a PIN number as his/her second credential.



None
None
PIN
HID Prox 10301
HID Prox 10302
HID Prox 10304
HID 33 Bit
HID 34 Bit
Corporate 1000
Prox Raw
Mag Track 2
H10301 (w/Sentinel)
H10301 (w/o Sentinel)
H10302 (custom)
H10304 (custom)
Corporate 1000 w/Sentinel
Corporate 1000 w/o Sentinel
OO 64 Bit
H10304 (custom w/Sentinel)
Corporate 1000 - 48 (Built-in)
Corporate 1000 - 48 (Custom)
MIFARE DESFire
CSN 56 Bit Reversed

Magnetic Encoding Minimum Lengths

Any entry greater than zero will force the encoding to match the specified length and pad the remaining characters with zeros.

- Facility - Enter the minimum length for the Facility Code.
- Card - Enter the minimum length for the Card Number.
- Issue - Enter the minimum length for the Issue Code.

This Page Intentionally Left Blank

Operators 4

In This Chapter

System operators generally manage and monitor the DNA Fusion access control software under different roles. As a result, the operators must be limited to the specific tasks they will perform. Operators can also be imported with the Active Directory (AD) Sync plugin and automatically assigned a profile with the appropriate settings.

DNA Fusion is designed to accommodate a range of application permissions via operator levels, passwords, and operator privileges. This chapter will explain how to add and modify system operators, configure operator profiles, and assign privileges to those operators.

Configuring Operators

Adding an Operator

1. **Select** DNA / Administrative / Operator Maintenance / Operator Privileges from the Main Menu.

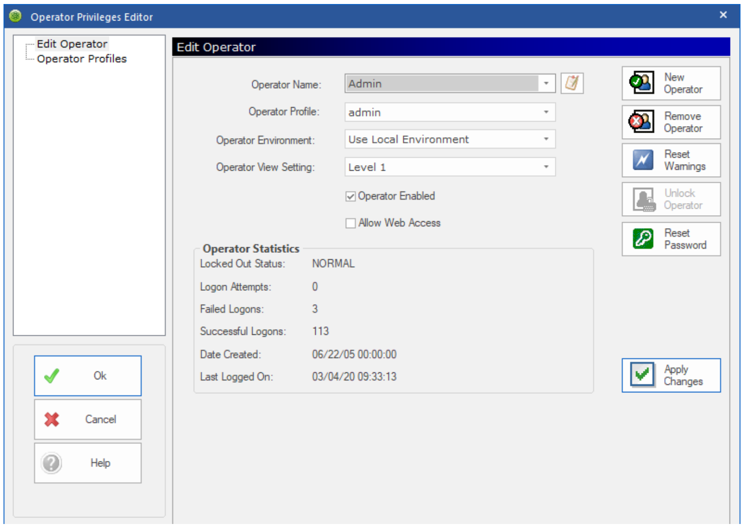
   OR

   Open the Operator Browser and **double-click** on the Operators header.

   See page 4-23 for instructions on opening the Operators Browser.

   The Operator Privileges Editor opens on the Edit Operator screen.

> *The* Edit Operator *dialog can also be accessed by clicking the* DNA Properties *button on the* Standard Toolbar *and selecting* Edit Operators *from the dialog menu.*



Operator Name: Admin
Operator Profile: admin
Operator Environment: Use Local Environment
Operator View Setting: Level 1
☑ Operator Enabled
☐ Allow Web Access

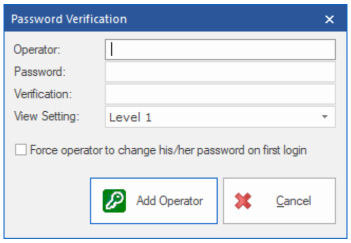
Operator Statistics
Locked Out Status: NORMAL
Logon Attempts: 0
Failed Logons: 3
Successful Logons: 113
Date Created: 06/22/05 00:00:00
Last Logged On: 03/04/20 09:33:13

This Page Intentionally Left Blank

2. **Click** the New Operator button.

   The Password Verification dialog opens.

   If Use Strong Passwords is checked in the DNA Properties dialog, the Password Verification screen will also display the required parameters.



Password Verification

Operator:

Password:

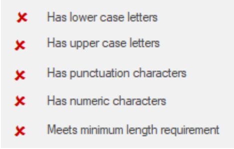
Verification:

View Setting: Level 1

☐ Force operator to change his/her password on first login

3. **Enter** a name for the Operator.
4. **Enter** a Password.

   If Use Strong Passwords is checked, the password must contain a lowercase letter, an uppercase letter, a punctuation character, a numeric character, and must meet the minimum 8-character length requirement. To enable the Strong Password option, see page 3-5.



✗ Has lower case letters

✗ Has upper case letters

✗ Has punctuation characters

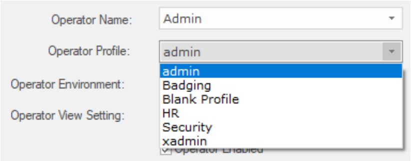
✗ Has numeric characters

✗ Meets minimum length requirement

5. **Re-enter** the password in the Verification field.
6. If desired, **check** Force operator to change his/her password on first login.
7. **Click** the Add Operator button.

   The operator is added to the Operator Name drop-down list.
8. **Select** an Operator Profile to assign to the selected operator.

   The profile determines the operator's privileges in DNA Fusion.



Operator Name: Admin

Operator Profile: admin

Operator Environment:

Operator View Setting:

9. **Select** the Operator Environment from the drop-down list.

   The Operator Environment is the operator's default application view in DNA Fusion. If any setting other than Use Local Environment is selected, the view will be pulled from the database. See page 4-21 for information on configuring Operator Environments.
10. If Use Local Environment was selected in the Operator Environment field, **select** the Operator View Setting from the drop-down list.

    The Operator View Setting is stored in the local registry and refers to the setting that will be displayed when the selected operator logs in. See page 4-21 for more information.
11. **Click** Apply Changes or OK to save the changes.

> **!** **Click** Apply Changes *before selecting a new operator or operator profile or all changes will be lost.*

Adding a Note

1. **Click** on the note icon next to the Operator Name drop-down menu.

   The Notes dialog allows operators or admins to write notes for a selected operator in the drop-down menu.
2. **Click** Ok to save the note.

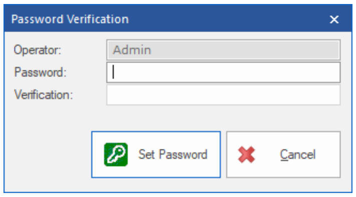
Removing an Operator

1. In the Edit Operators dialog, **select** the Operator Name from the drop-down.
2. **Click** the Remove Operator button.
3. **Click** Yes to confirm.

Changing an Operator's Password

1. In the Edit Operators dialog, **select** the Operator Name.
2. **Click** the Reset Password button.

   The Password Verification dialog appears.
3. **Enter** the new password and **click** Set Password.
4. **Click** Yes to confirm.



Password Verification

Operator: Admin

Password:

Verification:

> *An operator can also change his/her password by* selecting File / Set Password *from the* Main Menu*; this action only applies to the active operator.*

Configuring Operator Profiles

The DNA administrator has the authority to assign privileges and operator levels for all operators. These parameters determine what the operator can view, manage, and control.

Adding a Profile

1. **Select** DNA / Administrative / Operator Maintenance / Operator Privileges from the Main Menu.

   OR

   Open the Operators Browser and **double-click** on the Operators header.

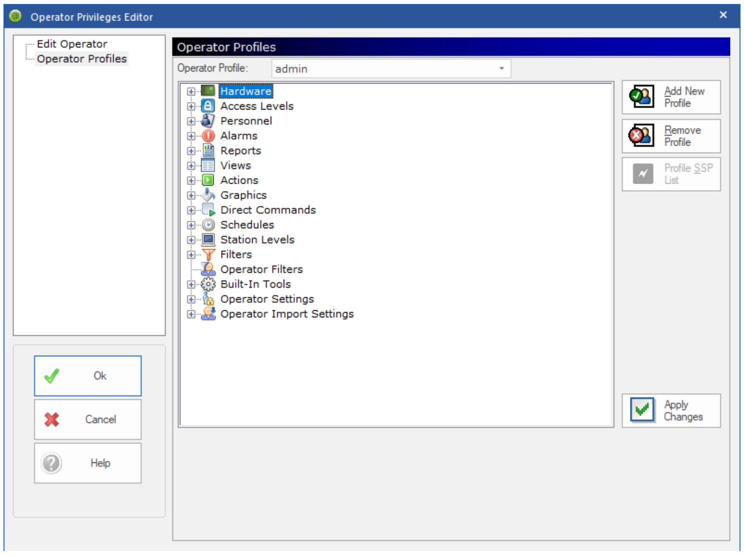
   See page 4-23 for instructions on opening the Operator Browser.

   The Operator Privileges Editor opens on the Edit Operator dialog.

> *The* Edit Operator *dialog can also be accessed by clicking the* DNA Properties *button on the* Standard Toolbar *and selecting* Edit Operators *from the dialog menu.*

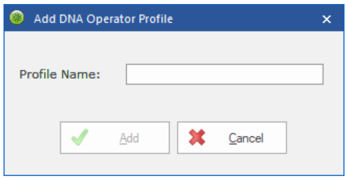
2. **Select** Operator Profiles from the dialog menu.

   The Operator Profiles dialog appears.



3. **Click** the Add New Profile button.

   The Add DNA Operator Profile dialog appears.



4. **Enter** a Profile Name and **click** Add.

   The Operator Profile is added to the drop-down list.

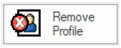
5. **Configure** the profile.

   See page 4-7 for information on configuring profiles.

> *Operator configuration is an administrative task reserved for DNA administrators. Use caution when configuring operator levels that affect the administrator profile to avoid being locked out of the system entirely. For this reason, Open Options recommends that changes NOT be made to the administrator profile.*

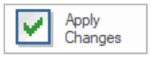
Removing a Profile

An operator profile can be removed if it is not assigned to any operators.

1. **Open** the Operator Privileges Editor dialog.
2. **Select** Operator Profiles from the dialog menu.
3. **Select** the Operator Profile from the drop-down list.
4. **Click** the Remove Profile button. 

   The Operator Profile is removed from the list.

Editing a Profile

1. **Open** the Operator Privileges Editor dialog.
2. **Select** Operator Profiles from the dialog menu.
3. **Select** the Operator Profile from the drop-down list.
4. **Edit** the profile.
5. **Click** the Apply Changes button to save the changes. 

> ! **Click** Apply Changes *before selecting a new operator or operator profile or all changes will be lost.*

> ⓘ *If an operator is logged in when a profile is changed, the changes will take effect the next time the operator logs in to DNA Fusion.*

Configuring a Profile

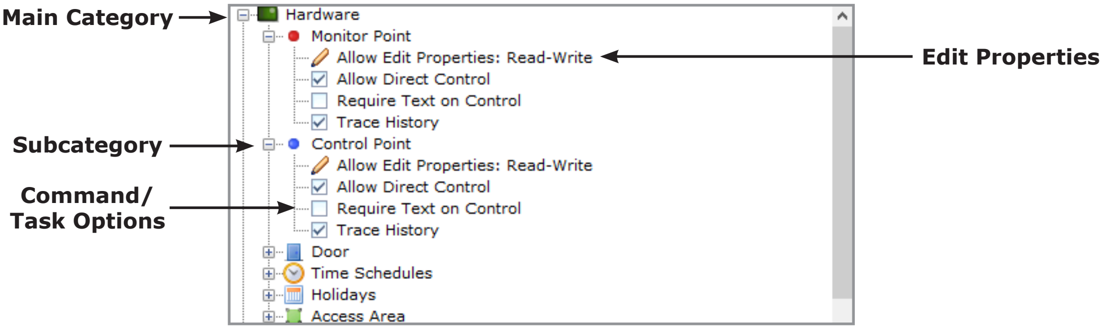
1. **Open** the Operator Profile dialog as described on page 4-5.
2. **Select** the desired Operator Profile from the drop-down list.
3. **Expand** each item in the menu and **configure** the profile's specific privileges.

   There are 2 pieces to each category: Edit Properties and Tasks or Commands

   See page 4-9 for an explanation of each operator privilege.

   The Privileges section allows the administrator to configure the various operator permissions to determine what actions the operator can and cannot perform within the system.

   The Privileges section consists of main categories and subcategories. Each item in the privileges tree has an Edit Properties option as well as various command/task options. If a command/task is checked, it is applied to any operator with the selected operator profile.

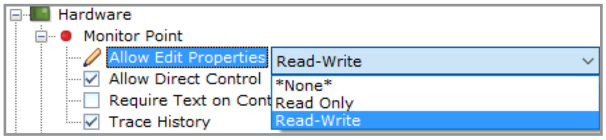


- Hardware
  - Monitor Point
    - Allow Edit Properties: Read-Write
    - ☑ Allow Direct Control
    - □ Require Text on Control
    - ☑ Trace History
  - Control Point
    - Allow Edit Properties: Read-Write
    - ☑ Allow Direct Control
    - □ Require Text on Control
    - ☑ Trace History
  - Door
  - Time Schedules
  - Holidays
  - Access Area

To configure the operator privileges, use one of the following methods:

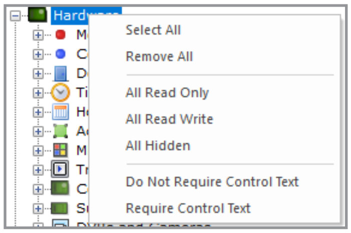
- **Check** individual commands/tasks and/or **select** an option from the Edit Properties drop-down:

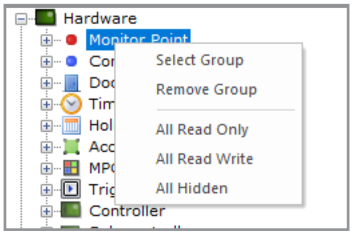
Edit Properties	
None	Restricts the operator from editing the object's properties.
Read Only	Allows the operator to view, but not edit, the object's properties.
Read-Write	Allows the operator to view and edit the object's properties.



- Hardware
  - Monitor Point
    - Allow Edit Properties: Read-Write
    - ☑ Allow Direct Control
    - □ Require Text on Cont
    - ☑ Trace History

- **Right-click** on a main category or subcategory and **select** an option from the context menu:



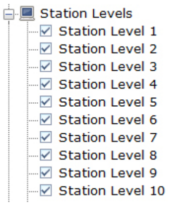


Options	
Select All / Select Group	Checks all privileges in the category/subcategory.
Remove All / Remove Group	Unchecks all privileges in the category/subcategory.
All Read Only	Sets all Edit Properties in the category/subcategory to Read Only.
All Read Write	Sets all Edit Properties in the category/subcategory to Read-Write.
All Hidden	Sets all Edit Properties in the category/subcategory to None.
Do Not Require Control Text	Unchecks Require Text on Control for all hardware objects; see page 4-9.
Require Control Text	Checks Require Text on Control for all hardware objects; see page 4-9.

4. **Expand** the Station Levels category and **select** the Station Levels for this operator.

   The DNA administrator has the authority to assign station levels to each Operator Profile. This setting determines which workstations the operator can use.

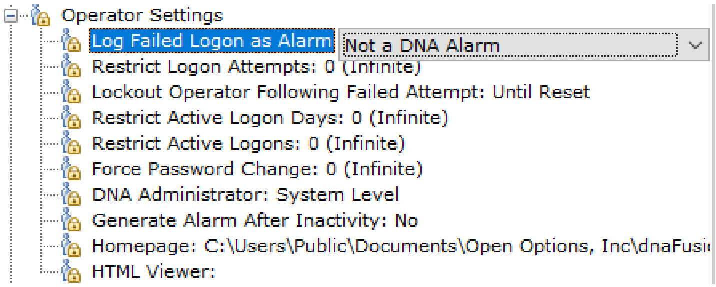
   If checked, the operator will be authorized to use any workstations configured with the station level. The DNA Station Level field in the Station Settings dialog determines the workstation's level. See page 3-3 for more information.



Station Levels
- ☑ Station Level 1
- ☑ Station Level 2
- ☑ Station Level 3
- ☑ Station Level 4
- ☑ Station Level 5
- ☑ Station Level 6
- ☑ Station Level 7
- ☑ Station Level 8
- ☑ Station Level 9
- ☑ Station Level 10

5. **Expand** the Operator Settings category and **select** a setting to configure its parameters.

   See page 4-18 for a description of each setting.



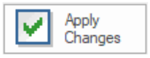
Operator Settings
- Log Failed Logon as Alarm: Not a DNA Alarm
- Restrict Logon Attempts: 0 (Infinite)
- Lockout Operator Following Failed Attempt: Until Reset
- Restrict Active Logon Days: 0 (Infinite)
- Restrict Active Logons: 0 (Infinite)
- Force Password Change: 0 (Infinite)
- DNA Administrator: System Level
- Generate Alarm After Inactivity: No
- Homepage: C:\Users\Public\Documents\Open Options, Inc\dnaFusi
- HTML Viewer:

The DNA Administrator *setting determines the administrative capabilities of the operator. Anyone designated as an administrator can add operators, configure operator profiles, and access* DNA Properties*.*

The options for administrator levels are:

- None - Operator only; no administrator privileges or capabilities.
- System Level - Can assign and edit any profile level (System, Regional, or Local).
- Regional Level - Can assign and edit Regional and Local Level profiles.
- Local Level - Can assign and edit Local Level profiles.

6. **Click** Apply Changes or OK to save the configuration.



Click Apply Changes *before selecting a new operator profile or all changes will be lost.*

If an operator is logged in when a profile is changed, the changes will take effect the next time the operator logs into DNA.

Operator Privileges

The following tables describe the various operator tasks or commands that can be configured for each profile. Privileges determine what actions the operator can perform in DNA Fusion. See the page numbers referenced in parentheses for additional information on some items.

Hardware

Many of the hardware objects have the same operator privileges. For more information on hardware, see Chapter 8: Hardware.

Subcategory	**Privileges**
Monitor Point (Input)	● Allow Direct Control - Control the hardware object. (8-23) ● Require Text on Control - Require the operator to enter audit text when executing a direct control command. ● Trace History - Run a trace history report for the object. (8-26)
Control Point (Output)	Same as Monitor Point.
Door (All Levels) * **Note:** Security Levels are configured in the Door Properties.	● Door Alerts - Configure door alerts. (8-40) ● Create/Modify/Remove Door Subgroup - Create, modify, and/or remove door subgroups in the ACM tab of the Hardware Browser. ● View Door Subgroup Report - Generate a Who Has Access report for a Door Subgroup. ● Door: Forced Arm - Arm or disarm the Forced option. (8-8) ● Door: Held Arm - Arm or disarm the Held option. (8-8) ● Door: Temporary Unlock - Initiate a Momentary Unlock command. (8-8) ● Door: Set Door Mode - Change the Door Mode (locked, unlocked, etc.). (8-5) ● Require Text on Control - Same as Monitor Point. ● Allow Precision Assignment - Assign precision access levels. (7-19) ● Trace History - Run a trace history report for the door/elevator. (8-19) ● Allow Door Follows Schedule Assignment - Configure the Door Follows Schedule feature. (8-11)
Time Schedules	Same as Monitor Point. (Chapter 5) Allows the operator to configure time schedules as well as Time Schedule Sets.
Holidays	Allows the operator to configure holidays as well as Holiday Sets. (Read-Write, Read Only, None) (5-11)
Access Area	Same as Monitor Point. (Chapter 11)
MPG (Monitor Point Group)	Same as Monitor Point. (Chapter 12)
Triggers & Macros	Same as Monitor Point. (Chapter 10)
Controller	● Reset Hardware - Reset the controller. (8-34) ● Connect - Connect the controller to the site. (8-34) ● Disconnect - Disconnect the controller from the site. (8-34) ● Reload Firmware - Download firmware to the controller. (8-34) ● Set Controller Time - Set the controller's time. (8-34) ● Require Text on Control - Same as Monitor Point. ● Calculate Memory - Calculate the SSP controller's memory. (8-53) ● Card Formats - Create and edit card formats. (8-83) ● Remove Controller - Delete controllers. (8-35) ● Download Configuration - Download hardware settings to the controller(s). (2-15) ● Web Login - Ability to log into the controller from the web page.
Subcontroller	● Remove Subcontroller - Delete subcontrollers. (8-37)

Subcategory	Privileges
DVRs and Cameras	● View Live Video - View live video in the Video View Manager. (8-45) ● View Archived Video - View archived video footage from the Events or Alarm Grid. ● Record Video - Record video on DVR server. (8-44) ● Allow PTZ Control - Control PTZ (pan, tilt, and zoom) cameras in the Video View Manager. (8-46) ● Allow Export Video and Email - Export video and send as e-mail attachment.
Miscellaneous	● Edit Site - Edit the hardware site(s). (8-49) ● Edit Channel - Edit the hardware channel(s). (8-50)
Universal Driver	● Allow Direct Control - Control universal drivers. ● Require Text on Control - Same as Monitor Point. ● UD Level - Specify the UD security level.
ASSA Specific Only applies to ASSA locks. See the DNA Integration Manual for more information on the ASSA integration.	● Replace Serial - Replace an ASSA lock's serial number. ● Confirm Door - Confirm an ASSA door within the DNA Fusion system. ● Reset Access Point - Reset an ASSA lock. ● Re-Load Provisioning Data - Reload the provisioned lock data. ● Initialize Device - Initialize an ASSA lock. ● Pulse/Lock/Unlock - Pulse, lock, or unlock an ASSA lock. ● Lockdown/Remove LockDown - Set the ASSA locks to lockdown mode. ● Add DSR - Add a door service router (DSR) to DNA Fusion. ● Force Changes to DSR - Force changes to the DSR. ● Load New Access Points - Load new ASSA locks. ● Add Access Mode - Set a lock access mode, e.g. PIN code, remote control, fingerprint, etc.
Stentofon	● Add Node - Allows the operator to add Stentofon nodes ● Edit Node - Edit a node within the DNA Fusion system. ● Delete Node - Delete the node from the system. ● Add Station - Add and configure Stentofon stations. ● Edit Station - Edit the station within the DNA Fusion system. ● Delete Station - Delete the station from the system. ● Make Call - Operator can initiate a Stentofon call. ● Answer Call - Answer a call within the DNA Fusion system. ● Cancel Call - Cancel a Stentofon call from DNA Fusion.

Subcategory	Privileges
ThyssenKrupp	● Add Group - Create ThyssenKrupp groups within the system. ● Remove Group - Remove an elevator group. ● Edit Group - Edit an existing group. ● Add Floor - Add ThyssenKrupp floors to DNA Fusion. ● Remove Floor - Remove a floor within the DNA Fusion system. ● Edit Floor - Edit an existing elevator floor. ● Add Floor Group - Allows the operator to create floor groups. ● Remove Floor Group - Deletes an existing floor group. ● Edit Floor Group - Edit a ThyssenKrupp floor group. ● Control Floors - Provides the operator the ability to control elevator floors. ● Add Kiosk - Create a ThyssenKrupp kiosk. ● Remove Kiosk - Delete a kiosk. ● Edit Kiosk - Edit an existing ThyssenKrupp kiosk. ● Link Door to Kiosk - Link the door to the ThyssenKrupp kiosk.
Isonas Doors	● Confirm Doors - Allows the operator to confirm Isonas doors. ● Upload Firmware - Update the Isonas controller firmware. ● Enroll BLE Credentials - Enroll Bluetooth® Low Energy (BLE) credentials.
Bosch Panels	● Discover Panel - Discover Bosch panels in the DNA Fusion system. ● Add Panel - Add Bosch panels to the DNA Fusion system. ● Delete Panel - Delete an existing Bosch panel. ● Edit Panel - Edit the properties of a Bosch panel. ● Edit Area - Edit a Bosch area within the DNA Fusion system. ● Edit Point - Edit a Bosch point within the DNA Fusion system. ● Edit Output - Edit a Bosch output within the DNA Fusion system. ● Arm Area - Provides the ability to arm a Bosch area. ● Disarm Area - Provides the ability to disarm a Bosch area. ● Bypass Point - Allows the operator to Bypass a Bosch point within the DNA Fusion system. ● Unbypass Point - Allows the operator to Unbypass a Bosch point within the DNA Fusion system. ● Activate Output - Provides the ability to activate Bosch outputs. ● Deactivate Output - Provides the ability to deactivate Bosch outputs. ● Add Authority Level Group - Create Bosch authority level groups. ● Remove Authority Level Group - Delete Bosch authority level groups. ● Add/Remove User - Add and remove Bosch users. ● Allow Passcode Editing - Permit editing of Bosch passcodes. ● Download Panel Users - Provides the ability to download Bosch panel users. ● Silence Bells - Authority to silence all Bosch panel bells.

Subcategory	Privileges
Kone	• Add Group - Create Kone groups within the system. • Remove Group - Remove an elevator group. • Edit Group - Edit an existing group. • Add Floor - Add Kone floors to DNA Fusion. • Remove Floor - Remove a floor within the DNA Fusion system. • Edit Floor - Edit an existing elevator floor. • Add Floor Group - Allows the operator to create floor groups. • Remove Floor Group - Deletes an existing floor group. • Edit Floor Group - Edit a Kone floor group. • Control Floors - Provides the operator the ability to control elevator floors. • Add DOP - Create a Kone DOP. • Remove DOP - Delete a DOP. • Edit DOP - Edit an existing Kone DOP. • Link Door to DOP - Link the door to the Kone DOP.
EngageIP	• Add Site - Create EngageIP site within the DNA Fusion system. • Remove Site - Remove an EngageIP site. • Edit Site - Edit an existing site. • Edit Gateway - Edit EngageIP gateway in DNA Fusion. • Edit Door - Edit a EngageIP doors within the DNA Fusion system. • Unlink All Doors - Allows the operator to unlock all EngageIP doors.
Schindler Elevator	• Edit Schindler Settings - Edit Schindler elevator settings with DNA Fusion. • Maintain Master Groups - Edit Schindler elevator master groups. • Info Ready - Allows reporting through right-clicking.

Access Levels

For more information on access levels, see Chapter 6: Access Levels.

Privileges
• Assign Access Level - Assign normal access levels.* • Assign High Security Access Level - Assign high security access levels.* • Assign Medium Security Access Level - Assign medium security access levels.* • Assign Low Security Access Level - Assign low security access levels.* • Assign Access Level (Custom 1-4) - Assign custom security access levels.* For more information on custom access levels, see page 3-26. * **Note:** If an operator is given permission to assign access levels, their operator profile must also contain Read-Write permission for the Access Levels option located under Personnel / Card Fields. • Add or Edit Access Level Groups - Add or edit access level groups. • View Access Level Groups - View access level groups in the Access Levels Browser. • Force Drag and Drop Confirmation on Access Level (Normal, High, Med, Low and Custom 1-4) - A confirmation dialog will appear when operators drag and drop an access level to a cardholder or card, regardless of the Do NOT tell me again setting. (7-14) • Allow Adding Cross Tenant Cardholders to Global Access Level - Add cardholders that belong to multiple tenant groups to a global access level. • Show Cardholder Name on Cross Tenant Access Level - View a cardholder's name next to access levels that are assigned to multiple tenants.

Personnel

For more information on personnel, see Chapter 7: Personnel.

Subcategory	Privileges
Personnel Actions	• Add Cardholder - Add personnel records. (7-3) • Remove Cardholder - Delete personnel records. (7-5) • Add Card - Add a card to a personnel record. (7-5) • Remove Card - Delete a card from a personnel record. (7-5) • Deactivate Card - Deactivate a card. (7-6) • Set Card Use Limit - Set the use limit on a card. (7-37) • Issue Free Pass - Issue a free anti-passback pass. (7-37) • Set Card Flags - Set card flags, e.g. Alarm Card or Watch Card. (7-35) • Download Personnel - Download personnel data to the controller(s). • Trace History - Run a trace history report for the selected card/cardholder. (7-35) • Add or Edit Personnel Group - Add or edit personnel groups. (7-24) • Add Cardholder to Personnel Group - Add cardholders to personnel groups. (7-25) • Allow Remove All Access - Remove all access levels from a card via right-click options in the Personnel Record or Personnel Browser. (7-21) • Allow Biometric Enrollment - Enroll cardholders through a biometric reader.(3-24) • Allow Removal of Biometric Templates - Erase biometric templates. (3-24) • Allow Has Access To - Run a has access to report for the selected card/cardholder. • Allow Non Tenant Hardware on Cardholder Trace History - Non tenant hardware will appear on trace history reports.
Personnel View (Tabs)	• Card # View - Access the Card # View tab on the Personnel Browser. • Name View - Access the Name View tab on the Personnel Browser. • Custom Tab 1-8 - Access Custom tabs on the Personnel Browser. (3-21)
Personnel Fields	This item contains all of the fields that are located on the Employee Info & Employee Info (Page 2) tabs of the Personnel Record. Items can be set to Read-Write, Read Only or None. • Location, Department, Site, Title - If selected, the operator will have the ability to configure the drop-down list for the field(s).
Personnel Custom Fields	This item contains all the fields that are located on the Custom Fields tab of the Personnel Record. Items can be set to Read-Write, Read Only or None. (3-17).
Card Fields	This item contains all the fields that are located on the Card tab of the Personnel Record. Items can be set to Read-Write, Read Only or None. (7-11)
Personnel Types	View cardholders with the selected Personnel Type. (7-1)
Assign Personnel Types	Assign the selected Personnel Type to cardholders. (7-7)
Card Types	View cardholders with the selected Card Type. • Extended - Add new Card Types as well as Disable Reasons. See page 3-26 for more information.
Assign Card Types	Assign the selected Card Type to cards. (7-11)
Photo Badging	• Photo Badging - Access the ID Badging tab in the Personnel Record; requires badging station. (21-21) • View Badge - View the badge on the ID Badging tab. (Photo Badging privilege must be checked.) (21-26) • Take Photo - Take a photo within DNA. (21-25)

Subcategory	Privileges
Photo Badging	● Add Photo - Import photos to the ID Badging tab. (7-41) ● Print Badge - Print a badge. (21-26) ● Remove Photo - Remove photos from a Personnel Record. ● View Photos - View cardholder photos.
Advanced Custom Settings	● Use Custom XML Permissions - If the Custom Personnel Permissions feature is used, check the Custom XML option to enable the feature for the selected profile. See page 4-16 for information. ● Perform Advanced Access Level Check - This option allows system administrators to enforce business rules to the assignment of access levels by calling a SQL-stored procedure named sp_DNA_AuthorizedAccess, which returns a true (-1) or false (0) value. If a true value is returned, the access level will be assigned to the card. If a false value is returned, a dialog will appear stating that the access level was not assigned. Contact Open Options Technical Support for more information. ● Use CardType for Deactivation Date - Allows the operator to define a deactivation date specific to a designated card type. This option is defined by a setting in the DNASettings table. Currently, a user interface to configure this option is not available. Contact Open Options Technical Support for more information.

Alarms

For more information on alarms, see Chapter 14: Events & Alarms.

Privileges
● Acknowledge All - Acknowledge all alarms in the Alarm Grid. ● Bring DnaFusion to Front on Alarm Grid - Enables the operator to access the Alarm Grid To Front dialog in the Alarm Grid Settings. (14-21) ● Clear All Alarms - Clear all alarms on the Alarm Grid that have returned to normal. ● Clear Selected Alarms - Clear the selected alarms on the Alarm Grid that have returned to normal.

Subcategory	Privileges
Allow Acknowledge	Priority: 1-15 - Acknowledge alarms with the specified priority levels. (14-24)
Require Dispatch Text	Priority: 1-15 - Requires the operator to enter dispatch text when an alarm is cleared or dismissed. (14-25)
Allow Dismiss Alarm	Priority: 1-15 - Dismiss alarms with the specified priority levels. (Dismissing an alarm does not require the alarm to return to the normal state.) (14-21)

Reports

For more information on reports, see Chapter 17: Reports.

Subcategory	Privileges
Access	If selected, allows the operator to run Access Reports.
Alarms	If selected, allows the operator to run Alarms Reports.
Events	If selected, allows the operator to run Events Reports.
Hardware Settings	If selected, allows the operator to run Hardware Settings Reports.
Personnel	If selected, allows the operator to run Personnel Reports.
Restored Archive Data	If selected, allows the operator to run Restored Archive Data Reports.
System	If selected, allows the operator to run System Reports.
Custom	If selected, allows the operator to run, add, and edit Custom Reports.

Views

If an operator has permission to perform a task but does not have the appropriate view privilege, he/she will not have access to the task's browser or window. For more information on views, see Chapter 2.

Privileges

- Access Areas - View the Access Areas option in the Hardware Tree (11-1).
- Alarms - Open the Alarm Grid (14-15).
- Access Levels - Open the Access Levels Browser (6-5).
- Events Manager - Open the Events Grid (14-5).
- Hardware Manager - Open the Hardware Browser (8-1).
- HTML Viewer - Open the HTML Viewer (16-1).
- Operators - Open the Operator Browser (4-23).
- Personnel - Open the Personnel Browser (7-1).
- Photo Recall - Open Photo Recall windows (7-43).
- Text Messaging - Open the Operator Messaging explorer. (4-23).
- IP Video 1 - Open the Video View Manager (8-45).
- Time Schedules - Open the Time Schedules Browser (5-1).
- Triggers and Macros - Permits the operator to open the Triggers & Macros Browser (10-1).
- Watch - Open the Watch Window (15-1).

Actions

The Actions category contains miscellaneous actions that were not included in previous sections.

Privileges

- Add to Watch - Add objects to the Watch Window (15-3).
- Remove From Watch - Remove objects from the Watch Window (15-3).
- Archive Profiles - Archive data (20-5).
- Restore Data - Restore archived data (20-6).
- Batch Processing - Complete batch processing tasks (20-14).
- Customize - Customize the application (2-9).
- Edit HTML Views - Add/edit the HTML Viewer (16-3).
- Actions E-Mail - Send e-mails from the Events or Alarm Grids. (14-8)
- Filter Events - Filter the Events Grid (14-5).
- Station Configuration - Administrative Function: DNA/Administrative
- Allow Do Not Ask Again - Select the Do Not Ask Again option on dialogs.
- Allow Do Not Show Again - Select the Do Not Show Again option on dialogs.
- Allow Situation Severe - Change the Situation Level Manager to Severe. (9-1)
- Allow Situation High - Change the Situation Level Manager to High. (9-1)
- Allow Situation Elevated - Change the Situation Level Manager to Elevated. (9-1)
- Allow Situation Guarded - Change the Situation Level Manager to Guarded. (9-1)
- Allow Situation Low - Change the Situation Level Manager to Low. (9-1)

Graphics

For more information on graphics, see Chapter 18: Graphic Maps.

Options

- Show Graphics - View normal graphic objects.
- Edit Graphics - Edit graphic maps.
- Arm All on Page - Arm all hardware objects on a graphics map.
- Disarm All on Page - Disarm all hardware objects on a graphics map.
- Acknowledges All on Page - Acknowledge all alarms on a graphics map.
- Allow Design - Edit a graphic map in Design Mode.

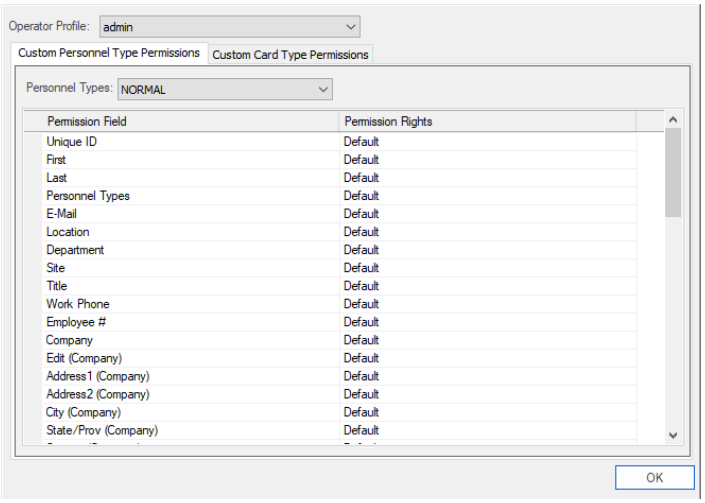
Custom Personnel Permissions

The Custom Personnel Permissions dialog allows the system administrator to configure permission rights for individual fields in the Personnel Record based on individual Personnel Types and Card Types. The permission rights apply to any operator with the designated operator profile.

> *If* Custom Personnel Permissions *are used, verify that* Use Custom XML Permissions *is selected for the operator profile. See page 4-14 for information.*

1. **Select** DNA / Administrative / Setup Custom Personnel Permissions from the Main Menu.

   The Custom Personnel Permissions dialog opens.



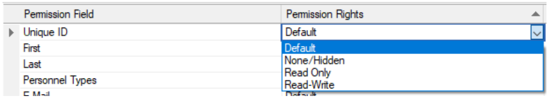
Operator Profile: admin

Custom Personnel Type Permissions
Custom Card Type Permissions

Personnel Types: NORMAL

Permission Field	Permission Rights
Unique ID	Default
First	Default
Last	Default
Personnel Types	Default
E-Mail	Default
Location	Default
Department	Default
Site	Default
Title	Default
Work Phone	Default
Employee #	Default
Company	Default
Edit (Company)	Default
Address1 (Company)	Default
Address2 (Company)	Default
City (Company)	Default
State/Prov (Company)	Default

2. **Select** an Operator Profile from the drop-down.
3. **Select** a Personnel Type from the drop-down.
4. **Select** the desired Permission Field and **click** the Permission Rights drop-down list.



Permission Field	Permission Rights
Unique ID	Default
First	
Last	
Personnel Types	

5. **Select** the Permission Right from the list.
   - None/Hidden - Hides the field so that the operator has no visibility.
   - Read Only - Allows the operator to view, but not edit, the field.
   - Read-Write - Allows the operator to view and edit the field. .
6. If desired, **select** a different Personnel Type and **repeat** steps 3 though 4.
7. If desired, **select** the Custom Card Type Permissions tab and **repeat** steps 3 through 6 for the desired Card Type(s).
8. **Click** OK to save the settings.

Direct Commands

For more information on direct commands, see page 8-29.

Options
• Manage Direct Commands - Add, edit, and remove direct commands in the User Commands Editor dialog.
• Require Text on Control - Require the operator to enter text before the command is executed.
• Execute - Execute a direct command in the Execute Direct Commands dialog.

Schedules

For more information on schedules, see Chapter 19: Scheduling.

Options
• Schedule Archives - Schedule archives.
• Schedule Batch Commands - Schedule batch files.
• Schedule Downloads - Schedule downloads.
• Schedule Reports - Schedule reports.

Tenants

Only available if Enable Tenants (Segregation) is checked in the DNA Properties dialog. For more information on tenants, see Chapter 13: Tenants.

Options
• Add Tenant - Add a new tenant.
• Remove Tenant - Remove a tenant.
• Tenants - View and generate reports for the specified tenant(s).

Station Levels

For more information on station levels, see page 4-8.

Options
• Station Levels 1-32 - Restrict operator access to the selected station levels.

Filters

For more information on event and alarm filters, see page 14-31.

Options
• Create Filters - Define event filters in the Filter Setup dialog.
• Assign Filters - Assign filters to hardware objects.

Operator Filters

For more information on filters, see page 14-31.

Options
If checked, the operator’s view will be limited to the selected filter.

Built-In Tools

Built-In Tools are applications available to use in DNA Fusion. For more information, see page 20-14.

Options

- Run Low Priority Tools - Allow the operator to use low level tools in Built-in Tools list. Low priority tools are marked green.
- Run Medium Priority Tools - Allow the operator to use medium level tools in Built-in Tools list. Medium priority tools are marked blue.
- Run High Priority Tools - Allow the operator to use high level tools in the Built-in Tools list. High priority tools are marked red.

Operator Settings

Operator settings are additional parameters applied to the operator profile. See page 4-8 for information.

Options

- Log Failed Logon as Alarm - Select the alarm priority from the drop-down list to generate an alarm if an operator fails to log on.
- Restrict Logon Attempts - Select the number of accepted login attempts before the operator is locked out.
- Lockout Operator Following Failed Attempt - If Restrict Logon Attempts is checked, select the length of the lockout period or select Until Reset to lock out the operator until an administrative reset.
- Restrict Active Logon Days - Restrict the number of logons by day (1-365 or infinite).
- Restrict Active Logons - Restricts the number of accepted logons (1-255 or infinite).
- Force Password Change - If set, prompts the operator to change their password after the specified number of days.
- DNA Administrator - Determines the operator's administrative level (system, regional, or local). See page 4-8 for details. Set to *None* to restrict access to all administrative functions, such as adding operators, configuring properties, performing system maintenance, etc.
- Generate Alarm After Inactivity - If set to Yes, generates an alarm when an operator is logged out from inactivity.
- Homepage - Designates a homepage file to open when an operator selects File / DNA Homepage from the Main Menu.
- HTML Viewer - Designates an HTML page to display when an operator selects File / HTML Viewer from the Main Menu.

Operator Import Settings

For more information on import settings, see page 4-19.

Options

- Active Directory Path - Imports the operators from the specified Active Directory group and automatically assigns the designated profile to the operators.

> **!** **Click** Apply Changes *before selecting a new operator or operator profile or all changes will be lost.*

Importing Operators

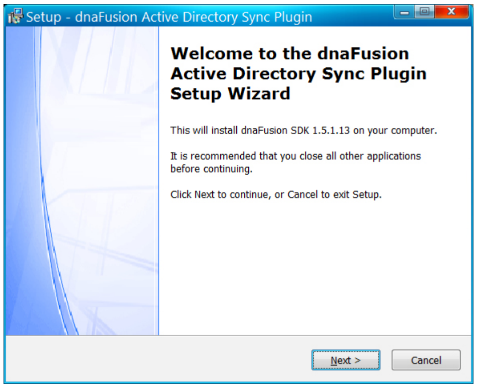
The Active Directory Sync plugin is used to import operators from Active Directory and automatically assign them a specific operator profile. An operator's account can also be disabled when an operator is removed from the Active Directory group.

Installing the AD Sync Plugin

Obtain the AD Sync plugin installation application from Open Options Technical Support.

1. **Double-click** the installation file to start the installation.

   The Welcome dialog appears.



Welcome to the dnaFusion Active Directory Sync Plugin Setup Wizard

This will install dnaFusion SDK 1.5.1.13 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

2. **Click** Next to begin the installation.

   The Ready to Install dialog opens.

3. **Click** Install.

   When the installation is complete, the Finished dialog appears.

4. **Click** Finish.

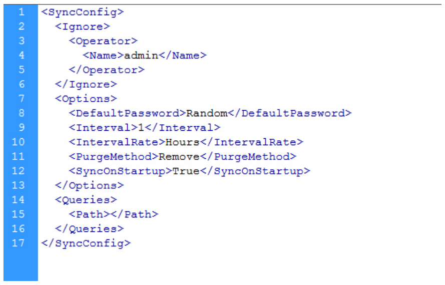
AD Sync Plugin Configuration

The AD Sync plugin is configured via the PluginADsync.config.Sample configuration file.

Default location:

- C:\Users \ Public \ Public Documents\ Open Options, Inc \ DNA Plugins

1. **Enter** the Active Directory path between the <Path> options.
2. If desired, **change** the other options.
3. **Save** the changes to the configuration file.



```
<SyncConfig>
  <Ignore>
    <Operator>
      <Name>admin</Name>
    </Operator>
  </Ignore>
  <Options>
    <DefaultPassword>Random</DefaultPassword>
    <Interval>1</Interval>
    <IntervalRate>Hours</IntervalRate>
    <PurgeMethod>Remove</PurgeMethod>
    <SyncOnStartup>True</SyncOnStartup>
  </Options>
  <Queries>
    <Path></Path>
  </Queries>
</SyncConfig>
```

Options

- Default Password - Determines how the default password will be set when operators are added.
  - □ Blank - Adds the operator without specifying a password.
  - □ Random - Adds the operator with a randomly generated 8-10 character password.
  - □ Static - Adds the operator and provides them with a static password. If this option is selected, insert a predefined password in the Static Password field.

> ❗ *Use caution when setting the* Default Password *to* Blank. *If the workstation does not use* NT Authentication, *operators will be able to sign in without a password. See page 3-5 for more information on NT Authentication.*

- Interval - Indicates the number of minutes or hours between synchronizations. Default is 1 hour
- Interval Rate - Determines the time frame that <Interval> represents. Default is hours.
  - □ Hours - Sets the Interval time to hours.
  - □ Minutes - Sets the Interval time to minutes.

- Purge Method - Specifies how operators will be purged when they are removed from the active directory group or no longer appear in active directory.
  - □ Disable - Deactivates the operator's account without removing the operator.
  - □ Remove - Deletes the operator from DNA Fusion.
- Static Password - Indicates the predefined password if Static is specified under the Default Password option.
- Sync On Startup
  - □ True - Sets the synchronization process to begin one (1) minute after the plugin starts.
  - □ False - Sets the synchronization process to start at the normal interval time.

Queries

- Path - Identifies the base LDAP path to search.
- Individual - Query string used to locate an individual record. Do NOT make changes to this string.
- Group - Query string used to retrieve all members of a particular group. Do NOT make changes to this string.
- Member Of - Query string used to identify if an individual is a member of a particular group. Do NOT make changes to this string.

Configure Import Settings

1. **Open** the Operators Privileges Editor.

   See page 4-6 for information on editing operator profiles.
2. **Select** Operator Profiles from the dialog menu.
3. **Expand** the Operator Import Settings option.
4. **Enter** the Active Directory Path where the desired operators reside.

   Example: CN=DNA Fusion Administrators,OU=DNA Fusion,OU=Domain Groups,DC=xxxxxx,DC=local
5. **Click** the Apply Changes button to save the changes or **click** OK to save the changes and close the dialog.

Configuring the Operator Environment

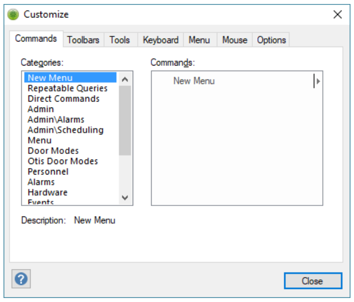
The DNA administrator can set up operator environments so that each Operator Profile has a different desktop view upon logging in to DNA Fusion.

DNA Fusion provides two options for configuring operator environments:

- Write the environment to the workstation's registry
- Pull the environment from the database

Local Registry

The operator must have permission to write to the workstation's local registry.



Description: New Menu

1. **Set** the Operator View Setting in the Edit Operator dialog.

   See page 4-3 for more information.

2. **Log in** to the workstation as the desired operator.

3. **Open** the Customize dialog and **configure** the desktop as desired.

   See Chapter 2 for more information on customizing DNA Fusion.

4. Exit DNA to save the new view settings.

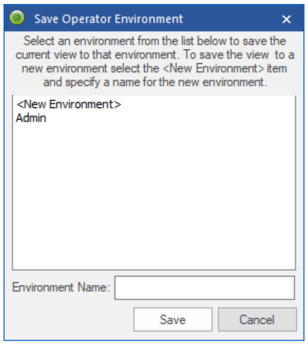
Database View

Configuring a New Environment

Environments can also be saved to the database and then assigned to an operator.

1. **Select** DNA / Administrative / Operator Maintenance / Save Operator Environment from the Main Menu.

   The Save Operator Environment dialog opens.

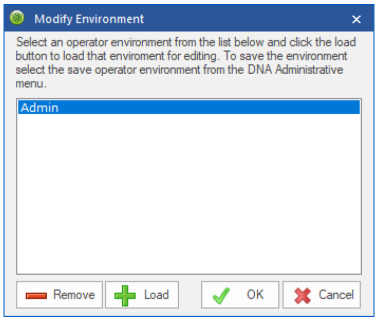


Select an environment from the list below to save the current view to that environment. To save the view to a new environment select the <New Environment> item and specify a name for the new environment.

2. **Select** the <New Environment> option, **enter** a name for the environment in the Environment Name field, and **click** the Save button.

3. **Select** DNA / Administrative / Operator Maintenance / Edit Operator Environment from the Main Menu.

   The Modify Environment dialog opens.



Select an operator environment from the list below and click the load button to load that enviroment for editing. To save the environment select the save operator environment from the DNA Administrative menu.

4. **Select** the desired operator environment and **click** the Load button. Load

   The selected operator environment is loaded to the workstation.

5. **Change** the DNA Fusion desktop to meet the operator's needs.

   Open the desired browsers, add and remove toolbar buttons, add and remove toolbars, open secondary toolbars, or create custom toolbars. See Chapter 2: Getting Started for more information on customizing the environment.

6. **Select** DNA / Administrative / Operator Maintenance / Save Operator Environment from the Main Menu.

   The Save Operator Environment dialog opens.

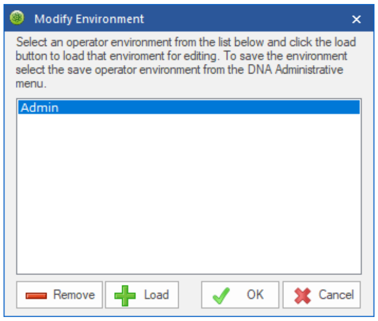
7. **Select** the desired Environment and **click** the Save button.

   The Operator Environment is saved and ready to be applied to an operator.

Modifying an Environment

1. **Select** DNA / Administrative / Operator Maintenance / Edit Operator Environment from the Main Menu.

   The Modify Environment dialog opens.



Modify Environment

Select an operator environment from the list below and click the load button to load that enviroment for editing. To save the environment select the save operator environment from the DNA Administrative menu.

Admin

2. **Select** the desired operator environment and **click** the Load button. Load

   The specified operator environment is loaded.

3. **Change** the DNA Fusion environment as needed.

   Open the desired browsers, add and remove toolbar buttons, add and remove toolbars, open secondary toolbars, or create custom toolbars. See Chapter 2: Getting Started for more information on customizing the environment.

4. **Select** DNA / Administrative / Operator Maintenance / Save Operator Environment from the Main Menu.

   The Save Operator Environment dialog opens.

5. **Select** the desired Environment and **click** the Save button.

   The Operator Environment is saved and changes will be applied to any operator assigned to the environment when they log in.

> ⓘ *If an operator is logged in when an environment is changed, the changes will take effect the next time the operator logs in to DNA.*

Operator Features

DNA Fusion offers a number of operator features through the Operators Browser.

Operators Browser

To open the Operators Browser:

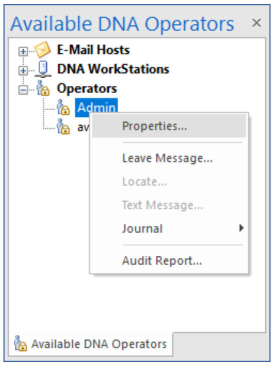
1. **Select** View / Explorers / Operators and Hosts from the Main Menu.

   The Operators Browser appears.

2. **Expand** the Operators header.

3. **Right-click** on the desired operator and **select** an option from the context menu:

   - Properties - Opens the Operator Privileges Editor dialog.
   - Leave Message - Opens the Message Waiting... dialog to leave a message for an operator. The message will be displayed when the operator logs in to the system.
   - Locate - Displays the station information for the selected operator (the operator must be logged in for this option to be available).
   - Text Message - Opens the Operator Messaging dialog to communicate with other operators.
   - Journal - Maintains a record of information from an operator in the DNA Journal.
   - Audit Report - Opens the Report Parameter Configuration dialog to run an Audit Report for the selected operator.



Leave Message

The Leave Message option allows the operator to leave a message for another operator who is not currently logged in to DNA Fusion. The message will be received immediately after he/she logs in to the system.

1. In the Operators Browser, **right-click** on the desired operator and **select** Leave Message.

   The Message Waiting... dialog opens.

2. If desired, **select** the Urgent checkbox.

   The message will appear in red text when received.

3. **Select** the Local checkbox to leave the message on the same station as the one on which the message is being composed.

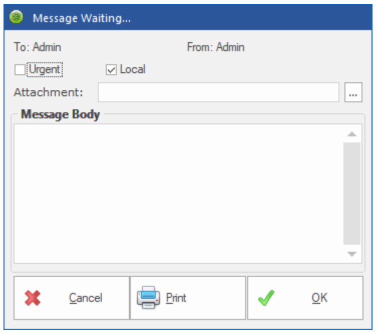
   OR

   Deselect the Local checkbox to display a drop-down menu listing each of the stations connected to the system as well as an ALL menu item. **Select** the desired station or ALL to leave the message on all the stations.

4. If desired, **select** the Browse button ... to add an attachment.

5. **Place** the cursor in the Message Body section and **type** the desired message.

6. **Click** OK to send the message or **click** Print to print the message.


Message Waiting...

To: Admin

From: Admin

□ Urgent ☑ Local

Attachment:

Locate

The Locate feature will display the station information where the selected operator is currently logged in.

1. In the Operators Browser, **right-click** on the desired operator and **select** Locate.

   The Locate dialog opens to display the station information.

2. **Click** OK to close the dialog.

Journal

Occasionally, an operator may need to maintain a record of information beyond what is normally retained by the database, e.g., commentary regarding situations, equipment, other operators, or his/her own actions.

For these tasks, the operator can use the DNA Journal. The journal feature allows an operator to record a text entry and/or view existing entries based on operator restrictions.

Creating a New Entry

1. In the Operators Browser, **right-click** on an operator and **select** Journal / New Entry.

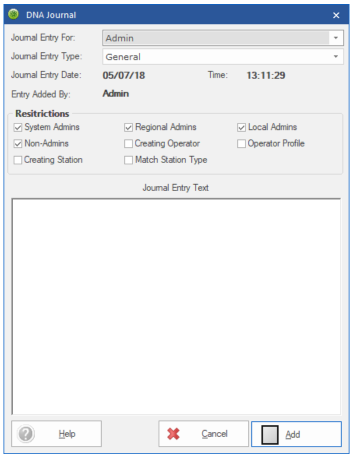
   The DNA Journal dialog opens in entry mode.

2. **Configure** the DNA Journal log.

   - Journal Entry For - Indicates the type of entry component; entries may be filtered by this field. Select one of the following options:
     - □ Operator - The entry is specific to the active operator.
     - □ Station - The entry is specific to the active workstation.
     - □ Authorization Server - The entry is specific to the authorization server.
     - □ DNA System - The entry is specific to the DNA system.
   - Journal Entry Type - Indicates a filter category for the journal entry.
   - Restrictions - Indicates who has permission to view the entry.

3. **Type** the desired message in the Journal Entry Text panel.

4. **Click** the Add button.



Journal Entry For: Admin

Journal Entry Type: General

Journal Entry Date: 05/07/18 Time: 13:11:29

Entry Added By: Admin

Resitrictions

☑ System Admins ☑ Regional Admins ☑ Local Admins

☑ Non-Admins □ Creating Operator □ Operator Profile

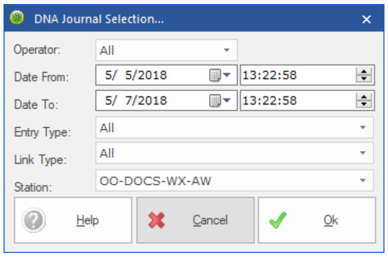
□ Creating Station □ Match Station Type

Journal Entry Text

Viewing an Entry

1. In the Operators Browser, **right-click** on an operator and **select** Journal / View.

   The DNA Journal Selection dialog opens, allowing the operator to filter the entries.



Operator: All

Date From: 5/ 5/2018 13:22:58

Date To: 5/ 7/2018 13:22:58

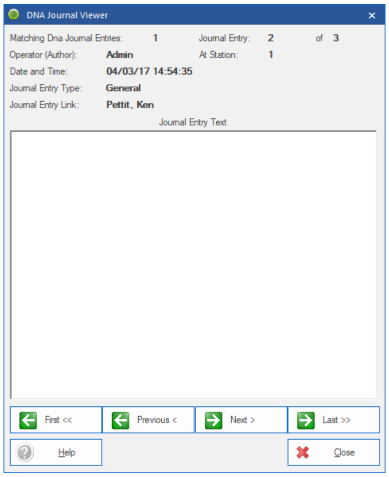
Entry Type: All

Link Type: All

Station: OO-DOCS-WX-AW

2. **Configure** the DNA Journal Selection dialog:

   - Operator - Filters the entries by operator name.
   - Date From/To - Filters the entries by the specified date and time range.
   - Entry Type - Filters the entries by the journal entry type.
   - Link Type - Filters the entries by the link type designated in the Journal Entry For field.
   - Station - Filters the entries by workstation.



Matching Dna Journal Entries: 1 Journal Entry: 2 of 3

Operator (Author): Admin At Station: 1

Date and Time: 04/03/17 14:54:35

Journal Entry Type: General

Journal Entry Link: Pettit, Ken

Journal Entry Text

3. **Click** OK to view the filtered results.

   The DNA Journal Viewer appears. An operator can only view entries for which the appropriate operator restriction was checked.

   The read-only fields indicate an entry's properties, including its chronological sequence, author, station of origin, date and time, entry type, and link type.

   Navigate through the entries with the green arrow buttons at the bottom of the dialog: First, Previous, Next, and Last.

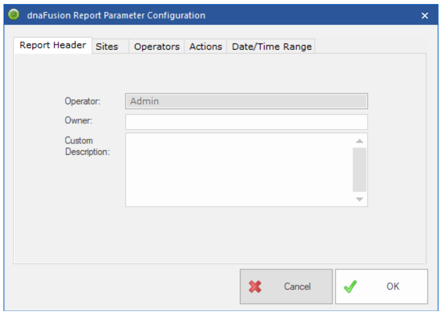
4. When finished, **select** the Close button to close the dialog.

Audit Report

An operator’s actions can be traced by running an Audit Report. Another operator report is the System Audit Trail report, which can be accessed from Reports in the Main Menu.

1. In the Operators Browser, **right-click** on the desired operator and **select** Audit Report.

   The Report Parameter Configuration dialog opens in a new window.



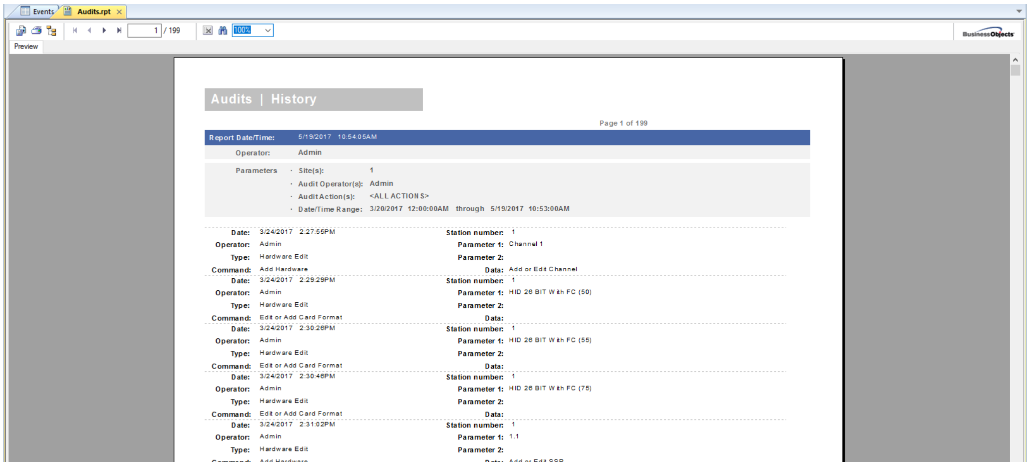
Operator: Admin
Owner:
Custom Description:

2. If desired, **enter** the Report Header information.
3. **Select** the Sites tab and **select** a site option.
4. **Select** the Operators tab and **select** the operator(s) to include in the audit report.

   The operator that is highlighted when you select the Audit Report option will be selected by default.
5. **Select** the Actions tab and **select** the desired operator actions to include in the report.
6. **Select** the Date/Time Range tab and **configure** the Date and Time options.
7. **Click** OK to generate the Audit Report.

   The report appears in the data window.

   For more information on navigating reports, see page 17-6.



```
Audits | History

                                                   Page 1 of 199
Report Date/Time:   5/19/2017  10:54:05AM
      Operator:     Admin
      Parameters  · Site(s):              1
                  · Audit Operator(s):    Admin
                  · Audit Action(s):      <ALL ACTIONS>
                  · Date/Time Range:      3/20/2017  12:00:00AM  through  5/19/2017  10:53:00AM

     Date:  3/24/2017  2:27:55PM          Station number:  1
 Operator:  Admin                            Parameter 1:  Channel 1
     Type:  Hardware Edit                    Parameter 2:
  Command:  Add Hardware                            Data:  Add or Edit Channel
     Date:  3/24/2017  2:29:29PM          Station number:  1
 Operator:  Admin                            Parameter 1:  HID 26 BIT With FC (50)
     Type:  Hardware Edit                    Parameter 2:
  Command:  Edit or Add Card Format                 Data:
     Date:  3/24/2017  2:30:26PM          Station number:  1
 Operator:  Admin                            Parameter 1:  HID 26 BIT With FC (55)
     Type:  Hardware Edit                    Parameter 2:
  Command:  Edit or Add Card Format                 Data:
     Date:  3/24/2017  2:30:46PM          Station number:  1
 Operator:  Admin                            Parameter 1:  HID 26 BIT With FC (75)
     Type:  Hardware Edit                    Parameter 2:
  Command:  Edit or Add Card Format                 Data:
     Date:  3/24/2017  2:31:02PM          Station number:  1
 Operator:  Admin                            Parameter 1:  1.1
     Type:  Hardware Edit                    Parameter 2:
  Command:  Add Hardware                            Data:  Add or Edit SSP
```

> *Use the* Ctrl *or* Shift *key to select multiple options in the* Report Parameter Configuration *dialog.*

NOTES:

Operator SSP Options

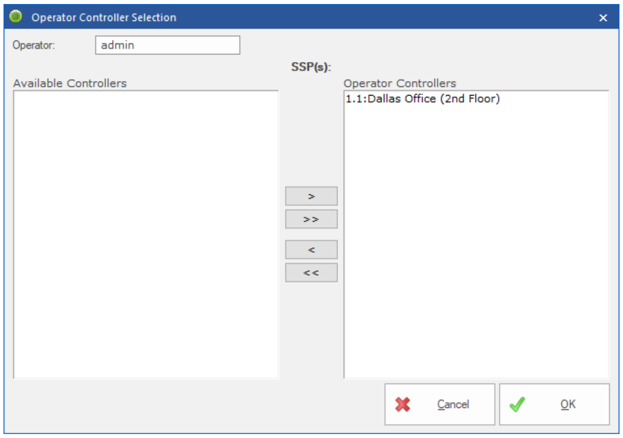
An administrator can grant or restrict operator access to specific SSPs without using the tenants feature. The operator's Events and Alarm Grid will be limited to the assigned controller(s); however, the operator will still be able to view all personnel.

Profile SSP List

To use the Profile SSP List button in the Operator Profiles dialog, the administrator must first select the Enable Operator SSP Lists checkbox in the Host Settings / DNA Properties dialog. See page 3-5 for information.

1. **Open** the Operator Profile dialog as described on page 4-5.
2. **Click** the Profile SSP List button. Profile SSP List

   The Operator Controller Selection dialog opens with a list of available SSPs.



Operator: admin

1.1:Dallas Office (2nd Floor)

3. **Select** the desired Controller from the Available Controllers panel and **click** the single right arrow button to move the selected controller to the Operator Controllers panel.

   OR

   Click the double right arrow button to move all Available Controllers to the Operator Controllers panel.
4. **Click** OK to save the changes and close the dialog.

   The operator profile will be restricted to the selected controllers.

This Page Intentionally Left Blank

Time & Holiday Schedules 5

In This Chapter

√ Adding Time Schedules & Time Sets
√ Controlling Time Schedules
√ Adding Holidays & Holiday Sets

Time schedules are predetermined time blocks that can be used to control access and automated features. Time schedules can be linked to access levels to regulate what times a cardholder has access to specific doors. They can also be paired with triggers to initiate predefined system actions known as macros. When associated with time schedules, certain devices will change behavior based on different times of the day or week.

A Holiday Type can be associated with a time schedule to allow exceptions to the normal schedule. For example, a door schedule could contain an exception for observed holidays to prevent the door from unlocking on days designated as a holiday.

Time Schedules

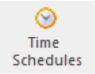
Time schedules are user-defined time ranges and associated weekdays that are stored in the controller for access control. A time schedule can include up to 12 time intervals. Each interval consists of a Begin and End time as well as an option to designate Holiday Types.

By default, each controller stores up to 255 time schedules. All time schedules are stored remotely at the controller once downloaded (along with personnel information and access levels).

Adding a Time Schedule

1. **Click** the Time Schedules button on the Standard Toolbar.

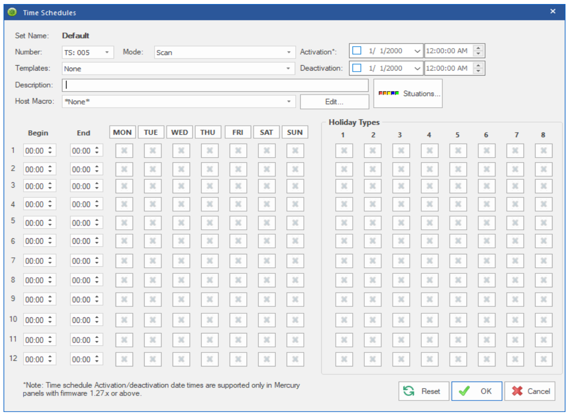
   The Time Schedules Browser opens.



2. **Right-click** in the browser and **select** New Time Schedule.

   The Time Schedules dialog opens.

   If the time schedule was added to a time schedule set, the Set Name will be displayed. See page 5-7 for information on sets.



Set Name: **Default**
Number: TS: 005
Mode: Scan
Activation*: □ 1/ 1/2000 12:00:00 AM
Templates: None
Deactivation: □ 1/ 1/2000 12:00:00 AM
Description:
Host Macro: *None*

										Holiday Types							
	Begin	End	MON	TUE	WED	THU	FRI	SAT	SUN	1	2	3	4	5	6	7	8
1	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
2	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
3	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
4	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
5	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
6	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
7	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
8	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
9	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
10	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
11	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
12	00:00	00:00	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

*Note: Time schedule Activation/deactivation date times are supported only in Mercury panels with firmware 1.27.x or above.

3. If needed, **select** a unique Number for the schedule.

   DNA automatically assigns the next available number.

4. **Select** a Mode from the drop-down list.

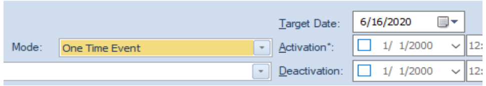
   - Off - The time schedule is inactive; no access granted.
   - On - The time schedule is active 24/7 regardless of the days and times specified. Access will be granted regardless of the time specified.
   - Scan - (Default setting) The system continually checks the time to determine which schedules should be activated. Access will be granted based on the scheduled time interval(s).
   - Scan, Always Honor Day of Week - The system continually checks to see which time schedules are to be activated regardless of programmed holiday dates.
   - One Time Event - The time schedule is active for one target date, then will deactivate when the target date expires.

This Page Intentionally Left Blank

5. **Enter** a Description for the time schedule.

   Typically, the description should indicate the schedule's time range or purpose, e.g. Working Hours 8:00 a.m. - 5:00 p.m. or Front Door Unlock Schedule.

6. If desired, **select** a Template to apply to the new time schedule.
7. If One Time Event was selected, **enter** the Target Date.
8. If desired, **set** a Activation/Deactivation date and time for the new time schedule.



Target Date: 6/16/2020

Mode: One Time Event

Activation*: □ 1/ 1/2000 12:

Deactivation: □ 1/ 1/2000 12:

> *Activation/Deactivation date and time are supported only on Mercury panels with firmware 1.27.x or above.*

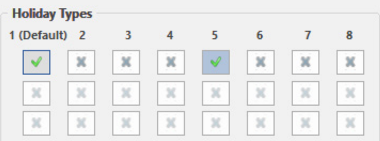
9. If desired, **click** the Situations button to configure Situation Levels for the schedule; see page 9-7.
10. If desired, **select** a Host Based Macro for the time schedule; see page 10-13.
11. **Enter** the Begin and End time(s) using military time designations (00:00-23:59).

    Each time schedule contains at least one (1) time interval and can contain a maximum of twelve (12) intervals.

> *If a time schedule needs to span midnight, set the* End *time to 11:59 p.m. (23:59) and* Begin *the next day at 12:00 a.m. (00:00). This will provide seamless coverage.*

12. **Select** which day(s) of the week to associate with each time interval.
13. **Select** which Holiday Types (1-8) to apply to each time interval.

    The Holiday Types checkboxes determine what times will be activated on holidays of a specified type. For example, if Holiday Types 1 and 5 are checked for an 08:00-17:00 time interval, the time schedule will become active from 8:00 a.m. to 5:00 p.m. on holidays that have been configured as Type 1 or Type 5 in the Holidays dialog. See page 5-9 for more information.



Holiday Types

1 (Default)	2	3	4	5	6	7	8
☑	☒	☒	☒	☑	☒	☒	☒
☒	☒	☒	☒	☒	☒	☒	☒
☒	☒	☒	☒	☒	☒	☒	☒

14. **Click** Save to save the new time schedule.
15. If the One Time Event mode is selected, **set** a Target Date and time.

    After setting a One Time Event, the time schedule will activate according to the set Target Date and will deactivate when the event ends.

Downloading Time Schedules

Time schedules must be downloaded to the controller in order to take effect. Downloads can be performed for all configured time schedules or for individual schedules. Once the download is complete, the time schedule(s) can be controlled from the host.

To download all time schedules:

1. **Right-click** in the Time Schedules Browser and **select** Download.

   The time schedules are downloaded to the controller.

To download an individual time schedule:

1. In the Time Schedules Browser, **right-click** on the desired Time Schedule and **select** Download.

   The time schedule is downloaded to the controller.

Editing a Time Schedule

1. **Right-click** on the Time Schedule and **select** Properties.
2. **Edit** the time schedule as needed.
3. **Click** OK to save the changes.

   The time schedule is updated.

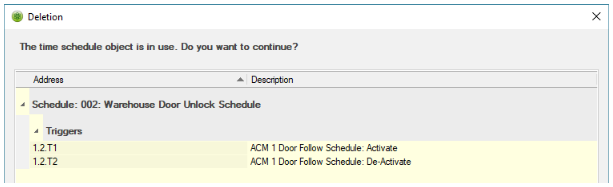
Deleting a Time Schedule

1. **Right-click** on the Time Schedule and **select** Remove.

   A confirmation dialog will appear.

2. **Click** Yes to confirm the deletion.

   The time schedule is removed from the browser.



The time schedule object is in use. Do you want to continue?

Address	Description
Schedule: 002: Warehouse Door Unlock Schedule	
Triggers	
1.2.T1	ACM 1 Door Follow Schedule: Activate
1.2.T2	ACM 1 Door Follow Schedule: De-Activate

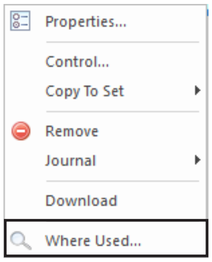
> *If the time schedule is currently in use (doors, triggers, etc.), the* Deletion *confirmation dialog will appear with a report of the affected objects. The time schedule cannot be deleted until the operator reconfigures the time schedules for these objects.*

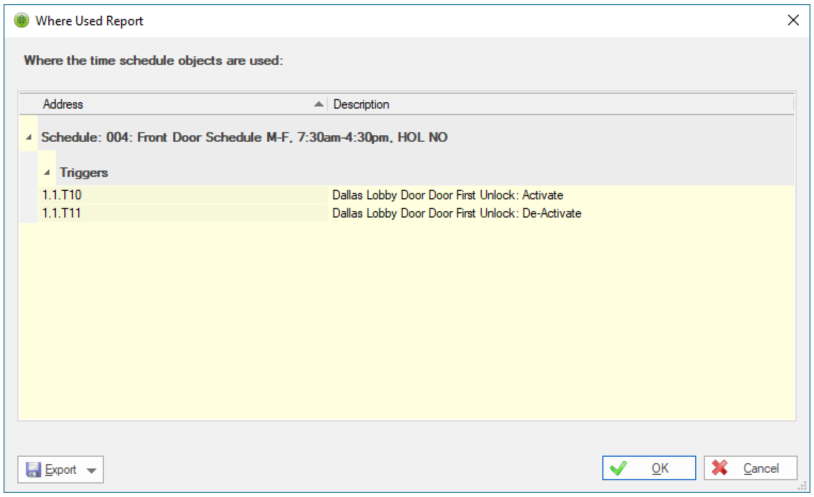
Where Used Report

The Where Used report lists all the areas where a time schedule has been used, e.g. access levels, door schedules, triggers, etc.

1. **Right-click** on the desired Time Schedule and **select** Where Used.

   The Where Used Report opens.





Where the time schedule objects are used:

Address	Description
Schedule: 004: Front Door Schedule M-F, 7:30am-4:30pm, HOL NO	
Triggers	
1.1.T10	Dallas Lobby Door Door First Unlock: Activate
1.1.T11	Dallas Lobby Door Door First Unlock: De-Activate

2. If desired, **select** the Export option.

   - Export Grid to CSV File - The Save As dialog appears; **rename** the file, **browse** to the desired location, and **click** Save.
   - Export Grid to Clipboard - Exports the information to the Windows Clipboard. The text can then be pasted in a separate document.

3. **Click** OK or Cancel to close the dialog.

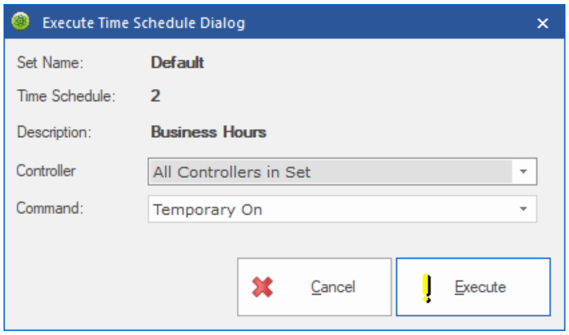
Controlling Time Schedules

Once the time schedules have been successfully downloaded to the SSP controller(s), they can be controlled from the Time Schedules Browser or Hardware Browser.

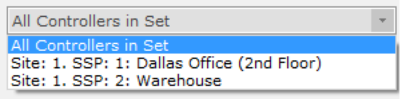
From the Time Schedules Browser

1. In the Time Schedules Browser, **expand** the desired Time Schedule Set.
2. **Right-click** on the desired Time Schedule and **select** Control.

   The Execute Time Schedule Dialog appears.



Set Name: Default
Time Schedule: 2
Description: Business Hours
Controller: All Controllers in Set
Command: Temporary On



All Controllers in Set
Site: 1. SSP: 1: Dallas Office (2nd Floor)
Site: 1. SSP: 2: Warehouse

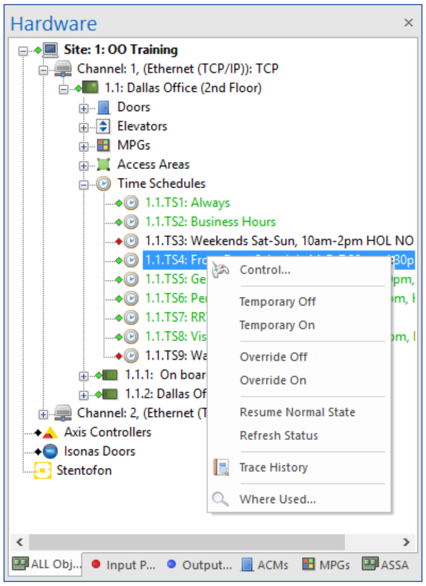
3. **Select** an individual Controller from the drop-down list.

   OR

   Select All Controllers in Set to control the time schedule for all controllers in the time schedule set.
4. **Select** the appropriate Command from the drop-down menu.
   - Temporary Off – Temporarily sets the time schedule mode to OFF. The next ON interval edge will return the schedule to its normal time-based state. Use the Resume Normal State command to restore the time schedule to the time-based control prior to the next interval edge.
   - Temporary On - Temporarily sets the time schedule mode to ON. The next OFF interval edge will return the schedule to its normal time-based state. Use the Resume Normal State command to restore the time schedule to the time-based control prior to the next interval edge.
   - Override Off - Sets the time schedule mode to OFF and overrides the Scan mode. Time intervals have no effect when this command is used. Use the Resume Normal State command to restore the time schedule to the time based control.
   - Override On - Sets the time schedule mode to ON and overrides the Scan mode. Time intervals have no effect when this command is used. Use the Resume Normal State command to restore the time schedule to the time-based control.
   - Resume Normal State – Puts the time schedule into the state as defined by time-based rules. Use this command to remove the Temporary On/Off and Override On/Off commands. The system will return to its “normal” state.
   - Refresh Status – Logs the current time schedule modes in the transaction log. Use this command to test triggers that are activated based on time schedule events.
5. **Click** Execute to send the command to the controller.
6. **Click** Cancel to close the dialog.

> ⓘ *Time schedules can also be controlled individually per controller from the* Hardware Browser*. See page 5-6 for more information.*

From the Hardware Browser



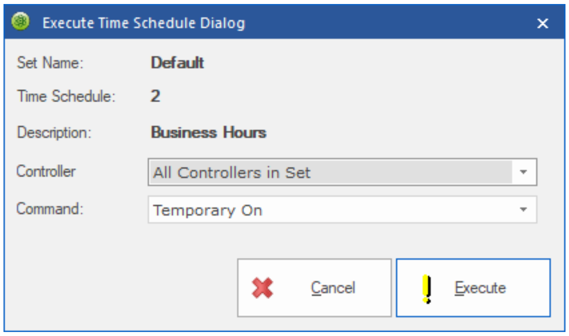
1. In the Hardware Browser, **locate** and **expand** the desired controller.
2. **Expand** the Time Schedules header.
3. **Right-click** on the desired Time Schedule and **select** the appropriate Command from the drop-down menu.

   The command is executed at the controller.

   OR

   Right-click on the desired Time Schedule and **select** Control.

   The Execute Time Schedule Dialog appears.



Set Name: Default

Time Schedule: 2

Description: Business Hours

Controller: All Controllers in Set

Command: Temporary On

4. **Select** the appropriate Command from the drop-down menu.
   - Temporary Off – Temporarily sets the time schedule mode to OFF. The next ON interval edge will return the schedule to its normal time-based state. Use the Resume Normal State command to restore the time schedule to the time-based control prior to the next interval edge.
   - Temporary On - Temporarily sets the time schedule mode to ON. The next OFF interval edge will return the schedule to its normal time-based state. Use the Resume Normal State command to restore the time schedule to the time-based control prior to the next interval edge.
   - Override Off - Sets the time schedule mode to OFF and overrides the Scan mode. Time intervals have no effect when this command is used. Use the Resume Normal State command to restore the time schedule to the time based control.
   - Override On - Sets the time schedule mode to ON and overrides the Scan mode. Time intervals have no effect when this command is used. Use the Resume Normal State command to restore the time schedule to the time-based control.
   - Resume Normal State – Puts the time schedule into the state as defined by time-based rules. Use this command to remove the Temporary On/Off and Override On/Off commands. The system will return to its "normal" state.
   - Refresh Status – Logs the current time schedule modes in the transaction log. Use this command to test triggers that are activated based on time schedule events.
5. **Click** Execute to send the command to the controller.

   The command is executed at the controller.
6. **Click** Cancel to close the dialog.

Time schedules can also be controlled from the Time Schedules Browser. *See page 5-5 for more information.*

Time Schedule Sets

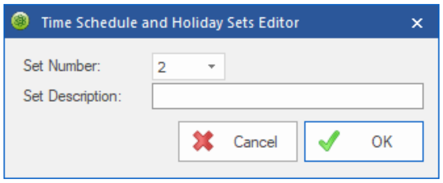
A time schedule set allows the operator to create numerous time schedules and assign them to one or more controllers. The controller will then be limited to the time schedules that are part of the assigned set. Keep in mind that each controller can store a maximum of 255 time schedules.

> *If a time schedule set is not specified in the* Controller Properties*, the controller will be downloaded with all time schedules listed under the* Default *tree object.*

Creating a Time Schedule Set

1. **Right-click** in the Time Schedules Browser and **select** New Time Set from the context menu.

   The Time Schedule and Holiday Sets Editor dialog opens.



Time Schedule and Holiday Sets Editor

Set Number: 2

Set Description:

2. If needed, **select** a different Set Number to identify the time schedule set.

   The next available number automatically populates in the field.

3. **Enter** a Description for the set.

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

   The set is added to the Time Schedules Browser.

5. **Right-click** on the Time Schedule Set and **select** Download.

> *After a time schedule set is configured, saved, and downloaded, it will appear in the* Controller Properties *dialog under the* Time Schedule Set *drop-down list. The drop-down field indicates which set of time schedules the controller will observe. See page 8-52 for more information.*

Adding Time Schedules to a Set

Time schedules can be added to a set using three methods:

- Copy an existing time schedule
- Drag and drop an existing time schedule
- Create a new schedule specific to the set

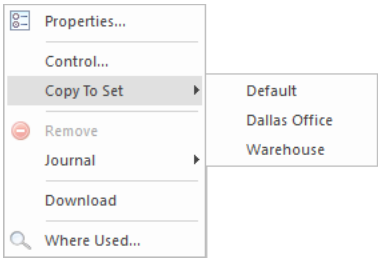
Copy a Time Schedule

1. In the Time Schedules Browser, **expand** the Time Schedule Set.

2. **Select** the desired time schedule(s).

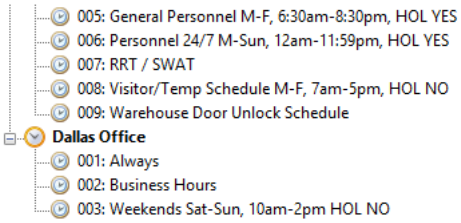
   Press and **hold** the Ctrl or Shift key to select multiple time schedules.

3. **Right-click** on the schedule(s) and **select** Copy to Set.



4. **Select** the desired Time Schedule Set.

   The time schedule(s) are copied to the specified set.



005: General Personnel M-F, 6:30am-8:30pm, HOL YES
006: Personnel 24/7 M-Sun, 12am-11:59pm, HOL YES
007: RRT / SWAT
008: Visitor/Temp Schedule M-F, 7am-5pm, HOL NO
009: Warehouse Door Unlock Schedule
Dallas Office
001: Always
002: Business Hours
003: Weekends Sat-Sun, 10am-2pm HOL NO

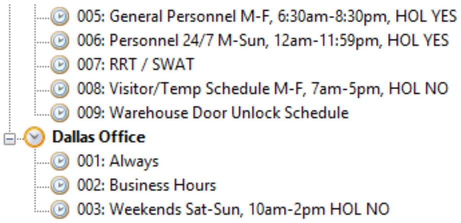
5. **Right-click** in the Time Schedules Browser and **select** Download.

Drag and Drop a Time Schedule

1. In the Time Schedules Browser, **expand** the desired Time Schedule Set.
2. **Select** the Time Schedule(s) that will be copied to another set.

   Press and **hold** the Ctrl or Shift key to select multiple time schedules.
3. **Drag** and **drop** the Time Schedule(s) to the desired Time Schedule Set.

   The time schedule(s) appear in the specified set.



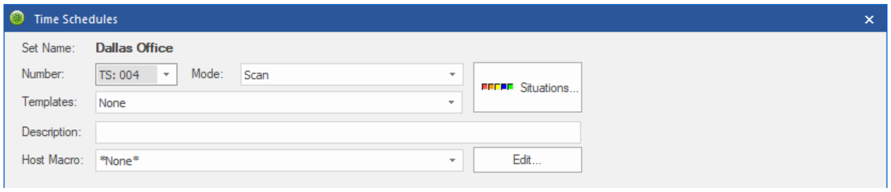
005: General Personnel M-F, 6:30am-8:30pm, HOL YES
006: Personnel 24/7 M-Sun, 12am-11:59pm, HOL YES
007: RRT / SWAT
008: Visitor/Temp Schedule M-F, 7am-5pm, HOL NO
009: Warehouse Door Unlock Schedule
Dallas Office
001: Always
002: Business Hours
003: Weekends Sat-Sun, 10am-2pm HOL NO

4. **Right-click** in the Time Schedules Browser and **select** Download.

Create a Set-Specific Time Schedule

1. In the Time Schedules Browser, **right-click** on the desired Time Schedule Set and **select** New Time Schedule.

   The Time Schedules dialog opens with the designated Set Name.



Time Schedules

Set Name: Dallas Office
Number: TS: 004
Mode: Scan
Templates: None
Description:
Host Macro: *None*

2. **Create** the Time Schedule.

   See page 5-1 for more information.

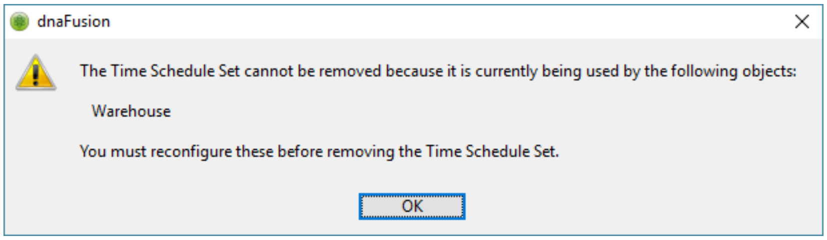
Deleting a Time Schedule Set

1. **Right-click** on the desired Time Schedule Set and **select** Remove Time Set.

   A confirmation dialog will appear.
2. **Click** Yes to confirm the deletion.

   The Time Schedule Set is removed from the Time Schedules Browser.

If the time schedule set is currently in use, an error message will appear with a list of affected objects. The operator must reconfigure the times schedules for these objects before removing the time schedule set.



dnaFusion

The Time Schedule Set cannot be removed because it is currently being used by the following objects:

Warehouse

You must reconfigure these before removing the Time Schedule Set.

Holidays

The operator can designate up to 255 different holidays in DNA Fusion. When a day is specified as a holiday, the system will treat it differently than a regular day (Mon-Sun). Holidays are defined by the date and duration of the holiday as well as their assigned type. Holidays allow for exceptions to be created based on date.

System users will often create holidays if their facility runs on an entirely different schedule during these days. For example, if a manufacturing plant is closed on Thanksgiving Day, the manager may not want the front doors to unlock as they do during regular business hours. Therefore, he would establish Thanksgiving Day as a holiday in DNA Fusion and would configure the doors' Time Schedules dialog without selecting the Holiday Type designated for Thanksgiving Day.

Holidays & Time Schedules

Holidays and time schedules share a special relationship. At midnight, the system checks to see if the day is designated as a holiday. If it is, the system checks to see if Holiday Types are checked for any of the time schedules. The system then verifies whether the Holiday Types checked for each time schedule correspond with the Holiday Type designated for the holiday itself. If it does, the time interval(s) will become active during the holiday.

Adding a Holiday

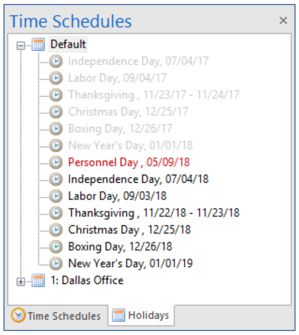
1. **Select** the Holidays tab in the Time Schedules Browser.
2. **Expand** the desired Holiday Set.

   The text color indicates the holiday's position on the calendar:

   - Gray – The holiday has already occurred.
   - Red – The holiday is today.
   - Black – The holiday is in the future.
3. **Right-click** inside the Holidays tab and **select** Add Holiday.

   The Holidays dialog displays.

   A holiday can span up to 127 days. Note that Saturday and Sunday are generally NOT included when selecting dates for a holiday schedule.

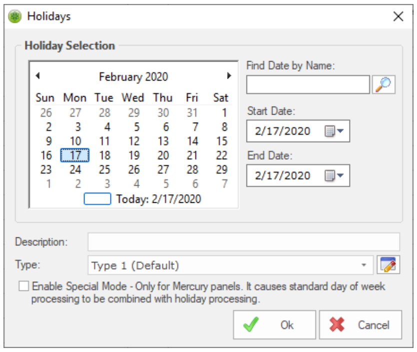


Time Schedules

- Default
  - Independence Day, 07/04/17
  - Labor Day, 09/04/17
  - Thanksgiving , 11/23/17 - 11/24/17
  - Christmas Day, 12/25/17
  - Boxing Day, 12/26/17
  - New Year's Day, 01/01/18
  - Personnel Day , 05/09/18
  - Independence Day, 07/04/18
  - Labor Day, 09/03/18
  - Thanksgiving , 11/22/18 - 11/23/18
  - Christmas Day , 12/25/18
  - Boxing Day, 12/26/18
  - New Year's Day, 01/01/19
- 1: Dallas Office

4. **Configure** the holiday using one of following methods:

   - Calendar - **Select** the holiday date(s) from the calendar. To select multiple consecutive dates, **drag** the mouse cursor or **press** and **hold** the Shift key.
   - Date Range - **Enter** a date range in the Start Date and End Date fields (M/DD/YYYY) or **select** the drop-down icon ▦▾ to use a calendar.
   - Search Field - Enter the holiday name or date in the Find Date by Name field and **click** the Search button. If the system recognizes the holiday, the Date and Description fields will auto-populate for the next occurrence. If the holiday is not recognized, the operator must manually select the date.



Holidays

Holiday Selection

February 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
1	2	3	4	5	6	7

Today: 2/17/2020

Find Date by Name:

Start Date: 2/17/2020

End Date: 2/17/2020

Description:

Type: Type 1 (Default)

☐ Enable Special Mode - Only for Mercury panels. It causes standard day of week processing to be combined with holiday processing.

The search field also accepts shortcut keys; for a list of available holiday shortcuts, see page 5-10. Enter the year after the shortcut to search for a holiday in a specific year.

5. **Enter** a Description for the holiday.
6. **Select** the Holiday Type from the drop-down list.

   The holiday types are used to link time schedules with holidays of a certain type. For instance, Type 1 holidays may designate a regular day off while Type 2 holidays are reserved for half days.
7. If desired, **check** the Enable Special Mode box (Only for Mercury panels).

   This mode allows the application to define time intervals that will become active only on designated days. This mode does not affect Day-of-Week based time zones and is not disruptive to normal access rights. When a special holiday is active, as well as the regular day-of-week time zones to be active.

8. **Click** OK.
9. **Right-click** in the Holidays tab and **select** Download.

Deleting a Holiday

1. **Right-click** on the Holiday and **select** Remove Holiday.

   A confirmation dialog will appear.
2. **Click** Yes to confirm the deletion.

   The holiday is removed from the holiday set.
3. **Right-click** in the Holidays tab and **select** Download.

Holiday Shortcuts

Enter one of the following shortcuts into the Find Date by Name field and **click** the Search button 🔍. If the holiday is recognized, the Date and Description fields will populate for the next occurrence.

Shortcut	Holiday/Day
X	Christmas Day
XE	Christmas Eve
E	Easter
GF	Good Friday
AW	Ash Wednesday
H	Halloween
NY	New Year's Day
NYE	New Year's Eve
J4	Independence Day (4th of July)
MD	Memorial Day
LD	Labor Day
VD	Veterans Day
CD	Columbus Day
TH	Thanksgiving
PD	Presidents Day
T	Today
N	Now
Y	Yesterday
TM	Tomorrow
NW	Next Week
N1	Next Sunday
N2	Next Monday
N3	Next Tuesday
N4	Next Wednesday
N5	Next Thursday
N6	Next Friday
N7	Next Saturday

Enter the year after the shortcut to search for future dates, e.g. X 2020*.*

Holiday Sets

Holiday sets, similar to time schedule sets, allow the operator to establish numerous holidays and assign them to specific SSP controllers. The controller(s) will then be limited to the holidays that are in the assigned holiday set. Keep in mind that each controller can store a maximum of 255 time schedules.

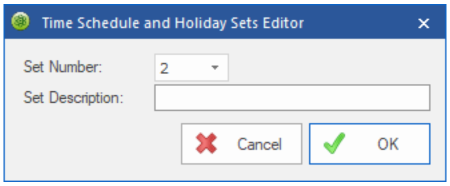
If a holiday set is not specified, all holidays listed under the Default tree object will be downloaded to the controller.

> *After a holiday set is configured, saved, and downloaded, it will appear in the* Controller Properties *dialog under the* Holiday Set *drop-down list. The drop-down field indicates which set of holidays the controller will observe. See page 8-52 for more information.*

Adding a Holiday Set

1. **Right-click** in the Holidays tab and **select** Add Holiday Set from the context menu.

   The Time Schedule and Holiday Sets Editor appears.



Time Schedule and Holiday Sets Editor

Set Number: 2

Set Description:

2. **Select** a Set Number that will serve to identify the holiday set.
3. **Enter** a Set Description.
4. **Click** OK to save the set.

Deleting a Holiday Set

1. **Right-click** on the desired Holiday Set and **select** Remove Holiday Set.

   A confirmation dialog will appear.
2. **Click** Yes to delete the set.

Adding Holidays to a Set

1. **Right-click** on the desired Holiday Set and **select** Add Holiday to This Set.

   The Holidays dialog appears.
2. **Configure** the Holiday and **select** OK.

   The Holiday is added to the selected Holiday Set.

> *Alternatively, the operator can* **drag** and **drop** *an existing* Holiday *to the* Holiday Set*.*

Removing Holidays from a Set

1. In the Holidays explorer, **expand** the Holiday Set.
2. **Right-click** on the desired Holiday and **select** Remove Holiday.

   A confirmation dialog will appear.
3. **Click** Yes to confirm the deletion.

   The holiday is removed from the set.

This Page Intentionally Left Blank

Access Levels 6

An access level is an entry point (i.e. door, elevator) combined with a time schedule or floor group that, when assigned to a card, determines when and where the cardholder has access within the system. Access levels can be added to individual cards or groups of cards. Depending on the Access Levels Per Card setting in the Controller Properties / Stored Quantities dialog, each card can be configured to store up to 6, 32, or 128 access levels per controller.

This chapter explains how to create, modify, and remove access levels. For information on assigning access levels to cards, see page 7-13.

Overview

DNA Fusion offers three (3) types of access levels:

- Global Access Level Group - Groups doors and elevators from multiple controllers under a common access level, which prevents the need for controller-specific access levels. Cardholders with a global access level group can access entry points from multiple controllers; see page 6-3 for more information.
- Legacy Access Level - Legacy access levels are created at the controller level; they consist of an ACM (i.e. door, elevator) and an associated time schedule. Legacy access levels are grouped together via Legacy Access Level Groups. See page 6-5 for information on legacy door access levels and page 6-9 for information on legacy elevator access levels.
- Legacy Access Level Group - Groups legacy access levels from various controllers together for ease of assignment to designated cards. See page 6-7 for more information.

> ⓘ Legacy Access Levels *must be created prior to creating the* Legacy Access Level Group*.*

> ! *At least one entry point (door or elevator; see pages 8-59 and 8-67) and one time schedule (see page 5-1) must be created prior to adding an access level. If elevators have been configured in the system, floor groups will need to be created; see page 6-9.*

Two optional advanced features can be applied to global and legacy access levels:

- Escort Requirement - Requires at least two (2) access levels: Is an Escort and Requires an Escort. A cardholder that requires an escort cannot gain access unless an Escort cardholder badges after them. See page 6-13 for more information.
- Auto-Expiration - Assigns an Activation Date and Deactivation Date to an access level. The access level will automatically activate and deactivate based on the configured dates. See page 6-15 for more information.

> ⓘ Controller Flags *and* Door Properties *must be configured to support advanced access level features. See pages 8-53 and 8-59 for more information.*

This Page Intentionally Left Blank

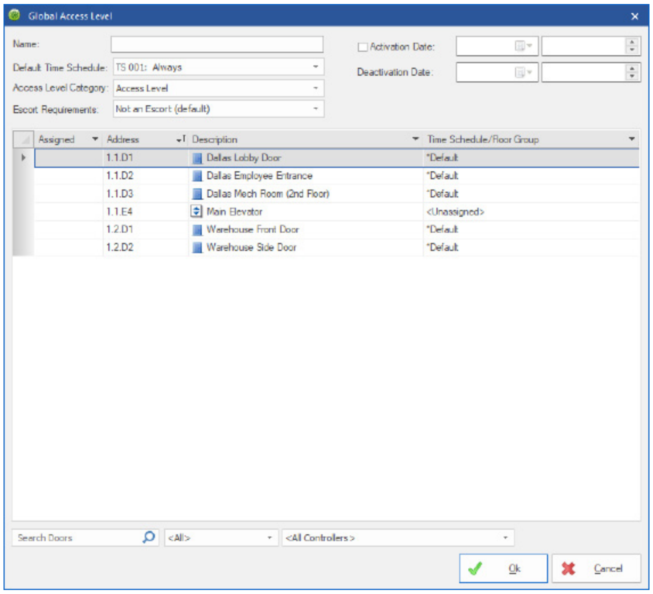
Global Access Levels

As of DNA Fusion version 6.1.0.12, operators can create Global Access Level Groups to group doors and elevators from multiple controllers under a common access level. In contrast to Legacy Access Level Groups, Global Access Level Groups can span multiple controllers without first requiring the operator to create individual, controller-specific access levels.

Creating a Global Access Level Group

1. In the Access Levels Browser, **right-click** on Access Level Groups and **select** Add Global Access Level Group.

   The Global Access Level dialog opens.



Global Access Level

Name:

Default Time Schedule: TS 001: Always

Access Level Category: Access Level

Escort Requirements: Not an Escort (default)

□ Activation Date:

Deactivation Date:

Assigned	Address	Description	Time Schedule/Floor Group
	1.1.D1	Dallas Lobby Door	*Default
	1.1.D2	Dallas Employee Entrance	*Default
	1.1.D3	Dallas Mech Room (2nd Floor)	*Default
	1.1.E4	Main Elevator	<Unassigned>
	1.2.D1	Warehouse Front Door	*Default
	1.2.D2	Warehouse Side Door	*Default

Search Doors <All> <All Controllers>

2. **Enter** a Name for the global access level group.

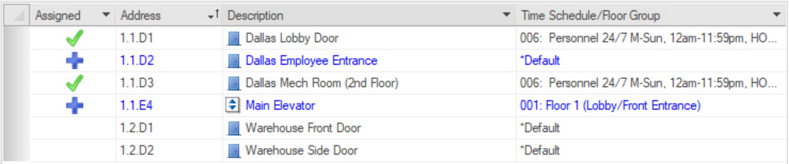
3. If desired, **select** a different Default Time Schedule and/or Access Level Category.

   The operator's privileges determine which access level categories are available; see page 4-12.

4. **Select** the Assigned column next to the desired doors and/or elevators.

   A ✚ appears in the Assigned column.

   If the door/elevator is already included in the group, a ✓ will auto-populate in the Assigned column.



Assigned	Address	Description	Time Schedule/Floor Group
✓	1.1.D1	Dallas Lobby Door	006: Personnel 24/7 M-Sun, 12am-11:59pm, HO…
✚	1.1.D2	Dallas Employee Entrance	*Default
✓	1.1.D3	Dallas Mech Room (2nd Floor)	006: Personnel 24/7 M-Sun, 12am-11:59pm, HO…
✚	1.1.E4	Main Elevator	001: Floor 1 (Lobby/Front Entrance)
	1.2.D1	Warehouse Front Door	*Default
	1.2.D2	Warehouse Side Door	*Default

5. If desired, **select** an individual Time Schedule from the drop-down menu for specific doors.

   This setting overrides the Default Time Schedule selection.

6. If an elevator is selected, **select** a Floor Group from the drop-down menu for each elevator.

   See page 6-9 for information on creating floor groups.

> *If a* Time Schedule Set *is assigned to the door or elevator's controller, the row will be highlighted in yellow. When the* Assigned *column is selected, the row will turn red to indicate that a* Time Schedule/Floor Group *must be selected.*

7. If desired, **configure** advanced access level options. See pages 6-13 and 6-15 for more information.

8. **Click** OK to save the Global Access Level dialog.

   The Global Access Level Group appears in the browser.

   Global Access Level Groups are designated by a folder with a red access level icon.

Editing a Global Access Level Group

1. **Right-click** on the Global Access Level Group and **select** Properties.

   The Global Access Level dialog opens.

2. **Edit** the Global Access Level Group:

   - To add a door or elevator: **Click** the Assigned column next to the desired ACM. A ✚ appears in the Assigned column.
   - To remove a door or elevator: If the door/elevator is already included in the group, a ✓ will appear in the Assigned column. **Click** the ✓ icon to remove the access level and a ▬ will appear.

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

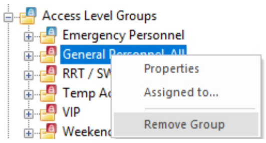
Removing a Global Access Level Group

1. **Right-click** on the Global Access Level Group and **select** Remove Group.

   A confirmation dialog will appear.

2. **Click** Yes to confirm the deletion.

   The access level group is removed from the browser.



> *Global Access Level Groups have a number of features. See page 6-19 for information.*

> *A cardholder's Access Level Groups can be easily converted to Legacy Groups by right-clicking on the cardholder or card.*

Legacy Access Levels

Legacy Access Levels contain doors and/or elevators from the same SSP controller. As a result, the operator must create the legacy access level at the controller level. Legacy Access Level Groups can be created to group the access levels from multiple controllers together for easier distribution to cardholders.

> Global Access Level Groups *can be created to group doors and elevators from multiple controllers under a common access level. See page 6-3 for more information.*

Creating a Legacy Door Access Level

1. **Click** the Access Levels button on the Standard Toolbar.

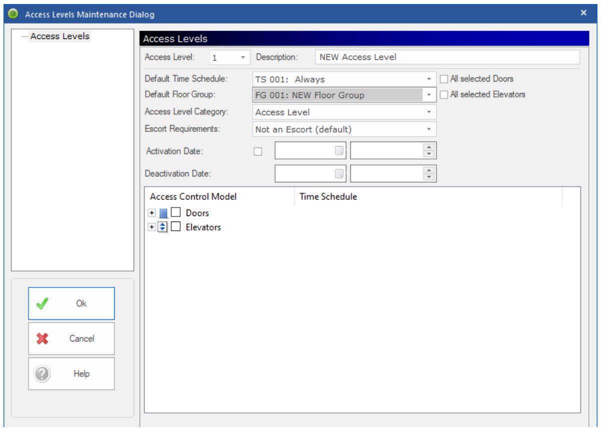
   OR

   Select View / Explorers / Access Levels from the Main Menu.

   The Access Levels Browser opens.

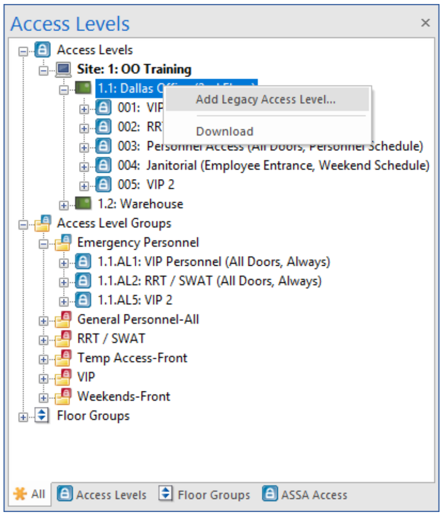
2. **Expand** the Access Levels tree, **right-click** on the desired Controller, and **select** Add Legacy Access Level.

   The Access Levels Maintenance Dialog appears.



Access Level: 1
Description: NEW Access Level
Default Time Schedule: TS 001: Always
□ All selected Doors
Default Floor Group: FG 001: NEW Floor Group
□ All selected Elevators
Access Level Category: Access Level
Escort Requirements: Not an Escort (default)
Activation Date: □
Deactivation Date:

Access Control Model	Time Schedule
+ □ Doors	
+ □ Elevators	



3. **Enter** a Description for the access level.
4. **Select** a Default Time Schedule to apply to the selected doors.
5. If desired, **check** All Selected Doors to apply the selected time schedule to all doors.

   This option overrides any time schedules selected for individual doors.

6. **Select** an Access Level Category to assign to the access level.

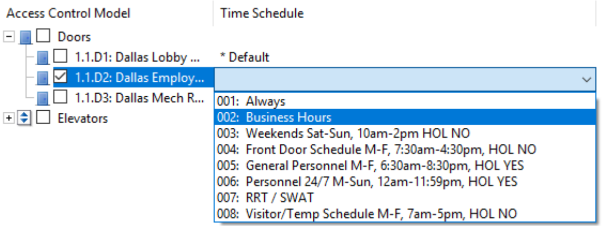
   The operator's privileges determine which access level categories are available; see page 4-12.

7. In the Access Control Model column, **expand** the Doors option and **select** the desired door(s).

   To select all the doors, **check** the main Doors header.

8. If desired, **select** an individual Time Schedule from the drop-down menu for specific doors.

   This setting applies a specific time schedule to the selected door.



Access Control Model	Time Schedule
□ Doors	
□ 1.1.D1: Dallas Lobby ...	* Default
☑ 1.1.D2: Dallas Employ...	
□ 1.1.D3: Dallas Mech R...	
+ □ Elevators	

001: Always
002: Business Hours
003: Weekends Sat-Sun, 10am-2pm HOL NO
004: Front Door Schedule M-F, 7:30am-4:30pm, HOL NO
005: General Personnel M-F, 6:30am-8:30pm, HOL YES
006: Personnel 24/7 M-Sun, 12am-11:59pm, HOL YES
007: RRT / SWAT
008: Visitor/Temp Schedule M-F, 7am-5pm, HOL NO

9. If desired, **configure** advanced access level options. See pages 6-13 and 6-15 for more information.
10. **Click** OK to save the access level.

    The Legacy Access Level will appear under the controller with a blue access level icon.

Editing a Legacy Door Access Level

1. **Right-click** on the Legacy Access Level and **select** Properties.

   The Access Level Editor dialog opens.

2. **Edit** the Access Level as needed.
3. **Click** OK to save the changes.

Deleting a Legacy Door Access Level

1. **Right-click** on the Legacy Access Level and **select** Remove Access Level.

   A confirmation dialog will appear.

2. **Click** Yes to confirm the deletion.

   The Legacy Access Level is removed from the browser.

Creating a Legacy Access Level Group

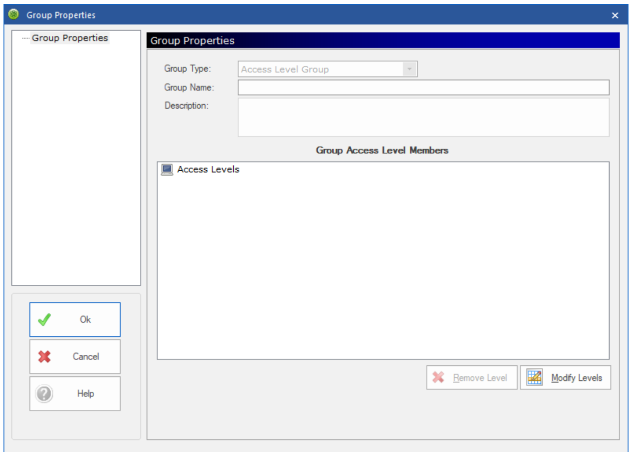
A Legacy Access Level Group includes legacy access levels from one or more controllers. When the legacy access level group is assigned to a cardholder, the cardholder will automatically receive the group's access levels.

If the legacy access level group is changed, all cardholders associated with the group will be affected.

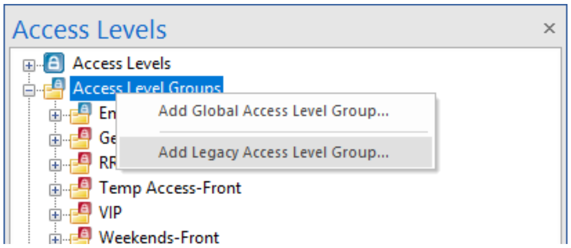
1. In the Access Levels Browser, **right-click** on Access Level Groups option and **select** Add Legacy Access Level Group.

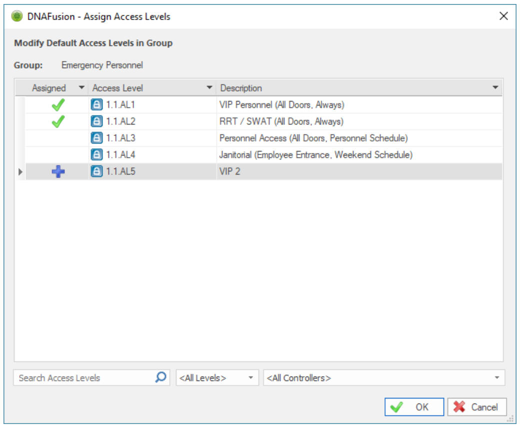
   The Group Properties dialog opens.

> *The* Add Legacy Access Level Group *option is only available if* Show Legacy Access Level Details *is checked in the* DNA Properties / Station Settings *dialog. See page 3-5 for information.*



Group Type: Access Level Group





Modify Default Access Levels in Group

Group: Emergency Personnel

Assigned	Access Level	Description
✓	1.1.AL1	VIP Personnel (All Doors, Always)
✓	1.1.AL2	RRT / SWAT (All Doors, Always)
	1.1.AL3	Personnel Access (All Doors, Personnel Schedule)
	1.1.AL4	Janitorial (Employee Entrance, Weekend Schedule)
✚	1.1.AL5	VIP 2

2. **Enter** a Group Name for the legacy access level group.
3. If desired, **enter** a Description.
4. **Click** the Modify Levels button.

   The Assign Access Levels dialog appears.
5. **Select** the Assigned column for the desired Access Level(s).

   A ✚ appears in the Assigned column.

   If the access level is already assigned to the group, a ✓ will auto-populate in the Assigned column.
6. **Click** OK; the access level is added to the Group Access Level Members section.
7. **Click** OK to save the Group Properties dialog.

   The Legacy Access Level Group appears in the browser.

   Legacy Access Level Groups are designated by a folder with a blue access level icon.

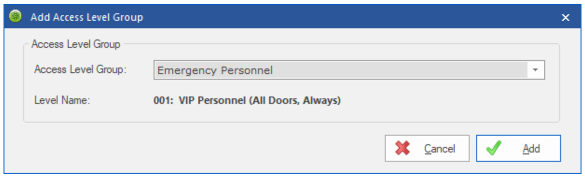
Adding a Legacy Access Level to a Group

In addition to the method above, legacy access levels can also be added to an Access Level Group through the Access Levels Browser.

1. **Right-click** on the desired Legacy Access Level and **select** Add to Group.

   The Add Access Level Group dialog appears.
2. **Select** the Access Level Group and **click** Add.

   The access level is added to the group. If a global access level group was selected, all of the doors/elevators assigned to the legacy access level will be added to the global access level group.



Access Level Group: Emergency Personnel

Level Name: **001: VIP Personnel (All Doors, Always)**

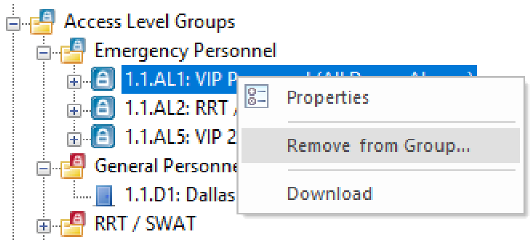
> *Alternatively, the operator can drag and drop the legacy access level into the access level group via the* Access Levels Browser.

Editing a Legacy Access Level Group

1. **Right-click** on the desired Legacy Access Level Group and **select** Properties.
2. **Edit** the Access Level Group:
   - To add an access level: **Click** the Assigned column next to the desired Access Level. A ✚ appears in the Assigned column.
   - To remove an access level: If the access level is already assigned to the group, a ✓ will appear in the Assigned column. **Click** the ✓ icon to remove the access level and a ▬ will be displayed.
3. **Click** OK to save the changes.

Removing a Legacy Access Level from a Group

1. In the Access Levels Browser, **right-click** on the desired Legacy Access Level under the Legacy Access Level Group and **select** Remove from Group.



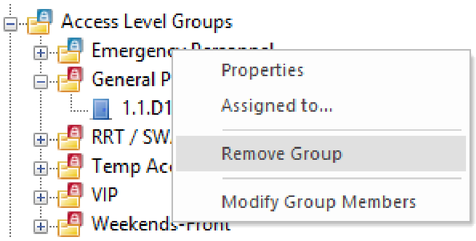
The Access Level is removed from the group.

Deleting a Legacy Access Level Group

1. **Right-click** on the Legacy Access Level Group and **select** Remove Group.

   A confirmation dialog will appear.
2. **Click** Yes to confirm the deletion.

   The Access Level Group is removed from the browser.



ⓘ Legacy Access Level Groups *have a number of features. See page 6-19 for information.*

Creating a Legacy Elevator Access Level

If elevators are configured in the system, an access level must be assigned to the appropriate floor group. Creating an elevator access level is a three-step process:

1. **Create** the Floor Group.
2. **Create** the Access Level.
3. **Link** the Floor Group to the Access Level.

> Global Access Level Groups *can be created to group doors and elevators from multiple controllers. See page 6-3 for more information.*

Creating a Floor Group

Floor groups are used to assign access to certain floors during specific hours. The floor group is then associated with an access level, which is assigned to card to grant access to the building's floors.

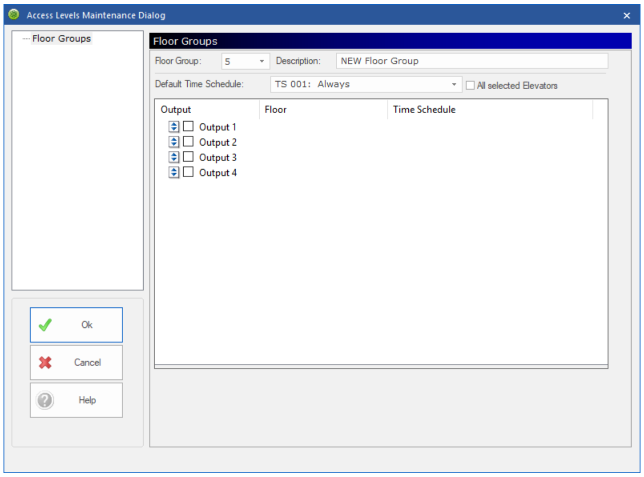
1. **Click** the Access Levels button on the Standard Toolbar.

   OR

   Select View / Explorers / Access Levels from the Main Menu.

   The Access Levels Browser opens.
2. **Select** the Floor Groups tab at the bottom of the browser.
3. **Expand** the Floor Groups tree to the desired Controller.
4. **Right-click** on the Controller with the elevator(s) and **select** Add Floor Group.

   The Access Levels Maintenance Dialog opens on the Floor Groups screen.



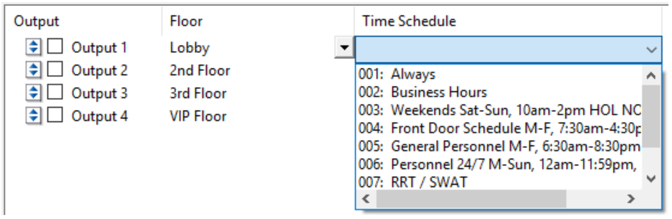
Floor Group: 5
Description: NEW Floor Group
Default Time Schedule: TS 001: Always
□ All selected Elevators

Output	Floor	Time Schedule
□ Output 1		
□ Output 2		
□ Output 3		
□ Output 4		

5. **Enter** a Description for the floor group.
6. **Select** a Default Time Schedule to apply to the floor group.
7. If desired, **check** All Selected Elevators to apply the Default Time Schedule to all selected elevators.

   This option overrides any time schedules selected for individual outputs below.
8. In the Output/Floor columns, **select** the Output(s)/Floor(s) that will be assigned to the floor group.

   Floor Names can be edited in the Controller Properties / Stored Quantities dialog; see page 8-52.
9. If desired, **select** an individual Time Schedule from the drop-down to associate with each output.



Output	Floor	Time Schedule
□ Output 1	Lobby	
□ Output 2	2nd Floor	
□ Output 3	3rd Floor	
□ Output 4	VIP Floor	

001: Always
002: Business Hours
003: Weekends Sat-Sun, 10am-2pm HOL NC
004: Front Door Schedule M-F, 7:30am-4:30p
005: General Personnel M-F, 6:30am-8:30pm
006: Personnel 24/7 M-Sun, 12am-11:59pm,
007: RRT / SWAT

10. **Click** OK to save the Floor Group.

Editing a Floor Group

1. In the Access Levels Browser, **right-click** on the Floor Group and **select** Properties.
2. **Edit** the Floor Group as needed.
3. **Click** OK to save the changes.

Deleting a Floor Group

1. In the Access Levels Browser, **right-click** on the Floor Group and **select** Remove Floor Group.

   A confirmation dialog appears.
2. **Click** Yes to confirm the deletion.

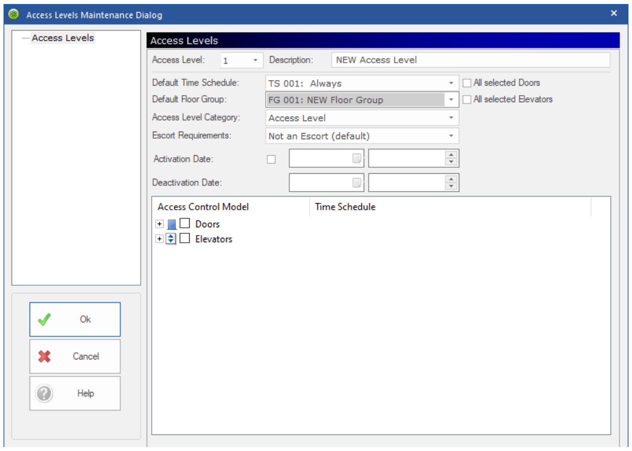
   The Floor Group is removed from the browser.

Creating the Access Level

Once the floor group has been configured, create or edit the access level and link the floor group to the access level. A single access level can include both door and elevator objects.

1. **Select** the Access Levels tab at the bottom of the Access Levels Browser.
2. **Expand** the Access Levels tree, **right-click** on the Controller that contains the elevator(s), and **select** Add Legacy Access Level.

   The Access Levels Maintenance Dialog opens.



Access Levels Maintenance Dialog

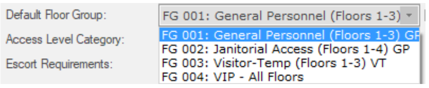
Access Levels

Access Level: 1
Description: NEW Access Level
Default Time Schedule: TS 001: Always
Default Floor Group: FG 001: NEW Floor Group
Access Level Category: Access Level
Escort Requirements: Not an Escort (default)
Activation Date:
Deactivation Date:
□ All selected Doors
□ All selected Elevators

Access Control Model	Time Schedule
+ □ Doors	
+ □ Elevators	

3. **Enter** a Description for the access level.
4. If the Access Level will include doors, **select** a Default Time Schedule for the doors.
5. **Select** a Default Floor Group to associate with the Elevator(s).

   This selection will determine the floors that the cardholder can access as well as the days and times they have access.



Default Floor Group: FG 001: General Personnel (Floors 1-3)
Access Level Category:
Escort Requirements:

FG 001: General Personnel (Floors 1-3) GP
FG 002: Janitorial Access (Floors 1-4) GP
FG 003: Visitor-Temp (Floors 1-3) VT
FG 004: VIP - All Floors

6. If desired, **check** All Selected Elevators to apply the selected floor group to all elevators.

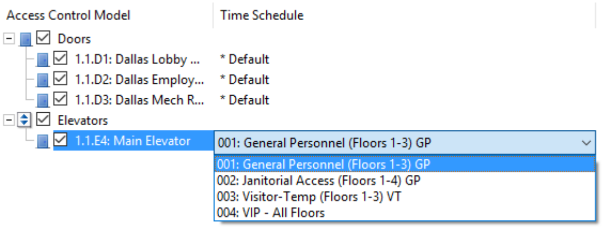
   This option overrides any floor groups selected for individual elevators.
7. **Select** the Access Level Category to assign to the access level.

   The operator's privileges determine which access level categories are available; see page 4-12.
8. In the Access Control Model column, **expand** the Elevators option and **select** the elevator(s).

   To select all the elevators, **check** the main Elevators header.
9. If the Access Level will include doors, **expand** the Doors option and **select** the door(s).

   To select all the doors, **check** the main Doors header.
10. If desired, **select** a Time Schedule/Floor Group for each ACM from the drop-down menu.

    This setting applies a specific time schedule/floor group to the selected door or elevator.



Access Control Model	Time Schedule
− ☑ Doors	
☑ 1.1.D1: Dallas Lobby ...	* Default
☑ 1.1.D2: Dallas Employ...	* Default
☑ 1.1.D3: Dallas Mech R...	* Default
− ☑ Elevators	
☑ 1.1.E4: Main Elevator	001: General Personnel (Floors 1-3) GP

001: General Personnel (Floors 1-3) GP
002: Janitorial Access (Floors 1-4) GP
003: Visitor-Temp (Floors 1-3) VT
004: VIP - All Floors

11. **Click** OK to save the access level.
12. **Right-click** on the Controller in the Access Levels Browser and **select** Download.

> ⓘ *An elevator's* Floor Groups *can also be added to existing* Access Level Groups*.*

NOTES:

Advanced Access Level Features

Escort Required Access Levels

The Escort Requirement feature restricts the cardholder's access unless another cardholder with an Escort access level badges after them. To use this feature, the operator must create at least two access levels: Is an Escort and Requires an Escort.

Once a Requires an Escort card is presented to a reader, the escort has 15 seconds to present an Is An Escort card before the system logs an Access Denied: No Escort Present event.

Creating a Global Escort Required Access Level

A global escort requirement affects doors and elevators across multiple controllers.

1. **Click** the Access Levels button on the Standard Toolbar.

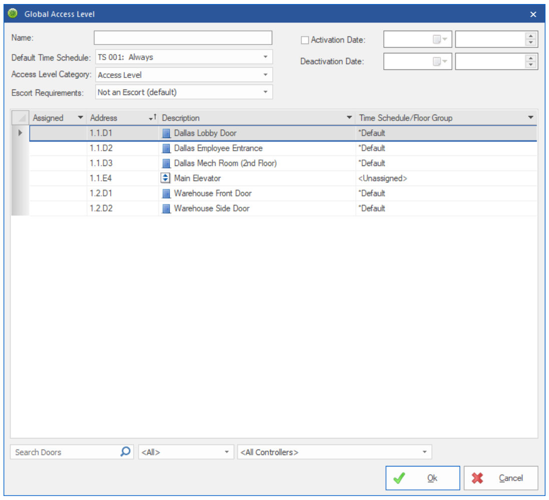
   OR

   Select View / Explorers / Access Levels from the Main Menu.

   The Access Levels Browser opens.

2. **Right-click** on the Access Level Groups header and **select** Add Global Access Level Group.

   The Global Access Level dialog opens.



Global Access Level

Name:

Default Time Schedule: TS 001: Always

Access Level Category: Access Level

Escort Requirements: Not an Escort (default)

□ Activation Date:

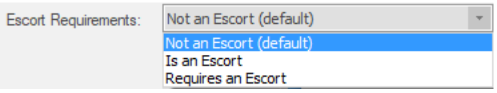
Deactivation Date:

Assigned	Address	Description	Time Schedule/Floor Group
	1.1.D1	Dallas Lobby Door	*Default
	1.1.D2	Dallas Employee Entrance	*Default
	1.1.D3	Dallas Mech Room (2nd Floor)	*Default
	1.1.E4	Main Elevator	<Unassigned>
	1.2.D1	Warehouse Front Door	*Default
	1.2.D2	Warehouse Side Door	*Default

3. **Enter** a Name for the access level.
4. **Select** a Default Time Schedule to apply to the selected ACM(s).
5. **Select** an Access Level Category to assign to the access level.

   The operator's privileges determine which access level categories are available; see page 4-12.

6. **Select** the desired Escort Requirement for the access level.
   - Not an Escort (Default) - No escort requirement.
   - Is an Escort - A cardholder with this access level will have access to the selected entry point(s) during the selected time schedule.
   - Requires an Escort - A cardholder with this access level will not have access to the selected entry point(s) unless an Escort cardholder badges after them.



Escort Requirements: Not an Escort (default)

7. In the Assigned column, **select** the doors and/or elevators that will receive the access level.
8. If desired, **select** an individual Time Schedule/Floor Group for each ACM.
9. **Click** OK to save the access level.
10. **Right-click** on the Controller in the Access Levels Browser and **select** Download.

Creating a Legacy Escort Required Access Level

A legacy escort requirement is created at the controller level; it only affects ACMs for a single SSP controller.

1. **Click** the Access Levels button on the Standard Toolbar.

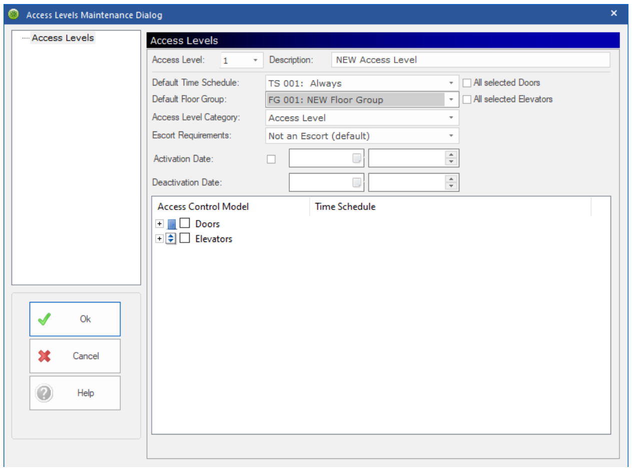
   OR

   Select View / Explorers / Access Levels from the Main Menu.

   The Access Levels Browser opens.

2. **Expand** the Access Levels tree, **right-click** on the Controller that contains the entry point(s), and **select** Add Access Level.

   The Access Levels Maintenance Dialog opens.



Access Level: 1
Description: NEW Access Level
Default Time Schedule: TS 001: Always
Default Floor Group: FG 001: NEW Floor Group
Access Level Category: Access Level
Escort Requirements: Not an Escort (default)
Activation Date: □
Deactivation Date:
□ All selected Doors
□ All selected Elevators

3. **Enter** a Description for the access level.
4. **Select** a Default Time Schedule to apply to the selected ACM(s).
5. If desired, **check** All Selected Doors to apply the Default Time Schedule to all doors.

   This option overrides any time schedules selected for individual doors.

6. If the Access Level will include elevators, **select** a Default Floor Group to associate with the Elevator(s).

   This selection will determine the floors that the cardholder can access as well as the days and times they have access.

7. If desired, **check** All Selected Elevators to apply the selected floor group to all elevators.

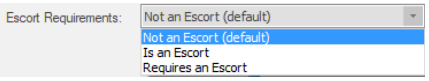
   This option overrides any floor groups selected for individual elevators.

8. **Select** the Access Level Category to assign to the access level.

   The operator's privileges determine which access level categories are available; see page 4-12.

9. **Select** the desired Escort Requirement for the access level.

   - Not an Escort (Default) - No escort requirement.
   - Is an Escort - A cardholder with this access level will have access to the selected entry point(s) during the selected time schedule.
   - Requires an Escort - A cardholder with this access level will not have access to the selected entry point(s) unless an Escort cardholder badges after them.



Escort Requirements: Not an Escort (default)

10. In the Access Control Model column, **expand** the Doors option and **select** the door(s).

    To select all the doors, **check** the main Doors header.

11. If needed, **expand** the Elevators option and **select** the elevator(s).

    To select all the elevators, **check** the main Elevators header.

12. If desired, **select** an individual Time Schedule/Floor Group for each ACM.
13. **Click** OK to save the access level.
14. **Right-click** on the Controller in the Access Levels Browser and **select** Download.

Auto-Expiring Access Levels

Auto-Expiring Access Levels will automatically activate and deactivate based on the dates specified in the access level; if needed, this feature can be paired with the Escort Requirement feature.

Creating a Global Auto-Expiring Access Level

1. **Click** the Access Levels button on the Standard Toolbar.

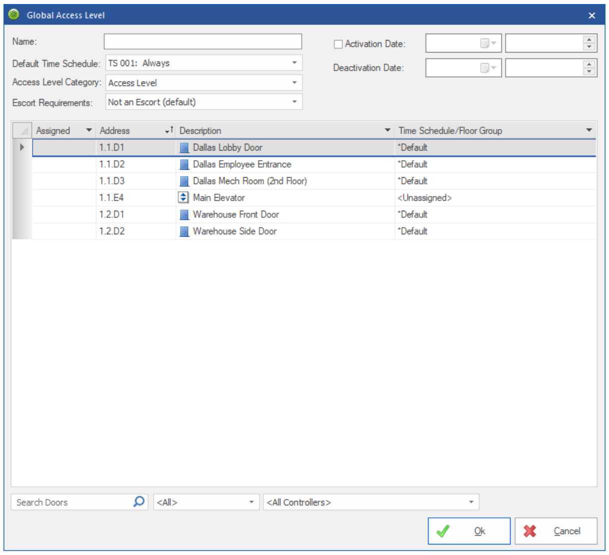
   OR

   Select View / Explorers / Access Levels from the Main Menu.

   The Access Levels Browser opens.

2. **Right-click** on the Access Level Groups header and **select** Add Global Access Level Group.

   The Global Access Level dialog opens.



Name:

Default Time Schedule: TS 001: Always

Access Level Category: Access Level

Escort Requirements: Not an Escort (default)

□ Activation Date:

Deactivation Date:

Assigned	Address	Description	Time Schedule/Floor Group
	1.1.D1	Dallas Lobby Door	*Default
	1.1.D2	Dallas Employee Entrance	*Default
	1.1.D3	Dallas Mech Room (2nd Floor)	*Default
	1.1.E4	Main Elevator	<Unassigned>
	1.2.D1	Warehouse Front Door	*Default
	1.2.D2	Warehouse Side Door	*Default

3. **Enter** a Name for the access level.

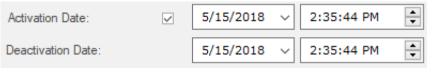
4. **Select** a Default Time Schedule to apply to the selected ACM(s).

5. **Select** an Access Level Category to assign to the access level.

   The operator's privileges determine which access level categories are available; see page 4-12.

6. **Check** the Activation Date box.

   The Activation Date and Deactivation Date fields become active.



Activation Date: ☑ 5/15/2018 2:35:44 PM

Deactivation Date: 5/15/2018 2:35:44 PM

7. **Enter** a date in the Activation Date field or **click** the down arrow to **select** from a calendar.

8. If needed, **edit** the Activation Time field.

9. **Enter** a date in the Deactivation Date field or **click** the down arrow to **select** from a calendar.

10. If needed, **edit** the Deactivation Time field.

11. In the Assigned column, **select** which ACM(s) will receive the auto-expiring access level.

12. If desired, **select** an individual Time Schedule/Floor Group option for each ACM.

13. **Click** OK to save the access level.

14. **Right-click** on the Controller in the Access Levels Browser and **select** Download.

Creating a Legacy Auto-Expiring Access Level

A legacy auto-expiring access level is created at the controller level; it only affects ACMs for a single SSP controller.

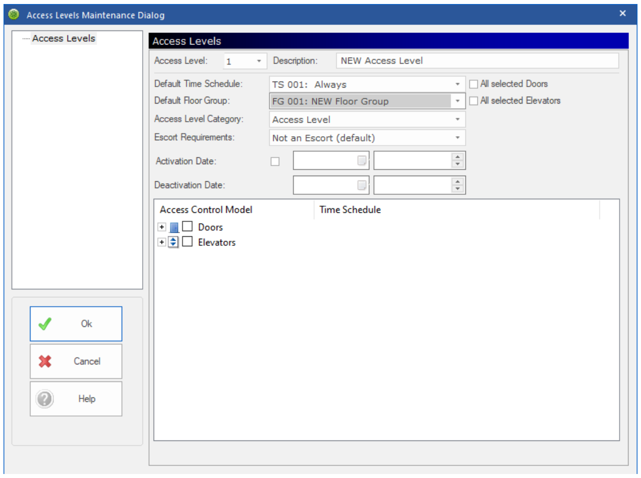
1. **Click** the Access Levels button on the Standard Toolbar.

   OR

   Select View / Explorers / Access Levels from the Main Menu.

   The Access Levels Browser appears.
2. **Expand** the Access Levels tree, **right-click** on the Controller that contains the entry point(s), and **select** Add Legacy Access Level.

   The Access Levels Maintenance Dialog opens.



Access Level: 1
Description: NEW Access Level
Default Time Schedule: TS 001: Always
☐ All selected Doors
Default Floor Group: FG 001: NEW Floor Group
☐ All selected Elevators
Access Level Category: Access Level
Escort Requirements: Not an Escort (default)
Activation Date: ☐
Deactivation Date:

Access Control Model	Time Schedule
+ ☐ Doors	
+ ☐ Elevators	

3. **Enter** a Description for the access level.
4. **Select** a Default Time Schedule to apply to the selected ACM(s).
5. If desired, **check** All Selected Doors to apply the Default Time Schedule to all doors.

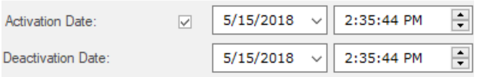
   This option overrides any time schedules selected for individual doors.
6. If the Access Level will include elevators, **select** a Default Floor Group to associate with the Elevator(s).

   This selection will determine the floors that the cardholder can access as well as the days and times they have access.
7. If desired, **check** All Selected Elevators to apply the selected floor group to all elevators.

   This option overrides any floor groups selected for individual elevators.
8. **Select** the Access Level Category to assign to the access level.

   The operator's privileges determine which access level categories are available; see page 4-12.
9. **Check** the Activation Date box.

   The Activation Date and Deactivation Date fields become active.



Activation Date: ☑ 5/15/2018 2:35:44 PM
Deactivation Date: 5/15/2018 2:35:44 PM

10. **Enter** a date in the Activation Date field or **click** the down arrow to **select** from a calendar.
11. If needed, **edit** the Activation Time field.
12. **Enter** a date in the Deactivation Date field or **click** the down arrow to **select** from a calendar.
13. If needed, **edit** the Deactivation Time field.
14. In the Access Control Model column, **expand** the Doors option and **select** the door(s).
    To select all the doors, **check** the main Doors header.
15. If needed, **expand** the Elevators option and **select** the elevator(s).
    To select all the elevators, **check** the main Elevators header.
16. If desired, **select** a Time Schedule/Floor Group for each ACM.
17. **Click** OK to save the access level.
18. **Right-click** on the Controller in the Access Levels Browser and **select** Download.

Precision Access Levels

Precision Access Levels assign specific doors to cardholders instead of access levels as described on pages 6-5 and 6-6. Precision Access Levels have a couple of drawbacks: (a) they require memory to be allocated on a per door/elevator basis, and (b) they can make it more difficult to manage and track where cardholders have access.

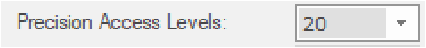
Setting Up Precision Access Levels

> Before Precision Access Levels can be assigned, they must be set up in the controller.

1. In the Hardware Browser, **right-click** on the Controller and **select** Properties.

   The Controller Properties dialog opens.

2. **Select** Stored Quantities from the dialog menu.
3. In the Quantities section, **set** the Precision Access Levels number equal to the ACM number of the last door or elevator that will be assigned to the controller's cardholders.

   Precision Access Levels: 20

   Example: If the system has 15 doors and 5 elevators but only doors 1-10 will be assigned via Precision Access Levels, the setting would be 10. If the system has 10 doors and 10 elevators but only doors 1 and 5 and elevators 10 and 20 will be assigned via Precision Access Levels, the setting would be 20 since ACM number 20 is included in the scheme.

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

   A confirmation dialog regarding memory requirements appears.

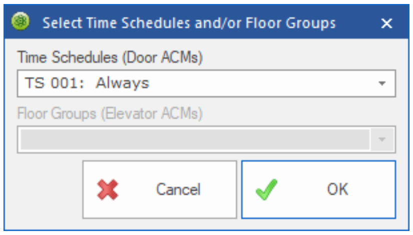
5. **Click** Yes.

   The controller resets to apply the new memory configuration. A reset temporarily causes the controller to lose communication; a full download takes place once it reconnects.

Assigning Precision Access Levels

1. **Open** the Hardware Browser and **expand** the Doors and Elevators objects.
2. **Open** the Personnel Record and **select** the Card tab.
3. **Drag** and **drop** the desired ACM (door or elevator) to the Access Levels section of the Card tab.

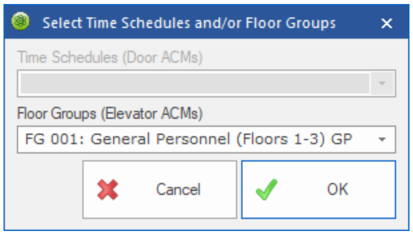
   The Select Time Schedules and/or Floor Groups dialog appears.

   Select Time Schedules and/or Floor Groups

   Time Schedules (Door ACMs): TS 001: Always

   Floor Groups (Elevator ACMs):

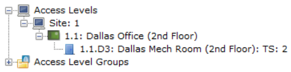
   Select Time Schedules and/or Floor Groups

   Time Schedules (Door ACMs):

   Floor Groups (Elevator ACMs): FG 001: General Personnel (Floors 1-3) GP

4. **Select** a Time Schedule for doors or Floor Group for elevators.
5. **Right-click** in the Personnel Record and **select** Update.

   The Precision Access Level appears in the Access Levels section with a door icon.

   Access Levels
Site: 1
1.1: Dallas Office (2nd Floor)
1.1.D3: Dallas Mech Room (2nd Floor): TS: 2
Access Level Groups

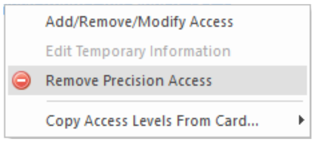
Removing Precision Access Levels

1. **Right-click** on the Precision Access Level and **select** Remove Precision Access.

   A confirmation dialog appears.

2. **Click** Yes to confirm the deletion.

   The precision access level is removed from the card.



NOTES:

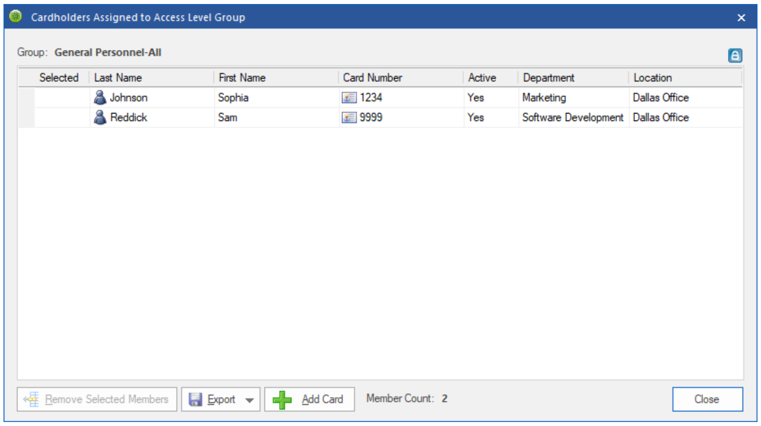
Access Level Group Features

Assigned To

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

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

   The Cardholders Assigned to Access Level Group dialog opens.



Group: General Personnel-All

Selected	Last Name	First Name	Card Number	Active	Department	Location
	Johnson	Sophia	1234	Yes	Marketing	Dallas Office
	Reddick	Sam	9999	Yes	Software Development	Dallas Office

Member Count: 2

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

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

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

Adding a Card

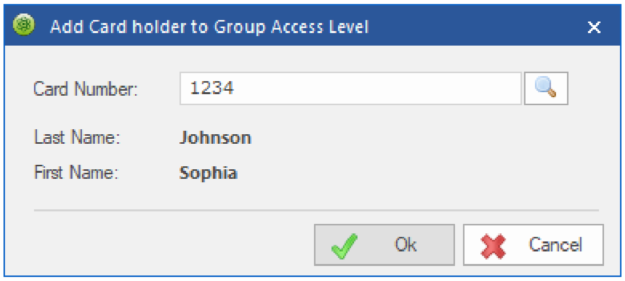
The Add Card option allows the operator to assign an access level using the card number.

1. From the Cardholders Assigned to Access Level Group dialog, **select** the Add Card button.

   The Add Cardholder to Group Access Level dialog appears.

2. **Enter** a Card Number and **select** the Search 🔍 button.

   If valid, the cardholder's First Name and Last Name will populate.



Card Number: 1234

Last Name: Johnson

First Name: Sophia

3. **Click** OK to add the card to the Access Level Group.

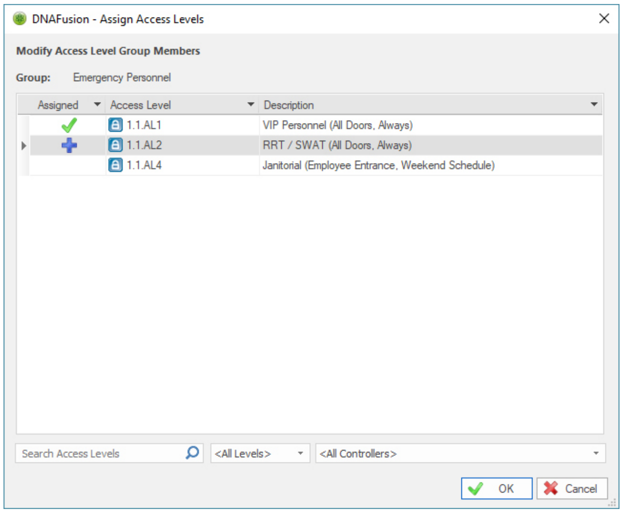
   The card information is added to the Cardholders Assigned to Access Level Group dialog and the card receives all access levels included in the access level group.

Modify Access Level Group Members

Legacy access level groups can be modified directly from the Access Levels Browser. This feature is not available for global access level groups.

1. **Right-click** on the Legacy Access Level Group in the Access Levels Browser and **select** Modify Group Members.

   The Assign Access Levels dialog opens.

   Modify Access Level Group Members

   Group: Emergency Personnel

Assigned	Access Level	Description
✓	1.1.AL1	VIP Personnel (All Doors, Always)
✚	1.1.AL2	RRT / SWAT (All Doors, Always)
	1.1.AL4	Janitorial (Employee Entrance, Weekend Schedule)

   To add an access level: **Click** the Assigned column next to the desired Access Level. A ✚ will appear in the Assigned column.

   To remove an access level: If the access level is already assigned to the group, a ✓ will appear in the Assigned column. **Click** the ✓ icon to remove the access level and a ▬ will appear.

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

Access Level Features

Assigned To

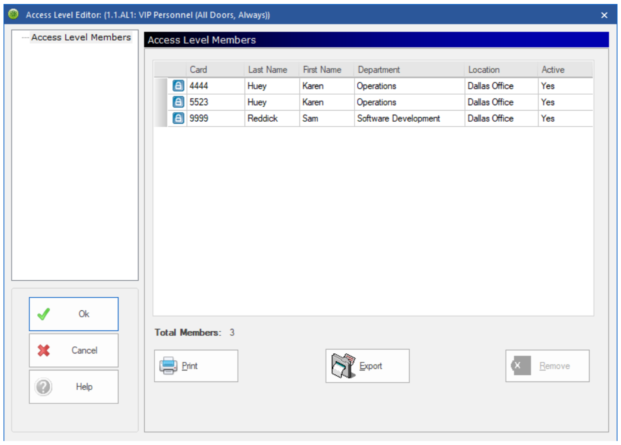
The Assigned To feature is an InfoReady report that allows the operator to audit the cardholders assigned to a legacy access level. It also provides an easy method to remove the access level from a selected card(s).

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

   OR

   Open an existing Access Level and **select** Access Level Members from the dialog menu.

   The Access Level Members dialog is displayed.

   Access Level Editor: (1.1.AL1: VIP Personnel (All Doors, Always))

   Access Level Members

Card	Last Name	First Name	Department	Location	Active
4444	Huey	Karen	Operations	Dallas Office	Yes
5523	Huey	Karen	Operations	Dallas Office	Yes
9999	Reddick	Sam	Software Development	Dallas Office	Yes

   Total Members: 3

   To remove the access level from a card, **select** the card and **click** Remove.

   A confirmation dialog will appear. **Click** Yes to remove the access level.

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

2. **Click** OK to close the dialog.

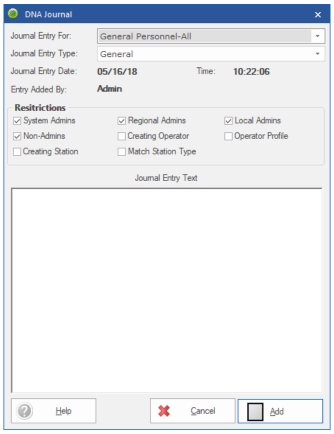
Journal Entries

The Journal feature allows the operator to record and view text entries based on operator restrictions.

Creating a New Entry

1. **Right-click** in the Access Levels Browser and **select** Journal / New Entry.

   The DNA Journal opens in entry mode.

   DNA Journal

   Journal Entry For: General Personnel-All

   Journal Entry Type: General

   Journal Entry Date: 05/16/18 Time: 10:22:06

   Entry Added By: Admin

   Resitrictions

   ☑ System Admins ☑ Regional Admins ☑ Local Admins

   ☑ Non-Admins □ Creating Operator □ Operator Profile

   □ Creating Station □ Match Station Type

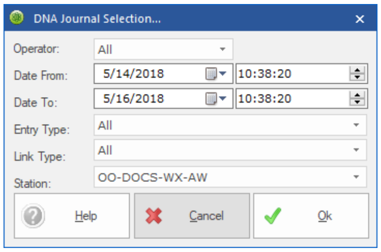
   Journal Entry Text

2. **Configure** the DNA Journal log.
   - Journal Entry For - Indicates the type of entry component; entries may be filtered by this field.
   - Journal Entry Type - Indicates a filter category for the journal entry.
   - Restrictions - Indicates who has permission to view the entry.
3. **Type** the desired message in the Journal Entry Text panel.
4. **Click** the Add button.

Viewing an Entry

1. **Right-click** in the Access Levels Browser and **select** Journal / View.

   The DNA Journal Selection dialog opens and allows the operator to filter the entries.

   DNA Journal Selection...

   Operator: All

   Date From: 5/14/2018 10:38:20

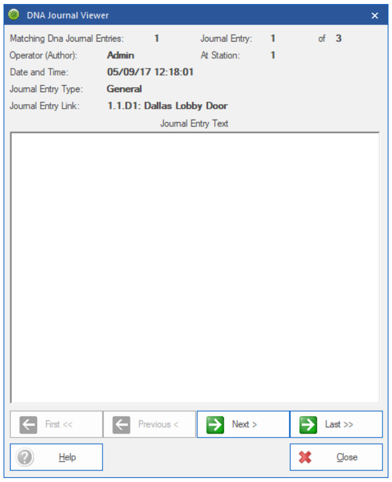
   Date To: 5/16/2018 10:38:20

   Entry Type: All

   Link Type: All

   Station: OO-DOCS-WX-AW

2. **Configure** the DNA Journal Selection dialog:
   - Operator - Filters the entries by operator name.
   - Date From/To - Filters the entries by the specified date and time range.
   - Entry Type - Filters the entries by the journal entry type.
   - Link Type - Filters the entries by the link type designated in the Journal Entry For field.
   - Station - Filters the entries by workstation.



DNA Journal Viewer

Matching Dna Journal Entries: 1 Journal Entry: 1 of 3

Operator (Author): Admin At Station: 1

Date and Time: 05/09/17 12:18:01

Journal Entry Type: General

Journal Entry Link: 1.1.D1: Dallas Lobby Door

Journal Entry Text

3. **Click** the OK button to view the results.

   The DNA Journal Viewer appears. An operator can only view entries for which the appropriate operator restriction was checked.

   The read-only fields indicate an entry's properties, including its chronological sequence, author, station of origin, date and time, entry type, and link type.

   Navigate through the entries with the green arrow buttons at the bottom of the dialog: First, Previous, Next, or Last.

4. When finished, **select** the Close button to close the dialog.

Personnel 7

In This Chapter

√ Adding and Removing Cardholders
√ Creating Personnel Groups
√ Assigning Access Levels
√ Using Cardholder Features
√ Importing Photos
√ Configuring Photo Recall Windows

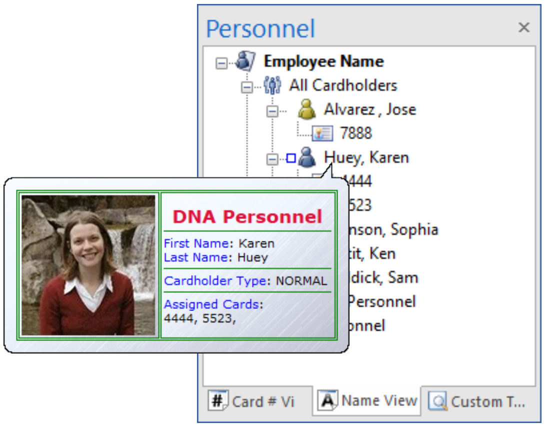
Personnel, also referred to as cardholders, are the people in the access control system who possess a card or credential that is required to access secured areas. Once an access card is added to a personnel record in DNA Fusion, the operator can assign access levels to the card. If a cardholder has multiple cards, each card will appear in a separate tab of the Personnel Record.

This chapter will explain how to add cardholders to the system, create personnel groups, and assign access levels to cards.

Personnel Browser

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

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



DNA Personnel
First Name: Karen
Last Name: Huey
Cardholder Type: NORMAL
Assigned Cards:
4444, 5523,

To open the Personnel Browser:

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

   OR

   Select View / Explorers / Personnel from the Main Menu.

   The Personnel Browser opens.

   The browser contains two default tabs (located at the bottom): Name View and Card # View. However, custom tabs can also be created; see page 3-19 for more information.

> *Hovering the cursor over a cardholder or card will display information about the object in the form of a tooltip. To enable this feature, check* Enable Tooltips *in the* Personnel Properties / Tree Properties *dialog. See page 3-21 for more information.*

Configuring the Browser

1. **Right-click** in the white area of the Personnel Browser and **select** Personnel Tree Properties.

   The Tree Properties dialog opens.

2. **Configure** the settings. See page 3-21 for more information.

Personnel Toolbar

The Personnel Toolbar provides commands and shortcuts to help manage system personnel.

Icon	Command	Description/Function
	Cardholder Properties	Opens the Personnel Record for the selected cardholder or card.
	Update Cardholder	Saves new information entered in the Personnel Record to the database.
	Add Cardholder	Opens a new personnel record in the data window.
	Remove Cardholder	Deletes the selected cardholder.
	Add Card	Adds a new card to the selected cardholder. This option is only available if a personnel record is open.
	Remove Card	Deletes the selected card from the database.
	Add Group	Opens the Group Properties dialog to create a personnel group.
	Download	Opens the Download Manager dialog to download database information (e.g. personnel) to the SSP controller.
	Use Limit	Opens the Set Use Limit Dialog to configure the use limit settings for the selected card.
	Free Pass	Opens the Set Anti-Passback Area dialog to issue a free anti-passback pass for the selected card.
	Set Flags	Opens the Card Flags dialog to set card flags, e.g. Alarm/Watch Card.
	Watch Item	Adds the selected card or cardholder to a Watch Window. This option is only available if the Watch Window is open.
	Personnel Search	Opens the Personnel SQL Builder dialog to search for cardholders that meet specific criteria. See page 3-22 for more information.
	Personnel Tabs	Opens the Personnel SQL Builder dialog to configure custom tabs in the Personnel Browser. A custom tab must be active to select this option.
	Photo Properties	Opens the Add Cardholder Photo dialog to add and remove photos for the selected cardholder. See page 7-41 for more information.
	Personnel Tree Properties	Opens the Personnel Tree Properties dialog.
	Refresh	Refreshes the Personnel Browser tree.

Managing Personnel

DNA Fusion offers a variety of personnel management features. Operators can:

- Add, edit, and remove cardholders and/or cards
- Activate and deactivate cards
- Edit multiple cards and cardholders simultaneously
- Set a card to vacation mode
- Add a block of cards

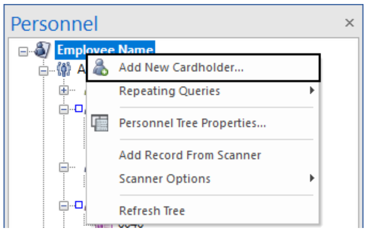
Adding Cardholders

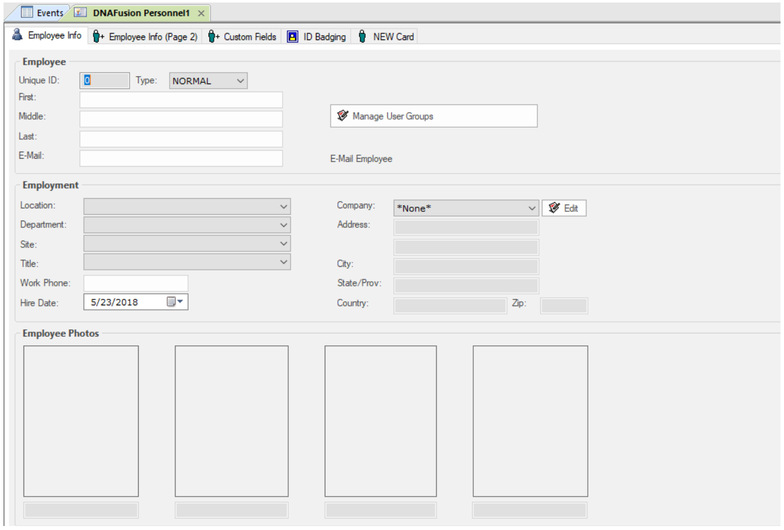
1. **Right-click** inside the Personnel Browser and **select** Add New Cardholder.

   OR

   Select Add Cardholder from the Personnel Toolbar.

   A blank Personnel Record opens.





Unique ID: 0 Type: NORMAL

Company: *None*

Hire Date: 5/23/2018

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

   See pages 7-7 through 7-12 for a description of each field and tab in the Personnel Record.

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

> ❗ *All personnel entries, whether new or modified data, must be saved to the database and downloaded to the controller. Otherwise, it will be lost upon exiting DNA Fusion and cannot be retrieved when the cardholder badges at a door. See page 7-4 for more information.*

Adding Cardholders with a Driver's License Scanner

A SnapShell or ScanShell ID Scanner can be used to create a new personnel record. The ID Scanner software development kit (SDK) must be installed on the station prior to using the scanner. Contact Open Options Technical Support to obtain the latest SDK installation file.

1. **Place** the cardholder's driver's license on the scanner.
2. **Right-click** in the Personnel Browser and **select** Add Record from Scanner.

   A new personnel record opens and auto-populates the driver's license information.
3. **Complete** the remaining personnel fields and **save** the record.

> ⓘ *The fields that will be captured during the scan are defined in the* Personnel Properties *dialog under* Drivers License Scanner Fields*. See page 3-17 for more information.*

Saving and Downloading Records

All personnel entries, whether new or modified data, must be saved to the database and downloaded to the controller. Otherwise, it will be lost upon exiting DNA Fusion and cannot be retrieved when the cardholder badges at a door.

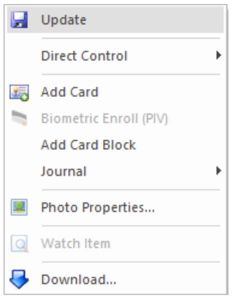
Saving a Record

1. **Click** the Update Cardholder button on the Personnel Toolbar.

   OR

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

   If a card has not been added to the Personnel Record, a confirmation dialog appears; **click** Yes to add a card or No to save the record without a card.



Downloading a Record

Records must be downloaded to the controller. The Update Cardholder option on the Personnel Toolbar will send the information to the database and the controller if an access level has been assigned to the card.

Open Options recommends performing an actual download when large amounts of information have been entered or changed.

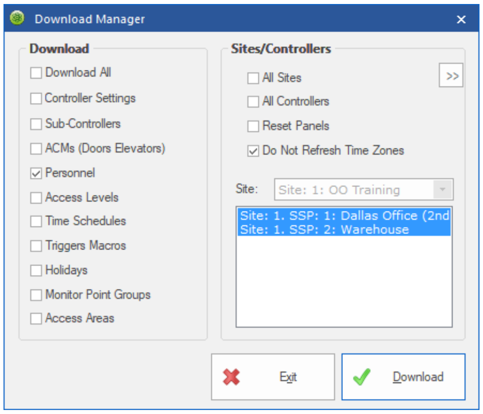
1. **Right-click** inside the Personnel Record and **select** Download.

   OR

   Click the Download button on the Personnel Toolbar.

   The Download Manager dialog opens.
2. **Select** the Personnel button.
3. **Select** the Site(s).
4. **Click** Download.

   A status bar will indicate the download's progress; **click** the Exit button to close the window without affecting the download.



Download
☐ Download All
☐ Controller Settings
☐ Sub-Controllers
☐ ACMs (Doors Elevators)
☑ Personnel
☐ Access Levels
☐ Time Schedules
☐ Triggers Macros
☐ Holidays
☐ Monitor Point Groups
☐ Access Areas

Sites/Controllers
☐ All Sites
☐ All Controllers
☐ Reset Panels
☑ Do Not Refresh Time Zones

Site: Site: 1: OO Training

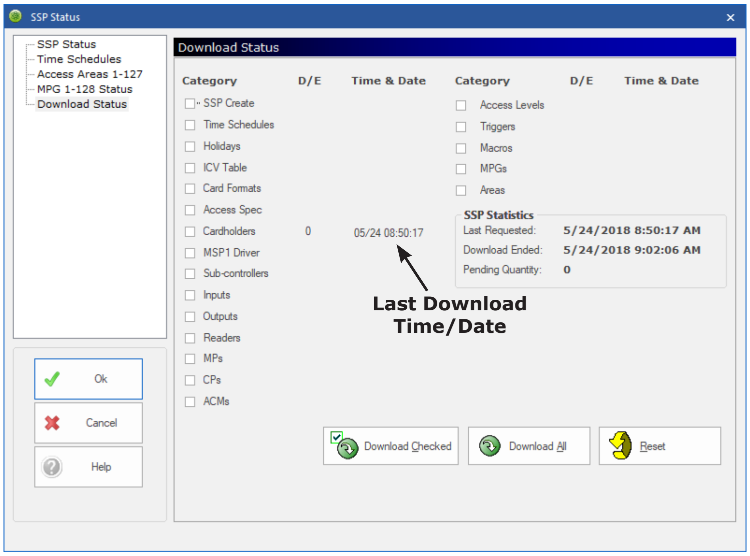
Site: 1. SSP: 1: Dallas Office (2nd
Site: 1. SSP: 2: Warehouse

Verifying the Last Download

The Download Status dialog can be used to verify the time and date of the last personnel download.

1. In the Hardware Browser, **right-click** on the Controller and **select** Status.

   The SSP Status dialog opens.
2. **Select** Download Status from the dialog menu.
3. **Locate** the Cardholders category to verify the time and date of the last download.



Category	D/E	Time & Date	Category	D/E	Time & Date
☐ SSP Create			☐ Access Levels		
☐ Time Schedules			☐ Triggers		
☐ Holidays			☐ Macros		
☐ ICV Table			☐ MPGs		
☐ Card Formats			☐ Areas		
☐ Access Spec					
☐ Cardholders	0	05/24 08:50:17			
☐ MSP1 Driver					
☐ Sub-controllers					
☐ Inputs					
☐ Outputs					
☐ Readers					
☐ MPs					
☐ CPs					
☐ ACMs					

SSP Statistics
Last Requested: 5/24/2018 8:50:17 AM
Download Ended: 5/24/2018 9:02:06 AM
Pending Quantity: 0

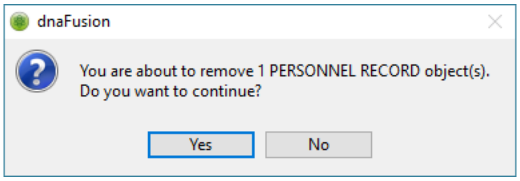
Removing Cardholders

When a cardholder is deleted, their record is moved so that the information is still retrievable but the cardholder is no longer visible in the Personnel Browser.

1. **Right-click** on the cardholder and **select** Remove Cardholder.

   A confirmation dialog appears.
2. **Click** Yes to remove the cardholder.

   The cardholder is removed from the Personnel Browser.



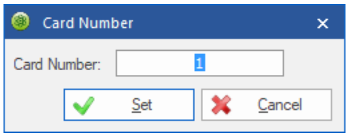
You are about to remove 1 PERSONNEL RECORD object(s).
Do you want to continue?

Adding Cards

1. **Right-click** in the Personnel Record and **select** Add Card.

   The Card Number dialog appears.
2. **Enter** the Card Number and **click** Set.

   The new card will appear as an additional tab in the record.



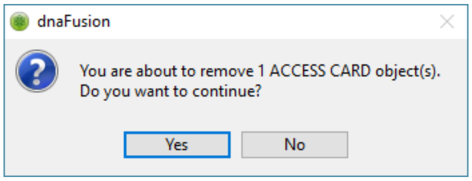
Card Number: 1

Removing Cards

When a card is deleted from a record, the card's events are still retrievable but the card no longer appears in the Personnel Browser.

1. **Open** the Personnel Record and **select** the desired Card.
2. **Right-click** in the record and **select** Remove Card.

   A confirmation dialog appears.
3. **Click** Yes to remove the card.



You are about to remove 1 ACCESS CARD object(s).
Do you want to continue?

> *Alternatively,* **right-click** *on the* Card *in the* Personnel Browser *and* **select** Remove Card*.*

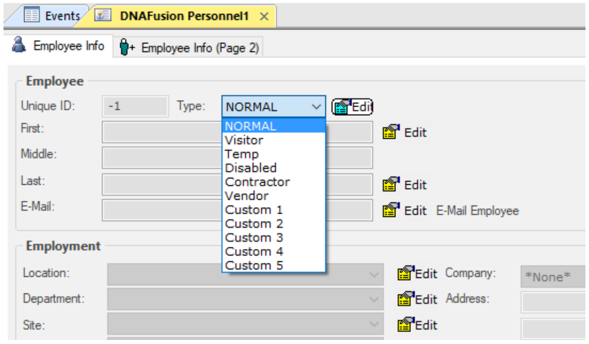
Editing Multiple Cardholders and Cards

Multiple cardholders or cards can be edited simultaneously; this includes the Personnel/Card Type as well as changing the Deactivation date.

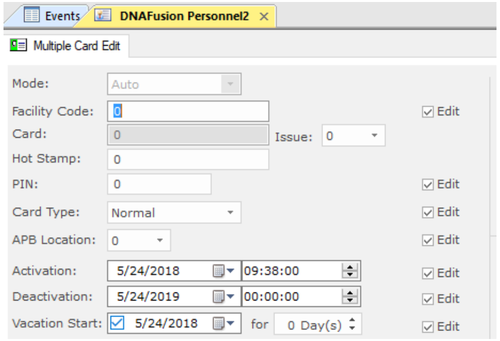
1. **Select** the cardholders or cards using the Control or Shift keys.
2. **Right-click** on one of the selections and **select** Properties.

   The Personnel Record appears.
3. **Select** Edit next to the desired field(s).

   The field(s) will become active.



Unique ID: -1 Type: NORMAL
First:
Middle:
Last:
E-Mail:
Location:
Department:
Site:
Company: *None*
Address:



Mode: Auto
Facility Code: 0
Card: 0 Issue: 0
Hot Stamp: 0
PIN: 0
Card Type: Normal
APB Location: 0
Activation: 5/24/2018 09:38:00
Deactivation: 5/24/2019 00:00:00
Vacation Start: ☑ 5/24/2018 for 0 Day(s)

4. **Edit** the information as needed.
5. **Right-click** inside the record and **select** Update.
6. **Close** the record.

Activating Cards

The following methods can be used to activate or reactivate a card:

- **Right-click** on the Card and **select** Direct Control / Activate Card. (7-37)
- **Select** the Activate Card checkbox in the Card tab of the Personnel Record. (7-12)
- **Right-click** on a card event in the Events Grid and **select** Personnel / Activate Card. (14-7)
- **Set** the Activation date in the Card tab of the Personnel Record. (7-11)

Deactivating Cards

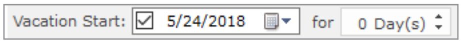
The following methods can be used to deactivate a card:

- **Right-click** on the Card and **select** Direct Control / Deactivate Card. (7-37)
- **Deselect** the Activate Card checkbox in the Card tab of the Personnel Record. (7-12)
- **Set** the Card Type to Disabled in the Card tab of the Personnel Record. (7-11)
- **Right-click** on a card event in the Events Grid and **select** Personnel / Deactivate Card (14-7)
- **Deactivate** from the Non-Use Report. (7-39)
- **Deactivate** an existing card when a new card is added. (7-21)
- **Deactivate** an existing card when a new badge is printed. (3-25)

Setting Cards to Vacation Mode

Cards can be temporarily deactivated during a cardholder's vacation time. The feature must be configured in the Controller Properties / Stored Quantities dialog. See page 8-53 for more information.

1. From the Card tab of the Personnel Record, **check** the Vacation Start box.
2. **Enter** the desired Start Date or **select** the date from the drop-down calendar.
3. **Select** the number of vacation days.
4. **Update** the Personnel Record.



Vacation Start: ☑ 5/24/2018 for 0 Day(s)

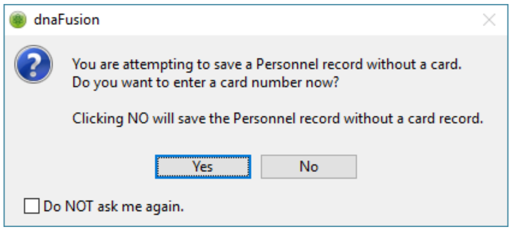
Adding Card Blocks

The operator can add a block of cards with consecutive card numbers to a personnel record.

1. **Create** a new cardholder without a card.

   See page 7-3 for instructions on adding cardholders.
2. **Enter** the cardholder information on the Employee Info tabs only.
3. **Right-click** in the record and **select** Update.

   A confirmation dialog will appear.

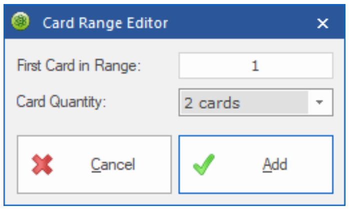


You are attempting to save a Personnel record without a card.
Do you want to enter a card number now?

Clicking NO will save the Personnel record without a card record.

4. **Click** No.
5. **Right-click** in the record and **select** Add Card Block.

   The Card Range Editor dialog appears.



First Card in Range: 1

Card Quantity: 2 cards

6. **Enter** the number of the First Card in Range and **select** the Card Quantity from the drop-down list.
7. **Click** Add to add the card block to the record.
8. **Update** the record.

Personnel Record

The Personnel Record stores information about cardholders and their credentials. It contains several tabs:

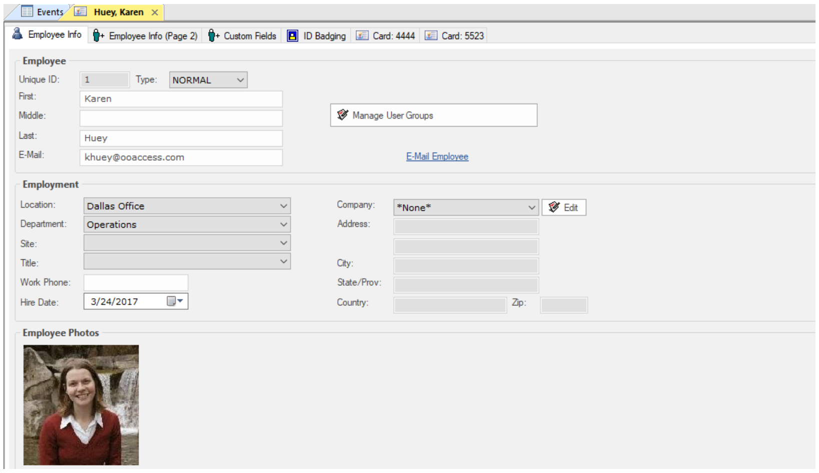
- Employee Info - General employee information.
- Employee Info (Page 2) - Personal employee information and custom fields.
- ID Badging - ID badge setup and printing. The workstation must be designated as a Badging Station in the Station Settings dialog. See page 3-3 for more information.
- Card - Card information, settings, and access levels.
- Custom Fields - Only available if Custom Fields are defined in the Personnel Properties dialog. See page 3-26 for more information.

Opening a Personnel Record

Use one of the following methods to open a personnel record:

- **Right-click** on the Cardholder or Card in the Personnel Browser and **select** Properties.
- **Double-click** on the Cardholder or Card in the Personnel Browser (does not work if the Expand on Double Click option is checked in the Personnel Tree Properties dialog).
- **Select** the Cardholder or Card in the Personnel Browser and **select** Personnel / Properties from the Main Menu.
- **Double-click** on the cardholder's event in the Events Grid.
- **Select** the Cardholder or Card in the Personnel Browser and **click** the Cardholder Properties option on the Personnel Toolbar.

Employee Info Tab



Employee

Unique ID: 1
Type: NORMAL
First: Karen
Middle:
Last: Huey
E-Mail: khuey@ooaccess.com

Employment

Location: Dallas Office
Department: Operations
Site:
Title:
Work Phone:
Hire Date: 3/24/2017
Company: *None*
Address:
City:
State/Prov:
Country:
Zip:

Employee

- Unique ID - A unique identification number for the cardholder. (Auto-populated)
- Type - Select a cardholder classification from the drop-down list: Normal, Visitor, Temp, Disabled, Contractor, Vendor, or Custom (1-5).

> ⓘ Custom Personnel Types *are configured in the* Personnel Properties / Custom Fields and Types *dialog. See page 3-26 for more information.*

- First / Middle / Last - Enter the cardholder's first, middle, and last names.
- E-Mail - Enter the cardholder's e-mail address.
  - □ E-Mail Employee - Opens a new e-mail to send to the cardholder's e-mail address. Requires an entry in the E-Mail field.
- Tenant - Select the cardholder's tenant group. This field is only available if Tenants is enabled on the workstation. For more information, see Chapter 13 in the DNA Fusion User Manual.
- Manage User Groups - Opens the User Groups Manager dialog to manage the cardholder's personnel groups. See page 7-28 for more information.

Employment

- Location - Select the cardholder’s work location from the predefined drop-down list.
- Department - Select the cardholder’s job department from the predefined drop-down list.
- Site - Select the cardholder’s employment site from the predefined drop-down list.
- Title - Select the cardholder’s job title from the predefined drop-down list.

> **Right-click** in the Location, Department, Site, or Title field and **select** Add Text to configure the drop-down options.

- Work Phone - Enter the cardholder’s work phone number.
- Hire Date - Enter the cardholder’s hire date (m/dd/yyyy) or select the date from the calendar. By default, this field auto-populates with the date that the personnel record was created.
- Company - Select the cardholder’s company from the predefined drop-down list. If address information is associated with the selected company, it will auto-populate in the Address, City, State/Prov, Country, and Zip fields.
  - Edit - Opens the Company Editor dialog to add, edit, and remove company information. See the Company Editor section below for more information.

Employee Photos

Displays up to four (4) cardholder photos. See page 7-41 for information on importing photos to a personnel record.

Company Editor

The Company Editor dialog is used to add, edit, and remove company information.

To add a company:

1. From the Personnel Record, **click** the Edit button next to the Company field.

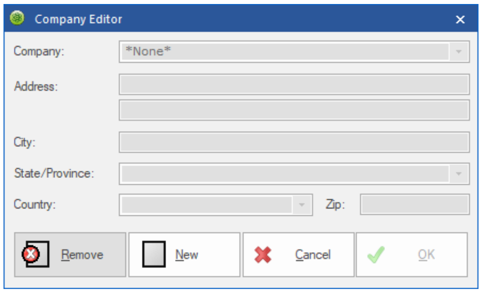
   The Company Editor dialog appears.

2. **Click** the New button to add a company.

   A prompt will appear.

3. **Click** Yes to clear the fields or No to keep the information.
4. **Enter** the information in the fields:
   - Company - Company’s name.
   - Address - Company’s address.
   - City - Company’s city.
   - State/Province - Company’s state/province.
   - Country - Company’s country.
   - Zip - Company’s zip code.
5. **Click** OK to save the information.

   The company is now available from the drop-down list.



To delete a company:

1. From the Personnel Record, **select** the Company from the drop-down list and **click** the Edit button.

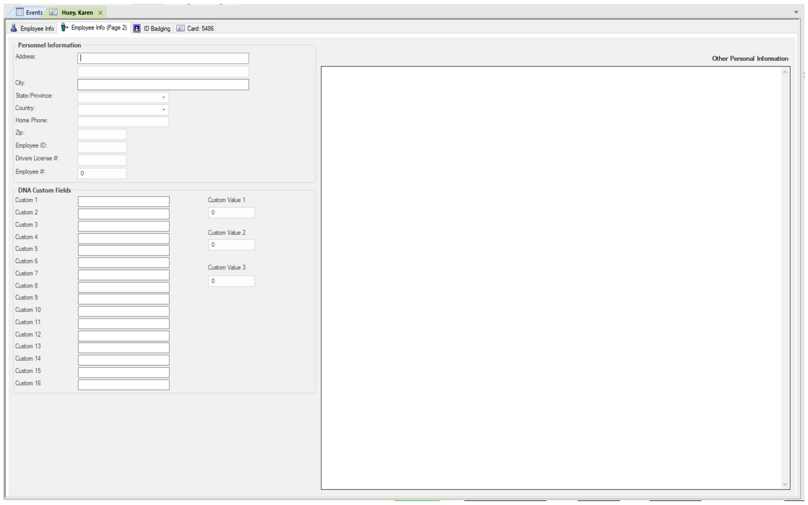
   The Company Editor dialog appears.

2. **Click** the Remove button.

   A confirmation dialog will appear.

3. **Click** Yes to delete the company.
4. **Click** OK to close the dialog.

Employee Info (Page 2) Tab



Personnel Information

Address:

City:

State/Province:

Country:

Home Phone:

Zip:

Employee ID:

Drivers License #:

Employee #: 0

DNA Custom Fields

Custom 1

Custom 2

Custom 3

Custom 4

Custom 5

Custom 6

Custom 7

Custom 8

Custom 9

Custom 10

Custom 11

Custom 12

Custom 13

Custom 14

Custom 15

Custom 16

Custom Value 1: 0

Custom Value 2: 0

Custom Value 3: 0

Other Personal Information

Personnel Information

- Address - Enter the cardholder’s street address, including the suite or apartment number.
- City - Enter the cardholder’s city of residence.
- State/Province - Enter the cardholder’s state of residence.
- Country - Enter the cardholder’s country of residence.
- Home Phone - Enter the cardholder’s home phone number.
- Zip - Enter the cardholder’s zip code.
- Employee ID - Enter the cardholder’s employee identification information. (Alphanumeric)
- Drivers License # - Enter the cardholder’s driver’s license number.
- Employee # - Enter the cardholder’s employee number. (Numeric only)

DNA Custom Fields

- Custom 1-16 - Enter alphanumeric text in the field(s).
- Custom Value 1-3 - Enter a numeric value in the field(s).

> ⓘ Custom Fields *must be defined through the* Personnel Properties / Custom Fields and Types *dialog. See page 3-26 for more information.*

Other Personal Information

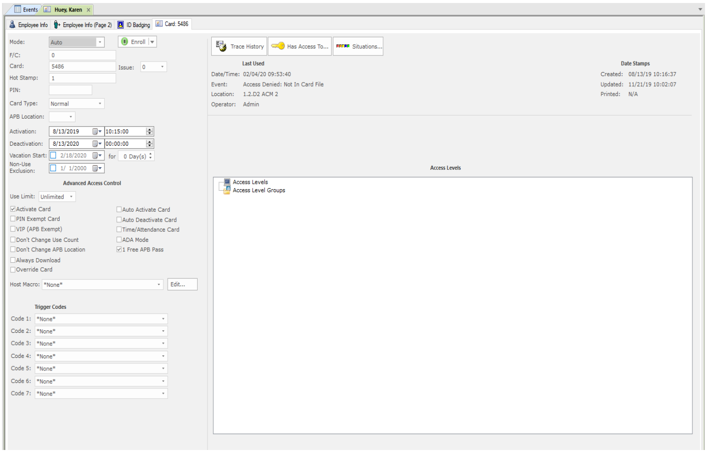
This section contains a text-entry field to store supplementary information about the cardholder.

ID Badging

See Chapter 21 for ID Badging information.

NOTES:

Card Tab



Mode: Auto

F/C: 0

Card: 5486   Issue: 0

Hot Stamp: 1

PIN:

Card Type: Normal

APB Location:

Activation: 8/13/2019 10:15:00

Deactivation: 8/13/2020 00:00:00

Vacation Start: □ 2/18/2020 for 0 Day(s)

Non-Use Exclusion: □ 1/ 1/2000

Advanced Access Control

Use Limit: Unlimited

☑ Activate Card
□ PIN Exempt Card
□ VIP (APB Exempt)
□ Don't Change Use Count
□ Don't Change APB Location
□ Always Download
□ Override Card
□ Auto Activate Card
□ Auto Deactivate Card
□ Time/Attendance Card
□ ADA Mode
☑ 1 Free APB Pass

Host Macro: *None*

Trigger Codes

Code 1: *None*
Code 2: *None*
Code 3: *None*
Code 4: *None*
Code 5: *None*
Code 6: *None*
Code 7: *None*

Last Used

Date/Time: 02/04/20 09:53:40
Event: Access Denied: Not In Card File
Location: 1.2.D2 ACM 2
Operator: Admin

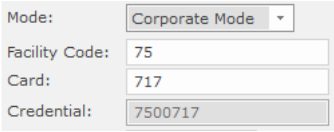
Date Stamps

Created: 08/13/19 10:16:37
Updated: 11/21/19 10:02:07
Printed: N/A

Access Levels

Access Levels
Access Level Groups

- Mode - Identifies the card format mode for the cardholder. This information is auto-populated based on the Default Mode setting in the Personnel Properties; see page 3-15 for more information. The Auto option should be selected unless the system is using multiple facility codes or Corporate Mode.
  - Auto - The default mode; uses the controller-stored card formats.
  - Corporate Mode - Supports multiple facility codes under each formatted bit structure. If selected, the operator must enter the card's Facility Code and Card Number. DNA Fusion will calculate the Credential number based on the Multiplier specified in the Personnel Properties dialog. [Example: Multiplier * F/C + Card # = Credential >> 1,000,000,000 x 6 = 6,000,000,000 + 449,166,208 = 6,449,166,208]
  - Multi - XX Bit Card - If selected, the operator will need to enter the card's Facility Code and Card Number. The Credential number will auto-populate based on the entered information.

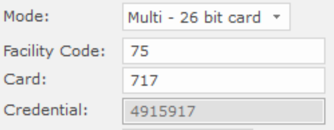


Mode: Corporate Mode

Facility Code: 75

Card: 717

Credential: 7500717



Mode: Multi - 26 bit card

Facility Code: 75

Card: 717

Credential: 4915917

- Facility Code - The number encoded in a card to distinguish it from other facilities or sites.
- Card - The card number assigned to the card. Personnel records can be added to the access control system without assigning a card to the record.
- Issue - Indicates the number of times the card has been issued to the cardholder (e.g., a replacement for a lost card). It is an internal number that is programmed on the card. If used, Store Issue Codes must be checked in the Controller Properties / Stored Quantities dialog. See pages 8-53 for more information. Issue codes can be automatically incremented; see page 3-16 for details.
- Hot Stamp - The number printed on the outside of the physical card.
- Credential - The hard-coded credential number that the system will read from the card.
- PIN - The cardholder's personal identification number; must be used at doors that require a PIN code.
- Card Type - Identifies the card classification: Normal, Visitor, Temporary, Disabled, Contractor, Vendor, Custom 1-5. If Disabled is selected, select a reason from the Why? drop-down; the card is deactivated.

> Custom Personnel/Card Types *can be set up in the* DNA Properties / Personnel Properties / Custom Fields and Types *dialog. See page 3-26 for more information.*

- APB Location - The number indicating the cardholder's anti-pass back (APB) area. If used, Store APB Location must be checked in the Controller Properties / Stored Quantities dialog.
- Activation - The card's activation date and time. Store Activation Date must be enabled in the Controller Properties / Stored Quantities dialog (enabled by default).
- Deactivation - The card's deactivation date and time. By default, the date is set for one (1) year after the Activation date. Store Deactivation Date must be enabled in the Controller Properties / Stored Quantities dialog (enabled by default).
- Vacation Start/For - The date range used to temporarily deactivate the card when the cardholder is on vacation. Store Vacation Date must be enabled in the Controller Properties / Stored Quantities dialog.
- Non-Use Exclusion - Excludes the card from Non-Use reporting.

Advanced Access Control

- Use Limit - Determines the maximum number of card uses. The default setting is Unlimited.
- Activate Card - Activates the card if checked and deactivates the card if unchecked. New cards will be active by default unless the Deactivate Card option is checked in the Personnel Properties dialog. See page 3-16 for more information.
- PIN Exempt Card - If checked, the card is exempt from any PIN requirements.
- VIP (APB Exempt) - If checked, the card is exempt from anti-pass back (APB) settings. This feature is primarily used for VIP cardholders such as presidents, CEOs, and business owners.
- Don't Change Use Count - Overrides the Use Limit setting. Do not check if Use Limit is set to Unlimited.
- Don't Change APB Location - Overrides the anti-pass back (APB) location. Do not check if the system does not use APB.
- Always Download - Downloads the card's information to the SSP controller prior to the card's first access request on any controller. This feature overrides the Download Personnel on Demand setting in the DNA Site (Driver) Configuration dialog. See page 20-3 for more information.
- Auto Activate Card - If checked, automatically activates the card when the card is presented to an Auto Activate Door.
- Auto Deactivate Card - If checked, automatically deactivates the card when the card is presented to an Auto Deactivate Door.
- Time/Attendance Card - If checked, sends specific card information to a separate database table when the card is presented to an In and Out Door. See page 8-57 for more information.
- ADA Mode - If checked, the card uses the ADA Settings designated in the Door Objects dialog to grant additional time for people with disabilities.
- 1 Free APB Pass - Permits one anti-pass back (APB) infraction before denying card access. Do not check if using VIP (APB Exempt).
- Override Cards - If checked, will allow the cardholder to bypass configured doors in the locked mode. This requires the cardholder and door to be configured with the override flag. See page 8-64 for door settings.
- Host Macro - If desired, select a Host-Based Macro from the drop-down to associate with the card.
    - Edit - Opens the Host Based Macro dialog to configure a host-based macro for the card. Host-based macros establish cause-and-effect relationships between points; see page 10-3.

Trigger Codes

- Code (1-7) - If desired, select up to seven Trigger Codes from the drop-down menus to associate with the card. See page 10-11 for more information.

Miscellaneous

- Trace History - Generates an InfoReady report of the card's transaction history for specific dates.
- Has Access To - Generates an InfoReady report that displays which doors the card can access.
- Situations - Opens the Situation Level Manager Settings dialog to disable the card during specific situation levels.
- Last Used - Displays the card's last used information, including the Date/Time, Event, Location, and Operator.
- Date Stamps - Displays the dates when the card was created, last updated, and last printed.

Access Levels

The Access Levels section contains a list of access levels assigned to the card. Operators can right-click to add, modify, and remove access. For more information on assigning and removing access levels, see page 7-13.

> **Right-click** *and* **select** Expand All *to expand all controllers and view each access level assigned to the card.*

Assigning Access Levels

For a cardholder to access an entry point, the appropriate access level must first be assigned to their card. Access levels define which entry point(s) the cardholder can access and what times access is available. Other types of access credentials, such as fobs, are referred to as "cards" throughout the system. For more information on access levels, see Chapter 6.

DNA Fusion provides various methods for assigning access levels to cards:

- Individual Card - Context Menu
- Individual Card - Card Record
- Drag and drop to an individual card or cardholder
- Copy active card access information
- Use the Temporary Access Level Upgrade feature
- Assign individual doors to a card (Precision Access Levels)
- Add the cardholder to a personnel group with default access levels
- Drag and drop access level to a personnel group
- Assign to cardholder through the Access Level / Assigned To dialog

> *Access levels can also be assigned to a cardholder when creating and modifying personnel groups. See page 7-23 for more information.*

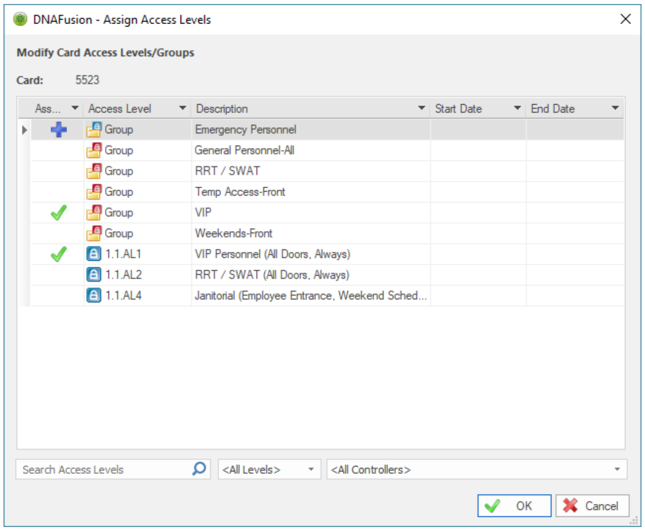
Individual Card

Access levels can be assigned to an individual card from the card's context menu or from within the Personnel Record. The operator can also drag and drop an access level to a cardholder or individual card.

Assign From the Context Menu

1. **Locate** the desired card in the Personnel Browser.
2. **Right-click** on the Card and **select** Modify Access.

   The Assign Access Levels dialog opens.

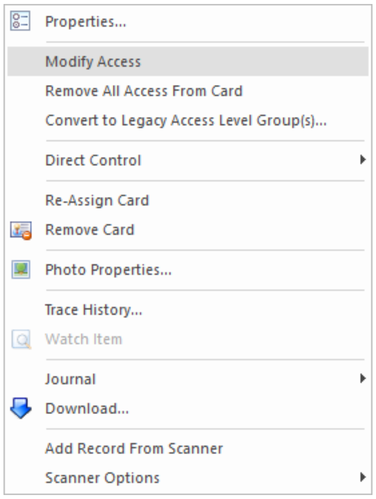


DNAFusion - Assign Access Levels

Modify Card Access Levels/Groups

Card: 5523

Ass...	Access Level	Description	Start Date	End Date
✚	Group	Emergency Personnel		
	Group	General Personnel-All		
	Group	RRT / SWAT		
	Group	Temp Access-Front		
✓	Group	VIP		
	Group	Weekends-Front		
✓	1.1.AL1	VIP Personnel (All Doors, Always)		
	1.1.AL2	RRT / SWAT (All Doors, Always)		
	1.1.AL4	Janitorial (Employee Entrance, Weekend Sched...		



- A green check ✓ indicates that the access level is already assigned to the card.
- A red minus sign ▬ indicates that the access level will be removed from the card.
- A blue plus sign ✚ indicates that the access level will be added to the card.

3. **Click** the Assigned field next to the desired access level(s).

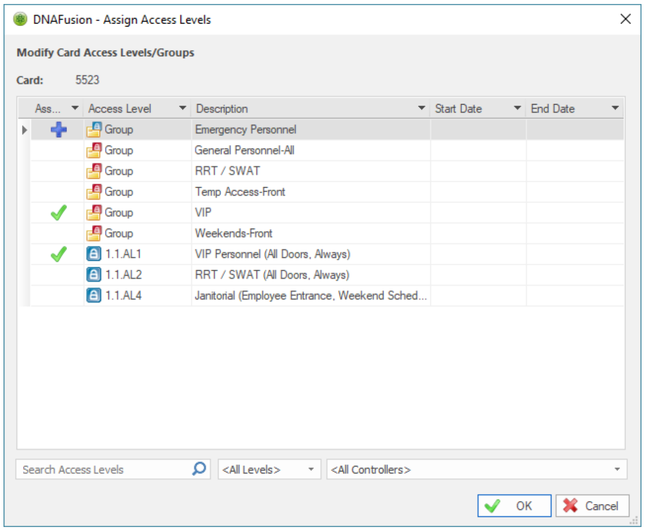
   A blue plus sign ✚ will appear next to the access level(s).
4. **Click** the OK button.

   The access level(s) are added to the card.

Assign From the Personnel Record

1. **Select** the Card tab from the Personnel Record.
2. **Right-click** inside the Access Levels section and **select** Add/Remove/Modify Access.

   The Assign Access Levels dialog opens.

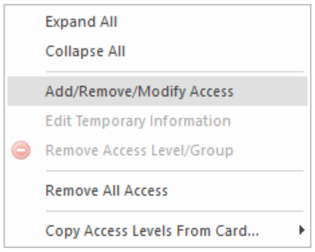


DNAFusion - Assign Access Levels

Modify Card Access Levels/Groups

Card: 5523

Ass...	Access Level	Description	Start Date	End Date
➕	Group	Emergency Personnel		
	Group	General Personnel-All		
	Group	RRT / SWAT		
	Group	Temp Access-Front		
✓	Group	VIP		
	Group	Weekends-Front		
✓	1.1.AL1	VIP Personnel (All Doors, Always)		
	1.1.AL2	RRT / SWAT (All Doors, Always)		
	1.1.AL4	Janitorial (Employee Entrance, Weekend Sched...		



Expand All
Collapse All
Add/Remove/Modify Access
Edit Temporary Information
Remove Access Level/Group
Remove All Access
Copy Access Levels From Card...

- A green check ✓ indicates that the access level is already assigned to the card.
- A red minus sign ➖ indicates that the access level will be removed from the card.
- A blue plus sign ➕ indicates that the access level will be added to the card.

3. **Click** the Assigned field next to the desired access level(s).

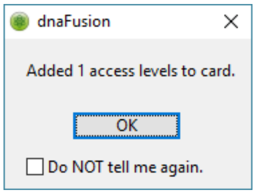
   A blue plus sign ➕ will appear next to the access level(s).
4. **Click** the OK button.

   The access level(s) are added to the card.

Drag & Drop to an Individual Card or Cardholder

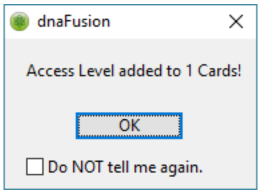
1. **Open** the Personnel Browser and the Access Levels Browser.
2. **Expand** the browser tree.
3. **Drag** and **drop** the Access Level to the desired Card or Cardholder.

   A confirmation dialog appears.



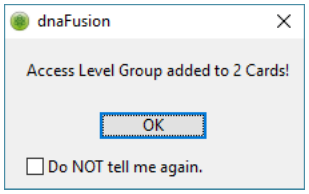
dnaFusion

Added 1 access levels to card.



dnaFusion

Access Level added to 1 Cards!



dnaFusion

Access Level Group added to 2 Cards!

> ⓘ *If the access level is dragged and dropped to a cardholder, the access level will be assigned to all of the cardholder's cards.*

4. **Click** OK.

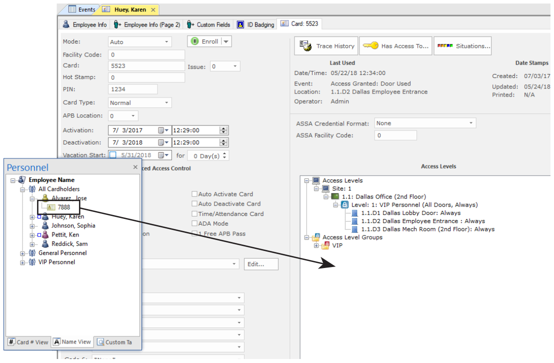
Copy Card Access

DNA Fusion provides numerous methods to distribute access levels, including copying an access level from another cardholder or card.

Copy From Another Cardholder or Card

Use one of the following methods to copy access levels:

- **Drag** a Card from the Personnel Browser to the Access Levels section of the desired Card tab.

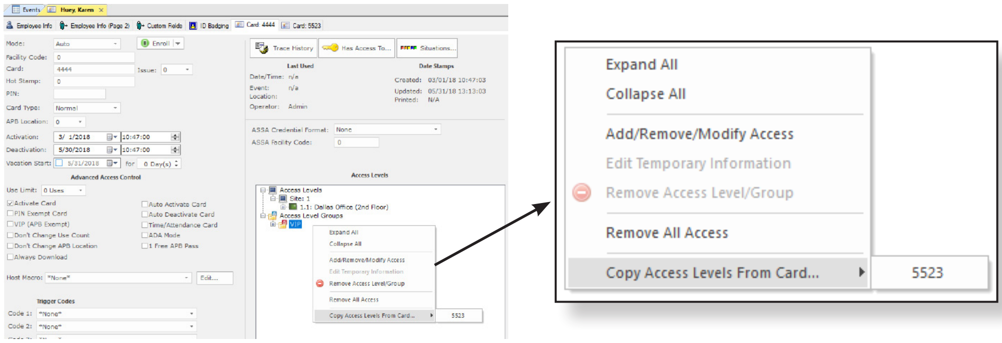
  

  1. **Open** the Personnel Record that will receive access and **select** the Card tab.
  2. In the Personnel Browser, **expand** the tree to the card with the desired access level(s).
  3. **Drag** the card with the desired access to the Access Levels section of the card that needs the access.

     The access levels are added to the card.
  4. **Right-click** in the Personnel Record and **select** Update.

- From the Card tab, **right-click** in the Access Levels section and **select** Copy Access Levels From Card.
  1. **Open** the Personnel Record and **select** the Card tab that will receive access.
  2. **Right-click** in the Access Levels section, **select** Copy Access Level From Card, and **select** the card with the desired access level(s).

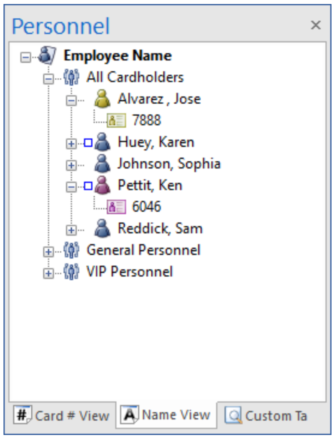
     The access levels are added to the card.

  
  Expand All
Collapse All
Add/Remove/Modify Access
Edit Temporary Information
Remove Access Level/Group
Remove All Access
Copy Access Levels From Card...
5523

  > *If the card number is grayed out,* **verify** *that the card record has been updated.*

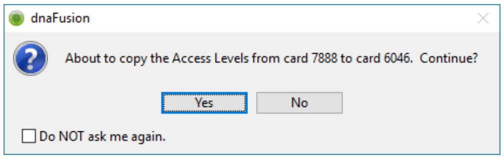
  3. **Right-click** in the record and **select** Update.

- In the Personnel Browser, **drag** the card with the desired access to the other card.

  1. **Open** the Personnel Browser and **expand** the tree to the card with the desired access.
  2. **Expand** the tree to the card that will receive the access.
  3. **Drag** the card with the desired access to the card that needs the access.

     A confirmation dialog appears.

     
     dnaFusion

     About to copy the Access Levels from card 7888 to card 6046. Continue?

     □ Do NOT ask me again.
  4. **Click** Yes to copy the access levels to the card.

     The access levels are added to the card.

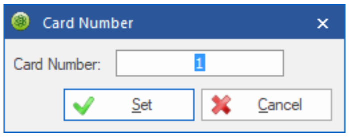
Copy Active Card Access Information

DNA Fusion can be configured to automatically assign a cardholder's active card information to a new card.

> *This feature requires the operator to check the* Copy Active Card Information to New Card *option in the* Personnel Properties *dialog. See page 3-16.*

1. **Right-click** in the Personnel Record and **select** Add Card.

   The Card Number dialog opens.

   Card Number

   Card Number: 1

2. **Enter** the Card Number and **click** Set.

   The new card appears as an additional tab in the record.

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

   The access levels from the original card are added to the new card.

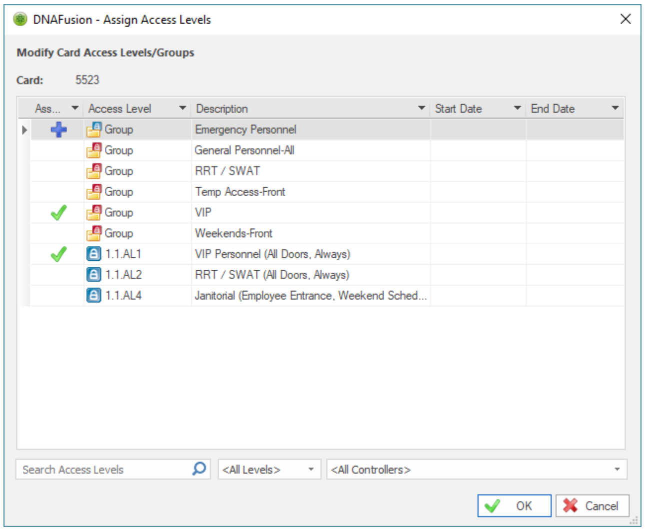
Temporary Access Level Upgrade

The Temporary Access Level Upgrade feature allows the operator to assign access levels to cards for a specified amount of time. If used, the Store Temporary Upgrade Date option must be checked in the Controller Properties dialog. See page 8-53 for more information.

Temporary Access Level Upgrades **only** work with Legacy Access Levels. The access level must be created prior to assigning a temporary access level to a card. For information on legacy access levels, see page 6-5.

1. From the Personnel Record, **select** the Card tab, **right-click** inside the Access Levels section, and **select** Add/Remove/Modify Access.

   The Assign Access Levels dialog opens.



DNAFusion - Assign Access Levels

Modify Card Access Levels/Groups

Card: 5523

Ass...	Access Level	Description	Start Date	End Date
✚	Group	Emergency Personnel		
	Group	General Personnel-All		
	Group	RRT / SWAT		
	Group	Temp Access-Front		
✓	Group	VIP		
	Group	Weekends-Front		
✓	1.1.AL1	VIP Personnel (All Doors, Always)		
	1.1.AL2	RRT / SWAT (All Doors, Always)		
	1.1.AL4	Janitorial (Employee Entrance, Weekend Sched...		

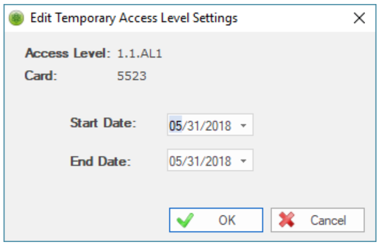
2. **Click** the Assigned field next to the desired access level(s).

   A blue plus sign ✚ will appear next to the selected access level(s).

ⓘ *Only one* Temporary (Legacy) Access Level *may be assigned per controller.*

3. **Double-click** on the selected Access Level.

   The Edit Temporary Access Level Settings dialog opens.



Edit Temporary Access Level Settings

Access Level: 1.1.AL1
Card: 5523

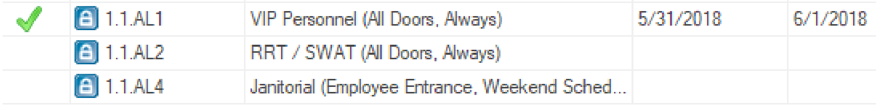
Start Date: 05/31/2018
End Date: 05/31/2018

4. **Enter** a Start and End Date or **click** the down arrows next to the Start and End Dates to select the dates from a calendar.

   A maximum of 255 days may be specified for the temporary access level.

5. **Click** OK to save the Temporary Dates.

   The dates populate in the Assign Access Levels dialog.



✓	1.1.AL1	VIP Personnel (All Doors, Always)	5/31/2018	6/1/2018
	1.1.AL2	RRT / SWAT (All Doors, Always)		
	1.1.AL4	Janitorial (Employee Entrance, Weekend Sched...		

6. **Click** OK.

   The temporary access level is added to the Access Levels section of the Card tab with a green 🔒 icon.

Editing Temporary Upgrade Dates

After a Temporary Access Level has been added to a card, the parameters can be edited from two locations: the Assign Access Levels dialog and the Card tab.

- Assign Access Levels Dialog

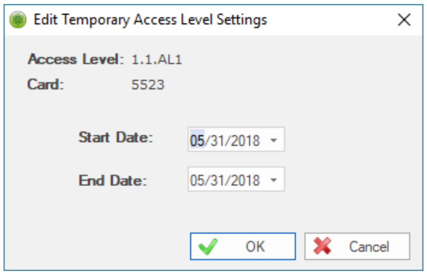
  1. **Select** the Card tab from the Personnel Record.
  2. **Right-click** in the Access Levels section and **select** Add/Remove/Modify Access.

     The Assign Access Levels dialog appears.
  3. **Double-click** on the Temporary Access Level.

     OR

     Right-click on the Temporary Access Level and **select** Edit Temporary Upgrade Dates.

     The Edit Temporary Access Level Settings dialog opens.



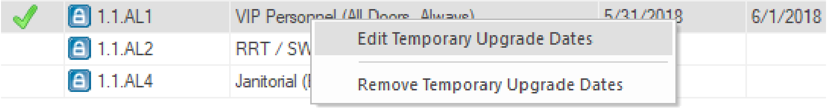
Edit Temporary Access Level Settings

Access Level: 1.1.AL1

Card: 5523

Start Date: 05/31/2018

End Date: 05/31/2018



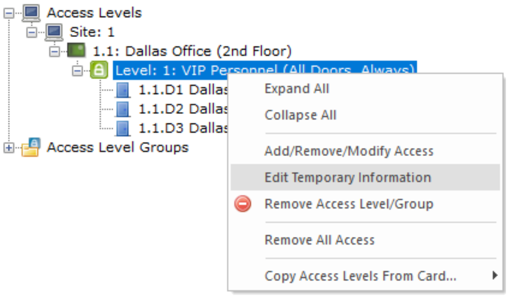
1.1.AL1	VIP Personnel (All Doors, Always)	5/31/2018	6/1/2018
1.1.AL2	RRT / SW		
1.1.AL4	Janitorial (I		

  4. **Edit** the Start Date and/or End Date.
  5. **Click** OK to save the changes.

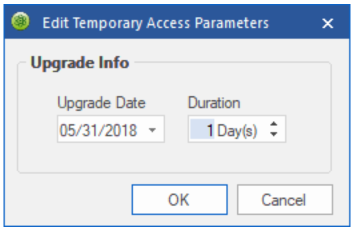
- Card Tab

  1. **Select** the Card tab in the Personnel Record.
  2. In the Access Levels section, **right-click** on the Temporary Access Level and **select** Edit Temporary Information.

     The Edit Temporary Access Parameters dialog appears.



Access Levels
Site: 1
1.1: Dallas Office (2nd Floor)
Level: 1: VIP Personnel (All Doors, Always)
1.1.D1 Dallas
1.1.D2 Dallas
1.1.D3 Dallas
Access Level Groups
Expand All
Collapse All
Add/Remove/Modify Access
Edit Temporary Information
Remove Access Level/Group
Remove All Access
Copy Access Levels From Card...



Edit Temporary Access Parameters

Upgrade Info

Upgrade Date: 05/31/2018

Duration: 1 Day(s)

  3. **Edit** the Upgrade Date or Duration as needed.
  4. **Click** OK to save the changes.

Removing Temporary Upgrade Dates

To remove the temporary upgrade dates from an access level:

1. From the Card tab of the Personnel Record, **right-click** in the Access Levels section and **select** Add/Remove/Modify Access.

   The Assign Access Levels dialog appears.
2. **Right-click** on the Temporary Access Level and **select** Remove Temporary Upgrade Dates.

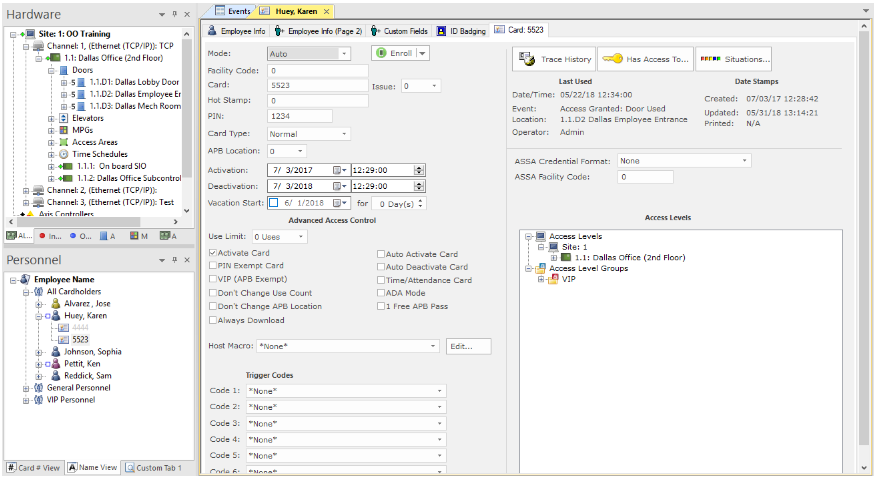
   The Start Date and End Date are removed from the access level.
3. **Click** OK to save the dialog.

Precision Access Levels

Precision Access Levels can be used to assign specific doors directly to a card without creating regular access levels.

> *Before the* Precision Access Levels *feature can be used, it must be configured in the* Controller Properties / Stored Quantities *dialog by setting the* Precision Access Levels Quantity *(see page 8-53). For example, if ACM 63 needs to be available for precision access assignment, select* 63 *from the drop-down. Precision access levels could then be assigned to all doors/elevators between 1 and 63.*

1. **Open** the Hardware Browser and **expand** the tree.
2. **Open** the desired Personnel Record and **select** the Card tab.



Mode: Auto

Facility Code: 0

Card: 5523 Issue: 0

Hot Stamp: 0

PIN: 1234

Card Type: Normal

APB Location: 0

Activation: 7/ 3/2017 12:29:00

Deactivation: 7/ 3/2018 12:29:00

Vacation Start: □ 6/ 1/2018 for 0 Day(s)

Advanced Access Control

Use Limit: 0 Uses

☑ Activate Card
□ PIN Exempt Card
□ VIP (APB Exempt)
□ Don't Change Use Count
□ Don't Change APB Location
□ Always Download
□ Auto Activate Card
□ Auto Deactivate Card
□ Time/Attendance Card
□ ADA Mode
□ 1 Free APB Pass

Host Macro: *None*

Trigger Codes

Code 1: *None*
Code 2: *None*
Code 3: *None*
Code 4: *None*
Code 5: *None*
Code 6: *None*

Last Used

Date/Time: 05/22/18 12:34:00
Event: Access Granted: Door Used
Location: 1.1.D2 Dallas Employee Entrance
Operator: Admin

Date Stamps

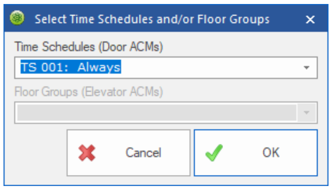
Created: 07/03/17 12:28:42
Updated: 05/31/18 13:14:21
Printed: N/A

ASSA Credential Format: None

ASSA Facility Code: 0

3. **Drag** and **drop** the Door from the Hardware Browser to the Access Levels section of the Card tab.

   The Select Time Schedules and/or Floor Groups dialog opens.

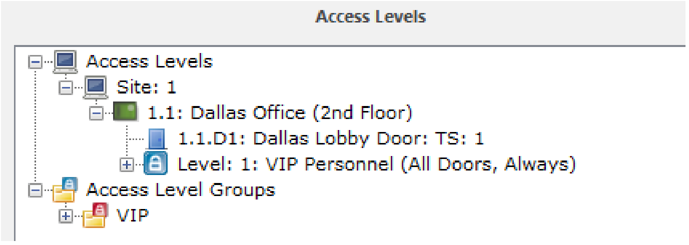


Time Schedules (Door ACMs): TS 001: Always

Floor Groups (Elevator ACMs):

4. **Select** the Time Schedule or Floor Group from the drop-down list and **click** OK.
5. **Right-click** in the Personnel Record and **select** Update.

   The door appears in the Access Levels section.


Access Levels

Access Levels
Site: 1
1.1: Dallas Office (2nd Floor)
1.1.D1: Dallas Lobby Door: TS: 1
Level: 1: VIP Personnel (All Doors, Always)
Access Level Groups
VIP

Removing Precision Access Levels

1. In the Access Levels section of the Card tab, **right-click** on the Precision Access Level and **select** Remove Precision Access.

   A confirmation dialog appears.
2. **Click** Yes to confirm.

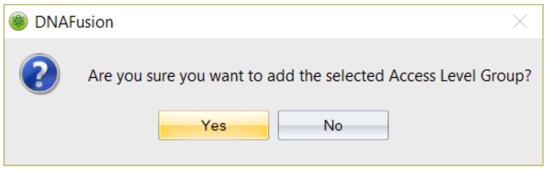
   The precision access level is removed from the card.

Add the Cardholder to a Personnel Group

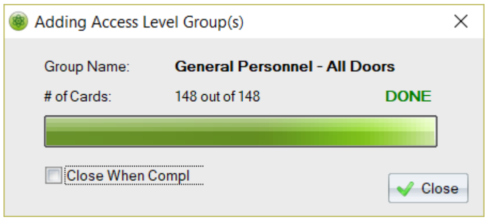
When cardholders are added to the personnel group, the default access levels are automatically assigned to their card(s). See page 7-23 for more information on personnel groups.

An access level can also be dragged and dropped to a personnel group with existing cardholders. This includes the All Cardholders group.

DNA Fusion will prompt the operator to assign the new access to the existing group members. **Click** Yes to assign the new access level(s) to the group's existing cardholders. A dialog will appear with the assignment progress.


DNAFusion

Are you sure you want to add the selected Access Level Group?


Adding Access Level Group(s)

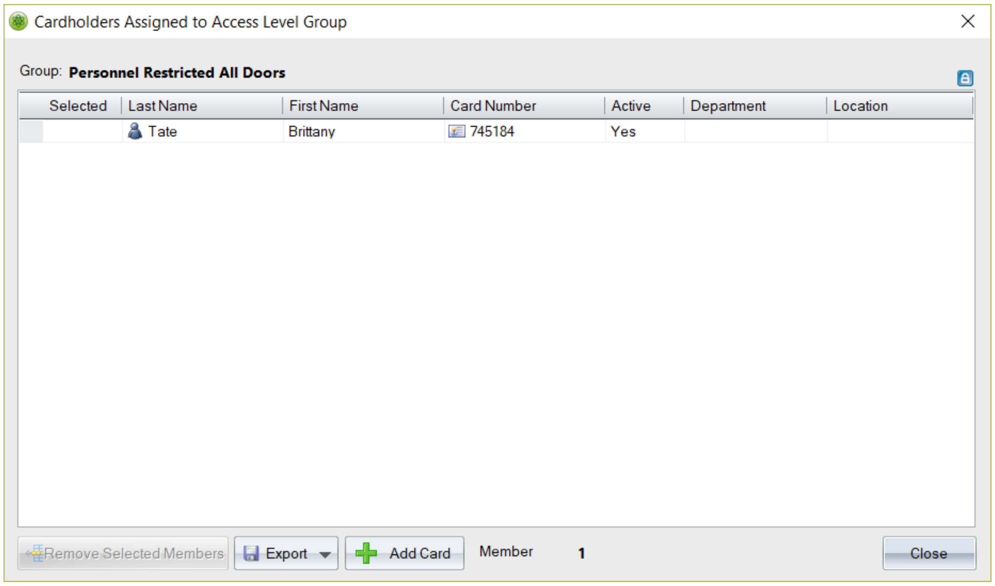
Group Name: General Personnel - All Doors

# of Cards: 148 out of 148 DONE

□ Close When Compl

Access Level / Assigned To Dialog

The Assigned To feature is an InfoReady report that allows the operator to audit the cardholders assigned to an access level group. It can also be used to add and remove the access level group from selected cards. See page 6-19 for more information on assigning access through the Assigned To dialog.


Cardholders Assigned to Access Level Group

Group: Personnel Restricted All Doors

Selected	Last Name	First Name	Card Number	Active	Department	Location
	Tate	Brittany	745184	Yes		

Member 1

Removing Access Levels from Cards

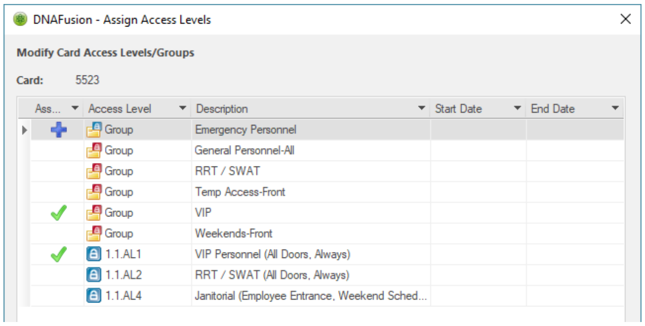
Cardholder access can be removed using several methods, including an option to remove all access levels.

Remove from Individual Card

Access levels can be assigned to an individual cardholder from within the Personnel Record.

1. **Open** the Personnel Record and **select** the Card tab.
2. **Right-click** inside the Access Levels section and **select** Add/Remove/Modify Access.

   The Assign Access Levels dialog opens.



Modify Card Access Levels/Groups

Card: 5523

Ass...	Access Level	Description	Start Date	End Date
✚	Group	Emergency Personnel		
	Group	General Personnel-All		
	Group	RRT / SWAT		
	Group	Temp Access-Front		
✓	Group	VIP		
	Group	Weekends-Front		
✓	1.1.AL1	VIP Personnel (All Doors, Always)		
	1.1.AL2	RRT / SWAT (All Doors, Always)		
	1.1.AL4	Janitorial (Employee Entrance, Weekend Sched...		

- A green check ✓ indicates that the access level is already assigned to the card.
- A red minus sign ▬ indicates that the access level will be removed from the card.
- A blue plus sign ✚ indicates that the access level will be added to the card.

3. **Click** the Assigned field next to the desired Access Level(s).

   The green checkmark will change to a red minus sign.
4. **Click** OK.

   The access levels are removed from the card.

> *Alternatively,* **right-click** *in the* Access Levels *section and* **select** Remove Access Level/ Group; **click** Yes *at the confirmation dialog.*

Remove All Access Levels

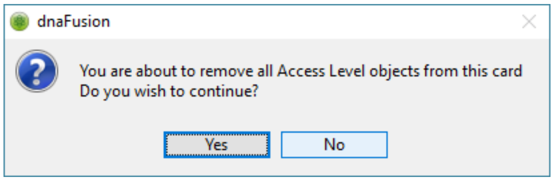
To remove all access levels from a card:

1. In the Personnel Browser, **right-click** on the Card and **select** Remove All Access from Card.

   OR

   In the Card tab, **right-click** in the Access Levels section and **select** Remove All Access.

   A confirmation dialog appears.



You are about to remove all Access Level objects from this card
Do you wish to continue?

2. **Click** Yes.

   All access levels are removed from the card.

Deactivate and Remove Access Levels when a New Card is Added

This option automatically deactivates and removes the access level information from an existing card when a new card is added to a personnel record.

1. In the Personnel Properties, **check** the Deactivate Existing Cards on New Card option.

   See page 3-16 for more information.

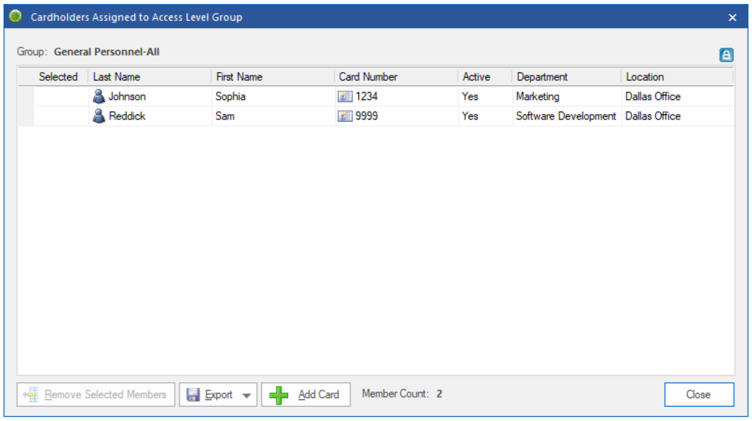
Remove from the Assigned To Report

Cardholder access can be removed when viewing the members of an access level. See page 6-19 for more information.

Access Level Groups

1. From the Access Levels Browser, **right-click** on the desired Global or Legacy Access Level Group and **select** Assigned To.

   The Cardholders Assigned to Access Level Group dialog appears.



Cardholders Assigned to Access Level Group

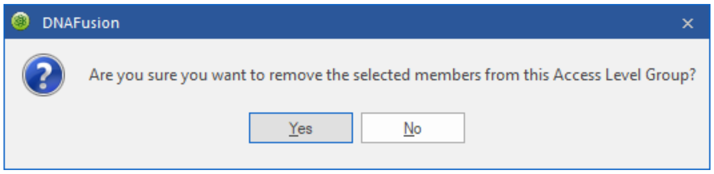
Group: General Personnel-All

Selected	Last Name	First Name	Card Number	Active	Department	Location
	Johnson	Sophia	1234	Yes	Marketing	Dallas Office
	Reddick	Sam	9999	Yes	Software Development	Dallas Office

Member Count: 2

2. **Select** the desired cardholder(s) and **click** Remove Selected Members.

   A confirmation dialog appears.



DNAFusion

Are you sure you want to remove the selected members from this Access Level Group?

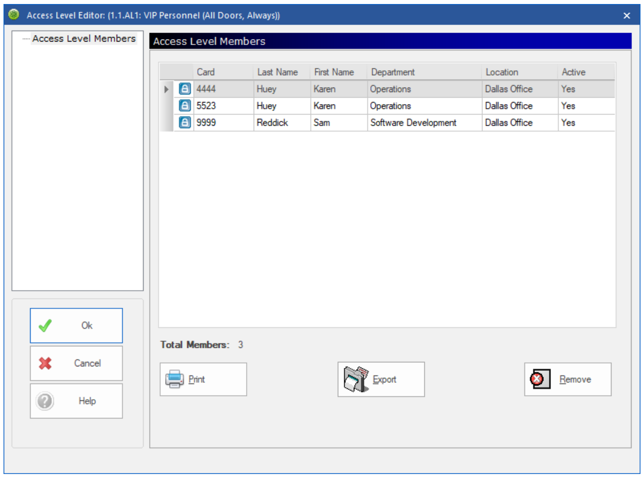
3. **Click** Yes.

   The group's access levels are removed from the selected card(s).

Legacy Access Levels

1. From the Access Levels Browser, **right-click** on the desired Access Level and **select** Assigned To.

   The Access Level Members dialog opens.



Access Level Editor: (1.1.AL1: VIP Personnel (All Doors, Always))

Access Level Members

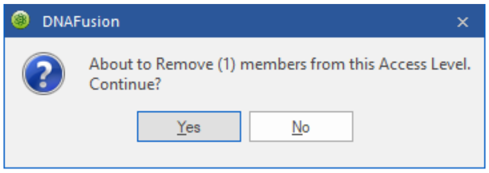
Card	Last Name	First Name	Department	Location	Active
4444	Huey	Karen	Operations	Dallas Office	Yes
5523	Huey	Karen	Operations	Dallas Office	Yes
9999	Reddick	Sam	Software Development	Dallas Office	Yes

Total Members: 3

2. **Select** the desired Card(s) and **click** Remove.

   Press the Ctrl or Shift key to select multiple cards.

   A confirmation dialog appears.



DNAFusion

About to Remove (1) members from this Access Level. Continue?

3. **Click** Yes.

   The legacy access level is removed from the card(s).

Personnel Groups

Personnel groups are used to organize cardholders into logical groups and assign default access levels to the group. When cardholders are added to the personnel group, the default access levels are automatically assigned to their card(s).

Creating a Personnel Group

1. In the Personnel Browser, **right-click** on the All Cardholders object and **select** Add New Group.

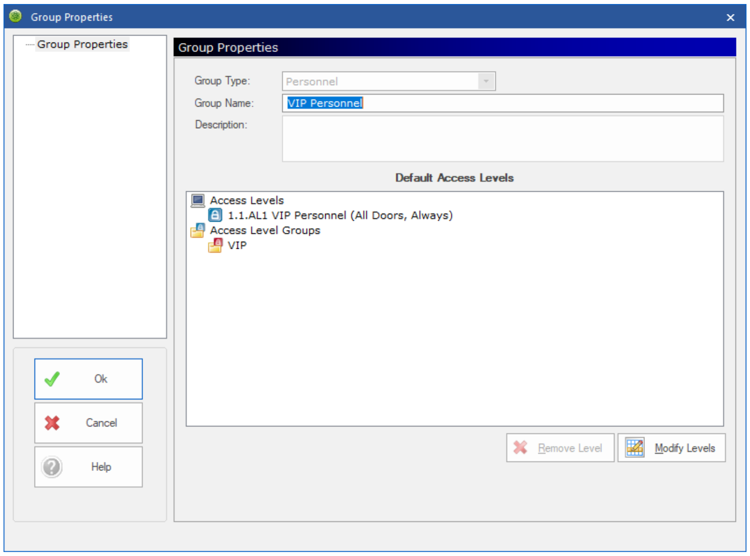
   OR

   Select Personnel / Add Personnel Group from the Main Menu.

   OR

   Right-click in the Personnel Browser and **select** Add New Personnel Group.

   The Group Properties dialog opens.



Group Properties

Group Type: Personnel

Group Name: VIP Personnel

Description:

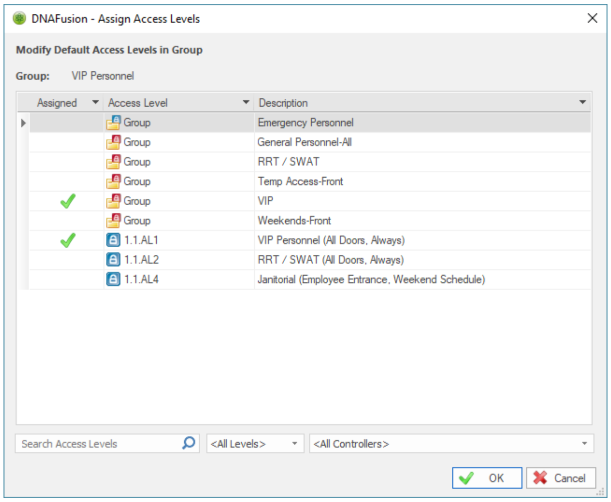
Default Access Levels

Access Levels
- 1.1.AL1 VIP Personnel (All Doors, Always)

Access Level Groups
- VIP

2. **Enter** a Group Name.
3. If desired, **enter** a Description for the group.
4. **Click** the Modify Levels button.

   The Assign Access Levels dialog opens.



DNAFusion - Assign Access Levels

Modify Default Access Levels in Group

Group: VIP Personnel

Assigned	Access Level	Description
	Group	Emergency Personnel
	Group	General Personnel-All
	Group	RRT / SWAT
	Group	Temp Access-Front
✓	Group	VIP
	Group	Weekends-Front
✓	1.1.AL1	VIP Personnel (All Doors, Always)
	1.1.AL2	RRT / SWAT (All Doors, Always)
	1.1.AL4	Janitorial (Employee Entrance, Weekend Schedule)

   To add an access level: **Click** the Assigned column next to the desired Access Level. A ✚ will appear in the Assigned column.

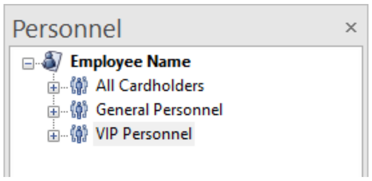
   To remove an access level: If the access level is already assigned to the group, a ✓ will appear in the Assigned column. **Click** the ✓ icon to remove the access level and a ▬ will appear.

5. **Click** OK to add the access level(s) to the personnel group.

   The access level(s) will appear in the Default Access Levels section.

6. **Click** OK.

   The personnel group is added to the Personnel Browser.



Personnel

Employee Name
- All Cardholders
- General Personnel
- VIP Personnel

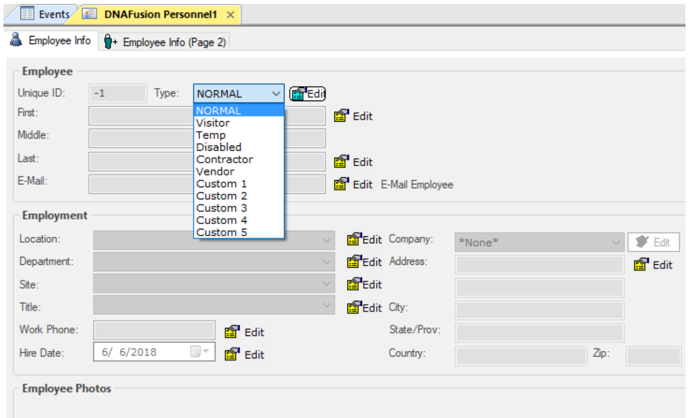
> **!** If an access level is added to a personnel group with existing cardholders, DNA Fusion will prompt the operator to assign the new access to existing group members. **Click** Yes to assign the new access level(s) to the group's existing cardholders.

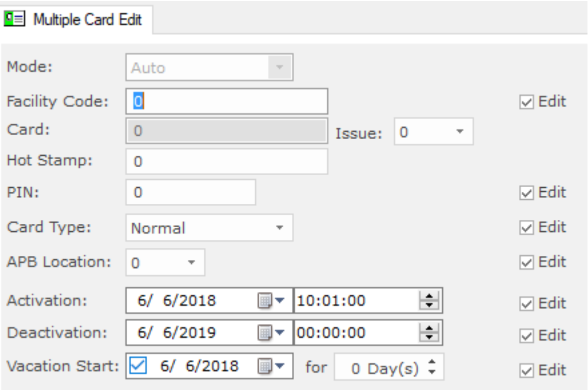
Editing Personnel Records in a Personnel Group

DNA Fusion provides a Group Edit feature for cardholders and cards in the same personnel group.

1. **Select** the desired tab from the Personnel Browser.
   - Name View - Edit cardholder information.
   - Card # View - Edit card information.
2. **Right-click** on the Personnel Group and **select** Group Edit Members.
3. **Select** the Edit button/checkbox next to the desired field(s).

   The field(s) will become active.




Multiple Card Edit

Mode: Auto

Facility Code: 0 ☑ Edit

Card: 0 Issue: 0

Hot Stamp: 0

PIN: 0 ☑ Edit

Card Type: Normal ☑ Edit

APB Location: 0 ☑ Edit

Activation: 6/ 6/2018 10:01:00 ☑ Edit

Deactivation: 6/ 6/2019 00:00:00 ☑ Edit

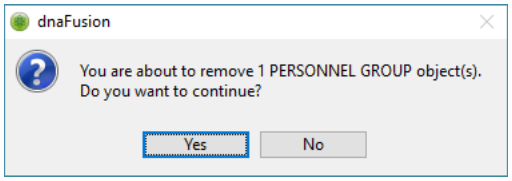
Vacation Start: ☑ 6/ 6/2018 for 0 Day(s) ☑ Edit

4. **Edit** the cardholder or card information as needed.
5. **Right-click** in the Personnel Record and **select** Update.

Deleting a Personnel Group

1. In the Personnel Browser, **right-click** on the Personnel Group and **select** Remove Personnel Group.

   A confirmation dialog appears.


dnaFusion

You are about to remove 1 PERSONNEL GROUP object(s).
Do you want to continue?

2. **Click** Yes to delete the group.

   The group is removed from the Personnel Browser.

Adding Cardholders to a Personnel Group

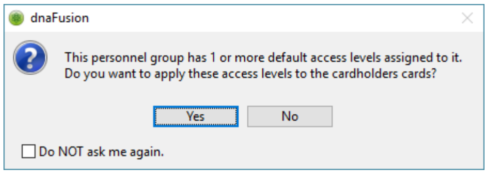
The following methods can be used to add cardholders to a personnel group:

- Drag and drop
- Add User(s) to Group option
- Auto-prompt
- Manage User Groups option
- Find Cardholder dialog

Drag and Drop

1. Open the Personnel Browser and **expand** the All Cardholders header.
2. **Drag** and **drop** the cardholder(s) to the desired Personnel Group.

   A confirmation dialog will appear if one or more access levels are assigned to the personnel group.



This personnel group has 1 or more default access levels assigned to it. Do you want to apply these access levels to the cardholders cards?

3. **Click** Yes to apply the default access level(s) to the cardholder's cards or No to add the cardholder to the group without applying the access level(s).

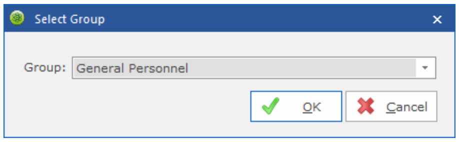
Add User(s) to Group

Cardholders can also be added to a group via the Add User(s) to Group option.

1. **Right-click** on the Cardholder(s) and **select** Add User(s) to Group.

   Press and **hold** the Control or Shift key to select multiple cardholders.

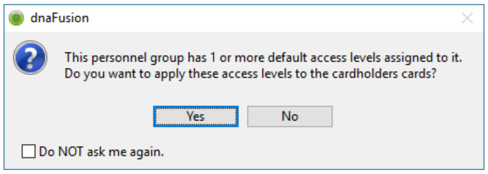
   The Select Group dialog opens.



Group: General Personnel

2. **Select** the Personnel Group from the drop-down list and **click** OK.

   A confirmation dialog will appear if one or more access levels are assigned to the personnel group.
3. **Click** Yes to apply the default access level(s) to the cardholder's cards or No to add the cardholder to the group without applying the access level(s).



This personnel group has 1 or more default access levels assigned to it. Do you want to apply these access levels to the cardholders cards?

Auto-Prompt When Adding New Cardholder

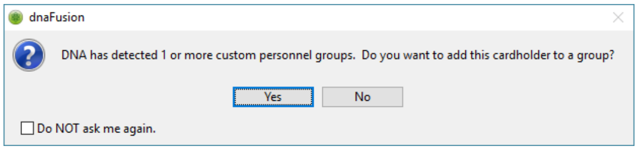
If a personnel record is updated or closed without adding an access level, and one or more personnel groups have been configured in the system, DNA Fusion will prompt the operator to add the card to a personnel group.

1. **Add** a new cardholder and **update** the record.

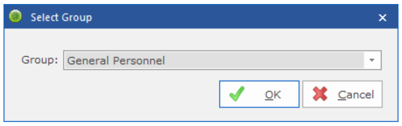
   A confirmation dialog appears.
2. **Click** Yes to add the card to a personnel group.

   The Select Group dialog opens.
3. **Select** the Personnel Group from the drop-down list.
4. **Click** OK.

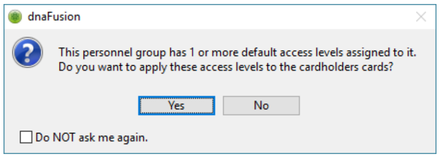
   A second confirmation dialog appears.
5. **Click** Yes to apply the group's default access level(s) to the cardholder's cards or No to add the cardholder to the group without applying the access levels.



DNA has detected 1 or more custom personnel groups. Do you want to add this cardholder to a group?



Group: General Personnel



This personnel group has 1 or more default access levels assigned to it. Do you want to apply these access levels to the cardholders cards?

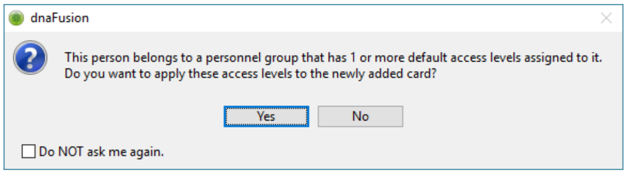
Auto-Prompt When Adding New Card

If a new card is added to a cardholder that already belongs to a personnel group, DNA Fusion will prompt the operator to apply the group's default access level(s) to the new card.

1. After the new card is added, **right-click** in the Personnel Record and **select** Update.

   A confirmation dialog appears.

2. **Click** Yes to apply the default access level(s) to the new card or No to add the new card without access level(s).


dnaFusion

This person belongs to a personnel group that has 1 or more default access levels assigned to it.
Do you want to apply these access levels to the newly added card?

□ Do NOT ask me again.

Manage User Groups

The Manage User Groups option in the Employee Info tab of the Personnel Record can be used to assign one or more personnel groups to a cardholder.

1. **Select** the Manage User Groups button in the Employee Info tab of the Personnel Record.

   The User Groups Manager dialog appears.

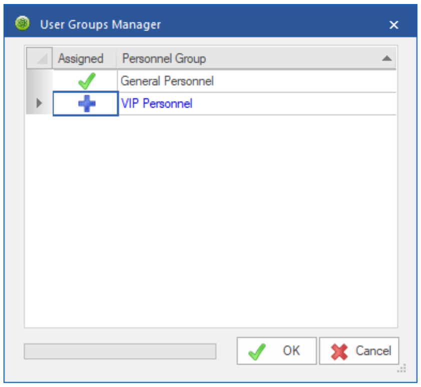
2. **Select** the Assigned column next to the desired Personnel Group.

   A blue plus icon ✚ appears.

3. **Click** OK.

   A confirmation dialog appears.

4. **Click** Yes to apply the default access level(s) to the cardholder's card(s) or No to add the cardholder to the group without applying the access level(s).


User Groups Manager

Assigned	Personnel Group
✓	General Personnel
✚	VIP Personnel

Find Cardholder

Operators can search for a cardholder based on specific criteria and then add them to a personnel group.

1. **Right-click** on the Personnel Group and **select** Add Cardholder to Group.

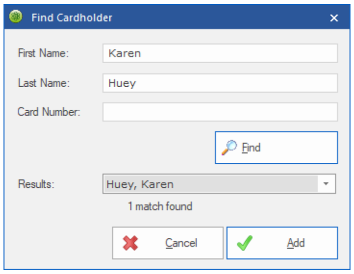
   The Find Cardholder dialog opens.

2. **Enter** the search criteria (First Name, Last Name, and/or Card Number) and **click** Find.

   The percent sign (%) acts as a wildcard.

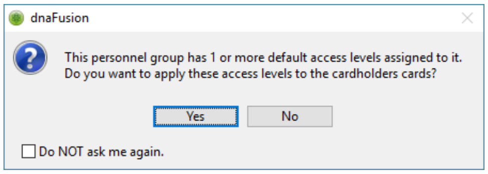
3. **Select** the cardholder from the Results drop-down and **click** Add.

   A confirmation dialog appears.


Find Cardholder

First Name: Karen
Last Name: Huey
Card Number:

Results: Huey, Karen
1 match found


dnaFusion

This personnel group has 1 or more default access levels assigned to it.
Do you want to apply these access levels to the cardholders cards?

□ Do NOT ask me again.

4. **Click** Yes to add the access level(s) or No to add the cardholder to the group without the access level(s).

Removing Cardholders from a Personnel Group

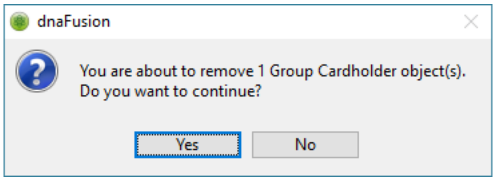
1. In the Personnel Browser, **expand** the Personnel Group object.

2. **Right-click** on the desired Cardholder in the personnel group and **select** Remove Cardholder from Group.

   A confirmation dialog appears.

3. **Click** Yes to remove the cardholder from the group.

   The cardholder is removed from the group; however, the group's access levels are not removed from the card.


dnaFusion

You are about to remove 1 Group Cardholder object(s).
Do you want to continue?

Managing Personnel Groups and Access Levels

DNA Fusion provides a number of options to manage a personnel group's access levels:

- Assign default access levels to a personnel group
- Add access levels to existing cards in a personnel group
- Remove default access levels from a personnel group
- Remove an access level from the cards in a personnel group

Assign Default Access Levels to a Personnel Group

When default access levels are assigned to a personnel group, any cardholders added to the group will automatically receive the default access levels.

1. **Double-click** on the desired Personnel Group in the Personnel Browser.

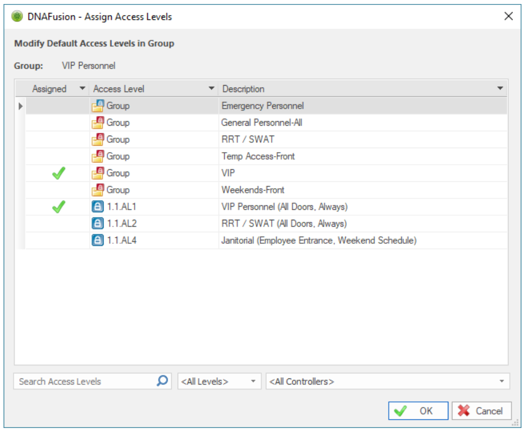
   OR

   Right-click on the Personnel Group and **select** Properties.

   The Group Properties dialog opens.

2. **Click** the Modify Levels button.

   The Assign Access Levels dialog appears.



DNAFusion - Assign Access Levels

Modify Default Access Levels in Group

Group: VIP Personnel

Assigned	Access Level	Description
	Group	Emergency Personnel
	Group	General Personnel-All
	Group	RRT / SWAT
	Group	Temp Access-Front
✓	Group	VIP
	Group	Weekends-Front
✓	1.1.AL1	VIP Personnel (All Doors, Always)
	1.1.AL2	RRT / SWAT (All Doors, Always)
	1.1.AL4	Janitorial (Employee Entrance, Weekend Schedule)

   To add an access level: **Click** the Assigned column next to the desired Access Level. A ✚ will appear in the Assigned column.

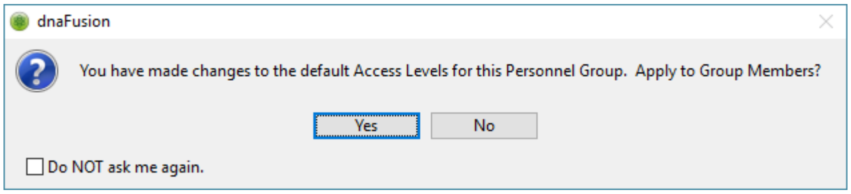
   To remove an access level: If the access level is already assigned to the group, a ✓ will appear in the Assigned column. **Click** the ✓ icon to remove the access level and a ▬ will appear.

3. **Click** OK to add the access level(s) to the personnel group.

   The access level(s) appear in the Default Access Levels section.

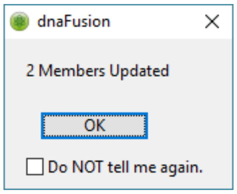
4. **Click** OK.

   If an access level is added to a personnel group with existing cardholders, a confirmation dialog will appear; **click** Yes to add the new access level(s) to the cardholders' cards.



dnaFusion

You have made changes to the default Access Levels for this Personnel Group. Apply to Group Members?



dnaFusion

2 Members Updated

Add Access Levels to Existing Cards in a Personnel Group

Operators can add access levels to existing cards in a personnel group using two methods:

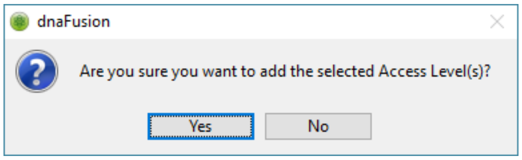
- Drag and drop an access level to the personnel group
- Use the Add Access Levels to Group Members option

> *Neither method will permanently add the access level to the personnel group. See page 7-27 for information on assigning default access levels to personnel groups.*

Drag and Drop

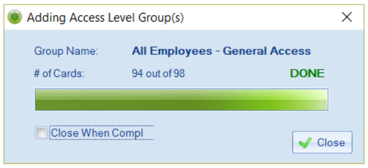
1. **Open** the Personnel Browser and Access Levels Browser and **expand** both trees.
2. **Drag** and **drop** an Access Level to the desired Personnel Group.

   A confirmation dialog appears.



dnaFusion

Are you sure you want to add the selected Access Level(s)?



Adding Access Level Group(s)

Group Name: All Employees - General Access

# of Cards: 94 out of 98 DONE

□ Close When Compl

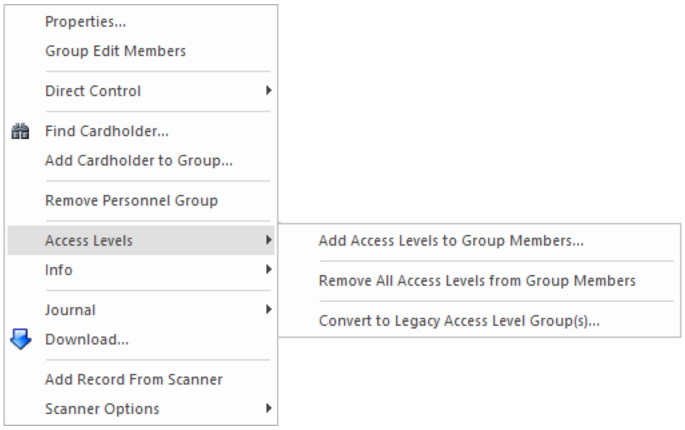
3. **Click** Yes to confirm.

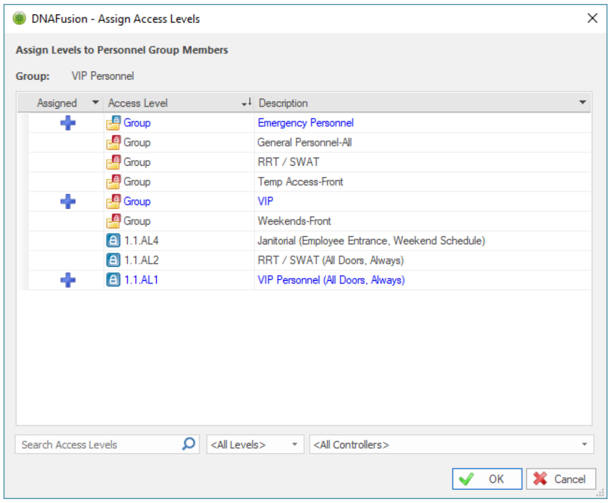
   The access level is added to all cards in the personnel group.
4. **Click** OK.

Add Access Levels to Group Members

1. In the Personnel Browser, **right-click** on the desired Personnel Group and **select** Access Levels / Add Access Levels to Group Members.

   The Assign Access Levels dialog opens.





DNAFusion - Assign Access Levels

Assign Levels to Personnel Group Members

Group: VIP Personnel

Assigned	Access Level	Description
✚	Group	Emergency Personnel
	Group	General Personnel-All
	Group	RRT / SWAT
	Group	Temp Access-Front
✚	Group	VIP
	Group	Weekends-Front
	1.1.AL4	Janitorial (Employee Entrance, Weekend Schedule)
	1.1.AL2	RRT / SWAT (All Doors, Always)
✚	1.1.AL1	VIP Personnel (All Doors, Always)

2. **Click** the Assigned field next to the desired Access Level(s).

   A blue plus sign ✚ will appear next to the Access Level(s).
3. **Click** OK to add the Access Level(s).

   The access levels are added to all cards in the personnel group.

Removing Access Levels from a Personnel Group

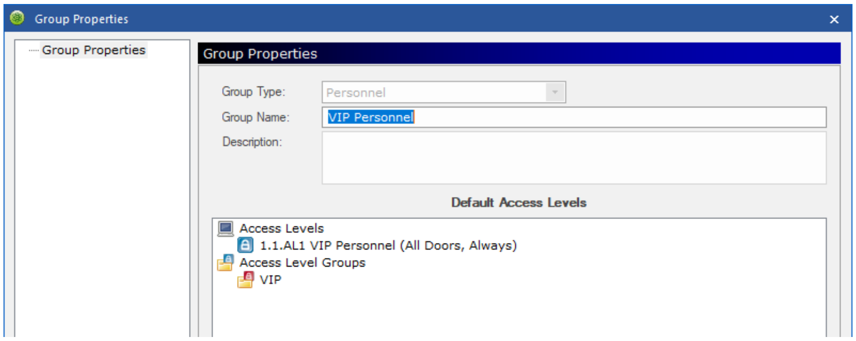
Operators can remove access levels from a personnel group via two methods:

- Remove default access levels from the personnel group
- Use the Remove All Access from Group Members option

Remove Default Access Levels

1. **Right-click** on the Personnel Group in the Personnel Browser and **select** Properties.

   The Group Properties dialog opens.



Group Properties

Group Properties

Group Properties

Group Type: Personnel

Group Name: VIP Personnel

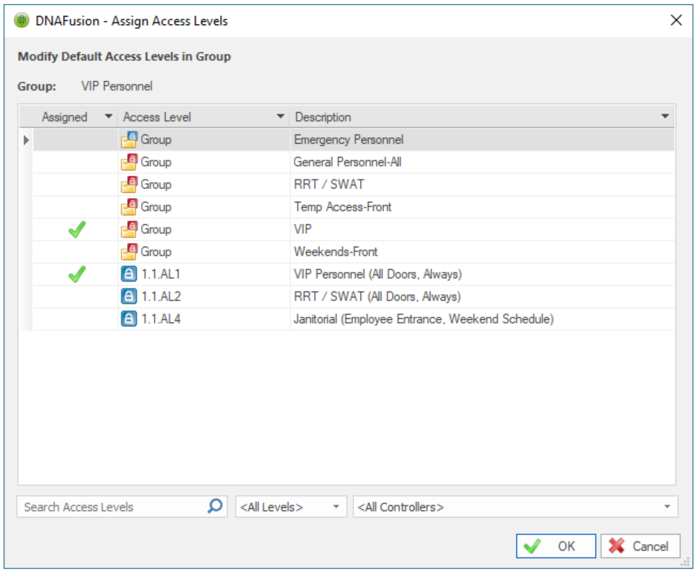
Description:

Default Access Levels

- Access Levels
  - 1.1.AL1 VIP Personnel (All Doors, Always)
- Access Level Groups
  - VIP

2. **Click** the Modify Levels button.

   The Assign Access Levels dialog appears.



DNAFusion - Assign Access Levels

Modify Default Access Levels in Group

Group: VIP Personnel

Assigned	Access Level	Description
	Group	Emergency Personnel
	Group	General Personnel-All
	Group	RRT / SWAT
	Group	Temp Access-Front
✓	Group	VIP
	Group	Weekends-Front
✓	1.1.AL1	VIP Personnel (All Doors, Always)
	1.1.AL2	RRT / SWAT (All Doors, Always)
	1.1.AL4	Janitorial (Employee Entrance, Weekend Schedule)

3. **Click** the Assigned column next to the desired Access Level(s).

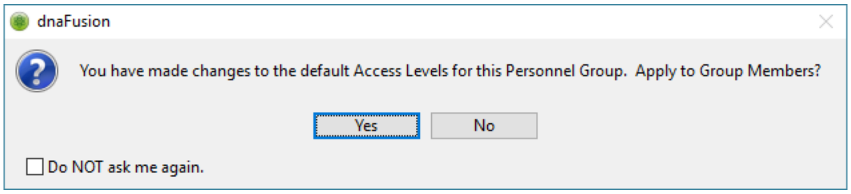
   The green checkmark ✓ changes to a red minus sign ➖ to mark it for removal.

4. **Click** OK.

   The access level(s) are removed from the personnel group and will disappear from the Default Access Levels section.

5. **Click** OK.

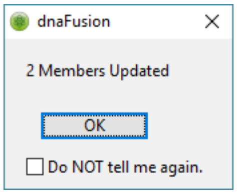
   If the access level(s) are being removed from a personnel group with existing cardholders, a confirmation dialog appears; **click** Yes to remove the access level(s) from the cardholders' cards.



dnaFusion

You have made changes to the default Access Levels for this Personnel Group. Apply to Group Members?

□ Do NOT ask me again.



dnaFusion

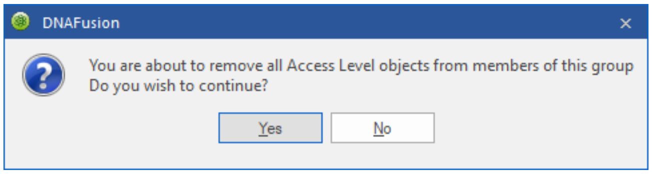
2 Members Updated

□ Do NOT tell me again.

Remove All Access Levels from Group Members

1. **Right-click** on the desired Personnel Group in the Personnel Browser.
2. **Select** Access Levels / Remove All Access Levels from Group Members.

   A confirmation dialog appears.



DNAFusion

You are about to remove all Access Level objects from members of this group
Do you wish to continue?

3. **Click** Yes.

   All access levels are removed from the cardholders’ cards.

Viewing Cardholders

Operators can locate and organize cardholders using several methods. Each method offers a different way to view or access the cardholder's information.

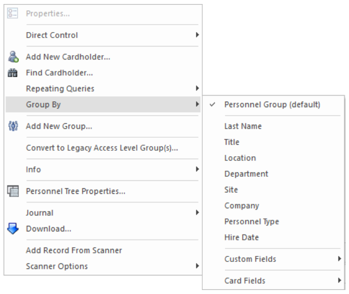
Group By

By default, the Personnel Browser is organized into personnel groups. However, DNA Fusion provides the ability to group the Personnel Browser by any repeatable field in the Personnel Record.

1. **Right-click** on the All Cardholders or All Cards header in the Personnel Browser and **select** Group By.
2. **Select** a Group By option from the list.

   The Personnel Browser is grouped by the selected field.

   The Card Fields options will be grayed out unless the Card # View tab is active in the Personnel Browser.



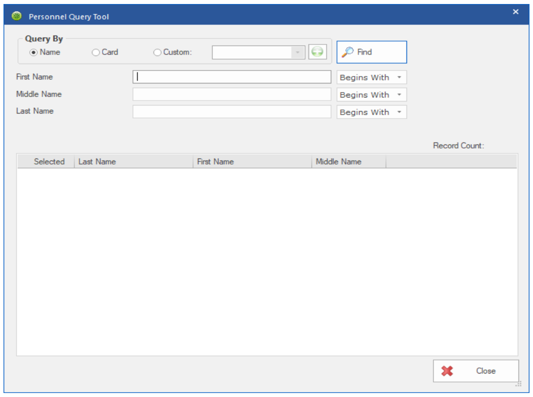
Custom Repeatable Queries (CRQs)

The Custom Repeatable Queries feature is used to perform a quick search for personnel records based on names, card numbers, or user-defined queries.

Running Repeating Queries (New)

1. **Right-click** on the All Cardholders or All Cards header in the Personnel Browser and **select** Repeating Queries (New).

   The Personnel Query Tool opens.
2. **Select** Name, Card, or Custom (see Creating Custom Queries).
3. If locating cardholders by Name, **select** an option from the drop-down menu next to First, Middle, and Last Name fields.
   - Begins With - The returned record(s) will begin with the entered text.
   - Contains - The returned record(s) will contain the entered text.
   - Exact - The returned record(s) will contain the exact entered text.
4. **Enter** the correct information in the First Name, Middle Name, or Last name fields.
5. **Click** on the Find button.
6. If desired, **double-click** on the cardholder to open the Personnel Record.
7. If locating cardholders by Card, **enter** the Card Number, Facility Code, or Hot Stamp.
8. **Click** on the Find Button.
9. If desired, **double-click** on the cardholder to open the Personnel Record.



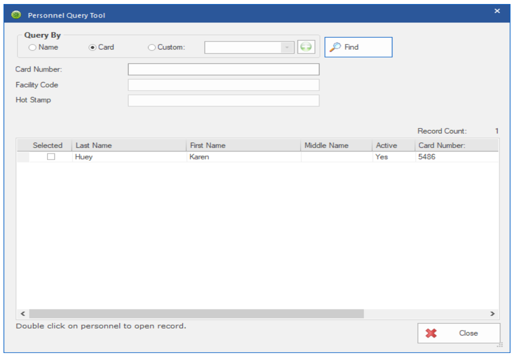
Personnel Query Tool

Query By: ● Name ○ Card ○ Custom:

First Name: Begins With
Middle Name: Begins With
Last Name: Begins With

Record Count:

Selected	Last Name	First Name	Middle Name



Personnel Query Tool

Query By: ○ Name ● Card ○ Custom:

Card Number:
Facility Code
Hot Stamp

Record Count: 1

Selected	Last Name	First Name	Middle Name	Active	Card Number:
□	Huey	Karen		Yes	5486

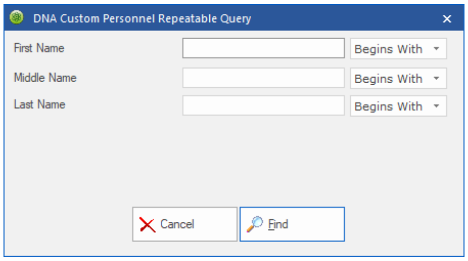
Double click on personnel to open record.

Running Repeating Queries (Legacy)

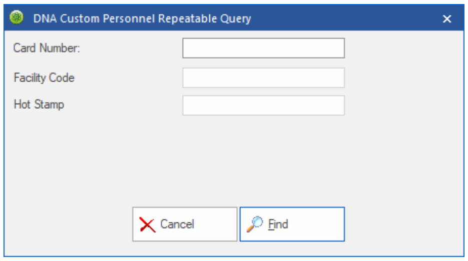
1. **Right-click** on the All Cardholders or All Cards header in the Personnel Browser and **select** Repeating Queries.
2. **Select** the Name or Card Number option to query the desired field.

   The DNA Custom Personnel Repeatable Query dialog opens.

   The percent sign (%) functions as a wild card.



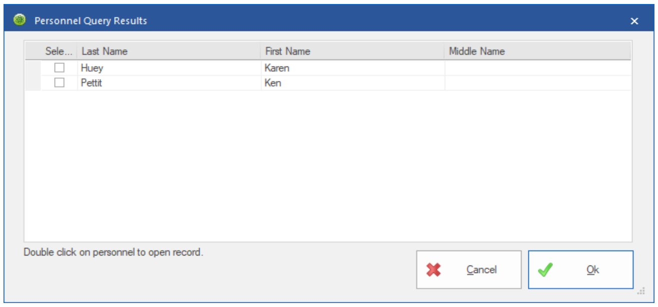
First Name: Begins With
Middle Name: Begins With
Last Name: Begins With



Card Number:
Facility Code
Hot Stamp

3. If needed, **select** a delimiter field.
   - Begins With - The returned record(s) will begin with the entered text.
   - Contains - The returned record(s) will contain the entered text.
   - Exact - The returned record(s) will contain the exact entered text.
4. **Enter** the information in the field(s) and **click** the Find button.

   The Personnel Query Results dialog opens.



Sele...	Last Name	First Name	Middle Name
□	Huey	Karen	
□	Pettit	Ken	

Double click on personnel to open record.

5. **Double-click** on a result to open the Personnel Record.

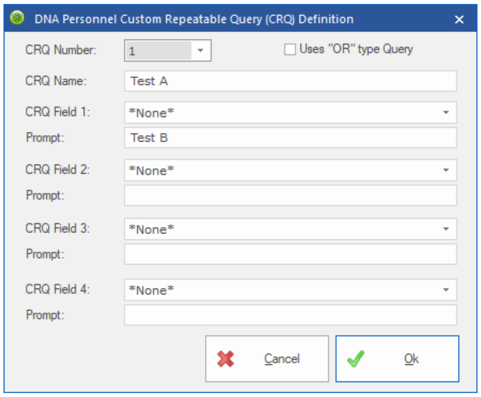
   The selected record opens in the data window.

Creating Custom Queries

The operator can create custom queries based on any personnel record field and save them for future use.

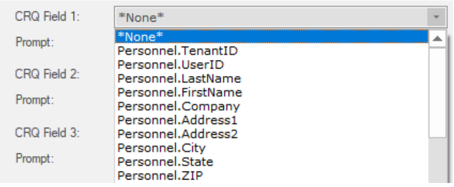
1. **Right-click** on the All Cardholders or All Cards header in the Personnel Browser and **select** Repeating Queries.
2. **Select** the Custom / New option to create a query.

   The DNA Personnel Custom Repeatable Query (CRQ) Definition dialog opens.



CRQ Number: 1
□ Uses "OR" type Query
CRQ Name: Test A
CRQ Field 1: *None*
Prompt: Test B
CRQ Field 2: *None*
Prompt:
CRQ Field 3: *None*
Prompt:
CRQ Field 4: *None*
Prompt:

3. **Enter** the following information:
   - CRQ Number - The unique ID (1-10) for the custom query.
   - CRQ Name - The query's display name in the Repeating Queries / Custom context menu.
   - CRQ Field (1-4) - The personnel record field referenced by the search query.



   - Prompt - The text that will appear in the DNA Custom Personnel Repeatable Query dialog when the custom query is selected from the context menu.
4. If desired, **click** the Uses "OR" Type Query checkbox to apply a conditional statement to the query.
5. **Run** the query as described on page 7-31.

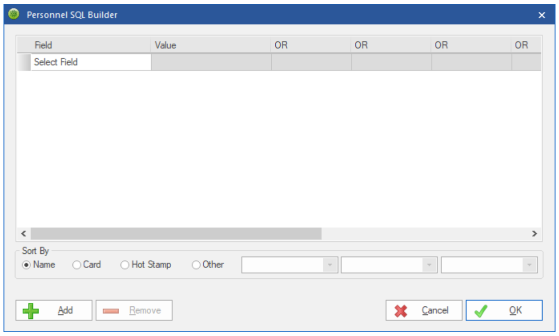
> *To edit or remove queries,* **select** *the* CRQ Number *from the drop-down list and* **edit** *or* **delete** *the information.*

Find Cardholder (Personnel SQL Builder)

The Personnel SQL Builder dialog is used to create a custom personnel group based on filtered criteria.

1. **Right-click** in the Personnel Browser and **select** Find Cardholder.

   The Personnel SQL Builder dialog opens.



2. **Select** a Field from the drop-down list.
3. **Enter** the desired criteria in the Value and OR fields.
4. If desired, **click** the Add button or **press** Enter to define more fields.
   To delete a field, select the field and click the Remove button.
5. If desired, **select** a Sort By option to sort the cardholders in the filtered group.
6. **Click** OK to apply the filter.

   A filtered personnel group will appear at the bottom of the Personnel Browser with the results. Find #1:
7. To delete a filtered personnel group, **right-click** on the group and **select** Remove Personnel Group.

   The group is removed from the Personnel Browser.

NOTES:

Personnel Features

A variety of features are available based on the object selected in the Personnel Browser.

Individual Cardholder Features

Individual cardholder features include the ability to view access information and run a trace history report.

Card Flags

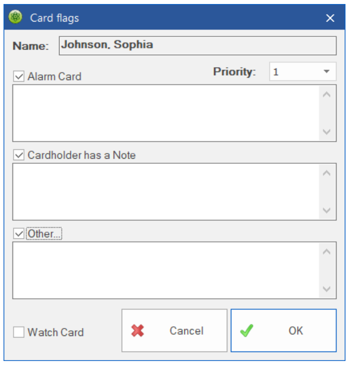
Flagged cards will display additional information in the Events Grid.

1. **Right-click** on the Cardholder or Card in the Personnel Browser and **select** Direct Control / Set Card Flags.

   OR

   Right-click in the Personnel Record and **select** Direct Control / Set Card Flags.

   The Card Flags dialog appears.



Card flags

Name: Johnson, Sophia

☑ Alarm Card Priority: 1

☑ Cardholder has a Note

☑ Other...

☐ Watch Card

2. **Check** the appropriate flag and **enter** any desired text.

   An icon will appear on the Events Grid when the card is used.

   - Alarm Card - Displays Alarm Card Used! in the Events Grid.
   - Cardholder Has a Note - Provides space to type a note.
   - Other - Provides space to type other information.
   - Watch Card - Displays Watch Card in the Events Grid.

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

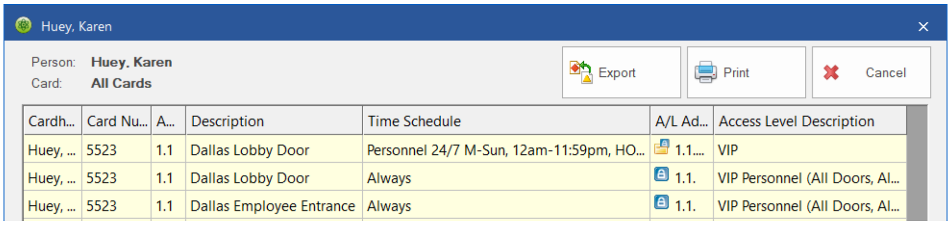
> *When a flagged card appears in the* Events Grid*,* **right-click** *and* **select** Personnel / Get/Set Note *to retrieve the* Card Flags *dialog for the associated card.*

Has Access To

This feature allows the operator to view which doors a cardholder can access.

1. **Right-click** on the Cardholder in the Personnel Browser and **select** Info / Has Access To.

   A dialog report opens for the selected cardholder.



Huey, Karen

Person: Huey, Karen
Card: All Cards

Cardh...	Card Nu...	A...	Description	Time Schedule	A/L Ad...	Access Level Description
Huey, ...	5523	1.1	Dallas Lobby Door	Personnel 24/7 M-Sun, 12am-11:59pm, HO...	1.1....	VIP
Huey, ...	5523	1.1	Dallas Lobby Door	Always	1.1.	VIP Personnel (All Doors, Al...
Huey, ...	5523	1.1	Dallas Employee Entrance	Always	1.1.	VIP Personnel (All Doors, Al...

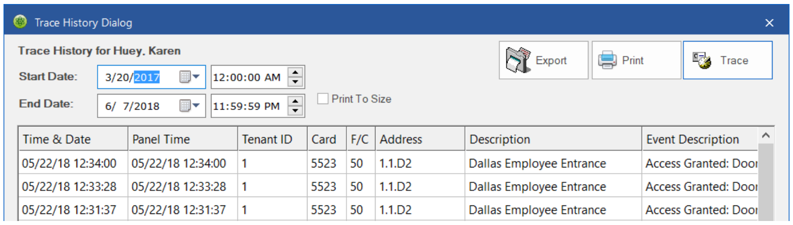
2. If desired, **print** or **export** the results to a CSV file (.csv).

Trace History

The Trace History feature displays event transactions associated with the cardholder for a specified date range.

1. **Right-click** on the Cardholder in the Personnel Browser and **select** Info / Trace History.

   The Trace History Dialog opens.



Trace History Dialog

Trace History for Huey, Karen

Start Date: 3/20/2017 12:00:00 AM

End Date: 6/ 7/2018 11:59:59 PM

☐ Print To Size

Time & Date	Panel Time	Tenant ID	Card	F/C	Address	Description	Event Description
05/22/18 12:34:00	05/22/18 12:34:00	1	5523	50	1.1.D2	Dallas Employee Entrance	Access Granted: Door
05/22/18 12:33:28	05/22/18 12:33:28	1	5523	50	1.1.D2	Dallas Employee Entrance	Access Granted: Door
05/22/18 12:31:37	05/22/18 12:31:37	1	5523	50	1.1.D2	Dallas Employee Entrance	Access Granted: Door

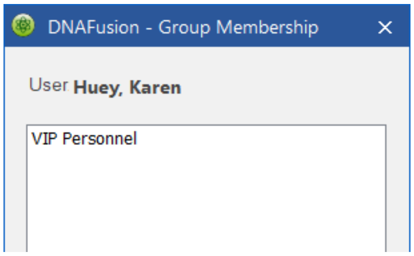
2. If a wider time and date range is needed, **enter** the Start and End Date/Time and **click** Trace.
3. If desired, **print** or **export** the results to a CSV file (.csv).

User Membership

The User Membership option displays a list of the cardholder's personnel groups.

1. **Right-click** on the Cardholder and **select** Info / User Membership.

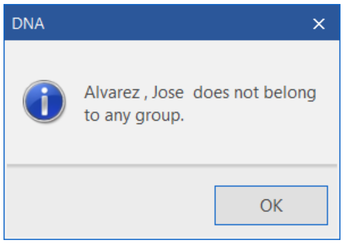
   The Group Membership dialog opens.



DNAFusion - Group Membership

User **Huey, Karen**

VIP Personnel



DNA

Alvarez , Jose does not belong to any group.

If the cardholder is not assigned to any personnel groups, a separate DNA message will appear.

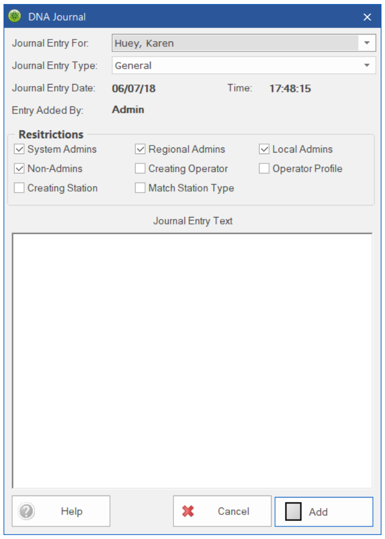
2. **Click** Close or OK to exit the dialog.

Journal

Creating a New Entry

1. **Right-click** on the Cardholder and **select** Journal / New Entry.

   The DNA Journal dialog opens in entry mode.



DNA Journal

Journal Entry For: Huey, Karen

Journal Entry Type: General

Journal Entry Date: 06/07/18 Time: 17:48:15

Entry Added By: Admin

Resitrictions

☑ System Admins ☑ Regional Admins ☑ Local Admins

☑ Non-Admins □ Creating Operator □ Operator Profile

□ Creating Station □ Match Station Type

Journal Entry Text

2. **Configure** the DNA Journal log. See page 4-24 for more information.
3. **Enter** the desired message in the Journal Entry Text section.
4. **Click** the Add button.

Viewing an Entry

1. **Right-click** on the Cardholder and **select** Journal / View.

   The DNA Journal Selection dialog opens to filter the entries.

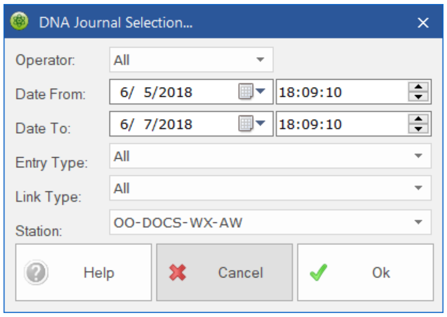
2. **Click** OK to view the results.

   The DNA Journal Viewier dialog appears.

   The DNA Journal Viewer appears. An operator can only view entries for which the appropriate operator restriction was checked.

   Navigate through the entries with the green arrow buttons at the bottom of the dialog: First, Previous, Next, and Last.

3. When finished, **select** the Close button to close the dialog.



DNA Journal Selection...

Operator: All

Date From: 6/ 5/2018 18:09:10

Date To: 6/ 7/2018 18:09:10

Entry Type: All

Link Type: All

Station: OO-DOCS-WX-AW

Individual Card Features

Individual card features include the ability to set use limits, issue a free pass, activate and deactivate cards, as well as reassign and remove cards from a personnel record.

Set Use Limit

The operator can set a use limit for a single card or for all cardholders. The Store Use Limit in the Controller Properties / Stored Quantities dialog must be checked in order for the controller to store the information; see page 8-53.

1. **Right-click** on the Card or Cardholder in the Personnel Browser and **select** Direct Control / Set Use Limit.

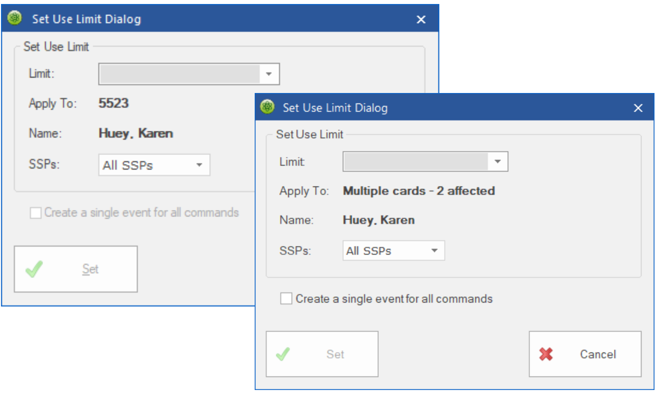
   OR

   Right-click in the Personnel Record and **select** Direct Control / Set Use Limit.

   OR

   Select Personnel / Set Use Limit from the Main Menu.

   The Set Use Limit Dialog appears.



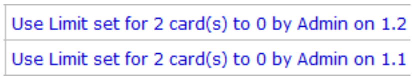
Apply To: 5523
Name: Huey, Karen
SSPs: All SSPs
□ Create a single event for all commands

Apply To: Multiple cards - 2 affected
Name: Huey, Karen
SSPs: All SSPs
□ Create a single event for all commands

2. **Select** the Limit option from the drop-down:
   - Zero Use Limit - Sets the use limit to 0.
   - Reset Use Limit - Sets the use limit to 255.
3. If desired, **select** a specific controller from the SSPs drop-down.

   Only doors and elevators from the selected controller will affect the use limit.
4. If multiple cards will be affected, **check** Create a Single Event for All Commands to display one transaction in the Events Grid for all cards.

   If All SSPs is selected, an event will populate in the Events Grid for each controller.



Use Limit set for 2 card(s) to 0 by Admin on 1.2

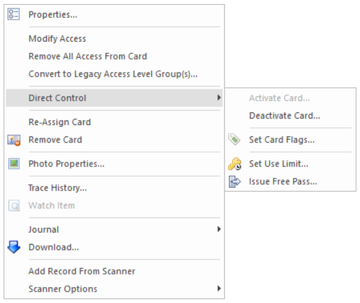
Use Limit set for 2 card(s) to 0 by Admin on 1.1

5. **Click** Set.

Activate/Deactivate Card

1. **Right-click** on the Card and **select** Direct Control / Activate Card or Deactivate Card.

   The card will immediately activate or deactivate based on the selection.



Reassign Card

The operator can reassign a card to another individual using one of two methods:

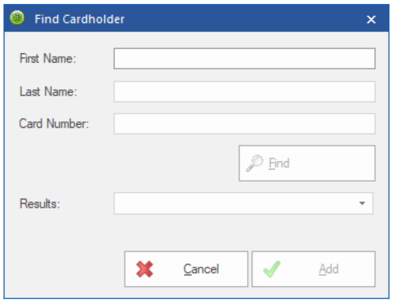
1. **Drag** the Card to the desired Cardholder and **click** Yes when the confirmation dialog appears.

   The card is reassigned to the cardholder.

   OR

1. **Right-click** on the Card and **select** Re-Assign Card.

   The Find Cardholder dialog opens.



2. **Enter** the cardholder's information.

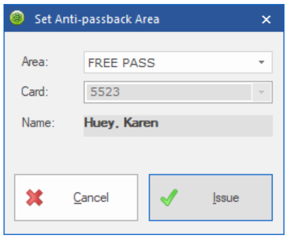
   The percent sign (%) functions as a wildcard character.
3. **Click** Find to populate the search results in the Results drop-down.
4. **Click** Re-Assign.

   A confirmation dialog appears.
5. **Click** Yes to reassign the card.

Issue Free Pass

1. **Right-click** on the Card and **select** Direct Control / Issue Free Pass.

   The Set Anti-Passback Area dialog appears.



Area: FREE PASS
Card: 5523
Name: Huey, Karen

2. **Select** an option from the Area drop-down and **click** Issue.

NOTES:

All Cardholders/All Cards Features

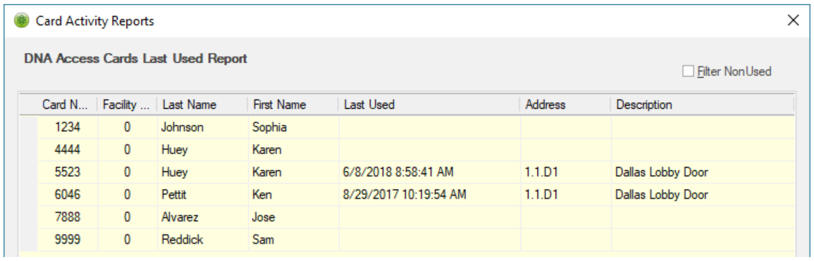
Features such as the Last Used and Non Use reports are available for all cardholders, all cards, or individual personnel groups.

Last Used

The Last Used Report provides a quick view of the last card events for all cardholders.

1. **Right-click** on All Cardholders in the Name View tab or All Cards in the Card # View tab and **select** Info / Last Used.

   The Card Activity Reports dialog opens.



Card Activity Reports

DNA Access Cards Last Used Report

□ Filter NonUsed

Card N...	Facility ...	Last Name	First Name	Last Used	Address	Description
1234	0	Johnson	Sophia			
4444	0	Huey	Karen			
5523	0	Huey	Karen	6/8/2018 8:58:41 AM	1.1.D1	Dallas Lobby Door
6046	0	Pettit	Ken	8/29/2017 10:19:54 AM	1.1.D1	Dallas Lobby Door
7888	0	Alvarez	Jose			
9999	0	Reddick	Sam			

2. If desired, **check** Filter NonUsed to remove information for cards that have not been used.
3. If desired, **export** the results to a CSV file (.csv) or to the clipboard.
4. **Click** OK to close the dialog.

Non Use

The Non Use Report displays cards that have not been used for a specified length of time.

1. **Right-click** on All Cardholders in the Name View tab or All Cards in the Card # View tab and **select** Info / Non-Use.

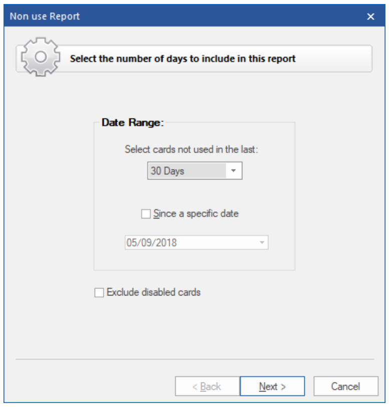
   The Non Use Report dialog opens.

2. **Select** the Date Range from the drop-down list and **click** the Next button.

   OR

   Check the Since a Specific Date box, **select** a date from the drop-down calendar, and **click** the Next button.

   If desired, **select** the Exclude Disabled Cards checkbox to include only active cards in the report.



Non use Report

Select the number of days to include in this report

Date Range:

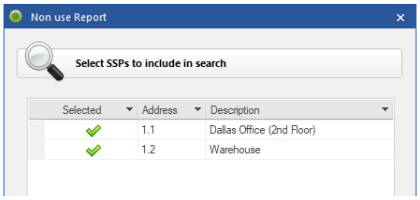
Select cards not used in the last: 30 Days

□ Since a specific date

05/09/2018

□ Exclude disabled cards

3. **Select** the desired Controllers and **click** Next.

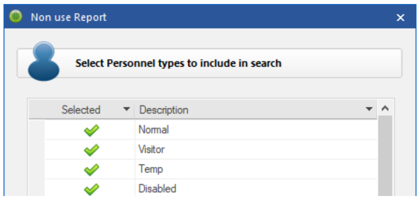


Non use Report

Select SSPs to include in search

Selected	Address	Description
✓	1.1	Dallas Office (2nd Floor)
✓	1.2	Warehouse

4. **Select** the desired Personnel Types and **click** Next.

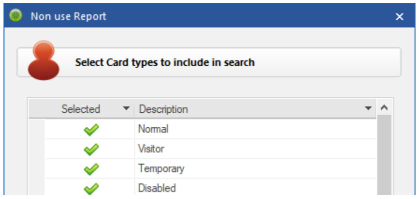


Non use Report

Select Personnel types to include in search

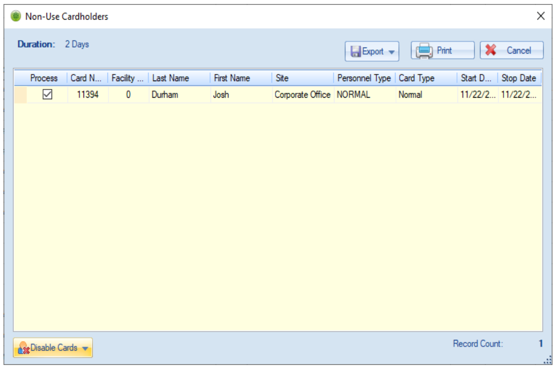
Selected	Description
✓	Normal
✓	Visitor
✓	Temp
✓	Disabled

5. **Select** the desired Card Types and **click** Finish.



Selected	Description
✓	Normal
✓	Visitor
✓	Temporary
✓	Disabled

The Non-Use Cardholders report opens.

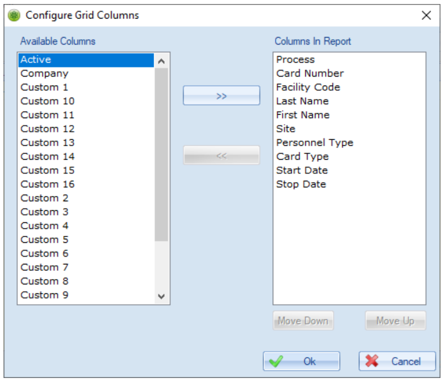


Duration: 2 Days

Process	Card N...	Facility ...	Last Name	First Name	Site	Personnel Type	Card Type	Start D...	Stop Date
☑	11394	0	Durham	Josh	Corporate Office	NORMAL	Normal	11/22/2...	11/22/2...

Record Count: 1

6. To make any adjustments to the grid columns, **right-click** and **select** Configure Grid.



Available Columns

Active
Company
Custom 1
Custom 10
Custom 11
Custom 12
Custom 13
Custom 14
Custom 15
Custom 16
Custom 2
Custom 3
Custom 4
Custom 5
Custom 6
Custom 7
Custom 8
Custom 9

Columns In Report

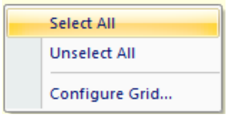
Process
Card Number
Facility Code
Last Name
First Name
Site
Personnel Type
Card Type
Start Date
Stop Date

Select any desired column variables and **click** the arrow button to add into the report. Use the Move Up and Move Down buttons to adjust the order of the columns.

7. If desired, **select** one or more cards to disable.

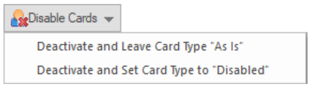
   The Disable Cards drop-down field becomes active.

   To select all of the cardholders, **right-click** in the report and **click** Select All.



8. **Select** the Deactivate option.

   The selected cards will turn gray.


Disable Cards
Deactivate and Leave Card Type "As Is"
Deactivate and Set Card Type to "Disabled"

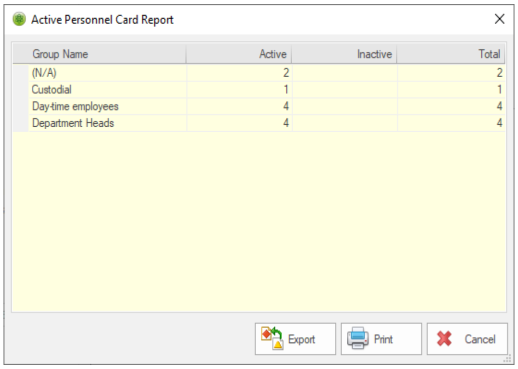
9. If desired, **export** the report to a CSV file (.csv) or to the clipboard.
10. If desired, **print** the report by selecting the Print button.
11. **Click** OK to close the report and **save** any changes.

Active Cards

The Active Personnel Card Report displays cards that are Active and Inactive within a Personnel Group.

1. **Right-click** on All Cardholders in the Name View or All Cards in the Card # View tab and **select** Info / Active Cards.

   The Active Personnel Card Report opens.
2. If desired, **export** the results to a CSV file (.csv).
3. If desired, **print** the results.



Group Name	Active	Inactive	Total
(N/A)	2		2
Custodial	1		1
Day-time employees	4		4
Department Heads	4		4

Cardholder Photos

Once a personnel record has been saved to the database, photos can be imported to the record. Photos can also be captured via DNA Fusion with a compatible camera; see Chapter 21 for more information. The photos can be triggered to display in the Photo Recall window.

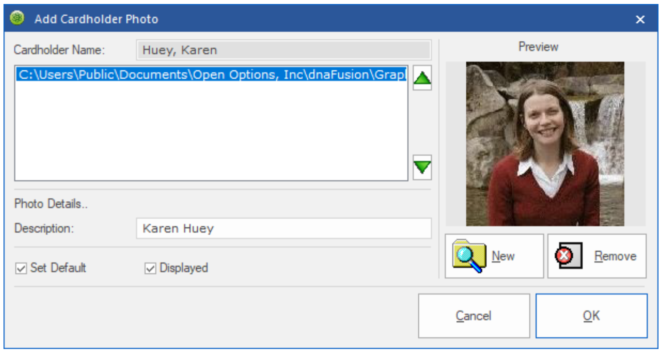
Importing Photos to a Record

1. With the Personnel Record open and updated, **right-click** inside the Employee Info: tab and **select** Photo Properties.

   OR

   Right-click on the Cardholder in the Personnel Browser and **select** Photo Properties.

   The Add Cardholder Photo dialog opens.



Add Cardholder Photo

Cardholder Name: Huey, Karen

C:\Users\Public\Documents\Open Options, Inc\dnaFusion\Grapl

Photo Details..

Description: Karen Huey

☑ Set Default ☑ Displayed

2. **Click** the New button and **browse** for the desired photo.
3. **Select** the checkboxes to designate the photo properties.
   - Set Default - Marks the photo as the default; the photo will appear in the Personnel Browser tooltip.
   - Displayed - Displays the photo on the Employee Info tab in the Personnel Record.
4. **Click** OK.
5. To save the record, **click** the Update Cardholder button on the Personnel Toolbar.

   OR

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

   A blue square appears to the left of the cardholder's name in the Personnel Browser, indicating that a photo is associated with the record.

> *If client workstations need access to photos, verify that the directory is shared and configure the directories path to point to the directory. Default directory paths can be configured by selecting* DNA / Administrative / DNA Directories *from the* Main Menu *(see page 20-1).*

Removing a Photo

1. **Right-click** inside the Employee Info tab of the Personnel Record and **select** Photo Properties.

   The Add Cardholder Photo dialog appears.
2. **Select** the photo link and **click** the Remove button. Remove
3. **Click** OK.
4. To save the record, **click** the Update Cardholder button on the Personnel Toolbar.

   OR

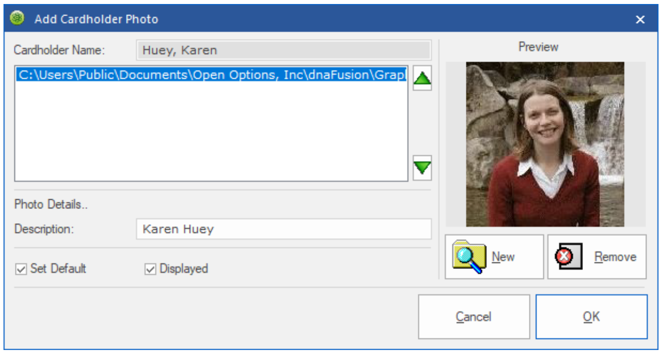
   Right-click in the Personnel Record and **select** Update.

Arranging Photos

Photos can be rearranged so that a recently added photo appears in the first position. Typically this would occur when printing badges.

1. **Right-click** inside the Employee Info tab of the Personnel Record and **select** Photo Properties.

   The Add Cardholder Photo dialog opens.

   Add Cardholder Photo

   Cardholder Name: Huey, Karen

   C:\Users\Public\Documents\Open Options, Inc\dnaFusion\Grapl

   Photo Details..

   Description: Karen Huey

   ☑ Set Default ☑ Displayed

2. **Select** the photo path and **click** the green arrows to move the photo up or down in the list.
3. **Click** OK.
4. To save the record, **click** the Update Cardholder button on the Personnel Toolbar or **right-click** in the Personnel Record and **select** Update.

Photo Recall

Photo Recall Windows display cardholder photos when the cardholder presents their card to a reader. Operators can configure up to four (4) separate windows; see page 7-41 for more information.

> ⓘ *Photos will only appear in the* Photo Recall Window *if* Use Revolving Recall Windows *is selected in the* DNA Properties *dialog. See page 3-5 for more information.*

Photo Recall Toolbar

The Photo Recall Toolbar contains quick-access commands related to the Photo Recall Window. The recall window must be open in order to use the toolbar.

Icon	Command	Description
	Go to Photo	Displays a drop-down list with the available photos.
	Zoom Out	Zooms out on the photo.
	Zoom In	Zooms in on the photo.
	Stop Cycling	Stops the photo recall cycle.
	Personnel Record	Displays the Personnel Record for the selected photo.
	Retrieve Note	Displays the Card Flags dialog.
	Pause	Pauses the photo recall cycle.
	E-Mail	E-mails the photo to the desired e-mail address.
	Other Photos	Displays the cardholder's other photos that were not flagged as the default.
	Setup Photo Recall	Displays the Photo Recall dialog.

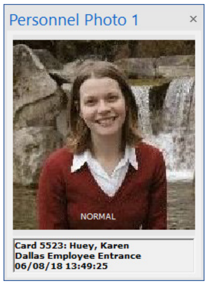
Opening a Photo Recall Window

To open a Photo Recall Window:

1. **Select** View / Windows / Photo Recall / Photo Recall 1-4 from the Main Menu.

   The selected window opens; it can remain open to compare the displayed photo with the employee's ID badge and/or the employee.

2. If this is the first time the Photo Recall Window has been used, **configure** the Photo Recall dialog. See page 7-41 for instructions.



Card 5523: Huey, Karen
Dallas Employee Entrance
06/08/18 13:49:25

Personnel Features

To access a personnel record, set card flags, or add a journal entry from the Photo Recall Window:

1. **Right-click** on the cardholder's photo and **select** Personnel.

   See page 7-35 for more information on cardholder features.

Configuring the Photo Recall Window

The Photo Recall Window must be configured before it will display photos.

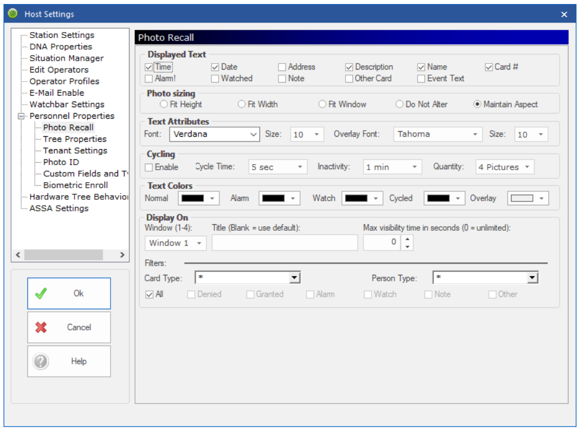


Photo Recall

Displayed Text: ☑ Time ☑ Date □ Address ☑ Description ☑ Name ☑ Card # □ Alarm! □ Watched □ Note □ Other Card □ Event Text

Photo sizing: ○ Fit Height ○ Fit Width ○ Fit Window ○ Do Not Alter ● Maintain Aspect

Text Attributes: Font: Verdana Size: 10 Overlay Font: Tahoma Size: 10

Cycling: □ Enable Cycle Time: 5 sec Inactivity: 1 min Quantity: 4 Pictures

Text Colors: Normal ■ Alarm ■ Watch ■ Cycled ■ Overlay □

Display On: Window (1-4): Window 1 Title (Blank = use default): Max visibility time in seconds (0 = unlimited): 0

Filters: Card Type: * Person Type: *

☑ All □ Denied □ Granted □ Alarm □ Watch □ Note □ Other

1. **Right-click** inside the Photo Recall Window and **select** Setup Photo Recall.

   OR

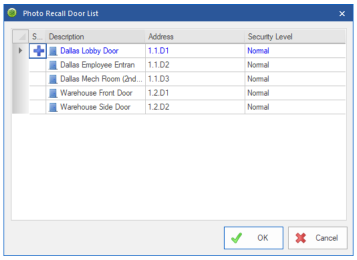
   Select Photo Properties / Photo Recall from the Host Settings.

   The Photo Recall dialog opens; see page 3-17 for more information.
2. **Check** the desired Displayed Text option(s) to display additional text or data in the Photo Recall Window.
3. **Select** a Photo Sizing radio button to set the photo dimensions in the Photo Recall Window.
4. **Select** the Text Attributes from the Font, Font Size, Overlay Font, and Overlay Font Size drop-down fields.
5. If desired, **select** the Enable checkbox to cycle the cardholder's photos.
6. If Cycling is enabled, **select** an option from the Cycle Time, Inactivity, and Quantity drop-down fields.
7. If desired, **select** a Text Color for Normal, Alarm, Watch, Cycled, and Overlay events.
8. If desired, **configure** the Display On setting for the desired window(s):
   - Window (1-4) - **Select** the Photo Recall Window from the drop-down.
   - Title - **Enter** text to change the title of the selected window. (Blank = Use Default)
   - Max Visibility Time in Seconds - **Enter** or **select** the maximum number of seconds to display the selected window. (0 = Unlimited).
   - Filters - **Select** a Card Type or Person Type from the drop-down menu(s).
9. **Click** OK to save the settings.

Assigning Specific Doors to a Photo Recall Window

If a specific door is assigned to the Photo Recall Window, cardholder photos will only appear in the window when the selected door is used.

> *This feature will NOT be available if* Use Revolving Recall Windows *is checked in the* DNA Properties *dialog.*



S...	Description	Address	Security Level
✚	Dallas Lobby Door	1.1.D1	Normal
	Dallas Employee Entran	1.1.D2	Normal
	Dallas Mech Room (2nd...	1.1.D3	Normal
	Warehouse Front Door	1.2.D1	Normal
	Warehouse Side Door	1.2.D2	Normal

1. **Right-click** in the Photo Recall Window and **select** Doors / Add Door.

   The Photo Recall Door List dialog appears.
2. **Select** the desired Door(s).

   A blue plus sign ✚ will appear.
3. **Click** OK.

   The selected door(s) will be assigned to the Photo Recall Window.

> *Alternatively, operators can drag and drop the desired door from the* Hardware Browser *to the* Photo Recall Window *to assign the door.*

Remove All Doors

To remove doors that have been assigned to a Photo Recall Window:

1. **Right-click** in the Photo Recall Window and **select** Doors / Remove All Doors.

   All doors assigned to the recall window will be removed.

Hardware Features 8

In This Chapter

DNA Fusion offers a number of different hardware features as well as the ability to control various hardware objects. Hardware features vary based on the selected object but include the ability to make journal entries related to the object and generate Who Has Access reports on the fly.

Hardware Browser

The Hardware Browser is an explorer window that contains a hierarchical "tree" of field devices that comprise the system. The hardware tree displays the status of objects by using status indicators to the left of the hardware object. Various licensed integrations may appear on the Hardware Browser.

To open the Hardware Browser:

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

   Or

   Select View / Explorers / Hardware from the Main Menu.

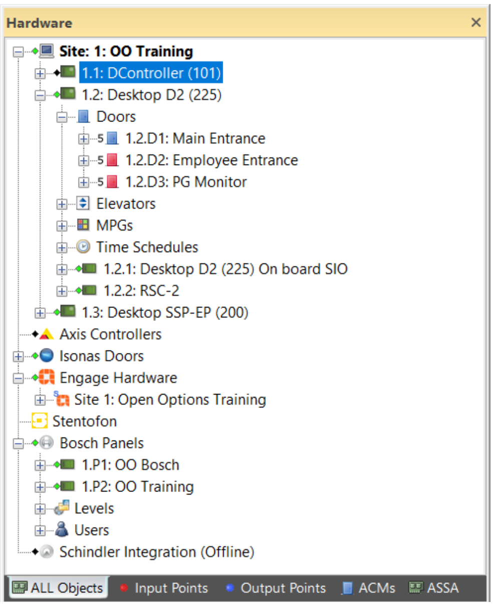
   The Hardware Browser appears.

   Status Indicators:

   - ◆ Green Diamond - Inactive
   - ◆ Red Diamond - Active
   - ◆ Yellow Diamond - Fault
   - ◆ Black Diamond - Offline

   Object Color:

   - Black - Normal condition
   - Gray - Offline object
   - Red - Alarm condition
   - Blue - Acknowledged alarm
   - Green - Returned to normal (but not acknowledged)



Hardware ✕

- Site: 1: OO Training
  - 1.1: DController (101)
  - 1.2: Desktop D2 (225)
    - Doors
      - 5 1.2.D1: Main Entrance
      - 5 1.2.D2: Employee Entrance
      - 5 1.2.D3: PG Monitor
    - Elevators
    - MPGs
    - Time Schedules
    - 1.2.1: Desktop D2 (225) On board SIO
    - 1.2.2: RSC-2
  - 1.3: Desktop SSP-EP (200)
- Axis Controllers
- Isonas Doors
- Engage Hardware
  - Site 1: Open Options Training
- Stentofon
- Bosch Panels
  - 1.P1: OO Bosch
  - 1.P2: OO Training
  - Levels
  - Users
- Schindler Integration (Offline)

ALL Objects | Input Points | Output Points | ACMs | ASSA

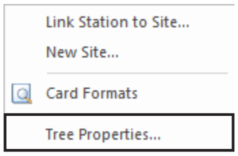
   Door Color:

   - Red Door - The door is currently in an alarm state, e.g. door held open or door forced open.
   - Blue Door - The door is currently in a normal state, e.g. closed.

Hover the mouse over a tree object in the Hardware Browser *to display the status of the object in the form of a tooltip.*

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 context menu.
3. **Configure** the settings. See page 3-27 for more information.

Hardware Toolbar

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

	Download Icon - Displays the Download Manager to download the database information to the controller.
	Control Icon - Displays the Direct Control Dialog for the selected hardware object.
	Hardware Properties Icon - Displays the Hardware Properties dialog for the selected hardware object. See pages 8-49 through 8-82 for more information on hardware properties.
	Add Hardware Icon - **Click** the arrow to display a drop-down menu of hardware objects. **Select** an option to display the Add dialog for the object. For more information on adding hardware, see Chapter 3: Hardware Configuration in the Technical Installation Manual.
	Delete Icon - Displays a confirmation dialog to delete the selected hardware object.
	Status Icon - Displays the Status dialog for the selected hardware object, if applicable.
	Default Template Icon - Applies the default template to the selected hardware object.
	Templates Icon - Displays the Template Manager dialog. See page 8-85 for more information.
	Watch Item Icon - Adds the selected hardware object to an existing Watch Window. The Watch Window must be open in order for this option to be available. For more information, see Chapter 15: Watch Window.
	Refresh Tree Icon - Updates the Hardware Browser tree.
	Homepage Icon - Launches the Home Page associated with the selected hardware object.
	Disable High Icon - Disables the IP Video Window from opening automatically on a High Priority alarm.
	Disable Normal Icon - Disables the IP Video Window from opening automatically on a Normal Priority alarm.
	Disable Low Icon - Disables the IP Video Window from opening automatically on a Low Priority alarm.
	Disable Custom Icon - Disables the IP Video Window from opening automatically on a Custom Priority alarm.
	Use Template Icon - Opens the Door Templates dialog for the selected hardware object. See page 8-85 for more information.

Controlling Doors

There are several ways to change the Door (Reader) Mode within the Hardware Browser. The mode, which is used for both doors and elevators, determines the type of access that the reader will allow.

There are also options to arm and disarm the Door Held and Door Forced status changes. This section will describe the various means of control including:

- The Door Options menu
- The Door Modes Toolbar
- The Direct Control Dialog

> *Access to door controls within DNA is not limited to the options above; try* **right-clicking** *on the door object in the* Watch Window*, from a* Graphics Map*, or in the* Events *or* Alarm Grid *and* **selecting** Hardware / Control*.*

Door Modes

The Door Mode indicates the state of a door. Below is an explanation of the various door modes.

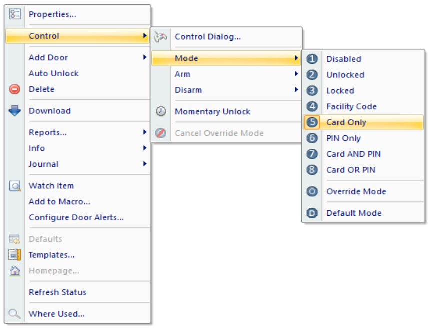
①	Reader Mode: Disabled Icon - Disables the reader. The door and all associated hardware objects remain locked without REX capability.
②	Reader Mode: Unlocked Icon - Unlocks the selected point and allows unlimited access. All cardholders will be granted access.
③	Reader Mode: Locked Icon - Locks the selected door. Card access will not be allowed, but the door can be used from the inside using the REX button.
④	Reader Mode: Facility Code Icon - Matches the facility code(s) stored in the SSP to approve entry. See page 8-83 for more information on facility codes.
⑤	Reader Mode: Card Only Icon - Requires a card with the correct card format and access level to be presented.
⑥	Reader Mode: PIN Icon - Requires a PIN code to be entered to gain access. PIN numbers are set in the Card Tab of the Cardholder's Record.
⑦	Reader Mode: Card AND PIN Icon - Both a card AND a PIN code are required to gain access to the associated point.
⑧	Reader Mode: Card OR PIN Icon - Either a card OR a PIN code is required to gain access to the associated point.
○	Override Mode Icon - Opens the Temporary ACR Override dialog. See page 8-5 for more information.
⊘	Cancel Override Mode Icon - Cancels the Temporary Override command. See page 8-6 for more information.
Ⓓ	Default Mode Icon - Sets the door to the Default Mode configured in the Door Objects dialog. See page 8-61 for more information.
P	Privacy Mode Icon - Only available for Schlage AD locks. The Privacy Mode prevents normal credentials from opening the door from the outside.
U	Office Mode Icon - Only available for Schlage AD locks. The Office Mode unlocks the door when a credential is presented, then automatically locks after the strike time has expired. To keep the door unlocked, push the button on the inside. The button will momentarily illuminate green. To return the lock to the locked state, push the button again or present a credential to the outside.
C	Classroom Mode Icon - Only available for Schlage AD locks. The Classroom Mode unlocks the door when a credential is presented, then automatically locks after the strike time has expired.

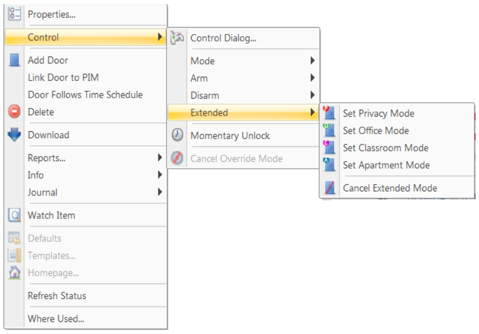
	Apartment Mode - Only available for Schlage AD locks. The Apartment Mode sets the door to be normally locked but never relocks the door automatically, which prevents users from being locked out. ● To unlock the door from the outside, present a credential. ● To unlock the door from the inside, push the inside button or, if using the MD chassis, retract the deadbolt. A means of egress is always available from the inside. ● When lever is rotated and door is opened, the request-to-exit switch is used in conjunction with the door position switch to cause the door to return to unlocked condition. ● To lock the door from the outside, present a credential. ● To lock the door from the inside, push the inside button or, for MD chassis, extend the deadbolt.
	Cancel Extended Mode - Only available for Schlage AD locks. Cancels the Extended Mode (Privacy, Office, Classroom or Apartment) commands.

Door Options

The easiest way to control a door is through the Door Options menu.

1. **Right-click** on the desired door(s) in the Hardware Browser.
   Use the Ctrl or Shift key to select multiple doors.





2. **Select** Control / Mode and **select** the correct Mode based on the table on page 8-3.

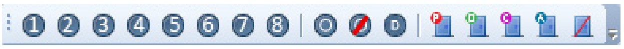
   The Door(s) change mode and the Reader Mode number changes in the Hardware Browser.

   The Door Options menu also includes access to Held / Forced as well as Momentary Unlock.

   If the door is equipped with a Schlage AD, an additional Extended item will appear in the menu.

Door Modes Toolbar

The Door Modes Toolbar allows quick access to change the door modes with the selection of a toolbar button. The desired door(s) must be selected before a toolbar button is used.



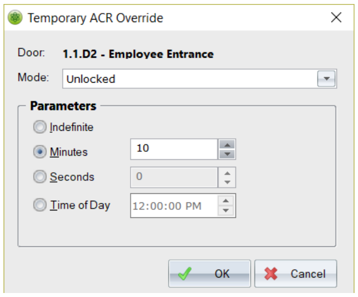
All the door modes as well as the Extended AD-400 lock modes can be accessed from the Door Modes Toolbar. For more information on secondary toolbars, see page 2-5.

Door Override Mode

The Door Override Mode can be used to override a door mode for a given amount of time. The selected mode is used during the specified time; once the temporary time expires, the door will revert back to its normal mode.

Example: A door is set up to be temporarily unlocked for five minutes to allow access without a card. If an event occurs that changes the door's mode (such as a time schedule becoming active), the door will not change to the new mode until the five minute override has passed or the override is cancelled.

The Door Override Mode has three possible parameters:



Temporary ACR Override

Door: **1.1.D2 - Employee Entrance**

Mode: Unlocked

Parameters

○ Indefinite

● Minutes 10

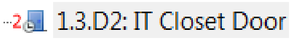
○ Seconds 0

○ Time of Day 12:00:00 PM

- Indefinite - Overrides the door's normal mode and sets the reader to the specified mode permanently. The override must be cancelled for the door to resume its normal state.
- Minutes - Sets the door mode on the selected door for the indicated amount of time. The number of minutes can be up to 16383 (over 11 days). The door will return to normal after the time has expired.
- Seconds - Sets the door mode on the selected door for the indicated amount of time. The number of seconds can be up to 100 seconds. The door will return to normal after the time has expired.
- Time of Day - Allows the operator to change the door mode until a specified ending time (in hours/ minutes).

  When using the Time of Day option, the mode will not necessarily end at the exact hour/minute you specify. Instead, it will last for a fixed number of whole minutes that is closest to the time specified.

  For example, if a door override mode was scheduled to end at 1:00:00 p.m., and it was 12:30:30 p.m. when the override was executed, the mode would end at 1:00:30 p.m.



When the Override Mode is used, a clock icon will appear on the Door in the Hardware Browser.

The Override Mode is supported in SSP-EP firmware 1.17.3. Support for the Time of Day parameter was added in 1.17.9, and support for the Indefinite parameter was added in 1.18.2.

Cancel Door Override Mode

After a door has been set in Override Mode, click the Cancel Override button. The door will return to its normal state.

Direct Control Dialog

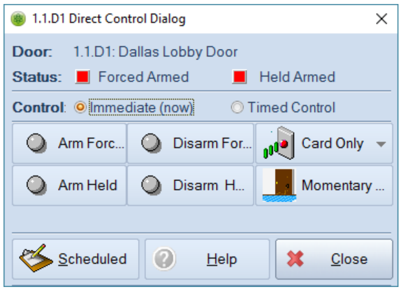
DNA allows the operator to directly perform various tasks on a selected door using the Direct Control Dialog. The dialog offers the following options:

- Change the Door Mode
- Issue a Momentary Unlock
- Arm & Disarm the Held and Forced Statuses
- Schedule One Time & Repeating Door Mode Changes

To open the Direct Control Dialog:

1. **Right-click** on the door(s) you wish to control and **select** Control / Control Dialog from the context menu.

   The Direct Control Dialog opens.



1.1.D1 Direct Control Dialog

Door: 1.1.D1: Dallas Lobby Door

Status: 🟥 Forced Armed 🟥 Held Armed

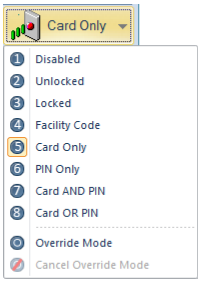
Control: ◉ Immediate (now) ○ Timed Control

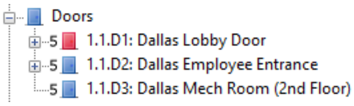
   - Door - Address and description of selected door (Read-only).
   - Status - Displays the Held and Forced statuses (Armed or Disarmed).
   - Control - Determines the type of control that will be executed.
     - □ Immediate Control - If selected, **click** a control item to immediately execute for the hardware object. See below for control information.
     - □ Timed Control - If selected, the Direct Control Dialog will expand and display scheduling options. See page 8-7 for more information on scheduling doors.

Immediate Control

1. **Select** the appropriate buttons to control the door.
   - Arm Forced - Arms the Door Forced alarm on a disarmed door.
   - Arm Held - Arms the Door Held alarm on a disarmed door.
   - Disarm Forced - Disarms the Door Forced alarm on an armed door. A green mask appears over the door icon. If both Forced and Held are disarmed, a red mask will appear.
   - Disarm Held - Disarms the Door Held alarm on an armed door. A blue mask appears over the door icon. If both Forced and Held are disarmed, a red mask will appear.
   - Door Mode - Indicates the current door mode for the door and displays a drop-down for the operator to set a new door mode. This setting determines the type of access that the reader will allow. See the table on page 8-3 and 8-4 for more information.

     The selected mode number appears next to the door object in the Hardware Browser. If the door is in an alarm state, the door will appear red in the Hardware Browser.





Doors
5 1.1.D1: Dallas Lobby Door
5 1.1.D2: Dallas Employee Entrance
5 1.1.D3: Dallas Mech Room (2nd Floor)

   - Momentary Unlock - When selected, unlocks the door for the Strike Time programmed in the Door Objects dialog. See page 8-61 for more information.
2. **Click** Close or X to close the dialog.

> *Doors can also be controlled by* **right-clicking** *on the* Door *and* **selecting** Control / Mode *to change the door mode or* Control / Arm or Disarm *to arm or disarm the door.*

Scheduling Doors (Timed Control)

The Timed Control option allows the operator to schedule two types of door control:

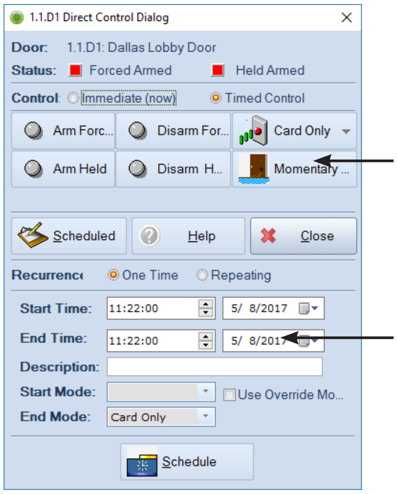
- One Time - A single event with defined Start/End Times as well as Start/End Modes. This type of scheduled control is stored in and initiated from the DNA driver at the time of the event.
- Repeating - Multiple regular occurrences based on a time schedule in which a trigger/macro combination is written and stored in the controller's memory. The time schedule must be created prior to the creation of the repeating control command. This can also be set up through the Door Properties / Auto Unlock dialog. See page 8-9 for more information.

One Time Scheduling

The One Time Scheduling feature offers the operator the ability to schedule a single event. This event will be stored in, and initiated from the driver at the time of the event.

1. **Select** the Timed Control radio button.

   The Scheduling section appears.



1.1.D1 Direct Control Dialog

Door: 1.1.D1: Dallas Lobby Door

Status: Forced Armed Held Armed

Control: ○ Immediate (now) ● Timed Control

Recurrence ● One Time ○ Repeating

Start Time: 11:22:00 5/ 8/2017

End Time: 11:22:00 5/ 8/2017

Description:

Start Mode:

□ Use Override Mo...

End Mode: Card Only

Timed Control Option

Scheduling Options

2. **Select** the One Time radio button.
3. **Enter** a Start Time and Date.
4. **Enter** a End Time and Date.
5. **Enter** a Description.

   This is a user-defined description for the action that will appear when the event is viewed in the future.
6. **Select** a Start Mode for the door(s) from the drop-down list. See table on page 8-3 for information.

   If desired, **check** Use Override Mode to apply the override functionality to the scheduled event. The Unlocked mode will auto-populate in the Start Mode drop-down.
7. **Select** an End Mode from the drop-down list.
8. **Click** the Schedule button.

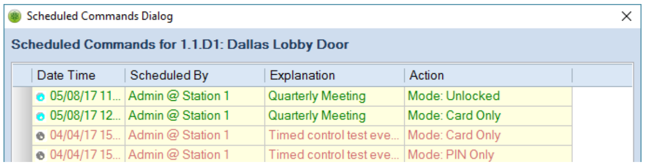
   A confirmation dialog will appear. **Click** OK.

   To view any scheduled commands, **click** the Scheduled button.

   The Scheduled Commands Dialog opens.

   If desired, **click** the History button to view previously scheduled commands.

   Future events are displayed in green while events that have already occurred appear red.



Scheduled Commands Dialog

Scheduled Commands for 1.1.D1: Dallas Lobby Door

Date Time	Scheduled By	Explanation	Action
05/08/17 11...	Admin @ Station 1	Quarterly Meeting	Mode: Unlocked
05/08/17 12...	Admin @ Station 1	Quarterly Meeting	Mode: Card Only
04/04/17 15...	Admin @ Station 1	Timed control test eve...	Mode: Card Only
04/04/17 15...	Admin @ Station 1	Timed control test eve...	Mode: PIN Only

Repeating Events

Repeating Scheduled Events are multiple regular occurrences of an event based on a time schedule. A trigger/macro combination will be written and stored in the controller's memory.

The time schedule must be created prior to the creation of the repeating control command. This function can be accomplished through the Door Properties. See page 8-9 for information.

1. **Select** the Timed Control radio button.

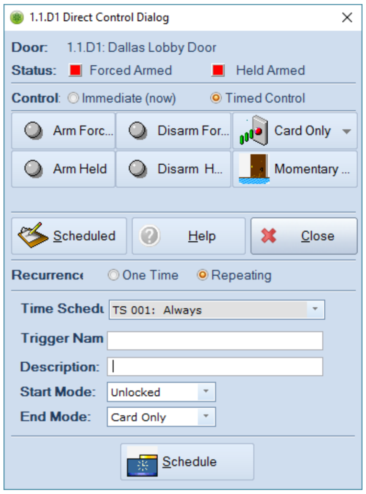
   The Direct Control Dialog will expand to show scheduling options.

2. **Select** the Repeating radio button.
3. **Select** a Time Schedule from the drop-down list to associate with the scheduled control.
4. **Enter** a Trigger Name.

   This is a user-defined name for the trigger that will appear in the Triggers & Macros Browser.

5. **Enter** a Description.
6. **Select** a Start Mode for the door(s) from the drop-down list.
7. **Select** an End Mode from the drop-down list.
8. **Click** the Schedule button to save the schedule.

   The wizard writes a trigger-and-macro combination that changes the door mode(s) based on the selected time schedule. The combination can be viewed by opening the Triggers & Macros Browser, selecting the correct SSP, and double-clicking the newly created trigger or macro. For more information on Triggers & Macros, see Chapter 10.



Door: 1.1.D1: Dallas Lobby Door
Status: 🟥 Forced Armed 🟥 Held Armed
Control: ○ Immediate (now) ● Timed Control
Recurrence: ○ One Time ● Repeating
Time Schedule: TS 001: Always
Trigger Name:
Description:
Start Mode: Unlocked
End Mode: Card Only

Controlling Multiple Doors

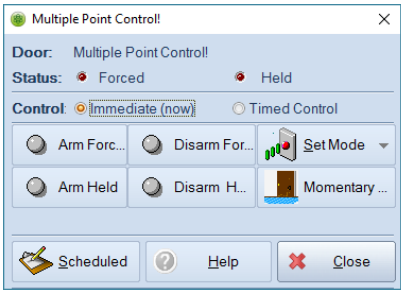
Multiple doors can be controlled at one time; this includes changing the door mode, arming or disarming the door, and scheduling commands.

1. **Select** the doors in the Hardware Browser using the Control or Shift key.

> **Select** *the* ACMs *tab in the* Hardware Browser *to display door objects only.*

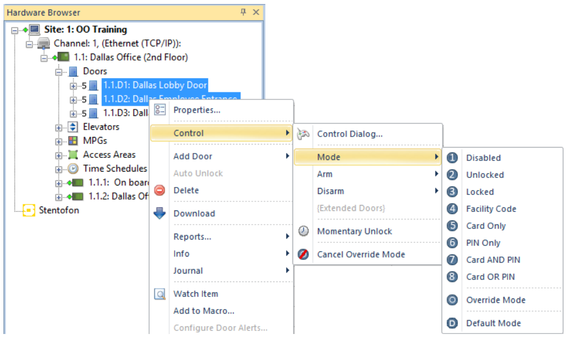
2. **Right-click** on the last door selected and **select** a Control option.

- Control Dialog - If selected, the Multiple Point Control! dialog opens. **Select** the desired option from the dialog. See page 8-6 for more information.



Door: Multiple Point Control!
Status: ● Forced ● Held
Control: ● Immediate (now) ○ Timed Control

- Context Menu - **Select** the Control option. See page 8-3 for more information.



Configuring a Door to Follow a Time Schedule

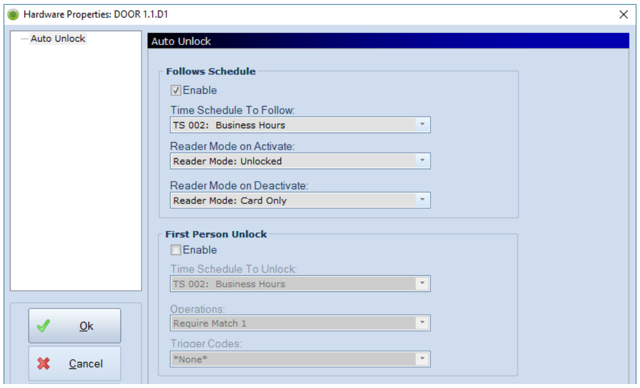
The Follows Schedule feature provides a quick way to set up a door(s) to adhere to a specified time schedule and designated door modes. If enabled, the system will generate a trigger-and-macro combination and store the commands in the controller's memory. The time schedule must be created prior to the repeating control command.

1. From the Door Properties dialog, **select** the Auto Unlock option from the dialog menu.

   Or

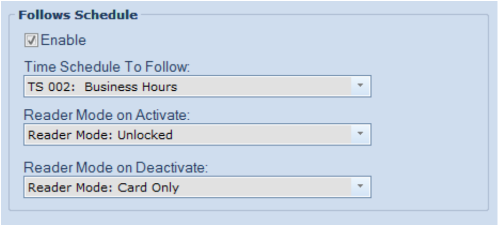
   Right-click on the Door in the Hardware Browser and **select** Auto Unlock from the context menu.

   The Auto Unlock dialog opens.



Follows Schedule
☑ Enable
Time Schedule To Follow: TS 002: Business Hours
Reader Mode on Activate: Reader Mode: Unlocked
Reader Mode on Deactivate: Reader Mode: Card Only

First Person Unlock
☐ Enable
Time Schedule To Unlock: TS 002: Business Hours
Operations: Require Match 1
Trigger Codes: *None*



Follows Schedule
☑ Enable
Time Schedule To Follow: TS 002: Business Hours
Reader Mode on Activate: Reader Mode: Unlocked
Reader Mode on Deactivate: Reader Mode: Card Only

2. In the Follows Schedule section, **select** the Enable checkbox to activate the feature.
3. **Select** the desired time schedule from the Time Schedule to Follow drop-down list.
4. **Select** the Door Mode to apply when the door's specified time schedule becomes active from the Reader Mode on Activate drop-down.
5. **Select** the Door Mode to apply when the door's specified time schedule becomes inactive from the Reader Mode on Deactivate drop-down.
6. **Click** OK to save the changes.

Configuring a Door to Use First Person Unlock

The First Person Unlock feature allows the operator to configure a door that will unlock during a specified time schedule after the first cardholder is granted access to the door. If enabled, the system will generate a trigger-and-macro combination and store it in the controller's memory.

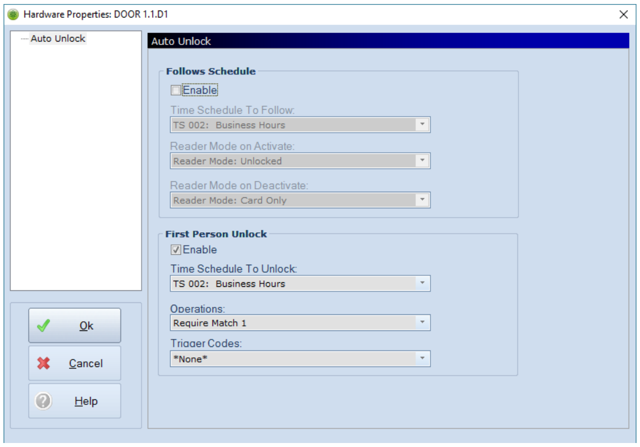
> *The door will remain in a secured mode even when the designated time schedule is active if no cardholders have accessed the door. Likewise, if a cardholder presents their card to the door when the time schedule is inactive, the door will remain secured.*

1. From the Door Properties dialog, **select** the Auto Unlock option from the dialog menu.

   Or

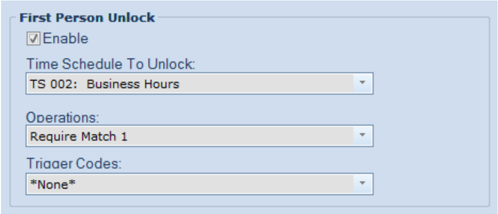
   Right-click on the Door in the Hardware Browser and **select** Auto Unlock from the context menu.

   The Auto Unlock dialog opens.



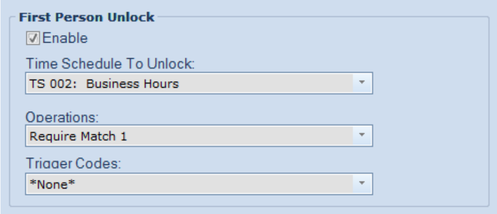
Follows Schedule
☐ Enable
Time Schedule To Follow: TS 002: Business Hours
Reader Mode on Activate: Reader Mode: Unlocked
Reader Mode on Deactivate: Reader Mode: Card Only

First Person Unlock
☑ Enable
Time Schedule To Unlock: TS 002: Business Hours
Operations: Require Match 1
Trigger Codes: *None*



First Person Unlock
☑ Enable
Time Schedule To Unlock: TS 002: Business Hours
Operations: Require Match 1
Trigger Codes: *None*

2. In the First Person Unlock section, **select** the Enable checkbox to activate the feature.



First Person Unlock

☑ Enable

Time Schedule To Unlock:
TS 002: Business Hours

Operations:
Require Match 1

Trigger Codes:
None

3. **Select** the desired time schedule from the Time Schedule to Unlock drop-down list.
4. **Select** an Operation from the drop-down list. See page 10-11 for more information.
5. **Select** a Trigger Code from the drop-down list. See page 10-11 for more information.
6. **Click** OK to save the changes.

Controlling Elevators

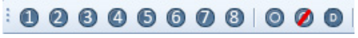
There are several ways to change the Elevator (Reader) Mode within the Hardware Browser (similar to doors). There are also options to arm and disarm the Held and Forced status changes. This section will describe the various means of control including:

- The Elevator Options menu
- The Door Modes Toolbar
- The Direct Control Dialog

> *Access to elevator controls within DNA is not limited to the above options; try* ***right-clicking*** *on the elevator object in the* Watch Window*, from a* Graphics Map*, or in the* Events *or* Alarm Grid *and* ***selecting*** Hardware / Control*.*

Door Modes Toolbar

The Door Modes Toolbar allows quick access to change the modes with the selection of a toolbar button. The desired elevator must be selected before the toolbar button is used.



For more information on secondary toolbars, see page 2-5. The following commands are available from the Door Modes Toolbar:

1	Reader Mode: Disabled Icon - Disables the reader. The door and all associated hardware objects remain locked without REX capability.
2	Reader Mode: Unlocked Icon - Unlocks the selected point and allows unlimited access. All cardholders will be granted access.
3	Reader Mode: Locked Icon - Locks the selected door. Card access will not be allowed, but the door can be used from the inside using the REX button.
4	Reader Mode: Facility Code Icon - Matches the facility code(s) stored in the SSP to approve entry. See page 8-81 for more information on facility codes.
5	Reader Mode: Card Only Icon - Requires a card with the correct card format and access level to be presented.
6	Reader Mode: PIN Icon - Requires a PIN code to be entered to gain access. PIN numbers are set in the Card Tab of the Cardholder's Record.
7	Reader Mode: Card AND PIN Icon - Both a card AND a PIN code are required to gain access to the associated point.
8	Reader Mode: Card OR PIN Icon - Either a card OR a PIN code is required to gain access to the associated point.
O	Override Mode Icon - Opens the Temporary ACR Override dialog. See page 8-12 for more information.
⊘	Cancel Override Mode Icon - Cancels the Temporary Override command. See page 8-12 for more information.
D	Default Mode Icon - Sets the elevator to the Default Mode configured in the Elevator Objects dialog. See page 8-69 for more information.

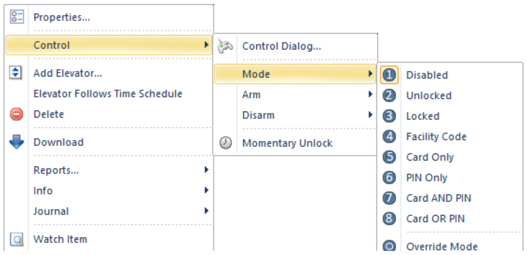
Elevator Options

The easiest way to control an elevator is through the Elevator Options menu.

1. **Right-click** on the desired elevator(s) in the Hardware Browser.
2. **Select** Control / Mode and **select** the correct Mode based on the table above.

   The Elevator Mode changes and the Reader Mode number changes in the Hardware Browser.

   The Elevator Options menu also includes access to Held / Forced as well as Momentary Unlock.

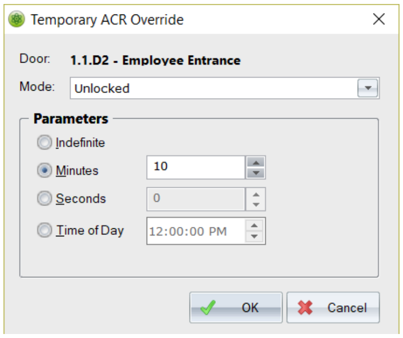


Elevator Override Mode

The Elevator Override Mode can be used to override an elevator mode for a given amount of time. The selected mode is used during the specified time; once the temporary time expires, the elevator will revert back to its normal mode.

Example: An elevator is set up to be temporarily unlocked for five minutes to allow access without a card. If an event occurs that changes the elevator's mode (such as a time schedule becoming active), the door will not change to the new mode until the five minute override has passed or the override is cancelled.

The Elevator Override Mode has three possible parameters:



Door: 1.1.D2 - Employee Entrance

Mode: Unlocked

Parameters

○ Indefinite

● Minutes 10

○ Seconds 0

○ Time of Day 12:00:00 PM

- Indefinite - Overrides the elevator's normal mode and sets the reader to the specified mode permanently. The override must be cancelled for the elevator to resume its normal state.
- Minutes - Sets the elevator mode on the selected elevator for the indicated amount of time. The number of minutes can be up to 16383 (over 11 days). The elevator will return to normal after the time has expired.
- Seconds - Sets the elevator mode on the selected door for the indicated amount of time. The number of seconds can be up to 100 seconds. The elevator will return to normal after the time has expired.
- Time of Day - Allows the operator to change the elevator mode until a specified ending time (in hours/minutes).

  When using the Time of Day option, the mode will not necessarily end at the exact hour/minute you specify. Instead, it will last for a fixed number of whole minutes that is closest to the time specified.

  For example, if an elevator override mode was scheduled to end at 1:00:00 p.m. and it was 12:30:30 p.m. when the override was executed, the mode would end at 1:00:30 p.m.

When the Elevator is set in Override Mode, a clock icon will appear on the Elevator in the Hardware Browser.

The Override Mode is supported in SSP-EP firmware 1.17.3. Support for the Time of Day parameter was added in 1.17.9, and support for the Indefinite parameter was added in 1.18.2.

Cancel Elevator Override Mode

After an elevator has been set in Override Mode, click the Cancel Override button. The elevator will return to its normal state.

Direct Control Dialog

DNA Fusion allows the operator to perform various direct tasks on a selected elevator using the Direct Control Dialog. The dialog offers the following options:

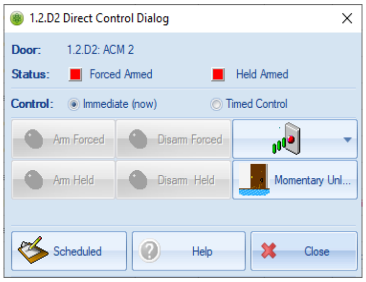
- Change the Elevator Mode
- Pulse a Designated Floor(s)
- Arm & Disarm the Held and Forced Statuses
- Schedule One Time & Repeating Elevator Mode Changes

> *Elevators can also be controlled by* **right-clicking** *on the* Elevator *and* **selecting** Control / Mode *to change the elevator reader mode.*

To open the Direct Control Dialog:

1. **Right-click** on the Elevator(s) and **select** Control / Control Dialog from the context menu.

   The Direct Control Dialog opens.



1.2.D2 Direct Control Dialog

Door: 1.2.D2: ACM 2

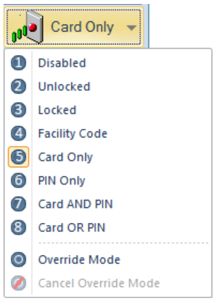
Status: 🟥 Forced Armed 🟥 Held Armed

Control: ● Immediate (now) ○ Timed Control

- Door - Address and description of the selected elevator (Read-only).
- Status - Displays the Held and Forced statuses (Armed or Disarmed).
- Control - Determines the type of control that will be executed.
  - ☐ Immediate Control - If selected, **click** a control item to immediately initiate. See below for control information.
  - ☐ Timed Control - If selected, the Direct Control Dialog will expand and display scheduling options. See page 8-15 for more information.

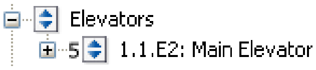
Immediate Control

1. **Select** the appropriate buttons to control the elevator.



- Elevator Mode - Indicates the current reader mode for the elevator and displays a drop-down for the operator to set the reader mode. This setting determines the type of access the reader will allow. See the table on page 8-11 for elevator mode information.

  The mode number appears next to the elevator object in the Hardware Browser.



- Pulse Floors - When selected, unlocks the selected floors for the amount of time specified in the Elevator Objects dialog. See page 8-69 for more information.

2. **Click** Close or X to close the dialog.

NOTES:

Scheduling Elevators (Timed Control)

The Timed Control option allows the operator to schedule two types of elevator control:

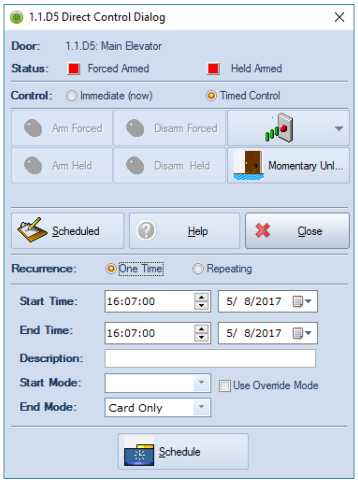
- One Time - A single event with defined Start/End Times as well as Start/End Modes. This type of scheduled control is stored and initiated from the DNA driver at the time of the event.
- Repeating - Multiple regular occurrences based on a time schedule in which a trigger/macro combination is written and stored in the controller's memory. The time schedule must be created prior to the creation of the repeating control command. This can also be set up through the Elevator Properties / Auto Unlock dialog.

One Time Scheduling

The One Time Scheduling feature offers the operator the ability to schedule a single event. This event will be stored in and initiated from the driver at the time of the event.

1. From the Direct Control Dialog, **select** the Timed Control radio button.

   The Scheduling section appears.



Door: 1.1.D5: Main Elevator

Status: 🟥 Forced Armed 🟥 Held Armed

Control: ○ Immediate (now) ● Timed Control

Recurrence: ● One Time ○ Repeating

Start Time: 16:07:00 5/ 8/2017

End Time: 16:07:00 5/ 8/2017

Description:

Start Mode: □ Use Override Mode

End Mode: Card Only

2. **Select** the One Time radio button.
3. If desired, **check** the Floors to be controlled in the Floors drop-down list.
4. **Enter** a Start Time and Date.
5. **Enter** an End Time and Date.
6. **Enter** a Description.

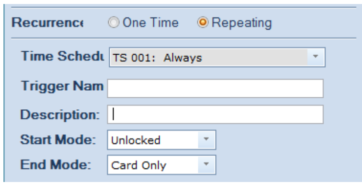
   This is a user-defined description for the action that will appear when the event is viewed in the future.
7. **Select** a Start Mode for the elevator(s) from the drop-down list.

   If desired, **check** Use Override Mode to apply the override functionality to the scheduled event. The Unlocked mode will auto-populate in the Start Mode drop-down.
8. **Select** an End Mode from the drop-down list.
9. **Click** the Schedule button.

   To view scheduled events, **click** the Scheduled button and **click** the History button.

Repeating Events

Repeating Scheduled Events are multiple regular occurrences of an event based on a time schedule. A trigger/macro combination will be written and stored in the controller's memory. The time schedule must be created prior to the creation of the repeating control command.



Recurrenc ○ One Time ● Repeating

Time Schedu TS 001: Always

Trigger Nam

Description:

Start Mode: Unlocked

End Mode: Card Only

1. **Select** the Repeating radio button.

   The Scheduling section will open.
2. If desired, **check** the Floors to be controlled in the Floors drop-down list.
3. **Select** a Time Schedule from the drop-down list to associate with the scheduled control.
4. **Enter** a Trigger Name.

   This is a user-defined name for the trigger that will appear in the Triggers & Macros Browser.

5. **Enter** a Description.
6. **Select** a Start Mode for the elevator(s) from the drop-down list.
7. **Select** an End Mode from the drop-down list.
8. **Click** the Schedule button to save the schedule.

   The wizard writes a trigger-and-macro combination that changes the elevator mode based on the selected time schedule. The combination can be viewed by opening the Triggers & Macros Browser, selecting the correct SSP and double-clicking the newly created trigger or macro. For more information on Triggers & Macros, see Chapter 10.

Controlling Multiple Elevators

Multiple elevators can be controlled at one time; this includes changing the elevator mode, arming or disarming the elevator, and scheduling events.

1. **Select** the elevators using the Control or Shift keys.
2. **Right-click** on the last elevator selected and **select** the control option.
   - Direct Control Dialog - **Select** the option from the dialog. See page 8-13 for more information.
   - Context Menu - **Select** the control option. See page 8-11 for more information.

Configuring an Elevator to Follow a Time Schedule

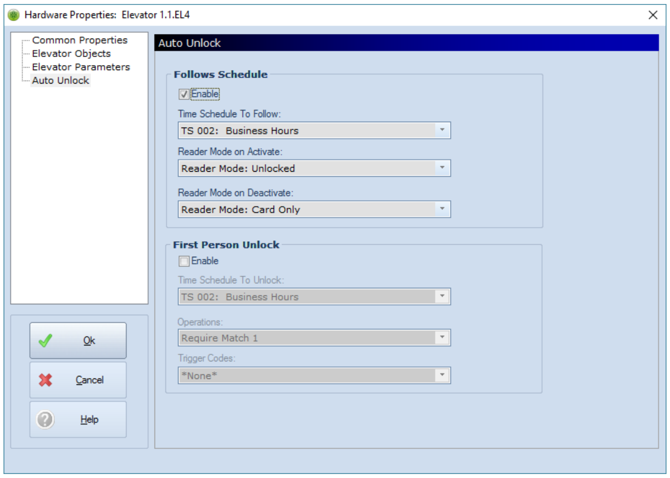
The Follows Schedule option provides a quick way to set up an elevator(s) to adhere to a specified time schedule and designated elevator modes. A system-generated trigger/macro combination is written and stored in the controller's memory. The time schedule must be created prior to the repeating control command.

1. From the Elevator Properties dialog, **select** the Auto Unlock option from the dialog menu.

   Or

   Right-click on the Elevator in the Hardware Browser and **select** the Elevator Follows Time Schedule option.

   The Auto Unlock dialog opens.



Hardware Properties: Elevator 1.1.EL4

Auto Unlock

Follows Schedule

☑ Enable

Time Schedule To Follow: TS 002: Business Hours

Reader Mode on Activate: Reader Mode: Unlocked

Reader Mode on Deactivate: Reader Mode: Card Only

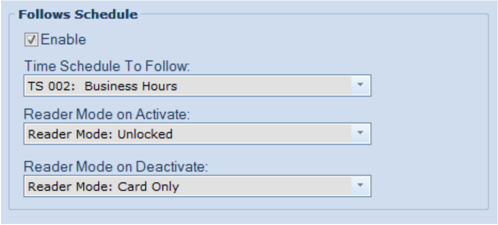
First Person Unlock

□ Enable

Time Schedule To Unlock: TS 002: Business Hours

Operations: Require Match 1

Trigger Codes: *None*



Follows Schedule

☑ Enable

Time Schedule To Follow: TS 002: Business Hours

Reader Mode on Activate: Reader Mode: Unlocked

Reader Mode on Deactivate: Reader Mode: Card Only

2. In the Follows Schedule section, **select** the Enable checkbox to activate the feature.
3. **Select** the desired time schedule from the Time Schedule to Follow drop-down list.
4. **Select** the Door Mode for the door when the specified time schedule becomes active from the Reader Mode on Activate drop-down list.
5. **Select** the Door Mode for the door when the specified time schedule becomes inactive from the Reader Mode on Deactivate drop-down list.
6. **Click** OK to save the changes.

Configuring an Elevator for First Person Unlock

The First Person Unlock feature allows the operator to configure an elevator that will unlock during a specified time schedule after the first cardholder is granted access to the reader. If enabled, the system will generate a trigger-and-macro combination and store it in the controller's memory. See page 8-9 for more information.

ACM Features

A number of features are available for doors and elevators, including the ability to see who has access to a specific door or trace the history of a selected ACM.

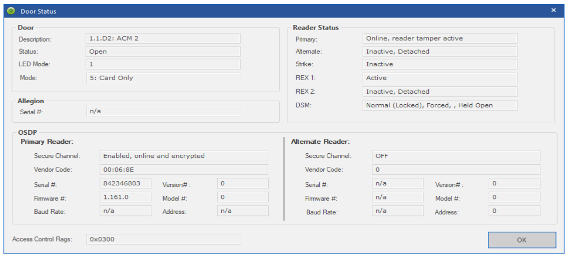
Status

Detailed status information, such as Door Status, Reader Mode, and Reader Status, can be displayed for the selected ACM using an InfoReady report.

1. **Right-click** on the ACM and **select** Info / Status.

   The Door Status dialog opens.

2. **Click** the OK button to close the dialog.



Door Status

Door

Description: 1.1.D2: ACM 2
Status: Open
LED Mode: 1
Mode: 5: Card Only

Allegion

Serial #: n/a

Reader Status

Primary: Online, reader tamper active
Alternate: Inactive, Detached
Strike: Inactive
REX 1: Active
REX 2: Inactive, Detached
DSM: Normal (Locked), Forced, , Held Open

OSDP

Primary Reader:

Secure Channel: Enabled, online and encrypted
Vendor Code: 00:06:8E
Serial #: 842346803 Version# : 0
Firmware #: 1.161.0 Model #: 0
Baud Rate: n/a Address: n/a

Alternate Reader:

Secure Channel: OFF
Vendor Code: 0
Serial #: n/a Version# : 0
Firmware #: n/a Model #: 0
Baud Rate: n/a Address: 0

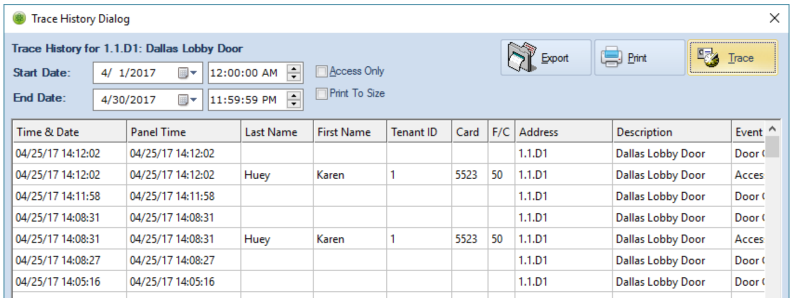
Access Control Flags: 0x0300

Trace History

A trace history report displays the last transactions for an ACM.

1. **Right-click** on the ACM and **select** Info / Trace History.

   The Trace History Dialog opens.



Trace History Dialog

Trace History for 1.1.D1: Dallas Lobby Door

Start Date: 4/ 1/2017 12:00:00 AM

End Date: 4/30/2017 11:59:59 PM

□ Access Only
□ Print To Size

Time & Date	Panel Time	Last Name	First Name	Tenant ID	Card	F/C	Address	Description	Event
04/25/17 14:12:02	04/25/17 14:12:02						1.1.D1	Dallas Lobby Door	Door (
04/25/17 14:12:02	04/25/17 14:12:02	Huey	Karen	1	5523	50	1.1.D1	Dallas Lobby Door	Acces
04/25/17 14:11:58	04/25/17 14:11:58						1.1.D1	Dallas Lobby Door	Door (
04/25/17 14:08:31	04/25/17 14:08:31						1.1.D1	Dallas Lobby Door	Door (
04/25/17 14:08:31	04/25/17 14:08:31	Huey	Karen	1	5523	50	1.1.D1	Dallas Lobby Door	Acces
04/25/17 14:08:27	04/25/17 14:08:27						1.1.D1	Dallas Lobby Door	Door (
04/25/17 14:05:16	04/25/17 14:05:16						1.1.D1	Dallas Lobby Door	Door (

2. If a wider time or date range is needed, **enter** the Start and End Date/Time and **click** the Trace button.

   If desired, narrow the results by **selecting** the Access Only checkbox and **clicking** the Trace button.

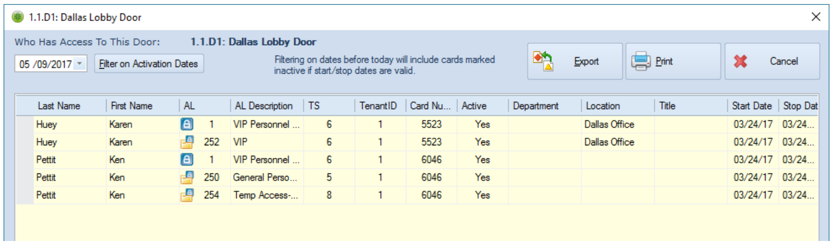
   The results can be exported, printed, or e-mailed by **selecting** the appropriate button. **Select** the Print to Size checkbox to size the report so that all columns appear on the same page.

Who Has Access

This feature allows you to generate an InfoReady report that details who has access to the selected ACM.

1. **Right-click** on the ACM and **select** Info / Who Has Access.

   The Who Has Access dialog appears.



1.1.D1: Dallas Lobby Door

Who Has Access To This Door: **1.1.D1: Dallas Lobby Door**

05 /09/2017

Filtering on dates before today will include cards marked inactive if start/stop dates are valid.

Last Name	First Name	AL	AL Description	TS	TenantID	Card Nu...	Active	Department	Location	Title	Start Date	Stop Dat
Huey	Karen	🔒 1	VIP Personnel ...	6	1	5523	Yes		Dallas Office		03/24/17	03/24...
Huey	Karen	📂 252	VIP	6	1	5523	Yes		Dallas Office		03/24/17	03/24...
Pettit	Ken	🔒 1	VIP Personnel ...	6	1	6046	Yes				03/24/17	03/24...
Pettit	Ken	📂 250	General Perso...	5	1	6046	Yes				03/24/17	03/24...
Pettit	Ken	📂 254	Temp Access-...	8	1	6046	Yes				03/24/17	03/24...

If the cardholder received their access from an Access Level Group, the icon 📂 will appear in the Access Level (AL) column. The results can be exported, printed, or e-mailed by **selecting** the appropriate button.

NOTES:

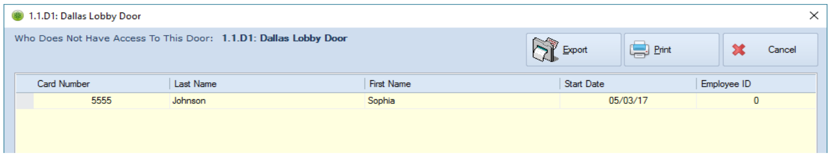
Who Does Not Have Access

This feature allows you to generate an InfoReady report that details who does not have access to the selected ACM.

1. **Right-click** on the ACM and **select** Info / Who Does Not Have Access.

   The Who Does Not Have Access dialog appears.

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

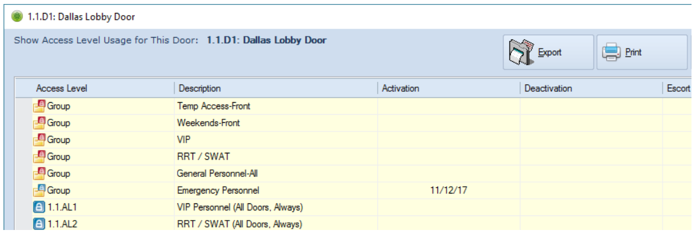


Who Does Not Have Access To This Door: **1.1.D1: Dallas Lobby Door**

Card Number	Last Name	First Name	Start Date	Employee ID
5555	Johnson	Sophia	05/03/17	0

Access Level Usage

The Access Level Usage feature allows you to generate an InfoReady report that details all of the access levels and access level groups associated with a selected ACM.



Show Access Level Usage for This Door: **1.1.D1: Dallas Lobby Door**

Access Level	Description	Activation	Deactivation	Escort
Group	Temp Access-Front			
Group	Weekends-Front			
Group	VIP			
Group	RRT / SWAT			
Group	General Personnel-All			
Group	Emergency Personnel	11/12/17		
1.1.AL1	VIP Personnel (All Doors, Always)			
1.1.AL2	RRT / SWAT (All Doors, Always)			

1. **Right-click** on the ACM object and **select** Info / Access Level Usage.

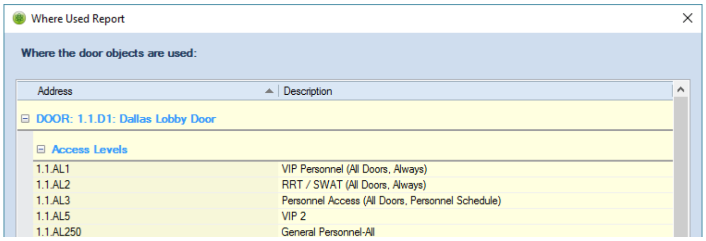
   The Access Level Usage dialog appears.

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

2. **Click** Cancel to close the dialog.

Where Used

The Where Used feature provides a grid displaying the doors associated relationships (i.e. triggers, macros, access levels, etc.).



Where the door objects are used:

Address	Description
DOOR: 1.1.D1: Dallas Lobby Door	
Access Levels	
1.1.AL1	VIP Personnel (All Doors, Always)
1.1.AL2	RRT / SWAT (All Doors, Always)
1.1.AL3	Personnel Access (All Doors, Personnel Schedule)
1.1.AL5	VIP 2
1.1.AL250	General Personnel-All

1. **Right-click** on the ACM object and **select** Where Used.

   The Where Used Report dialog opens.

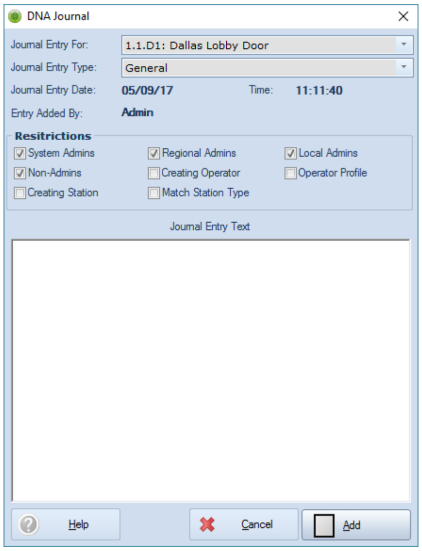
   The results can be exported to a CSV file or to the Clipboard using the Export button.

2. **Click** Cancel to close the dialog.

Journal Entries

The Journal feature allows you to record a text entry and view entries based on operator restrictions.

Creating a New Entry



Journal Entry For: 1.1.D1: Dallas Lobby Door

Journal Entry Type: General

Journal Entry Date: **05/09/17** Time: **11:11:40**

Entry Added By: **Admin**

Resitrictions

☑ System Admins ☑ Regional Admins ☑ Local Admins

☑ Non-Admins □ Creating Operator □ Operator Profile

□ Creating Station □ Match Station Type

1. **Right-click** on the ACM object and **select** Journal / New Entry.

   The DNA Journal dialog opens in entry mode.

2. **Configure** the DNA Journal log:

   - Journal Entry For - **Select** an entry component from the drop-down. Entries may be sorted based on this field.
   - Journal Entry Type - **Select** an entry category from the drop-down. Entries may be sorted based on this field.
   - Restrictions - **Select** the checkbox(es) to indicate who has the ability to view the journal entry.

3. **Place** cursor in the Journal Entry Text panel and **type** the desired message.

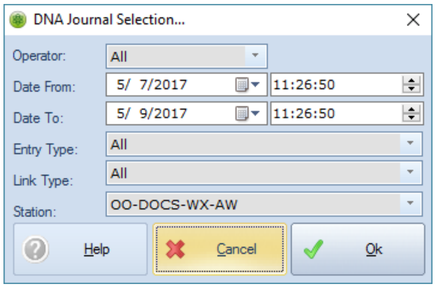
4. **Click** the Add button.

Viewing an Entry

1. **Right-click** on the ACM object and **select** Journal / View.

   The DNA Journal Selection dialog opens to view and filter entries.

2. **Configure** the DNA Journal Selection dialog.



Operator: All
Date From: 5/ 7/2017 11:26:50
Date To: 5/ 9/2017 11:26:50
Entry Type: All
Link Type: All
Station: OO-DOCS-WX-AW

3. **Click** the OK button to view the results.

   The DNA Journal Viewer will appear. The operator will only be able to view existing entries for which he/she has permission to access.

   The read-only fields indicate a journal entry’s properties, including the chronological sequence, author, station of origin, date and time, entry type, and entry link.

   Navigate through the entries using the green arrow buttons at the bottom of the panel.

4. When finished, **select** the Cancel button to close the dialog.

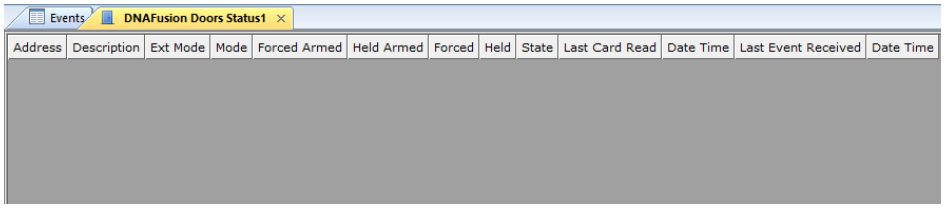
ACM Status Report

The ACM Status Report feature provides visibility to the status of any selected or configured ACMs; this includes both doors and elevators. The ACM Status Report is live and interactive so that the status of each object is updated in real-time and users are able to control the ACM directly from the status grid. It allows the operator to view all ACMs that are open or unlocked and documents each door status during shift changes in a simple grid environment.

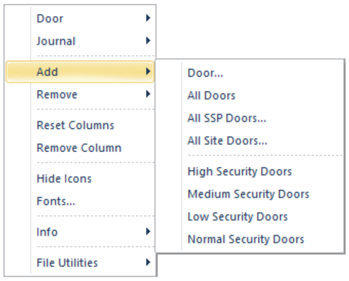
Generating an ACM Status Report

1. **Select** Hardware / ACM Status Report / New Report from the Main Menu.

   A blank ACM Status Grid appears.



Address	Description	Ext Mode	Mode	Forced Armed	Held Armed	Forced	Held	State	Last Card Read	Date Time	Last Event Received	Date Time



2. **Right-click** in the grid and **select** Add.

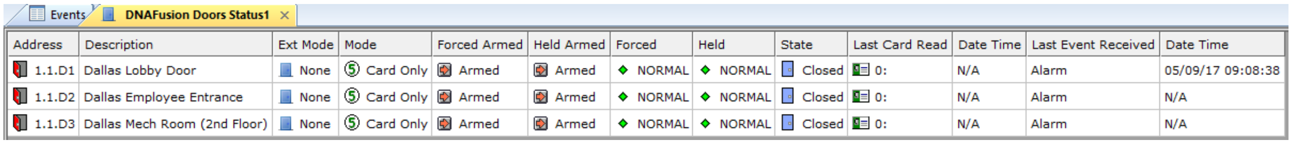
   The Add menu appears.

3. **Select** an option from the menu:

   - Door - Opens the Get Hardware Object dialog and allows the operator to **select** individual Doors. **Select** the Door from the drop-down list and **click** the OK button.
   - All Doors - Adds all Doors to the ACM Status Grid.
   - All SSP Doors - Opens the Get Hardware Object dialog and allows the operator to add Doors by selecting a Controller from the drop-down list.
   - All Site Doors - Opens the Get Hardware Object dialog and allows the operator to add Doors by selecting a Site from the drop-down list.
   - High Security Doors - Adds all the Doors that are designated as High Security to the ACM Status Grid.
   - Medium Security Doors - Adds all the Doors that are designated as Medium Security to the ACM Status Grid.
   - Low Security Doors - Adds all the Doors that are designated as Low Security to the ACM Status Grid.
   - Normal Security Doors - Adds all the Doors that are designated as Normal Security to the ACM Status Grid.

> ⓘ *Door security settings are configured in the* Door Objects *dialog. See page 8-61 for more information.*

The grid is populated with the selected Doors.

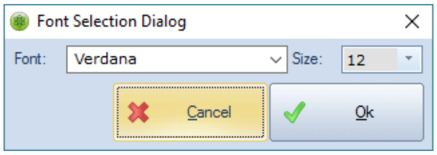


Address	Description	Ext Mode	Mode	Forced Armed	Held Armed	Forced	Held	State	Last Card Read	Date Time	Last Event Received	Date Time
1.1.D1	Dallas Lobby Door	None	Card Only	Armed	Armed	NORMAL	NORMAL	Closed	0:	N/A	Alarm	05/09/17 09:08:38
1.1.D2	Dallas Employee Entrance	None	Card Only	Armed	Armed	NORMAL	NORMAL	Closed	0:	N/A	Alarm	N/A
1.1.D3	Dallas Mech Room (2nd Floor)	None	Card Only	Armed	Armed	NORMAL	NORMAL	Closed	0:	N/A	Alarm	N/A

Formatting a Report

1. **Right-click** in the configured ACM Status Grid.

   - Remove Column - Removes the selected column from the grid.
   - Reset Columns - Resets the columns to the default setting.
   - Hide Icons - Removes the icons from the grid.
   - Fonts - Opens the Font Selection Dialog to configure the grid's font settings.



Font: Verdana
Size: 12

Saving an ACM Status Report

To save an ACM Status Report for future use:

1. **Right-click** in the configured ACM Status Grid.
2. **Select** File Utilities / Save As from the resulting menu.

   The Save As dialog opens.
3. **Enter** a Name for the report and **click** the Save button.

Opening a Saved ACM Status Report

To open a saved ACM Status Report:

1. **Select** Hardware / ACM Status / Open from the Main Menu.

   The Open dialog appears.
2. **Select** the ACM Report and **click** the Open button.

   The ACM Status Report opens.

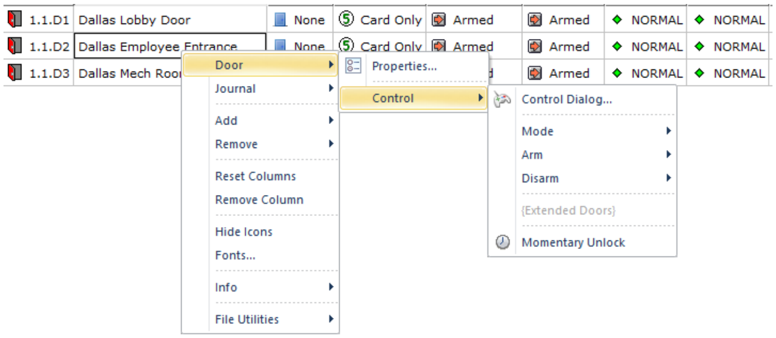
ACM Status Features

A number of features are available from the ACM Status Grid.

Controlling an ACM

1. **Right-click** on a Door in the ACM Status Grid and **select** Door / Control from the context menu.

   The Control menu appears.



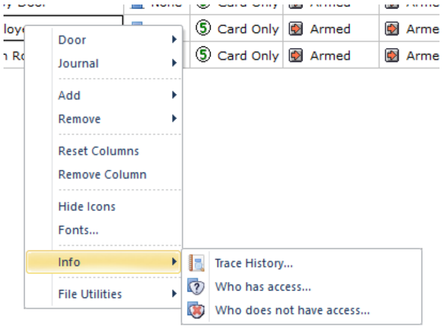
1.1.D1	Dallas Lobby Door	None	Card Only	Armed	Armed	NORMAL	NORMAL
1.1.D2	Dallas Employee Entrance	None	Card Only	Armed	Armed	NORMAL	NORMAL
1.1.D3	Dallas Mech Roo			d	Armed	NORMAL	NORMAL

2. **Select** a Control option.

   For more information on controlling doors, see page 8-3.

Info

Trace History



1. **Right-click** on the Door and **select** Info / Trace History.

   The Trace History Dialog will open. See page 8-17 for more information.

Who Has Access

1. **Right-click** on the Door and **select** Info / Who Has Access.

   The Who Has Access dialog appears. See page 8-17 for more information.

Who Does Not Have Access

1. **Right-click** on the Door and **select** Info / Who Does Not Have Access.

   The Who Does Not Have Access dialog appears. See page 8-17 for more information.

Controlling Input/Output Points

There are a number of ways to control the input and output points within the Hardware Browser (similar to doors). This section will describe the various means of control for both inputs and outputs including:

- The Point Options menu
- The Direct Control Dialog

Input / Output Options

The easiest way to control an input or output point is through the Point Options menu.

1. **Right-click** on the desired input or output point(s) in the Hardware Browser.
2. **Select** the correct State for the point(s) from the Control menu: Arm/Disarm for inputs or Activate/ Deactivate for outputs.

   The point(s) change state and the Hardware Tree is updated to reflect the state change. If an input is Disarmed, a colored box will appear over the input. If an output is Activated, the diamond next to the point will change from green to red. See page 8-24 for more detailed information.

> *Access to input/output controls within DNA is not limited to the above options; try* **right-clicking** *on the* Input *or* Output *in the* Watch Window*, from a* Graphics Map*, or in the* Events or Alarm Grid *and* **selecting** Hardware / Control*.*

Direct Control Dialog

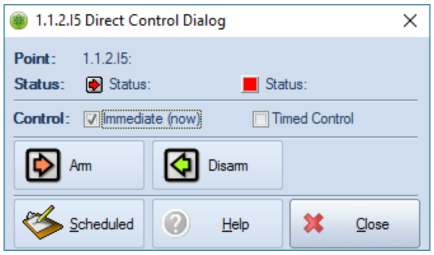
DNA allows the operator to perform various direct tasks on a selected input or output point(s) using the Direct Control Dialog. The dialog offers the following options:

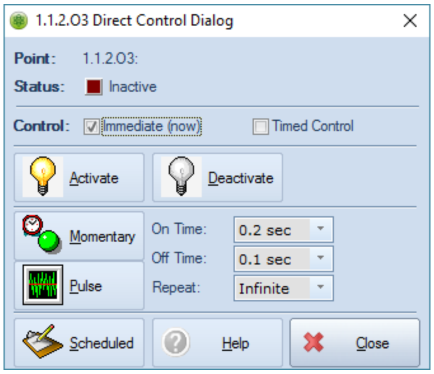
- Arm & Disarm the Input Point(s)
- Activate & Deactivate the Output Point(s)
- Momentary Activate or Pulse the Output Point(s)
- Schedule One Time & Repeating Arm & Disarm Events
- Schedule One Time & Repeating Activate & Deactivate Events

To open the Direct Control Dialog:

1. **Right-click** on the input or output point(s) you wish to control and **select** Control / Control Dialog from the context menu.

   The Direct Control Dialog will open for the selected point(s).

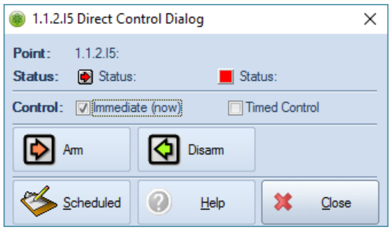

1.1.2.I5 Direct Control Dialog
Point: 1.1.2.I5:
Status: Status: Status:
Control: ☑ Immediate (now) □ Timed Control
Arm
Disarm
Scheduled
Help
Close



- Point - Address and description for the selected point (Read-only).
- Status - Armed status for the selected point (Armed/Disarmed or Active/Inactive).
- Control - Determines the type of control that will be executed.
  - □ Immediate (Now) - If checked, **select** a control item to immediately initiate. See page 8-24 for more information.
  - □ Timed Control - If checked, the Direct Control Dialog will expand to display scheduling options. See page 8-25 for more information.

Immediate Control

1. **Select** the appropriate buttons to control the input or output point(s):


1.1.2.I5 Direct Control Dialog

Point: 1.1.2.I5:

Status: Status: Status:

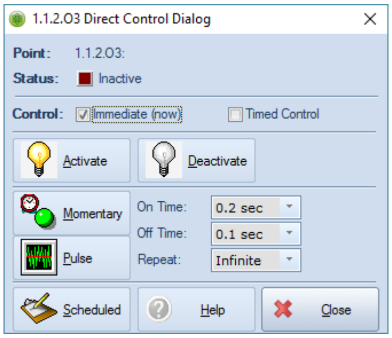
Control: ☑ Immediate (now) □ Timed Control

Input Options

- Arm - Arms the selected input point and logs the change of state in the Events Grid.
- Disarm - Disarms the selected input point. A red mask appears over the point in the Hardware Browser. The change of state is logged in the Events Grid; however, no alarm is generated.

Output Options

- Activate - Activates the selected output point and turns the indicator red.
- Deactivate - Deactivates the selected output point and turns the indicator green.
- Momentary - Activates the output for a specified amount of time.
- Pulse - Pulses the output point for a specified amount of time.
- On Time - Specifies the amount of time the point is active when a momentary or pulse command is executed.
- Off Time - Specifies the amount of time the point is inactive when a momentary or pulse command is executed.
- Repeat - Number of times the pulse will repeat when a Pulse command is executed.


1.1.2.O3 Direct Control Dialog

Point: 1.1.2.O3:

Status: Inactive

Control: ☑ Immediate (now) □ Timed Control

On Time: 0.2 sec

Off Time: 0.1 sec

Repeat: Infinite

2. **Click** Close or X to close the dialog.

Scheduling Input & Output Points (Timed Control)

The Timed Control option allows the operator to schedule two types of input/output control:

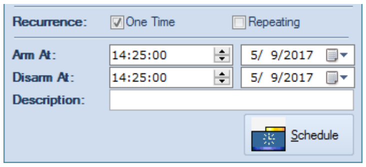
- One Time - A single event with defined Start/End Times as well as States. This type of scheduled control is stored in the host and is initiated from the DNA driver at the time of the event.
- Repeating - Multiple regular occurrences based on a time schedule in which a trigger/macro combination is written and stored in the controller's memory. The time schedule must be created prior to the creation of the repeating control command.

One Time Scheduling

The One Time Scheduling feature allows the operator to schedule a single event. This event will be stored in, and initiated from the driver at the time of the event. Consequently, the host computer must be on and DNA Fusion must be running at the time of the event. DNA can be at the login screen, but it must be running.

1. **Select** the Timed Control checkbox.

   The Scheduling section will open.

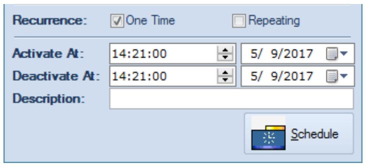


Recurrence: ☑ One Time ☐ Repeating

Arm At: 14:25:00 5/ 9/2017

Disarm At: 14:25:00 5/ 9/2017

Description:



Recurrence: ☑ One Time ☐ Repeating

Activate At: 14:21:00 5/ 9/2017

Deactivate At: 14:21:00 5/ 9/2017

Description:

2. **Select** the One Time checkbox.
3. **Enter** an Arm At Time and Date for inputs or **enter** an Activate At Time and Date for outputs.
4. **Enter** a Disarm At Time and Date for inputs or **enter** a Deactivate At Time and Date for outputs.
5. **Enter** a Description.

   This is a user-defined description that will appear when the event is viewed in the future.
6. **Click** the Schedule button.

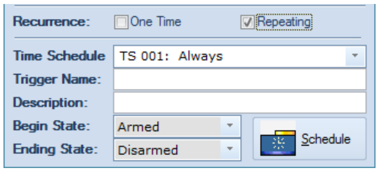
   To view any scheduled events, **click** the Scheduled button. To view past events, **click** the History button.

Repeating Events

Repeating Scheduled Events are multiple regular occurrences of an event based on a time schedule. A trigger/macro combination will be written and stored in the controller's memory. The time schedule must be created prior to the creation of the repeating control command.

1. **Select** the Timed Control checkbox.

   The Scheduling section will open.
2. **Select** the Repeating checkbox.
3. **Select** a Time Schedule from the drop-down list to associate with the scheduled control.



Recurrence: ☐ One Time ☑ Repeating

Time Schedule: TS 001: Always

Trigger Name:

Description:

Begin State: Armed

Ending State: Disarmed

4. **Enter** a Trigger Name.

   This is a user-defined name for the trigger that will appear in the Triggers & Macros Browser.
5. **Enter** a Description.
6. **Select** a Begin State from the drop-down list.
7. **Select** an Ending State from the drop-down list.
8. **Click** the Schedule button to save the schedule.

   The wizard writes a trigger-and-macro combination that changes the point's state based on the selected time schedule. The combination can be viewed by opening the Triggers & Macros Browser, selecting the correct SSP and double-clicking the newly created trigger or macro.

   For more information on Triggers & Macros, see Chapter 10.

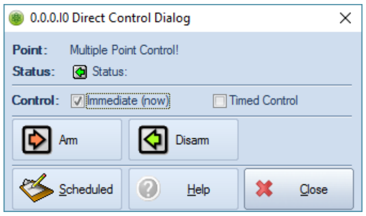
Controlling Multiple Points

Multiple input and output objects may be controlled at one time; this includes changing properties as well as scheduling events.

1. **Press** the Ctrl or Shift key and **select** the desired Input and Output Points.

> *The* Ctrl *and* Shift *keys can be used to select multiple items in the DNA Fusion environment. Press the* Ctrl *key to select multiple items individually or the* Shift *key to select all items between two points.*

2. **Right-click** on the last object selected and **select** Control / Control Dialog from the context menu.

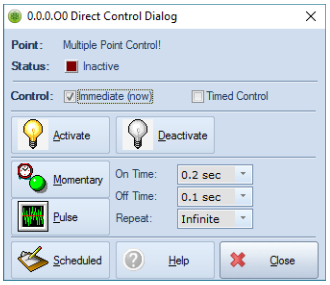


0.0.0.I0 Direct Control Dialog

Point: Multiple Point Control!

Status: Status:

Control: ☑ Immediate (now) □ Timed Control



0.0.0.O0 Direct Control Dialog

Point: Multiple Point Control!

Status: Inactive

Control: ☑ Immediate (now) □ Timed Control

On Time: 0.2 sec

Off Time: 0.1 sec

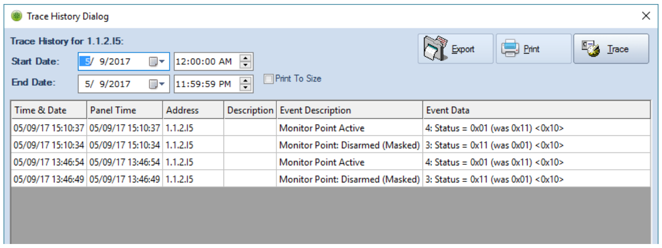
Repeat: Infinite

Trace History

A Trace History report can be run to view the last transactions of an input or output point.

1. **Right-click** on the Point and **select** Trace History.

   The Trace History Dialog opens.



Trace History Dialog

Trace History for 1.1.2.I5:

Start Date: 5/ 9/2017 12:00:00 AM

End Date: 5/ 9/2017 11:59:59 PM □ Print To Size

Time & Date	Panel Time	Address	Description	Event Description	Event Data
05/09/17 15:10:37	05/09/17 15:10:37	1.1.2.I5		Monitor Point Active	4: Status = 0x01 (was 0x11) <0x10>
05/09/17 15:10:34	05/09/17 15:10:34	1.1.2.I5		Monitor Point: Disarmed (Masked)	3: Status = 0x11 (was 0x01) <0x10>
05/09/17 13:46:54	05/09/17 13:46:54	1.1.2.I5		Monitor Point Active	4: Status = 0x01 (was 0x11) <0x10>
05/09/17 13:46:49	05/09/17 13:46:49	1.1.2.I5		Monitor Point: Disarmed (Masked)	3: Status = 0x11 (was 0x01) <0x10>

2. If a wider time or date range is needed, **enter** the Start and End Date/Time and **click** the Trace button.

   If desired, narrow the results by **selecting** Access Only and **clicking** the Trace button.

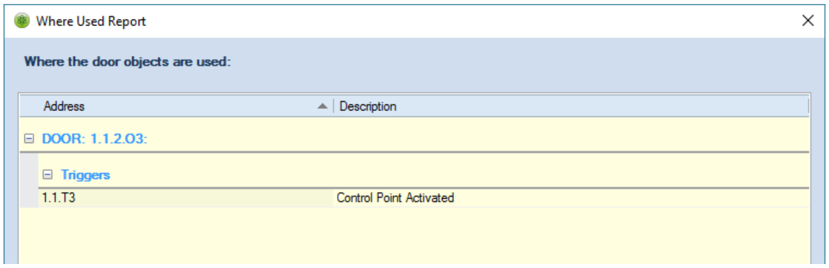
   The results can be exported, printed, or e-mailed by selecting the appropriate button.

Where Used

The Where Used feature provides a grid displaying the door's associated relationships, i.e. triggers, macros, access levels, etc.

1. **Right-click** on the Input or Output Point and **select** Where Used.

   The Where Used Report dialog appears.



Where Used Report

Where the door objects are used:

Address	Description
⊟ DOOR: 1.1.2.O3:	
⊟ Triggers	
1.1.T3	Control Point Activated

The results can be exported to a CSV file or to the Clipboard using the Export button.

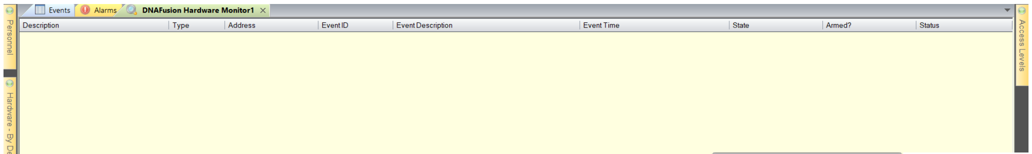
Hardware Monitor Report

The Hardware Monitor Report feature provides visibility to the status of any selected inputs, outputs and monitor point groups. The Hardware Monitor Report is live and interactive so that the status of each object is updated in real-time and users are able to control the points directly from the status grid. It allows the operator to view all points along with their status in a simple grid environment.

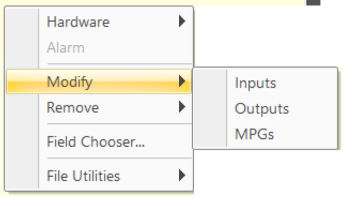
Generating a Hardware Monitor Report

1. **Select** Hardware / Hardware Monitor Report / New Report from the Main Menu.

   A blank Hardware Monitor Grid appears.



Description	Type	Address	Event ID	Event Description	Event Time	State	Armed?	Status

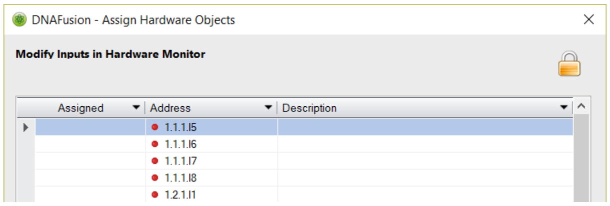


2. **Right-click** in the grid and **select** Modify.

   A context menu appears with the following options.

3. **Select** the desired option from the menu:

   - Inputs - Opens the Assign Hardware Object dialog and allows the operator to **select** individual Inputs. **Select** the Inputs from the list and **click** the OK button.

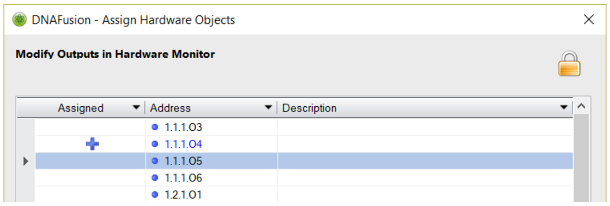


DNAFusion - Assign Hardware Objects

Modify Inputs in Hardware Monitor

Assigned	Address	Description
	1.1.1.I5	
	1.1.1.I6	
	1.1.1.I7	
	1.1.1.I8	
	1.2.1.I1	

   - Outputs - Opens the Assign Hardware Object dialog and allows the operator to **select** individual Output Points. **Select** the Outputs from the list and **click** the OK button.

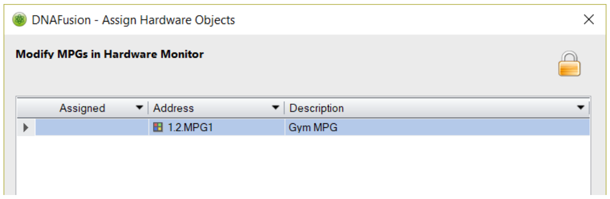


DNAFusion - Assign Hardware Objects

Modify Outputs in Hardware Monitor

Assigned	Address	Description
	1.1.1.O3	
✚	1.1.1.O4	
	1.1.1.O5	
	1.1.1.O6	
	1.2.1.O1	

   - MPGs - Opens the Assign Hardware Object dialog and allows the operator to **select** individual Monitor Point Groups. **Select** the MPGs from the list and **click** the OK button.



DNAFusion - Assign Hardware Objects

Modify MPGs in Hardware Monitor

Assigned	Address	Description
	1.2.MPG1	Gym MPG

The grid is populated with the selected objects.

Formatting a Report

1. **Right-click** in the configured Hardware Monitor Report Grid and select the Field Chooser item.

   - To Remove Column - Drag the column from the header row.
   - Add Columns - Drag the desired option from the Field Chooser dialog.
   - Hide Icons - Removes the icons from the grid.
   - Fonts - Opens the Font Selection Dialog to configure the grid's font settings.

Saving a Hardware Monitor Report

To save the Hardware Monitor Report for future use:

1. **Right-click** in the configured Hardware Monitor Report Grid.
2. **Select** File Utilities / Save As from the resulting menu.

   The Save As dialog opens.
3. **Enter** a Name for the report and **click** the Save button.

Opening a Saved Monitor Point Report

To open a saved Hardware Monitor Report:

1. **Select** Hardware / Monitor Point Group Report / Open from the Main Menu.

   The Open dialog appears.
2. **Select** the Monitor Point Group Report and **click** the Open button.

   The Report opens.

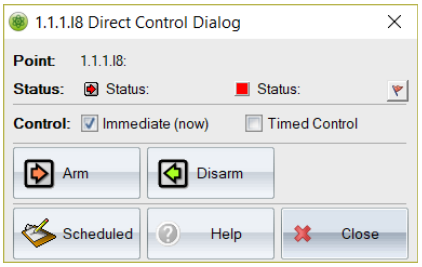
Hardware Monitor Features

A number of features are available from the Hardware Monitor Grid.

Controlling an Object

1. **Right-click** on an Object in the Hardware Monitor Report Grid and **select** Hardware / Control from the context menu.

   The Control menu appears.

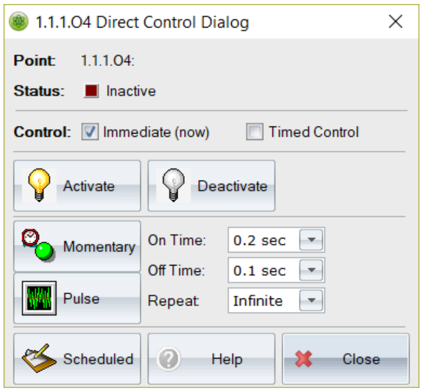


1.1.1.I8 Direct Control Dialog

Point: 1.1.1.I8:

Status: Status: Status:

Control: ☑ Immediate (now) ☐ Timed Control



1.1.1.O4 Direct Control Dialog

Point: 1.1.1.04:

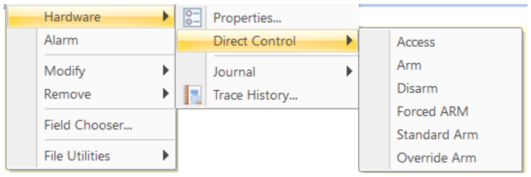
Status: Inactive

Control: ☑ Immediate (now) ☐ Timed Control

On Time: 0.2 sec

Off Time: 0.1 sec

Repeat: Infinite



2. **Select** a Control option.

   For more information on controlling inputs and outputs, see page 8-23.

Info

Trace History

1. **Right-click** on the Object and **select** Hardware / Trace History.

   The Trace History Dialog will open. See page 8-17 for more information.

Direct Commands

Direct commands can be used to link various commands together so that multiple items can be controlled at once. Users can create a custom button and link it to the direct command. For instance, a user may create a button that will directly unlock a specific door. The user can add the button to a new or existing toolbar and then place the toolbar in the main header of the application or on a graphic map for convenient access.

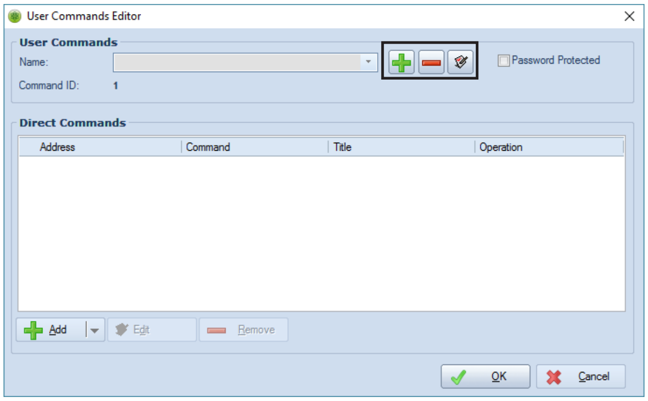
There are two steps to creating a custom button:

- Create the direct command
- Add the command to a toolbar

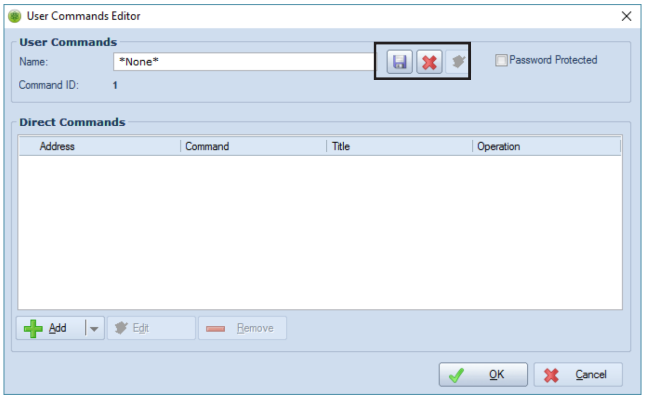
Creating a Direct Command

1. **Select** Hardware / Direct Commands / Manage from the Main Menu.

   The User Commands Editor dialog opens.



Command ID: 1



Name: *None*

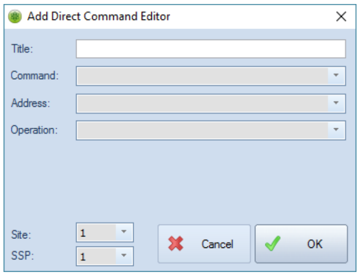
Command ID: 1

2. In the User Commands section, **click** the Add + button and **enter** a Name for the user command.
3. If desired, **select** the Password Protected checkbox.

   Note: If checked, DNA Fusion will prompt the user to enter his/her password before the command will be executed.
4. **Click** the Add + Add ▾ button in the Direct Commands section.

   The Add Direct Command Editor dialog opens.

   If an ASSA-, Mercury-, Engage-, or AXIS-based hardware command will be added, **click** the drop-down arrow next to the Add button and **select** the appropriate option from the menu. For more information see related integration manual.



Site: 1

SSP: 1

5. **Enter** a Title for the direct command.
6. **Select** the desired option from the Command drop-down menu.

   Depending on your selection, the remaining dialog fields will change.
7. **Select** the desired options from the Address and Operations drop-down lists.

   If the command is Set Temporary Override Mode, Process Batch File, Send Keypad Text, or Simulated Card Read, the user will need to configure other fields. If the command refers to a control point, the On Time, Off Time, and Repeat options may be configured.
8. **Select** the appropriate Site and SSP from the drop-down lists.
9. **Click** OK to save the command.

   The command will appear in the Direct Commands section of the User Commands Editor.

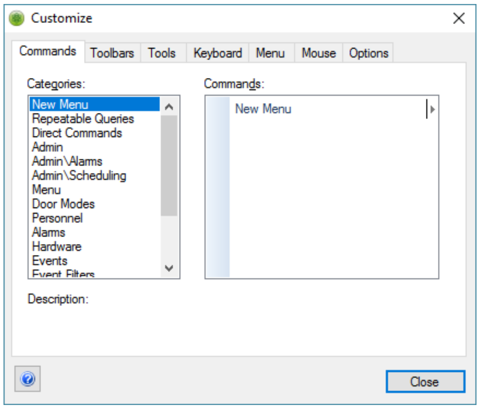
   If needed, repeat steps 4 through 8 until all desired direct commands have been added.
10. **Click** the Save 💾 icon to save the user command.
11. **Click** OK to close the dialog.

    The newly created command will appear as an option under Main Menu / Hardware / Direct Commands.

Adding a Direct Command to a Toolbar

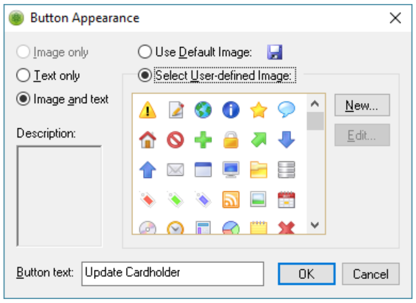
1. **Click** on the drop-down arrow to the right of the Standard Toolbar and **select** Add or Remove Buttons / Customize.

   The Customize dialog opens.



2. **Select** the Direct Commands option from the Categories section.
3. From the Commands section, **drag and drop** the Direct Command to the desired toolbar.

   The command will appear on the selected toolbar.



○ Image only
○ Text only
● Image and text
○ Use Default Image:
● Select User-defined Image:
Description:
Button text: Update Cardholder

4. With the Customize dialog still open, **right-click** on the button in the toolbar and **select** Button Appearance.

   The Button Appearance dialog opens.
5. **Select** the Image and Text radio button.
6. **Select** the image for the button and **click** OK.

   The new command will appear on the toolbar with the selected icon.

   For more information on customizing buttons, see page 2-13.

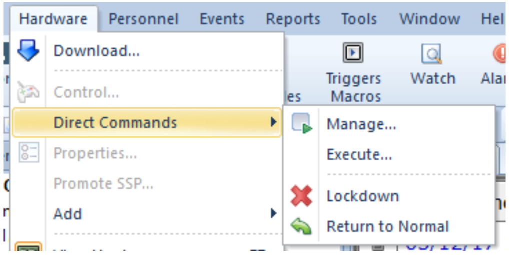
Executing a Direct Command

Users can execute direct commands in many ways:

- From the Direct Commands menu
- From the Execute Direct Commands dialog
- From a graphic map
- From a linked button

Direct Commands Menu

1. **Select** Hardware / Direct Commands from the Main Menu.



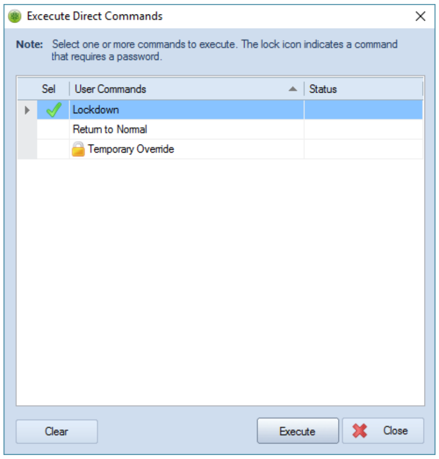
2. **Select** the desired command from the context menu.

Execute Direct Commands Dialog

1. **Select** Hardware / Direct Commands / Execute from the Main Menu.

   The Execute Direct Commands dialog appears.
2. **Select** one or more Commands to execute.

   Note: The Lock 🔒 icon indicates a command that requires a password.
3. **Click** the Execute button to execute the command(s).



Note: Select one or more commands to execute. The lock icon indicates a command that requires a password.

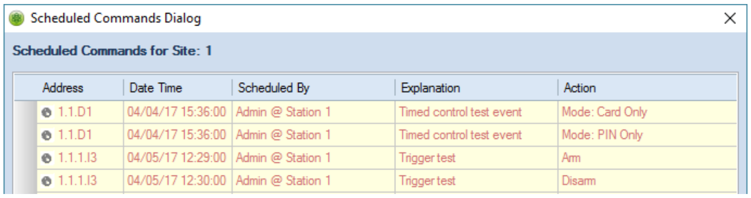
Sel	User Commands	Status
✓	Lockdown	
	Return to Normal	
	🔒 Temporary Override	

Site Options

A Site is a collection of channels and controllers that communicate with a common driver (DNADrvr32). The site will appear "Connected" on the status bar when it is communicating with the driver. Each site can communicate with up to 255 controllers.

Use caution when editing or selecting any of the following site options:

- Properties - Displays the Site Properties dialog. See page 8-49 for more information.
- Link Station to Site - Opens the Site Properties dialog to link the Workstation to a Site (establish a connection to the DNAdrvr service). If desired, click the New Site button to open the Add Site dialog.
- Unlink Site from Station - Option to unlink the Workstation from the Site. If selected, the driver stops communicating with field hardware.
- New / Edit / Delete Site - Opens a dialog to add or edit the site, as well as an option to delete the site. For more information, see page 8-49.
- Add Channel - Opens the Add Channel dialog to add a channel to the site. See page 8-50 for more information on channel properties.
- Add SSP - Opens the Controller Properties dialog to add a controller to the site. See page 8-51 for more information on controller properties.
- Scheduled Commands - Displays the One-Time Scheduled Commands for Hardware Objects across the entire Site. See page 8-7 for more information on scheduled commands.



Scheduled Commands Dialog

Scheduled Commands for Site: 1

Address	Date Time	Scheduled By	Explanation	Action
1.1.D1	04/04/17 15:36:00	Admin @ Station 1	Timed control test event	Mode: Card Only
1.1.D1	04/04/17 15:36:00	Admin @ Station 1	Timed control test event	Mode: PIN Only
1.1.1.I3	04/05/17 12:29:00	Admin @ Station 1	Trigger test	Arm
1.1.1.I3	04/05/17 12:30:00	Admin @ Station 1	Trigger test	Disarm

- Journal - Displays journal options for the site. See page 8-19 for more information.
  - □ New Entry - Opens the DNA Journal dialog to record a new text entry.
  - □ View - Opens the DNA Journal Selection dialog to filter which journal entries will appear in the DNA Journal Viewer. Only entries with the appropriate operator permissions will be accessible.
- Download - Opens the Download Manager dialog. It is imperative that records are downloaded to the SSP for them to be added to the panel. For more information on downloading, see page 2-15.
- Connection - Allows you to enable or disable site connection to the driver.
  - □ Disable Driver - If selected, the Site will become Disabled, and the option will change to Enable Driver. If Enable Driver is selected, the Site will become Enabled again.
- Refresh Status - Refreshes the site connection status.

Channel Options

The Channel is the path of communication from the server to the controller(s), e.g., Ethernet modem. Use caution when editing or selecting any of the following channel options:

- Properties - Displays the Add Channel dialog to edit the selected channel's properties. See page 8-50 for more information.
- Add SSP - Opens the Controller Properties dialog to add a new controller to the selected channel. See page 8-51 for more information.
- Delete - Removes the selected channel. Any controllers that are attached to the channel must be moved to another channel or removed before deleting the channel.
- Download - It is imperative that records are downloaded to the SSP in order for them to be added to the panel. For more information on downloading, see page 2-15.
- Journal - Allows you to record a text entry and view all journal entries for which you have the required operator permissions. For more information on creating or viewing journal entries, see page 8-19.
- Status - Opens the Channel Status dialog, which displays the channel's State as well as the DLL Version.

NOTES:

SSP (Controller) Options

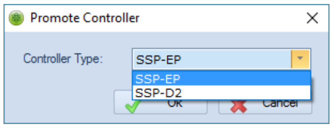
DNA Fusion offers a number of controller options, including the ability to check or refresh the status, create and view entries in the journal, and access the Download Manager.

Properties

Opens the Controller Properties dialog for the selected controller. See page 8-51 for more information.

Promote SSP

This option is only available if the selected SSP is a legacy controller (SSP, SSP/C, or SSP/E). The Promote SSP feature allows the board to be replaced with a current product and programmed into DNA Fusion. See Chapter 4 in the Technical Installation Manual for more information.



Controller Type: SSP-EP

1. **Right-click** on the Legacy Controller and **select** Promote SSP.

   The Promote Controller dialog appears.
2. **Select** the Controller Type from the drop-down list.
3. **Click** OK to update the Legacy Controller.

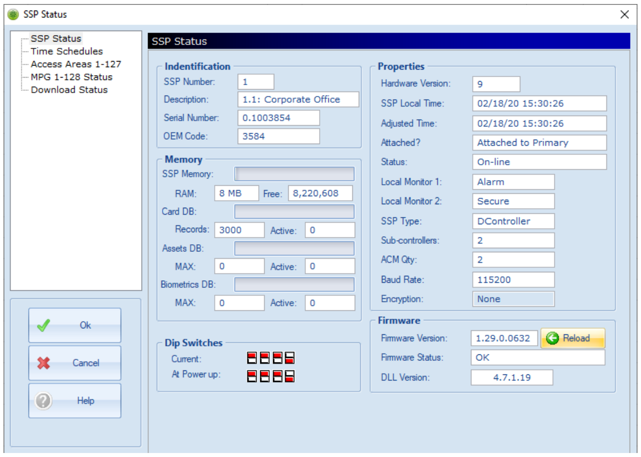
Edit Channel

Opens the Edit Channel dialog to edit the channel properties. See page 8-50 for more information.

Status

1. **Right-click** on the Controller and **select** Status from the context menu.

   The SSP Status dialog opens.



Indentification
SSP Number: 1
Description: 1.1: Corporate Office
Serial Number: 0.1003854
OEM Code: 3584

Memory
SSP Memory:
RAM: 8 MB Free: 8,220,608
Card DB:
Records: 3000 Active: 0
Assets DB:
MAX: 0 Active: 0
Biometrics DB:
MAX: 0 Active: 0

Dip Switches
Current:
At Power up:

Properties
Hardware Version: 9
SSP Local Time: 02/18/20 15:30:26
Adjusted Time: 02/18/20 15:30:26
Attached? Attached to Primary
Status: On-line
Local Monitor 1: Alarm
Local Monitor 2: Secure
SSP Type: DController
Sub-controllers: 2
ACM Qty: 2
Baud Rate: 115200
Encryption: None

Firmware
Firmware Version: 1.29.0.0632
Firmware Status: OK
DLL Version: 4.7.1.19

2. **Select** one of the status screens from the dialog menu.
   - SSP Status - Includes the following information about the selected controller:
     - □ Identification - Includes the controller name, number designation, serial number, and OEM code.
     - □ Memory - Shows the total and available SSP memory, including a breakdown of individual categories.
     - □ DIP Switches - Graphical display of the current DIP switch settings as well as those at power up.
     - □ Properties - Provides valuable information such as the controller's adjusted time, the communication status, and hardware configuration.
     - □ Firmware - Displays the controller's firmware version and an option to reload the firmware. See page 20-13 for more information.
   - Time Schedules - Displays the status of time schedules; results may be interrupted based on the Key.
   - Access Areas 1-127 - Displays the status of Access Areas; results may be interrupted based on the Key.
   - MPG 1-128 Status - Displays the status of MPGs; results may be interrupted based upon the Key.
   - Download Status - Provides information about each category's last download including any Duplicates or Errors (D/E). Also provides access to the Download Checked, Download All, and Reset commands. See page 8-34 for more information on the Reset option.

Controller Commands

The Controller Commands menu offers many high-level options such as connecting and disconnecting the controller, resetting the controller, and reloading firmware. Use caution when editing or selecting any of the command options below.

- Connect - Connects the controller to the host (channel). If the Controller is Offline and the Site is Connected, select the Connect option to reattempt communication.
- Disconnect - Disconnects the controller from the host (channel). When selected, the controller text will appear gray and a black diamond will be displayed indicating that the controller is offline.
- Reset - Deletes the information in the controller's memory; a full download reloads the controller with updated information. During the reset process, the controller will lose communication with DNA Fusion; depending on the amount of information being downloaded, this process could take a while.
- Disable (Remove from Service) - If selected, disables the controller from service and changes the menu option to Enable (Return to Service). When a controller is disabled, the controller icon will appear gray in the Hardware Browser. Toggle the option to enable the controller.
- Set Time - Sets the controller time to match the time on the server.
- Refresh Time Schedules - Logs the current state of the time schedules into the Events Grid. The command will affect all Time Schedules for the selected controller.
- Reload Firmware - Downloads the latest firmware to the selected controller.
- Scheduled Commands - Displays the One-Time Scheduled Commands for the selected controller. Note: Does not display scheduled Repeating Commands.
- Trigger Codes - Opens the Trigger Codes dialog to add, remove, and name the Trigger Codes that will appear in all Trigger Code drop-down lists. See page 10-11 for more information.
- Change Channel - Opens the SSP Channel... dialog to move the selected controller to another channel.

Add

The Add menu provides options to add various components to the controller.

- Add Access Area - Opens the Access Areas Dialog. See Chapter 11 for more information.
- Add Door - Opens the New Door dialog. See page 8-59 for more information on door properties.
- Add Elevator - Opens the New Elevator dialog. See page 8-67 for more information on elevator properties.
- Add MPG - Opens the Secured Areas (Area Points) dialog. See Chapter 12 for more information.
- Add Subcontroller - Opens the Subcontroller Properties dialog. See page 8-57 for more information.
- Keypad Command - Opens the Remote Keypad Command (RKC) dialog.

Journal

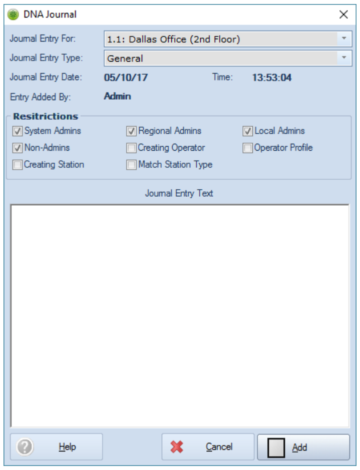
The Journal feature allows you to record a text entry and view entries based on operator restrictions.

Creating a New Entry

1. **Right-click** on the Controller object and **select** Journal / New Entry.

   The DNA Journal dialog opens in entry mode.

2. **Configure** the DNA Journal log:
   - Journal Entry For - **Select** an entry component from the drop-down. Entries may be sorted based on this field.
   - Journal Entry Type - **Select** an entry category from the drop-down. Entries may be sorted based on this field.
   - Restrictions - **Select** the checkbox(es) to indicate who has the ability to view the journal entry.
3. **Place** cursor in the Journal Entry Text panel and **type** the desired message.
4. **Click** the Add button to save the entry.



DNA Journal

Journal Entry For: 1.1: Dallas Office (2nd Floor)

Journal Entry Type: General

Journal Entry Date: 05/10/17 Time: 13:53:04

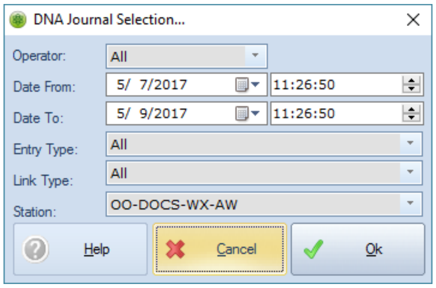
Entry Added By: Admin

Resitrictions

☑ System Admins ☑ Regional Admins ☑ Local Admins
☑ Non-Admins ☐ Creating Operator ☐ Operator Profile
☐ Creating Station ☐ Match Station Type

Journal Entry Text

Viewing an Entry



DNA Journal Selection...

Operator: All

Date From: 5/ 7/2017 11:26:50

Date To: 5/ 9/2017 11:26:50

Entry Type: All

Link Type: All

Station: OO-DOCS-WX-AW

1. **Right-click** on the Controller object and **select** Journal / View.

   The DNA Journal Selection dialog opens to view and filter entries.

2. **Configure** the DNA Journal Selection dialog.

3. **Click** the OK button to view the results.

   The DNA Journal Viewer will appear. The operator will only be able to view existing entries for which he/she has permission to access.

   The read-only fields indicate a journal entry's properties, including its chronological sequence, author, station of origin, date and time, entry type, and entry link.

   Navigate through the entries using the green arrow buttons at the bottom of the panel.

4. When finished, **select** the Close button to close the dialog.

Delete

Removes the selected controller from the system, including all attached hardware.

> *Caution: Once a controller and the attached hardware have been deleted, there is no way to undo the action; the controller will have to be re-added to the system.*

Card Formats

Opens the Card Formats Dialog to add, edit, copy, and remove card formats. See page 8-83 for more information.

Template

Opens the Templates Manager dialog to add, edit, and remove template settings for various hardware objects, including input points, output points, readers, and doors.

Download

Opens the Download Manager dialog. It is imperative that changes be downloaded to the SSP in order for them to be added to the panel. It is recommended that a complete download be performed when large amounts of information or changes have been entered.

1. **Right-click** on the Controller and **select** Download.

2. **Select** the appropriate Download checkbox(es).

3. **Select** the appropriate Sites/Controller checkbox(es).

4. If desired, **select** the individual Site(s)/Controller(s) and **click** OK.

   A status bar will appear to indicate the download's progress. **Click** the Exit button at any time to close the window without affecting the download.

Reports

Displays a list of hardware settings reports for the user to generate from the SSP.

1. **Right-click** on the Controller and **select** Reports / Hardware Settings Reports.

2. **Select** the desired report from the resulting list.

   The Report Parameter Configuration dialog opens. See Chapter 17 for more information on report configuration.

3. Use the tabs to **configure** the parameters for the selected report.

   Each tab will display a dialog box with a list of items.

4. **Click** OK.

   The selected report will open in the data window.

Homepage

Opens the designated Homepage for the selected controller. See page 8-51 for more information on setting homepages for controllers.

Refresh Status

Refreshes the selected controller’s status.

Subcontroller Options

DNA Fusion offers a number of subcontroller options, including the ability to check the status, create and view entries in the journal, and create templates. Use caution when editing or selecting any of the subcontroller options below.

Properties

Opens the Properties dialog for the selected subcontroller. See page 8-57 for detailed information about Subcontroller Properties.

Delete

Removes the selected subcontroller. Any subcontroller objects that are associated with a door or any other hardware object must be reconfigured before deleting the subcontroller.

> ⓘ *If a subcontroller has objects that are associated with a door (or other object), a dialog will appear with the address of the object(s).*

Download

Selecting Download at the subcontroller level is considered an individual download, and only information about the specific subcontroller will be sent to the controller. The Download Manager dialog is not displayed for individual downloads.

Download PIM/Readers Firmware

Downloads the latest firmware for PIM400 subcontroller and associated readers.

Add Input Points

Allows the operator to add a single input point to an Inovonics node. This option will be greyed out for other non-Inovonics subcontrollers.

Manage Input Points

Opens the Inovonics Input Manager dialog to add multiple input points to an Inovonics node. This option is greyed out for non-Inovonics subcontrollers.

Reload Firmware

Opens a confirmation dialog to allow the selected subcontroller's firmware to be updated. See page 20-13 for more information.

Status

Opens the Subcontroller Status dialog to display detailed status for the selected subcontroller, including Identification, Status, and Firmware information. This does not apply to on-board subcontrollers.

Journal

The Journal feature allows you to record a text entry and view entries based on operator restrictions. See page 8-19 for more information on adding and viewing entries.

Defaults

Applies Default template to the selected subcontroller.

Templates

Opens the Templates Manager dialog to add, edit, and remove template settings for various hardware objects, including input points, output points, readers, and doors.

Hompage

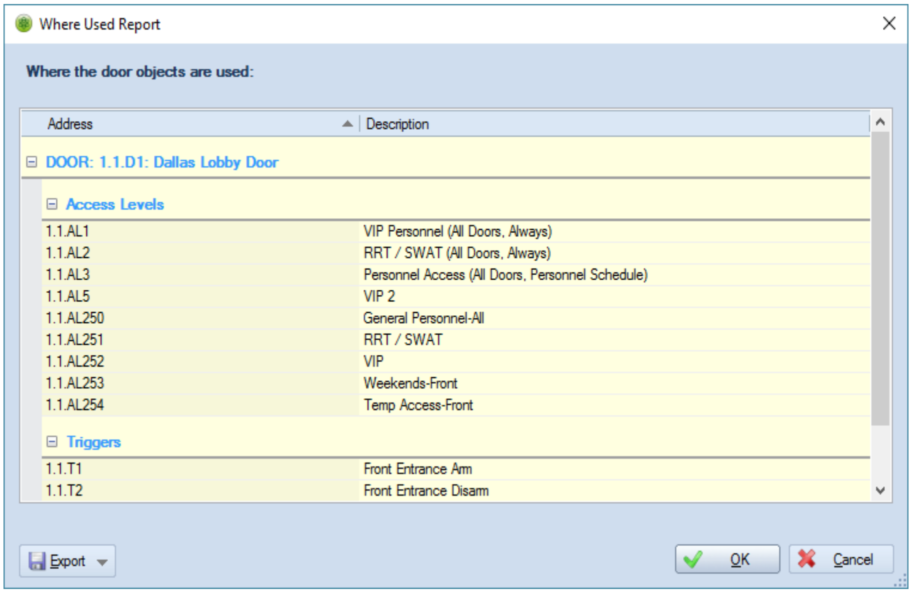
Opens the designated Homepage for the selected subcontroller.

Refresh Status

Refreshes the selected subcontroller's status.

Where Used

The Where Used feature provides a grid displaying the object's associated relationships, i.e. triggers, macros, etc.



Where the door objects are used:

Address	Description
DOOR: 1.1.D1: Dallas Lobby Door	
Access Levels	
1.1.AL1	VIP Personnel (All Doors, Always)
1.1.AL2	RRT / SWAT (All Doors, Always)
1.1.AL3	Personnel Access (All Doors, Personnel Schedule)
1.1.AL5	VIP 2
1.1.AL250	General Personnel-All
1.1.AL251	RRT / SWAT
1.1.AL252	VIP
1.1.AL253	Weekends-Front
1.1.AL254	Temp Access-Front
Triggers	
1.1.T1	Front Entrance Arm
1.1.T2	Front Entrance Disarm

ACM Options

There are a number of options available by right-clicking on the ACM.

Properties

Opens the Properties dialog for the selected ACM. See page 8-59 for information about Door Properties and see page 8-67 for more information on Elevator Properties.

Control

See page 8-3 for information on controlling doors and see page 8-11 for information on controlling elevators.

Add Door/Elevator

Opens the New Door/New Elevator dialog. See page 8-59 for more information on Door Properties and page 8-67 for more information on Elevator Properties.

Auto Unlock

Opens the Auto Unlock dialog. See page 8-66 for more information.

Delete

Removes the selected ACM. Use caution when selecting the Delete option since the door or elevator will be permanently removed from the system.

Download

Opens the Download Manager dialog. It is imperative that changes be downloaded to the SSP in order for them to be added to the panel. It is recommended that a complete download be performed when large amounts of information or changes have been entered.

1. **Right-click** on the ACM and **select** Download.
2. **Select** the appropriate Download checkbox(es).
3. **Select** the appropriate Sites/Controller checkbox(es).
4. If desired, **select** the individual Site(s)/Controller(s) and **click** OK.

   A status bar will appear to indicate the download's progress. **Click** the Exit button at any time to close the window without affecting the download.

Reports

ACM-specific reports are easy to generate from the selected object.

1. **Right-click** on the ACM and **select** Reports.

   A list of options appears.
2. **Configure** the Report Parameter Configuration dialog and **click** the OK button.

   See Chapter 17 for more information on reports.

Info

See page 8-17 for more information on the Info feature.

Journal

The Journal feature allows you to record a text entry and view entries based on operator restrictions. See page 8-19 for more information on adding and viewing entries.

Watch Item

Adds the selected ACM to the Watch Window. See Chapter 15 for more information.

Add to Macro

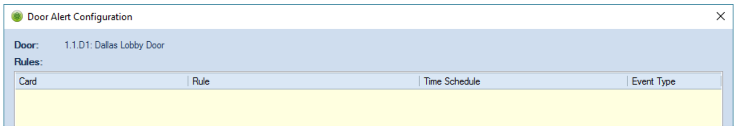
Opens the Macros Editor dialog to configure Door, Reader Mode, and Reader Override macro commands. See page 10-1 and 10-2 for more information on creating macros.

Configure Door Alerts

Opens the Door Alert Configuration dialog to configure, edit, and remove door alert rules for the selected door. Users can define rules by specific parameters, such as card numbers, trigger codes, time schedules, trigger events, and alarm priorities. If a door alert is triggered, an Alarm will appear in the Alarm Grid.

1. **Right-click** on the ACM in the Hardware Browser and **select** Configure Door Alerts.

   The Door Alert Configuration dialog opens.



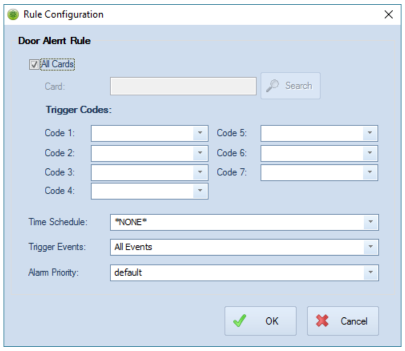
Door: 1.1.D1: Dallas Lobby Door

Rules:

Card	Rule	Time Schedule	Event Type

2. **Select** the New Rule button to add a new door alert rule.

   The Rule Configuration dialog opens.



☑ All Cards

Card:

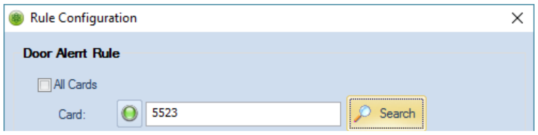
Code 1:
Code 2:
Code 3:
Code 4:
Code 5:
Code 6:
Code 7:

Time Schedule: *NONE*

Trigger Events: All Events

Alarm Priority: default

3. If desired, **uncheck** the All Cards checkbox to configure the rule for an individual Card.



□ All Cards

Card: ● 5523

   The Card field will become active and the Trigger Codes fields will turn gray.

   OR

   Select the All Cards checkbox to apply the rule to all cards in the system.

4. If needed, **enter** the Card Number and **select** the Search button.

   A green icon ● will appear for valid card numbers, or a red icon ● will appear for invalid card numbers.

5. If needed, **select** the desired Trigger Code(s) from the drop-down field(s).

   See page 10-11 for more information on trigger codes.

6. If desired, **select** a Time Schedule from the drop-down.

   If selected, the door alerts will only generate when the specified internal time schedule is active. See page 10-19 for more information.

7. **Select** a Trigger Events option from the drop-down.

8. **Select** an Alarm Priority from the drop-down.

   If Default is selected, the door alert rule will use the event-specific Priority set in DNA / Administrative / Alarms and Events / Logging. See page 14-25 for more information.

9. **Click** OK to save the configuration.

   The door alert rule is added to the Door Alert Configuration dialog.

10. **Click** OK to close the dialog.

Defaults

Applies the default template to the selected ACM.

Templates

Opens the Templates Manager dialog to add, edit, and remove template settings for the selected door. See page 8-85 for more information on templates.

Homepage

Opens the designated Homepage for the selected ACM. See page 8-59 for information on door homepages and 8-67 for information on elevator homepages.

Refresh Status

Refreshes the selected ACM's status.

Where Used

The Where Used feature provides a grid displaying the object's associated relationships, i.e. triggers, macros, access levels, etc.

Input and Output Options

The Input and Output Points allow the operator to access the Properties dialog, open the Download Manager, and add the object to the Watch Window.

Properties

Opens the Properties dialog for the selected point. See page 8-75 for more information about Input Properties and see page 8-79 for more information on Output Properties.

Control

See page 8-23 for information on controlling input and output points.

Remove From Service

Opens the Remove From Service dialog to take an input out of service based on the selected Parameter: Indefinite, Minutes, or Time of Day. See page 8-5 for more information on these options. Inputs that are removed from service will appear grey in the Hardware Browser next to a black diamond.

Return to Service

Returns an input point to service. The input object will change from grey to red in the Hardware Browser.

Download

Selecting Download at the input or output point level is considered an individual download, and only information about that specific point will be sent to the controller. The Download Manager dialog is not displayed for individual downloads.

Reports

1. **Right-click** on the Point, **select** Reports, and **select** the desired report option.
2. **Configure** the Report Parameter Configuration dialog and **click** the OK button.

   See Chapter 17 for more information on reports.

Journal

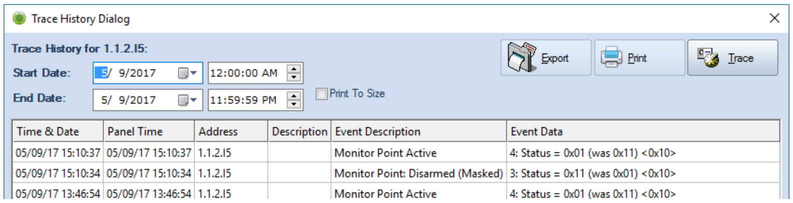
The Journal feature allows you to record a text entry and view entries based on operator restrictions. See page 8-19 for more information on adding and viewing entries.

Trace History

A trace history report displays the last transactions for the selected input or output point.

1. **Right-click** on the Point and **select** Trace History.

   The Trace History Dialog opens.



Trace History Dialog

Trace History for 1.1.2.I5:

Start Date: 5/ 9/2017 12:00:00 AM

End Date: 5/ 9/2017 11:59:59 PM

□ Print To Size

Time & Date	Panel Time	Address	Description	Event Description	Event Data
05/09/17 15:10:37	05/09/17 15:10:37	1.1.2.I5		Monitor Point Active	4: Status = 0x01 (was 0x11) <0x10>
05/09/17 15:10:34	05/09/17 15:10:34	1.1.2.I5		Monitor Point: Disarmed (Masked)	3: Status = 0x11 (was 0x01) <0x10>
05/09/17 13:46:54	05/09/17 13:46:54	1.1.2.I5		Monitor Point Active	4: Status = 0x01 (was 0x11) <0x10>

2. If a wider time or date range is needed, **enter** the Start and End Date/Time and **click** the Trace button.

   The results can be narrow down by **selecting** Access Only and **clicking** the Trace button.

   The results can printed or exported by selecting the appropriate button.

Watch Item

Adds the selected item to the Watch Window. See Chapter 15 for more information.

Defaults

Applies the default templates to the inputs and outputs associated with the selected point(s).

Templates

Opens the Templates Manager dialog to add, edit, and remove template settings for the selected hardware point. See page 8-85 for more information on templates.

Where Used

The Where Used feature provides a grid displaying the object's associated relationships, i.e. triggers, macros, access levels, etc.

Reader Options

DNA Fusion offers a number of reader options, including the ability to access the reader's properties, add a door to the selected reader, create and view journal entries, and create templates.

Properties

Opens the Properties dialog for the selected reader. See page 8-72 for more information about Reader Properties.

Download

Selecting Download at the reader level is considered an individual download, and only information about the selected reader will be sent to the controller. The Download Manager dialog is not displayed for individual downloads.

Add Door

Users can add a door with the default door template or choose from a list of predefined templates.

- Use Default - Opens the New Door dialog to configure a door with the default template settings. See page 8-59 for more information on door properties.
- Use Template - Opens the Door Templates dialog to add a door using a custom template. See page 8-85 for more information on templates.

Journal

The Journal feature allows you to record a text entry and view entries based on operator restrictions. See page 8-19 for more information on adding and viewing entries.

Defaults

Applies the default template to the selected reader.

Templates

Opens the Templates Manager dialog to add, edit, and remove template settings for the selected reader. See page 8-85 for more information on templates.

Homepage

Opens the designated Homepage for the selected reader. See page 8-72 for more information.

Viewing & Controlling DVR/NVR and IP Cameras

DNA Fusion incorporates a number of features to view and control cameras attached to a server from most major DVR/NVR manufacturers. For information on adding NVR/DVR system to DNA Fusion, see page 3-55 in the Technical Installation Manual. Video is stored and configured in the video management system (VMS).

The DVR Browser

The DVR Browser contains the DVR/NVR servers as well as the cameras associated to each server. Camera Groups can be created to logically or geographically organize cameras; users can then drag and drop the groups onto the Video View Manager for quick viewing.

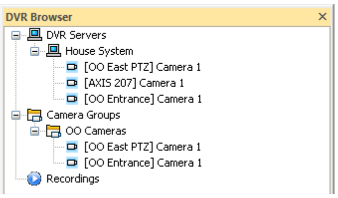
To open the DVR Browser:

1. **Click** the DVR Manager button on the Standard Toolbar.

   Or

   Select View / Explorers / DNA DVR from the Main Menu.

   The DVR Browser will appear.



DVR Browser
- DVR Servers
  - House System
    - [OO East PTZ] Camera 1
    - [AXIS 207] Camera 1
    - [OO Entrance] Camera 1
- Camera Groups
  - OO Cameras
    - [OO East PTZ] Camera 1
    - [OO Entrance] Camera 1
- Recordings

Cameras are listed under the DVR/NVR server they are associated with.

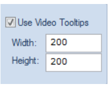
> *IP Cameras are listed under the* DVR Servers *header.* IP Cameras *can be added to* Camera Groups*; however, they will not support archived video playback and* Video Tooltips *will not be available.*

Using Video Tooltips

Video tooltips provide a camera view without opening any additional windows. Hover the mouse over any camera in the DVR Browser, and a live video window will open in the form of a video tooltip.

1. **Click** the DNA Properties button on the Standard Toolbar.
2. From the Station Settings page, **locate** the Tooltip Settings section.
3. **Select** the Use Video Tooltips checkbox.
4. **Enter** the desired Width and Height for the video tooltip window(s).
5. **Click** the OK button to save the settings.

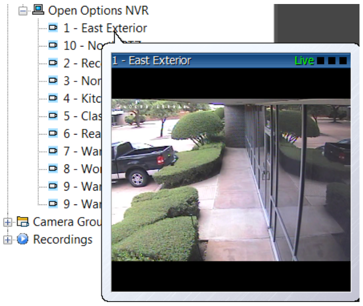
   When the mouse is placed on the camera's name in the DVR Browser, the camera's video stream will display as a pop-up tooltip.



☑ Use Video Tooltips

Width: 200

Height: 200



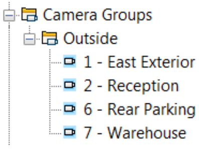
Creating Camera Groups

Camera groups allow the operator to group certain cameras together and drop the group into the Video View Manager to fill the display with the selected cameras.

1. With the DVR Browser open, **right-click** on the Camera Groups header and **select** Add Camera Group.

   The DVR Camera Group dialog opens.
2. **Enter** a Group Name and **click** OK to save the group.
3. **Expand** the Camera Groups section by **clicking** the plus sign (+).
4. **Drag and drop** the selected Camera(s) to the desired Camera Group.

   The Camera(s) will appear in the specified Camera Group. To remove a camera from a group, **right-click** on the Camera in the group and **select** Remove.



- Camera Groups
  - Outside
    - 1 - East Exterior
    - 2 - Reception
    - 6 - Rear Parking
    - 7 - Warehouse

To view a camera:

1. **Open** the DVR Browser and the Video View Manager.

   For more information on the Video Manager, see page 8-45.
2. **Drag and drop** the Camera or Camera Group to the Video View Manager.

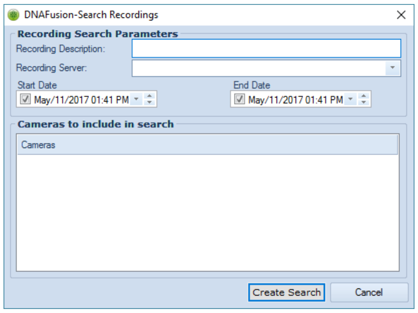
Adding Recordings

Users can create recordings with a defined start and stop time and then assign multiple cameras or camera groups to the recording item(s). This allows the operator to view the desired timeframe on multiple cameras simultaneously without having to set the time parameters for each camera. All recordings are pulled from the VMS.

To add a recording:

1. With the DVR Browser open, **right-click** on the Recordings option and **select** Add Recording.

   The Search Recordings dialog opens.



DNAFusion-Search Recordings

Recording Search Parameters

Recording Description:

Recording Server:

Start Date ☑ May/11/2017 01:41 PM

End Date ☑ May/11/2017 01:41 PM

Cameras to include in search

Cameras

2. **Enter** a Recording Description for the recordings search.
3. **Select** a Recording Server from the drop-down.
4. In the Start Date field, specify a start date by **clicking** the Down Arrow to open the calendar or by using the Up and Down Buttons.
5. In the End Date field, specify an end date by **clicking** the Down Arrow to open the calendar or by using the Up and Down Buttons.
6. **Right-click** in the Cameras section to add desired cameras to the search.
   - Add Camera - Opens the Camera dialog to select individual cameras. Multiple cameras can be selected from this dialog by using the Control or Shift keys.
   - Add Camera Group - Opens the Camera Group dialog to select individual camera groups. Multiple camera groups can be selected from this dialog by using the Control or Shift keys.
7. **Select** the Camera(s) or Camera Group(s) and **click** the OK button.
8. **Click** Create Search to save the search.

   The saved recording search will appear in the DVR Browser under the Recordings header.

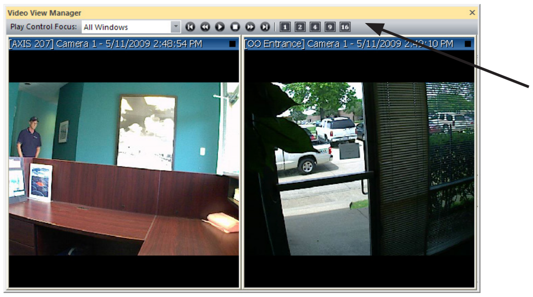
To play a recording:

1. **Open** the DVR Browser and the Video View Manager.

   For more information on the Video Manager, see page 8-45.

2. **Drag and drop** the Recording to the Video View Manager.

   The associated cameras will play the specified video recording. Use the video manager controls to play back the video.



Video View Manager
Play Control Focus: All Windows
1
2
4
9
16
[AXIS 207] Camera 1 - 5/11/2009 2:48:54 PM
[OO Entrance] Camera 1 - 5/11/2009 2:4[illegible]:10 PM

Video Manager Controls

To delete a saved recording:

1. With the DVR Browser open, **right-click** on the desired Recording.
2. **Select** Delete Recording from the context menu.

   The saved recording will be removed from the Recordings list.

Video Manager

DNA Fusion incorporates a flexible monitor matrix that can be used to view either live or recorded video from multiple cameras. The video display will automatically resize when cameras or camera groups are dropped directly into the matrix. Window and playback controls are built into the matrix for convenient access.

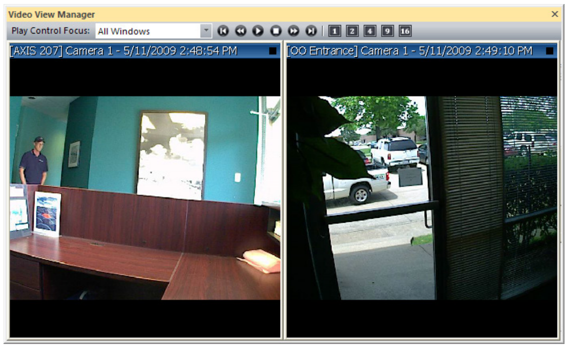
To open the Video Manager:

1. **Select** the Video Manager button on the Standard Toolbar.

   Or

   Select View / Windows / Video View Manager from the Main Menu.

   The Video View Manager window opens.


Video View Manager
Play Control Focus: All Windows
1 2 4 9 16
[AXIS 207] Camera 1 - 5/11/2009 2:48:54 PM
[OO Entrance] Camera 1 - 5/11/2009 2:49:10 PM

> Host Based Macros *can also be configured to automatically populate the* Video View Manager *windows when a particular event happens at a specific door. See page 10-16 for more information.*

Displaying Video

To display live cameras in the Video View Manager, **open** the DVR Browser and **drag** a Camera or Camera Group to the Video View Manager. The display will automatically readjust to the number of panes in the layout. If more than one window is displayed, **double-click** on a window to open it full screen.

> *Video is stored on the integrated Video Management System's server and is retrieved by DNA Fusion. DNA Fusion does not store or save video.*

Video View Manager Toolbar

The Video View Manager Toolbar provides a number of useful controls including playback options as well as the ability to specify the number of panes.

Play Control Focus: All Windows ▾	Play Control Focus - Indicates which window to apply the selected control.
☒	Clear Window Icon - Clears the Video View Manager of all active cameras.
⏮	Previous Segment Icon - Moves to the first image in the previous recorded sequence.
⏪	Step Backwards Icon - Moves to the image just before the one currently displayed.
▶	Play Icon - Plays recording forward in time.
■	Stop Icon - Stops the recorded video.
⏩	Step Forward Icon - Moves to the image just after the one currently displayed.
⏭	Next Segment Icon - Moves to the first image in the next recorded sequence.
1 2 4 9 16	Window Layout Icon - Number of window panes in the layout.

Video Manager Features

The Video View Manager offers a number of built-in features that allow the operator to control the cameras without leaving the DNA Fusion environment.

PTZ Control

If the camera has PTZ (Pan, Tilt, and Zoom) capability, the controls can be accessed from within the Video View Manager.

Many PTZ cameras can be controlled by pointing and clicking inside the images from the camera. If a set of crosshairs appears when hovering the mouse cursor over the images from a PTZ camera, point-and-click control is supported for the camera.

To control a camera:

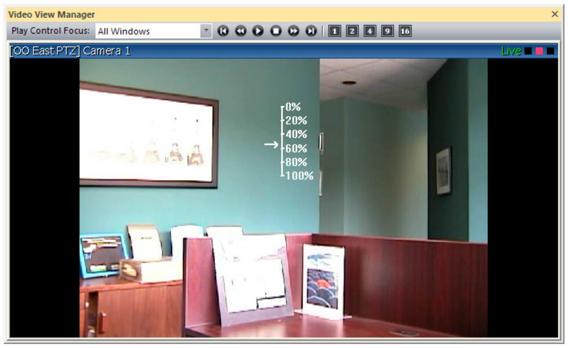
1. **Drag and drop** the desired Camera from the DVR Browser to the Video View Manager.
2. In the window with the camera, **click** the center of the desired location.

   The camera will move to the desired location.

To zoom a camera:

1. **Drag and drop** the desired Camera from the DVR Browser to the Video View Manager.
2. In the window with the camera, **click and hold** the left mouse button.

   A meter will appear on the screen.



3. With the left mouse button held, **select** the Zoom Level and **release** the mouse button.

   The camera will zoom to the selected level. Selecting a Zoom Level of 0% will return the camera to a whole image view.

Clear All Windows

The Clear All Windows option allows the operator to remove the cameras from the Video View Manager.

1. **Click** the ☒ button on the Video View Manager Toolbar.

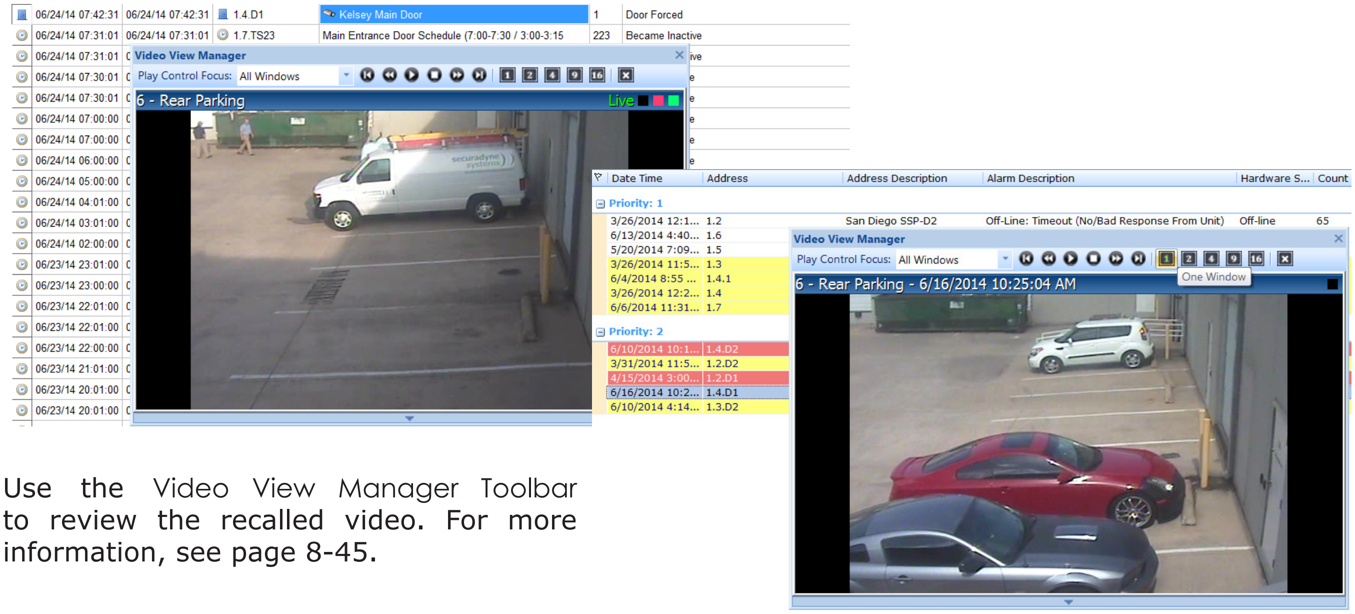
   The windows will clear of all live camera views and/or any recorded video.

Recalling from the Events and Alarms Grids

The camera can be viewed from both the Events and Alarm Grids in conjunction with the activity.

1. **Right-click** in the Events or Alarm Grid.
2. **Select** Hardware / Launch Camera from the context menu.

   The Video View Manager appears.



06/24/14 07:42:31	06/24/14 07:42:31	1.4.D1	Kelsey Main Door	1	Door Forced
06/24/14 07:31:01	06/24/14 07:31:01	1.7.TS23	Main Entrance Door Schedule (7:00-7:30 / 3:00-3:15	223	Became Inactive
06/24/14 07:31:01					
06/24/14 07:30:01					
06/24/14 07:30:01					
06/24/14 07:00:00					
06/24/14 07:00:00					
06/24/14 06:00:00					
06/24/14 05:00:00					
06/24/14 04:01:00					
06/24/14 03:01:00					
06/24/14 02:00:00					
06/23/14 23:01:00					
06/23/14 23:00:00					
06/23/14 22:01:00					
06/23/14 22:01:00					
06/23/14 22:00:00					
06/23/14 21:01:00					
06/23/14 20:01:00					
06/23/14 20:01:00					

Video View Manager
Play Control Focus: All Windows
6 - Rear Parking Live

Date Time	Address	Address Description	Alarm Description	Hardware S...	Count
Priority: 1					
3/26/2014 12:1...	1.2	San Diego SSP-D2	Off-Line: Timeout (No/Bad Response From Unit)	Off-line	65
6/13/2014 4:40...	1.6				
5/20/2014 7:09...	1.5				
3/26/2014 11:5...	1.3				
6/4/2014 8:55 ...	1.4.1				
3/26/2014 12:2...	1.4				
6/6/2014 11:31...	1.7				
Priority: 2					
6/10/2014 10:1...	1.4.D2				
3/31/2014 11:5...	1.2.D2				
4/15/2014 3:00...	1.2.D1				
6/16/2014 10:2...	1.4.D1				
6/10/2014 4:14...	1.3.D2				

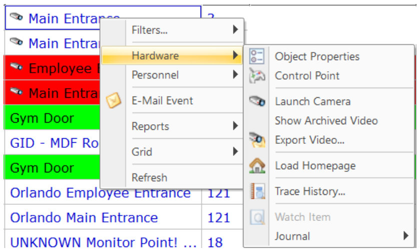
Video View Manager
Play Control Focus: All Windows
One Window
6 - Rear Parking - 6/16/2014 10:25:04 AM

Use the Video View Manager Toolbar to review the recalled video. For more information, see page 8-45.

Exporting Video

For installations with Exacq video integrations, an option to export video will appear in the menu. This option is available from the Event Grid, the Alarm Grid and while viewing video in the DVR Browser.

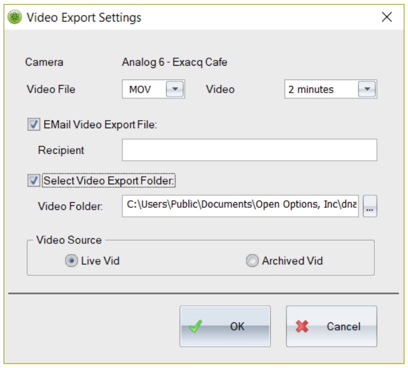
From the Event or Alarm Grid



1. **Right-click** on the desired event or alarm in the appropriate grid.

   Objects that have a camera associated with it will appear with a camera icon next to the Description in the event grid.
2. **Select** the Hardware / Export Video option from the context menu.

   The Video Export Setting dialog opens.



Video Export Settings

Camera Analog 6 - Exacq Cafe

Video File MOV Video 2 minutes

☑ EMail Video Export File:

Recipient

☑ Select Video Export Folder:

Video Folder: C:\Users\Public\Documents\Open Options, Inc\dna

Video Source

● Live Vid ○ Archived Vid

OK Cancel

3. If desired, **change** the Video File Format to AVI and **select** the desired video length.
4. If the file will be emailed to a recipient, **check** the EMail Video Export File option and **enter** the email address.
5. If the video will be stored in a folder, **check** the Select Video Export Folder option and **browse** to the desired export location.

   The video will be exported and emailed or saved to the designated location. Both options can be selected simultaneously.
6. **Click** the OK button.

   The export status will appear on the Status Bar at the bottom of the DNA Fusion window. The file will be either emailed to the specified recipient and/or saved in the desired location.

From the Video Manager

Video can be exported directly from the Video Manager with the added options to specify Live or Archived Video. For live selections, operators will be prompted for the amount of time to record the video for exporting.

1. **Select** the Video Manager button on the Standard Toolbar.

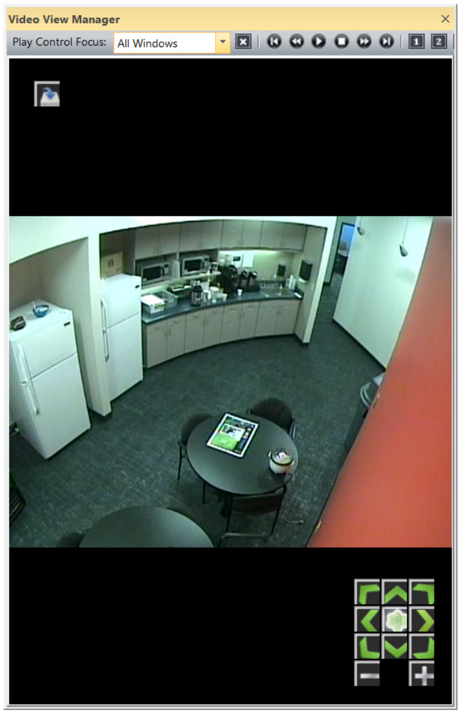
   Or

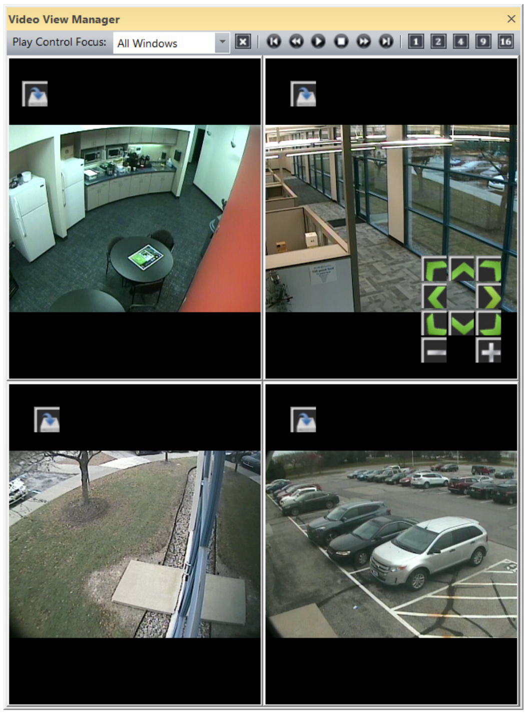
   Select View / Windows / Video View Manager from the Main Menu.

   The Video View Manager window opens.

2. **Open** the DVR Browser and **drag** a Camera or Camera Group to the Video View Manager.

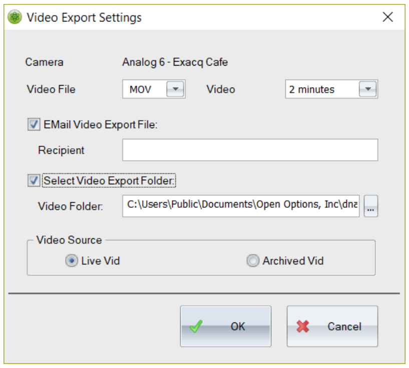
   The display will automatically readjust to the number of panes in the layout. If more than one window needed, select the number of panes from the Video toolbar. To open the image full screen, **double-click** on a window.





3. **Click** the Video Export button in the top right of the window.

   The Video Export Setting dialog opens.



Video Export Settings

Camera Analog 6 - Exacq Cafe

Video File MOV Video 2 minutes

☑ EMail Video Export File:

Recipient

☑ Select Video Export Folder:

Video Folder: C:\Users\Public\Documents\Open Options, Inc\dna

Video Source

● Live Vid ○ Archived Vid

4. If desired, **change** the Video File Format to AVI and **select** the desired video length.

5. If the file will be emailed to a recipient, **check** the EMail Video Export File option and **enter** the email address.

6. If the video will be stored in a folder, **check** the Select Video Export Folder option and **browse** to the desired export location.

   The video will be exported and emailed or saved to the designated location. Both options can be selected simultaneously.

7. **Select** the Video Source: Live Video or Archived Video.

   For live selections, select the Video length of time to record the video prior to exporting.

8. **Click** the OK button.

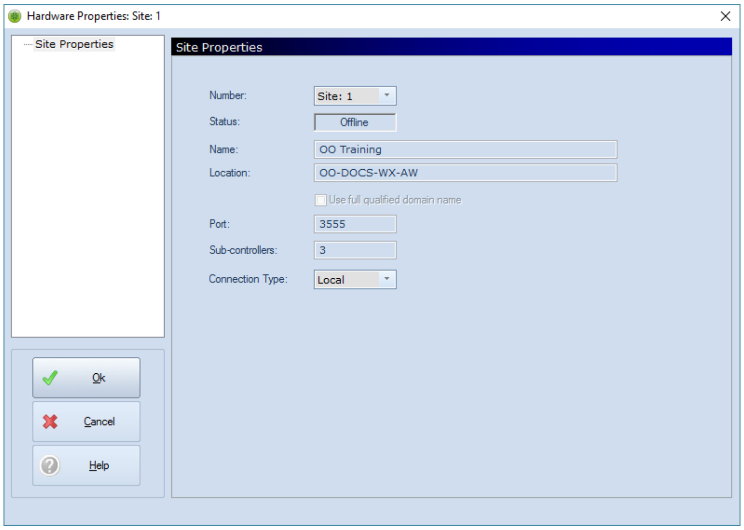
   The export status will appear on the Status Bar at the bottom of the DNA Fusion window. The file will be either emailed to the specified recipient and/or saved in the desired location.

   If the Select Video Export Folder option was checked, the folder with the recorded video will open.

Hardware Properties

Site Properties

A Site is defined as a collection of channels and controllers that communicate with a common driver. It is the location of the communicating hardware for a section or all of a given system. The site represents the status of the DNA driver (DNADrvr32).



Site Properties

Number: Site: 1

Status: Offline

Name: OO Training

Location: OO-DOCS-WX-AW

□ Use full qualified domain name

Port: 3555

Sub-controllers: 3

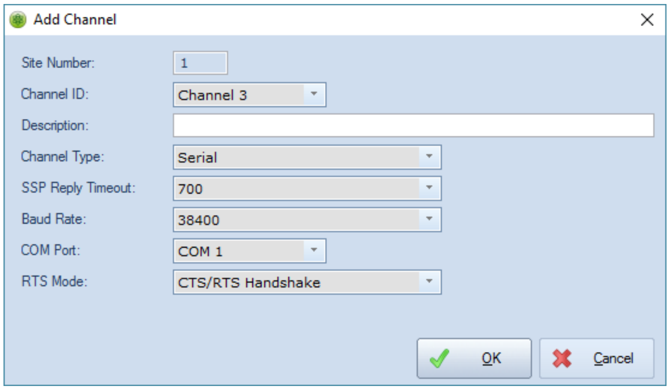
Connection Type: Local

> *Most installations will have only one site with multiple channels. Each site is essentially a separate driver that communicates to the various channels and controllers. Each driver can communicate with up to 255 controllers.*

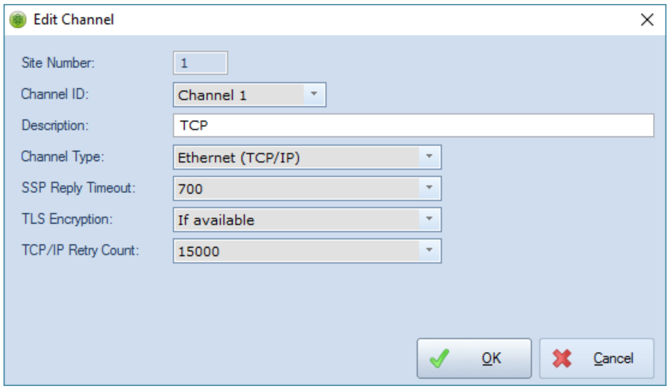
- Number - Displays the identification number for the site.
- Status - Indicates whether the driver is running.
- Name - Displays the user-defined site name (Read-only).
- Location - Displays the name of the computer on which a given site's DNADrvr32 driver resides.
  - Use full qualified domain name - This option can only be configured in the Add Site or Edit Site dialog. If checked, the Location field will display the host computer's fully qualified domain name (FQDM). An FQDM consists of a hostname, domain name, and top-level domain, and is written as *[hostname].[domain].[tld].* Example: Location: oo-docs-wx-aw.oo.local
- Port - Indicates the TCP/IP port number used to establish communication with the site's driver.
- Subcontrollers - Indicates the number of subcontrollers actively connected (online) to the site.
- Connection Type - Indicates the connection type to the site.
  - Local - Server workstation
  - Remote - Client workstation

Add/Edit 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 serial, ethernet, or modem communications.


Add Channel

Site Number: 1
Channel ID: Channel 3
Description:
Channel Type: Serial
SSP Reply Timeout: 700
Baud Rate: 38400
COM Port: COM 1
RTS Mode: CTS/RTS Handshake


Edit Channel

Site Number: 1
Channel ID: Channel 1
Description: TCP
Channel Type: Ethernet (TCP/IP)
SSP Reply Timeout: 700
TLS Encryption: If available
TCP/IP Retry Count: 15000

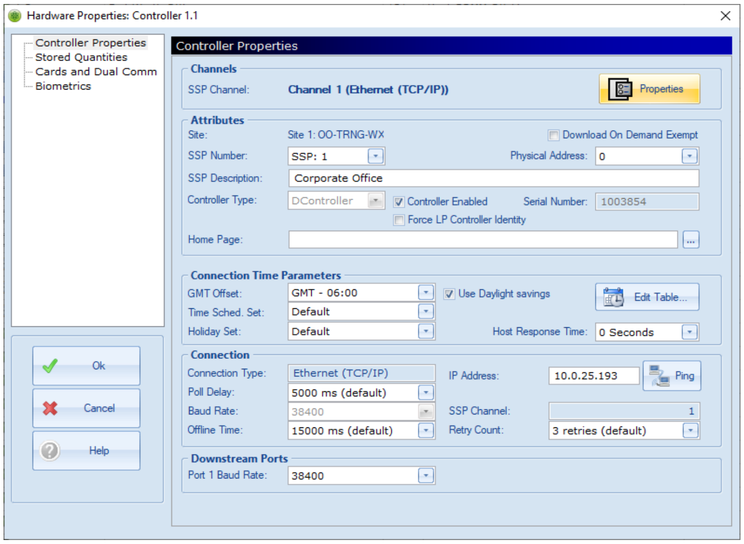
- Site Number - Displays the site identification number for the channel (Auto-populated).
- Channel ID - Drop-down field to select the number designation for a channel.
- Description - User-defined label for the channel.
- Channel Type - Method of communication connection. See page 3-7 of the Technical Installation Manual for more information.
  - □ Ethernet (TCP/IP) - If desired, the following options can be changed: SSP Reply Timeout, TLS Encryption, and TCP/IP Retry Count. Enter the IP Address in the SSP Properties dialog. See page 8-51 for more information.
  - □ Serial - Select the COM Port from the drop-down list.
  - □ Dial In/Out - Select the Modem Name from the drop-down list.
  - □ IP Client - Remote TCP/IP - Provides the ability for panels to connect to the driver rather than the normal method of the driver connecting to the panel. Used in situations where the panels are behind a Hosted/Managed firewall. Only one per site can be used. See page 3-7 in the Technical Installation Manual for more information.

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

- COM Port - Identifies the COM Port for serial connections to the controller. (Serial configuration only).
- TLS Encryption - Determines whether the TLS Encryption is always required or only required if available (TCP/IP configurations only).
- SSP Reply Timeout - SSP timeout in milliseconds. Recommended settings are 200-400 milliseconds for Serial channels, 600-800 milliseconds for TCP/IP channels.
- TCP/IP Retry Count - Number of times the driver will re-attempt communication between the host and an SSP after an unsuccessful attempt. Recommended setting is 10,000-20,000 seconds (TCP/IP configurations only).
- Baud Rate - Rate of transmission to the SSP (Serial configuration only).
- Modem Name - Modem designation in the Control Panel (Dial In/Out configurations only).
- RTS Mode - On/Toggle/Off/CTS-RTS Handshake (Serial configuration only).
  - □ On - Fixes the state of the RTS pin to ON. This setting is used with RS-232 with Hardware Handshake.
  - □ Toggle - Tells the port handler to set the RTS output to ON when data is being sent. This setting is used when the COM port is used in half-duplex mode, such as 2-wire RS-485 connection.
  - □ Off - Fixes the state of the RTS pin to OFF. For instance, setting 0 is used with RS-232 without Hardware Handshake.
  - □ CTS/RTS Handshake - Regulates communication based on the amount of traffic. This setting selects full hardware flow control. Hardware handshake is required if data transfer must be paused momentarily. Connections to the modems, terminal emulators (Lantronix), or connections at baud rates above 38,400 baud will require hardware flow control.
- Listening Port - Identifies the port on the server that remote panels will use for communication. Open Options recommends Port 3001. Only one per site can be used (Remote TCP/IP only).

Controller (SSP) Properties

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.



Controller Properties

Channels

SSP Channel: Channel 1 (Ethernet (TCP/IP))

Attributes

Site: Site 1: OO-TRNG-WX

□ Download On Demand Exempt

SSP Number: SSP: 1

Physical Address: 0

SSP Description: Corporate Office

Controller Type: DController

☑ Controller Enabled

Serial Number: 1003854

□ Force LP Controller Identity

Home Page:

Connection Time Parameters

GMT Offset: GMT - 06:00

☑ Use Daylight savings

Time Sched. Set: Default

Holiday Set: Default

Host Response Time: 0 Seconds

Connection

Connection Type: Ethernet (TCP/IP)

IP Address: 10.0.25.193

Poll Delay: 5000 ms (default)

Baud Rate: 38400

SSP Channel: 1

Offline Time: 15000 ms (default)

Retry Count: 3 retries (default)

Downstream Ports

Port 1 Baud Rate: 38400

Controller Properties

Channels

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

Attributes

- Site - Location of hardware (Auto-populated).
- SSP Number - Number designation for the controller.
- SSP Description - User-defined description of the controller; typically location- or function-related.
- Controller Type - Select the controller type from the drop-down list.

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

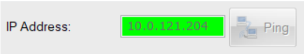
- Controller Enabled - Toggle checkbox to enable/disable the controller. Disabled controllers will appear gray in the Hardware Browser and do not communicate with the DNA driver.
- Serial Number - Display's the controller's identification number.
- Force LP Controller Identity - Only used when a Series 3 (LP) controller is in Legacy Mode (Dipswitch 4 is Set to ON). Toggle the checkbox to ensure that the correct firmware is downloaded.
- Home Page - A file associated with the controller that will open when the object goes into alarm.
- Download on Demand Exempt - If the driver has been configured to download personnel when they badge at a reader (Download Personnel on Demand), selecting this checkbox will override the setting and personnel will be downloaded normally.
- Physical Address - Physical address defined by the controller's DIP switch settings. This option should only be set on controllers with a serial connection.

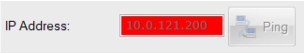
Connection Time Parameters

- GMT Offset - Number of hours offset from Greenwich Mean Time. This setting determines the controller's time. (Default = O GMT)
  - □ -5=Eastern Time
  - □ -6=Central Time
  - □ -7=Mountain Time
  - □ -7=Arizona
  - □ -8=Pacific Time
  - □ -9=Alaska
  - □ -10=Hawaii
- Time Schedule Set - Selected Time Schedule Set for the SSP. See page 5-7 for more information.
- Holiday Set - Selected Holiday Set for the SSP. See page 5-11 for more information.
- Use Daylight Savings - Check to automatically adjust for daylight saving time. If this option is not selected, a message will appear when closing the Controller Properties dialog.
- Edit Table - Opens the Daylight Savings Editor.
  - □ Add - Opens the Daylight Savings Date Editor to define a Start and End Date/Time.
  - □ Remove - Removes the selected Daylight Savings entry.
  - □ Edit - Opens the Daylight Savings Date Editor to edit the selected date pair.
  - □ Defaults - Restores the default Daylight Savings information.
- Host Response Time - If Host Verification is enabled in the Door Properties / Advanced dialog (see page 8-63), the SSP will report to the Host for access confirmation. The Host Response Time is a timeout value for that decision. If the delay exceeds the value, the SSP will complete the access granted cycle.

Connection

- Connection Type - Connection type defined in the channel properties. (Auto-populated)
  - □ TCP/IP Channels - For IP channels, enter the controller's IP Address or MAC Address.
    - ✦ A Ping button will appear. Clicking this option will attempt to ping the configured IP address. If a response is received, the box will turn green.
    - ✦ If any of the packets fail to be received, the box will appear yellow.
    - ✦ If no response from the address, the box will turn red.


IP Address: 10.0.121.204


IP Address: 10.0.121.200

  - □ Serial Channel - No further information is needed for serial channels.
  - □ Dial In / Out Channel - If the channel was configured as a Dial In/Out Channel, enter the Phone Number. Remember to include any leading digits. A comma creates a pause.
- Poll Delay - Time between each poll from the tree host to the SSP (Auto-populated).
- Baud Rate - Speed at which the SSP communicates with the subcontrollers. (DIP switches 6 and 7)

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

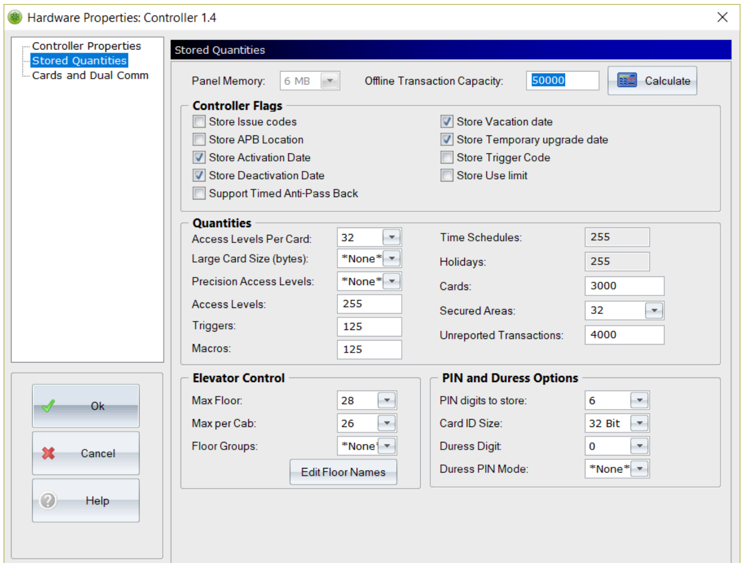
- SSP Channel - Displays the channel number associated with the controller. (Auto-populated)
- Retry Count - Number of times a poll can fail before a panel is determined to be offline. (Default = 3)
- Offline Time - The time between messages from the host prior to SSP offline condition. For dial-up connections,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

Downstream Ports

The following fields are determined by the Controller Type selection:

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

Stored Quantities



Panel Memory: 6 MB
Offline Transaction Capacity: 50000

Controller Flags

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

Quantities

Access Levels Per Card: 32
Large Card Size (bytes): *None*
Precision Access Levels: *None*
Access Levels: 255
Triggers: 125
Macros: 125
Time Schedules: 255
Holidays: 255
Cards: 3000
Secured Areas: 32
Unreported Transactions: 4000

Elevator Control

Max Floor: 28
Max per Cab: 26
Floor Groups: *None*

PIN and Duress Options

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

Controller Memory

- Panel Memory - The amount of memory on the controller (SSP).

Offline Transaction Capacity

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

Controller Flags

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

- Store Issue Codes - Stores Issue Codes for cards. The Issue Code number is used with magstripe cards and indicates the number of times a card has been issued to the cardholder (e.g. replacing a lost card). It is an internal number that is programmed on the card. See page 8-83 for card format information.
- Store APB Location - If selected, stores the Anti-Pass Back (APB) locations when using APB.
- Store Activation Date - Stores the activation date and prevents access prior to date set (Default).
- Store Deactivation Date - Stores the deactivation date and prevents access after date set (Default).
- Support Timed Anti-Pass Back - Stores time of last entry to use with Anti-Pass Back. This option must be selected in order to use Timed Anti-Pass Back. For more information, see Chapter 11.
- Store Vacation Date - Stores the dates set for the vacation feature. See page 7-11 for more information.
- Store Temporary Upgrade Date - Stores the temporary access level. See page 7-17 for more information.
- Store Trigger Code - Stores trigger codes for card events on trigger and macro events.
- Store Use Limit - If selected, a card's Use Limit will be stored in the controller. See page 7-37 for more information.

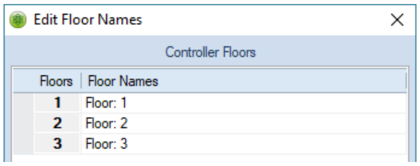
Quantities

- Access Levels Per Card - Number of access levels that can be assigned per card for the selected SSP. For more information on access levels, see Chapter 6.
- Large Card Size (bytes) - Provides support for large card sizes for PIV, PIV-I and T cards.
- Precision Access Levels - The maximum number of precision access levels that can be assigned. See page 6-17 for more information.

- Access Levels - The maximum number of access levels that can be stored in the controller (Max. 255).
- Triggers - Indicates the maximum number of triggers to store (Default = 125).
- Macros - Indicates the maximum number of macros to store (Default = 125).
- Time Schedules - Each controller is able to store 255 time schedules (Auto-populated).
- Holidays - Each controller is able to store 255 holidays (Auto-populated).
- Cards - Indicates the maximum number of cards that can be stored in the controller. Cardholders must have an access level associated with the controller.
- Secured Areas - The maximum number of secured areas that can be created in the controller.
- Unreported Transactions - Number of unreported transactions before an event is logged. An event will occur when this number is exceeded. This event can be used to trigger the SSP to dial back and report transactions.

Elevator Control

- Max Floor - Indicates the maximum number of floors in the building.
- Max per Cab - Select the maximum number of floors per cab. The number entered must be less than or equal to the Max Floor quantity.
- Floor Groups - Maximum number of elevator access levels per floor group.
- Edit Floor Names - Opens the Edit Floor Names dialog to enter floor names. The number of Floor Names that can be edited is determined by the Max Floor setting.
  - □ **Enter** a Floor Name for the desired Floor(s) and **click** OK.



Edit Floor Names

Controller Floors

Floors	Floor Names
1	Floor: 1
2	Floor: 2
3	Floor: 3

PIN and Duress Options

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

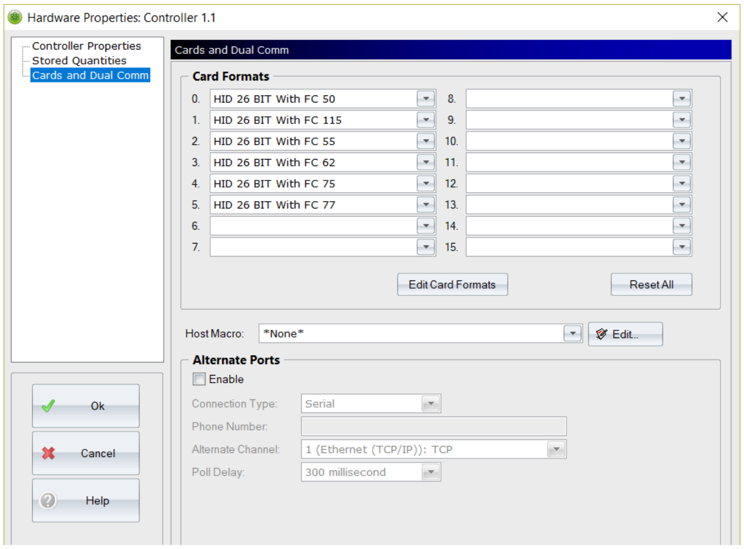
      If the Duress Digit is set to 6, then the cardholder's duress PIN would be 1230 – cardholder's original PIN 1234 + 6 = 1230.

      If the Duress Digit is set to 7, then the cardholder's duress PIN would be 1231 – cardholder's original PIN 1234 + 7 = 1231.

  If the Add option is selected, verify that duress PIN codes do not overlap with another cardholder's PIN number.
  - □ Append - If selected, the duress would be issued when the cardholder inserts the Duress Digit at the end of the cardholder's original PIN code.
    - ✦ Example: If the PIN Number is 1234 and the Duress Digit is set to 1, then the cardholder's Duress PIN would be 12341 – cardholder's original PIN 1234 with 1 inserted at the end = 12341.

      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



Hardware Properties: Controller 1.1

- Controller Properties
- Stored Quantities
- Cards and Dual Comm

Cards and Dual Comm

Card Formats

0.	HID 26 BIT With FC 50	8.	
1.	HID 26 BIT With FC 115	9.	
2.	HID 26 BIT With FC 55	10.	
3.	HID 26 BIT With FC 62	11.	
4.	HID 26 BIT With FC 75	12.	
5.	HID 26 BIT With FC 77	13.	
6.		14.	
7.		15.	

Host Macro: *None*

Alternate Ports

☐ Enable

Connection Type: Serial

Phone Number:

Alternate Channel: 1 (Ethernet (TCP/IP)): TCP

Poll Delay: 300 millisecond

Card Formats (Assets)

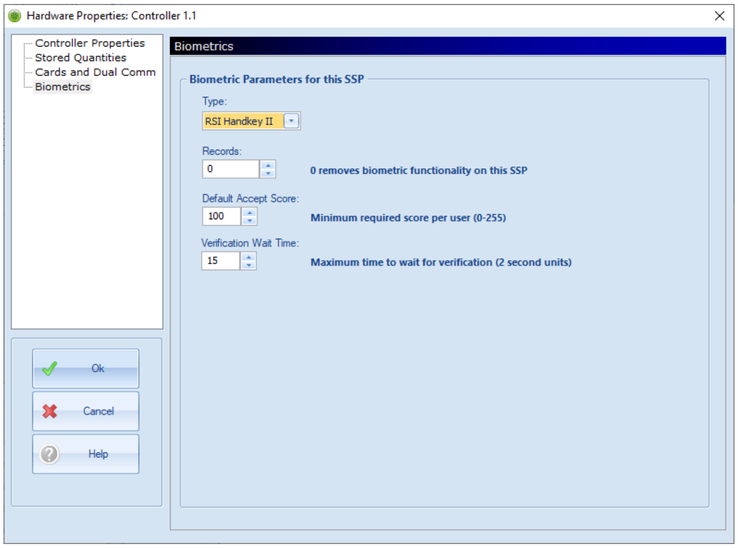
- Card Formats 0-15 - Select a card format from the drop-down list. See page 8-83 for more information on creating card formats.
- Edit Card Formats - Opens the Card Formats Dialog to add, copy, edit, or remove card formats. See page 8-83 for more information.
- Host Macro - Select the Host Based Macro to execute from the list or click the Edit button.
  - Edit - Opens the Host Based Macro (Global I/O) dialog. See page 10-13 for more information on Host Based Macros.

Alternate Ports

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

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

Biometrics



Biometrics

Biometric Parameters for this SSP

Type: RSI Handkey II

Records: 0 — 0 removes biometric functionality on this SSP

Default Accept Score: 100 — Minimum required score per user (0-255)

Verification Wait Time: 15 — Maximum time to wait for verification (2 second units)

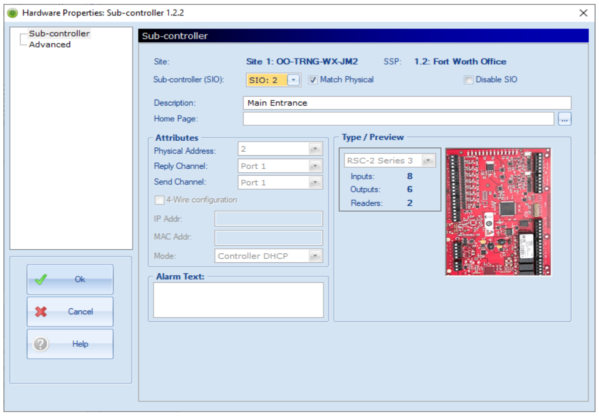
Biometric Parameters for this SSP

Biometrics display's on an Hardware Properties when the site is licensed for biometric readers.

- Type - Select a biometric reader from the drop-down menu.
- Records - Requires more than zero (0) records to download. A zero (0) removes all biometric functionality.
- Default Accept Score - Select the minimum acceptance score per user.
- Verification Wait Time - Select the maximum wait for verification.

Subcontroller Properties

Subcontrollers are a series of circuit boards that communicate information about field devices, such as readers and motion detectors, upstream to the controller (SSP).



Hardware Properties: Sub-controller 1.2.2

Sub-controller

Site: Site 1: OO-TRNG-WX-JM2 SSP: 1.2: Fort Worth Office

Sub-controller (SIO): SIO: 2 ☑ Match Physical ☐ Disable SIO

Description: Main Entrance

Home Page:

Attributes

Physical Address: 2

Reply Channel: Port 1

Send Channel: Port 1

☐ 4-Wire configuration

IP Addr:

MAC Addr:

Mode: Controller DHCP

Alarm Text:

Type / Preview

RSC-2 Series 3

Inputs: 8

Outputs: 6

Readers: 2

Sub-Controller

Address

- Site - Identifies the site name defined in the Site Properties dialog (Auto-populated).
- SSP - Name of the SSP controller attached to the subcontroller (Auto-populated).
- Subcontroller (SIO) - Subcontroller identification in the software.
  - □ Match Physical - Matches the physical address in the software with the DIP switch settings on the board. When selected, the SSP will attempt to communicate with the subcontroller using the subcontroller identification number. See the Hardware Manual for more information on DIP switch settings.
- Disable SIO - If checked, the subcontroller will be disabled and communication with the controller will stop.
- 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 DIP switches. This option will be grayed out when the Match Physical option is selected and will automatically increase as subcontrollers are added to the system. See the Hardware Manual for more information on DIP switch settings.
- 4-Wire Configuration - If checked, indicates the 4-Wire RS-485 communication is ON (Legacy hardware only).
- SSP Reply Channel - Identifies the SSP port that the subcontroller will use when communicating with the controller.
- SSP Send Channel - Reflects the SSP Reply Channel (Auto-populated).
- IP Addr - When the NSC-100/200 subcontroller is selected, the IP Addr field identifies the IP address assigned to the subcontroller.
- MAC - If the NSC-100 subcontroller is selected, the MAC field identifies the subcontroller's default MAC address.
- Host Name - If the NSC-200 subcontroller is selected, the Host Name field identifies the subcontroller's default MAC address.
- Mode - For NSC-100 subcontrollers, the Mode field identifies the subcontroller's network protocol. See page 3-33 in the Hardware Manual for more information.
  - □ Controller DHCP - The NSC-100's MAC address is automatically assigned an IP address from the controller, and the embedded DHCP server loads the IP address into the NSC-100. This method requires that the NSC-100 and the controller be in the same sub-net and not isolated by network switches.
  - □ Public DHCP - The NSC-100's MAC address is automatically assigned an IP address from the public DHCP server, and the embedded DHCP server loads the IP address into the NSC-100.
  - □ Static Address - The NSC-100 will be manually assigned a static IP address using the MR51E Address Tool.

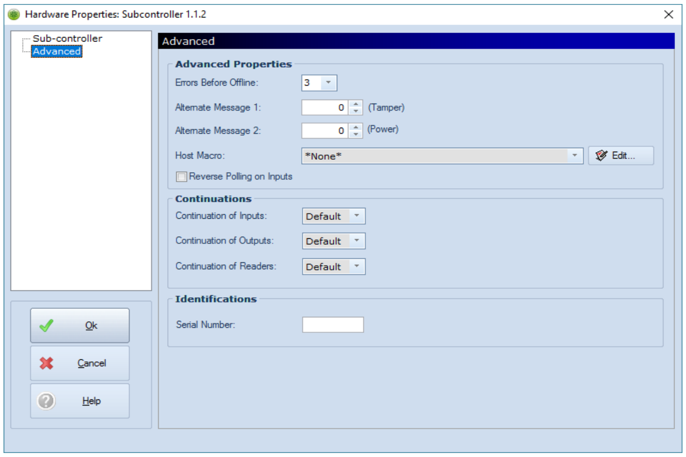
Type/Preview

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

Alarm Text

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

Advanced



Hardware Properties: Subcontroller 1.1.2

Advanced

Advanced Properties

Errors Before Offline: 3

Alternate Message 1: 0 (Tamper)

Alternate Message 2: 0 (Power)

Host Macro: *None*

□ Reverse Polling on Inputs

Continuations

Continuation of Inputs: Default

Continuation of Outputs: Default

Continuation of Readers: Default

Identifications

Serial Number:

Advanced Properties

- Errors Before Offline - Number of consecutive communication errors before the subcontroller is determined to be offline. (Default = 3)
- Alternate Message 1 (Tamper) - Changes the alarm priority for the cabinet tamper from the event-specific priority to the user-determined priority.
- Alternate Message 2 (Power) - Changes the alarm priority for the power tamper from the event-specific priority to the user determined priority.
- Host Macro - Select the Host Based Macro to execute.
  - ❑ Edit - Opens the Host Based Macro (Global I/O) dialog. See page 10-13 for more information on Host Based Macros.
- Reverse Polling on Inputs - Changes the order by which the system processes inputs. If selected, inputs will be processed from higher number to lower number.

Continuations

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

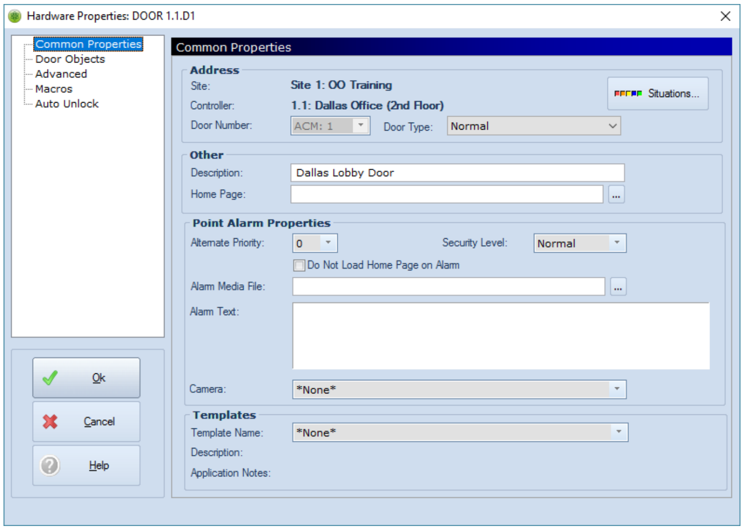
- Continuation of Inputs (Elevator Setting) - If the number of floors selected exceeds the available inputs for a single controller, inputs will be taken from the next consecutive subcontroller. This allows you to jump/skip subcontrollers with continuation.
- Continuation of Outputs (Elevator Setting)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

Identifications

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

Door Properties

A door, also referred to as an Access Control Model (ACM), performs two functions: validates requests and manages the access point.



Common Properties

Address

Site: Site 1: OO Training

Controller: 1.1: Dallas Office (2nd Floor)

Door Number: ACM: 1 Door Type: Normal

Other

Description: Dallas Lobby Door

Home Page:

Point Alarm Properties

Alternate Priority: 0 Security Level: Normal

□ Do Not Load Home Page on Alarm

Alarm Media File:

Alarm Text:

Camera: *None*

Templates

Template Name: *None*

Description:

Application Notes:

Common Properties

Address

- Site - Identifies the site associated with the door. (Auto-populated)
- Controller - Identifies the controller associated with the door. (Auto-populated)
- Door Number - Drop-down field to select the ACM number.
- Door Type - Determines how the door will function.
  - □ Normal - Door will operate as a regular access control door.
  - □ Muster - Door will operate as both a muster point and a regular access control door. See the Muster Report Manual for more information.
  - □ Auto Activate - Door will operate as a regular access control door, but if a badge is presented that has been designated an Auto Activate card, the badge will be activated. See page 7-11 for more information.
  - □ Auto Deactivate - Door will operate as a regular access control door, but if a badge is presented that has been designated an Auto Deactivate card, the badge will be deactivated. See page 7-11 for more information.
  - □ Time and Attendance In - Door will operate as a regular access control door, but if a badge is presented that has been designated a Time & Attendance card, the data will be collected and stored in a separate table as the In Time. See page 7-11 for more information.
  - □ Time and Attendance Out - Door will operate as a regular access control door, but if a badge is presented that has been designated a Time & Attendance card, the data will be collected and stored in a separate table as the Out Time. See page 7-11 for more information.
- Situations... - Opens the Situation Level Manager Settings dialog for the associated door. See Chapter 9 for more information.

Other

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

Point Alarm Properties

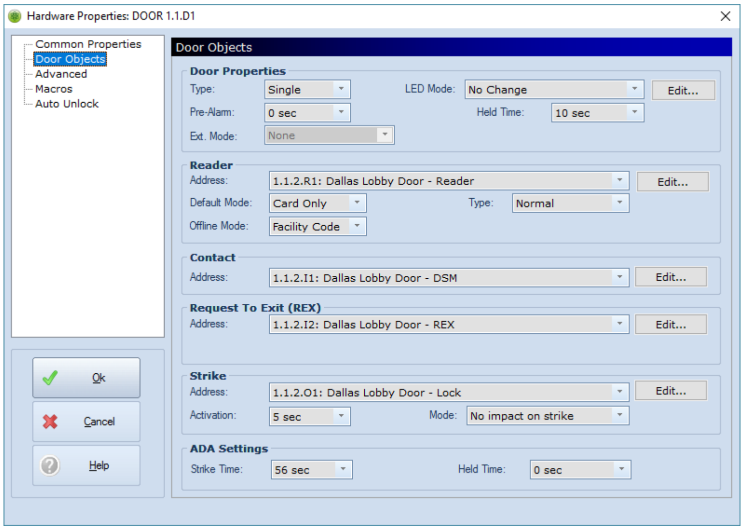
- Alternate Priority - If selected, overrides the default event-specific Alarm Priority set in DNA / Administrative / Alarms and Events / Logging. The alternate ID will be displayed in the Alarm Grid. See page 14-25 for more information.
- Security Level - Category designation. Allows administrator to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

Templates

The operator should create templates before applying them to hardware objects. See page 8-85 for more information on templates.

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

Door Objects



Door Objects

Door Properties

Type: Single | LED Mode: No Change

Pre-Alarm: 0 sec | Held Time: 10 sec

Ext. Mode: None

Reader

Address: 1.1.2.R1: Dallas Lobby Door - Reader

Default Mode: Card Only | Type: Normal

Offline Mode: Facility Code

Contact

Address: 1.1.2.I1: Dallas Lobby Door - DSM

Request To Exit (REX)

Address: 1.1.2.I2: Dallas Lobby Door - REX

Strike

Address: 1.1.2.O1: Dallas Lobby Door - Lock

Activation: 5 sec | Mode: No impact on strike

ADA Settings

Strike Time: 56 sec | Held Time: 0 sec

Door Properties

- Type - Specifies the type of door.
  - □ Single - Select this option to configure a single door with one reader.
  - □ In and Out - Select this option when using Access Areas or Anti-Pass Back; two readers will be assigned to the door.
  - □ Turnstile - Select this option to configure a turnstile door; the Strike Mode drop-down list will appear.
- Pre-Alarm - Number of seconds before the selected door reports a Door Held Pre-Alarm event/alarm, causing an event to be generated prior to a Door Held alarm.
- Ext. Mode - Only applies to Aperio and Schlage locks. The selected mode will make the door function in a specific manner. Refer to the Hardware Manual for more information.

> *Privacy Mode needs Aperio firmware 1.101.13 or greater and Mercury Firmware 1.25.6 or greater.*

- LED Mode - Defines the LED operation of the reader.
  - □ Edit - Opens the LED Function Configuration dialog to configure the LED settings for custom values.
- Held Time - Length of time an input will be ignored when it goes active during an Access Granted event. Indicates the number of seconds before the door reports a Door Held event/alarm. This only applies to inputs that are specified as the Door Contact.
- Strike Mode - Only appears if the Type was set to Turnstile; select a mode from the drop-down.
  - □ Pulse on Grant - Pulses the turnstile when access is granted.
  - □ Pulse on Door Cycle - Pulses the turnstile when the arm is cycled.

Reader

- Address - Specifies the reader’s address.
  - □ Edit - Opens the Reader Properties dialog. See page 8-72 for more information.
- Default Mode - Defines the normal state of the reader.
  - □ Disabled - Disables the reader; the door remains locked with no REX capability.
  - □ Unlocked - Allows unlimited access to the door without the need for an access level.
  - □ Locked - Access is not allowed, but the door can be used from the inside by using the REX button.
  - □ F/C Code - Only the facility code is checked for access authorization.
  - □ Card Only - Checks the card number for access authorization.
  - □ PIN Only - Verifies the PIN code for access authorization.
  - □ Card and PIN - Checks the card and PIN numbers for access authorization.
  - □ PIN or Card - Either the PIN or card number is checked for access authorization.

- Offline Mode - Defines the offline mode of the reader.
  - ☐ None - The door is not associated with a reader nor any additional door hardware.
  - ☐ Disabled - Disables the reader; the door remains locked with no REX capability.
  - ☐ Unlocked - Allows unlimited access to the door without the need for an access level.
  - ☐ Locked - Access is not allowed, but the door can be used from the inside by using the REX button.
  - ☐ Facility Code - Only the facility code is checked for access authorization.
- Type - Specifies the type of reader.
  - ☐ Normal - Standard card reader.
  - ☐ Keypad - A reader with a numeric keypad.
  - ☐ Text Keypad - A reader with both a numeric keypad and text display.

Contact

- Address - Specifies the address of the door contact.
  - ☐ Edit - Opens the Input Properties dialog for the door contact. See page 8-75 for more information.

Request to Exit (REX)

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

- Address - Specifies the address of the REX.
  - ☐ Edit - Opens the Input Properties dialog for the REX input. See page 8-75 for more information.

Out Reader

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

- Address - Specifies the address of the Out Reader; both readers must be wired to the door.
  - ☐ Edit - Opens the Reader Properties dialog for the reader. See page 8-72 for more information.
- Pair Door - Drop-down field to select a Door to pair with the Out Reader.

Strike

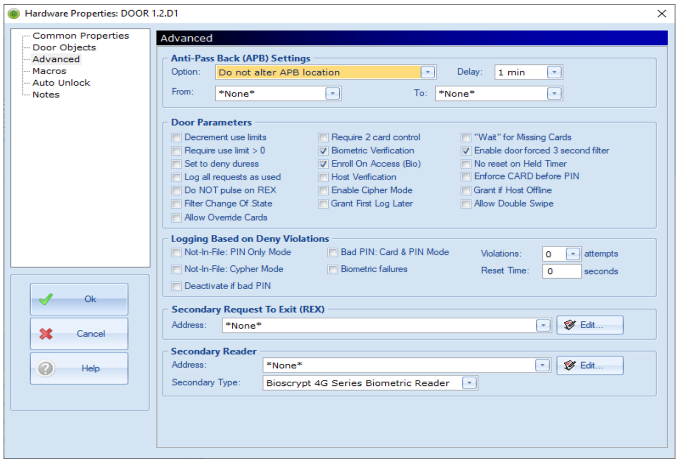
- Address - Specifies the address of the door strike.
  - ☐ Edit - Opens the Output Properties dialog for the strike. See page 8-79 for more information.
- Activation - Maximum number of seconds the door will be unlocked when an Access Granted event is received. Check code for your area.
- Mode - Defines how the door strike will behave when the door is opened.
  - ☐ No impact on strike - Opening the door or closing the door does not affect the activation timer.
  - ☐ Cut Short On Open - Strike activation timer is canceled and the strike is re-energized when the door is opened.
  - ☐ Cut Short On Close - Strike activation timer is canceled and the strike is re-engergized when the door is closed after being opened. Primarily used for magnetic doors.
  - ☐ Tailgate: Short On Open - Strike activation timer is canceled and the strike is re-energized when the door is opened. In addition, the adjacent relay is pulsed for one (1) second.
    - ✦ Example: If the strike is assigned to 1.1.1.O1 then 1.1.1.O2 would be pulsed for one (1) second.
  - ☐ Tailgate: Short On Close - Strike activation timer is canceled and the Strike is re-engergized when the door is closed after being opened. In addition, the adjacent relay is pulsed for one (1) second.
    - ✦ Example: If the strike is assigned to 1.1.1.O1 then 1.1.1.O2 would be pulsed for one (1) second.

ADA Settings

The following options are invoked for cardholders when ADA Mode is flagged in the Card Tab of the Cardholder's Record. See page 7-11 for more information.

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

Advanced



Hardware Properties: DOOR 1.2.D1

Advanced

Anti-Pass Back (APB) Settings

Option: Do not alter APB location

Delay: 1 min

From: *None*

To: *None*

Door Parameters

☐ Decrement use limits
☐ Require use limit > 0
☐ Set to deny duress
☐ Log all requests as used
☐ Do NOT pulse on REX
☐ Filter Change Of State
☐ Allow Override Cards

☐ Require 2 card control
☑ Biometric Verification
☑ Enroll On Access (Bio)
☐ Host Verification
☐ Enable Cipher Mode
☐ Grant First Log Later

☐ "Wait" for Missing Cards
☑ Enable door forced 3 second filter
☐ No reset on Held Timer
☐ Enforce CARD before PIN
☐ Grant if Host Offline
☐ Allow Double Swipe

Logging Based on Deny Violations

☐ Not-In-File: PIN Only Mode
☐ Not-In-File: Cypher Mode
☐ Deactivate if bad PIN

☐ Bad PIN: Card & PIN Mode
☐ Biometric failures

Violations: 0 attempts

Reset Time: 0 seconds

Secondary Request To Exit (REX)

Address: *None*

Secondary Reader

Address: *None*

Secondary Type: Bioscrypt 4G Series Biometric Reader

Anti-Pass Back (APB) Settings

See Chapter 11 for information on configuring Anti-Pass Back.

- Option - Drop-down field to select the type of anti-pass back.
  - □ Do not alter APB location - Anti-pass back is not in use.
  - □ Accept any location, change on entry - Accept any new location, change the user's location to the current reader, and generate an anti-pass back violation for an invalid entry. (Area-based Soft APB)
  - □ Check location, change on entry - Check user location; if a valid entry is made, change the user's location to the new location. If an invalid entry is attempted, do not grant access. (Area-based Hard APB)
  - □ Check last valid user - References the user's card number and will not allow access to the same card number until either a different card is presented at the reader or the APB delay expires. Requires Support Timed Anti-Pass Back to be enabled in the Controller Properties / Stored Quantities dialog. See page 8-53 for more information. (Reader-based APB using the reader's last user)
  - □ Check last ACR used, no location change - Does not allow a cardholder to present his or her card to the same reader twice in a row. Once access is granted at the reader, the user will not be granted access at the same reader again until the user presents his card at another reader in the system or until the APB delay expires. Requires Support Timed Anti-Pass Back to be enabled in the Controller Properties / Stored Quantities dialog. See page 8-53 for more information. (Reader-based APB using the cardholder's access history)
  - □ Check current location, change on entry - Similar to option #2, except that the APB delay will reset the user's area after the specified time. Requires Support Timed Anti-Pass Back to be enabled in the Controller Properties / Stored Quantities dialog. See page 8-53 for more information. (Area-based APB)
- Delay - The number of minutes before APB resets. Only used in conjunction with APB options #3-5. (Max. delay = 1092 minutes)
- From - The Access Area that the cardholder comes from.
- To - The Access Area that the cardholder enters.

Door Parameters

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

- Require 2 Card Control - Requires two (2) valid access credentials to be presented for access to be granted.
- Biometric Verification - Select if biometric hardware is being supported. This is an advanced feature and should be avoided unless the operator has an understanding of the ramifications.
- Enroll on Access (Bio) - Select if biometric hardware is being supported; the system will record the a person's biometric signature on the first presentation. This information will be used as the future reference.
- Host Verification - Host verification must be obtained prior to granting access. See page 8-54 Host Response Time to set the timeout parameter. If selected, access at this door will be dependent on communication with the DNA server.
- Enable Cipher Mode - Allows the user to enter the card number through a keypad.
- Grant First Log Later - Grants access to the door and then logs the event; allows instant access to the door. Door Used/Not Used events are not logged until door is actually opened or timeout expires. Applies to Access Granted events only.
- "Wait" for Missing Cards - If an access request is denied due to a Card Not in File event, the reader is put into the wait state and waits for a host response from the DNA server.
- Enable Door Forced 3 Second Filter - If selected, a Door Forced event will NOT be reported if the door is reopened within three (3) seconds of closing after an Access Granted event. (Default setting)
- No Reset on Held Timer - If the selected door is opened after an Access Granted event, and a subsequent card read occurs, the Held Time set in the Common Properties dialog will not start over.
- Enforce CARD before PIN - Requires the cardholder to badge before entering their PIN number.
- Grant If Host Offline - Access will be granted if the host is offline. Works in conjunction with Host Verification.
- Allow Double Swipe - Enables the double swipe feature for the door. If selected, the user can write a trigger and macro combination to execute programmed commands. See page 10-9 for more information.
- Allow Override Cards - Allows cardholders with Override Card credentials to bypass any door parameter and allow access to the door.

Logging Based on Deny Violations

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

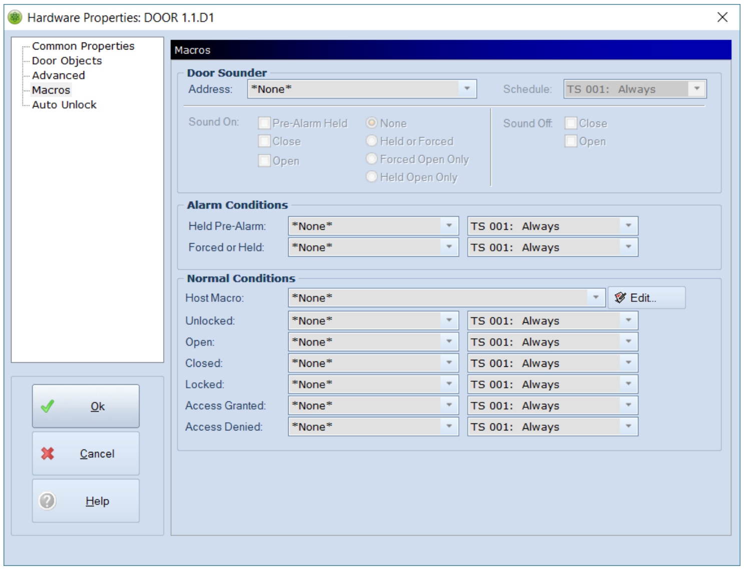
Secondary Request to Exit (REX)

- Address - Address of the secondary REX.
  - □ Edit - Opens the Output Properties dialog for the secondary REX. See page 8-79 for more information.

Secondary Reader

- Address - Drop-down list of readers to select for Reader 2.
  - □ Edit - Opens the Reader Properties dialog for this object. See page 8-72 for more information.
- Secondary Type - Drop-down list of reader types to select for Reader 2.

Macros



Door Sounder

Address: *None*   Schedule: TS 001: Always

Sound On: □ Pre-Alarm Held □ Close □ Open   ● None ○ Held or Forced ○ Forced Open Only ○ Held Open Only

Sound Off: □ Close □ Open

Alarm Conditions

Held Pre-Alarm:	*None*	TS 001: Always
Forced or Held:	*None*	TS 001: Always

Normal Conditions

Host Macro:	*None*	
Unlocked:	*None*	TS 001: Always
Open:	*None*	TS 001: Always
Closed:	*None*	TS 001: Always
Locked:	*None*	TS 001: Always
Access Granted:	*None*	TS 001: Always
Access Denied:	*None*	TS 001: Always

Door Sounder

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

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

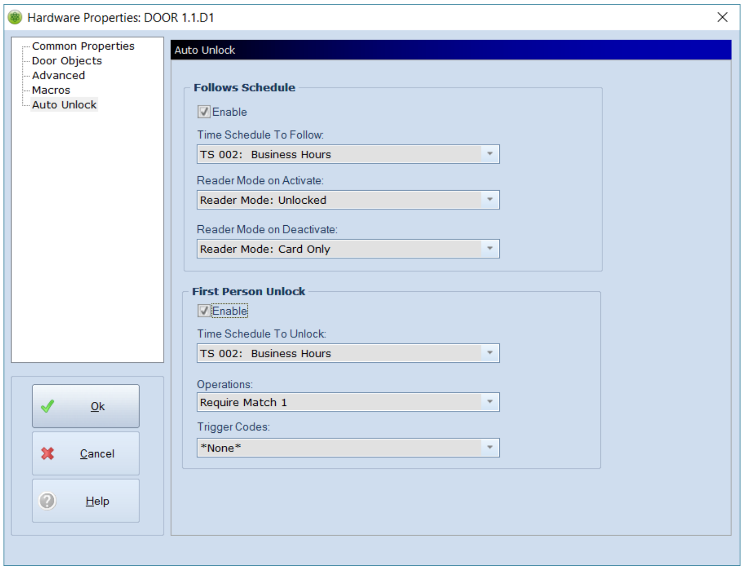
Alarm Conditions

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

Normal Conditions

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

Auto Unlock



Hardware Properties: DOOR 1.1.D1

Auto Unlock

Follows Schedule

☑ Enable

Time Schedule To Follow: TS 002: Business Hours

Reader Mode on Activate: Reader Mode: Unlocked

Reader Mode on Deactivate: Reader Mode: Card Only

First Person Unlock

☑ Enable

Time Schedule To Unlock: TS 002: Business Hours

Operations: Require Match 1

Trigger Codes: *None*

Follows Schedule

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

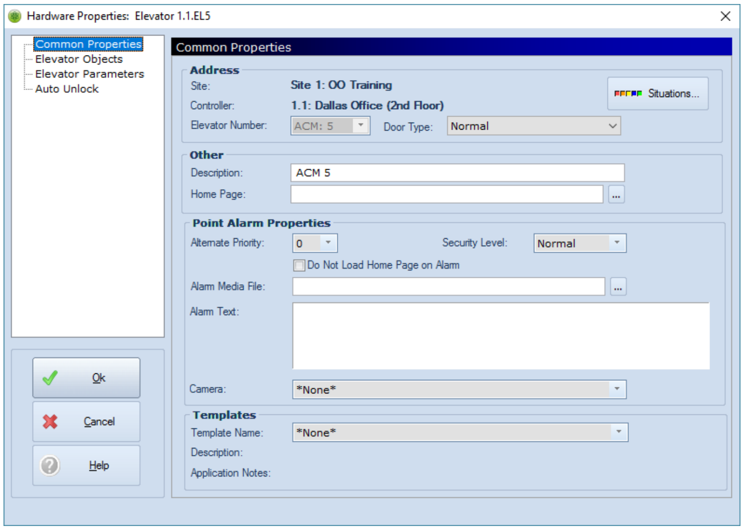
- Enable - If checked, activates the fields in the Follows Schedule section.
  - □ Time Schedule to Follow - Select the desired Time Schedule from the drop-down list.
  - □ Reader Mode on Activate - Select the Reader Mode for the door when the specified time schedule becomes active.
  - □ Reader Mode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

First Person Unlock

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

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

Elevator Properties



Address
Site: Site 1: OO Training
Controller: 1.1: Dallas Office (2nd Floor)
Elevator Number: ACM: 5 Door Type: Normal

Other
Description: ACM 5
Home Page:

Point Alarm Properties
Alternate Priority: 0 Security Level: Normal
☐ Do Not Load Home Page on Alarm
Alarm Media File:
Alarm Text:
Camera: *None*

Templates
Template Name: *None*
Description:
Application Notes:

The Elevators *option 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 *section. Switch tabs to refresh the view.*

Common Properties

Address

- Site - Identifies the site associated with the elevator (Auto-populated).
- Controller - Identifies the controller associated with the elevator (Auto-populated).
- Elevator Number - Drop-down field to select the ACM number. Defaults to the next available ACM number.
- Door Type - Determines how the door will function.
  - ☐ Normal - The door will operate as a regular access control door.
  - ☐ Muster - The door will operate as both a muster point and a regular access control door. See the Muster Report Manual for more information.
  - ☐ Auto Activate - The door will operate as a regular access control door, but if a badge is presented that has been flagged as an Auto Activate card, the badge will be activated. See page 7-11 for more information.
  - ☐ Auto Deactivate - The door will operate as a regular access control door, but if a badge is presented that has been flagged as an Auto Deactivate card, the badge will be deactivated. See page 7-11 for more information.
  - ☐ Time and Attendance In - The door will operate as a regular access control door, but if a badge is presented that has been flagged for Time & Attendance, the data will be collected and stored in a separate table as the In Time. See page 7-11 for more information.
  - ☐ Time and Attendance Out - The door will operate as a regular access control door, but if a badge is presented that has been flagged for Time & Attendance, the data will be collected and stored in a separate table as the Out Time. See page 7-11 for more information.
- Situations... - Opens the Situation Level Manager Settings dialog for the associated elevator. See Chapter 9 for more information.

Other

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

Point Alarm Properties

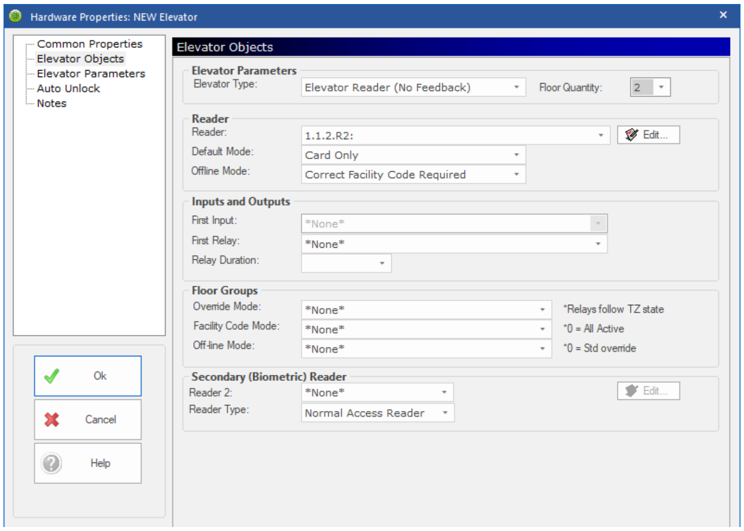
- Alternate Priority - If selected, overrides the default event-specific Alarm Priority set in DNA / Administrative / Alarms and Events / Logging. See page 14-25 for more information.
- Security Level - Category designation. Allows administrator to restrict operator use.
- Do Not Load Home Page on Alarm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

Templates

Templates are covered on page 8-85.

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

Elevator Objects



Elevator Objects

Elevator Parameters
Elevator Type: Elevator Reader (No Feedback)
Floor Quantity: 2

Reader
Reader: 1.1.2.R2:
Default Mode: Card Only
Offline Mode: Correct Facility Code Required

Inputs and Outputs
First Input: *None*
First Relay: *None*
Relay Duration:

Floor Groups
Override Mode: *None* *Relays follow TZ state
Facility Code Mode: *None* *0 = All Active
Off-line Mode: *None* *0 = Std override

Secondary (Biometric) Reader
Reader 2: *None*
Reader Type: Normal Access Reader

Elevator Parameters

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

Reader

- Reader - Specifies the elevator reader's address.
    - □ Edit - Opens the Reader Properties dialog. See page 8-72 for more information.
- Default Mode - Defines the normal state for the elevator.
- Offline Mode - Defines the offline mode for the elevator.

Inputs and Outputs

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

Floor Groups

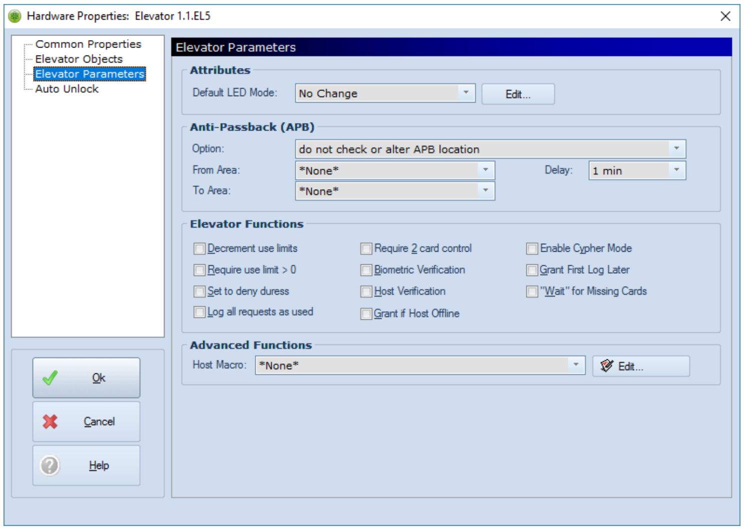
See page 6-9 for more information on floor groups.

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

Secondary (Biometric) Reader

- Reader 2 - Drop-down list of reader addresses to select for Reader 2.
    - □ Edit - Opens the Reader Properties dialog for this object.
- Reader Type - Drop-down list of reader types to select for Reader 2.

Elevator Parameters



Attributes

Default LED Mode: No Change

Anti-Passback (APB)

Option: do not check or alter APB location

From Area: *None*

Delay: 1 min

To Area: *None*

Elevator Functions

□ Decrement use limits
□ Require use limit > 0
□ Set to deny duress
□ Log all requests as used
□ Require 2 card control
□ Biometric Verification
□ Host Verification
□ Grant if Host Offline
□ Enable Cypher Mode
□ Grant First Log Later
□ "Wait" for Missing Cards

Advanced Functions

Host Macro: *None*

Attributes

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

Anti-Pass Back (APB)

See Chapter 11 for information on configuring Anti-Pass Back.

- Option - Drop-down field to select the type of anti-pass back.
  - Do not check or alter APB location - Anti-pass back is not in use.
  - Accept any location, change on entry - Accept any new location, change the user's location to the current reader, and generate an anti-pass back violation for an invalid entry. (Area-based Soft APB)
  - Check location, change on entry - Check user location; if a valid entry is made, change the user's location to the new location. If an invalid entry is attempted, do not grant access. (Area-based Hard APB)
  - Check this reader's last valid user - References the user's card number and will not allow access to the same card number until either a different card is presented at the reader or the APB delay expires. Requires Support Timed Anti-Pass Back to be enabled in the SSP Properties / Stored Quantities dialog. See page 8-53 for more information. (Reader-based APB using the reader's last user)
  - Check user's last ACR used, no location change - Does not allow a cardholder to present his or her card to the same reader twice in a row. Once access is granted at the reader, the user will not be granted access at the same reader again until the user presents his card at another reader in the system or until the APB delay expires. Requires Support Timed Anti-Pass Back to be enabled in the SSP Properties / Stored Quantities dialog. See page 8-53 for more information. (Reader-based APB using the cardholder's access history)
  - Check user's current location, change on entry - Similar to option #2, except that the APB delay will reset the user's area after the specified time. Requires Support Timed Anti-Pass Back be enabled in the SSP Properties/Stored Quantities dialog. See page 8-53 for more information. (Area-based APB)
- Delay - The number of minutes before APB resets. Only used in conjunction with APB options #3-5. (Max. delay = 255 minutes)
- From - The Access Area that the cardholder comes from.
- To - The Access Area that the cardholder enters.

Elevator Functions

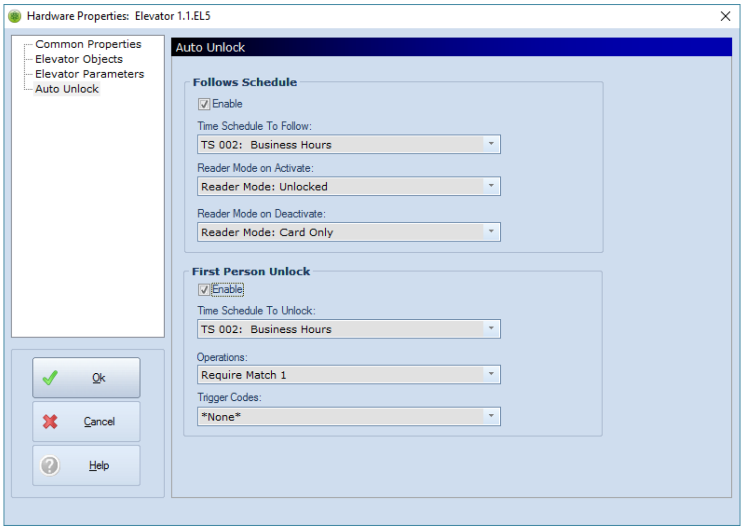
- Decrement Use Limits - The selected elevator will decrement Use Limits associated with cards.
- Require Use Limit > Zero - If a card's Use Limit reaches 0, do not grant access.
- Set to Deny Duress - Denies access when the controller receives a duress signal at the selected elevator. (PIN & Card Mode Only)

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

Advanced Functions

- Host Macro - Select the Host Based Macro to execute.
  - □ Edit - Opens the Host Based Macro (Global I/O) dialog. See page 10-13 for more information on Host Based Macros.

Auto Unlock



Hardware Properties: Elevator 1.1.EL5

- Common Properties
- Elevator Objects
- Elevator Parameters
- Auto Unlock

Auto Unlock

Follows Schedule

☑ Enable

Time Schedule To Follow: TS 002: Business Hours

Reader Mode on Activate: Reader Mode: Unlocked

Reader Mode on Deactivate: Reader Mode: Card Only

First Person Unlock

☑ Enable

Time Schedule To Unlock: TS 002: Business Hours

Operations: Require Match 1

Trigger Codes: *None*

Follows Schedule

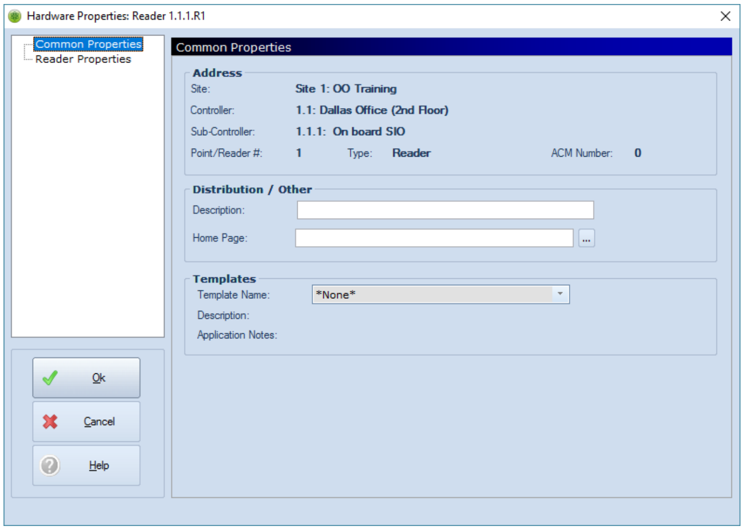
The Follows Schedule feature is used to set up an elevator to adhere to a specified time schedule and designated reader modes. See page 8-16 for more information.

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

First Person Unlock

The First Person Unlock feature allows the operator to configure an elevator that will unlock during a specified time schedule after the first cardholder is granted access to the reader. If enabled, the system will generate a trigger-and-macro combination and store it in the controller's memory. See page 8-16 for more information.

Reader Properties



Hardware Properties: Reader 1.1.1.R1

Common Properties

Address

Site: Site 1: OO Training

Controller: 1.1: Dallas Office (2nd Floor)

Sub-Controller: 1.1.1: On board SIO

Point/Reader #: 1 Type: Reader ACM Number: 0

Distribution / Other

Description:

Home Page:

Templates

Template Name: *None*

Description:

Application Notes:

Common Properties

Address

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

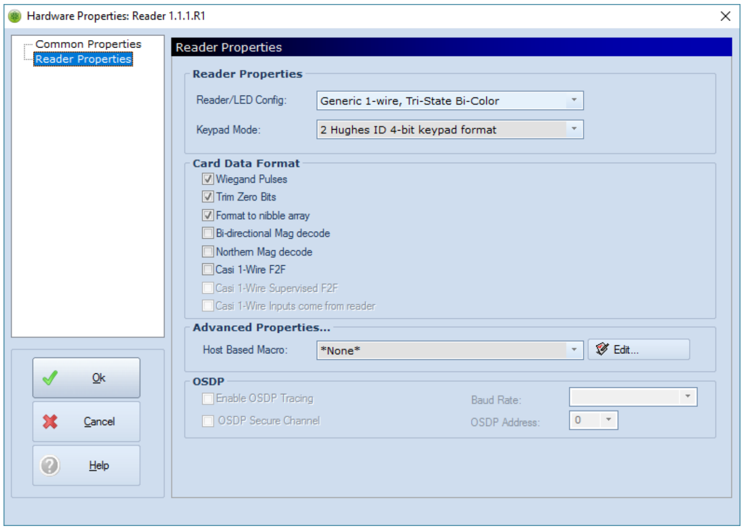
Distribution / Other

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

Templates

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

Reader Properties



Hardware Properties: Reader 1.1.1.R1

Reader Properties

Reader Properties

Reader/LED Config: Generic 1-wire, Tri-State Bi-Color

Keypad Mode: 2 Hughes ID 4-bit keypad format

Card Data Format

☑ Wiegand Pulses

☑ Trim Zero Bits

☑ Format to nibble array

☐ Bi-directional Mag decode

☐ Northern Mag decode

☐ Casi 1-Wire F2F

☐ Casi 1-Wire Supervised F2F

☐ Casi 1-Wire Inputs come from reader

Advanced Properties...

Host Based Macro: *None* Edit...

OSDP

☐ Enable OSDP Tracing Baud Rate:

☐ OSDP Secure Channel OSDP Address: 0

Reader Properties

- Reader/LED Config - Drop-down menu of the LED configurations.
- Keypad Mode - Drop-down menu of the keypad modes.

Card Data Format

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

Advanced Properties

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

OSDP

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

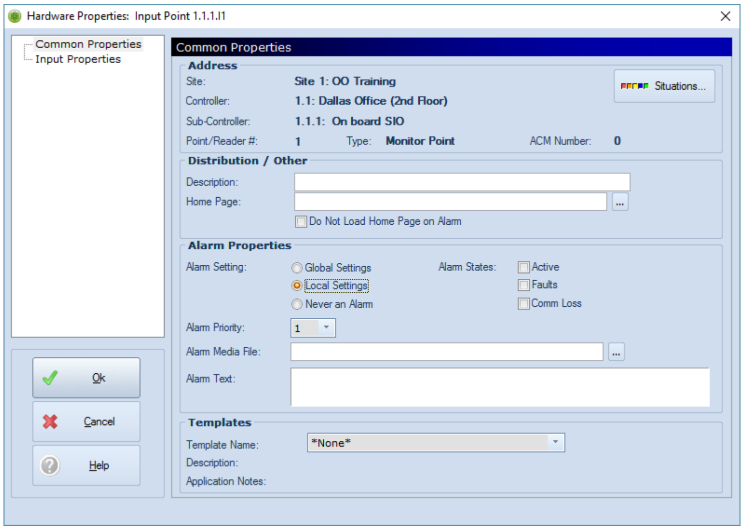
- Enable OSDP Tracing - Provides additional diagnostic information. This option should only be enabled if advised by Open Options Technical Support.
- OSDP Secure Channel - Encrypts the communication channel between the OSDP reader and the door controller.
- Baud Rate - Drop-down list to select the baud rate for the OSDP reader.
- OSDP Address - Drop-down list to select the address for the OSDP reader.

NOTES:

Input Point Properties

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

Common Properties



Hardware Properties: Input Point 1.1.1.I1

Common Properties

Address

Site: Site 1: OO Training

Controller: 1.1: Dallas Office (2nd Floor)

Sub-Controller: 1.1.1: On board SIO

Point/Reader #: 1 Type: Monitor Point ACM Number: 0

Distribution / Other

Description:

Home Page:

□ Do Not Load Home Page on Alarm

Alarm Properties

Alarm Setting: ○ Global Settings ● Local Settings ○ Never an Alarm

Alarm States: □ Active □ Faults □ Comm Loss

Alarm Priority: 1

Alarm Media File:

Alarm Text:

Templates

Template Name: *None*

Description:

Application Notes:

Address

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

Distribution / Other

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

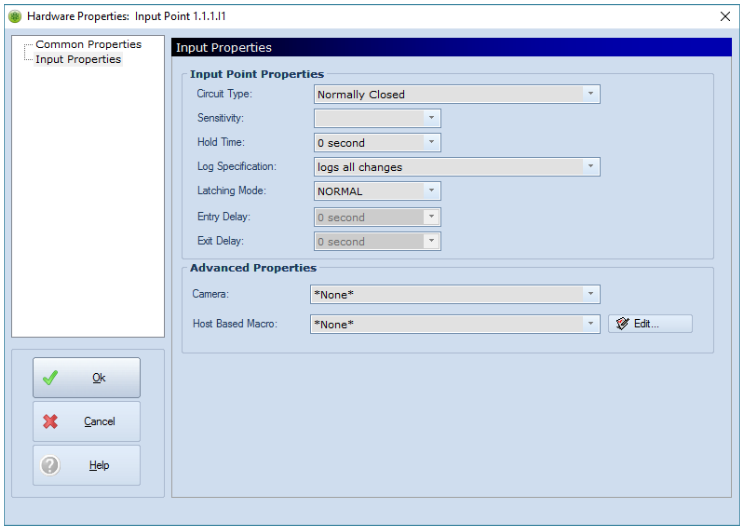
Alarm Properties

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

Templates

- Template Name - Select a template to configure the input point. See page 8-85.
- Description - Auto-populated by the template.
- Application Notes - Auto-populated by the template.

Input Properties


Hardware Properties: Input Point 1.1.1.I1

Input Properties

Input Point Properties

Circuit Type: Normally Closed

Sensitivity:

Hold Time: 0 second

Log Specification: logs all changes

Latching Mode: NORMAL

Entry Delay: 0 second

Exit Delay: 0 second

Advanced Properties

Camera: *None*

Host Based Macro: *None*

Input Point Properties

- Circuit Type - Defines the circuit when in the normal state.
  - □ Normally Closed - No End of Line Termination (EOL)
  - □ Normally Open - No EOL
  - □ Normally Closed (1K Safe, 2K Alarm) - With EOL
  - □ Normally Open (2K Safe, 1K Alarm) - With EOL
  - □ Custom Table 1-4
- Sensitivity - Number of consecutive input scans before a change of state is reported. A low sensitivity setting (2) requires the system to receive 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, as noise and other factors may cause the system to report numerous changes in state.*

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

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

- □ Latching - The contact closure will generate an alarm unless the point is masked within the entry delay time. If the door is opened, regardless if the door is shut again, an alarm will be generated (unless the monitor point is masked). This is the recommended setting. If selected, an Entry and Exit Delay should be set.

- Entry Delay - Warning period to allow for disarming of system. If the system is not disarmed within the entry delay, an alarm will be generated. Available if Non-Latching or Latching is selected for the Latching Mode.
- Exit Delay - Amount of time to delay before removing the mask to allow for arming of the system. Once the exit delay has expired, the mask is removed and the point is considered armed. Available if Non-Latching or Latching is selected for the Latching Mode.

Advanced Properties

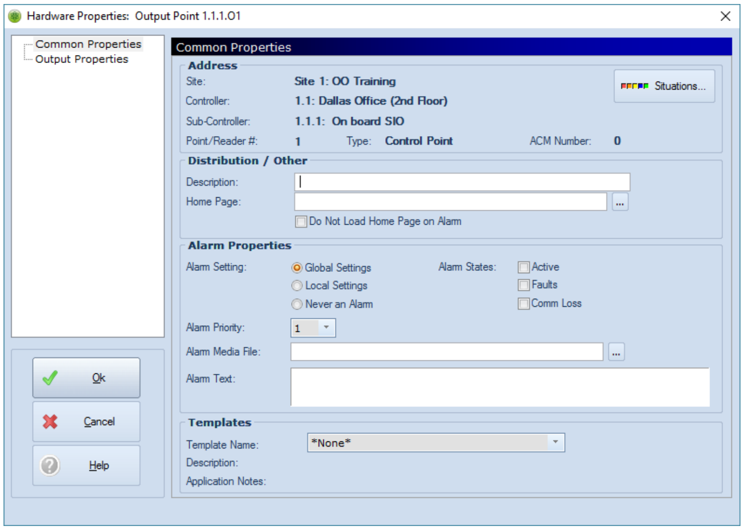
- Camera - Drop-down list of available cameras to associate with the input point. If selected, enables the Launch Camera and Show Archived Video options in the Events and Alarm Grid context menus. Selecting a menu option will populate the camera in the Video View Manager.
- Host Based Macro - Select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

NOTES:

Output Point Properties

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

Common Properties



Hardware Properties: Output Point 1.1.1.01

Common Properties

Address

Site: Site 1: OO Training

Controller: 1.1: Dallas Office (2nd Floor)

Sub-Controller: 1.1.1: On board SIO

Point/Reader #: 1 Type: Control Point ACM Number: 0

Distribution / Other

Description:

Home Page:

☐ Do Not Load Home Page on Alarm

Alarm Properties

Alarm Setting: ● Global Settings ○ Local Settings ○ Never an Alarm

Alarm States: ☐ Active ☐ Faults ☐ Comm Loss

Alarm Priority: 1

Alarm Media File:

Alarm Text:

Templates

Template Name: *None*

Description:

Application Notes:

Address

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

Distribution / Other

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

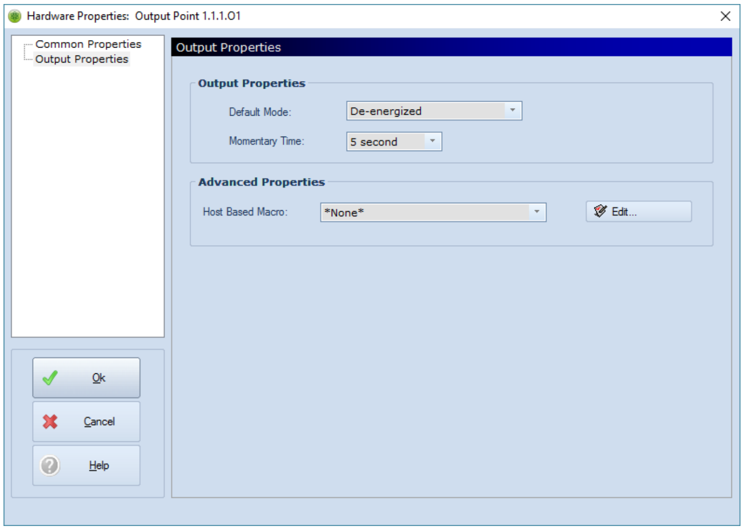
Alarm Properties

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

Templates

- Template Name - Select a template to configure the output point. See page 8-85.
- Description - Auto-populated by the template.
- Application Notes - Auto-populated by the template.

Output Properties



Hardware Properties: Output Point 1.1.1.01

Output Properties

Default Mode: De-energized

Momentary Time: 5 second

Advanced Properties

Host Based Macro: *None*

Output Properties

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

Advanced Properties

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

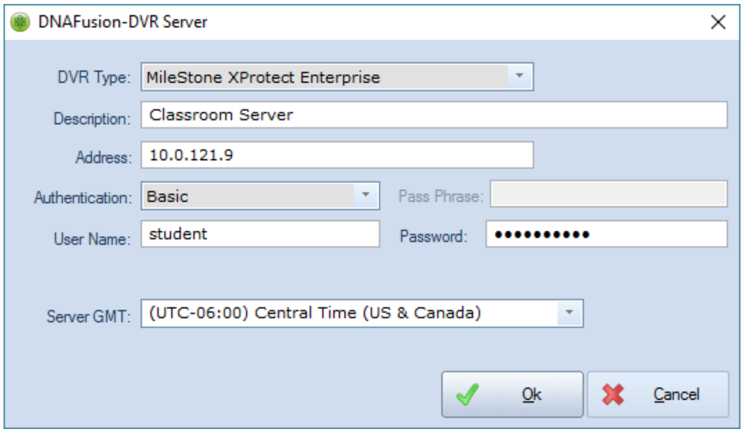
DVR Properties

DVR integration provides a seamless interface between DNA Fusion and the 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.

All DVRs are managed in the DVR Browser. For information on managing DVRs, see page 8-43.

There are numerous NVR/DVRs that are compatible with the DNA Fusion system. Options vary by NVR/DVR manufacturer.

DVR Server Properties



DNAFusion-DVR Server

DVR Type: MileStone XProtect Enterprise

Description: Classroom Server

Address: 10.0.121.9

Authentication: Basic

Pass Phrase:

User Name: student

Password: ••••••••••

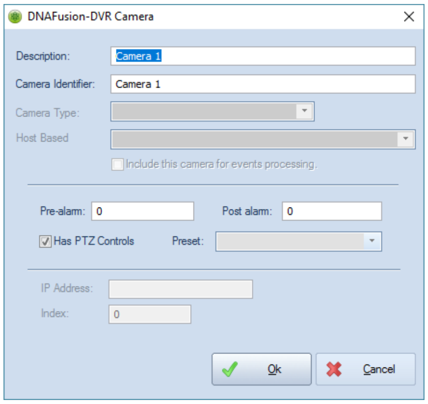
Server GMT: (UTC-06:00) Central Time (US & Canada)

- DVR Type - Identifies the type of DVR server.
- Description - User-defined description of the DVR server. Typically location-related.
- Address - The DVR server's IP address on the network.
- Authentication - Must match the authentication mode on the DVR server.
- Pass Phrase - Lensec cameras only.
- User Name - The User Name for the DVR server administrator.
- Password - The Password for the DVR server administrator.
- Bandwidth - ACTi and Verint cameras only.
- Server GMT - The GMT setting for the location of the DVR server.
- Port - Indicates the port number used to establish communication.
- Vigil Connect - Connection mode for Vigil SDK and 3xLogic SDK.

> *For 3xLogic SDK version 10.50.0400 uncheck the Use Vigil Connect box for direct server connection.*

DVR Camera Properties

After cameras have been associated with the DVR server, the Camera Properties will be available by expanding the DVR server and opening the individual camera.



DNAFusion-DVR Camera

Description: Camera 1

Camera Identifier: Camera 1

Camera Type:

Host Based

□ Include this camera for events processing.

Pre-alarm: 0

Post alarm: 0

☑ Has PTZ Controls

Preset:

IP Address:

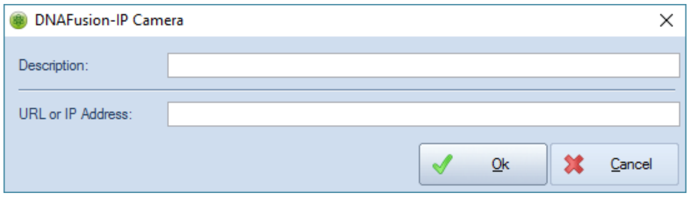
Index: 0

- Description - User-defined description of the DVR camera. Typically location-related.
- Camera Identifier - Description pulled from the DVR server. Do not change this field.
- Camera Type - Drop-down to select the camera model.
- Host Based - Select if using a Milestone or Avigilon camera.
- Include this camera for events processing - If checked, uses the camera events to execute a Host Based Macro.
- Pre-alarm - Sets the time to view in advance of the event or alarm.
- Post alarm - Sets the time to continue view after the event or alarm.
- Has PTZ Control - Select to indicate that the camera has pan, tilt, and zoom capability.

- Preset - If presets have been configured in the video management system, select a preset from the drop-down.
- IP Address - The IP address where the camera’s DVR server is located. (Bosch only)
- Index - The camera address. (Bosch only)

IP Camera Properties

Legacy cameras that are not connected to DVR or NVR systems can be added to DNA Fusion to allow operators to monitor the camera from the application.



- Description - Enter a name for the camera.
- URL or IP Address - The URL or IP address where the camera is located.

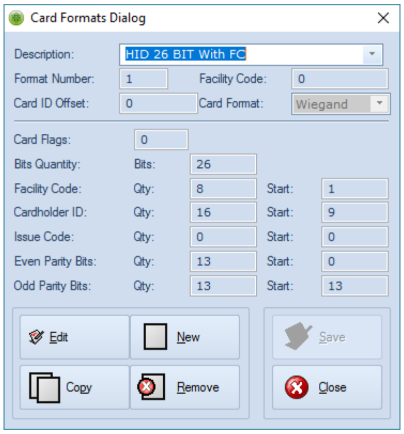
Card Formats

The Card Formats Dialog defines a format for the controller to take the raw data and format it into fields for access request processing. Multiple formats allow badges with different facility codes and/or data lengths to be used.

Creating a New Card Format

1. **Right-click** on the Controller in the Hardware Browser and **select** Card Formats from the context menu.

   The Card Formats Dialog opens.



Card Formats Dialog

Description: HID 26 BIT With FC
Format Number: 1
Facility Code: 0
Card ID Offset: 0
Card Format: Wiegand

Card Flags: 0

Bits Quantity:	Bits:	26		
Facility Code:	Qty:	8	Start:	1
Cardholder ID:	Qty:	16	Start:	9
Issue Code:	Qty:	0	Start:	0
Even Parity Bits:	Qty:	13	Start:	0
Odd Parity Bits:	Qty:	13	Start:	13

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

   The new format is added to the Description drop-down.

If the Issue Code *field will be used, enter the* Issue Code Bit Quantity *and specify the* Start Bit *in the* Issue Code Qty *and* Start *fields.*

Copying a Card Format

1. **Right-click** on the Controller in the Hardware Browser and **select** Card Formats from the context menu.

   The Card Formats Dialog opens.

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

   The new format is added to the Description drop-down.

Editing a Card Format

1. **Right-click** on the Controller in the Hardware Browser and **select** Card Formats from the context menu.

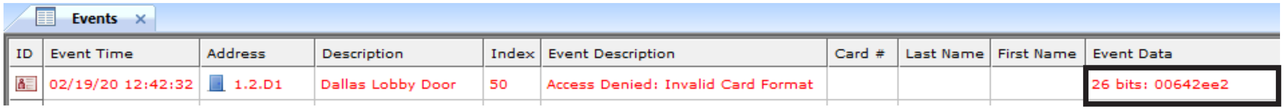
   The Card Formats Dialog opens.

2. **Click** the Edit button.
3. **Edit** the desired values in the Card Format fields.
4. **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 Events Grid and look at the Event Data for the Access Denied: Invalid Card Format event to determine the bit format.



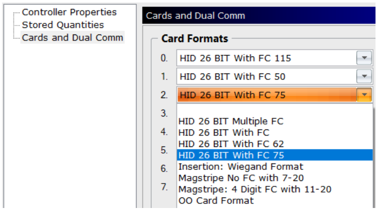
Events

ID	Event Time	Address	Description	Index	Event Description	Card #	Last Name	First Name	Event Data
	02/19/20 12:42:32	1.2.D1	Dallas Lobby Door	50	Access Denied: Invalid Card Format				26 bits: 00642ee2

3. **Assign** the generic card format that contains the same bit structure as the card to the SSP.

   See Assigning a Card Formation to the SSP below.

   In the example, the HID 26 BIT With FC would be selected.



Controller Properties
Stored Quantities
Cards and Dual Comm

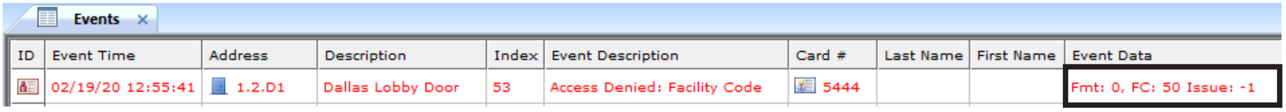
Cards and Dual Comm

Card Formats

0. HID 26 BIT With FC 115
1. HID 26 BIT With FC 50
2. HID 26 BIT With FC 75
3.
4.
5.
6.
7.

HID 26 BIT Multiple FC
HID 26 BIT With FC
HID 26 BIT With FC 62
HID 26 BIT With FC 75
Insertion: Wiegand Format
Magstripe No FC with 7-20
Magstripe: 4 Digit FC with 11-20
OO Card Format

4. **Present** the same card to the reader a second time.
5. **Check** the Event Data for the Access Denied: Facility Code event to determine the Facility Code (FC).



Events

ID	Event Time	Address	Description	Index	Event Description	Card #	Last Name	First Name	Event Data
	02/19/20 12:55:41	1.2.D1	Dallas Lobby Door	53	Access Denied: Facility Code	5444			Fmt: 0, FC: 50 Issue: -1

6. **Create** the card format by following the instructions on page 8-83 for Copying a Card Format.
7. **Assign** the newly created card format to the SSP.

   See Assigning a Card Formation to the SSP below.

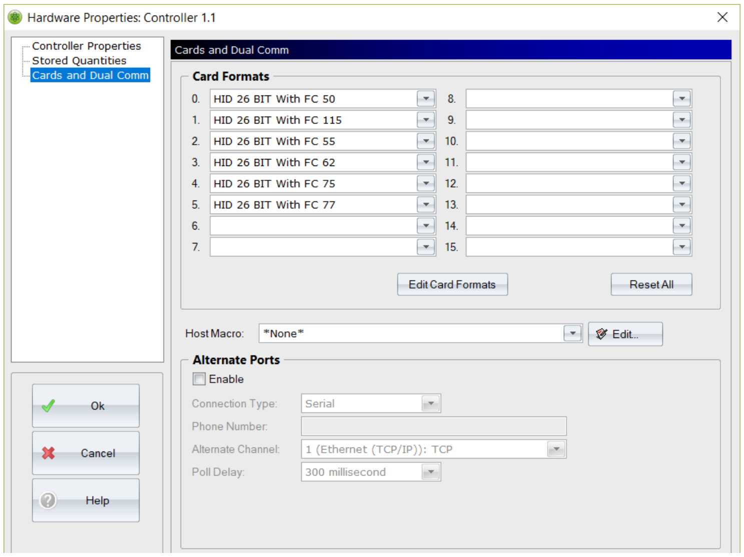
   Be sure to overwrite or delete the generic card format added in step 3.
8. **Download** the changes to the SSP.

Assigning a Card Format to the SSP

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

1. **Right-click** on the SSP in the Hardware Browser.
2. **Select** Properties from the menu.

   The Controller Properties dialog opens.
3. **Select** the Cards and Dual Comm tab from the dialog menu.



Hardware Properties: Controller 1.1

Controller Properties
Stored Quantities
Cards and Dual Comm

Cards and Dual Comm

Card Formats

0.	HID 26 BIT With FC 50	8.	
1.	HID 26 BIT With FC 115	9.	
2.	HID 26 BIT With FC 55	10.	
3.	HID 26 BIT With FC 62	11.	
4.	HID 26 BIT With FC 75	12.	
5.	HID 26 BIT With FC 77	13.	
6.		14.	
7.		15.	

Host Macro: *None*

Alternate Ports

☐ Enable

Connection Type: Serial

Phone Number:

Alternate Channel: 1 (Ethernet (TCP/IP)): TCP

Poll Delay: 300 millisecond

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

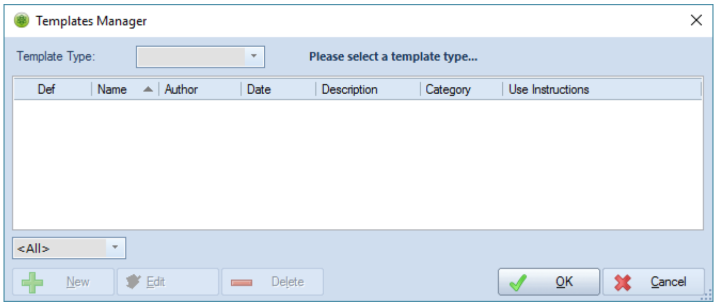
Templates

The Templates feature is used to create user-defined presets for various hardware objects, including doors, elevators, readers, and input/output points. Templates save specific hardware settings and store them for future use. If desired, users can also set a default template for each hardware type.

Creating a New Template

1. **Select** Hardware / Templates from the Main Menu.

   The Templates Manager dialog opens.



Please select a template type...

2. **Select** a Template Type from the drop-down.

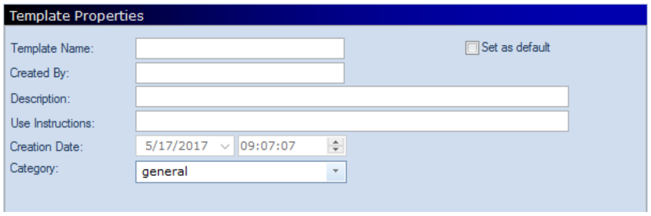
   Any existing templates for the selected hardware type will populate in the grid.

3. **Click** the New button.

   OR

   Right-click in the Templates Manager grid and **select** Add Template.

   The Template Properties dialog will appear for the selected hardware type.



Creation Date: 5/17/2017 09:07:07

Category: general

4. **Enter** a Template Name. (Required field)
5. If desired, **select** the Set as Default checkbox to set the template as the default option.
6. If desired, **enter** the author in the Created By field.
7. **Enter** a Description for the template.
8. If desired, **type** a message in the Use Instructions field.
9. **Select** an existing Category for the template using the drop-down list.

   Or

   Place the cursor in the field and **enter** a new Category.

10. **Select** a Properties option from the dialog menu.

    The corresponding dialog appears.

11. **Check** the Template checkbox next to the desired field(s).

    The checked field(s) will become active.

12. **Configure** the hardware settings. See pages 8-49 through 8-82 for detailed information about hardware properties.
13. When finished, **click** OK to save the template.

    The template is added to the Templates Manager.

14. **Click** OK in the Templates Manager to save the changes.

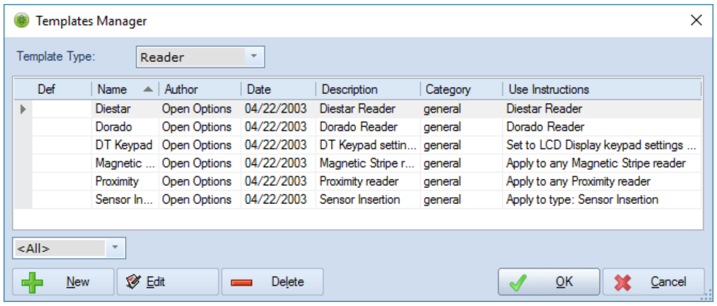
Editing a Template

1. **Select** Hardware / Templates from the Main Menu.

   The Templates Manager dialog opens.

2. **Select** a Template Type from the drop-down.

   A list of existing templates for the selected hardware type will appear.

   Template Type: Reader

Def	Name	Author	Date	Description	Category	Use Instructions
	Diestar	Open Options	04/22/2003	Diestar Reader	general	Diestar Reader
	Dorado	Open Options	04/22/2003	Dorado Reader	general	Dorado Reader
	DT Keypad	Open Options	04/22/2003	DT Keypad settin...	general	Set to LCD Display keypad settings ...
	Magnetic ...	Open Options	04/22/2003	Magnetic Stripe r...	general	Apply to any Magnetic Stripe reader
	Proximity	Open Options	04/22/2003	Proximity reader	general	Apply to any Proximity reader
	Sensor In...	Open Options	04/22/2003	Sensor Insertion	general	Apply to type: Sensor Insertion

   <All>

3. **Select** a Template and **click** Edit.

   Or

   Right-click on a Template and **select** Edit Template.

   The Template Properties dialog appears.

4. **Select** a Properties option from the dialog menu and **edit** the desired field(s).
5. **Click** OK to save the changes.
6. **Click** OK in the Templates Manager to save the changes and close the dialog.

Deleting a Template

1. **Select** Hardware / Templates from the Main Menu.

   The Templates Manager dialog opens.

2. **Select** a Template Type from the drop-down.

   A list of existing templates for the selected hardware type will appear.

3. **Select** a Template and **click** Delete.

   Or

   Right-click on a Template and **select** Delete Template.

   The selected Template is removed from the Templates Manager.

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

Applying a Template

1. From the Hardware Browser, **right-click** on one of the following hardware objects:
   - Door/Elevator
   - Reader
   - Input/Output Point
2. **Select** Templates from the context menu.

   The Templates Manager dialog opens for the selected hardware type.

3. **Select** a Template and click Apply to X.*

   The Template is applied to the selected hardware object.

4. **Click** OK to close the dialog.

* Where X represents Door, Reader, Input Point, or Output Point.

Situation Manager 9

In This Chapter	
√	Setting the Situation Level
√	Configuring the Situation Manager
√	Configuring Hardware
√	Authorizing Operators

The Situation Manager allows a system administrator to change the settings of an entire access control system in a single step. The administrator can choose between five security configurations, allowing them to reconfigure building security at the click of a button.

System parameters and business rules can be changed with one click using the Situation Manager. The following objects can be affected by changes to the Situation Manager settings:

- Doors & Elevators (ACMs)
- Inputs & Outputs
- Secured Areas
- Access Areas
- Time Schedules
- Card Access

Setting the Situation Level

Five situation levels are selectable, each of which can be named, color-coded, and customized to designate a different level of security. Changing the situation level can determine the cardholders who are allowed to gain access, the areas they may access, and the operation of access control equipment around the building.

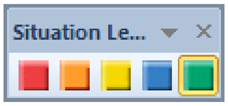
To set the Situation Level:

1. **Right-click** in the gray area next to the Standard Toolbar and **select** Situation Level Manager.

   The Situation Manager Toolbar opens. The operator can move the toolbar anywhere on the DNA desktop. See page 2-5 for more information on Secondary Toolbars.

2. **Select** one of the color-coded icons to change the Situation Level.

   All system settings affected by the Situation Manager will be updated to match the selected Situation Level configuration.



This Page Intentionally Left Blank

Configuring the Situation Manager

DNA administrators can customize each security configuration based on a variety of options. For example, in a "Warning" environment, all cardholders could access a particular door using their cards only, while in an "Alert" environment, only select cardholders could access a particular door using their card and PIN number.

Five color-coded threat levels are available from the Situation Manager dialog; each threat level can be renamed and customized to provide a different level of security.

To configure the Situation Manager:

1. **Select** DNA / Administrative / Properties from the Main Menu.

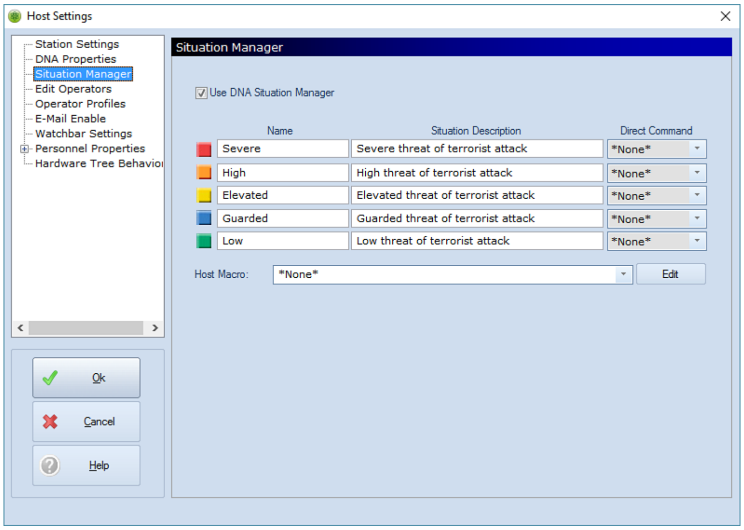
   OR

   Select the DNA Properties button from the Standard Toolbar.

   The Host Settings dialog opens.

2. **Select** Situation Manager from the Host Settings dialog menu.

   The Situation Manager dialog appears.



☑ Use DNA Situation Manager

	Name	Situation Description	Direct Command
🟥	Severe	Severe threat of terrorist attack	*None*
🟧	High	High threat of terrorist attack	*None*
🟨	Elevated	Elevated threat of terrorist attack	*None*
🟦	Guarded	Guarded threat of terrorist attack	*None*
🟩	Low	Low threat of terrorist attack	*None*

Host Macro: *None*

3. **Select** the Use DNA Situation Manager checkbox to enable the feature.
4. **Enter** a Name and Description for each corresponding color block.
5. If desired, **select** a Direct Command to associate with the situation level.

   The Direct Command will be fired after all the other commands have been executed.

   See page 8-27 for more information on direct commands.

6. If desired, **select** a Host Based Macro to associate with the Situation Manager.

   A Host Based Macro can be set to send emails or affect a hardware object when situation levels are changed. Only one Host Based Macro can be assigned to the Situation Manager, and it will be executed before any other commands are fired. See page 10-13 for more information on Host Based Macros.

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

NOTES:

Enabling Hardware Objects

Doors & Elevators

Doors and elevators can be configured to change reader modes based on the Situation Manager settings. See page 8-57 for Door Properties and page 8-65 for Elevator Properties.

1. **Right-click** on the Door or Elevator in the Hardware Browser and **select** Properties.

   The Door/Elevator Properties dialog opens.

2. **Click** the Situations... button.

   The Situation Level Manager Settings dialog appears.

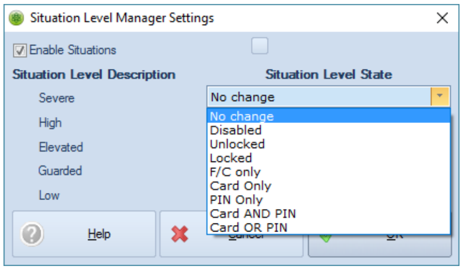
3. **Check** the Enable Situations checkbox.

4. **Select** the Situation Level State for each Situation Level.

   - Disabled - Disables the selected object.
   - Unlocked - Unlocks the selected object.
   - Locked - Locks the selected object.
   - F/C Only - Matches the facility code to approve entry.
   - Card Only - Requires a card with the correct format be presented.
   - PIN Only - Requires a PIN code be entered to gain access.
   - Card AND PIN - Requires both a card and PIN number to gain access.
   - Card OR PIN - Requires either a card or a PIN code be entered to gain access.

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

6. **Click** OK to close the Properties dialog.



Situation Level Manager Settings

☑ Enable Situations

Situation Level Description	Situation Level State
Severe	No change
High	
Elevated	
Guarded	
Low	

No change
Disabled
Unlocked
Locked
F/C only
Card Only
PIN Only
Card AND PIN
Card OR PIN

Input Points

1. **Right-click** on the Input object in the Hardware Browser and **select** Properties.

   The Input Properties dialog will open. See page 8-73 for Input Properties.

2. **Click** the Situations... button.

   The Situation Level Manager Settings dialog opens.

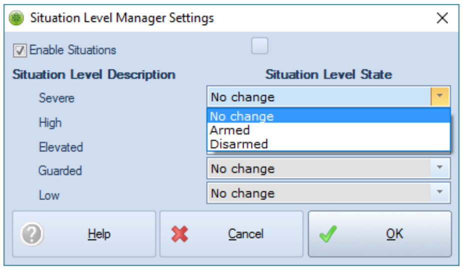
3. **Check** the Enable Situations checkbox.

4. **Select** the Situation Level State for each Situation Level.

   - Armed - Arms the point.
   - Disarmed - Disarms the point.

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

6. **Click** OK to close the Properties dialog.



Situation Level Manager Settings

☑ Enable Situations

Situation Level Description	Situation Level State
Severe	No change
High	
Elevated	
Guarded	No change
Low	No change

No change
Armed
Disarmed

Output Points

1. **Right-click** on the Output object in the Hardware Browser and **select** Properties.

   The Output Properties dialog will open. See page 8-77 for Output Properties.

2. **Click** the Situations... button.

   The Situation Level Manager Settings dialog opens.

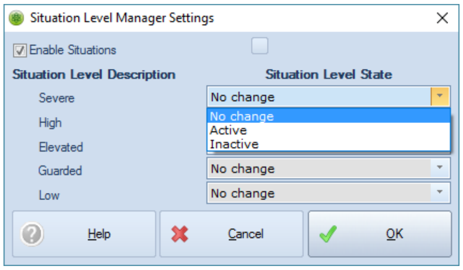
3. **Check** the Enable Situations checkbox.

4. **Select** the Situation Level State for each Situation Level.

   - Active - Activates the point.
   - Inactive - Deactivates the point.

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

6. **Click** OK to close the Properties dialog.



Situation Level Manager Settings

☑ Enable Situations

Situation Level Description	Situation Level State
Severe	No change
High	
Elevated	
Guarded	No change
Low	No change

No change
Active
Inactive

Secured Areas

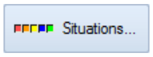
1. **Right-click** on the Secured Area in the Hardware Browser and **select** Properties.

   The Secured Areas dialog will open. See page 12-3 for Secured Areas Properties.

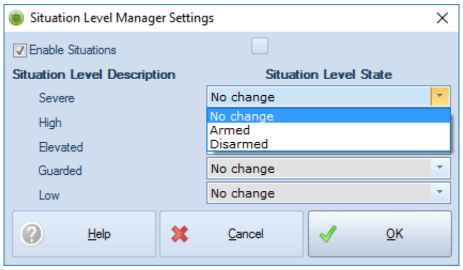
2. **Select** Area Points from the Secured Areas dialog menu.

   The Area Points dialog appears.

3. **Click** the Situations... button.

   The Situation Level Manager Settings dialog opens.



Situation Level Manager Settings

☑ Enable Situations □

Situation Level Description	Situation Level State
Severe	No change
High	
Elevated	
Guarded	No change
Low	No change

No change
Armed
Disarmed

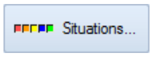
4. **Check** the Enable Situations checkbox.
5. **Select** the Situation Level Setting for each Situation Level.
   - Armed - Arms the Secured Area.
   - Disarmed - Disarms the Secured Area.
6. **Click** OK to save the settings.
7. **Click** OK to close the Properties dialog.

Access Areas

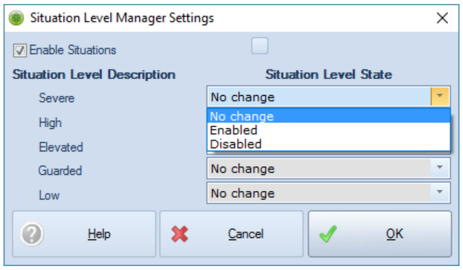
1. **Right-click** on the Access Area in the Hardware Browser and **select** Properties.

   The Access Areas Dialog will open. See page 11-1 for Access Areas Properties.

2. **Click** the Situations... button.

   The Situation Level Manager Settings dialog opens.



Situation Level Manager Settings

☑ Enable Situations □

Situation Level Description	Situation Level State
Severe	No change
High	
Elevated	
Guarded	No change
Low	No change

No change
Enabled
Disabled

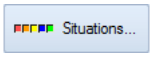
3. **Check** the Enable Situations checkbox.
4. **Select** the Situation Level Setting for each Situation Level.
   - Enabled - Enables the Access Area.
   - Disabled - Disables the Access Area.
5. **Click** OK to save the settings.
6. **Click** OK to close the Properties dialog.

Configuring Time Schedules

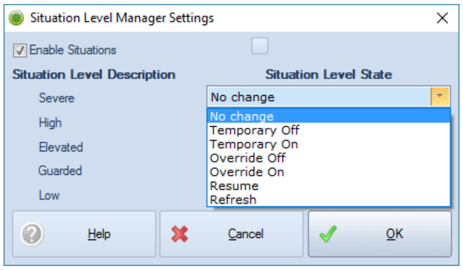
Time schedules can be customized to respond to changes in the situation level. Keep in mind that when a time schedule is controlled, it can affect cardholder access as well as door schedules. See page 5-1 for more information.

1. **Right-click** on the Time Schedule in the Time Schedules Browser and **select** Properties.

   The Time Intervals dialog opens.

2. **Click** the Situations... button. 

   The Situation Level Manager Settings dialog opens.

   Situation Level Manager Settings

   ☑ Enable Situations

Situation Level Description	Situation Level State
Severe	No change
High	
Elevated	
Guarded	
Low	

> *Note: The* Situations... *button will not be available for the default* Always *time schedule.*

3. **Check** the Enable Situations checkbox.

4. **Select** the Situation Level State for each Situation Level.

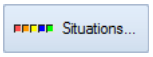
   - Temporary Off – Temporarily sets the time schedule mode to OFF. The next ON interval edge will return the schedule to its normal time-based state. Use the Resume command to restore the time schedule to the time-based control prior to the next interval edge.
   - Temporary On - Temporarily sets the time schedule mode to ON. The next OFF interval edge will return the schedule to its normal time-based state. Use the Resume command to restore the time schedule to the time-based control prior to the next interval edge.
   - Override Off - Sets the time schedule mode to OFF and overrides the time-based control. Overrides the Scan Mode and time intervals have no effect when this command is used. Use the Resume command to restore the time schedule to the time based control.
   - Override On - Sets the time schedule mode to ON and overrides the time-based control. Overrides the Scan Mode and time intervals have no effect when this command is used. Use the Resume command to restore the time schedule to the time-based control.
   - Resume – Puts the time schedule into the state as defined by time-based rules. Use this command to remove the Temporary On/Off and Override On/Off commands. The system will return to its “normal” state.
   - Refresh – Logs the current time schedule modes into the transaction log. Use this command to test triggers that are activated based on time schedule events.

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

6. **Click** OK to close the Time Intervals dialog.

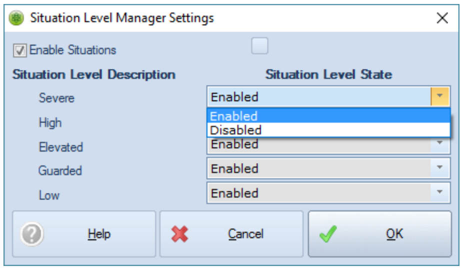
Establishing Card Access

A cardholder’s card can be deactivated when certain conditions are present and then reactivated at the appropriate time. See page 7-7 for information on opening a cardholder’s record.

1. **Open** the Cardholder’s Record for the selected cardholder.
2. **Select** the Card Tab.
3. **Click** the Situations... button. 

   Situations...

   The Situation Level Manager Settings dialog opens.



Situation Level Manager Settings

☑ Enable Situations

Situation Level Description	Situation Level State
Severe	Enabled Enabled Disabled
High	Enabled
Elevated	Enabled
Guarded	Enabled
Low	Enabled

4. **Check** the Enable Situations checkbox.
5. **Select** the Situation Level State for each Situation Level.
   - Enabled - Activates the cardholder’s card and allows access to the facility.
   - Disabled - Deactivates the cardholder’s card and restricts access to the facility.
6. **Click** OK to save the settings.
7. **Close** the Cardholder’s Record.

Configuring Operator Privileges

It is important to configure operator privileges so that certain operator profiles have permission to change the situation level in the Situation Manager.

1. **Select** DNA / Administrative / Operator Maintenance / Operator Privileges from the Main Menu.

   The Operator Privileges Editor dialog appears.

   Or

   Click the DNA Properties button on the Standard Toolbar.

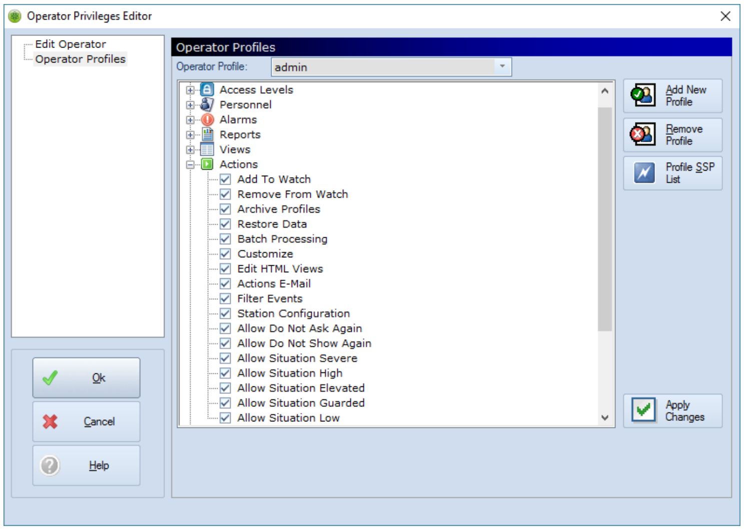
   The Host Settings dialog appears.

2. **Select** Operator Profiles from the dialog menu.

   The Operator Profiles dialog opens.

3. **Select** the desired Operator Profile from the drop-down menu.

4. **Expand** the Actions category and **check** the Allow Situation options that the operator profile will have permission to change. See pages 4-13 and 4-14 for more information.



Operator Privileges Editor

- Edit Operator
- Operator Profiles

Operator Profiles

Operator Profile: admin

- Access Levels
- Personnel
- Alarms
- Reports
- Views
- Actions
  - ☑ Add To Watch
  - ☑ Remove From Watch
  - ☑ Archive Profiles
  - ☑ Restore Data
  - ☑ Batch Processing
  - ☑ Customize
  - ☑ Edit HTML Views
  - ☑ Actions E-Mail
  - ☑ Filter Events
  - ☑ Station Configuration
  - ☑ Allow Do Not Ask Again
  - ☑ Allow Do Not Show Again
  - ☑ Allow Situation Severe
  - ☑ Allow Situation High
  - ☑ Allow Situation Elevated
  - ☑ Allow Situation Guarded
  - ☑ Allow Situation Low

5. **Click** Apply Changes to save the configuration.

   If an operator is logged in when a profile is changed, the changes will take effect the next time the operator logs in to DNA Fusion.

> ❗ *The* Apply Changes *button must be selected in order for changes to be saved. If not, changes will be lost when selecting another operator or closing the dialog box.*

This Page Intentionally Left Blank

Triggers & Macros 10

In This Chapter

√ Creating and Removing Macros
√ Managing Macro Commands
√ Adding and Removing Triggers
√ Using Trigger Codes and Trigger Variables
√ Creating Host Based Macros
√ Adding Macros to a Door

Triggers and Macros add dimension and flexibility to the system by allowing the operator to set up automated actions based on specific system events.

Creating triggers and macros is relatively simple once you have determined what action(s) to execute within the system. A trigger-and-macro combination is similar to an *if-then* statement, i.e. *if* a specific event occurs in the system (trigger), *then* a defined action will occur (macro).

Triggers provide a means for event-based control; macros are a canned list of commands that an operator might perform. The trigger defines the event for which a chain of actions is desired, and the macro executes the list of actions. Together, triggers and macros provide event-based control and provide better customization in DNA Fusion.

In this chapter, you will learn how to configure macros and how to define event triggers that activate those macros based on user-defined criteria.

Macros

In DNA Fusion, the operator is not required to create triggers and macros in a particular order. However, because macros are referenced via drop-down list in the triggers module, it is recommended that macros be configured first to complete the trigger and prevent additional steps.

A macro is a defined set of commands that performs various actions within the system. The number of commands is limited by the controller's available memory.

Examples of a macro:

- A command to activate or deactivate an output relay on a subcontroller.
- A command to unlock a door based on a given time schedule.
- A command to arm or disarm a monitor point.

Creating a Macro

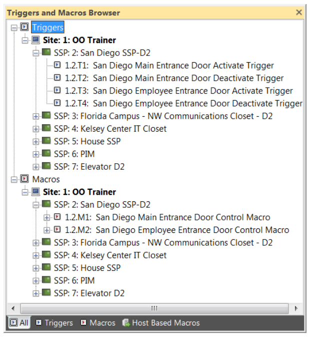
1. **Click** the Triggers & Macros button on the Standard Toolbar.

   The Triggers and Macros Browser opens.

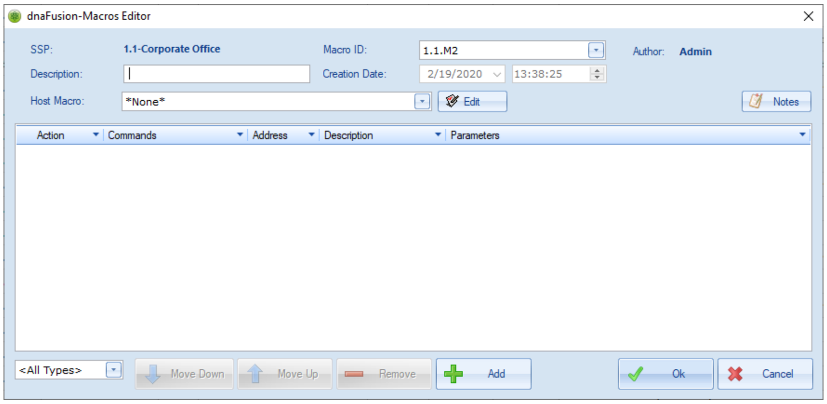
2. **Expand** the Macros object, **right-click** on the appropriate Controller object in the browser, and **select** Add Macro from the context menu.

> ***!*** *Macros are created and downloaded to the specific controller that contains the objects associated with the macro. It is important to select the appropriate controller when adding a macro to the system.*

The Macros Editor appears.


Triggers and Macros Browser
Triggers
Site: 1: OO Trainer
SSP: 2: San Diego SSP-D2
1.2.T1: San Diego Main Entrance Door Activate Trigger
1.2.T2: San Diego Main Entrance Door Deactivate Trigger
1.2.T3: San Diego Employee Entrance Door Activate Trigger
1.2.T4: San Diego Employee Entrance Door Deactivate Trigger
SSP: 3: Florida Campus - NW Communications Closet - D2
SSP: 4: Kelsey Center IT Closet
SSP: 5: House SSP
SSP: 6: PIM
SSP: 7: Elevator D2
Macros
Site: 1: OO Trainer
SSP: 2: San Diego SSP-D2
1.2.M1: San Diego Main Entrance Door Control Macro
1.2.M2: San Diego Employee Entrance Door Control Macro
SSP: 3: Florida Campus - NW Communications Closet - D2
SSP: 4: Kelsey Center IT Closet
SSP: 5: House SSP
SSP: 6: PIM
SSP: 7: Elevator D2
All
Triggers
Macros
Host Based Macros

3. **Enter** a Description for the macro.



dnaFusion-Macros Editor

SSP: 1.1-Corporate Office

Macro ID: 1.1.M2

Author: Admin

Description:

Creation Date: 2/19/2020 13:38:25

Host Macro: *None*

Action	Commands	Address	Description	Parameters

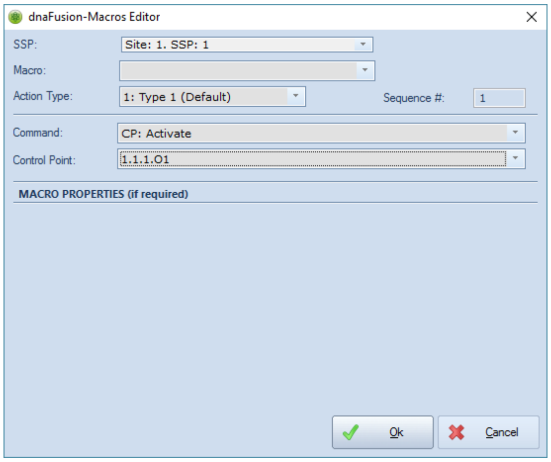
4. If desired, **select** a Host Based Macro from the drop-down list or **click** the Edit button Edit to create a new host based macro.

   If Edit is selected, refer to page 10-13 for more information.

5. **Click** the Add button to associate commands with the macro.

   Commands are executed in the order they are added or by the Action Type associated with the command. An infinite number of commands can be associated with the macro.

   A second Macros Editor appears.



dnaFusion-Macros Editor

SSP: Site: 1. SSP: 1

Macro:

Action Type: 1: Type 1 (Default)

Sequence #: 1

Command: CP: Activate

Control Point: 1.1.1.O1

MACRO PROPERTIES (if required)

6. **Select** an Action Type from the drop-down list.

   Because more than one macro command can be added to a macro, the action type specifies which macro commands will fire based on the action type referenced in the trigger. The Action Type field in the Macro relates to the Command field in the Trigger. See page 10-7 for more information.

   There are four Action Types (Type 1-4), but the system can only execute one action type per trigger. For instance, both the Unlock and Card Only door modes can be placed under a single macro, but each mode must be designated as a separate Action Type. Then, two triggers would link to the same macro but reference the appropriate Action Type.

> Action Types *are conditions and/or states attributed to a given macro command. If unfamiliar with this functionality, use* Type 1*, which is the default. Assigning action types to a macro command is an advanced feature of DNA.*

7. **Select** the desired Command from the drop-down menu.

   The remaining dialog fields will change based on the selection. Use the table on page 10-5 to configure the additional fields.

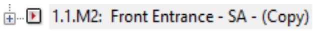
8. **Click** OK to save the macro.
   The macro appears in the Triggers and Macros Browser.

9. **Create** a Trigger to execute the desired Macro Commands. See page 10-7 for more information.

Copying and Removing a Macro

1. **Right-click** on the Macro object in the Triggers and Macros Browser and **select** Copy Macro or Remove Macro from the context menu.

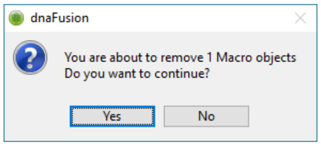
2. If Copy Macro is **selected**, the Macro is duplicated in the Triggers and Macros Browser.



1.1.M2: Front Entrance - SA - (Copy)

   The word Copy will appear in parentheses at the end of the description.

3. If Remove Macro is **selected**, a confirmation dialog will appear; **click** Yes to delete the Macro.



dnaFusion

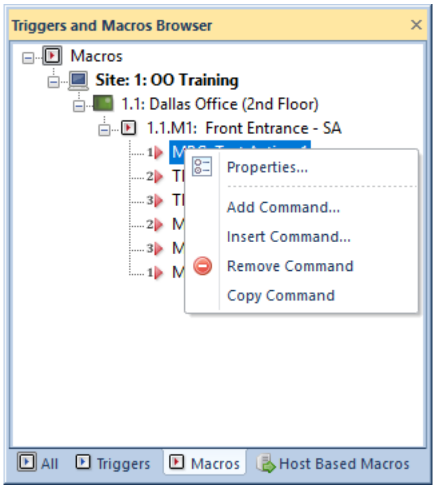
You are about to remove 1 Macro objects
Do you want to continue?

   The Macro is removed from the Triggers and Macros Browser.

Managing Macro Commands

Macro Commands can be added, inserted, removed, and/or copied using right-click options in the Triggers and Macros Browser.

Adding a Macro Command



1. With the Triggers and Macros Browser open, **expand** the Macros objects and **right-click** on the desired Macro Command.
2. **Select** Add Command from the context menu.

   The Macros Editor opens.
3. **Select** an Action Type from the drop-down list.

   See page 10-2 for more information.
4. **Select** the desired Command from the drop-down list.

   Depending on the selection, the field(s) below will change to allow for configuration of the command. Use the table on page 10-5 to complete the remaining fields.
5. **Click** OK to save the configuration.

   The command is added to the Triggers and Macros Browser below the macro's existing commands.
6. **Right-click** on the Macro and **select** Download from the context menu.

   The selected macro is downloaded to the controller's memory.

> *The* Add Command *option is also available by* **right-clicking** *on the desired* Macro *object. See page 10-4 for more right-click* Macro *options.*

Inserting a Macro Command

The Insert Command option offers a key distinction from the Add Command option with regard to placement. Whereas an added command is automatically placed below the macro's existing commands, an inserted command is placed directly above an existing command. This is important because macro commands are fired in the order they are listed in the Triggers and Macros Browser.

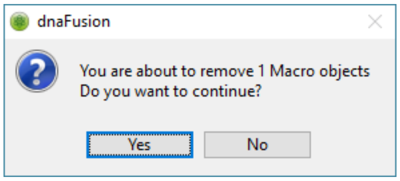
1. **Right-click** on the appropriate Macro Command and **select** Insert Command.
2. **Configure** the Macros Editor dialog as indicated in the Adding a Macro Command section.
3. **Click** OK to save the configuration.

   The new command is inserted directly above the selected command in the Triggers and Macros Browser.
4. **Right-click** on the Macro and **select** Download from the context menu.

Removing a Macro Command

1. **Right-click** on the desired Macro Command and **select** Remove Command.

   A confirmation dialog will appear.

   You are about to remove 1 Macro objects
   Do you want to continue?
2. **Select** Yes to confirm.

   The command is removed from the Triggers and Macros Browser.

Copying a Macro Command

1. **Right-click** on the desired Macro Command and **select** Copy Command.

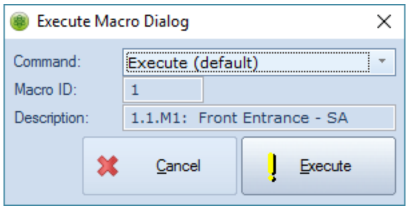
   The selected command is duplicated; the copy appears below the macro's existing command(s).

Controlling Macros

Operators can execute a macro command directly from the Triggers and Macros Browser or choose to resume or abort a delayed command. Direct controls are performed using the Execute Macro Dialog.

1. **Right-click** on the desired Macro object in the Triggers and Macros Browser and **select** Direct Control / Execute MACRO.

   The Execute Macro Dialog appears.



Command: Execute (default)
Macro ID: 1
Description: 1.1.M1: Front Entrance - SA

2. **Select** a Command from the drop-down list:
   - Abort a delayed macro - If the Command field in the Macros Editor is set to TM: Delay Command, selecting this option will cause the delayed command to stop firing. See page 10-5 for information.
   - Execute (default) - Fires the selected macro's Type 1 command(s).
   - Resume a delayed macro - If the Command field in the Macros Editor is set to TM: Delay Command, selecting this option will cause the delayed command to resume action and continue to the next macro command. Note: This option only applies to default Type 1 commands.
   - Execute (Type 2-4 commands) - Fires the selected macro's Type 2, 3, or 4 command(s).
   - Resume (Type 2-4 commands) - If the Command field in the Macros Editor is set to TM: Delay Command, selecting one of these options will cause the delayed Type 2, 3, or 4 command to resume action.
3. **Click** Execute to execute the direct command.

   The command is logged in the Events Grid.

> *Users can execute macro commands by action type using shortcut options.* **Right-click** *on the* Macro *object and* **select** Direct Control / Execute Type (1-4)*.*

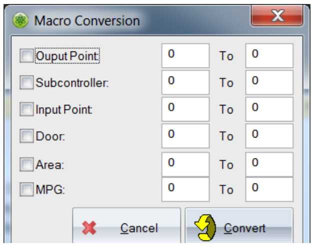
Macro Conversion

Macro commands can be moved to a separate macro location without reconfiguring the macro commands by using the Macro Conversion feature.

1. **Right-click** on the Macro object in the Triggers and Macros Browser and **select** Macro Conversion.

   The Macro Conversion dialog appears.
2. **Select** the macro's associated hardware object(s).
3. **Enter** a numeric value based on the macro's current hardware location and a numeric value based on the desired hardware destination.

   Example: To convert a macro's commands from MPG 1 to MPG 2, enter 1 and 2 as the numeric values.
4. **Click** the Convert button; the commands are moved to the chosen hardware location.



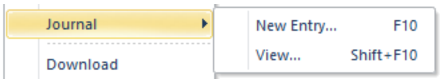
□ Ouput Point	0	To	0
□ Subcontroller:	0	To	0
□ Input Point	0	To	0
□ Door:	0	To	0
□ Area:	0	To	0
□ MPG:	0	To	0

Journal

The Journal feature is used to record a text entry and view entries based on operator restrictions.

1. From the Triggers and Macros Browser, **right-click** on the Macro object and **select** Journal / New Entry or View.

   See page 8-19 for information on creating and viewing a journal entry.



Download

Selecting Download at the macro level is considered an individual download, and only information about the specific macro will be sent to the controller. The Download Manager dialog is not displayed.

1. From the Triggers and Macros Browser, **right-click** on the Macro object and **select** Download.

   The selected macro is downloaded to the controller's memory.

Where Used

Opens the Where Used Report dialog, which displays the macro's associated relationships, e.g. triggers.

Command	Object	Additional Fields
Access Area	**Select** Area	If Set Occupancy, **enter** Occupancy
Cards: Issue Free Pass	**Select** Area	
Cards: Set Use Limit	**Select** All Cardholder Or **Specify** Cardholder	• If Cardholder, **enter** Card Number • **Select** Use Limit
CP (Control Point)	**Select** Control Point	• If Pulse, **enter** On Time • If Repeating Pulse, **enter** On Time, Off Time & Repeat
Door	**Select** Doors	
Door: Display Text on LCD Reader	**Select** Doors	• **Select** Text Type • **Select** Temp Duration • **Select** Tone • **Select** Tone Duration • **Select** Row • **Select** Column • **Enter** Text
Door: Reader LED Control	**Select** Doors	**Select** LED Index
Door: Simulated Card Read	**Select** the Door	• **Enter** the Card Format # • **Enter** the Facility Code • **Enter** the Card Number • If needed, **enter** Issue Code
Door: Temp Reader LED Command	**Select** the Door	• **Select** Color On • **Select** Color Off • **Select** Ticks On • **Select** Ticks Off • **Select** Repeat • **Select** Beeps
Elevator: Floor Pulse	**Select** Elevator	**Select** Floor
MP (Monitor Point)	**Select** Monitor Point	
MPG	**Select** MPG	• If Test Active, **select** Points Secure and Not Secure • If Text Armed, **select** Points Secure and Not Secure
Reader Mode	**Select** the Door	
Reader Override: Cancel	**Select** the Door	
Reader Override	**Select** the Door	• **Select** Indefinite, Minutes, Seconds, or Time of Day
SSP: Dial Out to HOST	**Enter** Dial	
SSP: Dial Out to HOST using Alternate Port	**Enter** Dial	
SSP: HEX Output to SIO Port	**Select** SIO	• **Select** BAUD Rate • **Select** Channel • **Enter** HEX DATA
Time: Time Schedule Control	**Select** Time Schedule	**Select** Command

Command	Object	Additional Fields
TM: Delay Command (Delay Interval 0.1 sec) * *A delay command will pause for the specified amount of time before it continues to the next macro command.	**Select** Delay	NOTE: This Delay Command requires the controller have firmware version 1.24.1 or later. A delay command will only accept an Abort or Resume trigger command; all others are ignored. See page 10-8.
TM: Delay Command (Delay Interval 1 sec)* *A delay command will pause for the specified amount of time before it continues to the next macro command.	**Select** Delay	A delay command will only accept an Abort or Resume trigger command; all others are ignored. See page 10-8.
TM: Macro Command	**Select** Macro	**Select** Command
TM: Set Trigger Variable	**Select** Trigger Variable	**Select** Variable Setting

Triggers

Triggers are events that occur in the access control system and cause other actions (macros) to take place. A trigger can be created to detect any number of specific transactions (events). Once the transaction is detected, the system evaluates the time schedule. If the time schedule is active, the trigger will proceed.

Adding a Trigger

Adding a trigger is similar to the process outlined on pages 10-1 and 10-2 for creating macros.

To add a trigger to the system:

1. **Click** the Triggers & Macros button on the Standard Toolbar.

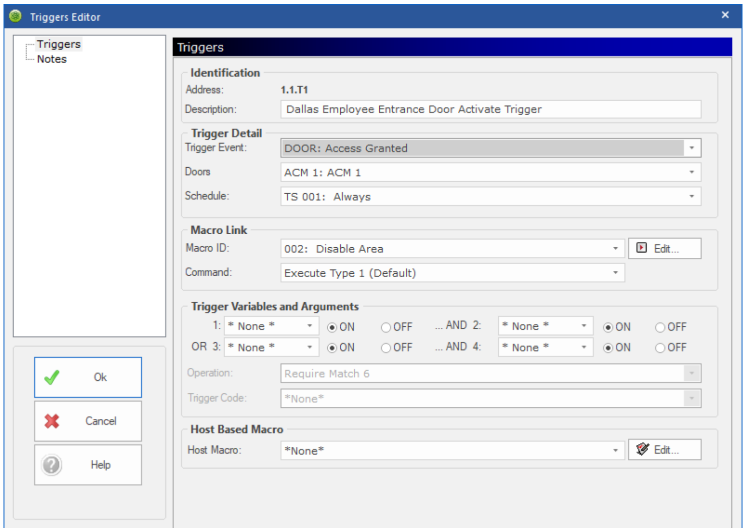
   Or

   Select View / Explorers / Triggers and Macros from the Main Menu.

   The Triggers and Macros Browser opens.

2. **Expand** the Triggers object, **right-click** on the appropriate Controller object in the browser, and **select** Add Trigger from the context menu.

   The Triggers Editor dialog appears.



Triggers Editor

Triggers
Notes

Triggers

Identification
Address: 1.1.T1
Description: Dallas Employee Entrance Door Activate Trigger

Trigger Detail
Trigger Event: DOOR: Access Granted
Doors: ACM 1: ACM 1
Schedule: TS 001: Always

Macro Link
Macro ID: 002: Disable Area
Command: Execute Type 1 (Default)

Trigger Variables and Arguments
1: * None * ● ON ○ OFF ... AND 2: * None * ● ON ○ OFF
OR 3: * None * ● ON ○ OFF ... AND 4: * None * ● ON ○ OFF
Operation: Require Match 6
Trigger Code: *None*

Host Based Macro
Host Macro: *None*

3. **Enter** a Description for the trigger.

4. **Select** a Trigger Event from the drop-down list.

   Depending on the Trigger Event selection, the remaining fields change to enable advanced configuration of the trigger, including Arguments, Variables and Trigger Codes. See pages 10-11 and 10-12 for more information.

5. **Select** an Object to assign to the Trigger Event.

   See table on page 10-9 for a complete list of trigger events and their associated hardware objects.

> ! *If* None *is selected for the* Doors *field, any* ACM *will execute the trigger.*

6. **Select** a Schedule from the drop-down list to associate with the Trigger Event.

   The trigger will only execute during the time intervals set by the time schedule.

7. **Select** a Macro ID to associate with the trigger.

8. **Select** the appropriate Command from the drop-down list.

   The Command field specifies which macro command Action Type to execute. In most cases, the default command, Execute Type 1 (Default), should be selected unless multiple commands are associated to the selected macro. See page 10-2 for more information.

- Execute Type 1 (Default) - Executes Type 1 (Default) macro commands
- Execute Type (2-4) - Executes Type 2, 3, or 4 macro commands
- Abort Execution - Aborts a delayed macro
- Resume Type (1-4) - Resumes a delayed Type 1, 2, 3, or 4 macro

9. If desired, **configure** the Trigger Variables and Arguments section.

   One or more of the following Arguments may appear depending on the Trigger Event selection:

   - Alarm Msg - Requires the specified alarm condition to be met before the trigger will execute.
   - Safe Msg - Requires the specified condition to be met before the trigger will execute.
   - Local Source - Select the event that will execute the trigger: Cabinet Tamper or Power Fault.
   - User Command - Enter the keypad command that will execute the trigger, e.g. *1234.

   Trigger Codes can also be configured to designate a specific card to execute the trigger. See page 10-11 for more information.

   Trigger Variables create a "toggle" effect on the trigger. See page 10-12 for more information.

10. If desired, **select** a Host Macro from the drop-down. See page 10-13 for more information.
11. **Click** OK to save the trigger.

    The trigger is added to the Triggers and Macros Browser.

12. **Right-click** on the Trigger and **select** Download from the context menu.

    The trigger is downloaded to the controller's memory.

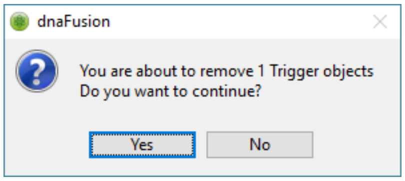
Removing a Trigger

1. **Right-click** on the desired Trigger in the Triggers and Macros Browser and **select** Remove Trigger.

   A confirmation dialog appears.

2. **Click** Yes to delete the Trigger.

   The trigger is removed from the Triggers and Macros Browser.


dnaFusion

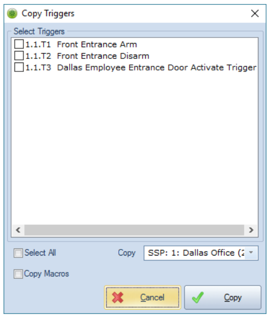
You are about to remove 1 Trigger objects
Do you want to continue?

Copying a Trigger

1. **Right-click** on the Controller in the Triggers and Macros Browser and select Copy...

   The Copy Triggers dialog appears.

2. **Select** the desired Trigger(s) individually or **check** the Select All option.
3. If desired, **check** Copy Macros to copy any macros associated with the trigger(s).
4. **Select** a Controller from the Copy drop-down to set the copy location.
5. **Click** the Copy button; the trigger(s) and macro(s) will be copied in the Triggers and Macros Browser.


Copy Triggers

Select Triggers

☐ 1.1.T1 Front Entrance Arm
☐ 1.1.T2 Front Entrance Disarm
☐ 1.1.T3 Dallas Employee Entrance Door Activate Trigger

☐ Select All

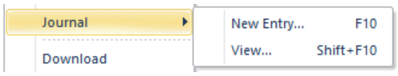
Copy: SSP: 1: Dallas Office (2

☐ Copy Macros

Journal

1. From the Triggers and Macros Browser, **right-click** on the Trigger object and **select** Journal / New Entry or View.

   See page 8-19 for information on creating and viewing a journal entry.



Download

1. From the Triggers and Macros Browser, **right-click** on the Trigger object and **select** Download.

   The selected trigger is downloaded to the controller's memory.

Trace History

Opens the Trace History Dialog, which displays the last transactions associated with the selected trigger.

Trigger Event	Object	Arguments & Variables (Optional)
Area: All Options	**Select** Area & Schedule	
BIOMETRIC: All Options	**Select** Address & Schedule	
CP (Control Point): All Options	**Select** Control Point & Schedule	
DOOR: Access Granted/ Denied	**Select** Door & Schedule	If desired, **select** an Operation and Trigger Code. See page 10-11 for information.
DOOR: ALARM (Forced, Held, or Both)	**Select** Door & Schedule	**Select** Alarm Msg: ● Forced Open only (held following...) ● Held Open only (only after normal...) ● Both (Forced then held open) ● Held Open, regardless of forced... ● Either (forced or held open, only one...) ● Trigger on any reader alarm
DOOR: APB Violation (Granted or Denied)	**Select** Door & Schedule	If desired, **select** an Operation and Trigger Code. See page 10-11 for information.
DOOR: Door Closed	**Select** Door & Schedule	**Select** Safe Msg: ● Held open pre-alarm only ● Forced Open is being cancelled ● Held Open is being cancelled ● Held or Forced is being cancelled ● Door Closed ● Door Opened
DOOR: Double Swipe Event	**Select** Door & Schedule	If desired, **select** an Operation and Trigger Code. See page 10-11 for information.
DOOR: Double Swipe Event (Locked/Unlocked)* *This command would be used on an uncontrolled door, i.e. Locked or Unlocked.	**Select** Door & Schedule	If desired, **select** an Operation and Trigger Code. See page 10-11 for information.
DOOR: DURESS Used (Granted OR Denied)	**Select** Door & Schedule	If desired, **select** an Operation and Trigger Code. See page 10-11 for information.
DOOR: Fault	**Select** Door & Schedule	
DOOR: Incomplete Card/PIN sequence	**Select** Door & Schedule	If desired, **select** an Operation and Trigger Code. See page 10-11 for information.
EXT DOOR: All Options	**Select** Doors & Schedule	
MP (Monitor Point)	**Select** Monitor Point & Schedule	

Trigger Event	Object	Arguments & Variables (Optional)
Monitor Point: Inactive (secure)	**Select** Point & Schedule	**Select** Safe Msg: ● Status is now inactive (was active) ● Status is now active (was inactive) ● Last state was ALARM ● Last state was FAULT ● Last state was ALARM or FAULT
MPG (Monitor Point Group): All Options	**Select** MPGs & Schedule	
READER: All Options	**Select** Door & Schedule	
REX (Request to Exit): All Options	**Select** Door & Schedule	
SSP: Controller Local Monitor Point Alarm	**Select** SSP & Schedule	**Select** Local Source: ● Cabinet Tamper or Power Fault
SSP: Controller Local Monitor Point Secure	**Select** SSP & Schedule	**Select** Safe Msg: ● Status is now inactive (was active) ● Status is now active (was inactive) ● Last state was ALARM ● Last state was FAULT ● Last state was ALARM or FAULT **Select** Local Source: ● Cabinet Tamper or Power Fault
SSP: Offline	**Select** SSP & Schedule	
SSP: Online	**Select** SSP & Schedule	
Sub-controller: All Options	**Select** SIO & Schedule	
Time Schedule: All Options	**Select** Time Schedule & Schedule	
User Command: User Command Requested	**Select** Door & Schedule	**Enter** the User Command

Trigger Codes

A trigger code is a numeric designation that, if configured in the cardholder's record, will execute an associated macro when the card containing the trigger code is presented to a reader. The trigger code is used as a modifier for the card to construct triggers that cause specific outcomes.

Trigger codes can be added to most door-based trigger events.

Creating Trigger Codes

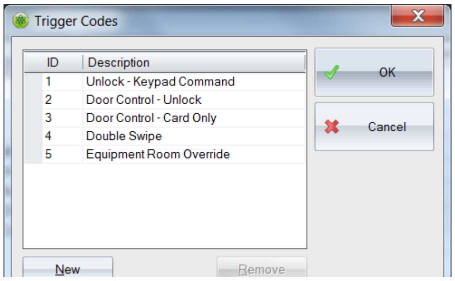
Before a Trigger Code can be applied to a Trigger, the operator must create the code.

1. From the Main Menu, **select** Hardware / Trigger Codes.

   Or

   Right-click on the Controller in the Hardware Browser and **select** Controller Commands / Trigger Codes.

   The Trigger Codes dialog opens.



ID	Description
1	Unlock - Keypad Command
2	Door Control - Unlock
3	Door Control - Card Only
4	Double Swipe
5	Equipment Room Override

2. **Click** the New button and **enter** a Description for the new code.
3. **Click** OK to save the changes.

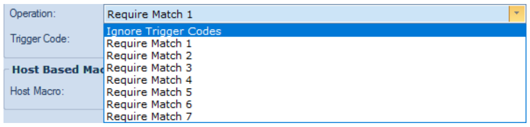
Adding Trigger Codes to a Trigger

1. **Create** the Trigger as described on page 10-7.

   If None is selected for the Doors field, any ACM used will execute the trigger.

2. **Select** an Operation from the drop-down list in the Trigger Variables and Arguments section.

   - Ignore Trigger Codes - Ignores the Trigger Codes function; does not require the Trigger Code set in the Triggers Editor dialog to match the specified slot in the Cardholder's Record.
   - Require Match 1-7 - Requires the Trigger Code selection in the Triggers Editor dialog to match a specified field (Code 1-7) in the Card Tab of the Cardholder's Record.

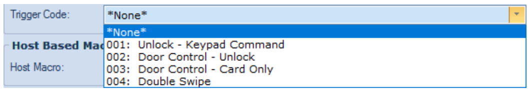


Operation: Require Match 1

Trigger Code:

Host Based Mac

Host Macro:



Trigger Code: *None*

Host Based Mac

Host Macro:

None
001: Unlock - Keypad Command
002: Door Control - Unlock
003: Door Control - Card Only
004: Double Swipe

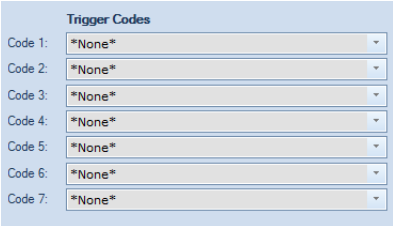
3. **Select** a Trigger Code from the drop-down list.
4. **Click** OK to save the trigger.
5. **Right-click** on the Trigger and **select** Download from the context menu.

Adding Trigger Codes to a Cardholder's Record

1. **Open** the Cardholder's Record and **select** the Card Tab as described on page 7-11.
2. From the Trigger Codes section, **select** the appropriate Trigger Code based on the following conditions:

   - If Ignore Trigger Codes was selected in the Triggers Editor dialog: set the Code 1-7 fields to *None*.
   - If Require Match 1-7 was selected in the Triggers Editor dialog: set the specified Code 1-7 field to match the Trigger Code selection in the Triggers Editor dialog.

     Example: If Require Match 1 was selected, the Code 1 field must match the selected Trigger Code.



Trigger Codes

Code 1: *None*

Code 2: *None*

Code 3: *None*

Code 4: *None*

Code 5: *None*

Code 6: *None*

Code 7: *None*

3. **Right-click** in the Cardholder's Record and **select** Update.

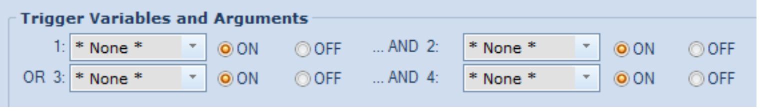
Trigger Variables

Trigger variables are an advanced feature of triggers and macros. If a value is selected for the trigger variable, the selected variable must be present in the controller before the trigger will execute. DNA Fusion allows up to 127 variables to be stored in the controller.

The most common use for trigger variables is to create a "toggle" effect. This occurs when the user creates a pair of identical triggers, except one trigger requires a variable to be OFF and the other requires a variable to be ON. Only one of the two triggers will execute for a given transaction.

Setting a Trigger Variable

1. **Create** the Trigger as described on page 10-7.
2. **Select** the Trigger Variable(s) from the drop-down list(s) in the Trigger Variables and Arguments section of the Triggers Editor dialog.



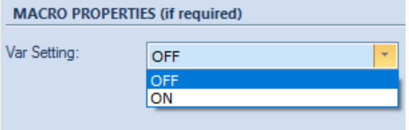
Trigger Variables and Arguments

1: * None * ● ON ○ OFF ... AND 2: * None * ● ON ○ OFF

OR 3: * None * ● ON ○ OFF ... AND 4: * None * ● ON ○ OFF

3. **Select** the appropriate radio button: ON or OFF.
4. **Click** OK to save the trigger.
5. **Create** another Trigger with the same Trigger Variable(s) selected.
6. **Select** the opposite condition: ON or OFF.

   This creates a toggle condition and requires the correct Trigger Variable(s) to be in the controller for the trigger to execute.
7. **Right-click** on the Trigger and **select** Download from the context menu.
8. **Create** a Macro to set the Trigger Variables. See page 10-1 for more information on creating macros.
9. **Add** a TM: Set Trigger Variable command to the macro and **select** an Action Type from the drop-down.
10. **Select** the Trigger Variable used in the Triggers.
11. In the Macro Properties section, **select** a Var Setting: ON or OFF.
12. **Click** OK to save the macro command.



MACRO PROPERTIES (if required)

Var Setting: OFF

13. **Repeat** steps 9 through 11 to add a second macro command.

    NOTE: the Action Type and Var Setting must not match the selections from step 9. For example, if the first macro command was set to Type 1 (Default) and ON, do not select these options for the second macro command. Instead, select Type 2 and OFF.
14. **Click** OK to save the second macro command.
15. **Click** OK to save the configured Macro.

Controlling a Trigger Variable

Operators can manually control trigger variables through the SSP Trigger Variables dialog.

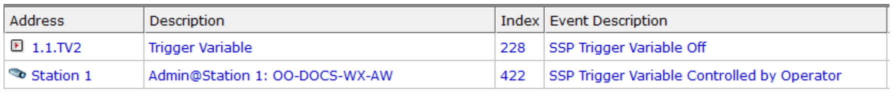
1. In the Triggers and Macros Browser, **right-click** on the Controller under the Triggers section and **select** Trigger Variables.

   The SSP Trigger Variables dialog opens.
2. **Select** a Trigger Variable to toggle its state.

   A green checkmark ✓ indicates the variable is ON.

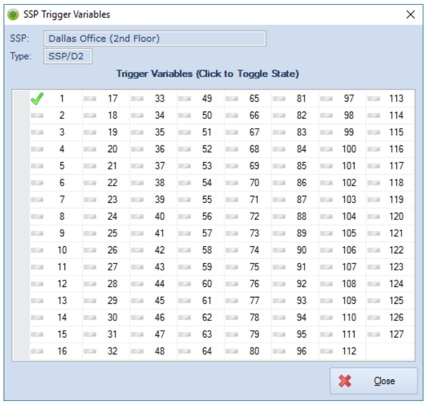
   A gray minus sign − indicates the variable is OFF.

   The status of the Trigger Variable is logged in the Events Grid.



Address	Description	Index	Event Description
1.1.TV2	Trigger Variable	228	SSP Trigger Variable Off
Station 1	Admin@Station 1: OO-DOCS-WX-AW	422	SSP Trigger Variable Controlled by Operator

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



SSP Trigger Variables

SSP: Dallas Office (2nd Floor)

Type: SSP/D2

Trigger Variables (Click to Toggle State)

✓ 1	− 17	− 33	− 49	− 65	− 81	− 97	− 113
− 2	− 18	− 34	− 50	− 66	− 82	− 98	− 114
− 3	− 19	− 35	− 51	− 67	− 83	− 99	− 115
− 4	− 20	− 36	− 52	− 68	− 84	− 100	− 116
− 5	− 21	− 37	− 53	− 69	− 85	− 101	− 117
− 6	− 22	− 38	− 54	− 70	− 86	− 102	− 118
− 7	− 23	− 39	− 55	− 71	− 87	− 103	− 119
− 8	− 24	− 40	− 56	− 72	− 88	− 104	− 120
− 9	− 25	− 41	− 57	− 73	− 89	− 105	− 121
− 10	− 26	− 42	− 58	− 74	− 90	− 106	− 122
− 11	− 27	− 43	− 59	− 75	− 91	− 107	− 123
− 12	− 28	− 44	− 60	− 76	− 92	− 108	− 124
− 13	− 29	− 45	− 61	− 77	− 93	− 109	− 125
− 14	− 30	− 46	− 62	− 78	− 94	− 110	− 126
− 15	− 31	− 47	− 63	− 79	− 95	− 111	− 127
− 16	− 32	− 48	− 64	− 80	− 96	− 112	

Host Based Macros

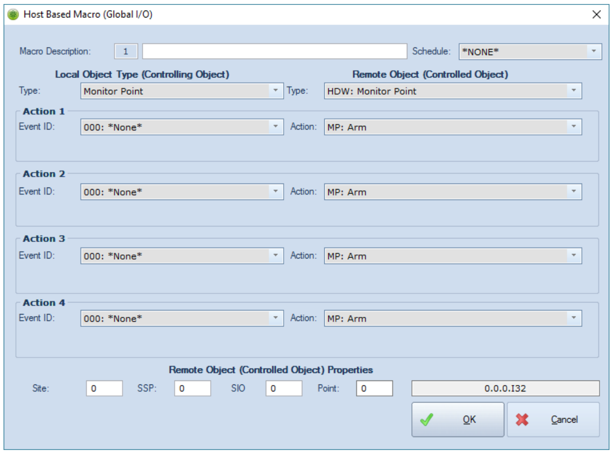
In addition to storing macros on a controller, DNA Fusion is capable of storing host-based macros that create cause-and-effect relationships between points on separate controllers.

Host Based Macros are programmed quite differently from regular triggers and macros, and as such, perform actions that wouldn't be possible with conventional trigger-macro configurations. For example, Host Based Macros must be assigned to the Controlling Object(s) in the Properties dialog. This creates a linkage that tells the system which object(s) will trigger and execute the Macro.

Creating a Host Based Macro

1. With the Triggers & Macros Browser open, **select** the Host Based Macros tab at the bottom of the browser.
2. **Right-click** on the Site object in the browser and **select** Add Host Macro.

   The Host Based Macros (Global I/O) dialog opens.



Host Based Macro (Global I/O)

Macro Description: 1
Schedule: *NONE*

Local Object Type (Controlling Object)
Type: Monitor Point

Remote Object (Controlled Object)
Type: HDW: Monitor Point

Action 1
Event ID: 000: *None*
Action: MP: Arm

Action 2
Event ID: 000: *None*
Action: MP: Arm

Action 3
Event ID: 000: *None*
Action: MP: Arm

Action 4
Event ID: 000: *None*
Action: MP: Arm

Remote Object (Controlled Object) Properties
Site: 0
SSP: 0
SIO 0
Point: 0
0.0.0.I32

3. **Enter** a Macro Description.

   The description will appear in a drop-down menu when the controlling object is configured.
4. If desired, **select** a Time Schedule for the Host Based Macro.

   See page 10-19 for information on creating Internal Time Schedules.
5. **Select** an Object Type from the Local Object Type (Controlling Object) drop-down menu.

   This is the controlling object type that will cause the macro to execute. Depending on the user's selection, the Event ID drop-down options will change.
6. **Select** the Event ID option(s) from the drop-down menu(s).

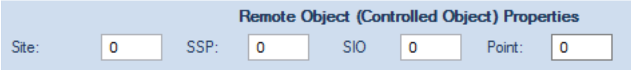
   Up to four separate actions can be configured.
7. **Select** the Remote Object Type (Controlled Object) from the drop-down menu.

   This is the controlled object that will receive the action as a result of the trigger event. Depending on the user's selection, the Action drop-down options will change and additional Parameters may be added.

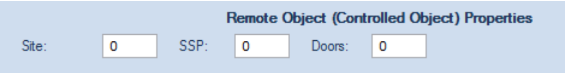
   See table on page 10-15 for more information.
8. **Select** an option(s) from the Action drop-down menu(s) corresponding to the selected Event ID(s).

   Up to four separate actions can be configured
9. If required, **configure** the Remote Object (Controlled Object) Properties section.

   This address tells the system which hardware object will be controlled.



Remote Object (Controlled Object) Properties
Site: 0
SSP: 0
SIO 0
Point: 0



Remote Object (Controlled Object) Properties
Site: 0
SSP: 0
Doors: 0

10. **Click** OK to save the Host Based Macro.
11. **Add** the Host Based Macro to the appropriate Controlling Object. See page 10-14 for more information.

> ! *Unlike regular triggers and macros, which are stored in the controller,* Host Based Macros *are stored locally in the host application. For a* Host Based Macro *to execute, the application must be running. The only exception is the* Email *macro, which is stored in the driver.*

Adding the Host Based Macro to the Controlling Object

Unless the Host Based Macro was created by clicking the Edit button in the Properties dialog of the Controlling Object, the Host Based Macro will need to be linked to the Controlling Object before it can be executed.

1. Depending on the type of Controlling Object selected, open the appropriate browser or dialog:
   - Subcontroller - In the Hardware Browser, **right-click** on the Subcontroller and **select** Properties; **select** Advanced from the dialog menu.
   - Door - In the Hardware Browser, **right-click** on the Door and **select** Properties; **select** Macros from the dialog menu.
   - Elevator - In the Hardware Browser, **right-click** on the Elevator and **select** Properties; **select** Elevator Parameters from the dialog menu.
   - MPG - In the Hardware Browser, **right-click** on the MPG and **select** Properties; **select** Area Points from the dialog menu.
   - Access Area - In the Hardware Browser, **right-click** on the Access Area and **select** Properties.
   - Input Points - In the Hardware Browser, **right-click** on the Input Point and **select** Properties; **select** Input Properties from the dialog menu.
   - Output Points - In the Hardware Browser, **right-click** on the Output Point and **select** Properties; **select** Output Properties from the dialog menu.
   - Reader - In the Hardware Browser, **right-click** on the Reader and **select** Properties; **select** Reader Properties from the dialog menu.
   - Time Schedule - In the Time Schedules Browser, **right-click** on a Time Schedule and **select** Properties.
   - Trigger - In the Triggers and Macros Browser, **right-click** on the Trigger and **select** Properties.
   - Macro - In the Triggers and Macros Browser, **double-click** on the Macro.
   - Access Card - In the Personnel Browser, **right-click** on the Cardholder or Card and **select** Properties; **select** the Card Tab from the Cardholder's Record.
   - Station - **Select** DNA Properties from the Standard Toolbar; **select** Station Settings from the dialog menu.
   - Situation Manager - **Select** DNA Properties from the Standard Toolbar; **select** Situation Manager from the dialog menu.
2. **Locate** the Host Macro field and **select** a Host Based Macro from the drop-down list.
3. **Click** OK to save the dialog.

   Or

   If Access Card object, **right-click** in the Cardholder's Record and **select** Update.

   A download prompt appears.
4. **Select** Yes to download the macro.

   The Host Based Macro is downloaded and linked to the controlling object.

> ⓘ Multiple objects may use the same Host Based Macro.

Host Based Macros Table

Controlled Object	Parameters
AXS: Control Axis Door	• **Select** the desired Action from the drop-down: Lock Down Door, Unlock Door, Lock Door, Facility Code, Card Only, PIN Only, Card and PIN, Card or PIN, or Momentary Unlock
ISS: Control Isonas Door	• **Select** the desired Action from the drop-down: Lock Down Door, Remove Lock Down, Unlock Door, Lock Door, Card Only, Card or PIN, or Momentary Unlock
BPN: Control Bosch Area	• **Select** the desired Action from the drop-down: Disarm or Master Arm
BPN: Control Bosch Point	• **Select** the desired Action from the drop-down: Bypass Point or Unbypass Point
BPN: Control Bosch Output	• **Select** the desired Action from the drop-down: Activate Output or Deactivate Output
TKE: Control ThyssenKrupp	• **Select** the desired Action from the drop-down: Lock Floor, Unlock Floor or Resume Normal
KON: Control Kone	• **Select** the desired Action from the drop-down: Lock Floor, Unlock Floor or Resume Normal
ENG: Control Engage	• **Select** the desired Action from the drop-down: Lock Down Door, Remove Lock Down Door, Unlock Door, Lock Door, or Momentary Unlock
CAM: Advanced Camera Macro	• **Select** the Station from the Action drop-down • **Click** the Build button to open the Advanced Camera Macro dialog • **Select** the View (1, 2, 4, 9, or 16), Mode (Live or Recorded), and Camera, and **enter** the Preset or Pre-Alarm time
CAM: Control Camera Recording	• **Select** Activate from the Action drop-down • **Click** the Build button to open the Control Camera Recording dialog and **select** the Recording Options
CRD: Card Access	• **Select** Activate from the Action drop-down • **Click** the Build button
EXT: Control Peripheral Object	• **Select** Set Card Use Limit from the Action drop-down and **enter** a Parameter (value) of 1 - 255. Values of 255 = Unlimited Or • **Select** Set Card Use Limit from the Action drop-down and **enter** a Parameter (value) of 1 - 255. Values of 255 = Unlimited
EXT: Control ASSA Access Point	• **Select** the desired Action from the drop-down: Lock Access Point, Unlock Access Point, Momentary Unlock Access Point, Lock Down Access Point, Remove Lock Down, Enable Access Point, or Disable Access Point • **Click** the Build button to open the ASSA Door Assignment dialog and **assign** the desired Door
HDW: Monitor Point	• **Select** the desired Action from the drop-down: Arm or Disarm • **Enter** the Input Address in the Remote Object Properties section
HDW: Control Point	• **Select** the desired Action from the drop-down: Activate, Deactivate, or Pulse • **Enter** the Output Address in the Remote Object Properties section

Controlled Object	Parameters
HDW: Door	• **Select** the desired Action form the drop-down: Momentarily Unlock Door, or Floor Pulse FLR 001-128 • **Enter** the number of Milliseconds in the Parameters field • **Enter** the ACM Address in the Remote Object Properties section
HDW: Arm Door	• **Select** the desired Action from the drop-down: Disarm Door Forced Open, Arm Door Forced Open, Disarm Door Held Open, Arm Both, or Disarm Both
HDW: Set Reader Mode	• **Select** the desired Action from the drop-down: Disabled, Unlocked, Locked, Correct Facility Code, Card Only, PIN Only, Card AND PIN, or Card OR PIN
HDW: Set Reader LED Mode	• **Select** Activate from the Action drop-down • **Enter** the LED Table Index (1, 2, or 3) in the Parameters field • **Enter** the ACM Address in the Remote Object Properties field
HDW: Time Schedule	• **Select** the desired Action from the drop-down: Temporary Off, Temporary On, Override Off, Override On, Resume Normal State, or Refresh Status
HDW: Monitor Point Group (MPG)	• **Select** the desired Action from the drop-down: Arm, Disarm, Access, Force ARM, Standard ARM, or Override ARM • **Enter** the MPG Address in the Remote Object Properties section
HDW: Access Control Area	• **Select** the desired Action from the drop-down: Enable, Disable, or Set Occupancy • **Enter** the number of Occupants in the Parameters field • **Enter** the Access Area Address in the Remote Object Properties section
HDW: Macro	• **Select** the desired Action from the drop-down: Macro Command, Macro Command TYPE 2, Macro Command TYPE 3, or Macro Command TYPE 4 • **Enter** the Macro Address in the Remote Object Properties section
HDW: Set Trigger Variable	• **Select** Trigger Variable Control from the Action drop-down. • **Enter** the Trigger Variable in the Parameters field • **Enter** the Trigger Variable Address in the Remote Object Properties section
HDW: Control SSP	• **Select** the desired Action from the drop-down: Attach SSP, Detach SSP, Dual Port Control, or SSP Hang Up Soon • **Enter** the desired variable in the Parameters field
HDW: Set SSP Set Time	• **Select** Activate from the Action drop-down • **Enter** the SSP Address in the Remote Object Properties section
HDW: Execute Direct Command	• **Select** the Station from the Action drop-down • **Click** the Build button to **select** the Direct Command: Lockdown, Return to Normal, or Temporary Override • **Enter** a variable in the Parameters field
HDW: LCD Text to Keypad	• **Select** Activate from the Action drop-down • **Click** the Build button and **enter** the LCD Text Parameters • **Enter** a variable in the Parameters field
HDW: Submit Batch File	• **Select** Activate from the Action drop-down • **Click** the Search button and **locate** the desired Batch File • **Enter** a variable in the Parameters field

Controlled Object	Parameters
HDW: HEX to SIO Port	• **Select** Activate from the Action drop-down • **Click** the Build button and **enter** the SIO HEX Output Parameters • **Enter** a variable in the Parameters field
HBM: Execute Host Macro List	• **Select** Activate from the Action drop-down • **Click** the Build button and **select** a Macro List from the dialog • **Enter** a variable in the Parameters field
HST: Run Program	• **Select** the Station from the Action drop-down • **Click** the Search button to **locate** the desired Program • **Enter** the path in the Parameters field
HST: Load External Page	• **Select** the Station from the Action drop-down • **Enter** the path in the Parameters field
HST: Load HTML Goto Page	• **Select** the Station from the Action drop-down • **Enter** the path in the Parameters field
HST: Load Camera	• **Select** the Station from the Action drop-down • **Click** the Build button to **select** the desired Camera • **Enter** a variable in the Parameters field
HST: Load Graphic Map	• **Select** the Station from the Action drop-down • **Click** the Search button to **select** the desired Graphic Map
HST: Email	• **Select** the Station from the Action drop-down • **Click** the Build button to enter the E-Mail and Replacement Text Parameters (see Appendix D) • **Enter** a variable in the Parameters field
HST: Play WAV File	• **Select** Activate from the Action drop-down • **Click** the Build button to **select** the Sound File • **Enter** path in the Parameters field
MIS: Log Off Station	• **Select** the Station from the Action drop-down
MIS: Situation Level Manager	• **Select** the desired Action from the drop-down: □ Situation Level Manager Set to Severe (Red) □ Situation Level Manager Set to High (Orange) □ Situation Level Manager Set to Elevated (Yellow) □ Situation Level Manager Set to Guarded (Blue) □ Situation Level Manager Set to Low (Green) □ Turn Situation Level Manager ON □ Turn Situation Level Manager OFF
DBM: Secured Area Auto Arm Record	• **Select** Activate from the Action drop-down
DBM: Add to Database With DSN	• **Select** Activate from the Action drop-down • **Click** the Build button and **enter** the Query and DSN in the dialog • **Enter** a variable in the Parameters field
DBM: Add to Database With Events Server	• **Select** Activate from the Action drop-down • **Click** the Build button and **enter** the Query in the dialog • **Enter** a variable in the Parameters field
DBM: Add to Database With Hardware Server	• **Select** Activate from the Action drop-down • **Click** the Build button and **enter** the Query in the dialog • **Enter** a variable in the Parameters field

Controlled Object	Parameters
DM: Add to Database With Personnel Server	• **Select** Activate from the Action drop-down • **Click** the Build button and **enter** the Query in the dialog • **Enter** a variable in the Parameters field
DBM: Add Logfile Entry	• **Select** Activate from the Action drop-down • **Click** the Build button and **enter** the Query and File in the dialog • **Enter** a variable in the Parameters field
UAD: Universal Driver	• **Select** Activate from the Action drop-down • **Click** the Build button and **select** a Driver Name from the dialog • **Enter** a variable in the Parameters field
DRV: HTTP Request	• **Select** the Station from the Action drop-down • **Click** the Build button and **enter** the HTTP Parameters for the dialog • **Enter** a variable in the Parameters field

Internal Time Schedules

Creating Internal Time Schedules

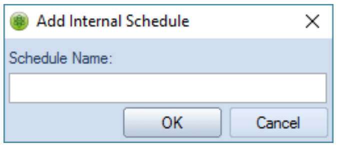
An Internal Time Schedule can be configured to limit the time frame in which a Host Based Macro will execute.

1. **Select** DNA / Administrative / Setup Internal Schedules from the Main Menu.

   The Internal Schedule Properties dialog opens.

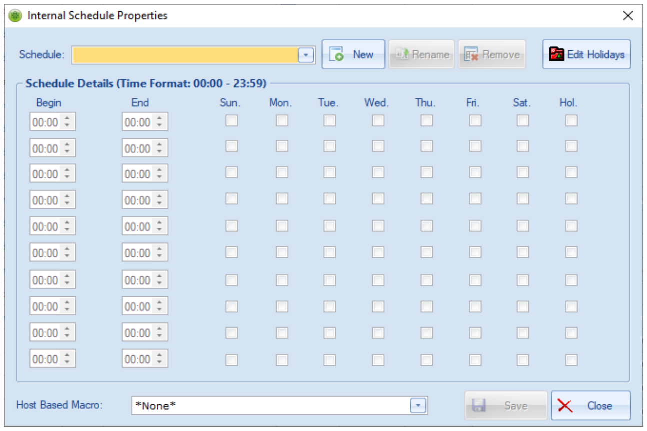
2. **Click** the New button.

   The Add Internal Schedule dialog appears.



3. **Enter** a Schedule Name and **click** the OK button.

   The Internal Schedules Properties dialog populates with the Schedule Name.



Schedule Details (Time Format: 00:00 - 23:59)

Begin	End	Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	Hol.
00:00	00:00	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□
00:00	00:00	□	□	□	□	□	□	□	□

Host Based Macro: *None*

4. **Configure** the Schedule Details section.

   Each time schedule is made up of ten possible intervals. An interval consists of a Begin and End time, the day(s) that the time schedule will be active, and a place to determine if the schedule will be active during defined holidays. At least one interval must be defined for the time schedule to be valid.

   a. **Enter** the Begin and End Time(s) using military time designations (00:00-23:59) for the appropriate interval.

   b. **Assign** the Time Interval to specific days of the week by **checking** the desired box(es).

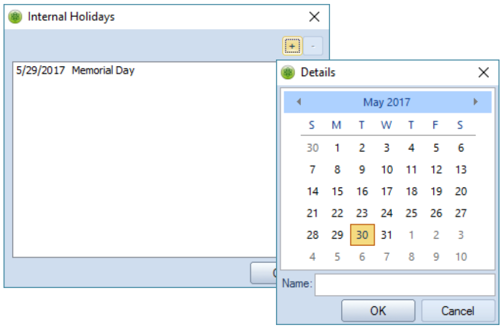
   c. The last box for each interval is labeled Hol and, when checked, will activate the time schedule during the specified time range on days that have been defined as holidays. See below for more information on adding internal holidays.

   d. If needed, **click** on the drop-down menu to select a Host Based Macro to be triggered.

5. **Click** the Save button to save the Internal Time Schedule.

   The time schedule will be added to the Schedule drop-down in the Host Based Macro (Global I/O) dialog.

Adding Internal Holidays



5/29/2017 Memorial Day

1. If desired, **click** the Edit Holidays button.

   The Internal Holidays dialog will open.

2. **Click** the plus sign + to add a new holiday.

   The Details dialog opens with a calendar.

3. **Enter** a Name and **select** a Date from the calendar.

4. **Click** the OK button to save the holiday.

   The holiday is added to the Internal Holidays list.

Editing Internal Time Schedules

1. **Select** DNA / Administrative / Setup Internal Schedules from the Main Menu.

   The Internal Schedule Properties dialog opens.
2. **Select** the desired Schedule from the drop-down list.
3. If desired, **click** the Rename button to edit the schedule’s name.
4. **Edit** the Schedule Details section as needed.
5. **Click** the Save button to save the changes.

Deleting Internal Time Schedules

1. **Select** DNA / Administrative / Setup Internal Schedules from the Main Menu.

   The Internal Schedule Properties dialog opens.
2. **Select** the desired Schedule from the drop-down list.
3. **Click** the Remove button.

   A confirmation dialog appears.
4. **Click** the Yes to delete the schedule.
5. **Click** the Save button to save the changes.

Editing Internal Time Schedule Holidays

1. **Select** DNA / Administrative / Setup Internal Schedules from the Main Menu.

   The Internal Schedule Properties dialog opens.
2. **Click** the Edit Holidays button.

   The Internal Holidays dialog appears.
3. **Double-click** the desired Holiday.

   The Details dialog opens.
4. **Edit** the Holiday as needed.
5. **Click** OK to save the changes.
6. **Click** the Close button to close the Internal Holidays dialog.

Deleting Internal Time Schedule Holidays

1. **Select** DNA / Administrative / Setup Internal Schedules from the Main Menu.

   The Internal Schedule Properties dialog opens.
2. **Click** the Edit Holidays button.

   The Internal Holidays dialog will open.
3. **Select** the desired Holiday and **click** the minus sign - to delete the new holiday.

   A confirmation dialog will appear.
4. **Click** Yes to delete the holiday.
5. **Click** OK to save the changes.
6. **Click** the Close button to close the Internal Holidays dialog.

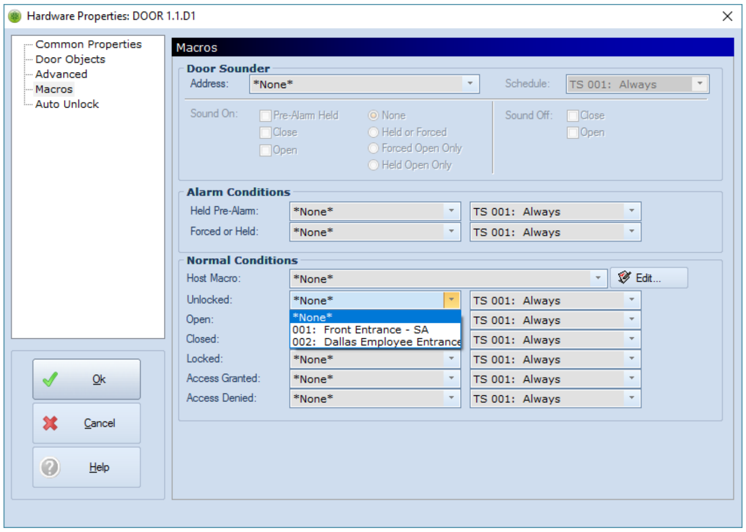
Adding a Macro to a Door

Existing macros can be added to a door to trigger an action based on the door condition.

1. **Open** the Hardware Browser and **expand** the tree.
2. **Right-click** on the Door you want to associate with the macro and **select** Properties.

   The Door Properties dialog appears.
3. **Select** Macros from the dialog menu.

   The Macros dialog opens. See page 8-65 for more information.



Door Sounder

Address: *None* — Schedule: TS 001: Always

Sound On: □ Pre-Alarm Held □ Close □ Open — ● None ○ Held or Forced ○ Forced Open Only ○ Held Open Only

Sound Off: □ Close □ Open

Alarm Conditions

Held Pre-Alarm:	*None*	TS 001: Always
Forced or Held:	*None*	TS 001: Always

Normal Conditions

Host Macro:	*None*	
Unlocked:	*None* *None* 001: Front Entrance - SA 002: Dallas Employee Entrance	TS 001: Always
Open:		TS 001: Always
Closed:		TS 001: Always
Locked:	*None*	TS 001: Always
Access Granted:	*None*	TS 001: Always
Access Denied:	*None*	TS 001: Always

4. **Select** the desired Macro from one of the drop-down lists next to a Trigger condition.
5. **Select** a Time Schedule to associate with the macro from the drop-down list.
6. **Click** OK.

   A download prompt will appear.
7. **Select** Yes to download the Macro.

   A trigger is added to the Triggers and Macros Browser.

ⓘ Multiple doors may reference the same Host Based Macro.

This Page Intentionally Left Blank

Access Areas & Anti-Pass Back 11

In This Chapter

Access Areas

What is an Access Area?

An Access Area is a defined area wherein all access points are secured by the system. The access points can be configured and adjusted to set parameters on occupancy and permission attributes.

Operators can limit the number of cardholders allowed in the area. The configuration includes a minimum and maximum occupancy count; if either of these numbers are reached, an event is logged in the system. These limits may be set so that no fewer than two cardholders are in the area.

Creating an Access Area

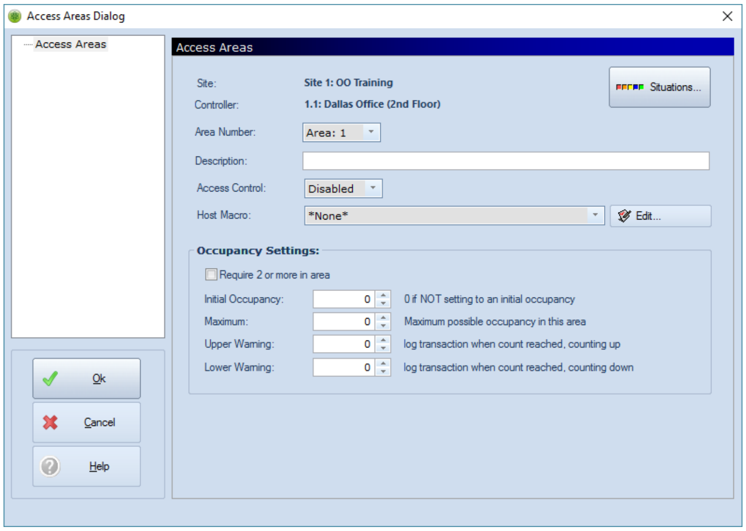
> *The* Access Control Areas *option must be checked in the* Hardware Tree Behavior *dialog for* Access Area *objects to be visible in the* Hardware Browser*. See page 3-27 for more information.*

1. **Right-click** on the Controller in the Hardware Browser and **select** Add / Add Access Area.

   Or

   Right-click on the Access Areas header in the Access Levels Browser and **select** Add.

   The Access Areas Dialog opens.



Site: Site 1: OO Training

Controller: 1.1: Dallas Office (2nd Floor)

Area Number: Area: 1

Description:

Access Control: Disabled

Host Macro: *None*

Occupancy Settings:

☐ Require 2 or more in area

Initial Occupancy:	0	0 if NOT setting to an initial occupancy
Maximum:	0	Maximum possible occupancy in this area
Upper Warning:	0	log transaction when count reached, counting up
Lower Warning:	0	log transaction when count reached, counting down

2. **Select** an Area Number from the drop-down list.

   The number is an arbitrary designation for the given access area.

3. **Enter** a Description for the area.

4. **Select** the appropriate type of Access Control from the drop-down:
   - No Change - The area's Occupancy Count will not change when cardholders access this area.
   - Disabled - Deactivates the area; cardholders will receive an Access Denied: Area Disabled event.
   - Enabled - Activates the area; cardholders will have access based on their assigned access level and the area's Occupancy Settings.
5. If desired, **select** a Host Based Macro from the drop-down list to associate with the Access Area.

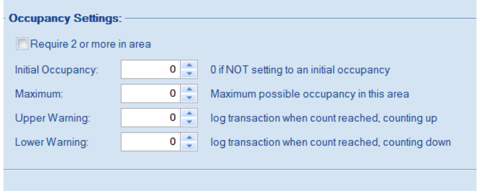
   See page 10-13 for more information on Host Based Macros.
6. If desired, **click** the Situations... button to enable the Situation Manager.

   See page 9-6 for more information.
7. If needed, **check** the Require 2 or more in area checkbox to require two separate access credentials to be recognized before access will be granted.

   NOTE: Do not check if Anti-Pass Back is being used.
8. **Enter** the Initial Occupancy.

   Leave this field set to 0 if you are not setting an initial occupancy.
9. **Enter** the Maximum number of occupants allowed in the area.

   If Anti-Pass Back will be used, this number should be more than the total number of access cards. When this number is reached, the system logs an event in the Events Grid.



Occupancy Settings:

□ Require 2 or more in area

Initial Occupancy: 0 — 0 if NOT setting to an initial occupancy

Maximum: 0 — Maximum possible occupancy in this area

Upper Warning: 0 — log transaction when count reached, counting up

Lower Warning: 0 — log transaction when count reached, counting down

10. If desired, **enter** the Upper Warning occupancy number.

    This is normally 5% less than the Maximum number. Reaching the Upper Warning number will generate an alarm to indicate that the maximum occupancy is close to being met.
11. If desired, **enter** the Lower Warning occupancy number.

    Reaching this number will generate an alarm indicating that the occupancy has fallen below a certain number.
12. **Click** OK to save the access area.
13. **Download** the changes to the controller.

    See page 2-15 for information on downloading.
14. **Add** the Access Area to the appropriate ACM to configure the To and From areas.

    See pages 11-3 (door) and 11-4 (elevator) for information on adding the access area to an ACM.

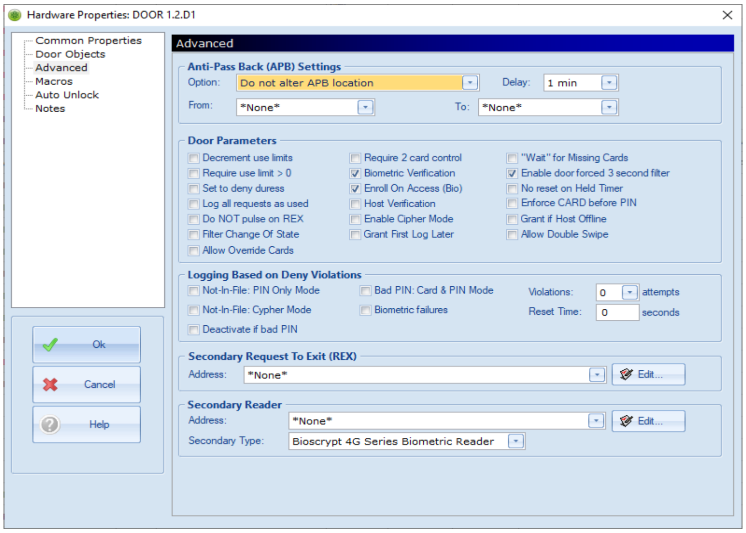
Adding an Access Area to a Door

1. In the Hardware Browser, **right-click** on an existing Door and **select** Properties or **create** a new door for the area.

   The Doors Properties dialog opens.

2. **Select** the Advanced option from the dialog menu.

   The Advanced dialog opens.



Anti-Pass Back (APB) Settings

Option: Do not alter APB location   Delay: 1 min

From: *None*   To: *None*

Door Parameters

☐ Decrement use limits
☐ Require use limit > 0
☐ Set to deny duress
☐ Log all requests as used
☐ Do NOT pulse on REX
☐ Filter Change Of State
☐ Allow Override Cards
☐ Require 2 card control
☑ Biometric Verification
☑ Enroll On Access (Bio)
☐ Host Verification
☐ Enable Cipher Mode
☐ Grant First Log Later
☐ "Wait" for Missing Cards
☑ Enable door forced 3 second filter
☐ No reset on Held Timer
☐ Enforce CARD before PIN
☐ Grant if Host Offline
☐ Allow Double Swipe

Logging Based on Deny Violations

☐ Not-In-File: PIN Only Mode
☐ Not-In-File: Cypher Mode
☐ Deactivate if bad PIN
☐ Bad PIN: Card & PIN Mode
☐ Biometric failures

Violations: 0 attempts
Reset Time: 0 seconds

Secondary Request To Exit (REX)

Address: *None*

Secondary Reader

Address: *None*
Secondary Type: Bioscrypt 4G Series Biometric Reader

3. **Select** the type of Anti-Pass Back from the Option drop-down list.

   - Accept any location, change on entry - Allows any user with the appropriate access into an area regardless of the user's current area. Changes the area number. (Area-based Soft Anti-Pass Back)

   - Check location, change on entry - Requires the cardholder to be in the correct area (as established in the reader's anti-pass back properties) before access is granted. (Area-based Hard Anti-Pass Back)

   - Check last valid user - References the user's card number and will not grant access to the same card number until a different card is presented at the reader or until the APB delay expires. Default Delay = 1 minute. (Reader-based Anti-Pass Back)

   - Check last ACR used, no location change - Prevents a cardholder from presenting his or her card to the same reader twice in a row. After the reader grants access, the cardholder will not be granted access at the same reader again until he/she presents the card at another reader in the system or until the APB delay expires. Default Delay = 1 minute. (Reader-based Anti-Pass Back)

   - Check current location, change on entry - Similar to option #2, except that the APB delay will reset the user's area after the specified time. Default Delay = 1 minute. (Area-based Timed Anti-Pass Back)

     For anti-pass back configuration, see page 11-7.

4. **Select** the From: area that the user will come from.

5. **Select** the To: area that the user will enter.

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

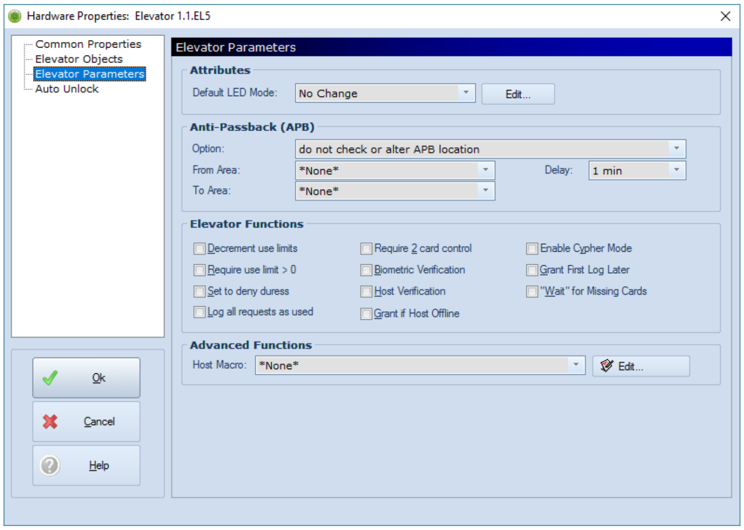
Adding an Access Area to an Elevator

1. In the Hardware Browser, **right-click** on an existing Elevator and **select** Properties or **create** a new elevator for the area.

   The Elevator Properties dialog opens.

2. **Select** the Elevator Parameters option from the dialog menu.

   The Elevator Parameters dialog appears.



Elevator Parameters

Attributes

Default LED Mode: No Change

Anti-Passback (APB)

Option: do not check or alter APB location

From Area: *None* Delay: 1 min

To Area: *None*

Elevator Functions

□ Decrement use limits	□ Require 2 card control	□ Enable Cypher Mode
□ Require use limit > 0	□ Biometric Verification	□ Grant First Log Later
□ Set to deny duress	□ Host Verification	□ "Wait" for Missing Cards
□ Log all requests as used	□ Grant if Host Offline	

Advanced Functions

Host Macro: *None*

3. **Select** the type of Anti-Pass Back from the Option drop-down list.

   NOTE: The first option, Do not alter APB location, disables the Anti-Pass Back feature.

   - Accept any location, change on entry - Allows any user with the appropriate access into an area regardless of the user's current area. Changes the area number. (Area-based Soft Anti-Pass Back)
   - Check location, change on entry - Requires the cardholder to be in the correct area (as established in the reader's anti-pass back properties) before access is granted. (Area-based Hard Anti-Pass Back)
   - Check this reader's last valid user - References the user's card number and will not grant access to the same card number until a different card is presented at the reader or until the APB delay expires. Default Delay = 1 minute. (Reader-based Anti-Pass Back)
   - Check user's last ACR used, no location change - Prevents a cardholder from presenting his or her card to the same reader twice in a row. After the reader grants access, the cardholder will not be granted access at the same reader again until he/she presents the card at another reader in the system or until the APB delay expires. Default Delay = 1 minute. (Reader-based Anti-Pass Back)
   - Check user's current location, change on entry - Similar to option #2, except that the APB delay will reset the user's area after the specified time. Default Delay = 1 minute. (Area-based Timed Anti-Pass Back)

     For anti-pass back configuration, see page 11-7.

4. **Select** the From: area that the user will come from.

5. **Enter** the To: area that the user will enter.

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

Access Area Features

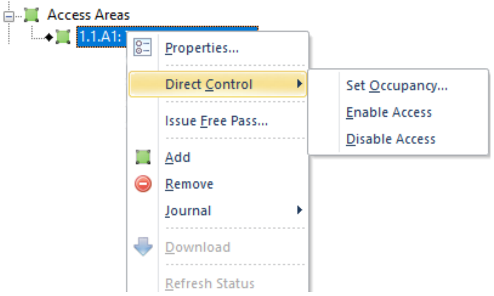
DNA Fusion offers a number of features for access areas and anti-pass back settings.

Enable/Disable an Access Area

Enabling and disabling an Access Area allows the system operator to quickly control access to the area.

1. **Expand** the Hardware Browser to view Access Areas.
2. **Right-click** on the Access Area and **select** Direct Control / Enable Access.

   Or



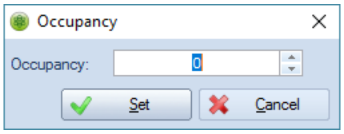
3. **Right-click** on the Access Area and **select** Direct Control / Disable Access.
   - Disable - Deactivates the area; cardholders will receive an Access Denied: Area Disabled event.
   - Enable - Activates the area; cardholders will have access based on their assigned Access Level and the Access Areas Occupancy Settings.

Set Occupancy

The Set Occupancy option manually adjusts the occupancy number for the Access Area.

1. **Expand** the Hardware Browser to view Access Areas.
2. **Right-click** on the Access Area and **select** Direct Control / Set Occupancy.

   The Occupancy dialog appears.



Occupancy

Occupancy: 0

3. **Enter** the Occupancy number and **click** Set.

   The Occupancy for the selected Access Area is set to the designated number.

Deleting an Access Area

1. **Expand** the Access Area selection in the Hardware Browser.
2. **Right-click** on the Access Area and **select** Remove.

   A confirmation dialog appears.
3. **Click** Yes to confirm the deletion.

   The access area is removed from the list.

NOTES:

Anti-Pass Back

Anti-Pass Back (APB) prevents a person from using a door if the system does not recognize them as being in the correct area. A cardholder must present their card at each reader in a specific order as they progress through the facility to be recognized by the system. If a cardholder fails to badge at a reader, and instead follows another cardholder into an area, an APB violation will occur when the cardholder badges because the cardholder was not detected in the correct area. APB also prevents a card from being passed back to an unauthorized user.

It is important to carefully plan your anti-pass back system. It is recommended that you obtain a layout of the facility where APB will be implemented. Using this layout, determine what areas or zones you will set up and which readers will control access in and out of these areas. Use the information to set up the anti-pass back features in DNA Fusion.

Types of Anti-Pass Back

DNA Fusion supports reader-based and area-based models with time-based extensions. Within those mechanisms, the anti-pass back rules can be set to "hard" or "soft" anti-pass back. Hard anti-pass back refers to rules that do not grant access to the user for anti-pass back violations, while soft anti-pass back refers to rules that allow access for anti-pass back violations and instead log an anti-pass back event in the system.

Area-Based

Area-based anti-pass back relies on knowing the user's location in the system at all times. Typically, area-based anti-pass back is implemented with readers that track the entry and exit points of an area. The location of the cardholder's last Access Granted event is stored in the cardholder's record. If the area in the cardholder's record matches the reader's current area, the cardholder will be granted access. Once entry has been detected, the cardholder's record will update to reflect the cardholder's new location.

Reader-Based

Reader-based anti-pass back refers to rules based on the access history of an individual reader. Typically, these rules prevent multiple people from using the same card at the same reader to access an area.

Two types of reader-based anti-pass back can be used: the first type stores the card number and time of the last Access Granted event in the reader; the second type stores the reader number of the last Access Granted event in the cardholder's record.

Configuring DNA to Use Anti-Pass Back

DNA Fusion must be configured for anti-pass back prior to implementing the feature.

1. In the Controller Properties / Stored Quantities dialog, **select** the Store APB Location checkbox.

   See page 8-53 for more information.

2. For general anti-pass back, **deselect** Support Timed Anti-Pass Back in the Stored Quantities dialog.

3. **Create** an Access Area for each of the anti-pass back locations.

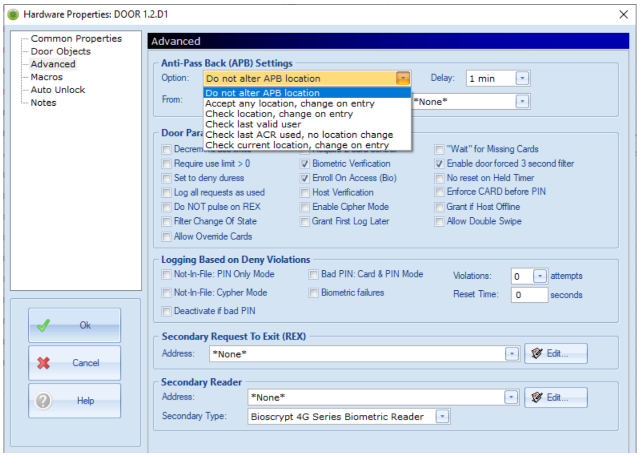
   At least two Access Areas must be created: a To: and From: area. See page 11-1 for information on creating access areas.

> ! *Because* Host Based Macros *will be used to communicate between panels, APB locations that cross multiple controllers require a constant connection to the server.*

NOTES:

Implementing Anti-Pass Back for a Door

1. **Open** the Advanced dialog for the door as described on page 11-3.



Advanced

Anti-Pass Back (APB) Settings

Option: Do not alter APB location

Delay: 1 min

From:

None

Do not alter APB location
Accept any location, change on entry
Check location, change on entry
Check last valid user
Check last ACR used, no location change
Check current location, change on entry

Door Para

□ Decrem		□ "Wait" for Missing Cards
□ Require use limit > 0	☑ Biometric Verification	☑ Enable door forced 3 second filter
□ Set to deny duress	☑ Enroll On Access (Bio)	□ No reset on Held Timer
□ Log all requests as used	□ Host Verification	□ Enforce CARD before PIN
□ Do NOT pulse on REX	□ Enable Cipher Mode	□ Grant if Host Offline
□ Filter Change Of State	□ Grant First Log Later	□ Allow Double Swipe
□ Allow Override Cards		

Logging Based on Deny Violations

□ Not-In-File: PIN Only Mode □ Bad PIN: Card & PIN Mode Violations: 0 attempts

□ Not-In-File: Cypher Mode □ Biometric failures Reset Time: 0 seconds

□ Deactivate if bad PIN

Secondary Request To Exit (REX)

Address: *None*

Secondary Reader

Address: *None*

Secondary Type: Bioscrypt 4G Series Biometric Reader

2. **Select** the type of Anti-Pass Back for the door from the Option drop-down list.

   NOTE: The first option, Do not alter APB location, disables the Anti-Pass Back feature.

   - Accept any location, change on entry - Allows any user with the appropriate access into an area regardless of the user's current area. Changes the area number. (Area-based Soft Anti-Pass Back)
   - Check location, change on entry - Requires the cardholder to be in the correct area (as established in the reader's anti-pass back properties) before access is granted. (Area-based Hard Anti-Pass Back)
   - Check last valid user - References the user's card number and will not grant access to the same card number until a different card is presented at the reader or until the APB delay expires. Default Delay = 1 minute. (Reader-based Anti-Pass Back)
   - Check last ACR used, no location change - Prevents a cardholder from presenting his or her card to the same reader twice in a row. After the reader grants access, the cardholder will not be granted access at the same reader again until he/she presents the card at another reader in the system or until the APB delay expires. Default Delay = 1 minute. (Reader-based Anti-Pass Back)
   - Check current location, change on entry - Similar to option #2, except that the APB delay will reset the user's area after the specified time. Default Delay = 1 min. (Area-based Timed Anti-Pass Back)

3. If needed, **set** the Delay time.

   Once the delay time expires, the system will reset so that a cardholder may gain access to the area. Max. delay = 1092 minutes.

4. **Select** the From: area that the user will come from.
5. **Select** the To: area that the user will enter.

> *Generally, the* From *and* To *settings will be reversed for each door or elevator in an* In/Out *reader configuration.*

6. **Check** any Door Parameter or Elevator Function settings to apply to the area.

> *When using APB, it is strongly recommended that you* ***deselect*** *the* Log All Requests as Used *setting in the* Door Parameters *section to prevent cardholders from being located in the wrong APB area.*
>
> *If this option is selected, and the cardholder presents their card at a reader without using the door, the system will assume the cardholder has entered the new area and will not grant access at the same reader again unless the* Delay *time has expired.*

7. **Click** OK to save the settings.
8. **Create** an Access Level for the APB door/elevator.

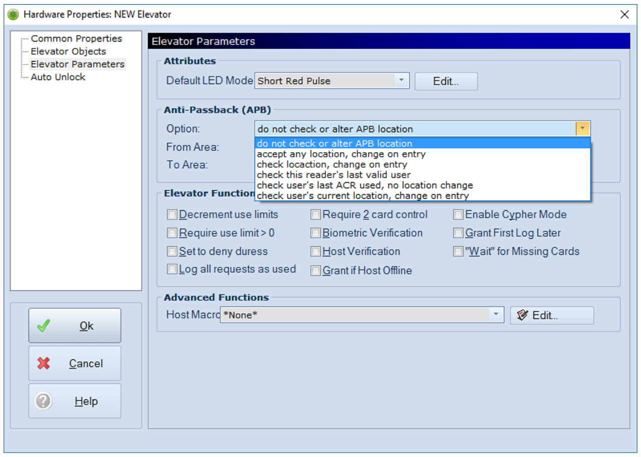
   See Chapter 6 for access level information.

9. **Assign** cardholders to the access level.

   See page 7-13 for more information on assigning access levels.

Implementing Anti-Pass Back for an Elevator

1. **Open** the Elevator Parameters dialog for the elevator as described on page 11-4.


Hardware Properties: NEW Elevator
Common Properties
Elevator Objects
Elevator Parameters
Auto Unlock
Elevator Parameters
Attributes
Edit..
Anti-Passback (APB)
From Area:
To Area:
do not check or alter APB location
accept any location, change on entry
check locaction, change on entry
check this reader's last valid user
check user's last ACR used, no location change
check user's current location, change on entry
Elevator Function
Advanced Functions
Edit..
Ok
Cancel
Help

Default LED Mode: Short Red Pulse

Option: do not check or alter APB location

□ Decrement use limits
□ Require use limit > 0
□ Set to deny duress
□ Log all requests as used
□ Require 2 card control
□ Biometric Verification
□ Host Verification
□ Grant if Host Offline
□ Enable Cypher Mode
□ Grant First Log Later
□ "Wait" for Missing Cards

Host Macro: *None*

2. **Select** the type of Anti-Pass Back for the elevator from the Option drop-down list.

   NOTE: The first option, Do Not Check or Alter APB location, disables the Anti-Pass Back feature.

   - Accept any location, change on entry - Allows any user with the appropriate access into an area regardless of the user's current area. Changes the area number. (Area-based Soft Anti-Pass Back)
   - Check location, change on entry - Requires the cardholder to be in the correct area (as established in the reader's anti-pass back properties) before access is granted. (Area-based Hard Anti-Pass Back)
   - Check this reader's last valid user - References the user's card number and will not grant access to the same card number until a different card is presented at the reader or until the APB delay expires. Default Delay = 1 minute. (Reader-based Anti-Pass Back)
   - Check user's last ACR used, no location change - Prevents a cardholder from presenting his or her card to the same reader twice in a row. After the reader grants access, the cardholder will not be granted access at the same reader again until he/she presents the card at another reader in the system or until the APB delay expires. Default Delay = 1 minute. (Reader-based Anti-Pass Back)
   - Check user's current location, change on entry - Similar to option #2, except that the APB delay will reset the user's area after the specified time. Default Delay = 1 min. (Area-based Timed Anti-Pass Back)

3. If needed, **set** the Delay time.

   Once the delay time expires, the system will reset so that a cardholder may gain access to the area. Max. delay = 255 minutes.

4. **Select** the From: area that the user will come from.
5. **Enter** the To: area that the user will enter.

> *Generally, the* From *and* To *settings will be reversed for each elevator in an* In/Out *reader configuration.*

6. **Select** any Elevator Function settings to apply to the area.

> *When using APB, it is strongly recommended that you* ***deselect*** *the* Log All Requests as Used *setting in the* Elevator Functions *section to prevent cardholders from being located in the wrong APB area.*
>
> *If this option is selected, and the cardholder presents his/her card at a reader without using the elevator, the system will assume the cardholder has entered the new area and will not grant access at the same reader again unless the* Delay *time has expired.*

7. **Click** OK to save the settings.
8. **Create** an Access Level for the APB elevator.

   See Chapter 6 for access level information.

9. **Assign** cardholders to the access level.

   See page 7-13 for more information on assigning access levels.

Anti Pass-Back Features

DNA Fusion offers a number of features for access areas and anti-pass back settings.

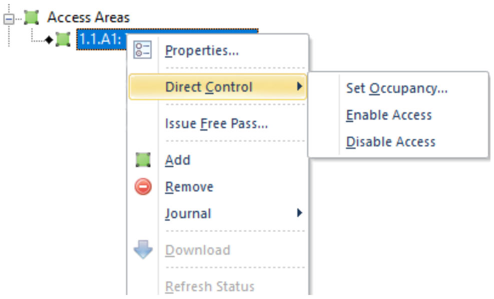
Enable/Disable an Area

Enabling and disabling an Access Area allows the system operator to quickly control access to the area.

1. **Expand** the Hardware Browser to view Access Areas.
2. **Right-click** on the Access Area and **select** Direct Control / Enable Access.

   Or

3. **Right-click** on the Access Area and **select** Direct Control / Disable Access.
   - Disable - Deactivates the area; cardholders will receive an Access Denied: Area Disabled event.
   - Enable - Activates the area; cardholders will have access based on their assigned Access Level and the Access Areas Occupancy Settings.

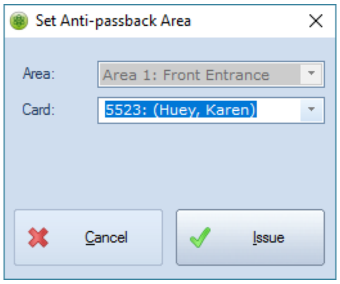


Issue Free Pass

Operators can issue a Free Pass for a card after an APB infraction to allow the cardholder to exit the area.

1. **Expand** the Hardware Browser to view Access Areas.
2. **Right-click** on the Access Area and **select** Issue Free Pass.

   The Set Anti-Pass Back Area dialog opens.



Area: Area 1: Front Entrance

Card: 5523: (Huey, Karen)

3. **Select** the Card from the drop-down list.
4. **Click** Issue.

   The free pass is applied to the selected cardholder.

> *A* Free Pass *can also be issued from the* Personnel Browser *by* **right-clicking** *on the cardholder's* Card *and* **selecting** Direct Control / Issue Free Pass*.*

This Page Intentionally Left Blank

Secured Areas 12

In This Chapter

Secured Areas are areas that can be armed and disarmed using a PIN code. Secured areas must be set up with an RSC-DT Keypad Reader. If a reader with a keypad is used, the display text functionality for the keypad will be negated.

Creating a secured area in DNA Fusion involves four steps:

1. Create the Monitor Point Group (MPG)
2. Make the MPG a secured area
3. Build triggers and macros
4. Configure the hardware

Creating a Secured Area

Setting Up the MPG

The MPGs *option must be checked in the* Hardware Tree Behavior *dialog for* MPG *objects to be visible in the* Hardware Browser. *See page 3-27 for more information.*

1. **Right-click** on the Controller in the Hardware Browser and **select** Add / Add MPG.

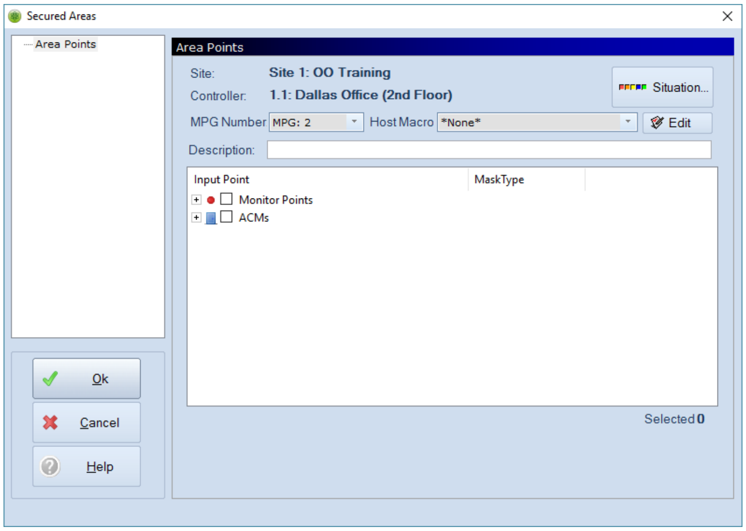
   Or

   Right-click on the MPGs object in the Hardware Browser and **select** Add MPG.

   Or

   Select Hardware / Add / MPG from the Main Menu.

   The Area Points dialog appears.



Secured Areas

Area Points

Site: Site 1: OO Training

Controller: 1.1: Dallas Office (2nd Floor)

MPG Number MPG: 2 Host Macro *None*

Description:

Input Point	MaskType
□ Monitor Points	
□ ACMs	

Selected 0

2. If desired, **select** an MPG Number from the drop-down list.

   The number is an arbitrary designation for the given secured area.

3. If desired, **select** a Host Macro from the drop-down to associate with the area.

   See page 10-13 for more information.

4. **Enter** a Description for the area.

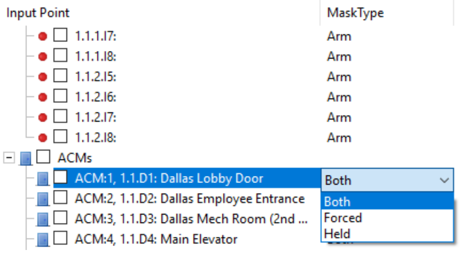
5. If desired, **enable** Situation Manager by **selecting** the Situations... button.

   See page 9-6 for more information.

6. In the Input Point column, **expand** the trees and **select** the desired Monitor Points and/or ACMs.

   ACMs are the keypads as well as any doors you want to control with the Secured Area.

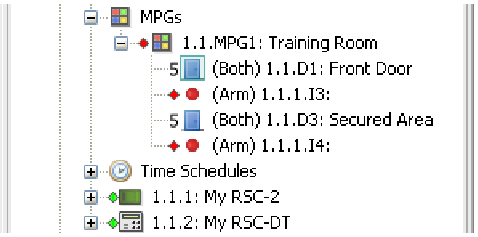
7. If desired, **select** a MaskType for each ACM point from the drop-down menu: Both, Forced, or Held.



Input Point	MaskType
● □ 1.1.1.I7:	Arm
● □ 1.1.1.I8:	Arm
● □ 1.1.2.I5:	Arm
● □ 1.1.2.I6:	Arm
● □ 1.1.2.I7:	Arm
● □ 1.1.2.I8:	Arm
□ ACMs	
□ ACM:1, 1.1.D1: Dallas Lobby Door	Both
□ ACM:2, 1.1.D2: Dallas Employee Entrance	Both
□ ACM:3, 1.1.D3: Dallas Mech Room (2nd ...	Forced
□ ACM:4, 1.1.D4: Main Elevator	Held

8. **Click** OK to save the Secured Area.

   The area appears in the Hardware Browser under MPGs.

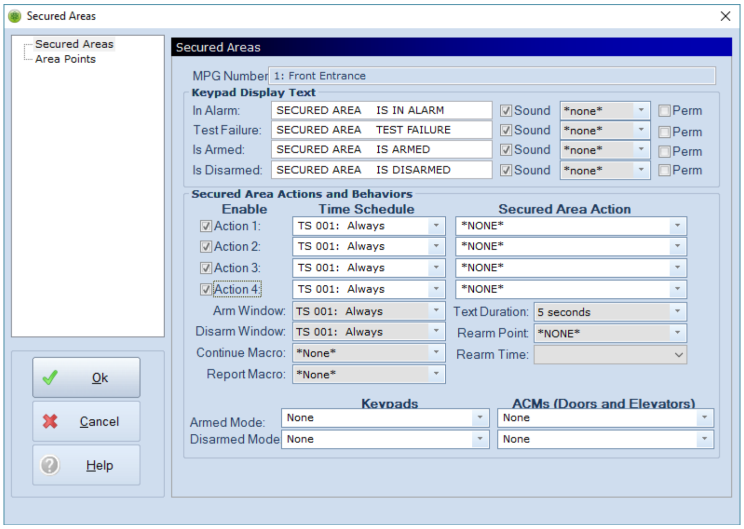


MPGs
1.1.MPG1: Training Room
5 (Both) 1.1.D1: Front Door
(Arm) 1.1.1.I3:
5 (Both) 1.1.D3: Secured Area
(Arm) 1.1.1.I4:
Time Schedules
1.1.1: My RSC-2
1.1.2: My RSC-DT

Setting Up the Secured Area

1. **Right-click** on the MPG and **select** Make Secured Area from the context menu.

   The Secured Areas dialog opens.



Secured Areas

MPG Number: 1: Front Entrance

Keypad Display Text

In Alarm:	SECURED AREA IS IN ALARM	☑ Sound	*none*	☐ Perm
Test Failure:	SECURED AREA TEST FAILURE	☑ Sound	*none*	☐ Perm
Is Armed:	SECURED AREA IS ARMED	☑ Sound	*none*	☐ Perm
Is Disarmed:	SECURED AREA IS DISARMED	☑ Sound	*none*	☐ Perm

Secured Area Actions and Behaviors

Enable	Time Schedule	Secured Area Action
☑ Action 1:	TS 001: Always	*NONE*
☑ Action 2:	TS 001: Always	*NONE*
☑ Action 3:	TS 001: Always	*NONE*
☑ Action 4:	TS 001: Always	*NONE*

Arm Window: TS 001: Always — Text Duration: 5 seconds

Disarm Window: TS 001: Always — Rearm Point: *NONE*

Continue Macro: *None* — Rearm Time:

Report Macro: *None*

	Keypads	ACMs (Doors and Elevators)
Armed Mode:	None	None
Disarmed Mode	None	None

> *Only* MPGs *that have a keypad reader associated with them will be promoted to* Secured Areas*. See page 12-9 for secured areas hardware configuration information.*

2. **Populate** the appropriate fields to configure the secured area settings.

Secured Areas

Identification

- MPG Number - Number and user-defined description of the MPG. (Auto-populated)

Keypad Display Text

- In Alarm - Editable text that will appear in the keypad display when the area is in alarm.
- Test Failure - Editable text that will appear in the keypad display upon test failure.
- Is Armed - Editable text that will appear in the keypad display when the area is armed.
- Is Disarmed - Editable text that will appear in the keypad display when the area is disarmed.
- Sound - If checked, the designated event will generate a sound. Select the sound type from the drop-down list.
- Perm - Designates whether the text is permanent or temporary.

Secured Area Actions and Behaviors

This section allows for indirect control of the Secured Area, such as arming and disarming. There must be a Time Schedule available to associate with the event. The control portion of the action will occur when the assigned time schedule is activated.

- Action 1 - 4 - **Select** a Time Schedule and a Secured Area Action. If selected, the area will automatically assume the specified action when the associated time schedule becomes active.
  - Conditionally Arm Area - Arms the area; all zones must be inactive.
  - Disarm Area - Disarms the area and masks all the points in the group.
  - Force Arm Area - Arms the area even if there are active zones.
- Arm Window - **Select** a Time Schedule to associate with the arm window. If the area is not armed by the specified time, an event will be generated.
- Disarm Window - **Select** a Time Schedule to associate with the disarm window. If the area is not disarmed by the specified time, an event will be generated.
- Continue Macro - **Select** a Macro from the drop-down list.

- Text Duration - **Select** the Duration for temporary text to remain on the keypad display (Default = 5 seconds).
- Rearm Point - **Select** an Input from the drop-down list.
- Rearm Time - **Select** a Duration from the drop-down list.
- Keypads: Armed Mode - Defines the keypad mode when the area is armed.
- Keypads: Disarmed Mode - Defines the keypad mode when the area is disarmed.
- ACMs: Armed Mode - Defines the ACM mode when the area is armed.
- ACMs: Disarmed Mode - Defines the ACM mode when the area is disarmed .

Area Points

This dialog allows you to associate different types of hardware with the Secured Area. By default, the points that were associated with the MPG will automatically be assigned to the Secured Area. However, you can add others based on the desired functionality.

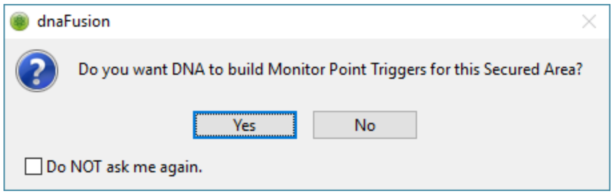
- Site - Number and description of the site. (Auto-populated)
- Controller - Address and description of the controller. (Auto-populated)
- MPG Number - Number of the MPG. (Auto-populated)
- Host Macro - Drop-down to select a Host Based Macro to associated with the area.
- Description - Description created during MPG setup . (Auto-populated)
- Input Explorer - Available Monitor Points, ACMs and Control Points.

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

   This will begin the process of building the Macros that control the Secured Area.

4. When prompted to download the information, **click** Yes.

   A confirmation dialog will appear.



dnaFusion

Do you want DNA to build Monitor Point Triggers for this Secured Area?

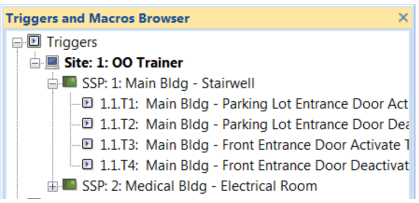
□ Do NOT ask me again.

5. **Click** Yes to build the associated triggers.

   This builds a trigger for each Monitor Point associated with the area that will activate the alarm text.

Building Arm/Disarm Triggers

The next step is to create the triggers that will arm and disarm the designated Secured Area based on card access. If Actions 1-4 were configured in the Secured Areas Actions & Behaviors section, the area may arm and disarm based on a time schedule as well. For more information on triggers, see Chapter 10: Triggers & Macros.

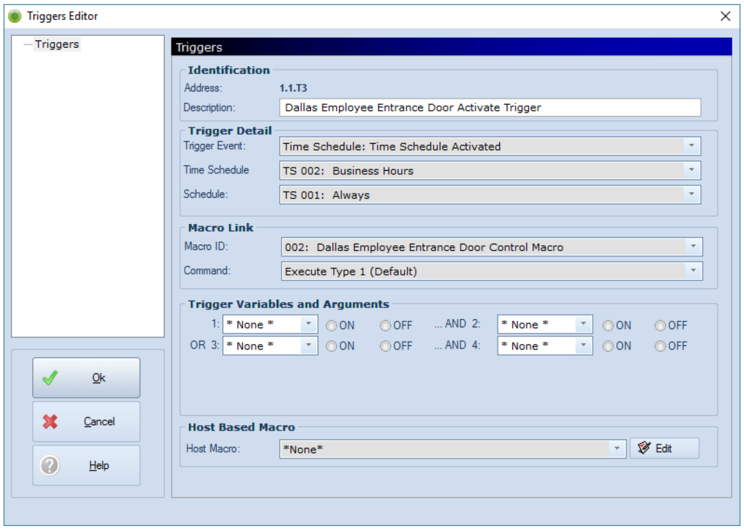


Triggers and Macros Browser

- Triggers
  - Site: 1: OO Trainer
    - SSP: 1: Main Bldg - Stairwell
      - 1.1.T1: Main Bldg - Parking Lot Entrance Door Act
      - 1.1.T2: Main Bldg - Parking Lot Entrance Door Dea
      - 1.1.T3: Main Bldg - Front Entrance Door Activate T
      - 1.1.T4: Main Bldg - Front Entrance Door Deactivat
    - SSP: 2: Medical Bldg - Electrical Room

1. **Open** the Triggers and Macros Browser and **expand** the Triggers tree to the appropriate controller.
2. **Right-click** on the Controller and **select** Add Trigger from the menu.

   The Triggers Editor dialog opens.



Triggers

Identification

Address: 1.1.T3

Description: Dallas Employee Entrance Door Activate Trigger

Trigger Detail

Trigger Event: Time Schedule: Time Schedule Activated

Time Schedule: TS 002: Business Hours

Schedule: TS 001: Always

Macro Link

Macro ID: 002: Dallas Employee Entrance Door Control Macro

Command: Execute Type 1 (Default)

Trigger Variables and Arguments

1: * None * ○ON ○OFF ... AND 2: * None * ○ON ○OFF

OR 3: * None * ○ON ○OFF ... AND 4: * None * ○ON ○OFF

Host Based Macro

Host Macro: *None*

3. **Configure** the following parameters:

Arm the System (Trigger #1)

- Description - **Enter** a description for the trigger. (Example: Training Room Arm)
- Trigger Event - **Select** Door: Access Granted from the drop-down list. It is possible to choose other events, however this option is used to control the Secured Areas from the keypad reader.
- Doors - **Select** the desired ACM from the drop-down list.
- Schedule - **Select** the desired Time Schedule from the drop-down list. The area will be armed when this schedule is active.
- Macro ID - **Select** the correct Macro (SA) from the drop-down list. This macro was created when the secured area was built. The address of the macro will be different, but the description will be followed by '-SA.'
- Command - **Select** Execute Type 1 (Default) from the drop-down list.
- Operation - **Select** Ignore Trigger Codes from the drop-down list.
- Trigger Variables - Variable 1 = OFF

  Set based on the Trigger Variable in the linked Macro. Generally, when the Secured Area is created, it will associate the Trigger Variable number to the number of the Secured Area. (Example: SA #1 macro will control Trigger Variable #1)

Disarm the System (Trigger #2)

- Description - **Enter** a description for the trigger. (Example: Training Room Disarm)
- Trigger Event - **Select** Door: Access Granted. It is possible to choose other events, however this option is used to control the Secured Areas from the keypad reader.
- Doors - **Select** the desired ACM from the drop-down list.
- Schedule - **Select** the desired Time Schedule from the drop-down list. The area will be disarmed when this schedule is active.

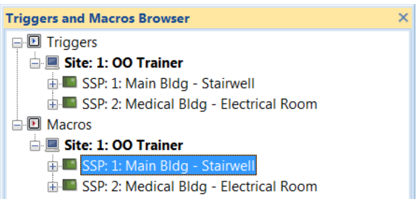
- Macro ID - **Select** the correct Macro (SA) from the drop-down list. This macro was created when the secured area was built. The address of the macro will be different, but the description will be followed by '-SA.'
- Command - **Select** Execute Type 2.
- Operation - **Select** Ignore Trigger Codes.
- Trigger Variables - Variable 1 = ON

4. **Click** OK.

> *It is recommended that the above steps be completed for each* Secured Area *before continuing. This will keep the* Arm/Disarm Triggers & Macros *grouped together for easier identification in the* Triggers and Macros Browser*.*

Building a Chime Macro & Trigger

A macro can be built to create an entry delay that will make the keypad beep for a specified amount of time to remind the user to disarm the system.

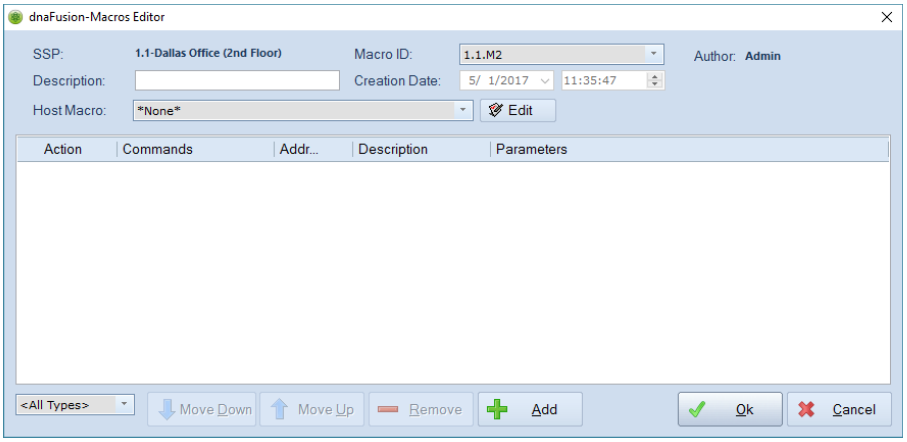


Triggers and Macros Browser

- Triggers
  - Site: 1: OO Trainer
    - SSP: 1: Main Bldg - Stairwell
    - SSP: 2: Medical Bldg - Electrical Room
- Macros
  - Site: 1: OO Trainer
    - SSP: 1: Main Bldg - Stairwell
    - SSP: 2: Medical Bldg - Electrical Room

1. In the Triggers and Macros Browser, **expand** the Macros tree down to the appropriate Controller.
2. **Right-click** on the Controller and **select** Add Macro from the context menu.

   The Macros Editor dialog opens.



dnaFusion-Macros Editor

SSP: 1.1-Dallas Office (2nd Floor)

Macro ID: 1.1.M2

Author: Admin

Description:

Creation Date: 5/ 1/2017 11:35:47

Host Macro: *None*

Action	Commands	Addr...	Description	Parameters

3. **Enter** a Description.
4. **Click** OK.

Adding Macro Commands

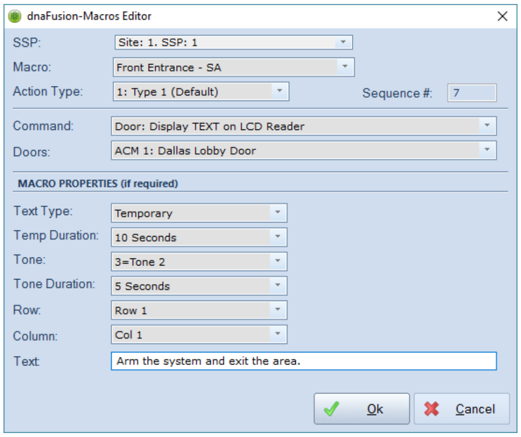
1. **Right-click** on the newly created Macro and **select** Macro Commands / Add Command.

   Or

   From the Macros Editor dialog, **click** the Add button.

   The Macros Command Editor appears.

2. **Configure** the following parameters to enable the keypad tone that will sound for the designated entry point until the Secured Area is disarmed.
   - Action Type - **Select** Type 1 (Default) from the drop-down list.
   - Command - **Select** Door: Display TEXT on LCD Reader from the drop-down list.
   - ACM (Access Control Model) - **Select** the desired ACM from the drop-down list.
   - Text Type - **Select** Temporary from the drop-down list.
   - Temp Duration - **Select** the Duration for temporary text from the drop-down list.
   - Tone - **Select** the Tone from the drop-down list.
   - Tone Duration - **Select** the Tone Duration from the drop-down list.
   - Row - If desired, **select** the Row from the drop-down list to display the text.
   - Column - If desired, **select** the Column from the drop-down list to display the text.
   - Text - **Enter** the desired Text to display on the keypad screen.



dnaFusion-Macros Editor

SSP: Site: 1. SSP: 1

Macro: Front Entrance - SA

Action Type: 1: Type 1 (Default)

Sequence #: 7

Command: Door: Display TEXT on LCD Reader

Doors: ACM 1: Dallas Lobby Door

MACRO PROPERTIES (if required)

Text Type: Temporary

Temp Duration: 10 Seconds

Tone: 3=Tone 2

Tone Duration: 5 Seconds

Row: Row 1

Column: Col 1

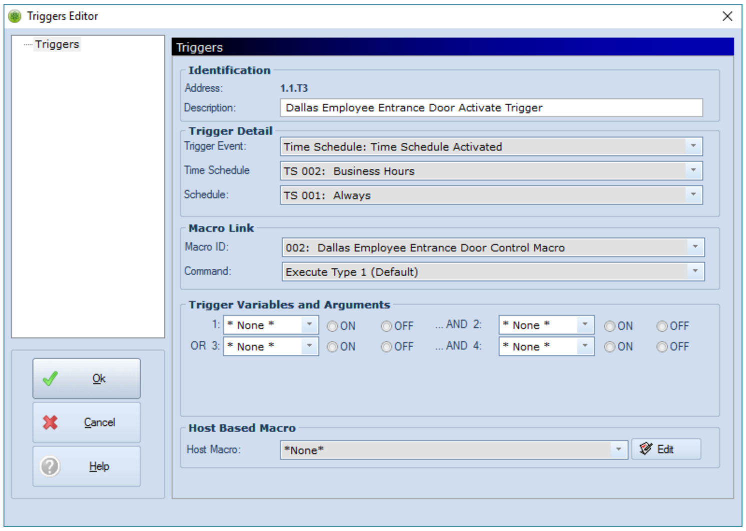
Text: Arm the system and exit the area.

3. **Click** OK.

Creating the Chime Trigger

1. In the Triggers & Macros Browser, **expand** the Trigger tree to the appropriate Controller.
2. **Right-click** on the Controller and **select** Add Trigger from the context menu.

   The Triggers Editor dialog opens.



Triggers Editor

Triggers

Identification

Address: 1.1.T3

Description: Dallas Employee Entrance Door Activate Trigger

Trigger Detail

Trigger Event: Time Schedule: Time Schedule Activated

Time Schedule: TS 002: Business Hours

Schedule: TS 001: Always

Macro Link

Macro ID: 002: Dallas Employee Entrance Door Control Macro

Command: Execute Type 1 (Default)

Trigger Variables and Arguments

1: * None * ○ ON ○ OFF ... AND 2: * None * ○ ON ○ OFF

OR 3: * None * ○ ON ○ OFF ... AND 4: * None * ○ ON ○ OFF

Host Based Macro

Host Macro: *None*

3. **Configure** the following parameters:
   - Description - **Enter** a description for the chime trigger. (Example: Training Room Chime)
   - Trigger Event - **Select** MP: Entry Delay in Progress from the drop-down list.
   - Monitor Point - **Select** the Monitor Point from the drop-down list. The address will be different based on the SSP number and the point designated as the Entry Point.
   - Schedule - **Select** the desired Time Schedule from the drop-down list. The chime will only sound when the time schedule is active.
   - Macro ID - **Select** the appropriate Macro from the drop-down list.

     This is the macro that was created on page 12-7.
   - Command - **Select** Execute Type 1 (Default) from the drop-down list.
4. **Click** OK.

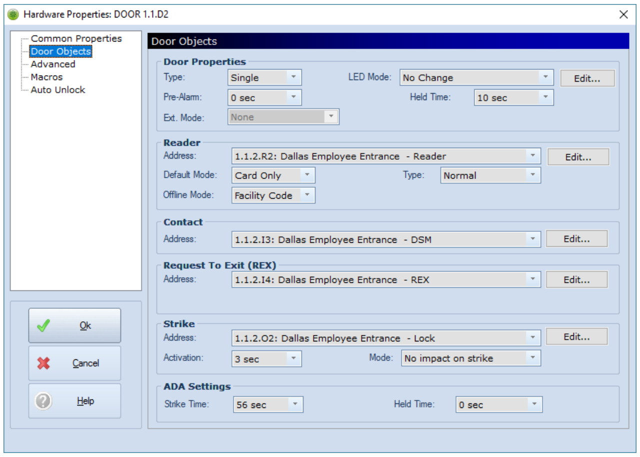
> *It is recommended that the above steps be completed for each keypad that needs to "countdown" the entry delay.*

Hardware Configuration

In order for the keypad to function properly, you will need to make some changes to the hardware properties.

Doors and Readers

1. **Right-click** on the Door with the keypad and **select** Properties.
   The Door Properties dialog opens.
2. **Select** Door Objects from the dialog menu.



Hardware Properties: DOOR 1.1.D2

Door Objects

Door Properties
Type: Single
LED Mode: No Change
Pre-Alarm: 0 sec
Held Time: 10 sec
Ext. Mode: None

Reader
Address: 1.1.2.R2: Dallas Employee Entrance - Reader
Default Mode: Card Only
Type: Normal
Offline Mode: Facility Code

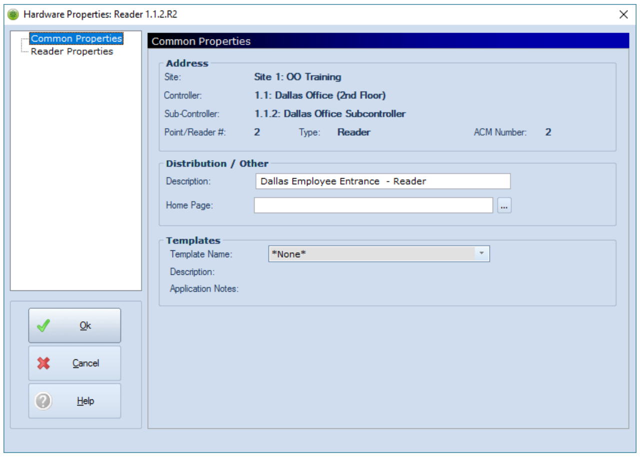
Contact
Address: 1.1.2.I3: Dallas Employee Entrance - DSM

Request To Exit (REX)
Address: 1.1.2.I4: Dallas Employee Entrance - REX

Strike
Address: 1.1.2.O2: Dallas Employee Entrance - Lock
Activation: 3 sec
Mode: No impact on strike

ADA Settings
Strike Time: 56 sec
Held Time: 0 sec

3. **Set** the Default Mode to PIN or Card.
4. **Select** the desired Offline Mode from the drop-down:
   - None - No reader is associated with the door.
   - Disabled - Disables the reader; the door remains locked with no REX capability.
   - Unlocked - Unrestricted access; the door remains unlocked.
   - Locked - Access is not authorized; the door remains locked with REX capability.
   - Facility Code - Access is authorized if a correct facility code is used.
5. **Set** the Reader Type to Text Keypad.
6. **Click** the Edit button in the Reader section.
   The Reader Properties dialog appears.
7. **Select** Common Properties from the dialog menu.



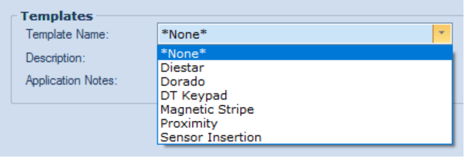
Hardware Properties: Reader 1.1.2.R2

Common Properties

Address
Site: Site 1: OO Training
Controller: 1.1: Dallas Office (2nd Floor)
Sub-Controller: 1.1.2: Dallas Office Subcontroller
Point/Reader #: 2 Type: Reader ACM Number: 2

Distribution / Other
Description: Dallas Employee Entrance - Reader
Home Page:

Templates
Template Name: *None*
Description:
Application Notes:



Templates
Template Name: *None*
Description:
Application Notes:

8. In the Templates section, **select** DT Keypad from the Template Name drop-down menu.
   Selecting this template will populate the reader properties needed for keypad functionality.
9. **Click** OK to save the settings.
   A download confirmation dialog will appear.
10. **Click** Yes to download.

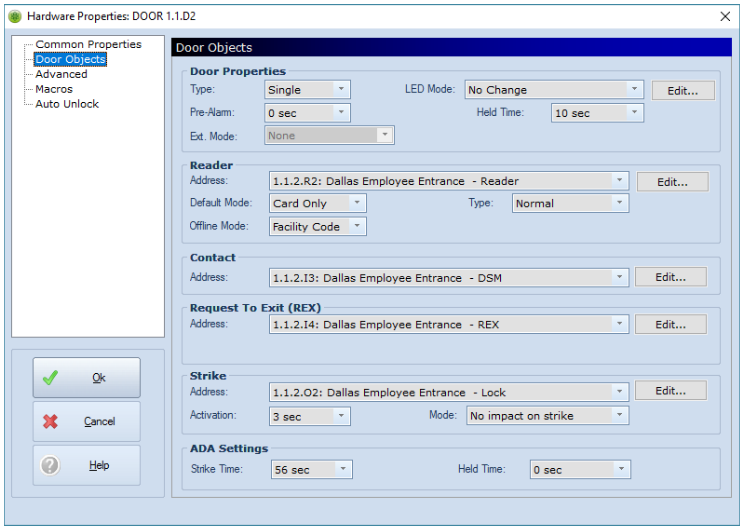
Setting Entry & Exit Delays

Entry and exit delays are easily accessed from within the Door Properties dialog.

1. **Right-click** on the Door with the keypad and **select** Properties.

   The Door Properties dialog opens.

2. **Select** Door Objects from the dialog menu.



Hardware Properties: DOOR 1.1.D2

- Common Properties
- Door Objects
- Advanced
- Macros
- Auto Unlock

Ok
Cancel
Help

Door Objects

Door Properties

Type: Single
LED Mode: No Change
Pre-Alarm: 0 sec
Held Time: 10 sec
Ext. Mode: None

Reader

Address: 1.1.2.R2: Dallas Employee Entrance - Reader
Default Mode: Card Only
Type: Normal
Offline Mode: Facility Code

Contact

Address: 1.1.2.I3: Dallas Employee Entrance - DSM

Request To Exit (REX)

Address: 1.1.2.I4: Dallas Employee Entrance - REX

Strike

Address: 1.1.2.O2: Dallas Employee Entrance - Lock
Activation: 3 sec
Mode: No impact on strike

ADA Settings

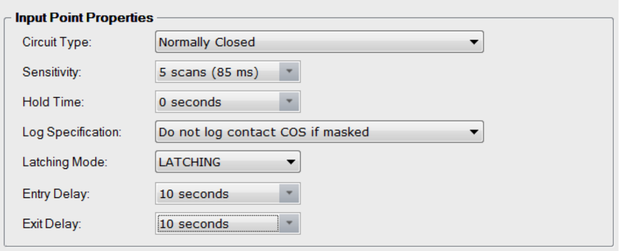
Strike Time: 56 sec
Held Time: 0 sec

3. **Click** the Edit button in the Contact section.

   The Input Properties dialog appears.

4. **Select** Input Properties from the dialog menu.

5. In the Input Point Properties section, **configure** the Latching Mode using the information below:



Input Point Properties

Circuit Type: Normally Closed
Sensitivity: 5 scans (85 ms)
Hold Time: 0 seconds
Log Specification: Do not log contact COS if masked
Latching Mode: LATCHING
Entry Delay: 10 seconds
Exit Delay: 10 seconds

- Latching Mode - Specifies the type of latching mode. Only used to configure entry and exit delays common with secured areas.
  - Normal - Select this option when no entry or exit delay is used.
  - Non-Latching - Generates an alarm if the point is still in alarm status after the entry time has expired. If the door is opened and immediately closed (within the entry delay), an alarm will not be generated. An event will be logged when the change of state happens, but no alarm would be received.
  - Latching - Generates an alarm when the door is opened (regardless of whether the door is shut again) unless the point is masked within the entry delay time. This is the recommended setting.
- 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.
- 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 armed.

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

7. **Click** the Edit button in the Request to Exit (REX) section and **configure** the Input Point Properties as shown in Step 5.

8. **Click** OK to save the changes to the Door Properties.

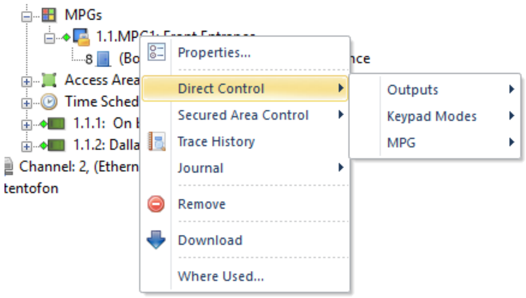
Controlling Secured Areas

DNA Fusion allows the operator to perform direct tasks on a selected secured area. There are three types of control for the secured area:

- Secured Area Direct Control - Controls outputs, keypads modes, and MPGs.
- Secured Area Control - Arms, disarms, and conditionally arms the area.
- Object Direct Control - Controls a secured area's associated hardware objects. For more information on controlling hardware, see Chapter 8.

Secured Area Direct Control

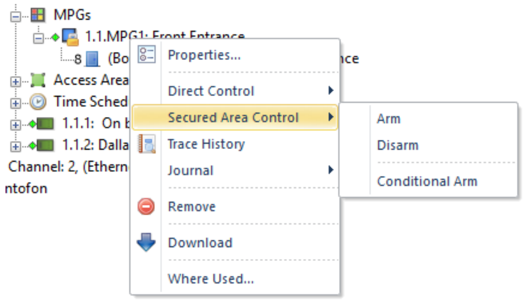
1. **Right-click** on the Secured Area (under MPGs) in the Hardware Browser and **select** Direct Control.



- Outputs:
  - □ Activate - Activates the selected output point.
  - □ Deactivate - Deactivates the selected output point.
- Keypad Modes:
  - □ Armed - Arms the secured area.
  - □ Disarmed - Disarms the secured area.
- MPG:
  - □ Arm - Arms the MPG.
  - □ Disarm - Disarms the MPG.
  - □ Access - If no points are masked, the secured area will allow access.
  - □ Forced ARM - Arms the secured area even if one or more areas are faulted.
  - □ Standard Arm - Arms the secured area if no points are active.
  - □ Override Arm - Arms the secured area and overrides any faulted areas.

Secured Area Control

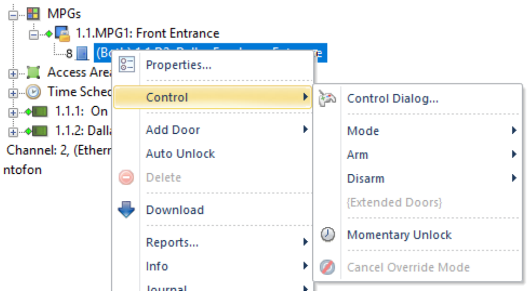
1. **Right-click** on the Secured Area (under MPGs) in the Hardware Browser and **select** Secured Area Control.



- Arm - Arms the secured area.
- Disarm - Disarms the secured area .
- Conditional Arm - Conditionally arms the secured area.

Object Direct Control

1. **Right-click** on the hardware object under the Secured Area in the Hardware Browser and **select** Control / Direct Control. See Chapter 8 for more information on controlling hardware.



- Control Dialog - Opens the Direct Control Dialog for the selected object.
- Mode - Changes the object's mode.
- Arm: Forced / Held - Arms the Forced or Held door conditions.
- Disarm: Forced / Held - Masks the Forced or Held door conditions.
- Momentary Unlock - Unlocks the door for the programmed strike time.
- Cancel Override Mode - Cancels the temporary door override mode.

NOTES:

Keypad Commands

Keypad commands can be programmed to allow the user to control hardware objects from the keypad.

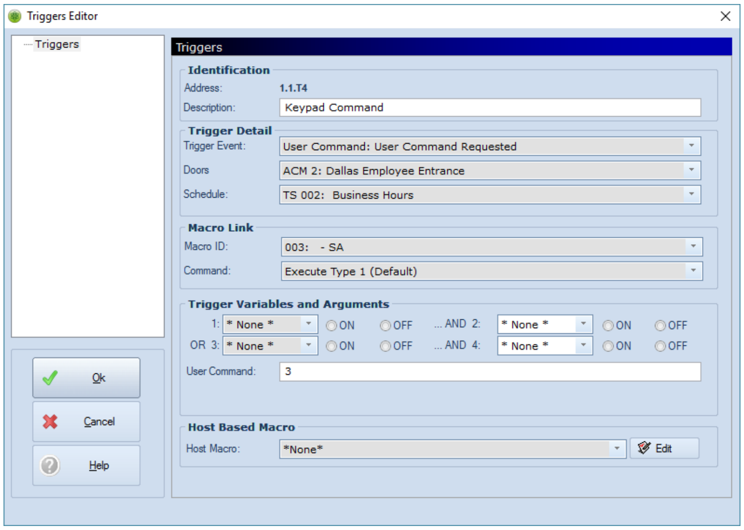
Adding Commands

1. **Create** a Macro to execute the desired commands.

   For more information on creating macros, see page 10-1.

2. **Create** a Trigger and **select** User Command: User Command Requested for the Trigger Event.

   The User Command field appears. For more information on creating triggers, see page 10-7.



Identification

Address: 1.1.T4

Description: Keypad Command

Trigger Detail

Trigger Event: User Command: User Command Requested

Doors ACM 2: Dallas Employee Entrance

Schedule: TS 002: Business Hours

Macro Link

Macro ID: 003: - SA

Command: Execute Type 1 (Default)

Trigger Variables and Arguments

1: * None * ○ON ○OFF ... AND 2: * None * ○ON ○OFF

OR 3: * None * ○ON ○OFF ... AND 4: * None * ○ON ○OFF

User Command: 3

Host Based Macro

Host Macro: *None*

3. **Select** a Door to associate with the trigger.
4. **Select** a Schedule to associate with the trigger.
5. **Select** the Macro created in Step 1.
6. **Enter** the numerical keypad code in the User Command field.

   This number will execute the macro when entered on the keypad.

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

Executing Keypad Commands

To execute a keypad command:

1. **Press** the Command button.
2. **Enter** the keypad command code created in Step 6 above.
3. **Press** the Command button again.

   The command is executed.

Basic Keypad Operation

Arming the System

Before arming the system, close all protected doors and windows, and stop movement in areas protected by motion detectors.

If the LED light is off, you have no AC power. Restore power if possible. If not, contact your installing company.

To arm the system:

1. **Enter** your Access Code and **press** the Command button on the keypad. As each digit is entered, the keypad sounder will beep.

   Your Access Code: ____________________

2. When the Access Code has been entered, the keypad display will read "Secured Area Is Armed" and the keypad will beep.

   If all the zones are not closed, "Secured Area Test Failure" will appear on the keypad display along with a list of points and their addresses.

3. If an incorrect Access Code is entered, the keypad display will read "Invalid".

   To correct a mistake when entering a code, press the Arrow key and **enter** the Access Code again.

4. When the keypad displays "Secured Area Is Armed", leave the premises before the Exit Delay expires.

   At the end of the Exit Delay, all lights on the keypad will be shut OFF; the system is now armed.

Disarming the System

Enter the premises through the designated entry or exit door. The keypad will sound a constant tone to indicate that the system must be disarmed.

To disarm the system:

1. **Enter** your Access Code and press the Command button on the keypad.

   If an error is made entering the code, press the Arrow key and **enter** the Code again.

2. When the correct Access Code is entered, the keypad display will read "Secured Area Is Disarmed", and the sounder will be silenced; your system is now disarmed.

   An Access Code must be entered before the Entry Delay expires or an alarm will occur.

   If an alarm occurred while the system was armed, the display will show "Secured Area Is In Alarm".

   Enter your Access Code to cancel the alarm and return the keypad back to "Ready" mode.

Tenants 13

In This Chapter

√ Enabling Tenants
√ Creating Tenant SSP Groups
√ Assigning Tenants to Operators
√ Assigning Cardholders to a Tenant

The Tenants feature allows for hardware and cardholders to be visually separate in DNA Fusion.

If configured, personnel, hardware, events, and alarms will only display for the assigned SSP controller(s). Users can assign tenant groups to specific operator profiles, which limits the operator's visibility and privileges in the system. For example, an operator can be restricted to a single controller or assigned privileges to all controllers and cardholders for a whole system view.

> *If the* Tenants *feature is enabled, operators will only be able to generate system reports for tenants assigned to their profile. See Chapter 17 for more information on reports.*

Setting Up Tenants

Each workstation must be configured for the Tenants function to work properly.

Enabling Tenants

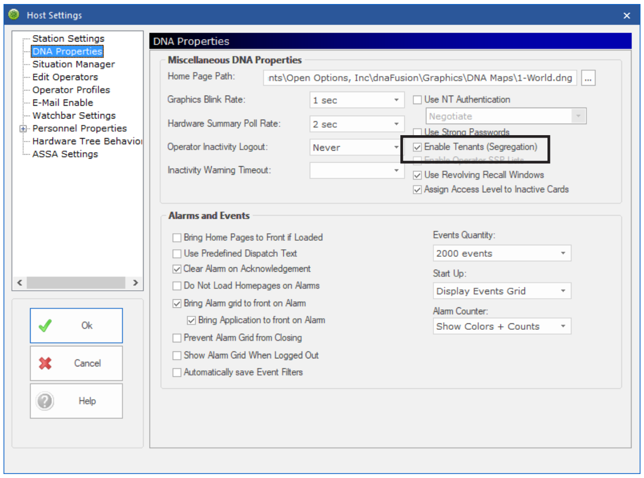
The Tenants setting in Host Settings must be enabled for the tenants options to be available.

1. **Select** DNA Properties from the Standard Toolbar.

   OR

   Select DNA / Administrative / Properties from the Main Menu.

2. In the DNA Properties dialog, **check** the Enable Tenants (Segregation) checkbox.



Miscellaneous DNA Properties

Home Page Path: nts\Open Options, Inc\dnaFusion\Graphics\DNA Maps\1-World.dng

Graphics Blink Rate: 1 sec

Hardware Summary Poll Rate: 2 sec

Operator Inactivity Logout: Never

Inactivity Warning Timeout:

□ Use NT Authentication

Negotiate

□ Use Strong Passwords

☑ Enable Tenants (Segregation)

□ Enable Operator SSP Lists

☑ Use Revolving Recall Windows

☑ Assign Access Level to Inactive Cards

Alarms and Events

□ Bring Home Pages to Front if Loaded

□ Use Predefined Dispatch Text

☑ Clear Alarm on Acknowledgement

□ Do Not Load Homepages on Alarms

☑ Bring Alarm grid to front on Alarm

☑ Bring Application to front on Alarm

□ Prevent Alarm Grid from Closing

□ Show Alarm Grid When Logged Out

□ Automatically save Event Filters

Events Quantity: 2000 events

Start Up: Display Events Grid

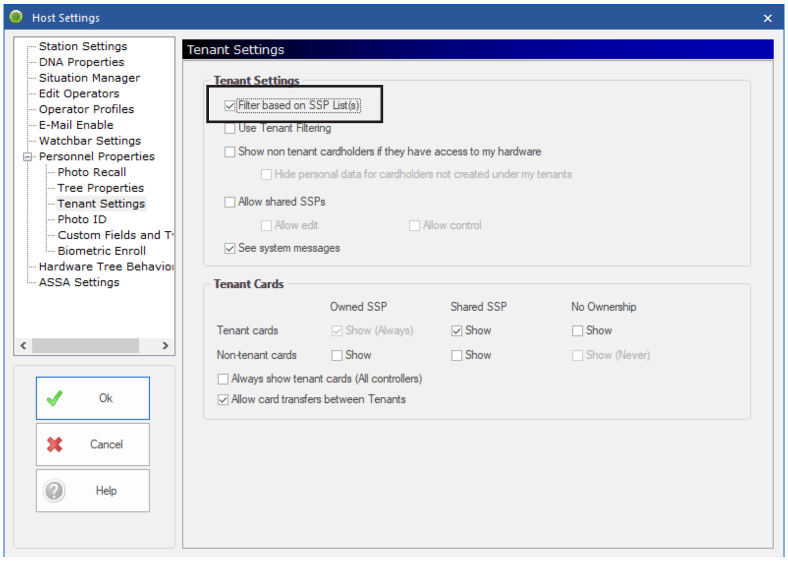
Alarm Counter: Show Colors + Counts

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

> *Beginning with version 7.0.0.45, the* DNA Indexing Utility *dialog prompts the operator to sync the database indexes when changing the tenant mode on the server.*

Filter on SSP List

1. **Select** Personnel Properties / Tenant Settings from the Host Settings dialog menu.



Tenant Settings

Tenant Settings

☑ Filter based on SSP List(s)

☐ Use Tenant Filtering

☐ Show non tenant cardholders if they have access to my hardware

☐ Hide personal data for cardholders not created under my tenants

☐ Allow shared SSPs

☐ Allow edit ☐ Allow control

☑ See system messages

Tenant Cards

	Owned SSP	Shared SSP	No Ownership
Tenant cards	☑ Show (Always)	☑ Show	☐ Show
Non-tenant cards	☐ Show	☐ Show	☐ Show (Never)

☐ Always show tenant cards (All controllers)

☑ Allow card transfers between Tenants

2. **Check** the Filter Based on SSP List(s) option.

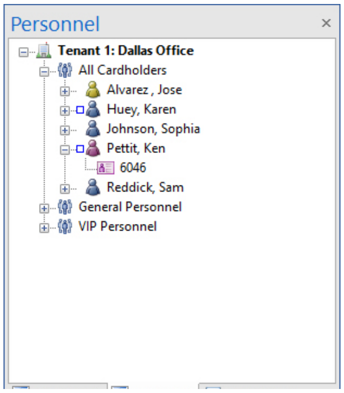
   This setting filters the events and hardware by SSP for the current tenant checked.

3. If desired, **configure** the remaining Tenant Settings:

   - Use Tenant Filtering - Check if Alarm Escalation and Event Filtering will be used in combination with tenants. See page 14-27 for more information.
   - Show non tenant cardholders if they have access to my hardware - Displays non-tenant activity in the Events Grid.
     - Hide personal data for cardholder not created under my tenants - Hides the cardholder's first and last names; only the card number will be visible.
   - Allow Shared SSPs - Allows tenants to share SSP controllers. This allows the system owner to share SSPs and/or control of the SSPs with this client.
     - Allow Edit - Allows the operator to edit configurable settings on shared SSPs.
     - Allow Control - Allows the operator to control hardware on shared SSPs.
   - See System Messages - Displays system messages for the operator on the active workstation.
   - Tenant Cards
     - Owned SSP: Show (Always) - Displays tenant cards on tenant SSPs. (Read-only; always enabled)
     - Shared SSP: Show - Displays tenant cards on shared SSPs.
     - No Ownership: Show - Displays tenant cards on SSPs other than tenants.
   - Non-Tenant Cards
     - Owned SSP: Show - Displays non-tenant cards on tenant SSPs.
     - Shared SSP: Show - Displays non-tenant cards on shared SSPs.
     - No Ownership: Show (Never) - Displays non-tenant cards on SSPs other than tenants. (Read only; always disabled)
   - Allow Shared SSPs - Allows SSPs to be shared between tenants. This allows the system owner to share SSPs and/or control of the SSPs with this client.
   - Always Show Tenant Cards (All Controllers) - Override button; enables all checkboxes on the Tenant Cards row regardless of their configuration.
   - Allow Card Transfers between Tenants - Allows a card to be assigned to another tenant on the system.

4. **Click** OK to save the settings.
5. **Restart** DNA Fusion.

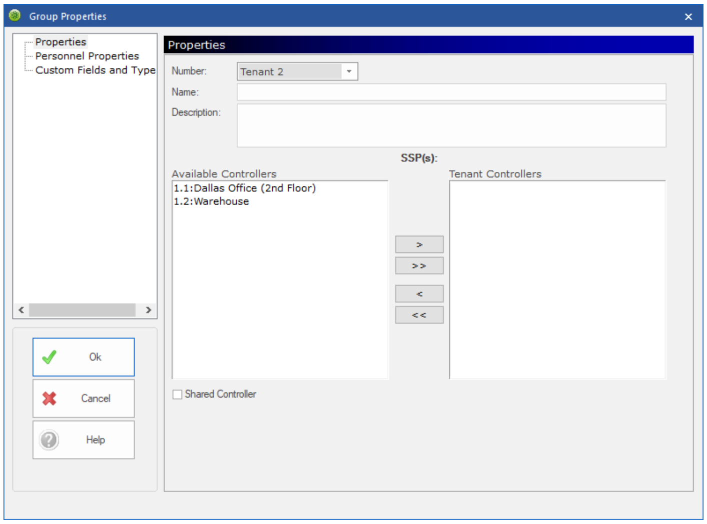
Creating Tenant SSP Groups



Tenant 1: Dallas Office
All Cardholders
Alvarez , Jose
Huey, Karen
Johnson, Sophia
Pettit, Ken
6046
Reddick, Sam
General Personnel
VIP Personnel

1. **Right-click** in the Personnel Browser and **select** Add Tenant.

   The Group Properties dialog opens.



Properties

Number: Tenant 2

Name:

Description:

SSP(s):

Available Controllers
1.1:Dallas Office (2nd Floor)
1.2:Warehouse

Tenant Controllers

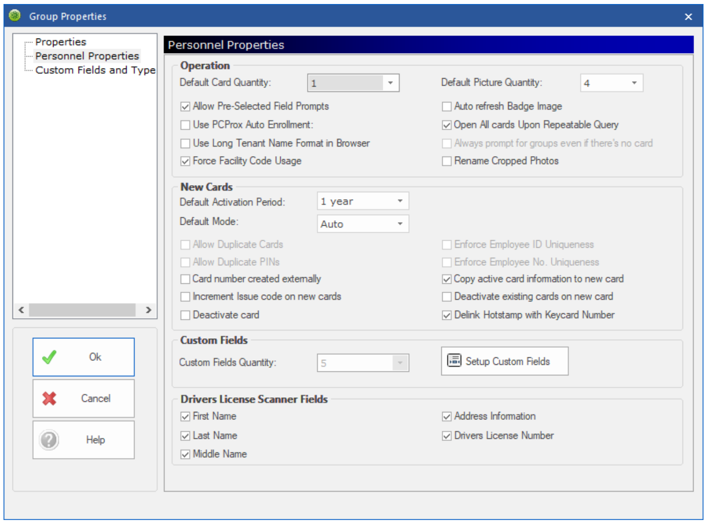
□ Shared Controller

2. **Enter** a Name and Description for the Tenant Group.
3. **Select** the SSP from the Available Controllers section and **click** the > button to add it to the Tenant Controllers section.

   If all Available Controllers are desired, **select** the >> button and all available controllers will move to the Tenant Controllers section.

   To remove controllers, **select** the < or << button.
4. If desired, **select** Personnel Properties from the Group Properties dialog menu.

   The Personnel Properties dialog opens.



Personnel Properties

Operation

Default Card Quantity: 1
Default Picture Quantity: 4

☑ Allow Pre-Selected Field Prompts
□ Use PCProx Auto Enrollment:
□ Use Long Tenant Name Format in Browser
☑ Force Facility Code Usage
□ Auto refresh Badge Image
☑ Open All cards Upon Repeatable Query
□ Always prompt for groups even if there's no card
□ Rename Cropped Photos

New Cards

Default Activation Period: 1 year
Default Mode: Auto

□ Allow Duplicate Cards
□ Allow Duplicate PINs
□ Card number created externally
□ Increment Issue code on new cards
□ Deactivate card
□ Enforce Employee ID Uniqueness
□ Enforce Employee No. Uniqueness
☑ Copy active card information to new card
□ Deactivate existing cards on new card
☑ Delink Hotstamp with Keycard Number

Custom Fields

Custom Fields Quantity: 5

Drivers License Scanner Fields

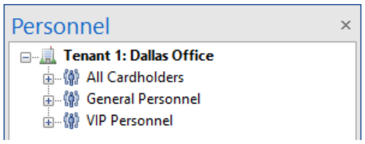
☑ First Name
☑ Last Name
☑ Middle Name
☑ Address Information
☑ Drivers License Number

5. **Configure** the Personnel Properties options.

   See page 3-15 for more information.
6. If desired, **select** Custom Fields and Types from the Group Properties dialog menu.
7. **Configure** the Custom Fields.

   See page 3-26 for more information.
8. **Click** OK to save the settings and add the Tenant to the Personnel Browser.

   To view tenants in the browser, the tenant must be selected in the Operator Profiles dialog. See page 4-5 for more information.



Tenant 1: Dallas Office
All Cardholders
General Personnel
VIP Personnel

NOTES:

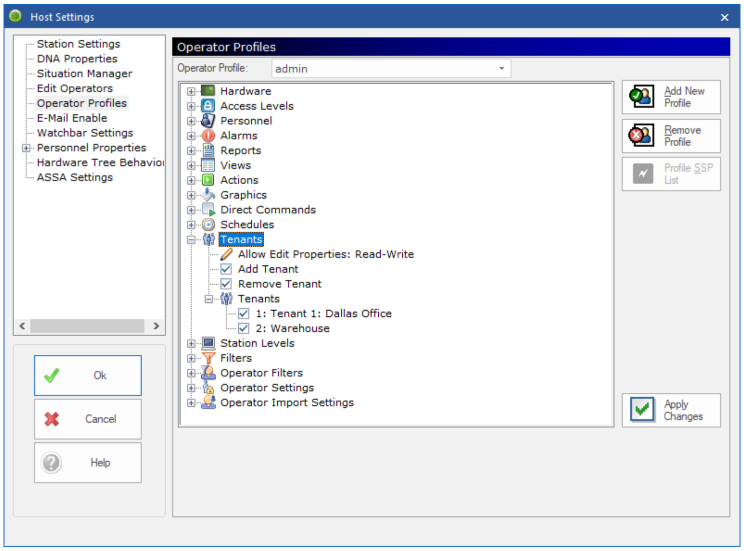
Assigning Tenants to Operators

Operator profiles must be created for each tenant group in order to restrict multi-tenant viewing.

> *At least one profile should have access to ALL* Tenant Groups*. See page 4-5 for more information on configuring operator privileges.*

1. **Select** the DNA Properties button on the Standard Toolbar.
2. **Select** Operator Profiles from the dialog menu.

   The Operator Profiles dialog opens.
3. **Select** the Operator Profile from the drop-down or **create** a new profile.
4. **Expand** the Tenants header.



Operator Profile: admin

Allow Edit Properties: Read-Write
☑ Add Tenant
☑ Remove Tenant
Tenants
☑ 1: Tenant 1: Dallas Office
☑ 2: Warehouse

5. **Expand** the Tenants sub-header.
6. **Select** the Tenant Group(s) to assign to the selected Operator Profile.
7. **Click** the Apply Changes button to save the settings.
8. **Click** OK.

   All operators assigned to the operator profile will have access to the selected Tenant Group(s), both in the Hardware Browser and the Personnel Browser.

> **Expand** *the Operator Settings and* **set** *the* DNA Administrator *option to* Regional *or* Local Level to prevent operators from viewing all tenants in a report*.*

> *Cardholders must be assigned to the* Tenant Group*. See page 13-7 for more information.*

NOTES:

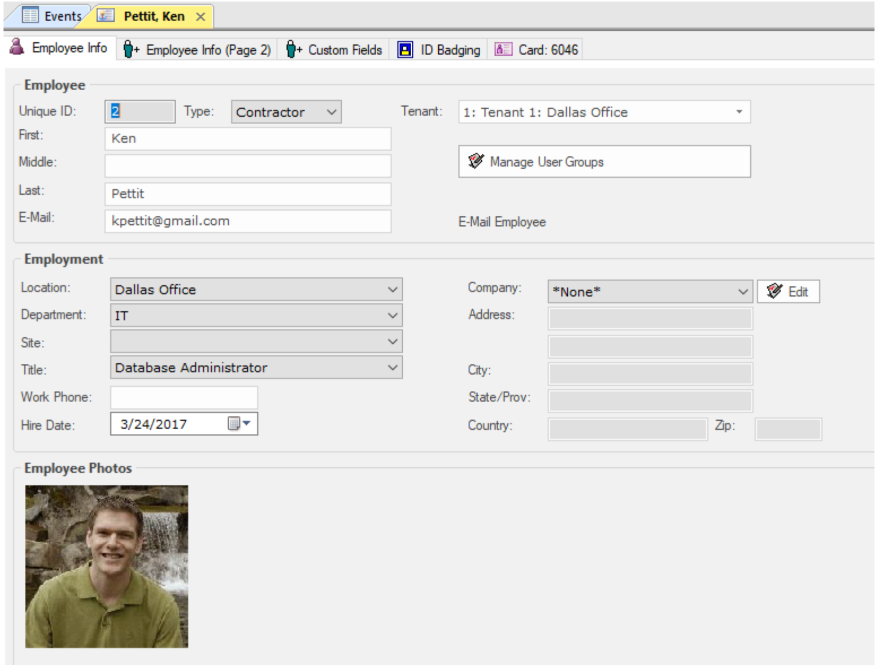
Assigning Cardholders to a Tenant

In order for a cardholder to appear in the correct tenant group, they must be assigned to the tenant when the cardholder is created or after the Tenants feature has been enabled.

1. **Select** the desired Tenant Group from the Personnel Browser and **open** a Personnel Record.

   See Chapter 7 for information on adding cardholders.

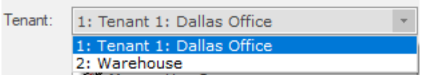
   > *If a specific tenant is assigned to the operator, new cardholders will automatically be added to the tenant group.*



Unique ID: 2 Type: Contractor Tenant: 1: Tenant 1: Dallas Office
First: Ken
Middle:
Last: Pettit
E-Mail: kpettit@gmail.com

Location: Dallas Office Company: *None*
Department: IT Address:
Site:
Title: Database Administrator City:
Work Phone: State/Prov:
Hire Date: 3/24/2017 Country: Zip:

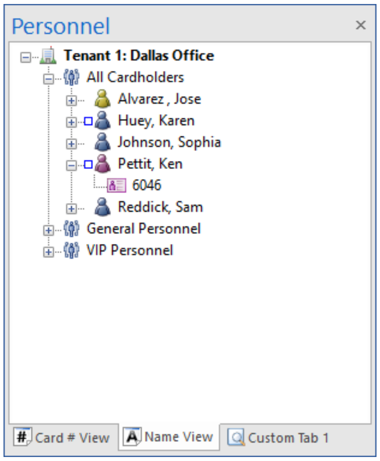
2. **Select** the desired Tenant from the drop-down.



Tenant: 1: Tenant 1: Dallas Office
1: Tenant 1: Dallas Office
2: Warehouse

3. **Enter** the remaining cardholder information.
4. **Right-click** in the Personnel Record and **select** Update to save the record.

   The record is added to the selected Tenant Group and is only visible to operators with the Tenant Group assigned to their profile.



NOTES:

Assigning Cardholder Access

In a Tenant environment, each operator can only see the hardware and access levels associated to their assigned Tenant. Access is assigned to cards in any of the methods outlined in the Personnel chapter on page 7-13.

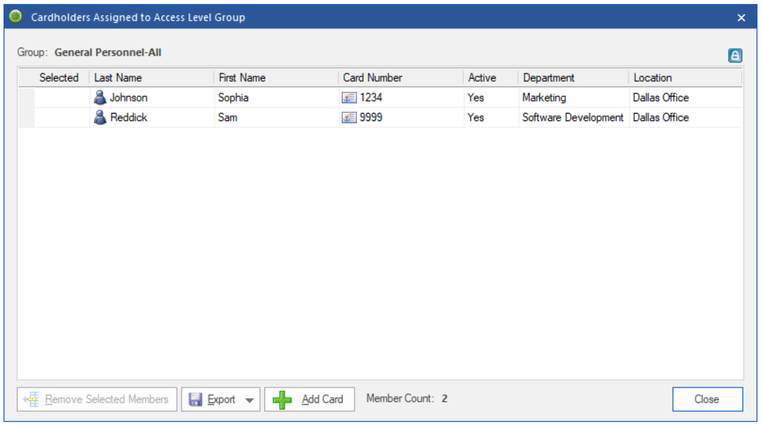
If an cardholder from another Tenant needs an access level that is not associated with their Tenant, an operator from the desired Tenant may use the Assigned To feature in the Access Level browser to provide the needed access level.

Adding an Access Level Via the Assigned To

The Assigned To feature is an InfoReady report that allows the operator to audit the cardholders assigned to a global or legacy access level group. It can also be used to add the access level group to selected cards.

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

   The Cardholders Assigned to Access Level Group dialog opens.



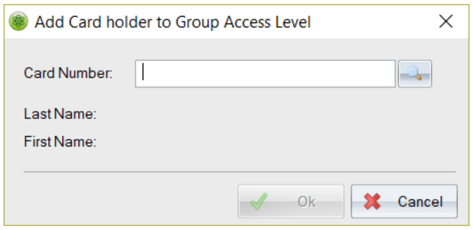
Group: General Personnel-All

Selected	Last Name	First Name	Card Number	Active	Department	Location
	Johnson	Sophia	1234	Yes	Marketing	Dallas Office
	Reddick	Sam	9999	Yes	Software Development	Dallas Office

Member Count: 2

2. **Select** the Add Card button.

   The Add Cardholder to Group Access Level dialog appears.



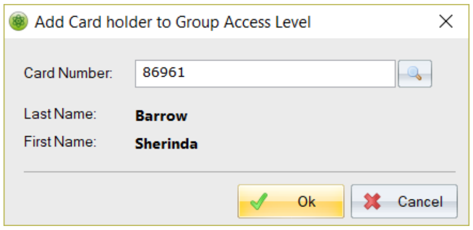
Card Number:

Last Name:

First Name:

3. **Enter** a Card Number and **select** the Search 🔍 button.

   If valid, the cardholder's First Name and Last Name will populate.



Card Number: 86961

Last Name: **Barrow**

First Name: **Sherinda**

4. **Click** OK to add the card to the Access Level Group.

   The card information is added to the Cardholders Assigned to Access Level Group dialog and the card receives all access levels included in the access level group.

This Page Intentionally Left Blank

Events & Alarms 14

In This Chapter

- √ Using the Events Grid
- √ Access Denied Codes
- √ Handling Alarms
- √ Controlling Hardware from the Alarm Grid
- √ Configuring Logging for Events & Alarms

The Events and Alarm Grids are data windows that contain system information and allow the user to monitor real-time conditions of the physical environment as well as review a history of system events.

The data windows can be closed by clicking the X button in the data window tab, which will appear either above or below the grid depending on the configuration in the Station Settings dialog (see page 3-3). A number of options for the Events and Alarm Grids can be set in the DNA Properties dialog. For more information, see page 3-6.

Events

An event is the logged report of a system activity or incident. For example, when a cardholder presents their card at a door, an event is sent to the host computer(s). The event documents pertinent information such as the cardholder's name, the card number, the time and date, and a description of the activity.

The events displayed in the grid are based on the settings in the Event Logging Editor. See page 14-27 for more information.

Events Toolbar

DNA Fusion provides a number of useful commands and shortcuts to manage the Events Grid. These commands are available from the Events Toolbar when an event is selected. The toolbar actions are also available by right-clicking on an event and selecting an option from the context menu.

⏸	Pause Icon - Pauses the Events Grid; events will no longer display in the grid.
	Print Preview Icon - Displays a print preview of the Events Grid.
	Personnel Record Icon - Displays the Cardholder's Record for the card associated with the event.
	Retrieve Note Icon - Displays the Card Flags dialog for the card associated with the event. See page 7-35 for more information.
	Photo Verification Icon - Populates the Photo Recall Window for the cardholder's record associated with the event. See page 7-43 for more information.
	Launch Camera Icon - Opens the Video View Manager for the camera associated with the event point. See page 8-43 for more information.
	Control Icon - Displays the Direct Control Dialog for the selected point or object. For more information on controlling hardware, see Chapter 8: Hardware Features.

☰	Point Properties Icon - Displays the Point Properties dialog for the selected point or object. For more information on hardware properties, see Chapter 8: Hardware Features.
🏠	Home Page Icon - Launches the home page associated with the selected object.
✉	E-mail Event Icon - Only available if Enable E-mail is checked in the Host Settings. Displays the Mail Event Dialog to send an e-mail with the selected event data. See page 14-8 for more information.
📋 ▾	Reports Icon - Drop-down menu to generate a report for the selected event. For more information on reports, see Chapter 17: Reports.
📹	Export Video Icon - Opens the Export Video Dialog to send an e-mail with the selected video from the selected event. See page 8-47 for more information.

Events Filters Toolbar

DNA Fusion provides many useful filters to manage the Events Grid. These commands are available from the Events Filters Toolbar. Event Filters may also be viewed by right-clicking in the Events Grid; see page 14-5 for more information.

🚪	Door Icon - Shows and hides all door events.
➡	Arm Events Icon - Shows and hides all armed events.
⬅	Disarm Events Icon - Shows and hides all disarmed events.
⚑	Secure Icon - Displays and sorts secure events.
⚑	Alarm Events Icon - Displays and sorts alarm events.
🔌	Comm Events Icon - Displays and sorts communication events.
🟩	Area Events Icon - Shows and hides all access area events.
▦	MPG Icon - Shows and hides all MPG (Monitor Point Group) events.
🕒	Time Triggers Macros Icon - Shows and hides all time, trigger, and macro events.
ℹ	Operator Commands Icon - Shows and hides all operator command events.
🪪	Access Granted Icon - Shows and hides all access granted events.
🪪	Access Denied Icon - Shows and hides all access denied events.
🔄	Mode Change Icon - Shows and hides all mode change events.
⚠	Operator Alarm Handling Icon - Filters the list for operator alarm handling events.
▪▪▪	Miscellaneous Icon - Shows and hides all miscellaneous events.
▣	Hardware Filters Icon - Hides the filtered hardware events.
📹	Camera Events Icon - Toggles camera-related events.
▣	Stentofon Events - Toggles Stentofon-related events.
▲	Axis Events Icon - Toggles Axis-related events.
⊕	Isonas Events Icon - Toggles Isonas-related events.

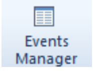
	Bosch Events Icon - Toggles Bosch-related events.
	Engage Events Icon - Toggles Engage-related events.
	Card Numbers Icon - Displays the Card Numbers Filters dialog box.
	Tenant Filters Icon - Shows and hides tenant events.
	Operator Filters Icon - Filters the list for operator commands.
	Index Filter Icon - Opens the Index Selection Dialog to select advanced filter options. See page 14-5 for more information.
	Date Time Range Filter Icon - Opens the Date Range Dialog to filter events by specified date and time parameters.
	Source Types Icon - Opens the Event Sources Filter dialog to filter events based on selected source types.
	Clear All Filters Icon - Clears all filters in the Events Grid. See page 14-5 for more information.
	Filtered Icon - Toggles between the filtered and non-filtered view.

Events Grid

The Events Grid displays the events in chronological order with the most recent events shown at the top. Date, time, user and location are recorded as well as a description of the event. The grid documents all system activity designated as an event in the Event Logging Editor. For more information, see page 14-25.

To open the Events Grid:

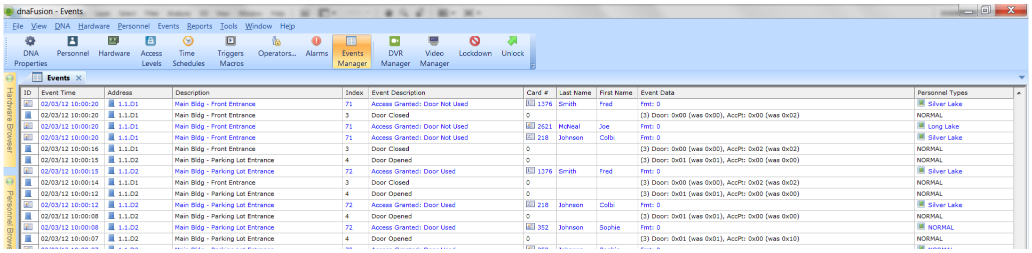
1. **Click** the Events Manager button on the Standard Toolbar.



   Or

   Press Shift + F2 on the keyboard.

   The Events Grid appears in the data window.



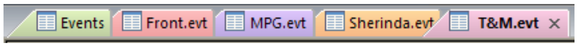
ID	Event Time	Address	Description	Index	Event Description	Card #	Last Name	First Name	Event Data	Personnel Types
	02/03/12 10:00:20	1.1.D1	Main Bldg - Front Entrance	71	Access Granted: Door Not Used	1376	Smith	Fred	Fmt: 0	Silver Lake
	02/03/12 10:00:20	1.1.D1	Main Bldg - Front Entrance	3	Door Closed	0			(3) Door: 0x00 (was 0x00), AccPt: 0x00 (was 0x02)	NORMAL
	02/03/12 10:00:20	1.1.D1	Main Bldg - Front Entrance	71	Access Granted: Door Not Used	2621	McNeal	Joe	Fmt: 0	Long Lake
	02/03/12 10:00:20	1.1.D1	Main Bldg - Front Entrance	71	Access Granted: Door Not Used	218	Johnson	Colbi	Fmt: 0	Silver Lake
	02/03/12 10:00:16	1.1.D1	Main Bldg - Front Entrance	3	Door Closed	0			(3) Door: 0x00 (was 0x00), AccPt: 0x02 (was 0x02)	NORMAL
	02/03/12 10:00:15	1.1.D2	Main Bldg - Parking Lot Entrance	4	Door Opened	0			(3) Door: 0x01 (was 0x01), AccPt: 0x00 (was 0x00)	NORMAL
	02/03/12 10:00:15	1.1.D2	Main Bldg - Parking Lot Entrance	72	Access Granted: Door Used	1376	Smith	Fred	Fmt: 0	Silver Lake
	02/03/12 10:00:14	1.1.D1	Main Bldg - Front Entrance	3	Door Closed	0			(3) Door: 0x00 (was 0x00), AccPt: 0x02 (was 0x02)	NORMAL
	02/03/12 10:00:12	1.1.D2	Main Bldg - Parking Lot Entrance	4	Door Opened	0			(3) Door: 0x01 (was 0x01), AccPt: 0x00 (was 0x00)	NORMAL
	02/03/12 10:00:12	1.1.D2	Main Bldg - Parking Lot Entrance	72	Access Granted: Door Used	218	Johnson	Colbi	Fmt: 0	Silver Lake
	02/03/12 10:00:08	1.1.D2	Main Bldg - Parking Lot Entrance	4	Door Opened	0			(3) Door: 0x01 (was 0x01), AccPt: 0x00 (was 0x00)	NORMAL
	02/03/12 10:00:08	1.1.D2	Main Bldg - Parking Lot Entrance	72	Access Granted: Door Used	352	Johnson	Sophie	Fmt: 0	NORMAL
	02/03/12 10:00:07	1.1.D2	Main Bldg - Parking Lot Entrance	4	Door Opened	0			(3) Door: 0x01 (was 0x01), AccPt: 0x00 (was 0x10)	NORMAL

Multiple Event Windows

Multiple event windows can be configured to display different elements.

1. **Right-click** in the Events Grid and **select** Grid / Save Settings.
2. If needed, **browse** to the desired location, **enter** a File Name and **click** the Save button.
3. **Right-click** in the Events Grid and **select** Grid / Load Settings.
4. **Locate** the .evt file and **click** the Open button.

   A new grid will appear in the Data Window.



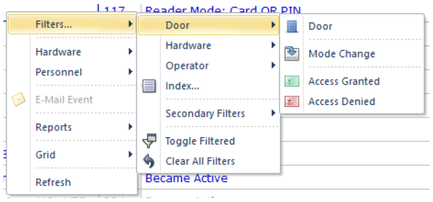
5. **Apply** the desired Filter(s) to the new grid.

Filtering Data

Users can filter information in the Events Grid to display specific attributes or components.

1. **Right-click** in the Events Grid and **select** Filters from the context menu.
2. **Select** the desired filter or secondary filter from the menu.

   The Events Grid will only display the events that are applicable to the filtered attribute.



   Or

1. **Drag and drop** a hardware or personnel object to the Events Grid.
2. To filter by multiple objects, **drag and drop** the additional objects to the Events Grid.

   The Events Grid will only display the events that are applicable to the selected object(s).

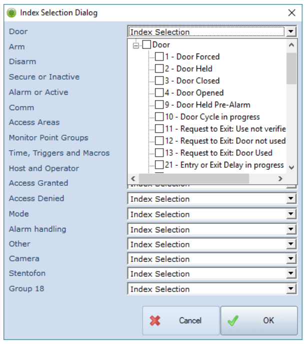
To clear the filter(s):

1. **Right-click** in the Events Grid and **select** Filters / Clear All Filters.

   The Events Grid is cleared of all filters.

Index Filter

The Index Filter allows the user to select specific events, which provides greater flexibility to filtering. The index number is located in the Events Grid.



Door: Index Selection
- □ Door
  - □ 1 - Door Forced
  - □ 2 - Door Held
  - □ 3 - Door Closed
  - □ 4 - Door Opened
  - □ 9 - Door Held Pre-Alarm
  - □ 10 - Door Cycle in progress
  - □ 11 - Request to Exit: Use not verifie
  - □ 12 - Request to Exit: Door not used
  - □ 13 - Request to Exit: Door Used
  - □ 21 - Entry or Exit Delay in progress

Arm
Disarm
Secure or Inactive
Alarm or Active
Comm
Access Areas
Monitor Point Groups
Time, Triggers and Macros
Host and Operator
Access Granted
Access Denied: Index Selection
Mode: Index Selection
Alarm handling: Index Selection
Other: Index Selection
Camera: Index Selection
Stentofon: Index Selection
Group 18: Index Selection

1. **Right-click** in the Events Grid and select Filters / Index from the context menu .

   The Index Selection Dialog opens.

2. **Select** the desired Event(s) from the drop-down list(s).

   Events can be selected from multiple categories.

3. **Click** the OK button.

   The grid is filtered by the selected event(s).

Exporting the Events Grid

The Events Grid can be exported to a .csv file.

1. **Right-click** in the Events Grid and **select** Grid / Export.

   The Save As dialog opens.
2. **Browse** to the desired location and **enter** a File Name.
3. **Click** the Save button.

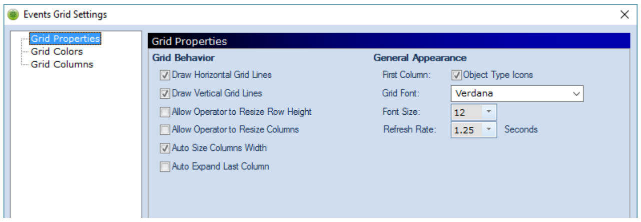
   A confirmation dialog will appear.
4. **Click** OK to export the report.

Events Grid Settings

The Events Grid can be customized based on operator preferences. For example, if a controller is located in a different time zone, the user can add Panel GMT Offset as one of the grid columns.

1. **Right-click** in the Events Grid and **select** Grid / Grid Properties.

   The Events Grid Settings dialog opens.



Grid Properties

Grid Behavior

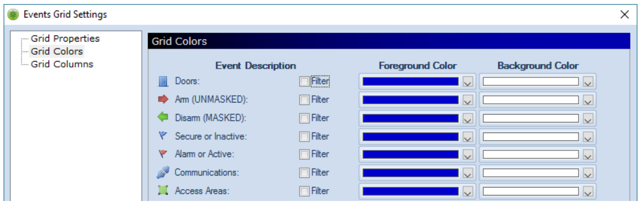
☑ Draw Horizontal Grid Lines
☑ Draw Vertical Grid Lines
☐ Allow Operator to Resize Row Height
☐ Allow Operator to Resize Columns
☑ Auto Size Columns Width
☐ Auto Expand Last Column

General Appearance

First Column: ☑ Object Type Icons
Grid Font: Verdana
Font Size: 12
Refresh Rate: 1.25 Seconds

2. **Configure** the Grid Properties options.
   - Draw Horizontal / Vertical Grid Lines - Toggles the grid lines between rows and columns in the Events Grid.
   - Allow Operator to Resize Row Height / Columns - If selected, allows the operator to adjust row height and column width in the Events Grid.
   - Auto Size Columns Width - Automatically sets column widths in the grid.
   - Auto Expand Last Column - Automatically expands the last column of the grid to fit the data window.
   - Object Type Icons - Select this checkbox to display object icons in the Events Grid. Must be selected to see Card Flags that have been set for a cardholder.
   - Grid Font - Drop-down to select the grid font.
   - Font Size - Drop-down to select the grid font size.
   - Refresh Rate - Drop-down to select the refresh rate of the Events Grid (in seconds).
3. **Select** Grid Colors from the dialog menu.

   The Grid Colors dialog opens.

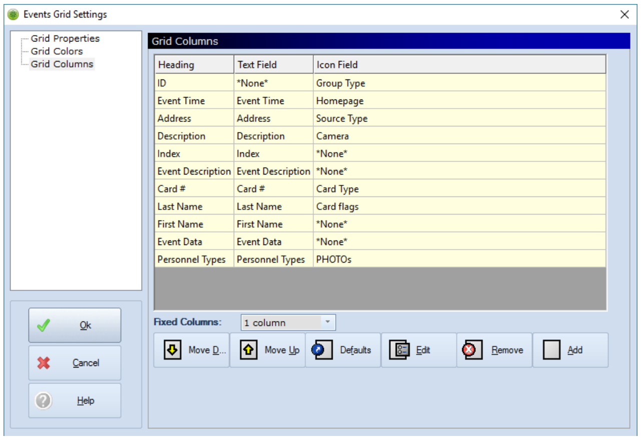


Grid Colors

Event Description		Foreground Color	Background Color
Doors:	☐ Filter	🟦	☐
Arm (UNMASKED):	☐ Filter	🟦	☐
Disarm (MASKED):	☐ Filter	🟦	☐
Secure or Inactive:	☐ Filter	🟦	☐
Alarm or Active:	☐ Filter	🟦	☐
Communications:	☐ Filter	🟦	☐
Access Areas:	☐ Filter	🟦	☐

4. **Select** Foreground and Background Colors for the various Event Descriptions.
5. If desired, **check** Filter for specific Event Descriptions.
6. **Select** Grid Columns from the dialog menu.

   The Grid Columns dialog opens.

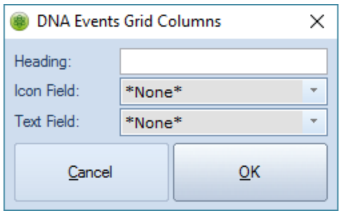


Grid Columns

Heading	Text Field	Icon Field
ID	*None*	Group Type
Event Time	Event Time	Homepage
Address	Address	Source Type
Description	Description	Camera
Index	Index	*None*
Event Description	Event Description	*None*
Card #	Card #	Card Type
Last Name	Last Name	Card flags
First Name	First Name	*None*
Event Data	Event Data	*None*
Personnel Types	Personnel Types	PHOTOs

Fixed Columns: 1 column

7. **Configure** the Grid Columns.
   - Fixed Columns - Drop-down to select the number of fixed columns. These columns correspond with their position in the Grid Columns dialog and will freeze in place when horizontally scrolling the grid.
   - Move Up/Move Down - Moves the selected column.
   - Defaults - Resets the grid columns to the default setting.
   - Edit - Opens the DNA Events Grid Columns dialog to edit the selected column.
   - Remove - Removes the selected column.
   - Add - Opens the DNA Events Grid Columns dialog to add a new column.
     a. **Enter** a name in the Heading field.
     b. If desired, **select** an Icon Field from the drop-down list.
     c. **Select** the desired field from the Text Field drop-down.
     d. **Click** OK.



Heading:
Icon Field: *None*
Text Field: *None*

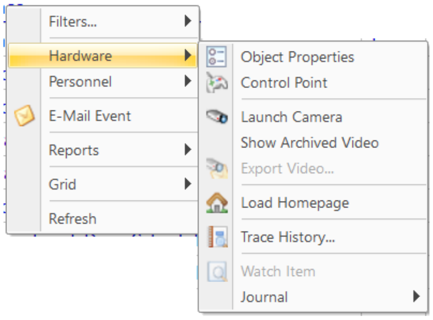
8. **Click** OK to save the configuration.

Accessing Hardware & Cardholders from the Events Grid

Controlling Hardware

Operators can access and control hardware objects directly from the Events Grid.

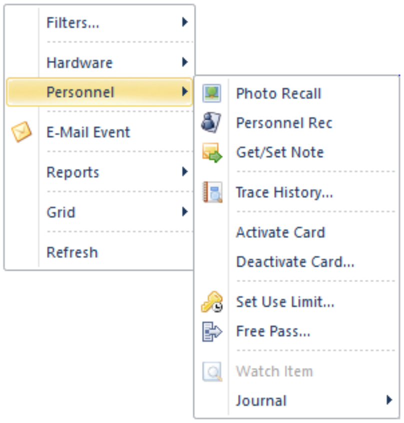
1. In the Events Grid, **right-click** on the desired event and **select** an option from the Hardware menu.
   - Object Properties - Opens the Properties dialog for the selected object. (8-49)
   - Direct Control - Opens the Direct Control dialog. See page 8-3 through 8-24 for more information on the Direct Control Dialog.
   - Launch Camera - Launches the Camera associated with the selected object. (8-45)
   - Show Archived Video - Opens the Video View Manager to play back a saved Recording associated with the selected object. (8-45)
   - Export Video - (Exacq Vision Integration Only) Exports the video to an email format. See page 8-47 for more information.
   - Load Homepage - Loads the Homepage associated with the selected object.
   - Trace History - Runs a Trace History report for the object. (8-17)
   - Watch Item - If the Watch Window is open, the object will be added to the Watch Window. For more information, see Chapter 15: Watch Windows.
   - Journal - Opens the DNA Journal window or opens the DNA Journal Selection dialog. (8-19)



Accessing Cardholders

Operators can perform a number of cardholder functions from the Events Grid.

1. In the Events Grid, **double-click** on an access event or **right-click** on the desired cardholder and **select** an option from the Personnel menu.
   - Photo Recall - Opens the Photo Recall window if a photo is associated with the cardholder. (7-43)
   - Personnel Rec - Opens the Cardholder's Record associated with the selected cardholder.
   - Get/Set Note - Opens the Card Flags dialog to retrieve or add a note to the Cardholder's Record. (7-35)
   - Trace History - Runs a Trace History report for the selected cardholder. (7-35)
   - Activate Card - Activates the selected card. (7-37)
   - Deactivate Card - Deactivates the selected card. (7-37)
   - Set Use Limit - Opens the Set Use Limit dialog. (7-37)
   - Free Pass - Opens the Set Anti-Passback Area dialog. (7-37)
   - Watch Item - If the Watch Window is open, the object will be added to the Watch Window. For more information, see Chapter 15: Watch Window.
   - Journal - Opens the DNA Journal window or opens the DNA Journal Selection dialog. (7-36)

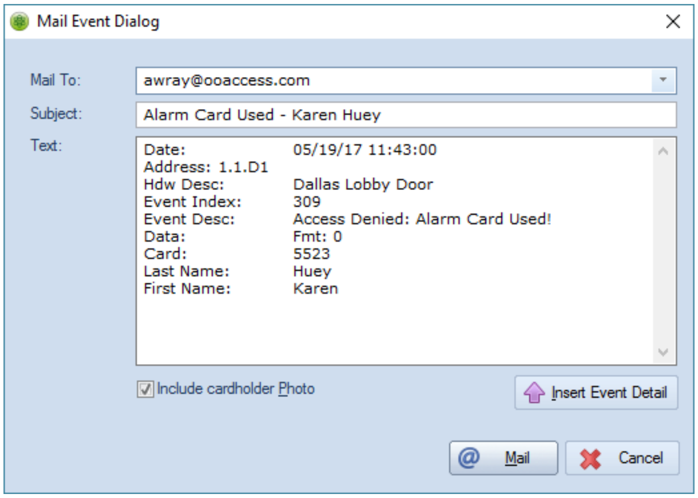


E-Mail Event

If the E-Mail Enable feature is configured in the Host Settings, operators can e-mail event data directly from the Events Grid. See page 3-11 for more information.

1. **Right-click** on the desired event in the Events Grid and select E-Mail Event.

   The Mail Event Dialog opens.



Mail To: awray@ooaccess.com

Subject: Alarm Card Used - Karen Huey

Text:

```
Date:          05/19/17 11:43:00
Address: 1.1.D1
Hdw Desc:      Dallas Lobby Door
Event Index:   309
Event Desc:    Access Denied: Alarm Card Used!
Data:          Fmt: 0
Card:          5523
Last Name:     Huey
First Name:    Karen
```

☑ Include cardholder Photo

2. **Select** an e-mail recipient from the Mail To: drop-down or **enter** a new e-mail address.

   The drop-down includes all e-mail addresses added to the E-Mail Recipients List; see page 3-11.

3. **Enter** a Subject and, if desired, **type** a message in the Text panel.

4. **Click** the Insert Event Detail button. Insert Event Detail

   The selected event data is added to the Text panel.

5. If desired, **select** the Include Cardholder Photo checkbox.

   Note: this option is only available if a cardholder is associated with the event.

6. **Click** the Mail button. Mail

   The event data is e-mailed to the designated recipient.

> *The* Mail Event Dialog *is also available from the* Alarm Grid*.* **Right-click** *on the desired alarm point and* **select** E-Mail*, or* **select** *the* E-Mail Alarm Icon *from the* Alarms Toolbar*. See page 14-15 for more information.*

Access Denied Codes

By default, all Access Denied events will be logged in the Events Grid. Each access denied event will display a code statement indicating the reason. This may prove helpful in determining the correct resolution, if needed.

Event Logged	**Definition / Solution**
Access Denied: After Deactivation Date	A card was presented after the deactivation date. SOLUTION: Change the Deactivation Date in the Card Tab of the Cardholder's Record. (7-11)
Access Denied: Airlock is Busy	A card was presented while the airlock is in use. SOLUTION: Wait until the airlock cycles.
Access Denied: Alarm Card Used!	A card was presented that has been flagged as an alarm card. SOLUTION: Uncheck Alarm Card in the Card Flags dialog. (7-33)
Access Denied: Anti-passback violation	A card was presented that violated the Anti-Pass Back protocol. SOLUTION: If Timed Anti-Pass Back, wait for the Delay time to expire or issue a Free Pass to the cardholder. (11-9)
Access Denied: Area Disabled	A card was presented at an entry point to an Access Area, but was denied because the area has been disabled. SOLUTION: Enable the specified Access Area. (11-5)
Authentication or Validation failure - HID PIV/Technology Industries	If the panel reaches out to the authentication server and the authentication server is unable to validate the credential, DNA Fusion will send back "Authentication or Validation Failure." The Event Data will contain some additional information as to why it failed. SOLUTION: Ensure there is a valid credential being used. Check Event Data for more information.
Connection Issue with AAM - HID PIV/ Technology Industries	The panel is unable to connect to the Auxiliary Authentication Module. The server operating either Technology Industries Entry Point Server or HID pivCLASS server is not reachable by the SSP running the authentication module. SOLUTION: Ensure servers are operating properly and effectively communicating with either Technology Industries Entry Point Server or HID pivCLASS server.
Access Denied: Biometric Verification Error	The user's biometric signature (e.g. fingerprint) does not match what is stored in the controller for that cardholder. SOLUTION: Verify that the biometric signature stored in the controller matches the one used at the biometric reader.
Access Denied: Count Exceeded	A cardholder has exceeded the deny violation count for a door. SOLUTION: Adjust the Logging Based on Deny Violations settings in the Door Properties / Advanced dialog, or increase the Violations count (8-63).
Access Denied: Credential Read Error	The credential was denied because the credential could not be read correctly. SOLUTION: Present the credential again or replace if damaged.
Access Denied: Deactivated Card	A card was presented that is no longer activated. SOLUTION: Right-click on the card and select Activate or select the Activate checkbox in the Card Tab of the Cardholder's Record. (7-12)

Event Logged	Definition / Solution
Access Denied: Elevator - Elevator -Timed out	The cardholder exceeded the elevators hold limit and failed to select a floor. SOLUTION: Increase the Relay Duration in DNA Fusion.
Access Denied: Floor not in Floor Served	The desired floor is not accessible to the cardholder. SOLUTION: add desired floor into floor group.
Access Denied: Floor Request not Authorized	The desired floor is not authorized for the cardholder. SOLUTION: Add cardholder to desired floor.
Access Denied: Elevator - Elevator Unknown	The elevator that was accessed is unknown. SOLUTION: Ensure that the elevator is added to the controller.
Access Denied: Duress Code Detected	A duress code was entered on a keypad or a card was presented in a manner indicating a duress code at an entry point. SOLUTION: In the Advanced settings of the Door Properties, check the Set to Deny Duress option. (8-63)
Access Denied: Facility Code	A card was presented with an invalid Facility Code. SOLUTION: If a valid Facility Code, program the code into the system. (8-55 & 8-83)
Access Denied: Failed the Bio Test: No Bio Record	A cardholder badged at a biometric reader configured for biometric verification, but they do not have any biometric data (e.g. fingerprint, etc.) stored in the controller. SOLUTION: Store the cardholder's biometric data in the controller.
Access Denied: Failed the Bio Test: No Bio Device	A cardholder badged at a biometric reader configured for biometric verification, but there is a communication issue between the controller and the biometric device (e.g. the controller is offline). SOLUTION: Verify that the biometric device is connected to the network.
Access Denied: F/C Extension	A card was presented with an invalid Facility Code Extension. SOLUTION: If valid FC, program the code into the system.
Access Denied: Host Denied Access	A card was presented at an entrance that requires approval from the host, but the host did not approve the card. SOLUTION: Uncheck Host Verification (8-62) or verify that the cardholder has been entered in the system and the correct access level was assigned.
Access Denied: Incomplete Card and PIN	The reader is set to Card AND PIN mode, but the cardholder did not enter their PIN number. SOLUTION: The cardholder must provide both credentials (card and PIN) at the entry point, or the operator must adjust the Door Mode. (8-3)
Access Denied: Invalid Card Format	A card was presented with a card format that does not match any in the database. SOLUTION: If a valid Card Format, program the format into the system. (8-83)
Access Denied: Invalid PIN	A PIN was entered that did not match any PIN in the database. SOLUTION: Verify cardholder's PIN number has been entered and the correct Access Level assigned. (7-9)

Event Logged	Definition / Solution
Access Denied: Issue Code	A card was presented with an issue code that is no longer activated. SOLUTION: The cardholder must use a correct card or the operator must update the Issue Code in the Card Tab of the Cardholder's Record. (7-9)
Access Denied: Level	A card was presented that was not assigned an access level for this entry point. SOLUTION: If applicable, assign the cardholder the correct Access Level for the entry point. (7-13)
Access Denied: Locked	The door mode was configured to be locked and unresponsive to card presentation or PIN input. SOLUTION: Change the Door Mode to for the specified door to Card Only to allow card access. (8-3)
Access Denied: No Asset Present	The authorized asset is not present. SOLUTION: Ensure that the asset is present at the entry point.
Access Denied: No escort card presented	A cardholder with an escort requirement presented their card at an entry point, but was not followed by an escort card before the timeout occurred (default = 15 seconds). SOLUTION: A cardholder with an Is an Escort access level must present their card after the cardholder with the Escort Requirement.
Access Denied: No Host Approval	A card was presented at an entrance that requires approval from the host but no response was received from the host. SOLUTION: In the Advanced settings of the Door Properties, the Host Verification option has been checked. (8-63)
Access Denied: Not In Card File	A card was presented that does not match any card in the controller's memory. SOLUTION: If the cardholder's name appears in the Events Grid, verify that the correct Access Level has been assigned to the cardholder. (7-13) If assigned an access level, Download the cardholder's information to the controller. (7-4)
Access Denied: Occupancy Limit	A card was presented at an entry point to an access area, but the area has reached its maximum occupancy count. SOLUTION: Wait for the Occupancy Count to decrease or adjust the Maximum setting in the Access Areas Dialog (11-2).
Access Denied: Prior to Activation Date	A card was presented before the scheduled activation date. SOLUTION: If applicable, adjust the Activation Date in the Card Tab of the Cardholder's Record. (7-9)
Access Denied: Second Card not Presented	One card was presented at a reader that requires two cards to grant access, but the second card was not presented within the allotted timeframe. SOLUTION: The cardholder must present two valid cards to the reader within the allotted timeframe, or the operator must uncheck Require 2 Card Control in the Advanced dialog (8-61).
Access Denied: Time	A card with the appropriate access level was presented at an entry point, but the time schedule associated with the access levels is not active. SOLUTION: If applicable, adjust the time schedule for the assigned access level. (5-5 & 6-3)
Access Denied: Unauthorized Assets	The asset(s) presented is unauthorized at this entry point. SOLUTION: Authorize the asset to the desired entry point.

Event Logged	Definition / Solution
Access Denied: Use Limit	A card was presented at an entry point, but the card has exceeded its maximum number of uses. SOLUTION: If applicable, adjust the cardholder's Use Limit number. (7-37)
Bio verify failed, have card data, no template data available	HandKey II Only - A cardholder badged at a biometric reader, but they do not have any biometric data stored in the controller. SOLUTION: Store the cardholder's biometric data in the controller.
Bio verify completed - failed	HandKey II Only - The user's biometric signature (e.g. fingerprint) does not match what is stored in the controller for that cardholder. SOLUTION: Verify that the biometric signature stored in the controller matches the one used at the biometric reader.
Bio verify failed, no card or data available	Handkey II Only - A cardholder badged at a biometric reader, but has no card or data available. SOLUTION: Store card and biometric data in the controller.
ASSA - Access Denied Busy	ASSA DSR Only – The lock is busy (e.g. communicating with the DSR) and cannot process the card read. SOLUTION: Wait until the lock is no longer busy.
ASSA - Access Denied Bolted	ASSA DSR Only – The dead bolt is engaged and the cardholder is not a "master" user. SOLUTION: Assign a deadbolt override access level to the cardholder.
ASSA - Access Denied Panic	ASSA DSR Only – The lock is in Panic Mode, which is not supported by DNA Fusion. SOLUTION: Change the mode of the ASSA lock in the LCT.
ASSA - Access Denied Privacy	ASSA DSR ONLY - The lock is in Privacy mode. SOLUTION: Change the mode of the ASSA lock in the LCT.
Axis – Access Denied (Anonymous)	Axis Only – A cardholder attempted to use a REX, but the door is locked or set to a Door Mode that doesn't allow access. SOLUTION: Change the Axis Door Mode.
Axis – Access Denied (Credential)	Axis Only – A card was presented that was not assigned an access level for this entry point. SOLUTION: If applicable, assign the cardholder the correct Access Level for the entry point. (7-13)
Axis – Access Denied (Credential Not Found)	Axis Only – A card was presented, but based on the current card format(s), there is not a matching credential in the controller's database. SOLUTION: Verify that the correct card number is assigned to the cardholder. If needed, select the appropriate Card Format in the AXIS Controller Properties / Card Formats dialog. Only one card format may be assigned to Axis controllers.
Bosch Panel - Access Denied: Interlocked	Bosch Only - An interlocked point assigned to a door must be in a normal state (example: door closed) before access is granted. SOLUTION: Doors that are interlocked must be closed before access is granted for either door.
Bosch Panel - Access Denied: No rights in area by card	Bosch Only - The card presented is not authorized for that area. SOLUTION: Verify that the cardholder is authorized for that area or authorize card to the area.

Event Logged	Definition / Solution
Bosch Panel - Access Denied: No rights in area by passcode	Bosch Only - A passcode was entered that is not authorized for that area. SOLUTION: Add user's passcode to the access level.
Bosch Panel- Access Denied - Unknown ID	Bosch Only - An unknown user has attempted access to the area. SOLUTION: Create a Bosch User ID for the unknown user and add access to area.
Elevator Dispatch Error, Invalid Destination	TKE Only - The elevator's dispatch destination is invalid. SOLUTION: Add the desired floor as a destination.
Elevator Dispatch Error, No elevators on Automatic	TKE Only - There are no elevator dispatching automatically. SOLUTION: Set an elevator to dispatch automatic when a card is presented.
Engage - Access Denied: Before Activation Date	Engage Only - A credential is being used before the Activation Date. SOLUTION: Present credential on the specified Activation Date or adjust the date.
Engage - Access Denied: Credential Expired	Engage Only - An expired credential was presented to a reader. SOLUTION: Verify that the credential has been deactivated and adjust the expiration date.
Engage - Access Denied: Not Within Schedule	Engage Only - A credential was presented, but was not within the set time schedule. SOLUTION: Present the credential within the set time schedule or adjust the schedule.
Engage - Access Denied	Engage Only - Cardholder has not been authorized to use the door. SOLUTION: Verify that the cardholder has access and that the information has been downloaded to the door.
Kone Elevator - Dispatch Error, Access Denied	Kone Only - The cardholder's requested dispatch has been denied. SOLUTION: Assign the desired access level group to cardholder.
Kone Elevator - Dispatch Timed Out	Kone Only - The elevator door timed out due to duration. SOLUTION: Increase Open Time in the Kone DOP Settings.
Schindler - Access Denied, Access interrupted	Schindler Only - Access to the elevator was interrupted. SOLUTION: Locate the source of interruption and re-present a credential. Contact technical support if issue persists.
Schindler - Access Denied: Anti-Passback	Schindler Only - The cardholder has trigger an anti-passback violation. SOLUTION: Verify the type of anti-passback. If area-based, ensure that the cardholder is in the correct area. If reader-based, ensure that the cardholder is using the correct credential.
Schindler - Access Denied: Destination floor locked	Schindler Only - The destination floor is locked in DNA Fusion. SOLUTION: In the Hardware Browser, right-click on the locked elevator and select Control / Mode / Unlocked.
Schindler - Access Denied: Destination not distinct	Schindler Only - The elevator destination is not well defined. SOLUTION: Ensure that the floor information is correct.

Event Logged	Definition / Solution
Schindler - Access Denied: Destination not reachable by this group	Schindler Only - Cardholder is attempting to access a floor that is not assigned to their Master Group. SOLUTION: Assigned cardholder to the desired Master Group.
Schindler - Access Denied: Generic	Schindler Only - The credential being presented is using the wrong generic card format SOLUTION: Ensure that the credential is using the correct generic card format.
Schindler - Access Denied: ID Expired	Schindler Only - The cardholder's ID is expired. SOLUTION: Extend the cardholder's deactivation date.
Schindler - Access Denied: ID Invalid	Schindler Only - The cardholder is using an ID that is not authorized to be used. SOLUTION: Add personnel record to the cardholder.
Schindler - Access Denied: ID not yet valid	Schindler Only - The cardholder is attempting to gain access to an area before the ID's activation date. SOLUTION: Adjust Activation Date for the cardholder.
Schindler - Access Denied: Invalid key input	Schindler Only - The cardholder's PIN was entered incorrectly. SOLUTION: Ensure cardholder is inputting correct PIN or adjust PIN.
Schindler - Access Denied: No Access	Schindler Only - The cardholder has no access to the Master Group. SOLUTION: Add desired Profile (access level) to cardholder.
Schindler - Access Denied: No ID	Schindler Only - No ID was associated with the credential being used. SOLUTION: Add credential to desired personnel record.
Schindler - Access Denied: No Lift	Schindler Only - Elevator to desired floor is out of service. SOLUTION: Ensure Elevator is working properly. Contact Schindler for any issue regarding service.
Schindler - Access Denied: No SOM task	Schindler Only - There are no tasks assigned to Schindler's Special Operating Mode. SOLUTION: Disable the SOM or assign a task.
Schindler - Access Denied: Origin Floor locked	Schindler Only - The elevators origin floor is locked. SOLUTION: Ensure that the Origin Floor is unlocked.
Schindler - Access Denied: Refused	Schindler Only - Cardholder's does not have access to the elevator. SOLUTION: Add access level to the cardholder.
Schindler - Access Denied: Try again (allocation to closing the door)	Schindler Only - Elevator closed after credential was presented. SOLUTION: Present credential again.

* Each Access Denied Code has a corresponding code for Magstripe cards that indicates the direction the card was swiped. The (<<) arrows indicate that card was swiped right to left.

Alarms

Alarms are user-defined signals that notify the operator of specific changes in system hardware. These changes in state are reported and managed in the Alarm Grid. Additionally, users can set and monitor alarms using graphic pages. For more information, see Chapter 18: Graphic Maps.

DNA Fusion offers a sophisticated array of alarm monitoring tools. This section covers the basic capabilities of the Alarm Grid and Alarms Toolbar, as well as the versatility of DNA in handling alarms for a given workstation.

Alarms Toolbar

Each button on the Alarms Toolbar represents a command used to control alarms in the Alarm Grid. The toolbar options are also available by right-clicking on an alarm in the grid.

The Alarms Toolbar is context-sensitive so that only the options applicable to a given alarm status are enabled. If an icon (or menu item) is not available, it will appear as a "ghost" object, i.e. greyed out.

⧉	Select All Icon - Allows the operator to select all of the current alarms on the grid for a specific control, e.g. Acknowledge or Clear.
✓	Acknowledge Alarm Icon - Allows the operator to acknowledge a selected alarm.
✕	Clear Alarm Icon - Clears the grid of the selected alarm. Only available after an alarm is acknowledged and returns to normal.
☒	Clear Selected Icon - Clears the grid of all selected alarms. Like the Clear Alarm option, this icon is only available after an alarm is acknowledged and returns to normal.
✖	Dismiss Alarm Icon - Dismisses the selected alarm.
🎮	Control Icon - Populates the Direct Control Dialog for the selected alarm point. For more information on controlling hardware, see Chapter 8: Hardware Features.
☰	Point Properties Icon - Opens the Properties dialog for the selected alarm point. For more information on hardware properties, see Chapter 8: Hardware Features.
ⓘ	Alarm Information Icon - Toggles the Alarm Information panel in the data window, which displays predefined alarm information and instructions. See page 14-18 for more information.
📹	Camera Icon - Only available if a camera is associated with the alarm point. If selected, displays the camera in the Video View Manager. See page 8-43 for more information.
⌂	Home Page Icon - Opens the homepage for the selected alarm point. The homepage is configured in the point's Properties dialog. For more information on hardware properties, see Chapter 8: Hardware Features.
✉	E-mail Alarm Icon - Displays the Mail Event Dialog to send an e-mail with the selected alarm data. See page 14-8 for more information.
📹	Export Video Icon - Opens the Export Video Dialog to send an e-mail with the selected video from the selected event. See page 8-47 for more information.

NOTES:

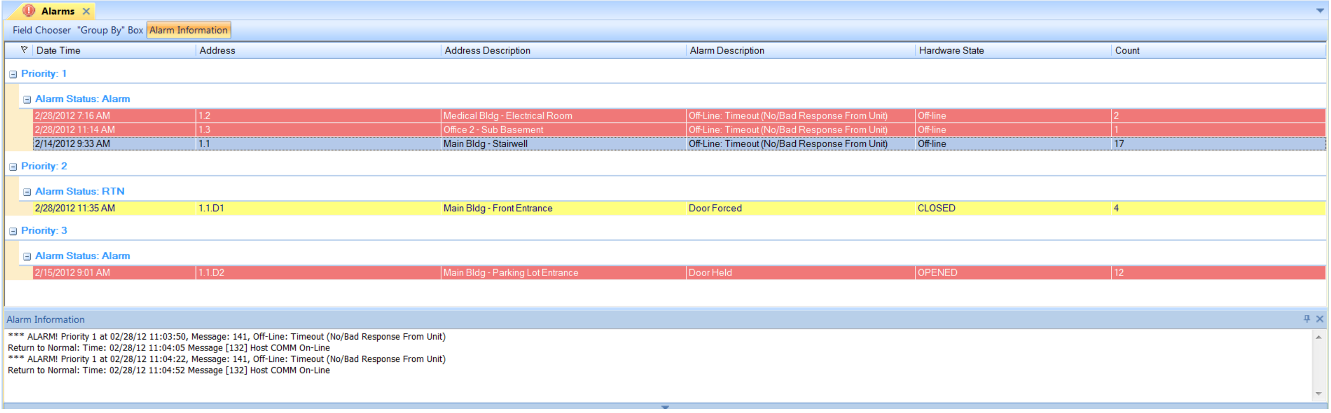
Alarm Grid

The Alarm Grid is a data window comprised of a "matrix" or spreadsheet record of alarm events.

To open the Alarm Grid, use one of the following two methods:

- **Select** the Alarm button from the Standard Toolbar. Alarms
- **Double-click** the Alarm Status field on the Status Bar. Alarm Status: 0 - 0 - 0

Opening the Alarm Grid will bring it to the front of the application interface and will display any alarms that have not been dismissed or acknowledged/cleared.



▽ Date Time	Address	Address Description	Alarm Description	Hardware State	Count
⊟ Priority: 1					
⊟ Alarm Status: Alarm					
2/28/2012 7:16 AM	1.2	Medical Bldg - Electrical Room	Off-Line: Timeout (No/Bad Response From Unit)	Off-line	2
2/28/2012 11:14 AM	1.3	Office 2 - Sub Basement	Off-Line: Timeout (No/Bad Response From Unit)	Off-line	1
2/14/2012 9:33 AM	1.1	Main Bldg - Stairwell	Off-Line: Timeout (No/Bad Response From Unit)	Off-line	17
⊟ Priority: 2					
⊟ Alarm Status: RTN					
2/28/2012 11:35 AM	1.1.D1	Main Bldg - Front Entrance	Door Forced	CLOSED	4
⊟ Priority: 3					
⊟ Alarm Status: Alarm					
2/15/2012 9:01 AM	1.1.D2	Main Bldg - Parking Lot Entrance	Door Held	OPENED	12

Alarm Information

```
*** ALARM! Priority 1 at 02/28/12 11:03:50, Message: 141, Off-Line: Timeout (No/Bad Response From Unit)
Return to Normal: Time: 02/28/12 11:04:05 Message [132] Host COMM On-Line
*** ALARM! Priority 1 at 02/28/12 11:04:22, Message: 141, Off-Line: Timeout (No/Bad Response From Unit)
Return to Normal: Time: 02/28/12 11:04:52 Message [132] Host COMM On-Line
```

The Alarm Grid presents the alarm information in a condensed format to conserve screen space, and organizes all pertinent data in an easy-to-read format. The grid consists of twelve adjustable columns to describe various alarm properties as well as options to toggle the Field Chooser dialog, "Group By" Box, and Alarm Information panel. For more information, see page 14-18.

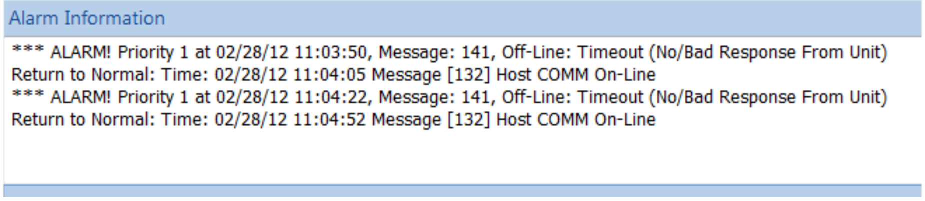
Column	Description
▽	The alarm status icon.
Priority	The user-defined priority of this alarm.
Date Time	The date and time that the alarm occurred based on the operator's time zone.
Address	The hardware address of the specific alarm point.
Address Description	A user-defined address description of the alarm point.
Alarm Description	Supplemental alarm text information.
Hardware State	The current status of the hardware.
Count	The count indicating how many times this specific alarm point has changed state since it was acknowledged and cleared.
Alarm Status	The status of the alarm condition.
Card #	The card number associated with the alarm, if applicable.
User	The name of the cardholder who triggered the alarm, if applicable.
Panel Time	The date and time that the alarm occurred based on the controller's time zone.*

* By default, the Panel Time column is not displayed in the Alarm Grid; it can be added by using the Field Chooser dialog. See page 14-16 for more information on customizing the grid.

Alarm Grid Features

All alarms will display specific text information regarding the alarm. With the alarm count feature and the expandable and collapsible alarm text, hundreds of alarms can be viewed simultaneously on the grid.

- The Alarm Count feature is useful during periods of system maintenance or hardware device failure. With this feature, the alarm point only creates a single entry on the grid, and the Count column automatically increases to indicate the total number of state changes for the alarm point.
- The Alarm Information panel displays alarm information for the selected alarm, including previous alarm incidents and predefined instructions.



Alarm Information

```
*** ALARM! Priority 1 at 02/28/12 11:03:50, Message: 141, Off-Line: Timeout (No/Bad Response From Unit)
Return to Normal: Time: 02/28/12 11:04:05 Message [132] Host COMM On-Line
*** ALARM! Priority 1 at 02/28/12 11:04:22, Message: 141, Off-Line: Timeout (No/Bad Response From Unit)
Return to Normal: Time: 02/28/12 11:04:52 Message [132] Host COMM On-Line
```

- The Ctrl and Shift keys can be used to select multiple alarms and control them simultaneously. This includes the Acknowledge, Clear, and Dismiss commands.

Customizing the Alarm Grid

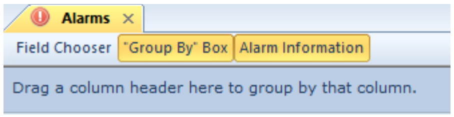
The Alarm Grid provides several tools to help manage alarm events.

Grouping the Alarm Grid

The Alarm Grid can be grouped by any column header, including Alarm Status and Priority.

1. **Select** the "Group By" Box option at the top of the Alarm Grid.

   A drag-and-drop area appears above the grid columns.



2. **Drag** the desired column header(s) to the area.

   The Alarm Grid is grouped by the header(s).

Arranging the Columns

Alarm Grid columns can be customized so that only the relevant columns are visible.

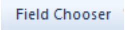
To remove a column:

1. **Drag** the column away from the header until a black "X" is visible.
2. **Drop** the column anywhere in the DNA environment.

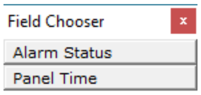
   The header column is removed from the Alarm Grid.

To replace a column:

Once a column header has been removed, it will appear in the Field Chooser dialog.

1. **Click** the Field Chooser option at the top of the Alarm Grid. 

   The Field Chooser dialog will open with the removed columns.



2. **Drag** the desired column to any location on the Alarm Grid header until two red arrows appear.
3. **Insert** the column in the desired location.

   The column will appear in the Alarm Grid.

> *The* Alarm Information, Group By Box, *and* Field Chooser *features can also be accessed by selecting* Alarms *from the* Main Menu. *The* Alarm Grid *must be active in the data window for this menu category to be available.*

Alarm Grid Settings

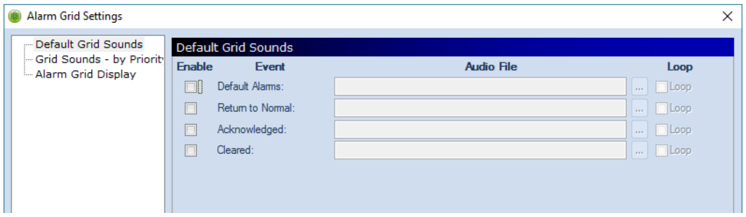
DNA Fusion provides a series of dialogs to modify the alarm grid settings, including sounds, text attributes, and colors.

Default Grid Sounds

The Default Grid Sounds dialog is used to assign a unique sound to default alarms and various alarm states. The sound can be any .wav file available to the system.

1. **Right-click** in the Alarm Grid and **select** Grid Setup from the context menu.

   The Alarm Grid Settings / Default Grid Sounds dialog will open.



Alarm Grid Settings

- Default Grid Sounds
- Grid Sounds - by Priority
- Alarm Grid Display

Default Grid Sounds

Enable	Event	Audio File	Loop
□	Default Alarms:		□ Loop
□	Return to Normal:		□ Loop
□	Acknowledged:		□ Loop
□	Cleared:		□ Loop

2. **Select** the Enable checkbox for the desired Event(s).

   The Audio File and Loop fields become active.

3. **Click** the Browse button to locate the Audio File for each Event.

4. If desired, **select** the Loop checkbox to continue playing the sound until another action occurs.

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

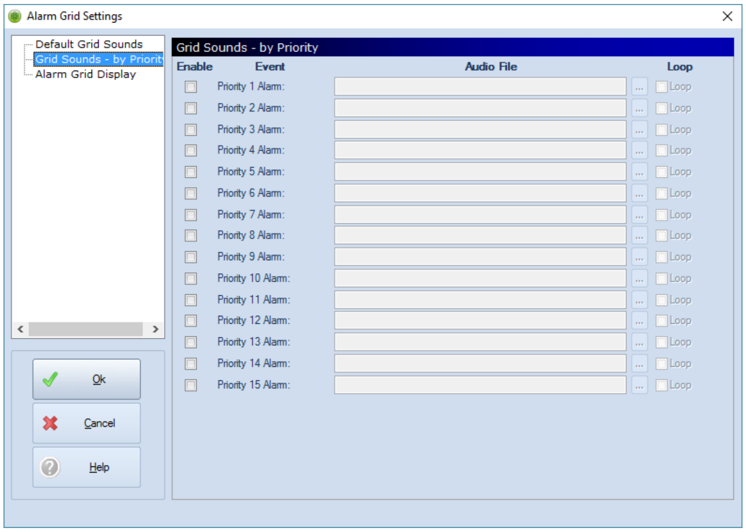
Grid Sounds - by Priority

The Grid Sounds - by Priority dialog is used to assign unique sounds to alarm priorities. The sound can be any .wav file available to the system. See page 14-27 for more information on alarm priorities.

1. **Right-click** in the Alarm Grid and **select** Grid Setup from the context menu.

   The Alarm Grid Settings dialog opens.

2. **Select** Grid Sounds - By Priority from the dialog menu.



Alarm Grid Settings

- Default Grid Sounds
- Grid Sounds - by Priority
- Alarm Grid Display

Grid Sounds - by Priority

Enable	Event	Audio File	Loop
□	Priority 1 Alarm:		□ Loop
□	Priority 2 Alarm:		□ Loop
□	Priority 3 Alarm:		□ Loop
□	Priority 4 Alarm:		□ Loop
□	Priority 5 Alarm:		□ Loop
□	Priority 6 Alarm:		□ Loop
□	Priority 7 Alarm:		□ Loop
□	Priority 8 Alarm:		□ Loop
□	Priority 9 Alarm:		□ Loop
□	Priority 10 Alarm:		□ Loop
□	Priority 11 Alarm:		□ Loop
□	Priority 12 Alarm:		□ Loop
□	Priority 13 Alarm:		□ Loop
□	Priority 14 Alarm:		□ Loop
□	Priority 15 Alarm:		□ Loop

3. **Select** the Enable checkbox for the desired Event(s).

   The Audio File and Loop fields become active.

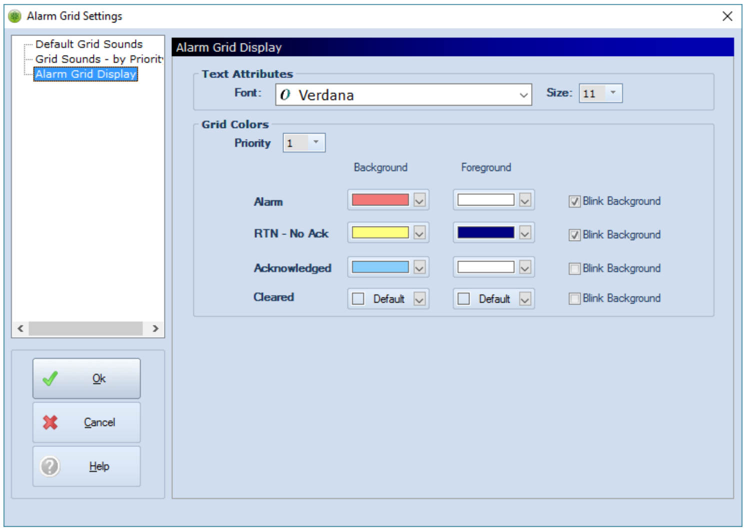
4. **Click** the Browse button to locate the Audio File for each Event.

5. If desired, **select** the Loop checkbox to continue playing the sound until another action occurs.

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

Alarm Grid Display

The Alarm Grid Display dialog is used to modify colors in the Alarm Grid based on the Alarm Priority and Alarm Status. The grid colors can be customized for each priority and status.



Alarm Grid Settings

- Default Grid Sounds
- Grid Sounds - by Priorit
- Alarm Grid Display

Alarm Grid Display

Text Attributes

Font: Verdana Size: 11

Grid Colors

Priority 1

	Background	Foreground	
Alarm	🟥	⬜	☑ Blink Background
RTN - No Ack	🟨	🟦	☑ Blink Background
Acknowledged	🟦	⬜	☐ Blink Background
Cleared	☐ Default	☐ Default	☐ Blink Background

1. **Right-click** in the Alarm Grid and **select** Grid Setup from the context menu.

   The Alarm Grid Settings dialog will open.

2. **Select** Alarm Grid Display from the dialog menu.

3. **Select** the desired Font from the drop-down list.

4. **Select** the desired Size from the drop-down list.

5. **Select** a Priority from the drop-down list.

   See page 14-27 for more information on setting alarm priorities.

6. **Select** the Background and Foreground colors for each Alarm State.

   The Foreground selection will determine the color of the text for the specified alarm priority.

   - Alarm: A new alarm message that appears when a change of state is detected.
   - RTN - No Ack: An alarm that has returned to normal but has not been recognized (acknowledged) by the operator.
   - Acknowledged: An alarm that has been recognized by the operator.
   - Cleared: An alarm that has been acknowledged, responded to, and cleared from the alarm grid.

7. If desired, **check** the Blink Background box.

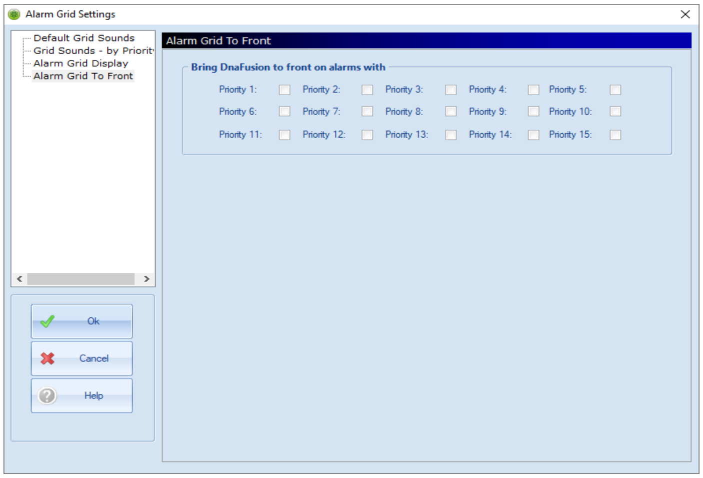
   The alarm's background color will blink when the condition is met.

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

Alarm Grid To Front

The Alarm Grid To Front dialog is used to filter alarms by priority.

1. **Right-click** in the Alarm Grid and **select** Grid Setup.
2. **Select** Alarm Grid To Front from the dialog menu.



Alarm Grid Settings

- Default Grid Sounds
- Grid Sounds - by Priorit
- Alarm Grid Display
- Alarm Grid To Front

Alarm Grid To Front

Bring DnaFusion to front on alarms with

Priority 1: ☐	Priority 2: ☐	Priority 3: ☐	Priority 4: ☐	Priority 5: ☐
Priority 6: ☐	Priority 7: ☐	Priority 8: ☐	Priority 9: ☐	Priority 10: ☐
Priority 11: ☐	Priority 12: ☐	Priority 13: ☐	Priority 14: ☐	Priority 15: ☐

3. **Select** which priorities will allow the alarm grid to move to the front of DNA Fusion.
4. **Click** Ok.

Handling Alarms

The system operator is responsible for recognizing and responding to an alarm condition. This section explains the basics of how an alarm is managed after it appears in the Alarm Grid. Handling alarms involves multiple steps for the operator, all of which can be performed using the Alarm Grid.

In DNA Fusion, alarms can exist in one of two states:

- Active – The point has changed from its normal state to an alarm state.
- Inactive – The point has not changed to an alarm state, or it has returned to its normal state.

Depending on the operator's action, the alarm has four possible conditions:

- Unacknowledged Alarm – A new alarm message. A change of state was detected.
- Acknowledged Alarm – An alarm that has been recognized by the operator.
- Cleared Alarm – An alarm that has been acknowledged and cleared from the Alarm Grid.
- Dismissed Alarm – An alarm that has been dismissed by the operator whether or not the hardware object has returned to normal (RTN).

When handling alarms from the Alarm Grid, the operator can monitor (and must recognize) the current status of the alarm. The status is determined by a combination of the aforementioned states and conditions.

Under normal operations, the process for handling an alarm would be as follows:

Step	Action	State	Condition
1.	An alarm appears in the grid	Active	Unacknowledged
2.	The operator recognizes the alarm	Active	Acknowledged
3.	The alarm returns to normal state	Inactive	Acknowledged
4.	Operator clears alarm	Inactive	Cleared

The operator has three different avenues to work from when handling, monitoring and responding to alarms in the Alarms Grid:

- Alarms Toolbar
- Menus
  - □ Alarms option from the Main Menu
  - □ Context menu available by right-clicking on an alarm
- Keystroke / Shortcut Keys
  - □ Acknowledge F5 shortcut key
  - □ Clear F8 shortcut key
  - □ Custom keystroke combinations

The Administrator has the ability to clear all alarms in the Alarm Grid*.* **Select** DNA / Administrative / Alarms and Events / Clear All Alarms or **right-click** in the grid and **select** Clear All Alarms*. All pending alarms will be cleared from the* Alarm Grid*.*

NOTES:

Alarm Status

Alarm status icons are color-coded to identify the alarm point's current condition. This will help determine the appropriate operator response to handle the alarm.

Alarm Status Icon	Alarm Status Definition	Operator Response	Operator Action
Alarm 🚩	A change has occurred to a normal condition that has resulted in an alarm.	The operator should acknowledge the alarm.	**Select** ✓ or F5.
RTN 🚩	The condition that resulted in the alarm has returned to its normal state, but must be acknowledged by the operator.	The operator should acknowledge the alarm.	**Select** ✓ or F5.
ACK 🚩	The alarm has been recognized by the operator, but the condition has not returned to normal.	No action is required to by the operator but the physical condition causing the alarm may need to be addressed.	No action is required; however, the operator may need to change the physical condition of the problem in order for the condition to return to normal.
Clear 🚩	The alarm has been recognized by the operator; its condition has returned to normal and awaits clearing by the operator.	The operator should clear the alarm.	**Select** ✖ or ☒ or F8 or Shift-F8 (Clear All).

An Acknowledged Alarm *cannot be cleared until the alarm state has returned to normal, i.e., all alarms must be both acknowledged and indicate a "returned-to-normal" status before they can be cleared. The operator may use the* Dismiss *option to remove an alarm from the* Alarm Grid *prior to both conditions occurring.*

If the system connection has been interrupted, select View / Refresh *from the* Main Menu *to display the current alarm data. Operators should also perform a refresh if they log out and back in, or if the* Alarm Grid *seems unresponsive.*

Dispatch Text

The Dispatch Text feature allows comments to be entered or selected during alarm acknowledgement to record relevant information.

Dispatch text can be entered in one of two ways:

- Freehand entry
- Predefined entry

Freehand Text Entry

The freehand method allows the operator to manually type the alarm information into a dialog.

1. **Configure** the Logging & Priority settings.

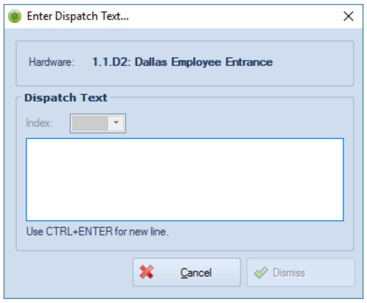
   See page 14-27 for more information on configuring alarms.

2. **Configure** the Operator's Profile to Require Dispatch Text for the various priorities.

   See page 4-5 for more information on configuring profiles.

3. When an alarm is presented, **handle** the alarm as explained on page 14-21.

   Upon Clearing or Dismissing an alarm, the Enter Dispatch Text dialog appears.



Enter Dispatch Text...

Hardware: 1.1.D2: Dallas Employee Entrance

Dispatch Text

Index:

Use CTRL+ENTER for new line.

Cancel | Dismiss

4. **Type** a comment and **click** the Clear/Dismiss button.

   The alarm is removed from the Alarm Grid and the Dispatch Text is saved to the Events Grid under the Event Data field for the Alarm Cleared/Dismissed event.

Predefined Text Entry

Predefined Dispatch Text requires the operator to select from a list of entries.

1. **Configure** the Alarms Logging & Priority settings.

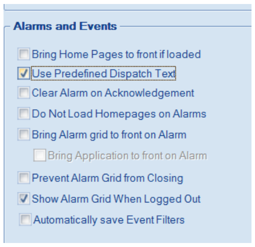
   See page 14-27 for more information on configuring alarms.

2. **Configure** the Operator's Profile to Require Dispatch Text for an alarm.

   See page 4-5 for more information on configuring operator profiles.

3. From the DNA Properties dialog window, **select** the checkbox for Use Predefined Dispatch Text.

   See page 3-6 for more information.

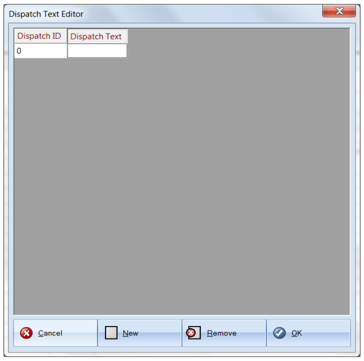


Alarms and Events

□ Bring Home Pages to front if loaded
☑ Use Predefined Dispatch Text
□ Clear Alarm on Acknowledgement
□ Do Not Load Homepages on Alarms
□ Bring Alarm grid to front on Alarm
□ Bring Application to front on Alarm
□ Prevent Alarm Grid from Closing
☑ Show Alarm Grid When Logged Out
□ Automatically save Event Filters

4. **Select** DNA / Administrative / Alarms and Events / Dispatch Text from the Main Menu.

   The Dispatch Text Editor dialog appears.



Dispatch Text Editor

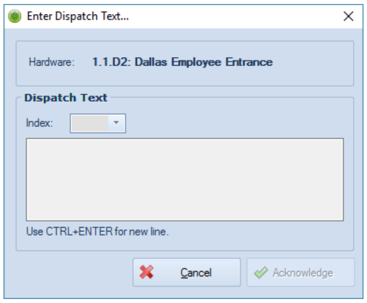
Dispatch ID	Dispatch Text
0	

Cancel | New | Remove | OK

5. **Click** the New button.
6. **Enter** a Dispatch ID number and the Dispatch Text in the appropriate fields.
7. **Click** the New button to add additional lines.
8. **Click** OK to save.
9. When an alarm is presented, **handle** the alarm as explained on page 14-21.

   Upon Clearing or Dismissing an alarm, the Enter Dispatch Text dialog appears.

> *If* Clear Alarm on Acknowledgment *is checked in the* DNA Properties *dialog, the* Enter Dispatch Text *dialog will appear when the alarm is* Acknowledged*. See page 3-6 for more information.*


Enter Dispatch Text...

Hardware: 1.1.D2: Dallas Employee Entrance

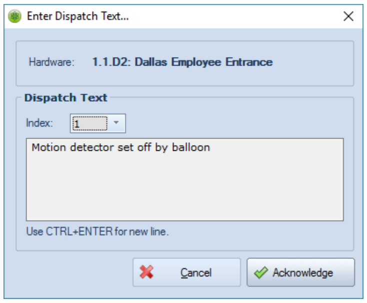
Dispatch Text

Index:

Use CTRL+ENTER for new line.

10. **Select** the Predefined Dispatch Text from the Index drop-down.

    The text will populate in the dialog.


Enter Dispatch Text...

Hardware: 1.1.D2: Dallas Employee Entrance

Dispatch Text

Index: 1

Motion detector set off by balloon

Use CTRL+ENTER for new line.

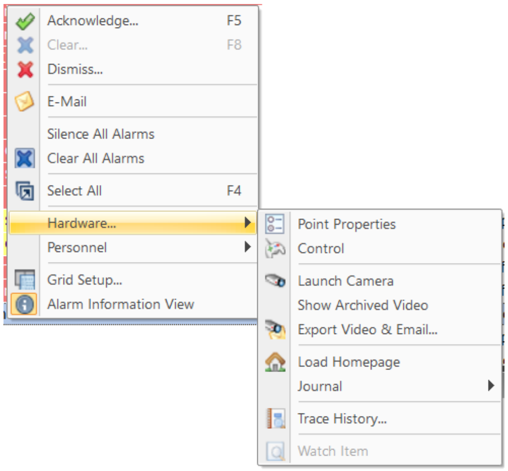
11. **Click** the Acknowledge, Clear, or Dismiss button.

    The alarm is removed from the Alarm Grid and the Dispatch Text is saved to the Events Grid under the Event Data field for the alarm event.

Accessing Hardware from the Alarm Grid

DNA Fusion allows the operator to access hardware and perform direct controls on a selected point from the Alarm Grid.

1. To access the hardware functions, **right-click** on the desired object in the Alarm Grid and **select** Hardware from the context menu.



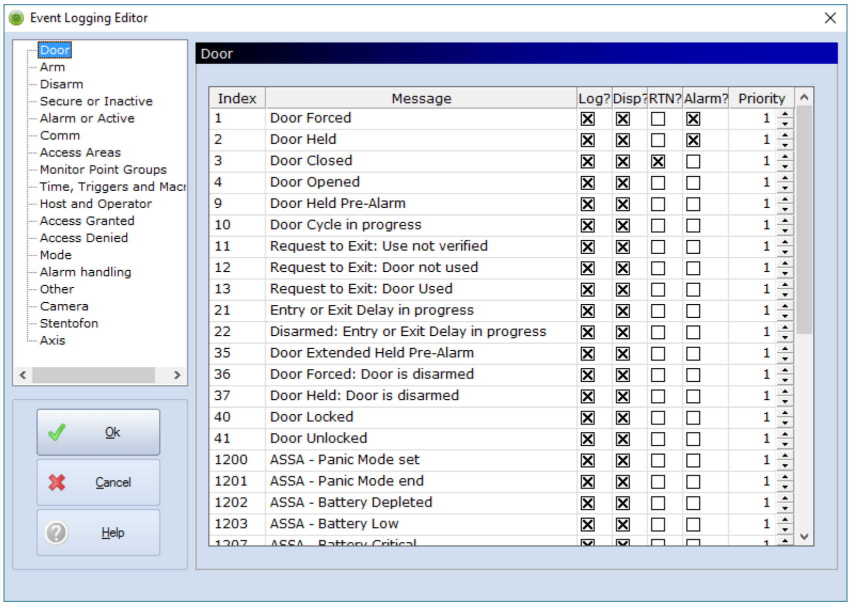
- Point Properties - Opens the Properties dialog for the selected alarm point. (8-47)
- Control - Opens the Direct Control Dialog. See pages 8-3 through 8-22 for more information.
- Launch Camera - Launches the Camera associated with the selected alarm point. (8-43)
- Show Archived Video - Opens the Video View Manager to play back a saved Recording associated with the selected alarm point. (8-43)
- Export Video - (Exacq Vision Integration Only) Exports the video to an email format. See page 8-45 for more information.
- Load Homepage - Loads the Homepage associated with the selected alarm point.
- Journal - Opens the DNA Journal window or opens the DNA Journal Selection dialog. (8-18).
- Trace History - Runs a Trace History report for the selected alarm point. (8-17).
- Watch Item - If the Watch Window is open, the object will be added to the Watch Window. For more information, see Chapter 15: Watch Windows.

Configuring the Alarms & Events Logging

The system administrator will need to configure which alarms and events will be reported to the Alarm Grid. By default, none of the events are marked as Alarm; however, the RTN (return-to-normal) conditions are selected.

1. **Select** DNA / Administrative / Alarms and Events / Logging from the Main Menu.

   The Event Logging Editor dialog opens.



Door

Index	Message	Log?	Disp?	RTN?	Alarm?	Priority
1	Door Forced	☒	☒	□	☒	1
2	Door Held	☒	☒	□	☒	1
3	Door Closed	☒	☒	☒	□	1
4	Door Opened	☒	☒	□	□	1
9	Door Held Pre-Alarm	☒	☒	□	□	1
10	Door Cycle in progress	☒	☒	□	□	1
11	Request to Exit: Use not verified	☒	☒	□	□	1
12	Request to Exit: Door not used	☒	☒	□	□	1
13	Request to Exit: Door Used	☒	☒	□	□	1
21	Entry or Exit Delay in progress	☒	☒	□	□	1
22	Disarmed: Entry or Exit Delay in progress	☒	☒	□	□	1
35	Door Extended Held Pre-Alarm	☒	☒	□	□	1
36	Door Forced: Door is disarmed	☒	☒	□	□	1
37	Door Held: Door is disarmed	☒	☒	□	□	1
40	Door Locked	☒	☒	□	□	1
41	Door Unlocked	☒	☒	□	□	1
1200	ASSA - Panic Mode set	☒	☒	□	□	1
1201	ASSA - Panic Mode end	☒	☒	□	□	1
1202	ASSA - Battery Depleted	☒	☒	□	□	1
1203	ASSA - Battery Low	☒	☒	□	□	1
1207	ASSA - Battery Critical	☒	☒	□	□	1

2. **Select** an object category from the dialog menu.
3. **Select** the desired parameters for each event:
   - Log? - Logs the event to the database.
   - Disp? - Displays the event in the Events Grid.
   - RTN? - Sets the event as a return-to-normal (RTN) condition for an alarm.
   - Alarm? - Displays the event as an alarm in the Alarm Grid.

   If an alarm event is identified, a return-to-normal (RTN) condition must be selected in order to clear the alarm. For example, if Door Held *or* Door Forced *is identified as an* Alarm *condition, then* Door Closed *must be flagged as an* RTN *condition in the* Event Logging Editor *for the operator to be able to* Clear *the alarm.*

   - Priority - Sets the alarm priority number.
4. Repeat steps 2 and 3 until all objects have been configured.
5. **Click** OK to save the settings.

NOTES:

Event Filtering and Alarm Escalation

Event Filtering and Alarm Escalation allow the operator to automatically filter events via workstation or operator profile as well as escalate alarms to e-mail. When events are generated, they will be routed through the system to the correct workstation or operator.

Alarms can be emailed to designated addresses based on the Filter Definitions and Alarm Priorities.

Configuring Event Filtering

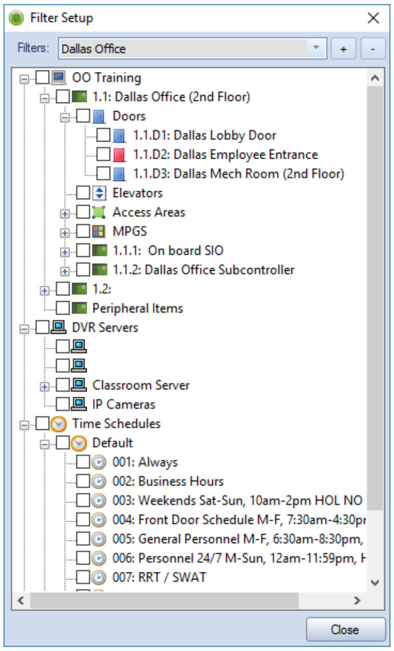
Setting Up Event Filters

1. **Select** DNA / Administrative / Setup Filters from the Main Menu.

   The Filter Setup dialog opens.

2. **Select** the Add button + to create a new Event Filter.

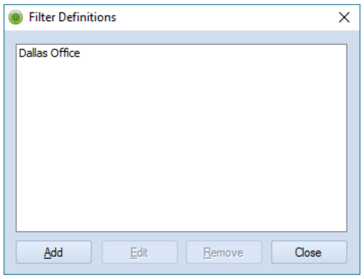
   The Filter Definitions dialog appears.



Filter Setup

Filters: Dallas Office

OO Training
1.1: Dallas Office (2nd Floor)
Doors
1.1.D1: Dallas Lobby Door
1.1.D2: Dallas Employee Entrance
1.1.D3: Dallas Mech Room (2nd Floor)
Elevators
Access Areas
MPGS
1.1.1: On board SIO
1.1.2: Dallas Office Subcontroller
1.2:
Peripheral Items
DVR Servers
Classroom Server
IP Cameras
Time Schedules
Default
001: Always
002: Business Hours
003: Weekends Sat-Sun, 10am-2pm HOL NO
004: Front Door Schedule M-F, 7:30am-4:30pı
005: General Personnel M-F, 6:30am-8:30pm,
006: Personnel 24/7 M-Sun, 12am-11:59pm, H
007: RRT / SWAT

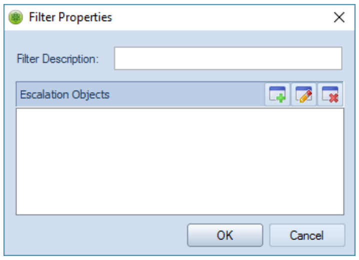


Filter Definitions

Dallas Office

3. **Click** the Add button to create a new Filter Definition.

   The Filter Properties dialog opens.



Filter Properties

Filter Description:

Escalation Objects

4. **Enter** a description in the Filter Description field and **click** the OK button.

   If desired, **click** the Add New Escalation Object button.

   See page 14-30 for more information on Alarm Escalation.

5. **Expand** the tree objects in the Filter Setup dialog and **check** the desired components.

   If an SSP controller is selected, the filter will have access to all hardware on the controller.

6. **Click** the Close button to save the setting and exit the dialog.

7. **Apply** the Operator Filter to an operator profile(s) or workstation(s). See below for more information.

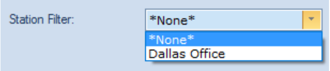
Applying the Event Filters

Once created, event filters can be assigned to a specific workstation or to an operator's profile.

To assign the Event Filter to a workstation:

1. **Open** the Host Settings / Station Settings dialog.
2. **Select** the desired filter from the Station Filter drop-down and **click** OK.

   See page 3-3 for more information.

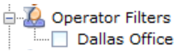


Station Filter: *None*

None
Dallas Office

To assign the Event Filter to an operator profile:

1. **Open** the Operator Profiles dialog.
2. **Expand** the Operator Filters header and **select** the desired Filter from the list.
3. **Click** OK.



Operator Filters
□ Dallas Office

Configuring Alarm Escalation

1. **Select** DNA / Administrative / Setup Escalation from the Main Menu.

   The Filter Definitions dialog opens.

   Or

   Select DNA / Administrative / Setup Filters from the Main Menu.

   The Filter Setup dialog opens.

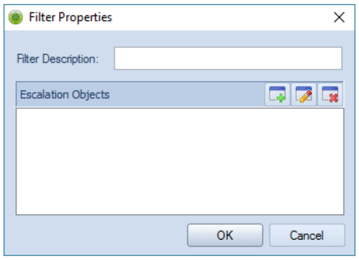
   This option allows for the combination of the Event Filtering and Alarm Escalation features. See page 14-29 for information on configuring Event Filtering.

2. **Click** the Add button to create a new Alarm Escalation filter.

   Or

   Select a configured Event Filter and **click** the Edit button.

   The Filter Properties dialog appears.



3. **Enter** a Filter Description for the Event Filter.

4. **Click** the Add New Escalation Object button.

   The Escalation Properties dialog opens.

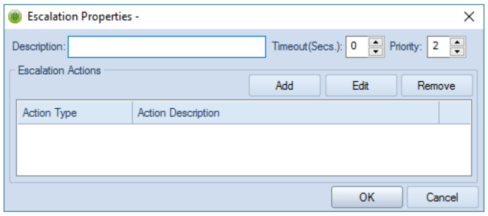
5. **Enter** a Description.

6. **Enter** a number (in seconds) in the Timeout field.

   After an alarm is received, if the operator does not respond to the condition in the set amount of time, the alarm will be escalated per the settings.

7. **Enter** the desired Alarm Priority to escalate.

   If the generated alarm matches the Priority setting, the alarm will be escalated after the designated amount of time.

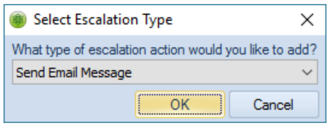


Timeout(Secs.): 0

Priority: 2

8. **Select** the Add button.

   The Select Escalation Type dialog opens.



What type of escalation action would you like to add?

Send Email Message

9. **Select** Send Email Message from the drop-down list and **click** OK.

   The Escalation Email Properties dialog appears.

10. **Enter** the Description, From, To, and Subject Matter fields.

11. If desired, **enter** information in the Body section and **click** OK.

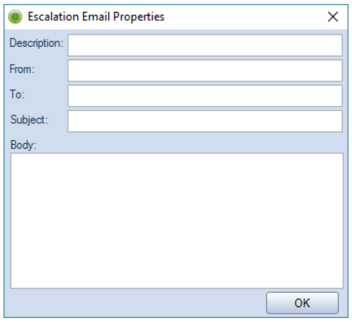
12. **Click** OK to save the Escalation Properties dialog.

13. **Click** OK to save the Filter Properties dialog.

    The Email Authentication settings in the Driver Setup must be configured properly for the e-mail to be sent. See page 20-3 for more information.

14. **Apply** the Operator Filter to an operator profile(s) or workstation(s).

    See page 14-29 for more information.



Watch Window 15

In This Chapter

The Watch Window feature is a unique and useful tool that helps the operator monitor objects (e.g., cardholders, doors, and alarms) that require the most attention.

Watch windows are data windows that allow the operator to monitor specific alarms, track individual events, and receive an alert when such events occur.

For example, the operator might track:

- When a specific cardholder enters
- When a specific door is opened
- When a specific cardholder enters through a specific door

Using the Watch Windows

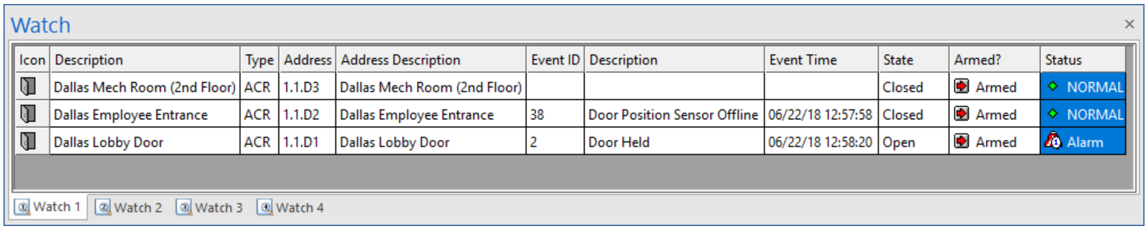
To open the Watch Window:

1. **Select** the Watch button from the Standard Toolbar.

   OR

   Select View / Windows / Watch from the Main Menu.

   The Watch Window will appear at the bottom of the DNA Fusion environment. The operator can dock the window anywhere in the application interface.



Watch

Icon	Description	Type	Address	Address Description	Event ID	Description	Event Time	State	Armed?	Status
	Dallas Mech Room (2nd Floor)	ACR	1.1.D3	Dallas Mech Room (2nd Floor)				Closed	Armed	◆ NORMAL
	Dallas Employee Entrance	ACR	1.1.D2	Dallas Employee Entrance	38	Door Position Sensor Offline	06/22/18 12:57:58	Closed	Armed	◆ NORMAL
	Dallas Lobby Door	ACR	1.1.D1	Dallas Lobby Door	2	Door Held	06/22/18 12:58:20	Open	Armed	Alarm

2. **Select** a tab to display the desired window: Watch 1-4.

Configuring the Watch Windows

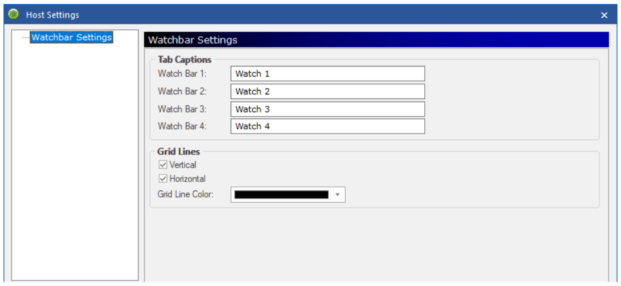
1. **Right-click** in the Watch Window and **select** Watch Window Setup.

   OR

   Select DNA Properties / Watchbar Settings.

   The Watchbar Settings dialog opens.

2. **Enter** a Tab Caption for the desired Watch Bar(s).
3. If desired, **select** the Vertical and Horizontal checkboxes to toggle Grid Lines in the Watch Window.
4. If desired, **select** a Grid Line Color from the drop-down.
5. **Click** OK to save the settings.



Tab Captions

Watch Bar 1: Watch 1

Watch Bar 2: Watch 2

Watch Bar 3: Watch 3

Watch Bar 4: Watch 4

Grid Lines

☑ Vertical

☑ Horizontal

Grid Line Color: ■

This Page Intentionally Left Blank

Adding Watch Objects

Watch Objects are the items that will appear in the Watch Window grid(s).

1. **Open** the desired Watch Window tab to add the objects.
2. **Select** the desired object from its Browser and **drag** and **drop** it into the Watch Window.

   OR

   Right-click on the desired object and **select** Watch Item.

   The object will appear in the active Watch Window.

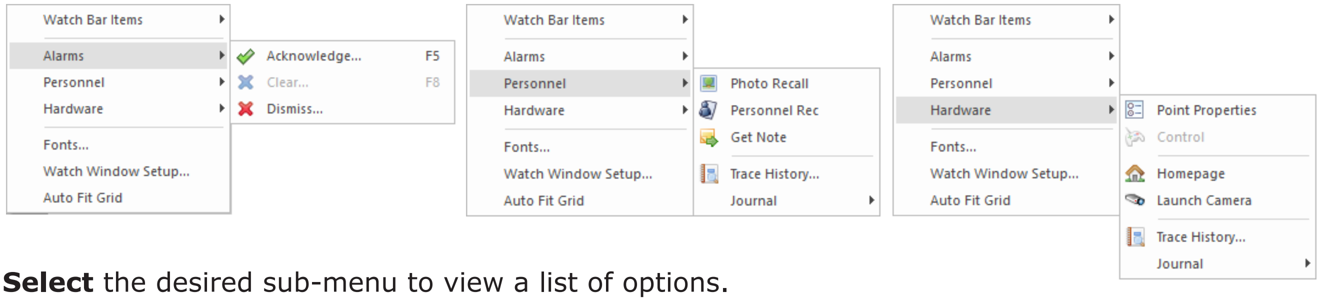
Watch Object Options

Depending on the Watch Object, a number of right-click options are available.

To view the available options:

1. With the Watch Window open, **right-click** on the Watch Object.

   A context menu will appear.



2. **Select** the desired sub-menu to view a list of options.
   - Alarms - Allows the operator to control the alarm point from the Watch Window. See Chapter 14 for more information.
   - Personnel - Allows the operator to access a Personnel Record, open a Photo Recall Window, set Card Flags, run a Trace History report, and use the Journal feature. See Chapter 7 for more information.
   - Hardware - Provides access to the selected object's Properties as well as the ability to control the hardware from the Watch Window. Users can also launch an associated Homepage or Camera, run a Trace History report, and use the Journal feature. See Chapter 8 for more information.

Removing Watch Objects

Watch Objects can be removed individually, cleared from an individual tab, or cleared from all tabs.

To remove individually:

1. **Right-click** on the object in the Watch Window and **select** Watch Bar Items / Remove.

   The object will disappear from the Watch Window.

To clear an individual tab:

1. **Right-click** in the desired Watch Window and **select** Watch Bar Items / Clear Tab.

   All objects are removed from the selected tab.

To clear from all tabs:

1. **Right-click** in the Watch Window and **select** Watch Bar Items / Clear All.

   All objects are removed from the four Watch Windows.

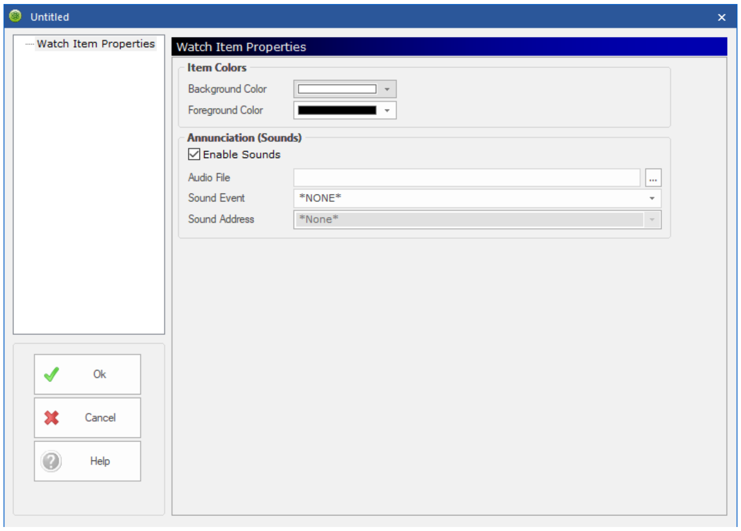
NOTES:

Configuring Watch Objects

Watch Window items can be configured individually.

1. **Right-click** on the Watch Object and **select** Watch Bar Items / Properties from the context menu.

   The Watch Item Properties dialog opens.



Watch Item Properties

Item Colors

Background Color

Foreground Color

Annunciation (Sounds)

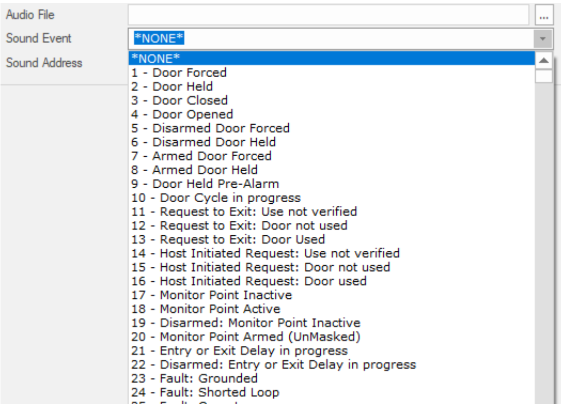
☑ Enable Sounds

Audio File

Sound Event: *NONE*

Sound Address: *None*

2. **Configure** the object using the drop-down menus:
   - Background Color - The background color for the selected object.
   - Foreground Color - The foreground color for the selected object.
   - Enable Sounds - If checked, the selected Audio File will play when the associated Sound Event occurs.
   - Audio File - The path to the selected Audio File.
   - Sound Event - The event that will trigger the Audio File.
   - Sound Address - The object address where the Sound Event will occur to trigger the Audio File.
3. **Click** the Browse button to select a WAV file (.wav) to associate with the object.
4. **Select** the desired Sound Event from the drop-down list.



Audio File

Sound Event: *NONE*

Sound Address

NONE
1 - Door Forced
2 - Door Held
3 - Door Closed
4 - Door Opened
5 - Disarmed Door Forced
6 - Disarmed Door Held
7 - Armed Door Forced
8 - Armed Door Held
9 - Door Held Pre-Alarm
10 - Door Cycle in progress
11 - Request to Exit: Use not verified
12 - Request to Exit: Door not used
13 - Request to Exit: Door Used
14 - Host Initiated Request: Use not verified
15 - Host Initiated Request: Door not used
16 - Host Initiated Request: Door used
17 - Monitor Point Inactive
18 - Monitor Point Active
19 - Disarmed: Monitor Point Inactive
20 - Monitor Point Armed (UnMasked)
21 - Entry or Exit Delay in progress
22 - Disarmed: Entry or Exit Delay in progress
23 - Fault: Grounded
24 - Fault: Shorted Loop

5. **Select** a hardware location from the Sound Address drop-down list.

   The Alarm File *will not play unless the* Sound Event *occurs at the designated* Sound Address*.*

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

This Page Intentionally Left Blank

HTML Viewer 16

In This Chapter

√ Using the HTML Viewer
√ Adding Pages & URLs to the HTML Viewer

The built-in HTML Viewer is a data window that allows the user to view web content directly within the application as well as add custom HTML pages and multimedia to any system. This may include information such as a company's web page, facility layout, phone list, policies and procedures, etc.

All HTML pages are added to the viewer menu by using the DNAFusion HTML Editor.

The HTML Viewer is a global setting, which allows the administrator to configure the feature at any client workstation. After the HTML Viewer is configured, the settings will be available at all client workstations.

Using the HTML Viewer

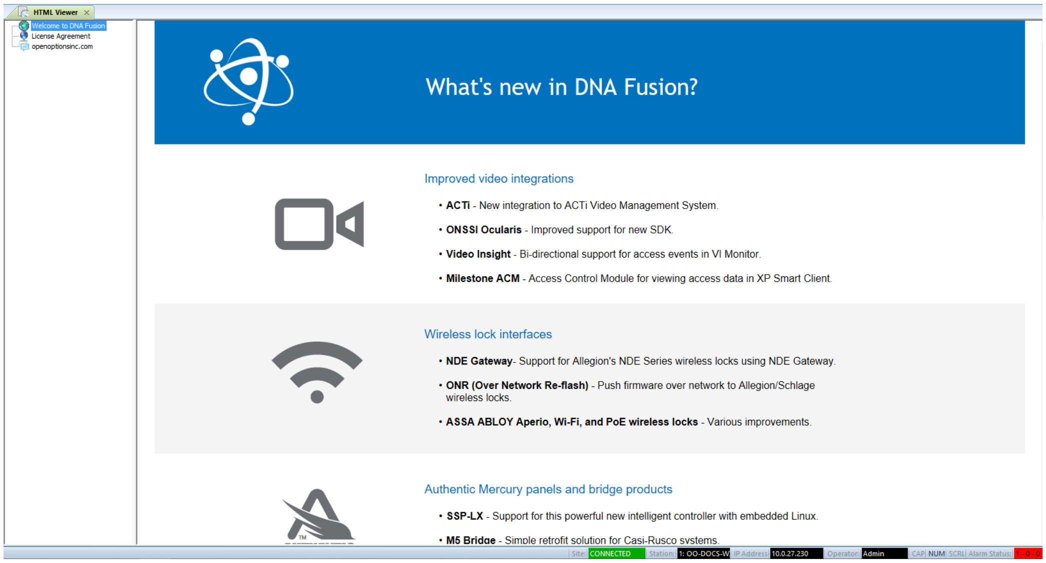
To open the HTML Viewer:

1. **Select** File / HTML Viewer from the Main Menu.

   OR

   Press the F3 shortcut key.

   The HTML Viewer opens.



What's new in DNA Fusion?

Improved video integrations

- **ACTi** - New integration to ACTi Video Management System.
- **ONSSI Ocularis** - Improved support for new SDK.
- **Video Insight** - Bi-directional support for access events in VI Monitor.
- **Milestone ACM** - Access Control Module for viewing access data in XP Smart Client.

Wireless lock interfaces

- **NDE Gateway**- Support for Allegion's NDE Series wireless locks using NDE Gateway.
- **ONR (Over Network Re-flash)** - Push firmware over network to Allegion/Schlage wireless locks.
- **ASSA ABLOY Aperio, Wi-Fi, and PoE wireless locks** - Various improvements.

Authentic Mercury panels and bridge products

- **SSP-LX** - Support for this powerful new intelligent controller with embedded Linux.
- **M5 Bridge** - Simple retrofit solution for Casi-Rusco systems.

Operators can opt to display the HTML Viewer *upon startup. In the* DNA Properties *dialog, select* DNA HTML Viewer *from the* Start Up *drop-down menu.*

2. **Click** or **double-click** links in the HTML Tree to navigate to the destination points.

   The associated page is displayed.

   See page 16-3 for information on adding pages and URLs.

This Page Intentionally Left Blank

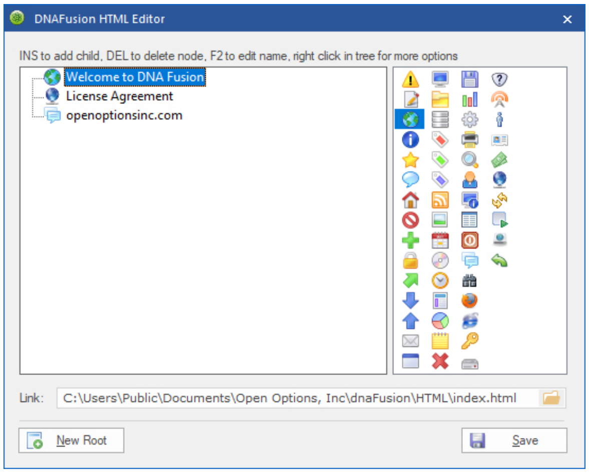
Adding Pages & URLs

The HTML Tree includes the pages and URLs that operators can view in the data window. The DNAFusion HTML Editor dialog is used to modify the HTML Tree.

To open the HTML Editor:

1. **Select** DNA / Administrative / Edit HTML Tree from the Main Menu.

   The DNAFusion HTML Editor dialog appears.



DNAFusion HTML Editor

INS to add child, DEL to delete node, F2 to edit name, right click in tree for more options

- Welcome to DNA Fusion
- License Agreement
- openoptionsinc.com

Link: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\HTML\index.html

The operator can add new root pages to the tree or add "child" pages to an existing root.

New Root Page

A root page will appear as a main item in the HTML Tree.

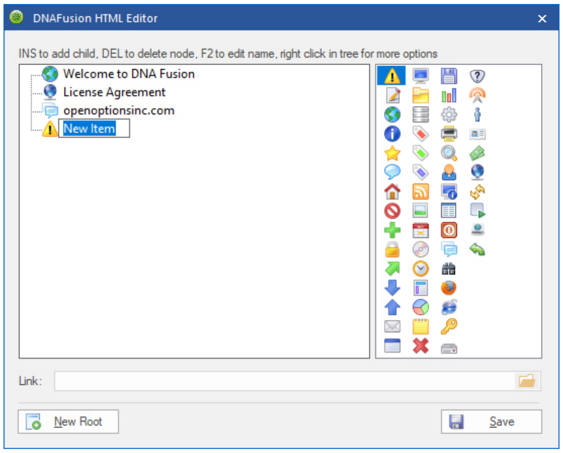
To add a new root page:

1. **Select** the New Root button. New Root

   OR

   From the DNAFusion HTML Editor dialog**, right-click** on an item in the HTML Tree and **select** Insert Before or Insert After from the context menu.

   A New Item will appear in the tree.



DNAFusion HTML Editor

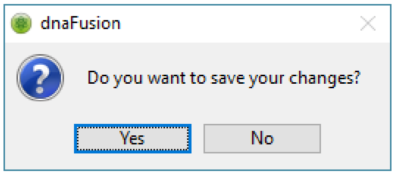
INS to add child, DEL to delete node, F2 to edit name, right click in tree for more options

- Welcome to DNA Fusion
- License Agreement
- openoptionsinc.com
- New Item

Link:

2. **Enter** a name for the new page.
3. In the Link field, **select** the File button to browse for the desired file or **enter** the file address.
4. **Select** an icon for the new link.
5. **Click** the Save button.

   A confirmation dialog appears.



dnaFusion

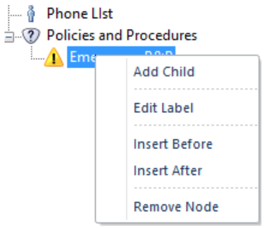
Do you want to save your changes?

6. **Select** Yes to save the changes.

   The root page is added to the HTML Tree.

New Child Page

A child page appears in the tree as a sub-item to a root page.



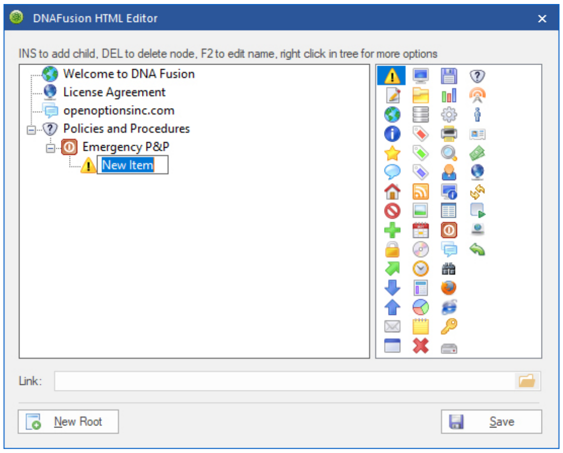
1. **Select** a Root Page in the DNAFusion HTML Viewer Editor dialog.
2. **Right-click** on the page and **select** Add Child.

   OR

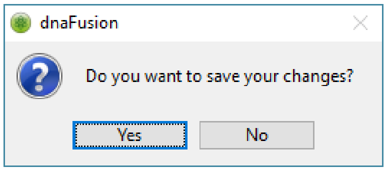
   Press the Insert key on the keyboard.

   A Child Page will appear in the tree under the selected Root.
3. **Enter** a name for the new page.
4. In the Link field, **select** the File button 📂 to browse for the desired file or **enter** the file address.
5. **Select** an icon for the new link.
6. **Click** the Save button.

   A confirmation dialog will appear.



INS to add child, DEL to delete node, F2 to edit name, right click in tree for more options



Do you want to save your changes?

7. **Select** Yes to save the changes.

   The new child page is added beneath the selected root page.

Edit HTML Page

1. **Select** DNA / Administrative / Edit HTML Tree from the Main Menu.

   The DNAFusion HTML Editor appears.
2. **Right-click** the desired page and **select** Edit Label.
3. **Edit** the page name.
4. If needed, **select** the File button 📂 in the Link field to browse for the desired file location or **enter** the file address.
5. **Select** an icon for the link.
6. **Click** the Save button.

   A confirmation dialog will appear.
7. **Select** Yes to save the changes.

Remove HTML Page

1. **Select** DNA / Administrative / Edit HTML Tree from the Main Menu.

   The DNAFusion HTML Editor appears.
2. **Right-click** the desired page and **select** Remove Node.

   A confirmation dialog will appear.
3. **Select** Yes to delete the page.

   The page is removed from the HTML Tree.
4. **Click** the Save button to save the dialog.

   A confirmation dialog will appear.
5. **Select** Yes to save the changes.

Reports 17

In This Chapter

- √ Types of Reports
- √ Generating Reports
- √ Creating Custom Reports
- √ Printing and Exporting Reports

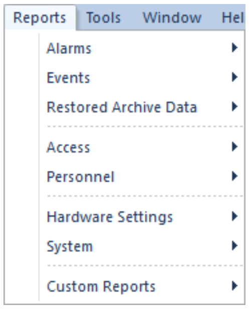
The Reports feature in DNA Fusion is a user-friendly tool used to generate a detailed account of information gathered by the program. Reports are highly customizable and allow the user to tailor data for a specific purpose.

> ⓘ If the Tenants feature is enabled, reports will only display information for the operator's assigned tenants.

Reports

DNA Fusion provides a large selection of default reports, with the option to create custom reports if needed. To generate a default report, select Reports from the Main Menu and choose from the following menu options:

Access



- Access Levels by SSP - Displays the access levels for the selected controller(s) according to set parameters.
- Access Level Descriptions - Shows the description for each access level.
- Legacy Access Level Groups - Shows the access level(s) and description(s) for the selected Legacy Access Level Group(s).
- Global Access Level Details - Displays pertinent details for the selected Global Access Level Group(s), including the associated activation/deactivation date(s) and time schedule/floor group(s).
- Access Level Group Assignments - Displays what cards, if any, are assigned to the selected Global Access Level Group(s).
- Floors - Provides floor group information, including the floor name(s) and assigned time schedule(s).
- Door Access Profile - Shows the access levels that are associated with each entry point.
- Who Has Access Door(s) - Displays which cardholders have access to the selected door(s).
- Access Level Last Used - Displays the time and date that the selected access level(s) were last used.
- ASSA Access Levels - Provides a report of the ASSA access levels along with the name and card number of the personnel assigned to the level.

Alarms

- Alarms History - Provides a history of all the alarms based on the defined parameters.
- Acknowledged Alarms - Displays only the Acknowledged alarms based on the defined parameters.
- Pending Alarms - Reports the alarms that have not been Acknowledged by an operator.

Events

- Event History - Provides the ability to run an event-specific report based on card numbers, personnel, event, and/or device-specific parameters.
- DMP Receiver Transactions - Displays an event-specific report for DMP transactions only.
- Bosch Receiver Transactions - Displays an event-specific report for Bosch transactions only.

- ThyssenKrupp Elevator Access - Provides a report that displays the elevator access events for ThyssenKrupp elevators. The report includes the event date and time along with the kiosk accessed.
- Event Log Settings - Shows the current Events & Alarms Logging settings.

Hardware Settings

- Sites - Displays site and station information as well as the number of controllers and subcontrollers attached to the site.
- Channels - Shows all channel information for the site(s).
- Controllers (SSP) - Provides information on the controllers attached to the system.
- Controllers DST Settings - Displays the Daylight Savings Time settings for the selected controller(s).
- Sub-Controller (SIO) - Reports the subcontroller's model, address, and channel.
- Monitor Points - Displays the monitor point's properties, including circuit type and log specification.
- Control Points - Shows the control point's properties as well as momentary time and normal state.
- Readers - Reports the reader properties, including mode, type, and card format information.
- Elevators - Displays the elevator information, including maximum floors and associated hardware.
- Cameras - Provides information on the cameras programmed into the system.
- Monitor Point Groups (MPG) - Displays the address and description for all MPGs in the system.
- Card Formats - Shows which card formats are stored in the selected controller(s).
- Doors - Displays the door information, including associated hardware.
- Door Contacts - Displays the door contact information for all doors in the system.
- Request to Exit (RTE) - Provides the REX information for all doors in the system.
- Door Strikes - Shows the lock information for all doors in the system.
- APB Doors - Reports information for all doors and access areas using Anti-Pass Back in the system.
- ASSA and Allegion Doors - Displays information for all ASSA and Allegion doors in the system.
- Operator SSP Assignments - Reports the Site, the Controller, and which operators are assigned to those SSPs.
- Bosch Panel Reports - Provides a list of Bosch reports including panels, areas, points, and outputs.
- Engage Reports - Provides a menu of Engage reports covering sites, gateways, and doors.

Personnel

- Companies - Displays the company information for all companies entered in the system, including the address.
- Personnel - Card Information - Shows all the cardholders in alphabetical order with their card numbers activation and deactivation dates, and card status.
- Personnel - General - Provides all the cardholders in alphabetical order along with their company, department job, title, work phone and employee identification.
- Personnel - Access - Reports all the cardholders in alphabetical order with their card numbers, assigned access level(s), and card status.
- Personnel - Groups - Displays the personnel groups and the cardholders associated with each group.
- Personnel - Summary - Provides a summary of the cardholder record including card number, card type, location, company, and department.
- Personnel - Daily Card Usage - Displays a report that can be viewed based on Cards Per Day Only or Cards Per User. The report will provide the total number of cards used on a daily basis.
- Personnel - Printed - Generates a report that displays the date a card was printed along with the cardholder's name and card number.
- Personnel - Schindler - Generate a report that displays the name card number, department, and profile/access of personnel accessing Schindler specific devices.

Restored Archive Data

- Acknowledged Alarms - Displays any restored acknowledged alarms based on the defined parameters.
- Audit Trail - Displays any restored audit trail events based on the defined parameters.
- Event History - Displays any restored event history (transactions) based on the defined parameters.

System

- Audit Trail - Displays the operator's actions based on the defined parameters.
- Holidays - Shows the holidays that have been programmed into the system, including the date and duration of the holiday.
- Macros - Provides information on the system macros, including action and hardware address.
- Time Schedules - Reports the time schedules that have been programmed in to the system, including begin and end times as well as the days of the weeks.
- Triggers - Displays information on the system triggers, including the trigger event, trigger address and the linked macro information.
- Auto Armed Secured Areas - Generates a report that shows the auto arm information for Secured Areas.
- Host Based Macros - Generates a report that displays the Event ID, Action, and Parameters of a host based macro. The report can be specified by hardware types.
- Door Follows Time Schedule Report - Provides information on each door's time schedule setting as well as any one-time scheduled events.
- Station Status - Displays the sites client workstation information including the station name, IP address, current operator, status, badging station status, and last login information.
- Operators - Shows the operators within the system, the assigned operator profiles, the administrator settings, and the last logon information.

Custom Reports

All custom reports created in the system are displayed here. See page 17-7 for more information.

NOTES:

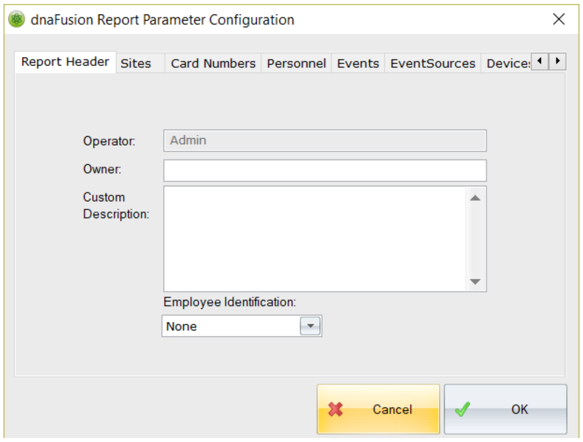
Generating a Report

1. To open any of these reports, **select** Reports from the Main Menu.
2. **Select** the desired report from one of the menu categories.

   For example, to open the Events History report from the Events category, **select** Reports / Events / Events History from the Main Menu.

   The DNAFusion Report Parameter Configuration dialog appears.

   > *If* Enable Tenants (Segregation) *is checked in the* DNA Properties *dialog, an additional tab labeled* Tenants *will appear in the* Report Parameter Configuration *dialog. The operator can only filter the report by tenants assigned to their operator profile. See page 4-14 for more information.*



dnaFusion Report Parameter Configuration

Operator: Admin

Owner:

Custom Description:

Employee Identification: None

3. **Complete** the Report Header information.

   The information will appear on the report banner on the first page.

   The Operator field will default to the operator who is currently logged in. The Owner is the person who requested the report. The Custom Description field is a general description of the report.

   If needed, select the Employee Identification to use: Employee Number or Employee ID
4. Use the tabs to **configure** the remaining Parameters for the selected report.

   Each tab will display a separate dialog with a list of items.

   For tabs with multiple attributes, the list can be sorted by the different columns by clicking on the column header. An asterisk (*) designates the active sort field.
5. **Click** OK.

   The selected report will generate.

   Once a report is open, the Reports options in the Main Menu change to allow the user to reconfigure the report. To edit the parameters of an open report, select Reports / Parameters from the Main Menu.

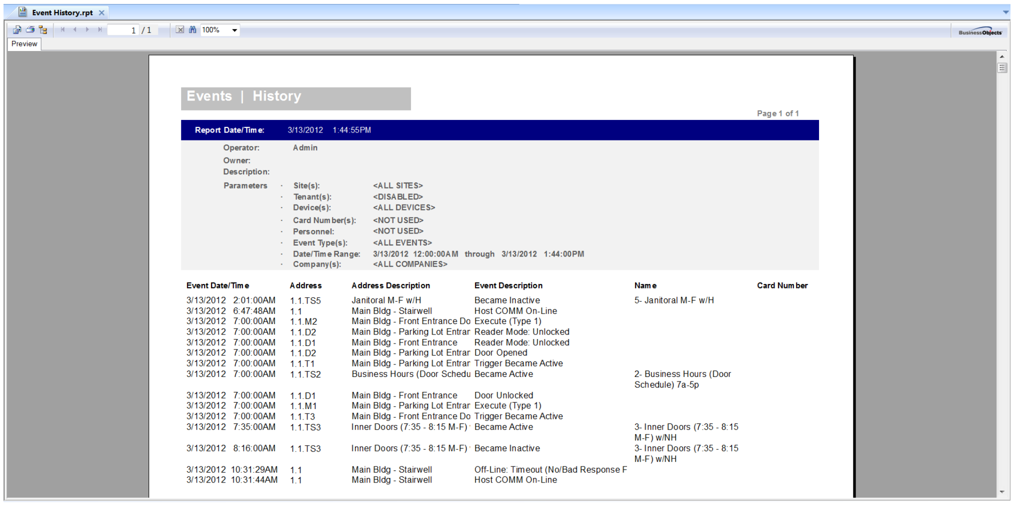
Reports Toolbar

DNA Fusion provides a Reports Toolbar that allows the operator to quickly filter and print the report.

🔄	Report Refresh Icon - Refreshes the active report. The Report Date/Time will update to the current date and time.
{ }	Report Parameters Icon - Displays the Report Parameter Configuration dialog for the active report.
SQL	Report SQL Icon - Displays the DNAFusion Report SQL Query dialog for the active report.
🖨	Print Report Icon - Displays the Print dialog to print the active report.
* “Active” refers to the top report if multiple reports are open.	

Navigating the Report

Report controls are also available from a toolbar located at the top of the report window. These icons allow the operator to navigate through the report, change the view, print the report, search the report for specific items, and even export the report to several destinations in a variety of formats.



Event History.rpt

1 / 1 100%

Preview

Events | History

Page 1 of 1

Report Date/Time: 3/13/2012 1:44:55PM

Operator: Admin
Owner:
Description:

Parameters
· Site(s): <ALL SITES>
· Tenant(s): <DISABLED>
· Device(s): <ALL DEVICES>
· Card Number(s): <NOT USED>
· Personnel: <NOT USED>
· Event Type(s): <ALL EVENTS>
· Date/Time Range: 3/13/2012 12:00:00AM through 3/13/2012 1:44:00PM
· Company(s): <ALL COMPANIES>

Event Date/Time	Address	Address Description	Event Description	Name	Card Number
3/13/2012 2:01:00AM	1.1.TS5	Janitoral M-F w/H	Became Inactive	5- Janitoral M-F w/H	
3/13/2012 6:47:48AM	1.1	Main Bldg - Stairwell	Host COMM On-Line		
3/13/2012 7:00:00AM	1.1.M2	Main Bldg - Front Entrance Do	Execute (Type 1)		
3/13/2012 7:00:00AM	1.1.D2	Main Bldg - Parking Lot Entrar	Reader Mode: Unlocked		
3/13/2012 7:00:00AM	1.1.D1	Main Bldg - Front Entrance	Reader Mode: Unlocked		
3/13/2012 7:00:00AM	1.1.D2	Main Bldg - Parking Lot Entrar	Door Opened		
3/13/2012 7:00:00AM	1.1.T1	Main Bldg - Parking Lot Entrar	Trigger Became Active		
3/13/2012 7:00:00AM	1.1.TS2	Business Hours (Door Schedu	Became Active	2- Business Hours (Door Schedule) 7a-5p	
3/13/2012 7:00:00AM	1.1.D1	Main Bldg - Front Entrance	Door Unlocked		
3/13/2012 7:00:00AM	1.1.M1	Main Bldg - Parking Lot Entrar	Execute (Type 1)		
3/13/2012 7:00:00AM	1.1.T3	Main Bldg - Front Entrance Do	Trigger Became Active		
3/13/2012 7:35:00AM	1.1.TS3	Inner Doors (7:35 - 8:15 M-F)	Became Active	3- Inner Doors (7:35 - 8:15 M-F) w/NH	
3/13/2012 8:16:00AM	1.1.TS3	Inner Doors (7:35 - 8:15 M-F)	Became Inactive	3- Inner Doors (7:35 - 8:15 M-F) w/NH	
3/13/2012 10:31:29AM	1.1	Main Bldg - Stairwell	Off-Line: Timeout (No/Bad Response F		
3/13/2012 10:31:44AM	1.1	Main Bldg - Stairwell	Host COMM On-Line		

💾	Export Report Icon - Displays the Export dialog. See page 17-9 for more information.
🖨	Print Report Icon - Displays the Print dialog. See page 17-9 for more information.
🗂	Toggle Group Tree Icon - Toggles an explorer that includes a tree of grouped report items.
⏮	Go to First Page Icon - Displays the first page of the report.
◀	Go to Previous Page Icon - Displays the previous page of the report.
▶	Go to Next Page Icon - Displays the next page of the report.
⏭	Go to Last Page Icon - Displays the last page of the report.
3 / 28	Page Number Indicator - Displays the current page number and the total pages in the report. To display a different page, **enter** the desired page number and **press** Enter.
☒	Stop Loading Icon - Stops the loading process and displays the last page of the partial load. The page indicator total will display the last page number and a "+" to indicate that only a portion of the information was loaded.
🔭	Search Text Icon - Displays the Search dialog and allows the operator to enter a character string. The application will find the next matching string of characters and will highlight them with a blue outlined box.
100% ▾	Zoom Control Icon - Drop-down menu to select the zoom percentage. The Zoom Control defaults to 100%.

Creating a Custom Report

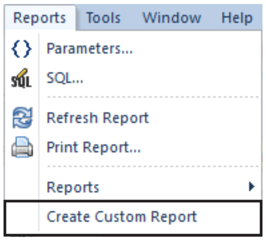
Users can create and maintain up to 20 customized reports. This is particularly useful when the operator wishes to save a report configuration that will be used repeatedly. After creating a custom report, the report is saved so the operator may recall or schedule it later.

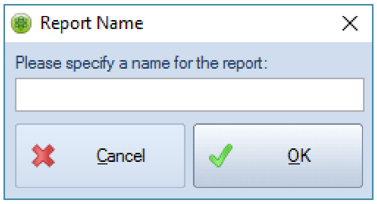
1. **Open** the desired report and **configure** the parameters with the exception of the Date/Time Range option.

   The report will open in the data window.

2. From the Reports tab of the Main Menu, **select** the Create Custom Report option.

   The Report Name dialog opens.





3. **Enter** a name for the report and **click** the OK button.

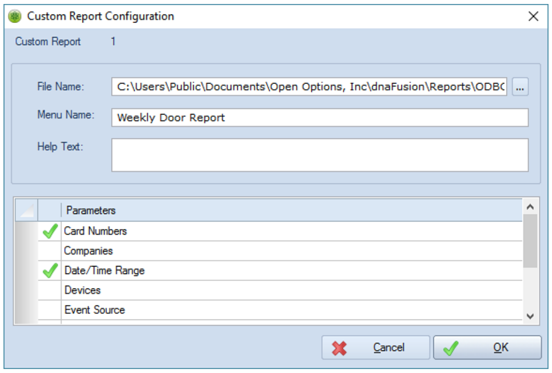
   The Custom Report Configuration dialog appears.

4. **Enter** a Menu Name and any desired Help Text.

   These entries will appear in the Reports menu.

5. **Select** any desired Parameters checkboxes.

   Parameters that are relevant to the selected report are available for selection. Checking a parameter will make it configurable when the report is generated. Leaving a parameter unselected will make it unavailable when the custom report is generated.



Custom Report 1

File Name: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\Reports\ODBC

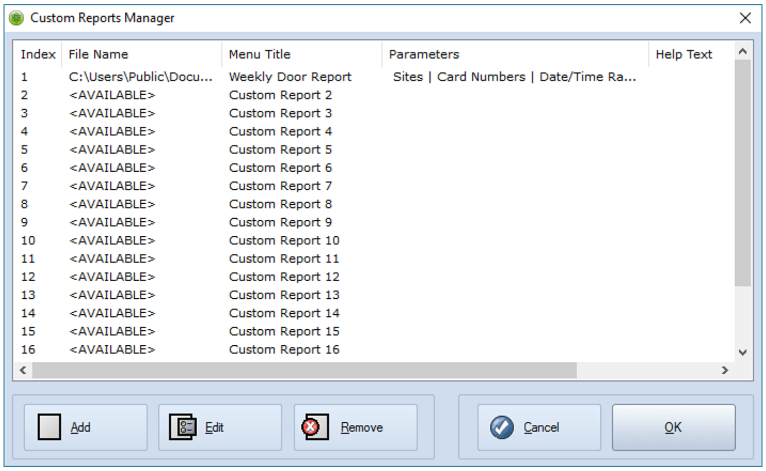
Menu Name: Weekly Door Report

Help Text:

	Parameters
✓	Card Numbers
	Companies
✓	Date/Time Range
	Devices
	Event Source

6. **Click** OK to save the report.

   The Custom Reports Manager dialog will appear and the new report will appear in the next available slot.



Index	File Name	Menu Title	Parameters	Help Text
1	C:\Users\Public\Docu...	Weekly Door Report	Sites | Card Numbers | Date/Time Ra...	
2	<AVAILABLE>	Custom Report 2		
3	<AVAILABLE>	Custom Report 3		
4	<AVAILABLE>	Custom Report 4		
5	<AVAILABLE>	Custom Report 5		
6	<AVAILABLE>	Custom Report 6		
7	<AVAILABLE>	Custom Report 7		
8	<AVAILABLE>	Custom Report 8		
9	<AVAILABLE>	Custom Report 9		
10	<AVAILABLE>	Custom Report 10		
11	<AVAILABLE>	Custom Report 11		
12	<AVAILABLE>	Custom Report 12		
13	<AVAILABLE>	Custom Report 13		
14	<AVAILABLE>	Custom Report 14		
15	<AVAILABLE>	Custom Report 15		
16	<AVAILABLE>	Custom Report 16		

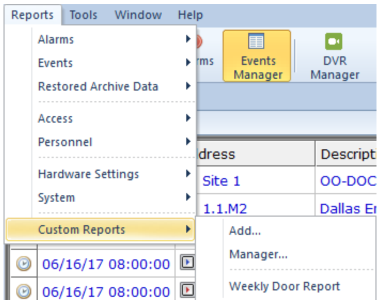
7. **Review** the custom report's configuration.

   Highlight the desired custom report in the list. The Add, Edit, and Remove buttons modify the selected report as indicated.

8. **Click** the OK button to save the dialog.

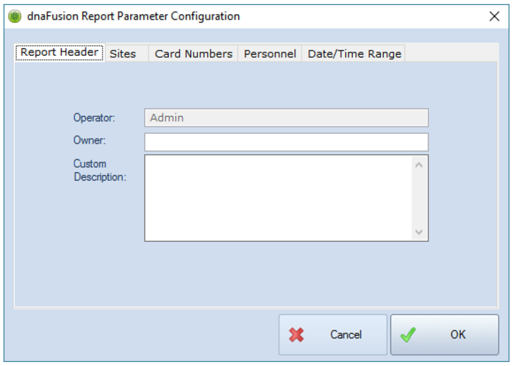
   The custom report is now listed in the Main Menu under Reports / Custom Reports.

Generating a Custom Report



1. To open a custom report, **select** Reports / Custom Report from the Main Menu.
2. **Select** the desired custom report from the resulting menu.

   The DNAFusion Report Parameter Configuration will appear with tabs based on the parameters selected in the Custom Report Configuration dialog.


dnaFusion Report Parameter Configuration

Operator: Admin

Owner:

Custom Description:

3. **Complete** the Report Header information.
4. Use the tabs to **configure** the remaining Parameters for the custom report.
5. **Click** OK.

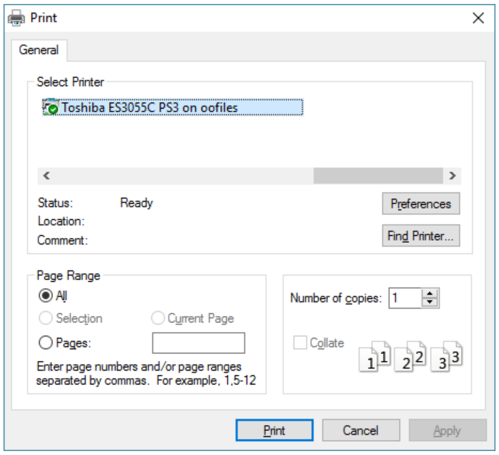
   The report will open in the data window.

   If desired, use the Reports tab in the Main Menu to adjust and control the report.

Printing a Report

1. With the desired report open, **click** the Print icon in the Reports Toolbar.

   The Print dialog opens.



Select Printer

Toshiba ES3055C PS3 on oofiles

Status: Ready

Location:

Comment:

Page Range

● All

○ Selection ○ Current Page

○ Pages:

Enter page numbers and/or page ranges separated by commas. For example, 1,5-12

Number of copies: 1

□ Collate

2. **Select** the desired printer from the Select Printer area.
3. **Select** or **enter** the Number of Copies.
4. **Click** the Print button.

Exporting a Report

1. With the selected report open, **click** the Export Report icon.

   The Export dialog appears.

2. **Select** a Format from the drop-down list and enter the parameters for the selected format.
   - Acrobat Format (PDF) - Maintains the original formatting of the report.
   - Crystal Reports (RPT) - Requires Crystal to open the report.
   - HTML 3.2 - Opens in an Internet window. Maintains the original formatting.
   - HTML 4.0 - Opens in an Internet window. Maintains the original formatting.

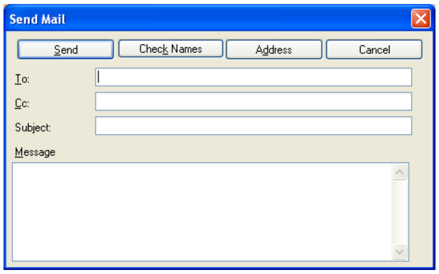
   > *The operator will need to specify a file path when exporting in an HTML format. The file name of the report and the file name of the "temp" file can not be the same.*

   - MS Excel 97-2000 (XLS) - Maintains the original formatting of the report.
   - MS Excel 97-2000-Data only (XLS) - Separates data into columns.
   - MS Word (RTF) - Maintains the original formatting of the report.
   - MS Word - Editable (RTF) - Maintains the original formatting of the report and allows for editing.
   - ODBC - Requires the selection of a dsn from the list.

   > *When exporting in ODBC format, "Application" and "Disk File" are the same.*

   - Record Style - Columns with spaces (REC) - Produces an EpiData file.
   - Record Style - Columns without spaces (REC) - Produces an EpiData file.
   - Report Definition (TXT) - Provides the report parameters in a .txt file
   - Rich Text Format (RTF) - Maintains the original formatting of the report.
   - Separated Values (CSV) - Excel format with data separated into rows.
   - Tab Separated Text (TTX) - Exports to a .ttx file.
   - Text (TXT) - Exports to a simple text file.
   - XML - Extensible Markup Language.

3. **Select** the Destination from the drop-down list.
    - Application - The report is exported directly to the application for the selected format type.
    - Disk File - The program saves the report to a file path location that the operator specifies. (Default)
    - Exchange Folder - The report is exported to a Microsoft® Exchange folder. The operator selects the folder, and the report is stored there in the format that the operator specifies. A Microsoft Exchange folder can contain standard notes (mail), files, and instances of Microsoft Exchange forms.
    - Lotus Domino - The report is exported to the Lotus Domino server.
    - Lotus Domino Mail - The program displays a dialog box through which the report may be e-mailed directly in the specified format to an email address that the operator enters. The operator may type a message and the report is attached by default.
    - Microsoft Mail (MAPI) - The program displays a dialog box through which the report may be e-mailed directly in the specified format to an email address that the operator enters. The operator may type a message and the report is attached by default.



4. Based on the selection above, **click** OK or Send when finished.

When exporting a report to MAPI, the e-mail application must be running simultaneously with DNA at the time the e-mail is configured AND at the time the e-mail is sent. A dialog will appear verifying the application can access Microsoft Outlook. Specify an amount of time and click Yes*.*

MS Outlook 2000 SP1 + SR1 and later editions will prompt the current Windows user for permission before allowing DNA to access it. Consequently, the Microsoft Mail destination option will not operate as an automatic functionality at the scheduled time.

Scheduling a Report

See page 19-9 for information on scheduling a report.

Graphic Maps 18

In This Chapter

- √ Creating Graphic Maps
- √ Linking Graphic Maps to Hardware & Hyperlinks
- √ Using Graphic Maps to Control Hardware
- √ Using Graphic Maps to Handle Alarms

Graphic maps are flexible tools used to visually represent an external hardware platform. A map can depict various hardware states via graphic objects and provide quick access to user commands, such as alarm acknowledgement, direct control, and object properties.

DNA Fusion also provides versatile audio capability, including customized status and alarm sounds as well as audio instruction.

Graphics

The graphic maps in DNA Fusion are object-oriented, which means they can be moved and manipulated as a single entity. Each graphic object's properties can be used to represent different hardware states and statuses. In addition, the maps may be linked together to create a drill-down effect or linked to external applications and websites.

Graphic maps have two modes: Design and Run. The design mode allows the operator to modify the graphic map and add, link, or configure graphic objects. The run mode locks a configured graphic object and disables modifications, but allows the operator to control hardware devices and alarms from the graphic map.

Graphics Toolbar

The Graphics Toolbar allows the operator to draw and customize objects on a graphic map.

Icon	Command	Description
↖	Select	Selects an object in the graphic map.
╲	Line	Draws a line.
▭	Rectangle	Draws a rectangle. Can represent an object's state using background and foreground colors.
⬭	Oval	Draws an oval. Can represent an object's state using background and foreground colors.
	Polyline	Draws a polyline (unclosed) object.
	Polygon	Draws a polygon (closed) object. Can represent an object's state using background and foreground colors.
↗	Pointer	Draws an arrow.
✎	Freehand	Draws a freehand object.

Icon	Command	Description
🖍	Hi Lite	Highlights an object.
▨	Redact	Blocks a selected portion of the graphic map to prevent visibility. Can be used to link the user to other pages, objects, zoom levels, and macros. Can also be used to make video containers.
ab|	Text	Creates a text object.
🗒	Note	Displays a text notepad with a colored background. Can show state using the background color (translucent).
▭	Stamp	Creates a boxed text stamp object. Can show state using a linked file.
▾	Rubber Stamp	Creates a stamp object with predefined text selected from the drop-down list. Can show state using a linked file.
📌	Hot Spot	Creates a "hotspot" button on the graphic map that can be used as a link to another page.
📌	Freehand Hotspot	Draws a freehand "hotspot" button on the graphic map that can be used as a link to another page.
▭	Button	Creates a text button that can be used to link the user to other pages, objects, zoom levels, and macros.
⊗	Point	Places a cross-hair object. Can show state using a file (.bmp, .jpg, icon, etc.). Used to link cameras.
🔊	Audio	Creates an object for playing various audio formats. Allows you to change the file automatically when an alarm condition occurs. Can be used to detect a change in state.
🎥	Video	Creates a video object for playing various video files or linking to a capture card. Allows you to change the file automatically upon an alarm. Can be used to detect a change in state.
📏	Ruler	Draws a line with measurement (in millimeters).
┼	Cross Product	Draws a cross hair object with measurements (in millimeters).
∧	Protractor	Draws a protractor object to measure the angle (in degrees) between two points.
📌	Pushpin	Creates an object that expands to reveal additional text when selected. When Run Mode is selected, the map changes and the text box expands to reveal detailed text.
🖌	Design	If selected, activates toolbar icons on the Graphics Toolbar and allows the user to edit the graphic map.
▶	Run	If selected, disables toolbar icons on the Graphics Toolbar and activates the graphic map. Graphic objects are not editable in this mode.

Graphic Alignment Toolbar

The Graphic Alignment Toolbar is used to align objects on the graphic map. The following graphic alignment commands are available from the toolbar.

Icon	Command	Description
	Align Center	Aligns the object with the center of the selected objects.
	Align Left	Aligns the object with the left edge of the selected objects.
	Align Right	Aligns the object with the right edge of the selected objects.
	Align Top	Aligns the object with the top of the tallest objects selected.
	Align Bottom	Aligns the object with the bottom of the shortest objects selected.
	Space Horizontally	Evenly spaces the selected objects even horizontally.
	Space Vertically	Evenly spaces the selected objects even vertically.
	Same Size	Makes the selected objects the same size.
	Same Height	Makes the selected objects the same height.
	Same Width	Makes the selected objects the same width.
	Flip	Flips the selected object.
	Rotate	Opens the Rotation Degrees dialog to set the Rotation degree for the selected object.
	Rotate 90˚	Rotates the selected object 90 degrees.
	Rotate 180˚	Rotates the selected object 180 degrees.
	Rotate 270˚	Rotates the selected object 270 degrees.

NOTES:

Creating a New Graphic Map

Graphic maps are built on an existing graphic page such as a floor map or building diagram. Most available graphic formats are supported in DNA Fusion.

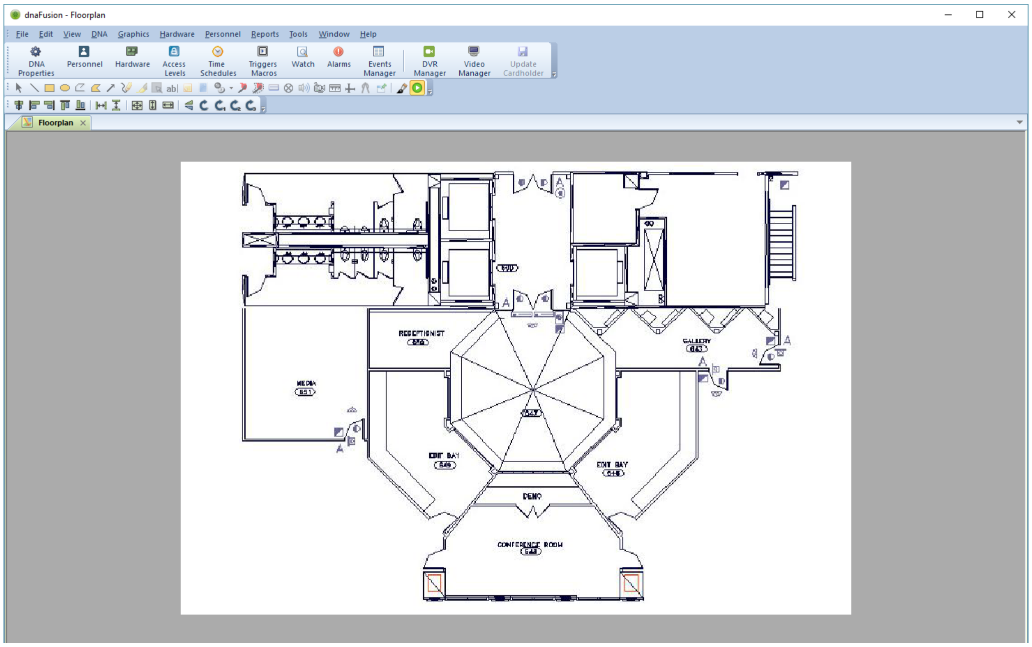
To create a graphic map:

1. **Select** File / Graphic Maps / Design (New) from the Main Menu.

   The Open File dialog appears. Files should be in the .jpeg or .bmp format.

2. **Browse** to the desired graphic file and **click** Open.

   The graphic map loads in the data window.



When a graphic map is active in the data window, the Graphics *option will be available from the* Main Menu *as an alternative to the toolbars.*

3. **Select** Design Mode from the Graphics Toolbar.

   The tools on the Graphics Toolbar become available for selection.

4. **Configure** the graphic map using the Graphics Toolbar and the Graphic Alignment Toolbar.

   The selected tool will remain active until another object is selected.

5. **Right-click** on the object to configure each object's properties, such as foreground/background colors, font, fill, text, etc.

6. After an object's properties are configured, **choose** from the following options:

   - Leave the object as a simple visual presentation.
   - Link the object to a live hardware point. See page 18-7.
   - Link the object to a hyperlink object, such as an external website or program. See page 18-9.
   - Link the object to another DNA Fusion graphic map. See page 18-9.

7. When the map is complete, **select** File / Graphic Maps / Save As and **enter** a File Name for the map.

   The graphic map will be saved as a .dng (DNA Graphic File). If the original file source changes, the .dng file will be automatically updated to the new image.

Graphic maps may be stored in any directory accessible to the computer as long as the Graphic Maps *option in the* DNA Directories *dialog points to the correct location. Ensure that the chosen location is always available when requested and does not require special mappings and/or network identifications. See page 20-1 for more information.*

NOTES:

Linking to Hardware

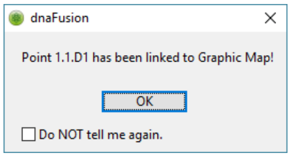
Use one of two methods to link hardware to a graphic object:

- Drag & Drop
- Manually Link

Drag & Drop

1. **Open** the Hardware Browser.
2. **Drag** and **drop** the hardware component to the graphic object.

   A confirmation dialog appears.



dnaFusion

Point 1.1.D1 has been linked to Graphic Map!

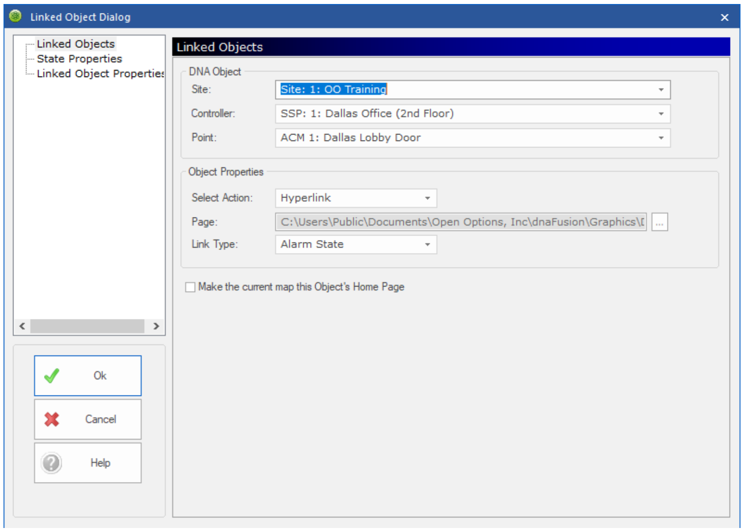
□ Do NOT tell me again.

3. **Click** OK to confirm the link.
4. **Right-click** on the linked object and **select** Linked Object Properties to configure the point (see steps 4 through 12 in the Manually Link section).

Manually Link

1. **Right-click** on the graphic object.
2. **Select** Link Hardware and the hardware you wish to link.

   The Linked Object Dialog will appear for the selected hardware object.



Linked Object Dialog

Linked Objects

DNA Object

Site: Site: 1: OO Training

Controller: SSP: 1: Dallas Office (2nd Floor)

Point: ACM 1: Dallas Lobby Door

Object Properties

Select Action: Hyperlink

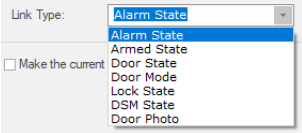
Page: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\Graphics\[

Link Type: Alarm State

□ Make the current map this Object's Home Page

3. **Configure** the address for the object by **selecting** the Site, Controller, and Point, if applicable.
4. **Select** the Action to occur when the object is selected.
   - None - No action.
   - Control/Ack (default) - Opens the Direct Control Dialog when the object is not in alarm or the Alarm Acknowledgement Dialog when the object is in alarm.
   - Control - Opens the Direct Control Dialog.
   - Acknowledge - Opens the Alarm Acknowledgement Dialog when the selected object is in alarm.
   - Page Zoom - Zooms to another page when the object is selected. When Page Zoom is selected, the Page field becomes active and the operator may select a graphic page to load in the application.
   - Hyperlink - Opens a web page or runs an external program.
5. **Select** the Link Type from the drop-down list.

   Indicates the type of state this link will monitor; the drop-down options will change based on the hardware type. This setting determines the available options on the Status Properties page.
6. If desired, **check** Make the current map this Object's Home Page to display the current graphic map whenever an alarm occurs at the hardware address.

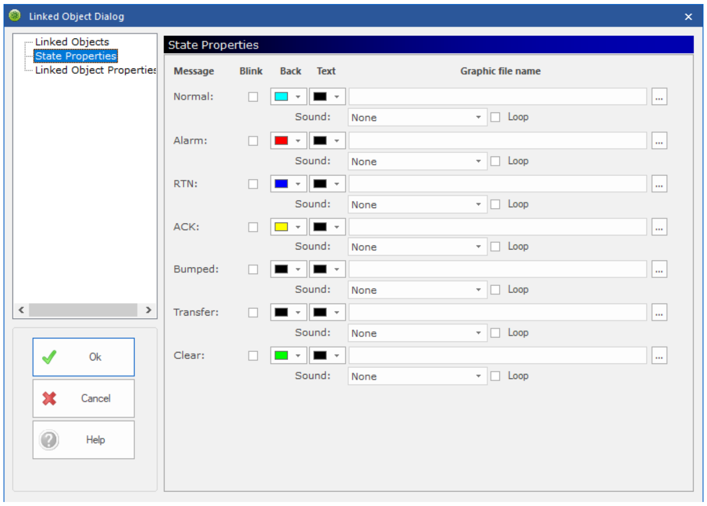


Link Type: Alarm State

□ Make the current

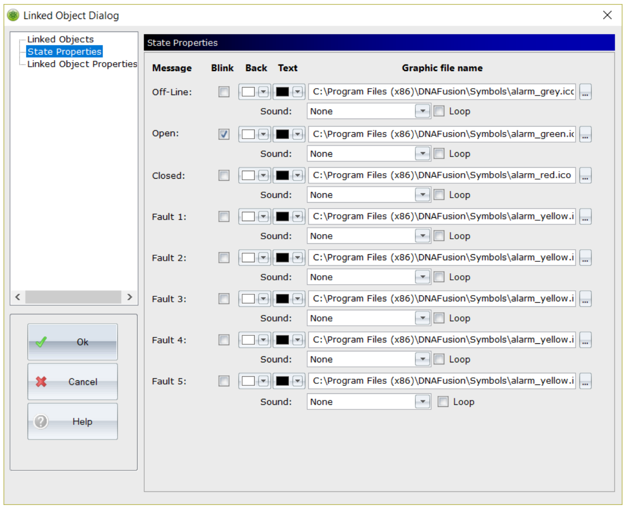
7. **Select** State Properties from the dialog menu.

   The State Properties dialog opens. State Properties are determined by the Link Type selected in Step 6.



State Properties

Message	Blink	Back	Text	Graphic file name	Sound	Loop
Normal:	□	🟦	■		None	□
Alarm:	□	🟥	■		None	□
RTN:	□	🟦	■		None	□
ACK:	□	🟨	■		None	□
Bumped:	□	■	■		None	□
Transfer:	□	■	■		None	□
Clear:	□	🟩	■		None	□



State Properties

Message	Blink	Back	Text	Graphic file name	Sound	Loop
Off-Line:	□	□	■	C:\Program Files (x86)\DNAFusion\Symbols\alarm_grey.icc	None	□
Open:	☑	□	■	C:\Program Files (x86)\DNAFusion\Symbols\alarm_green.ic	None	□
Closed:	□	□	■	C:\Program Files (x86)\DNAFusion\Symbols\alarm_red.ico	None	□
Fault 1:	□	□	■	C:\Program Files (x86)\DNAFusion\Symbols\alarm_yellow.i	None	□
Fault 2:	□	□	■	C:\Program Files (x86)\DNAFusion\Symbols\alarm_yellow.i	None	□
Fault 3:	□	□	■	C:\Program Files (x86)\DNAFusion\Symbols\alarm_yellow.i	None	□
Fault 4:	□	□	■	C:\Program Files (x86)\DNAFusion\Symbols\alarm_yellow.i	None	□
Fault 5:	□	□	■	C:\Program Files (x86)\DNAFusion\Symbols\alarm_yellow.i	None	□

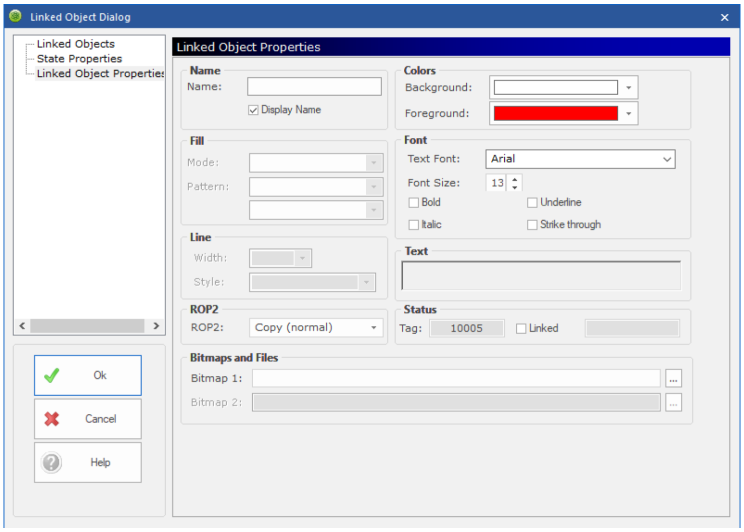
8. **Configure** the properties of the desired state(s).

   Each state can be assigned a unique sound to various alarm conditions/points as they are geographically represented on the map. The sound can be any .wav file available to the system.

   - Blink - If checked, the graphic object will blink when the selected alarm state occurs.
   - Back - Select the background color for the graphic object from the drop-down.
   - Text - If using text, select the text color from the drop-down.
   - Graphic File - If using a graphic file, click the Browse ... button to find the location.
   - Sound - If desired, select a sound from the drop-down to assign a unique sound to each alarm state.
   - Loop - If checked, the sound will continue to play on a loop until another action occurs.

9. **Select** Linked Object Properties from the dialog menu.

   The Linked Object Properties dialog opens.



Name
Name:
☑ Display Name

Colors
Background: □
Foreground: 🟥

Fill
Mode:
Pattern:

Font
Text Font: Arial
Font Size: 13
□ Bold □ Underline
□ Italic □ Strike through

Line
Width:
Style:

Text

ROP2
ROP2: Copy (normal)

Status
Tag: 10005 □ Linked

Bitmaps and Files
Bitmap 1:
Bitmap 2:

10. **Configure** the properties of the linked graphic object.

    The available fields will change based on the type of graphic object selected.

11. **Click** OK to save the dialog(s).

12. **Select** File / Graphic Maps / Save from the Main Menu to save the graphic map.

> **Right-click** *on the graphic map to set the* Default Properties *for graphic objects. Any objects added to the graphic map will automatically assume the configured properties.*

Creating Hyperlinks

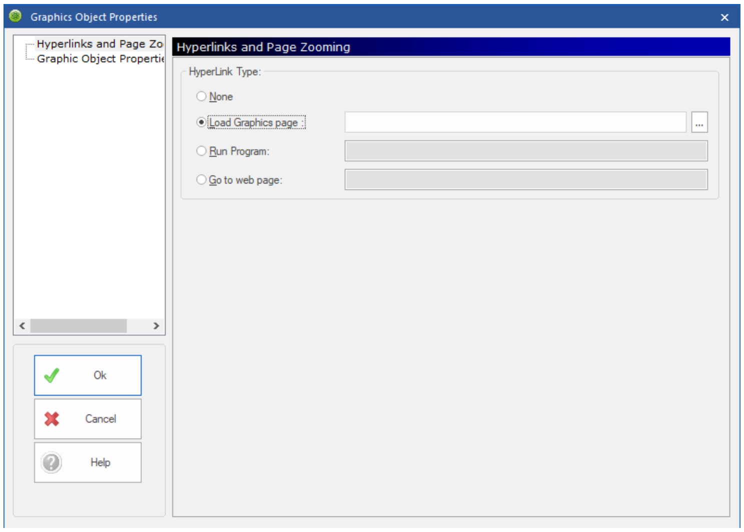
The operator can create three types of hyperlinks:

- Links to other DNA pages
- Links to external programs
- Links to web sites

To create a hyperlink:

1. **Create** the desired object, i.e., button or hotspot.
1. **Right-click** on the object you wish to link and **select** Object Properties / Hyperlink.

   The Graphics Object Properties / Hyperlinks and Page Zooming dialog opens.



HyperLink Type:

○ None

● Load Graphics page :

○ Run Program:

○ Go to web page:

2. **Select** the desired Hyperlink Type:
   - None - If selected, the object will not be associated with a hyperlink.
   - Load Graphics Page - If selected, **click** the Browse button to link the object to a DNA graphic page.
   - Run Program - If selected, **enter** an executable file (.exe) to link the object to an external application.
   - Go to Web Page - If selected, **enter** a web address to link the object to a web site.
3. If desired, **select** Graphic Object Properties from the dialog menu and **configure** the properties.
4. **Click** OK to save the dialog(s).
5. **Select** File / Graphic Maps / Save from the Main Menu to save the graphic map.

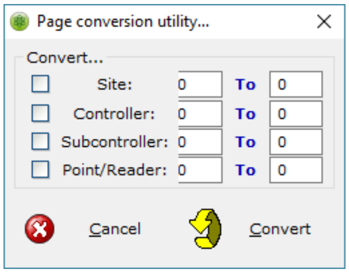
Page Conversion Utility

The Page Conversion Utility expedites the development of similarly constructed pages.

To use this tool:

1. **Load** a configured graphic map.
2. **Select** File / Graphic Maps / Save As.
3. **Enter** a new File Name and **click** Save.
4. **Select** Design Mode from the Graphics Toolbar.
5. **Select** Graphics / Hardware Linkage / Page Conversion from the Main Menu.

   The Page Conversion Utility dialog opens.



Page conversion utility...

Convert...

□	Site:	0	To	0
□	Controller:	0	To	0
□	Subcontroller:	0	To	0
□	Point/Reader:	0	To	0

6. **Select** the object(s) to convert by **checking** the appropriate checkbox(es).
7. **Enter** the Site number to Convert From.
8. **Enter** the Site, Controller, Subcontroller and/or Point/Reader to Convert To.
9. **Select** the Convert button to convert the addresses of all objects.
10. **Select** Cancel to close the dialog.
11. **Select** File / Graphic Maps / Save from the Main Menu to save the page with the new addresses.

Linked Page Objects

A number of graphic objects are useful when designing graphic maps. For a list of all available graphic objects, see the Graphics Toolbar on pages 18-1 and 18-2.

Buttons

A button can be used as a link to other pages; it is especially useful when linked to a hardware object for control purposes.

1. **Select** the Button icon from the Graphics Toolbar.
2. **Draw** the Button on the graphic map.
3. **Right-click** on the button and **select** one of the following options:
   - Link to Graphics Page - Opens the Hyperlinks and Page Zooming dialog to link the graphic object to another graphic page, an external program, or a website. See page 18-9 for more information.
   - Link Hardware - Opens the Linked MACRO Dialog to link the graphic object to a specific hardware address for control purposes. See page 18-7 for more information.
4. If desired, **right-click** on the button and **select** Button Properties to format and configure the button's appearance.
5. **Click** OK to close the dialog.

Hi-Lite Tool

The hi-lite tool uses colors to represent state changes.

1. **Select** the Hi-Lite icon from the Graphics Toolbar.
2. **Draw** the Hi-Lite area on the map.
3. **Link** the Hi-Lite area to a hardware object as described on page 18-7.
4. **Right-click** on the Hi-Lite area and **select** Linked Object Properties.
5. **Select** a Select Action for the object.
6. **Select** the Link Type (this is the state being monitored by the hi-lite object).
7. **Select** State Properties from the dialog menu and **configure** the states as described on page 18-8.

   The State Properties are determined by the Link Type selected in Step 6.
8. **Select** a color from the Back drop-down to set the object's background color.
9. **Click** OK to close the dialog.

Point Tool

The point tool can depict state changes using a file such as a bitmap (.bmp), JPEG (.jpg), or icon (.ico). It can also be used to link a camera to a graphic map; see page 18-12 for more information.

1. **Select** the Point icon from the Graphics Toolbar.
2. **Place** the Point on the graphic map.
3. **Link** the Point to a hardware object as described on page 18-7.
4. **Right-click** on the Point area and **select** Linked Object Properties.
5. **Select** a Select Action for the object.
6. **Select** the Link Type (this is the state being monitored by the point object).
7. **Select** State Properties from the dialog menu and **configure** the states as described on page 18-8.

   The State Properties are defined by the Link Type selected in Step 6.
8. **Click** the Browse button to locate the graphic file for each state.
9. **Click** OK to close the dialog.

Pushpin Tool Icon

The pushpin tool can display a number of items, including the cardholder's photo and event text.

1. **Select** the Pushpin icon from the Graphics Toolbar.
2. **Draw** the Pushpin area on the map.
3. **Link** the Pushpin to a hardware object as described on page 18-7.
4. **Right-click** on the Pushpin area and **select** Linked Object Properties.
5. **Select** a Select Action for the object.
6. **Select** the Link Type (this is the state being monitored by this object).
   - Photo Detail Combo - Displays the cardholder's photo as well as any configured event text.
7. **Select** State Properties from the dialog menu and **configure** the states as described on page 18-8.

   The State Properties are defined by the Link Type selected in Step 6.
8. **Click** the Browse button and **select** the desired Replacement Text (see Appendix D).
9. **Click** OK to close the dialog.

Cameras

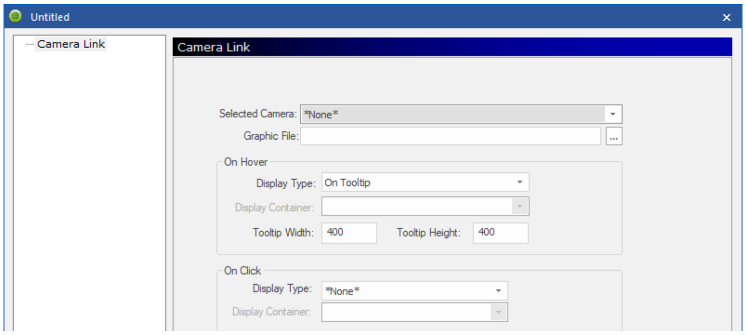
To view a camera on a graphic map, the operator must either send the video to a static container or display it via tooltip. This feature is only available if DVR/NVR Cameras are integrated with DNA Fusion.

1. If sending to a static container, **select** the Redact icon from the Graphics Toolbar.

   If displaying via tooltip, skip to Step 5.
2. **Draw** a Redact area on the graphic map to use as the video container.
3. **Right-click** on the Redact area and **select** Link Hardware / Make Video Container.

   The Video Container dialog opens.
4. **Enter** the Container Name and **click** OK.
5. **Select** the Point icon from the Graphics Toolbar.
6. **Place** the Point on the graphic map.
7. **Right-click** on the Point area and **select** Link Hardware / Link Camera.

   The Camera Link dialog appears.



Selected Camera: *None*

Graphic File: ...

On Hover

Display Type: On Tooltip

Display Container:

Tooltip Width: 400 Tooltip Height: 400

On Click

Display Type: *None*

Display Container:

8. **Select** the camera from the Selected Camera drop-down.
9. **Click** the Browse button next to the Graphic File field and **select** a file to display on the graphic map.
10. In the On Hover: Display Type drop-down, **select** the location to display the camera.
    - On Tooltip - Displays the camera in a tooltip on the Point object when the graphic map is in Run Mode; **configure** the Tooltip Width and Height fields to adjust the tooltip dimensions.
    - To Graphic Container - **Select** the desired video container from the Display Container drop-down list.
11. If desired, in the On Click: Display Type drop-down, **select** To Graphic Container and **specify** the desired Display Container to display the camera when the selected video container is clicked.
12. **Click** OK to save the settings.

Working with Existing Maps

Opening a Map

1. **Select** File / Graphic Maps / Open from the Main Menu.

   The Open File dialog appears.

2. **Browse** to the desired .dng file and **click** Open.

   The file opens in the data window.

Editing a Map

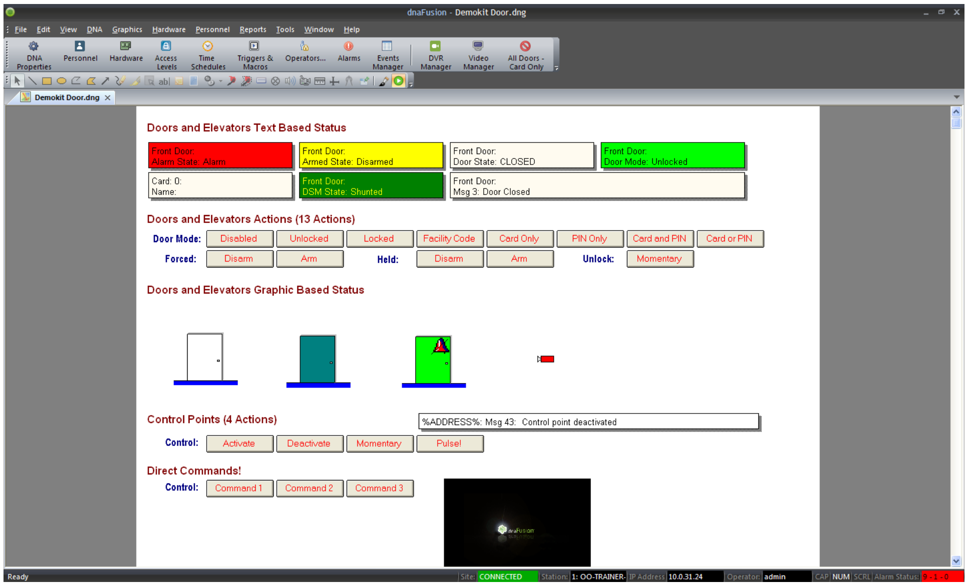
If the original source file changes, replace the image with a file named the same as the original source and the image will automatically be updated in the .dng file.

1. **Select** File / Graphic Maps / Open from the Main Menu.

   The Open File dialog appears.

2. **Browse** to the desired .dng file and **click** Open.

   The file opens in the data window.



Doors and Elevators Text Based Status

Front Door:
Alarm State: Alarm

Front Door:
Armed State: Disarmed

Front Door:
Door State: CLOSED

Front Door:
Door Mode: Unlocked

Card: 0:
Name:

Front Door:
DSM State: Shunted

Front Door:
Msg 3: Door Closed

Doors and Elevators Actions (13 Actions)

Doors and Elevators Graphic Based Status

Control Points (4 Actions)

%ADDRESS%: Msg 43: Control point deactivated

Direct Commands!

Ready | Site: CONNECTED | Station: 1: OO-TRAINER- | IP Address 10.0.31.24 | Operator: admin | CAP | NUM | SCRL | Alarm Status: 9 - 1 - 0

3. **Select** Design Mode from the Graphics Toolbar.

   The tools on the Graphics Toolbar become available for selection.

4. **Configure** the graphic map using the Graphics Toolbar and the Graphics Alignment Toolbar.

   The selected tool will remain active until another object is selected.

5. **Right-click** on the object to configure each object's properties, such as foreground/background colors, font, fill, text, etc.

6. After an object's properties are configured, **choose** from the following options:

   - Leave the object as a simple visual presentation.
   - Link the object to a live hardware point. See page 18-7.
   - Link the object to a hyperlink object, such as an external website or program. See page 18-9.
   - Link the object to another DNA Fusion graphic map. See page 18-9.

7. When the map is complete, **select** File / Graphic Maps / Save As, **enter** a File Name for the map, and **click** the Save button.

NOTES:

Using the Graphic Map

When a configured graphic map is set to Run Mode, operators can control a linked object, respond to alarms, and edit object properties.

Live Graphics Toolbar

DNA Fusion provides a Live Graphics Toolbar to control a configured graphic map. The following commands are available from the toolbar.

Icon	Command	Description
🔭	Locate	Opens the Locate Graphics Object dialog to search for a graphics object based on a hardware address or description.
⬇	Download	Displays the Download Manager dialog to download database information to the controller.
➡	Disarm All	Disarms all points on the graphic map.
⬅	ARM All	Arms all points on the graphic map.
✓	Acknowledge All	Acknowledges all alarms on the graphic map.

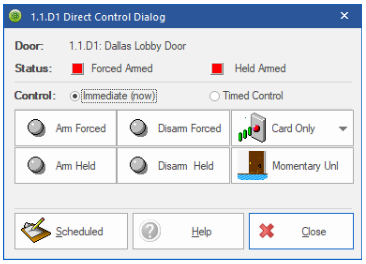
> *Press the plus (+) or minus (-) key to zoom in and out of the graphic map.*

Controlling a Linked Object

1. With the graphic map open, **right-click** on the desired object and **select** Direct Control.

   The Direct Control Dialog opens.

2. **Select** the option to control the point. For more information, see Chapter 8: Hardware Features.


1.1.D1 Direct Control Dialog

Door: 1.1.D1: Dallas Lobby Door

Status: 🟥 Forced Armed 🟥 Held Armed

Control: ● Immediate (now) ○ Timed Control

Acknowledging/Dismissing an Alarm

For more information on alarms, see Chapter 14: Events & Alarms.

1. **Right-click** on the alarm object in the graphic map and **select** Acknowledge or Acknowledge All.

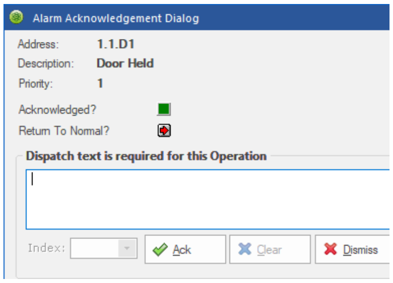
   The Alarm Acknowledgement Dialog appears.

2. If dispatch text is required, **enter** the Dispatch Text and **click** Ack.

   The alarm object's state will become Acknowledged. If the object's state has Returned to Normal, the Clear option will become available.

3. **Click** the Clear button to complete the alarm response process.

   If the object's state has not returned to normal, the Dismiss option may be selected. Dismiss requires the alarm status to be Acknowledged or Return to Normal to complete the alarm response cycle.


Alarm Acknowledgement Dialog

Address: 1.1.D1

Description: Door Held

Priority: 1

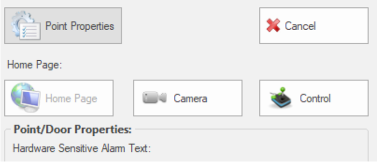
Acknowledged? 🟩

Return To Normal? ➡

Dispatch text is required for this Operation

4. If desired, **click** the Point Properties button to expand the dialog and view the following options:

   - Home Page - Opens the object's associated homepage, if applicable.
   - Camera - Opens the object's associated camera, if applicable.
   - Control - Opens the Direct Control Dialog for the selected object.
   - Point/Door Properties - Displays any Alarm Text for the selected object.


Home Page:

Point/Door Properties:

Hardware Sensitive Alarm Text:

> *All objects on the graphics map that are in alarm can be* Acknowledged *simultaneously by* **right-clicking** *on the object and* **selecting** *the* Acknowledge All *option.*

Arming/Disarming Linked Objects

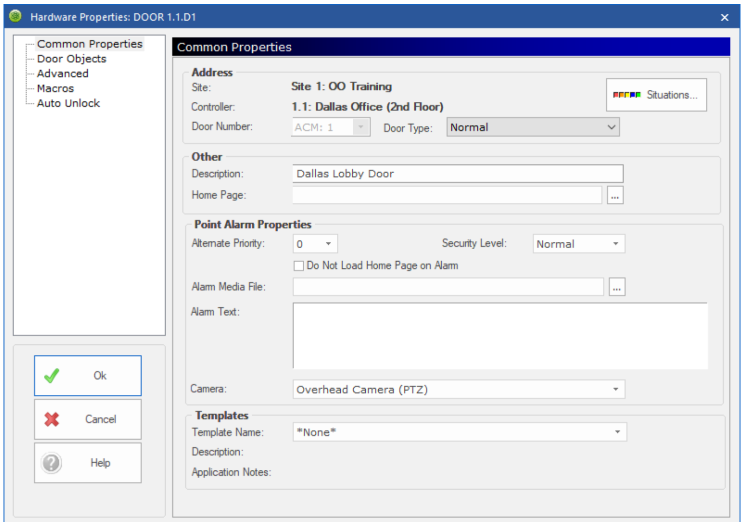
1. **Right-click** on the graphic object and **select** ARM All Inputs or Disarm All Inputs.

   The inputs are armed or disarmed.

Object Properties

1. **Right-click** on the object and **select** Point Properties.

   The Properties dialog for the selected object type opens.



Common Properties

Address

Site: Site 1: OO Training

Controller: 1.1: Dallas Office (2nd Floor)

Door Number: ACM: 1 Door Type: Normal

Other

Description: Dallas Lobby Door

Home Page:

Point Alarm Properties

Alternate Priority: 0 Security Level: Normal

□ Do Not Load Home Page on Alarm

Alarm Media File:

Alarm Text:

Camera: Overhead Camera (PTZ)

Templates

Template Name: *None*

Description:

Application Notes:

2. **Configure** or **edit** the dialog(s).

   For more information on hardware properties, see Chapter 8: Hardware Features.

3. **Click** OK to close the dialog.

Locking/Unlocking Objects

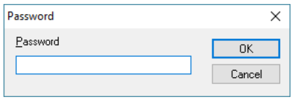
The operator can set a password requirement to prevent graphic objects from being moved or edited.

1. With a graphic map open in Design Mode, **right-click** on the desired graphic object and **select** Lock.

   OR

   Select Graphics / Page Objects / Lock Objects from the Main Menu.

   The Password or Password Needed dialog opens.

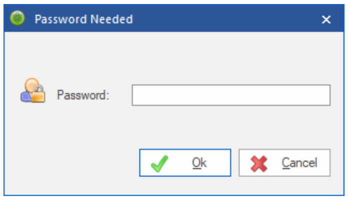


2. **Enter** a Password and **click** OK.

   A lock icon appears on the graphic object.

3. To unlock a locked object, **right-click** on the object, **select** Unlock All, and **enter** the Password created in Step 2.

   All objects with the designated password are unlocked.



Scheduling 19

In This Chapter

√ Creating and Editing Archive Data Schedules
√ Creating and Editing Batch File Schedules
√ Creating and Editing Download Schedules
√ Creating and Editing Report Schedules

The Scheduling feature is designed to eliminate repetitive tasks in DNA Fusion by automating or scheduling the tasks to perform on a one-time or recurring basis. Scheduling can be used to automatically complete a task when the operator is unavailable to do so manually; however, the host DNA application must remain open.

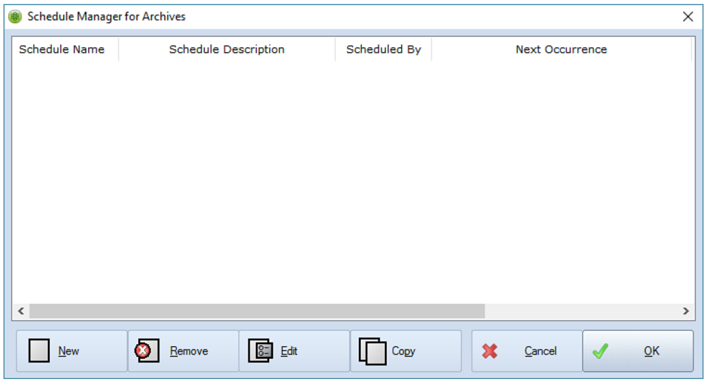
Schedules

DNA Fusion offers four types of scheduling:

- Archive Data - The Archive Data Schedule Configuration dialog allows the operator to simultaneously schedule archive times for three types of data: Acknowledged Alarms, Audit Trails (Operator Actions), and Transactions (Events History). The operator can also designate a number of days to keep each type of archived data. In DNA Fusion 7.0 a new Archive feature was released. The new feature is driver based and does not require the host application be open. See page 20-5 for more information.
- Batch Files - The Batch File Schedule Configuration dialog allows for additional flexibility under specific situations. Contact Open Options for more information on Batch Files.
- Downloads - The Download Schedule Configuration dialog allows the operator to schedule downloads for specific hardware components in the system, as well as panel resets and time schedule refreshes.
- Reports - The Report Schedule Configuration dialog is used to schedule reports based on specific parameters and properties, such as sites/tenants, date/time range, and report destination.

Schedule Manager

The scheduling process remains largely the same regardless of the schedule type. A separate Schedule Manager dialog is used to manage the schedules for each category.



- New - Opens the Schedule Configuration dialog to create a new schedule.
- Remove - Removes the selected schedule.
- Edit - Opens the Schedule Configuration dialog to edit an existing schedule.
- Copy - Duplicates the selected schedule and adds it to the Schedule Manager below the original schedule. The copy number will appear in parentheses at the end of the Schedule Name, e.g. (Copy #01).

> ! *DNA Fusion must remain open on the host computer to run a scheduled task. If the application is closed, the scheduled task will not run and an action prompt will appear the next time a user logs in to the system. Contact Open Options Technical Support for other scheduling options.*

This Page Intentionally Left Blank

Archive Data

The Archive Data option features the ability to simultaneously schedule three types of data (audit trails, acknowledged alarms, and transactions) to be archived on a one-time or recurring basis. In DNA Fusion 7.0 a new Archive feature was released. The new feature is driver based and does not require the host application be open. See page 20-5 for more information.

As more event information is stored in the database, the database grows larger. Archiving data allows you to remove old data from the database and create room for new information.

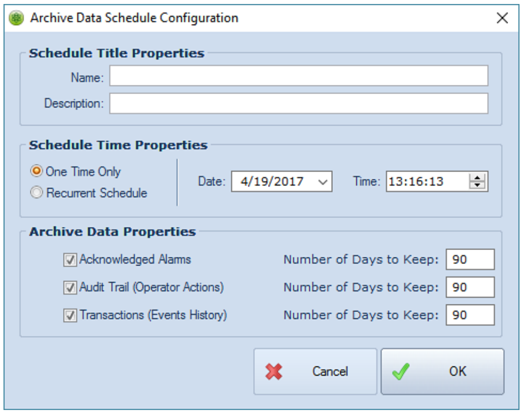
Creating a New Schedule

1. **Select** DNA / Administrative / Scheduling / Archive Data from the Main Menu.

   The Schedule Manager for Archives dialog appears.

2. **Click** the New button.

   The Archive Data Schedule Configuration dialog opens.



Archive Data Schedule Configuration

Schedule Title Properties

Name:

Description:

Schedule Time Properties

● One Time Only
○ Recurrent Schedule

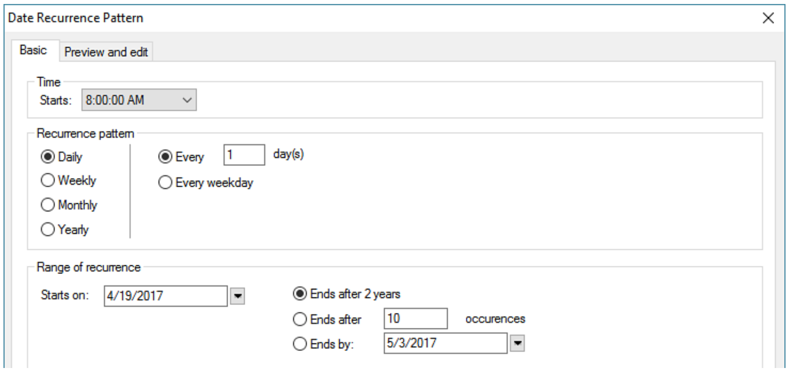
Date: 4/19/2017 Time: 13:16:13

Archive Data Properties

☑ Acknowledged Alarms Number of Days to Keep: 90
☑ Audit Trail (Operator Actions) Number of Days to Keep: 90
☑ Transactions (Events History) Number of Days to Keep: 90

3. **Enter** a Name and Description for the schedule.
4. To modify the recurrence of the schedule, **select** the Recurrent Schedule radio button.
5. **Click** the Modify Recurrence button. Modify Recurrence

   The Date Recurrence Pattern dialog appears.



Date Recurrence Pattern

Time

Starts: 8:00:00 AM

Recurrence pattern

● Daily ○ Weekly ○ Monthly ○ Yearly

● Every 1 day(s)
○ Every weekday

Range of recurrence

Starts on: 4/19/2017

● Ends after 2 years
○ Ends after 10 occurences
○ Ends by: 5/3/2017

6. **Configure** the dialog:
   - Time - **Select** a start time for the schedule from the drop-down menu.
   - Recurrence Pattern - **Select** an interval for the schedule to repeat.
   - Range of Recurrence - **Select** a start and end date for the recurring schedule.

> *The administrator may wish to establish a later* Ends By *date such as five years in the future. Note that projecting dates into the distant future with a frequent* Recurrence Pattern *will draw heavily from system resources and could take a long time to complete.*

7. **Click** OK to save the recurrence schedule and close the window.
8. **Select** the desired Archive Data Properties checkbox(es) and **enter** the desired Number of Days to Keep.
9. **Click** OK to save the schedule.

   The schedule is added to the Schedule Manager for Archives dialog.

Editing a Schedule

1. **Select** DNA / Administrative / Scheduling / Archive Data from the Main Menu.

   The Schedule Manager for Archives dialog opens.

2. **Select** the desired schedule and **click** Edit.

   The Archive Data Schedule Configuration dialog appears.

3. **Edit** the schedule as needed.

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

Deleting a Schedule

1. **Select** DNA / Administrative / Scheduling / Archive Data from the Main Menu.

   The Schedule Manager for Archives dialog opens.

2. **Select** the desired schedule and **click** Remove.

   The schedule is removed from the Schedule Manager.

Copying a Schedule

The purpose of the Copy function is to replicate an existing schedule's properties and apply them to a new schedule that will operate similarly. The operator should edit the copied schedule to prevent any duplicates.

1. **Select** DNA / Administrative / Scheduling / Archive Data in the Main Menu.

   The Schedule Manager for Archives dialog opens.

2. **Select** the desired schedule and **click** Copy.

   The schedule is duplicated in the Schedule Manager.

3. **Edit** the copied schedule.

Batch Files

The Batch Files option provides additional flexibility under specific situations. Contact Open Options for more information on Batch Files.

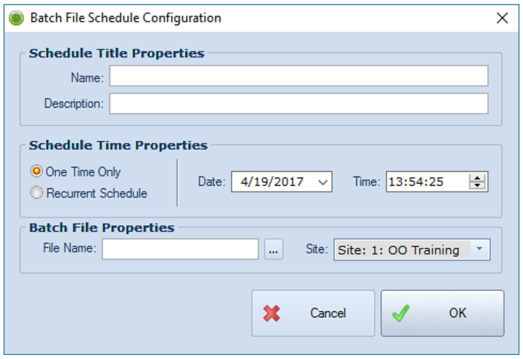
Creating a New Schedule

1. **Select** DNA / Administrative / Scheduling / Batch Files from the Main Menu.

   The Schedule Manager for Batch Files dialog opens.

2. **Click** the New button.

   The Batch File Schedule Configuration dialog appears.



Batch File Schedule Configuration

Schedule Title Properties

Name:

Description:

Schedule Time Properties

● One Time Only

○ Recurrent Schedule

Date: 4/19/2017

Time: 13:54:25

Batch File Properties

File Name:

Site: Site: 1: OO Training

3. **Enter** a Name and Description for the schedule.
4. To modify the recurrence of the schedule, **select** the Recurrent Schedule radio button.
5. **Click** the Modify Recurrence button. Modify Recurrence

   The Date Recurrence Pattern dialog appears.

6. **Configure** the dialog.

   See page 19-3 for more information.

7. **Click** OK to save the recurrence schedule and close the window.
8. **Locate** the batch file by selecting the Browse ... button.

   The Open dialog appears.

9. **Select** the batch file and **click** Open.
10. **Select** the Site from the drop-down list.
11. **Click** OK to save the schedule.

    The schedule is added to the Schedule Manager for Batch Files dialog.

Editing a Schedule

1. **Select** DNA / Administrative / Scheduling / Batch Files from the Main Menu.

   The Schedule Manager for Batch Files dialog opens.

2. **Select** the desired schedule and **click** Edit.

   The Batch Files Schedule Configuration dialog appears.

3. **Edit** the schedule as needed.
4. **Click** OK to save the changes.

Deleting a Schedule

1. **Select** DNA / Administrative / Scheduling / Batch Files from the Main Menu.

   The Schedule Manager for Batch Files dialog opens.

2. **Select** the desired schedule and **click** Remove.

   The schedule is removed from the Schedule Manager.

Copying a Schedule

The purpose of the Copy function is to replicate an existing schedule's properties and apply them to a new schedule that will operate similarly. The operator should edit the copied schedule to prevent any duplicates.

1. **Select** DNA / Administrative / Scheduling / Batch Files from the Main Menu.

   The Schedule Manager for Batch Files dialog opens.

2. **Select** the desired schedule and **click** Copy.

   The schedule is duplicated in the Schedule Manager.

3. **Edit** the copied schedule.

Downloads

The Downloads option allows the operator to schedule one-time or recurring downloads for specific hardware components. The download(s) can also be filtered by specific sites and/or controllers.

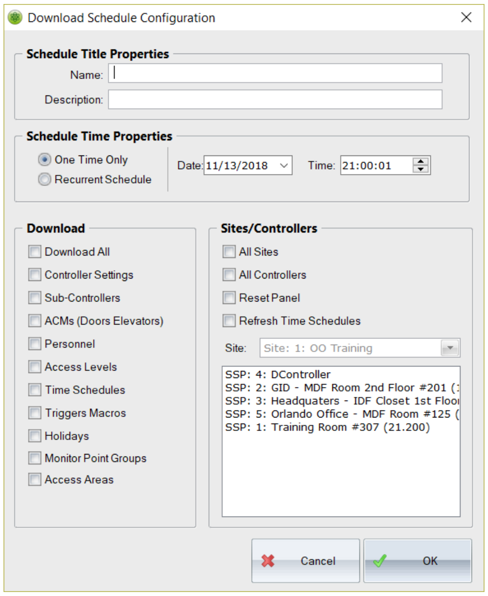
Creating a New Schedule

1. **Select** DNA / Administrative / Scheduling / Downloads from the Main Menu.

   The Schedule Manager for Downloads dialog appears.

2. **Click** the New button.

   The Download Schedule Configuration dialog opens.



Download Schedule Configuration

Schedule Title Properties

Name:

Description:

Schedule Time Properties

● One Time Only
○ Recurrent Schedule

Date: 11/13/2018 Time: 21:00:01

Download

- □ Download All
- □ Controller Settings
- □ Sub-Controllers
- □ ACMs (Doors Elevators)
- □ Personnel
- □ Access Levels
- □ Time Schedules
- □ Triggers Macros
- □ Holidays
- □ Monitor Point Groups
- □ Access Areas

Sites/Controllers

- □ All Sites
- □ All Controllers
- □ Reset Panel
- □ Refresh Time Schedules

Site: Site: 1: OO Training

```
SSP: 4: DController
SSP: 2: GID - MDF Room 2nd Floor #201 (1
SSP: 3: Headquaters - IDF Closet 1st Floor
SSP: 5: Orlando Office - MDF Room #125 (
SSP: 1: Training Room #307 (21.200)
```

3. **Enter** a Name and Description for the schedule.

4. To modify the recurrence of the schedule, **select** the Recurrent Schedule radio button.

5. **Click** the Modify Recurrence button. Modify Recurrence

   The Date Recurrence Pattern dialog appears.

6. **Configure** the dialog.

   See page 19-3 for more information.

7. **Click** OK to save the recurrence schedule and close the window.

8. **Select** the desired Download checkbox(es).

9. **Select** the desired Sites/Controllers options.

10. **Click** OK to save the schedule.

    The schedule is added to the Schedule Manager for Downloads dialog.

Editing a Schedule

1. **Select** DNA / Administrative / Scheduling / Downloads from the Main Menu.

   The Schedule Manager for Downloads dialog opens.

2. **Select** the desired schedule and **click** Edit.

   The Downloads Schedule Configuration dialog appears.

3. **Edit** the schedule as needed.

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

Deleting a Schedule

1. **Select** DNA / Administrative / Scheduling / Downloads from the Main Menu.

   The Schedule Manager for Downloads dialog opens.

2. **Select** the Event and **click** the Remove button.

   The schedule is removed from the Schedule Manager.

Copying a Schedule

The purpose of the Copy function is to replicate an existing schedule's properties and apply them to a new schedule that will operate similarly. The operator should edit the copied schedule to prevent any duplicates.

1. **Select** DNA / Administrative / Scheduling / Downloads from the Main Menu.

   The Schedule Manager for Downloads dialog opens.

2. **Select** the desired schedule and **click** Copy.

   The schedule is duplicated in the Schedule Manager.

3. **Edit** the copied schedule.

Reports

The Reports option allows the operator to schedule reports based on specific parameters and properties, such as sites/tenants, date/time range, and report destination.

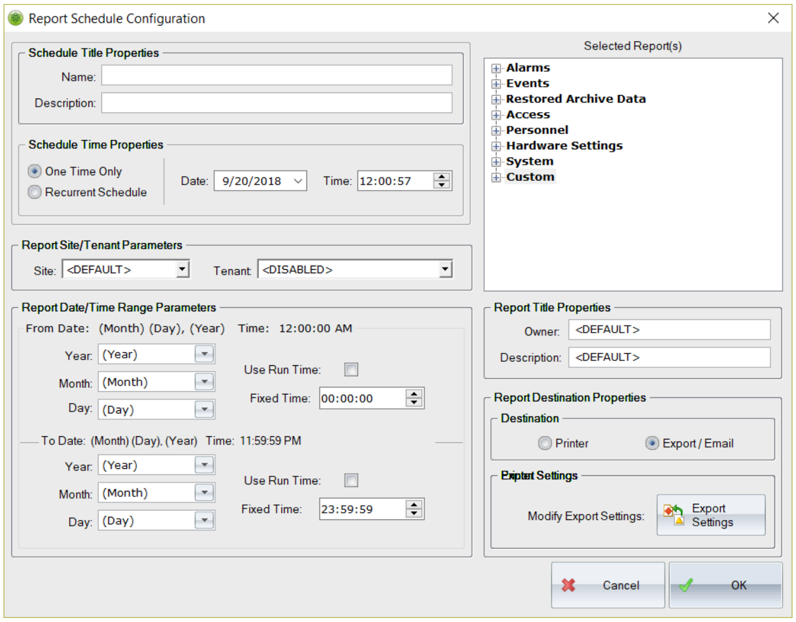
Creating a New Schedule

1. **Select** DNA / Administrative / Scheduling / Reports from the Main Menu.

   The Schedule Manager for Reports dialog opens.

2. **Click** the New button.

   The Report Schedule Configuration dialog appears.



Report Schedule Configuration

Schedule Title Properties
Name:
Description:

Schedule Time Properties
● One Time Only
○ Recurrent Schedule
Date: 9/20/2018
Time: 12:00:57

Report Site/Tenant Parameters
Site: <DEFAULT>
Tenant: <DISABLED>

Report Date/Time Range Parameters
From Date: (Month) (Day), (Year) Time: 12:00:00 AM
Year: (Year)
Month: (Month)
Day: (Day)
Use Run Time: □
Fixed Time: 00:00:00
To Date: (Month) (Day), (Year) Time: 11:59:59 PM
Year: (Year)
Month: (Month)
Day: (Day)
Use Run Time: □
Fixed Time: 23:59:59

Selected Report(s)
⊞ Alarms
⊞ Events
⊞ Restored Archive Data
⊞ Access
⊞ Personnel
⊞ Hardware Settings
⊞ System
⊞ Custom

Report Title Properties
Owner: <DEFAULT>
Description: <DEFAULT>

Report Destination Properties
Destination
○ Printer
● Export / Email
Export Settings
Modify Export Settings:

3. **Enter** a Name and Description for the schedule.
4. **Expand** the Selected Report(s) tree and **check** the desired report(s).
5. To modify the recurrence of the schedule, **select** the Recurrent Schedule radio button.
6. Click the Modify Recurrence button. Modify Recurrence

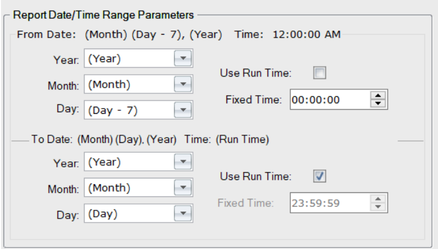
   The Date Recurrence Pattern dialog appears.

7. **Configure** the dialog.

   See page 19-3 for more information.

8. **Click** OK to save the recurrence schedule and close the window.
9. If desired, **select** Report Site and/or Tenant Parameters from the drop-down list(s).
10. **Select** the Report Date/Time Range Parameters using the drop-down menus for the From Date: Year/Month/Day and the To Date: Year/Month/Day.

    When capturing a time range, the parameter is determined from the date of the report, so that the parameters will be selected in terms of "report date minus x," i.e., From Date: -3 years, -6 months, or -2 days to To Date: –1 year, -5 months, or -1 day.



Report Date/Time Range Parameters
From Date: (Month) (Day - 7), (Year) Time: 12:00:00 AM
Year: (Year)
Month: (Month)
Day: (Day - 7)
Use Run Time: □
Fixed Time: 00:00:00
To Date: (Month) (Day), (Year) Time: (Run Time)
Year: (Year)
Month: (Month)
Day: (Day)
Use Run Time: ☑
Fixed Time: 23:59:59

    The Year parameters reach from –20 years to 2025; the Month parameters reach from –11 months to any of the specific months of the year; and the Day parameters reach from –30 days to the 31st day of the month or can be set simply to "the last day of the month (Last DOM)."

    If desired, **check** Use Run Time to use the scheduled run time as the basis for the report.

    The example above displays a scheduled report that will run weekly, based on the Recurrent Schedule, and provide information for the previous seven days of activity.

11. In the Report Title Properties section, **enter** the Owner and Description.

    The default owner is the operator currently logged in to DNA Fusion, and the default description is the Description entered in the Schedule Title Properties.

12. **Select** a Destination in the Report Destination Properties section.

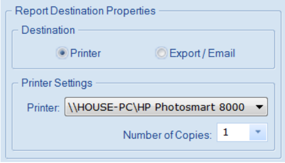
    - Printer - Sends the report to the specified Printer. See below for more information.
    - Export / Email - Opens the Export dialog. See below for more information.

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

    The schedule is added to the Schedule Manager for Reports dialog.

Printing a Scheduled Report

1. **Select** the Printer option in the Destination area.



Report Destination Properties

Destination

● Printer ○ Export / Email

Printer Settings

Printer: \\HOUSE-PC\HP Photosmart 8000

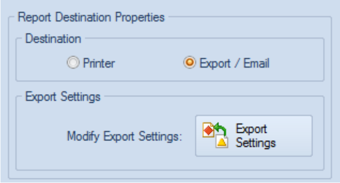
Number of Copies: 1

2. **Select** the desired printer from the drop-down list in the Printer Settings area.
3. **Select** the Number of Copies from the drop-down list. (Max. = 10)

Exporting a Scheduled Report

1. **Select** the Export / Email option in the Destination area.

   The Printer Settings area will become the Export Settings area.



Report Destination Properties

Destination

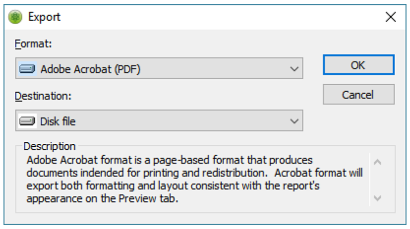
○ Printer ● Export / Email

Export Settings

Modify Export Settings:

2. **Click** the Export Settings button.

   The Export dialog opens.



Export

Format: Adobe Acrobat (PDF)

Destination: Disk file

Description

Adobe Acrobat format is a page-based format that produces documents indended for printing and redistribution. Acrobat format will export both formatting and layout consistent with the report's appearance on the Preview tab.

3. **Select** the Format and Destination from the drop-down lists.

   For more information on exporting a report, see page 17-7.

4. **Click** OK.
5. **Enter** any Parameters for the selected Format.

> ! *Whether exporting a report to an e-mail destination manually or via scheduling, the e-mail application must be running simultaneously with DNA Fusion at the time the e-mail is configured AND at the time the e-mail is to be sent. Contact Open Options Technical Support for other email options.*

Editing a Schedule

1. **Select** DNA / Administrative / Scheduling / Reports from the Main Menu.

   The Schedule Manager for Reports dialog opens.

2. **Select** the desired schedule and **click** Edit.

   The Reports Schedule Configuration dialog appears.

3. **Edit** the schedule as needed.

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

Deleting a Schedule

1. **Select** DNA / Administrative / Scheduling / Reports from the Main Menu.

   The Schedule Manager for Reports dialog opens.

2. **Select** the desired schedule and **click** Remove.

   The schedule is removed from the Schedule Manager.

Copying a Schedule

The purpose of the Copy function is to replicate an existing schedule's properties and apply them to a new schedule that will operate similarly. The operator should edit the copied schedule to prevent any duplicates.

1. **Select** DNA / Administrative / Scheduling / Reports from the Main Menu.

   The Schedule Manager for Reports dialog opens.

2. **Select** the desired schedule and **click** Copy.

   The schedule is duplicated in the Schedule Manager.

3. **Edit** the copied schedule.

This Page Intentionally Left Blank

System Settings & Maintenance 20

In This Chapter

System Settings

The system settings in DNA Fusion include driver setup and DNA directories.

Configuring DNA Directories

DNA Fusion stores various objects in default folders, including photos, templates, and graphic map files. Client machines will need access to the default storage locations in order to view photos and retrieve archived data.

Server and/or client directories should be configured if any of the following conditions apply:

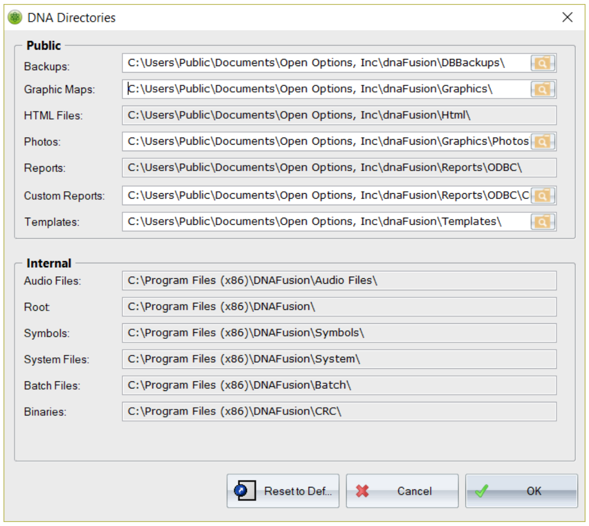
- Clients are connected to the server (Clients only if default locations are used on the server)
- Files are stored on the server in a location other than the default folders (Both server and clients)
- Files are stored on a network drive (Both server and clients)

To configure the directories:

1. With Fusion open, **select** DNA / Administrative / DNA Directories from the Main Menu.

   The DNA Directories dialog opens.

   The Backups, Graphic Maps, Photos, Custom Reports, and Templates directories can be directed to another location.



DNA Directories

Public

Backups: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\DBBackups\
Graphic Maps: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\Graphics\
HTML Files: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\Html\
Photos: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\Graphics\Photos
Reports: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\Reports\ODBC\
Custom Reports: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\Reports\ODBC\C
Templates: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\Templates\

Internal

Audio Files: C:\Program Files (x86)\DNAFusion\Audio Files\
Root: C:\Program Files (x86)\DNAFusion\
Symbols: C:\Program Files (x86)\DNAFusion\Symbols\
System Files: C:\Program Files (x86)\DNAFusion\System\
Batch Files: C:\Program Files (x86)\DNAFusion\Batch\
Binaries: C:\Program Files (x86)\DNAFusion\CRC\

2. **Click** the Browse button next to the desired directory.

   The Browse for Folder dialog opens.

   See page 20-10 for more information on the directory files.
3. **Locate** the desired folder and **click** OK.

   The server and all client machines must have the required permissions to access the selected location.
4. **Repeat** steps 2 through 3 until all the directories have been configured.
5. **Repeat** the above steps for the server and all client machines.
6. If needed, **click** the Reset to Default button to restore the default directories.
7. **Click** OK to save the dialog.

This Page Intentionally Left Blank

Driver Setup

The Driver Setup dialog includes a number of high-level settings, including Site Driver Behavior and E-mail Authentication.

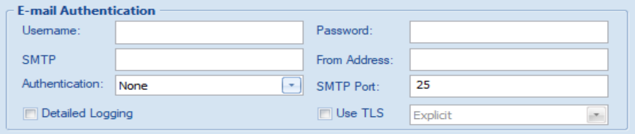
> *Use caution when configuring the* Driver Setup dialog*. The operator should be aware of the ramifications of their changes.*

E-mail Authentication

The E-mail Authentication dialog must be configured so DNA Fusion can send e-mails when the application is not open. Please note the DNA driver (DNAdrvr32) must be running in order for e-mails to be delivered.

1. **Select** DNA / Administrative / Driver Setup from the Main Menu.

   The DNA Site (Driver) Configuration dialog opens.



E-mail Authentication

Username:

Password:

SMTP

From Address:

Authentication: None

SMTP Port: 25

☐ Detailed Logging

☐ Use TLS

Explicit

2. **Enter** a Windows username in the Username field.
3. **Enter** the Password for the designated user.
4. **Enter** the Mail Server's Name in the SMTP field.

   If configured, the Mail Server's Name and Outbound Port information can be obtained by entering the following command from the Windows Command Prompt.

   Netsh diag connect mail

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

   Example:
   Mailer Server Name
   OutboundMailPort = 25
5. **Select** the Authentication mode from the drop-down list.
6. **Enter** a From Address for the e-mails.
7. If needed, **check** the Use TLS checkbox and **select** the correct Mode.
8. **Click** OK to save the settings.
9. **Verify** that the computer can connect to the Mail Server's port (25).

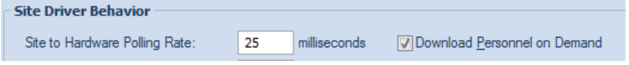
   If there is no connection to port 25, see the system administrator and request that SMTP be enabled and/or modify any anti-virus software to allow the DNA Fusion application (dnafusion.exe) to e-mail third parties.

Download Personnel on Demand

The Download Personnel on Demand option will only download cardholder information when the controller receives an access request. This reduces the amount of card information stored in the controller. By default, the option is turned off. If used, the operator can set individual SSPs to Exempt.

1. **Select** DNA / Administrative / Driver Setup from the Main Menu.

   The DNA Site (Driver) Configuration dialog opens.
2. **Check** the Download Personnel on Demand option.



Site Driver Behavior

Site to Hardware Polling Rate: 25 milliseconds

☑ Download Personnel on Demand

   When a card is presented with valid access, but no record is stored in the controller for the cardholder (Access Denied: Not In Card File), the cardholder's information will be downloaded to the controller. After the card is presented a second time, the cardholder will be granted access.
3. To designate a controller as Exempt, **select** the Download on Demand Exempt checkbox in the Controller Properties dialog and click OK.

   All cardholders with access will be downloaded to the controller. See page 8-49 for more information.

NOTES:

System Maintenance

Preventive maintenance tasks need to be performed regularly to ensure optimal system performance.

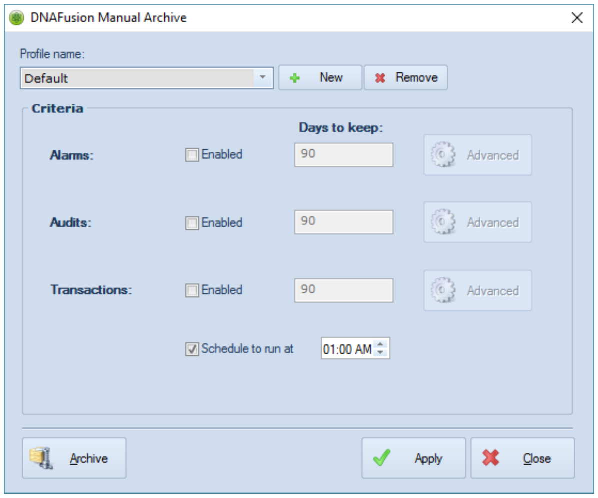
Archive Profiles

As more event information is sent to the database, the database grows larger and its capacity to store new information diminishes. The Archive Profiles feature allows system users to archive old data using predefined profiles, which are created using three sets of criteria: Alarms, Audits, and Transactions.

To create an archive profile:

1. **Select** DNA / Administrative / DNA Data Management / Archive Profiles from the Main Menu.

   The DNAFusion Manual Archive dialog opens.



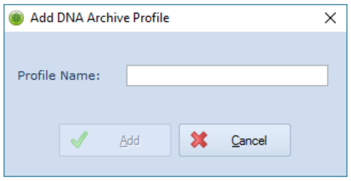
Profile name: Default

		Days to keep:
Alarms:	□ Enabled	90
Audits:	□ Enabled	90
Transactions:	□ Enabled	90

☑ Schedule to run at 01:00 AM

2. **Click** the New button.

   The Add DNA Archive Profile dialog appears.



Profile Name:

3. **Enter** a Profile Name and **click** Add.

   The new profile is added to the Profile Name drop-down list.
4. **Select** the Enabled checkbox(es) to toggle the desired Criteria.
5. **Enter** the number of Days to Keep. (Default = 90)

   Information older than the selected number of days will be saved to an archive file. The operator can retrieve the file using the Restore Data feature. See page 20-6 for more information.

   Or

   If desired, **click** the Advanced button to configure individual criteria options.

   See page 20-6 for more information on advanced configuration.

> Advanced *options will override the* Days to Keep *field in the* DNAFusion Manual Archive *dialog. If used, the operator must configure all advanced options for the selected criteria.*

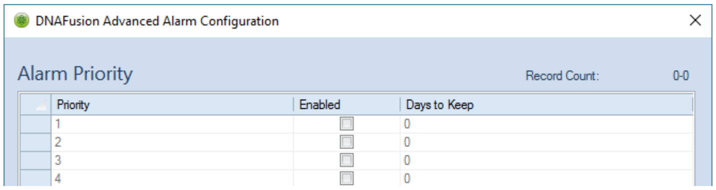
6. **Click** the Apply button to save the archive profile.
7. **Click** OK to confirm.
8. If desired, **click** the Archive button to archive the data.
9. **Click** OK to confirm.
10. **Click** Close to close the dialog.

> *The* Default *profile can be scheduled to automatically archive data at a specific time each day.* **Select** Default *from the* Profile Name *drop-down list,* **configure** *the* Criteria*,* **check** Schedule to Run At*, and* **specify** *a* Time *to schedule the archive profile.*
>
> *If the scheduling option is grayed out, verify that the workstation is not using an older archive service. From the* Control Panel*,* **open** Services*,* **right-click** *on* DNA Fusion Archive Service*, and* **select** Stop*.*

Advanced Configuration

If the Advanced button is selected in the DNAFusion Manual Archive dialog, the user can set individual archive settings for alarm priorities, audit actions, and event actions. Because these settings will override the Days to Keep field in the DNAFusion Manual Archive dialog, all advanced options for the selected Criteria must be configured.

- Alarms - Opens the DNAFusion Advanced Alarm Configuration dialog to specify archive settings based on the Alarm Priority. **Select** the Enabled checkboxes and **enter** a number of Days to Keep for each priority.



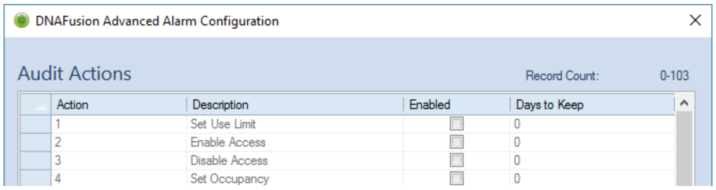
DNAFusion Advanced Alarm Configuration

Alarm Priority

Record Count: 0-0

Priority	Enabled	Days to Keep
1	☐	0
2	☐	0
3	☐	0
4	☐	0

- Audits - Opens the DNAFusion Advanced Alarm Configuration dialog to specify archive settings based on Audit Actions, i.e. operator actions. **Select** the Enabled checkboxes and **enter** a number of Days to Keep for each action.



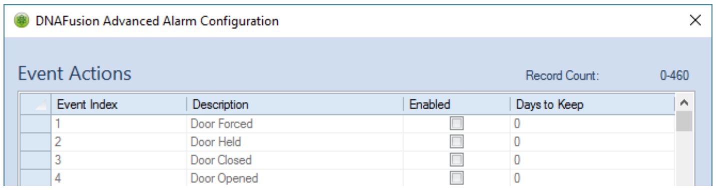
DNAFusion Advanced Alarm Configuration

Audit Actions

Record Count: 0-103

Action	Description	Enabled	Days to Keep
1	Set Use Limit	☐	0
2	Enable Access	☐	0
3	Disable Access	☐	0
4	Set Occupancy	☐	0

- Transactions - Opens the DNAFusion Advanced Alarm Configuration dialog to specify archive settings based on Event Actions, i.e. transaction history. **Select** the Enabled checkboxes and **enter** a number of Days to Keep for each event.



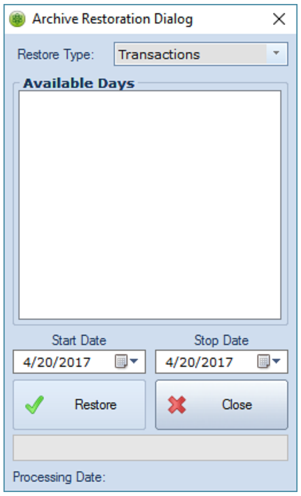
DNAFusion Advanced Alarm Configuration

Event Actions

Record Count: 0-460

Event Index	Description	Enabled	Days to Keep
1	Door Forced	☐	0
2	Door Held	☐	0
3	Door Closed	☐	0
4	Door Opened	☐	0

Restoring Archived Data



Archive Restoration Dialog

Restore Type: Transactions

Available Days

Start Date: 4/20/2017

Stop Date: 4/20/2017

Processing Date:

1. **Select** DNA / Administrative / DNA Data Management / Restore Data from the Main Menu.

   The Archive Restoration Dialog will display.
2. **Select** the Restore Type from the drop-down list: Alarms, Audits, or Transactions.
3. **Select** from the Available Days.
4. **Enter** a Start and Stop Date.
5. **Click** Restore.

   A confirmation dialog will appear.
6. **Click** OK to close the dialog.
7. **Click** Close to close the Archive Restoration Dialog.

   The operator can now generate a Restored Archived Data report. See page 17-2 for more information.

> *Once a set of archives is restored, the previously restored archives are removed from the database. Keep this in mind when retrieving data.*

Backup & Restore

Because each company, business, or organization has different system maintenance needs and desires, it is not possible for Open Options to prescribe specific recommendations for backing up a given access control system. Therefore, the responsibility of deciding how to best protect system data must rest with the system administrator.

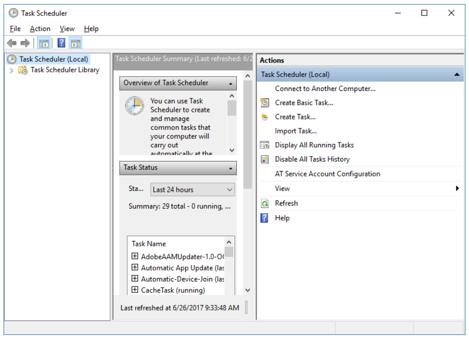
It is important that administrators run backups during periods of minimal activity in the database.

SQL Server 2012 Express

Administrators should perform regular backups of the DNA SQL Server database. If the site is running SQL Server 2012 Express, use the Backup files provided with the DNA Fusion installation and schedule the backup via Windows Task Scheduler.

1. From the Control Panel, **select** System and Security / Administrative Tools / Task Scheduler.

   The Task Scheduler dialog opens.



You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the

Summary: 29 total - 0 running, ...

Last refreshed at 6/26/2017 9:33:48 AM

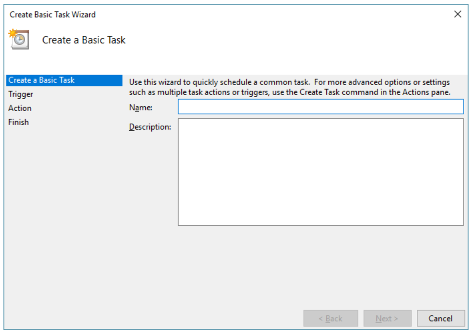
2. **Select** the Create Basic Task option from the Actions menu.

   The Create Basic Task Wizard dialog opens.

3. **Enter** a Name and, if desired, **enter** a Description and **click** Next.

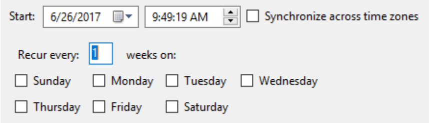
   The Task Trigger dialog appears.

4. **Select** a Task Trigger and **click** the Next button.



Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.

5. Depending on the trigger selection in Step 4, **configure** the Recurrence options and **click** Next.

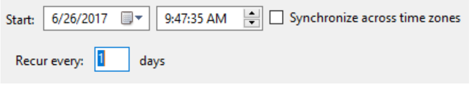


Start: 6/26/2017 9:49:19 AM ☐ Synchronize across time zones

Recur every: 1 weeks on:

☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday

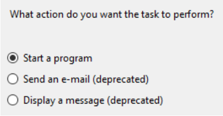
☐ Thursday ☐ Friday ☐ Saturday



Start: 6/26/2017 9:47:35 AM ☐ Synchronize across time zones

Recur every: 1 days

6. **Select** the Start a Program option from the Action dialog and **click** the Next button.



What action do you want the task to perform?

● Start a program

○ Send an e-mail (deprecated)

○ Display a message (deprecated)

7. From the Start a Program screen, **click** the Browse button and **locate** the Backup file.

   Default location: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\DBBackups\

8. **Click** the Next button to continue scheduling.

   The Summary screen is displayed.

9. **Click** the Finish button.

   The backup will be stored in the following location: C:\Users\Public\Documents\Open Options, Inc\dnaFusion\DBBackups\. By default, the account that runs the SQL Server is NT AUTHORITY\NetworkServer. This account does not have permission to access the Backup folder in the path mentioned above.

   Open Options recommends that the path be changed to C:\Program Files\Microsoft SQL Server\MSSQL10_50.OPENOPTIONS\MSSQL\Backup\DNAFusion.bak or that the account that runs the SQL Server Driver be changed to Local System since it has rights to all folders.

   To specify a different location, **right-click** on the Backup Batch file, **select** Edit and change the location. If the Backup file location is changed, the Restore file location must be changed to match the Backup file location.

> *The default network service account does not have permission to access the* C:\Users\Public\Documents\Open Options, Inc\dnaFusion\DBBackups\ *path.*

Restore

To restore a backup:

1. **Double-click** the Restore file that was copied to the Tools folder.

   The previous backup will be restored.

   Default location:

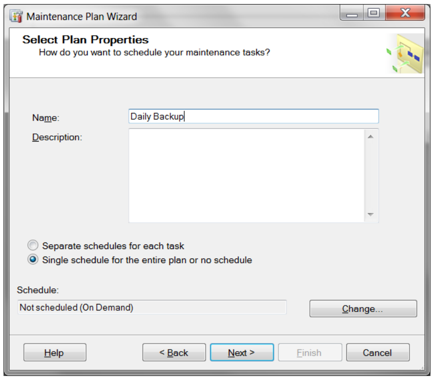
   - 32-bit OS - C:\Program Files\DNAFusion\Tools
   - 64-bit OS - C:\Program Files (x86)\DNAFusion\Tools

SQL Server Maintenance Plan

If you are using SQL Server, complete your backup and restore activities by setting up a Maintenance Plan for the DNA Fusion database.

1. **Open** SQL Server Management Studio.
2. **Right-click** on the Maintenance Plans option and **select** Maintenance Plan Wizard.
3. **Right-click** on the nPowerDna database option and **select** All Tasks / Maintenance Plan.

   The Maintenance Plan Wizard will open.



Maintenance Plan Wizard

Select Plan Properties

How do you want to schedule your maintenance tasks?

Name: Daily Backup

Description:

○ Separate schedules for each task

● Single schedule for the entire plan or no schedule

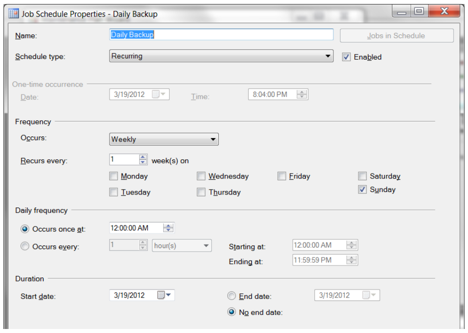
Schedule:

Not scheduled (On Demand)

4. **Click** the Next button to begin the process.

   The Select Plan Properties page opens.
5. **Enter** a Name and if desired, **enter** a Description and **click** Next.
6. **Click** the Change button to set the Maintenance Plan on a schedule.

   The Job Schedule Properties - Maintenance Plan dialog opens.



Job Schedule Properties - Daily Backup

Name: Daily Backup

Schedule type: Recurring ☑ Enabled

One-time occurrence

Date: 3/19/2012 Time: 8:04:00 PM

Frequency

Occurs: Weekly

Recurs every: 1 week(s) on

□ Monday □ Wednesday □ Friday □ Saturday

□ Tuesday □ Thursday ☑ Sunday

Daily frequency

● Occurs once at: 12:00:00 AM

○ Occurs every: 1 hour(s) Starting at: 12:00:00 AM Ending at: 11:59:59 PM

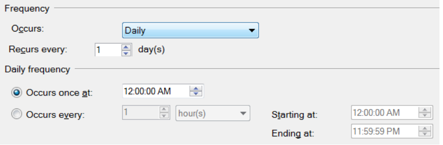
Duration

Start date: 3/19/2012 ○ End date: 3/19/2012

● No end date:

7. **Select** the desired Frequency and configure the Recurrence options.

   Depending on the Frequency selection, each option provides a different set of options.



Frequency

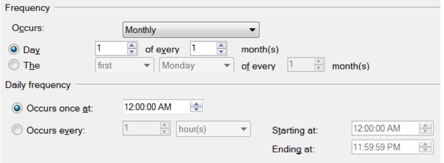
Occurs: Daily

Recurs every: 1 day(s)

Daily frequency

● Occurs once at: 12:00:00 AM

○ Occurs every: 1 hour(s) Starting at: 12:00:00 AM Ending at: 11:59:59 PM



Frequency

Occurs: Monthly

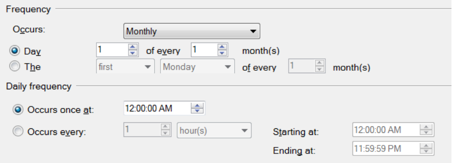
● Day 1 of every 1 month(s)

○ The first Monday of every 1 month(s)

Daily frequency

● Occurs once at: 12:00:00 AM

○ Occurs every: 1 hour(s) Starting at: 12:00:00 AM Ending at: 11:59:59 PM



Frequency

Occurs: Monthly

● Day 1 of every 1 month(s)

○ The first Monday of every 1 month(s)

Daily frequency

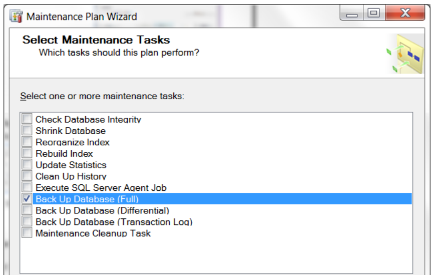
● Occurs once at: 12:00:00 AM

○ Occurs every: 1 hour(s) Starting at: 12:00:00 AM Ending at: 11:59:59 PM

8. If desired, specify the Duration and **click** the OK button.

   The Select Plan Properties page opens.
9. **Click** Next to specify the Maintenance Tasks.
10. From the Maintenance Tasks dialog, **select** the Back Up Database (Full) option and **click** the Next button.

    The Maintenance Task Order dialog opens.



Maintenance Plan Wizard

Select Maintenance Tasks

Which tasks should this plan perform?

Select one or more maintenance tasks:

□ Check Database Integrity

□ Shrink Database

□ Reorganize Index

□ Rebuild Index

□ Update Statistics

□ Clean Up History

□ Execute SQL Server Agent Job

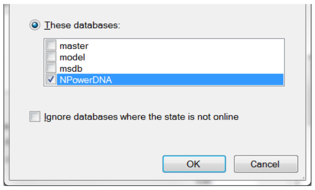
☑ Back Up Database (Full)

□ Back Up Database (Differential)

□ Back Up Database (Transaction Log)

□ Maintenance Cleanup Task

11. **Click** the Next button to specify the database.
12. **Select** the Database(s) drop down list, **check** the NPowerDNA database and **click** the OK button.



● These databases:

□ master

□ model

□ msdb

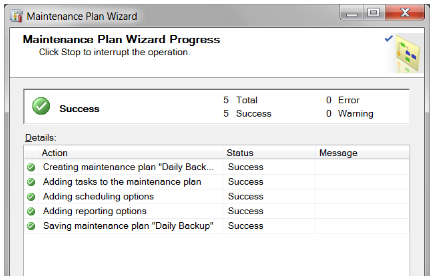
☑ NPowerDNA

□ Ignore databases where the state is not online

13. **Check** the Verify backup integrity option and if desired, **change** the Folder path.
14. **Click** the Next button to configure the Report Options.
15. **Select** the desired Report Options and **click** Next.

    The Summary Page is displayed.
16. **Click** the Finish button.

    If the Maintenance fails to run, check the Permission Settings for the database.



Maintenance Plan Wizard

Maintenance Plan Wizard Progress

Click Stop to interrupt the operation.

Success 5 Total 0 Error

5 Success 0 Warning

Details:

Action	Status	Message
Creating maintenance plan "Daily Back...	Success	
Adding tasks to the maintenance plan	Success	
Adding scheduling options	Success	
Adding reporting options	Success	
Saving maintenance plan "Daily Backup"	Success	

System Backup Files

The items listed in the DNA Directories dialog are not saved to the database. As a result, IT administrators must determine another method for backing up these files.

Because DNA Fusion stores various objects in default folders, including photos, templates, and graphic map files, the folders must be configured to a shared drive to provide access to client machines.

File	Description
Backups	This directory houses the database backup files.
Biometrics	This directory houses the personnel biometric data. The Biometrics directory is located in the Graphics folder.
DNA Maps	This directory houses the graphic maps that have been configured. The DNA Maps directory is located in the Graphics folder.
Photos	This directory houses the personnel photos when the photos are captured through a camera attached to a Badging Station. The Photos directory is located in the Graphics folder.
Signatures	This directory houses the personnel signatures. The Signatures directory is located in the Graphics folder.
HTML Files	This file stores the HTML Tree configuration as well as the help files. The file resides on the server.
Reports	This directory houses the default reports.
Custom Reports	This directory houses the custom reports.
Schedules	This directory houses DAT files (.dat) regarding scheduling configurations for each of the functions indicated: archives, batch files, downloads, and reports.
Templates	This directory houses the badge templates as well as .gax files that contain the default access level information for a personnel group.

ⓘ *The* HTML Files *and* Reports *directories cannot be changed or relocated.*

Software Upgrades

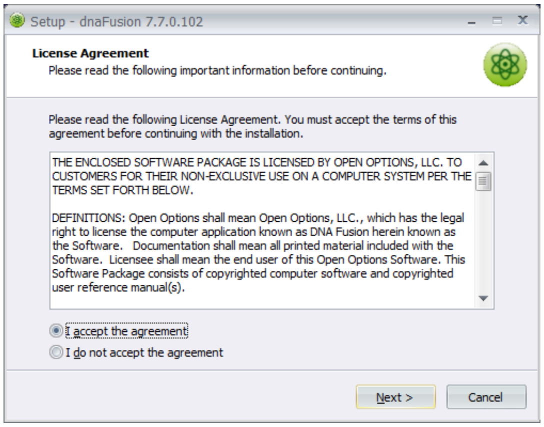
DNA Fusion software upgrades do not require additional licenses. After receiving an upgrade link or install file from Open Options, the upgrade should be performed at the server before updating client workstations. Any clients connected to the system will be upgraded the first time they connect to the upgraded server.

> *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.*

To upgrade DNA:

> *If clients are connected to the server, run* Setup.exe *to push the current software version to the client workstations. The* Service Pack *only updates the active workstation.*

1. **Close** DNA Fusion.
2. **Locate** and **double-click** the upgrade executable file.



Setup - dnaFusion 7.7.0.102

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

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

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

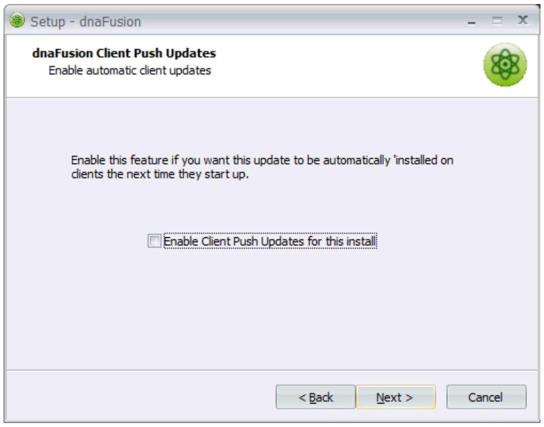
● I accept the agreement

○ I do not accept the agreement

The License Agreement screen appears.

3. **Click** Next.
4. **Follow** the install wizard instructions.

> *The* Client Push Updates *screen will appear during a* Server Full Install *upgrade only. Performing a* Service Pack *upgrade does not provide an option to push client updates.*



Setup - dnaFusion

dnaFusion Client Push Updates

Enable automatic client updates

Enable this feature if you want this update to be automatically 'installed on clients the next time they start up.

□ Enable Client Push Updates for this install

NOTES:

Firmware Updates

Firmware acts as a middleman between the software and hardware. For best system performance results, update the firmware to the most recent version.

Firmware should be updated after any changes to the system, including the following:

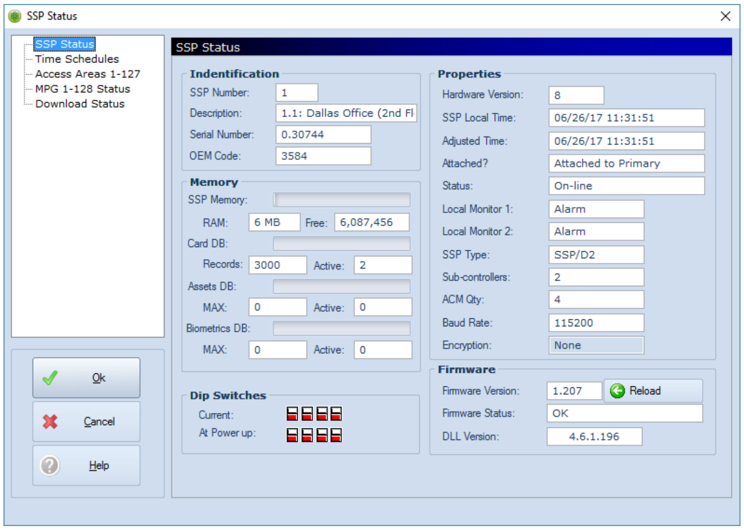
- Installing a new system
- Upgrading to a new DNA version
- Adding a new controller
- Replacing a controller
- Connecting to a controller the first time

Controller

To update the firmware:

1. In the Hardware Browser, **right-click** on the Controller and **select** Status from the context menu.

   The SSP Status dialog opens.



SSP Status

Indentification
SSP Number: 1
Description: 1.1: Dallas Office (2nd Fl
Serial Number: 0.30744
OEM Code: 3584

Memory
SSP Memory:
RAM: 6 MB Free: 6,087,456
Card DB:
Records: 3000 Active: 2
Assets DB:
MAX: 0 Active: 0
Biometrics DB:
MAX: 0 Active: 0

Dip Switches
Current:
At Power up:

Properties
Hardware Version: 8
SSP Local Time: 06/26/17 11:31:51
Adjusted Time: 06/26/17 11:31:51
Attached? Attached to Primary
Status: On-line
Local Monitor 1: Alarm
Local Monitor 2: Alarm
SSP Type: SSP/D2
Sub-controllers: 2
ACM Qty: 4
Baud Rate: 115200
Encryption: None

Firmware
Firmware Version: 1.207
Firmware Status: OK
DLL Version: 4.6.1.196

2. **Click** the Reload button.

   A confirmation dialog will appear.

3. **Click** Yes to reload the firmware.

   The Reload button will become grayed out and the Firmware Status will display Loading.

   When the firmware download is complete, Firmware Status will display OK.

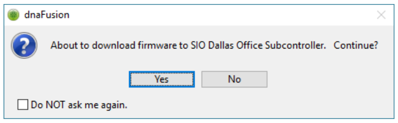
4. **Click** OK to close the SSP Status dialog.

Subcontrollers

A subcontroller's firmware can be updated from the Hardware Browser.

1. **Right-click** on the Subcontroller and **select** Reload Firmware from the menu.

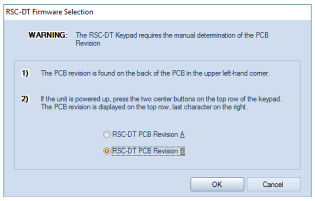
   Depending on the subcontroller, a dialog will appear.



dnaFusion

About to download firmware to SIO Dallas Office Subcontroller. Continue?

☐ Do NOT ask me again.



RSC-DT Firmware Selection

WARNING: The RSC-DT Keypad requires the manual determination of the PCB Revision

1) The PCB revision is found on the back of the PCB in the upper left-hand corner.

2) If the unit is powered up, press the two center buttons on the top row of the keypad. The PCB revision is displayed on the top row, last character on the right.

○ RSC-DT PCB Revision A
● RSC-DT PCB Revision B

2. **Follow** the directions on the screen.

   The subcontroller's firmware is reloaded.

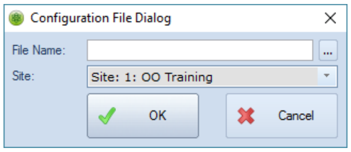
NOTES:

Batch Processing

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

1. **Select** DNA / Administrative / Batch Processing from the Main Menu.

   The Configuration File Dialog opens.



File Name:

Site: Site: 1: OO Training

2. **Click** the Browse button and **locate** the desired command file.

   Command files should be placed in the following location:

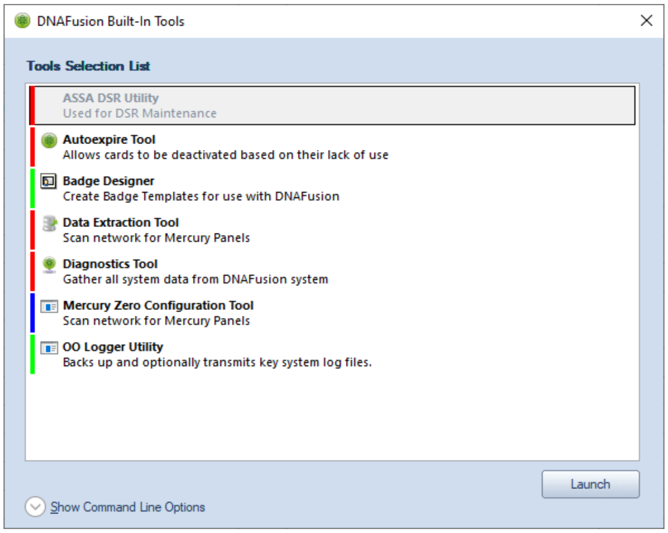
   - 32-bit OS - C:\Program Files\DNAFusion\Batch
   - 64-bit OS - C:\Program Files (x86)\DNAFusion\Batch

3. **Select** the desired Site from the drop-down list.
4. **Click** OK to download the file to the controller.

Built-in Tools

The Tools option in the Main Menu contains a list of built-in tools. The operator/administrator can select a tool from the Tool Selection List and will launch the desired application.

1. **Select** Tools, from the Main Menu.



Tools Selection List

ASSA DSR Utility
Used for DSR Maintenance

Autoexpire Tool
Allows cards to be deactivated based on their lack of use

Badge Designer
Create Badge Templates for use with DNAFusion

Data Extraction Tool
Scan network for Mercury Panels

Diagnostics Tool
Gather all system data from DNAFusion system

Mercury Zero Configuration Tool
Scan network for Mercury Panels

OO Logger Utility
Backs up and optionally transmits key system log files.

2. **Select** desired tool from the Tool Selection List.
3. **Click** Launch.

ASSA DSR Utility

This utility is a support tool to help maintain DSR's integrated with DNA Fusion.

AutoExpire Tool

Allows cards to be deactivated based on their lack of use. The operator can set the number of days a credential can remain inactive before the tool deactivates the credential.

Badge Designer

This utility is used to create badge templates. See Chapter 21 for more information on ID Badging.

Data Extraction Tool

The Data Extraction Tool is used to export any desired tables from a database in an easy and concise matter. See TB 20-9 for more information about the utility.

Diagnostics Tool

Gather all system data from DNA Fusion system. This tool allows the operator to see information about the system. This information is useful when attempting to solve an issue.

Mercury Zero Configuration Tool

This tool is used to scan the network for mercury panels. This tool is used to access a panels Configuration Manager. See page 2-3 in the Hardware Manual for more information.

OO Logger Utility

This tool backs up and optionally transmits key system log files. The operator can configure switches ON and OFF to back up logs for DNA Fusion or other license integrations.

ID Badging 21

In This Chapter

- √ Designing a Badge Template
- √ Configuring Badge Types
- √ Setting Up ID Badging in DNA
- √ Taking a Photo
- √ Previewing & Printing a Badge

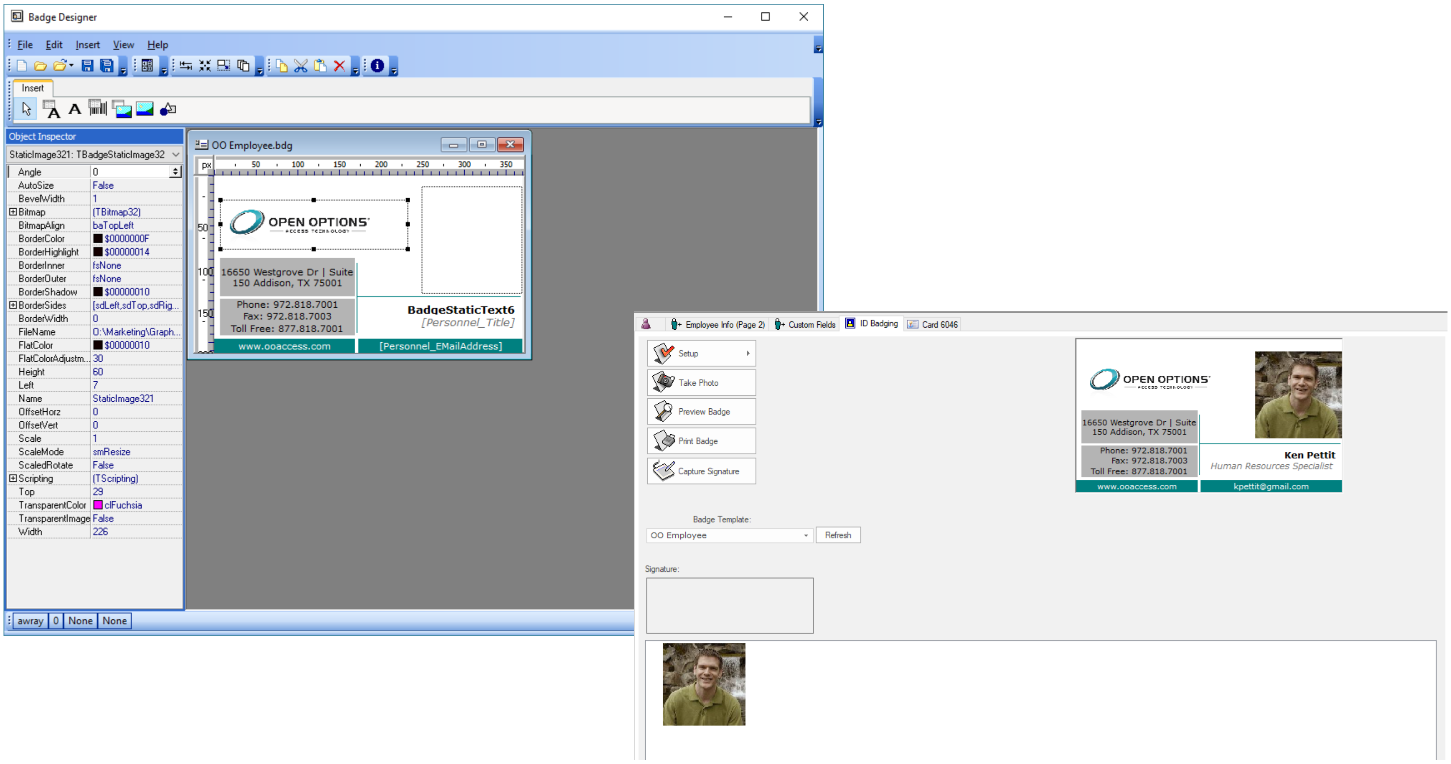
For clarification purposes, this manual assumes that the processes discussed in this section will be performed on a station enabled as Badging Station. See page 3-3 for more information on enabling ID Badging for a station.

A Badging Station contains two modules:

- The Badge Designer
- The Badge Manager

The Badge Designer is an external application used to design badge templates. Component objects (i.e., graphic, text field, and bar code placeholders) are placed on the badge model to fashion how the badges will appear. The template is then named and saved to the operator's local hard drive or a common shared folder if more than one badging station is used. The placeholders will be populated by specific database information to create individual badges.

In the Badge Manager, the operator selects a badge template, takes a photo, and prints the badge. The Badge Manager is located in the ID Badging tab of the cardholder's record. ID Badging



StaticImage321: TBadgeStaticImage32

Angle	0
AutoSize	False
BevelWidth	1
⊞ Bitmap	(TBitmap32)
BitmapAlign	baTopLeft
BorderColor	■ $0000000F
BorderHighlight	■ $00000014
BorderInner	fsNone
BorderOuter	fsNone
BorderShadow	■ $00000010
⊞ BorderSides	[sdLeft,sdTop,sdRig...
BorderWidth	0
FileName	O:\Marketing\Graph...
FlatColor	■ $00000010
FlatColorAdjustm...	30
Height	60
Left	7
Name	StaticImage321
OffsetHorz	0
OffsetVert	0
Scale	1
ScaleMode	smResize
ScaledRotate	False
⊞ Scripting	(TScripting)
Top	29
TransparentColor	■ clFuchsia
TransparentImage	False
Width	226

Badge Template: OO Employee

This Page Intentionally Left Blank

Badge Designer

Opening Badge Designer

1. In the File Explorer, **open** the Badge Designer application.

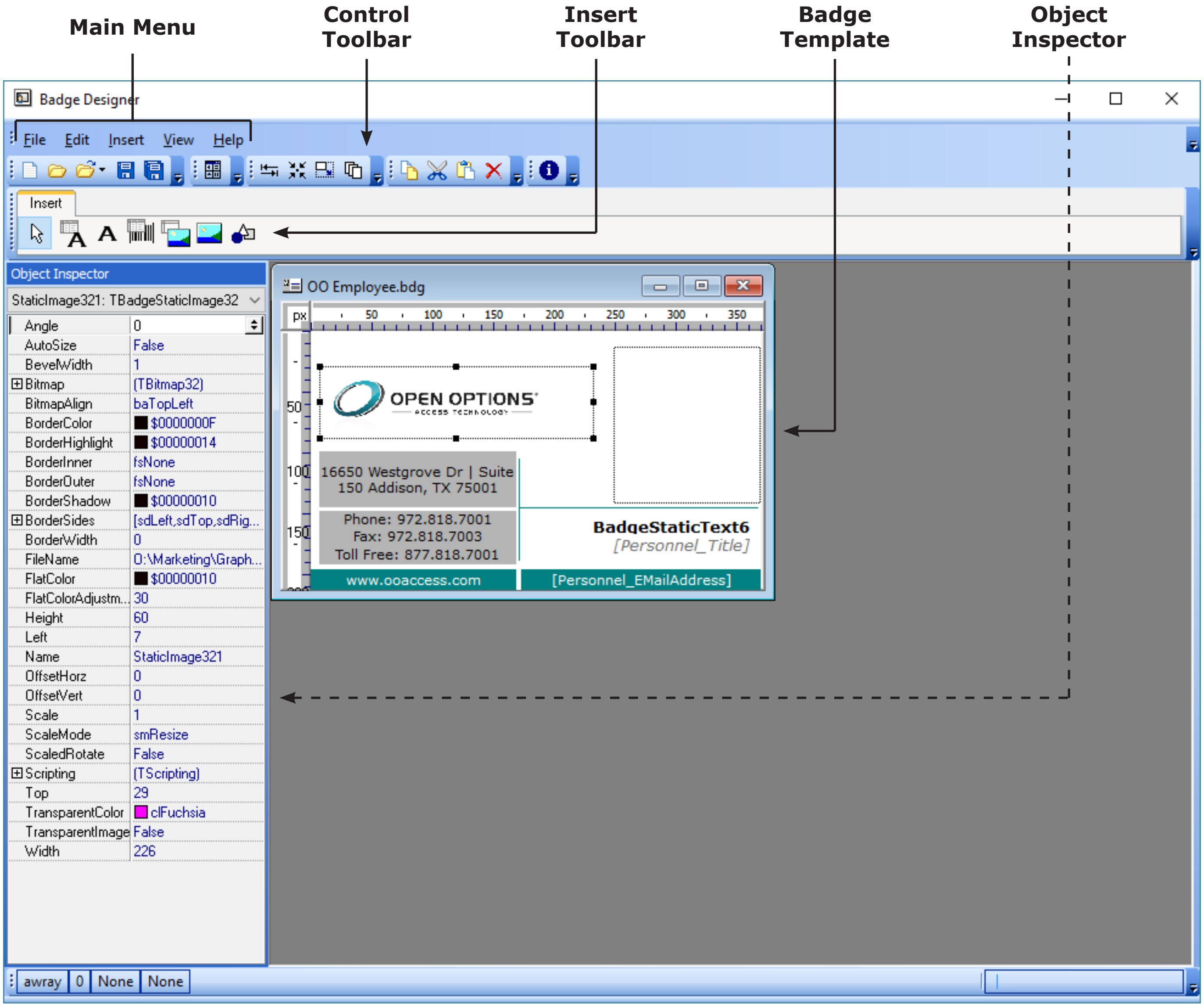
   The default location is C:\Program Files\DNA Fusion\BadgeDesigner.exe for 32-bit OS and C:\Program Files (x86)\DNA Fusion\BadgeDesigner.exe for 64-bit OS.

The Badge Designer Environment

Badge Designer has a relatively simple and user-friendly interface.

The main screen consists of five (5) principal elements:

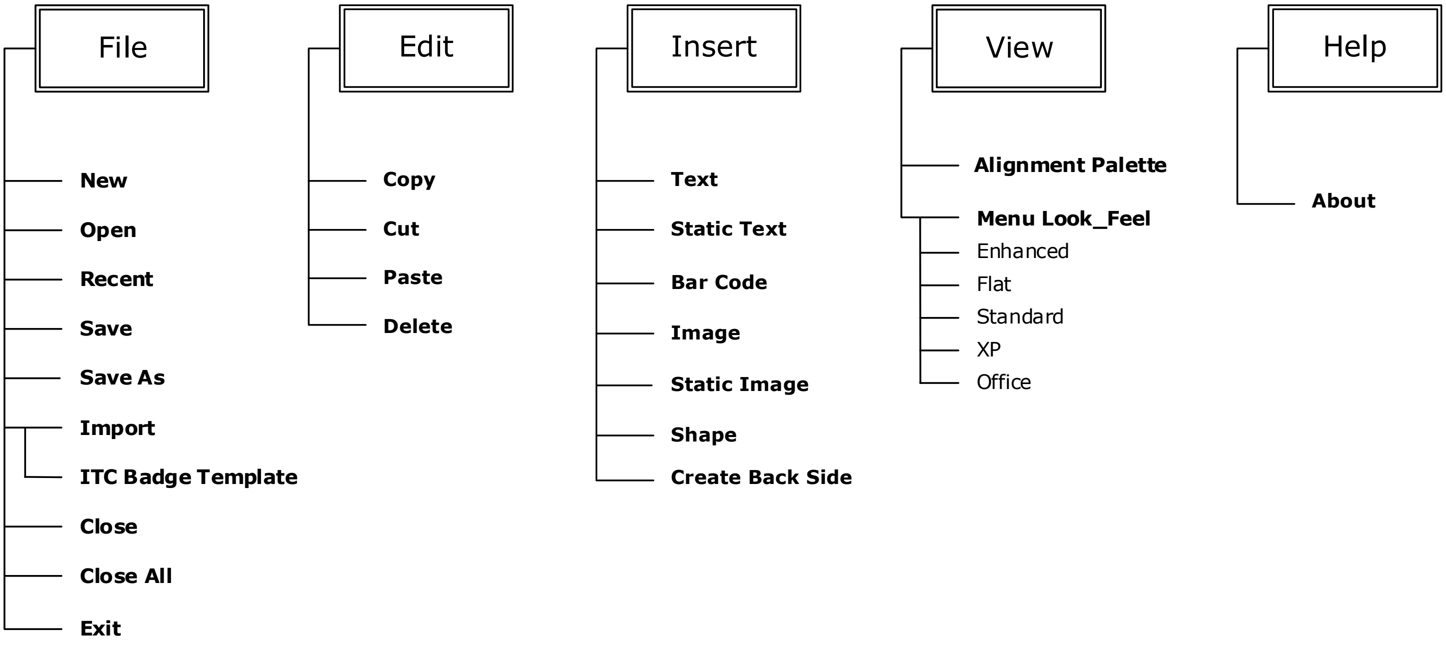
- Main Menu
- Control Toolbar
- Insert Toolbar
- Badge Template
- Object Inspector



Angle	0
AutoSize	False
BevelWidth	1
⊞ Bitmap	(TBitmap32)
BitmapAlign	baTopLeft
BorderColor	■ $0000000F
BorderHighlight	■ $00000014
BorderInner	fsNone
BorderOuter	fsNone
BorderShadow	■ $00000010
⊞ BorderSides	[sdLeft,sdTop,sdRig...
BorderWidth	0
FileName	O:\Marketing\Graph...
FlatColor	■ $00000010
FlatColorAdjustm...	30
Height	60
Left	7
Name	StaticImage321
OffsetHorz	0
OffsetVert	0
Scale	1
ScaleMode	smResize
ScaledRotate	False
⊞ Scripting	(TScripting)
Top	29
TransparentColor	■ clFuchsia
TransparentImage	False
Width	226

Main Menu

From the Main Menu, the operator can manage the badge file, construct the badge, and control the display. They can also configure the badge properties (i.e. shape, size, and color) and insert components onto the badge template.



File

- Various options related to a badge file (.bdg).

Edit

- Various options related to editing a badge file (.bdg).

Insert

- Text - Inserts a text placeholder onto the template.
- Static Text - Inserts text onto the template that will remain the same for each badge.
- Bar Code - Inserts a bar code placeholder on the template.
- Image - Inserts an image placeholder on the template.
- Static Image - Inserts an unchanging graphic onto the template from a stated file path.
- Shape - Inserts a resizable, colorable white box onto the template. The operator can change the shape by using the Object Inspector.
- Create Back Side - Inserts a back side area below the existing badge area.

View

- Alignment Palette - Displays the Alignment Palette.
- Menu Look_Feel - Adjusts the menu theme.

Help

- About - Displays version and copyright information.

Control Toolbar

The Control Toolbar contains a number of commands that allow the operator to control and manipulate the badge template.

📄	New Icon - Opens the New Template dialog to create a new template.
📂	Open Icon - Displays the Open dialog to open an existing badge template file.
📂▾	Open Recent Icon - Displays a list of the files recently opened in the application.
💾	Save Icon - Saves an existing file or opens the Save As dialog if the file is new.
💾	Save As Icon - Opens the Save As dialog to save the current file.
▦	Show Alignment Palette Icon - Displays the Alignment Palette.
⇤⇥	Align Icon - Displays the Alignment dialog to configure the object’s vertical and horizontal alignment.
⤧	Align to Grid Icon - Aligns the selected object with the template’s grid lines.
⬚	Size Icon - Displays the Size dialog to configure the object’s width and height.
⧉	Select All Icon - Selects all objects on the template.
⧉	Copy Icon - Copies the selected object to the clipboard.
✂	Cut Icon - Cuts the selected object and stores it in the clipboard.
📋	Paste Icon - Pastes the contents of the clipboard.
✕	Delete Icon - Deletes the selected object.
ℹ	About Icon - Displays the About Badge Designer dialog.

Insert Toolbar

The Insert Toolbar allows the operator to select and insert objects on the badge template.

	Select Icon - Select objects on the template.
A	Text Icon - Inserts a text placeholder on the badge template. The text will be determined by the database field assigned to the text object.
A	Static Text Icon - Inserts a text object that will remain the same for each badge.
	Bar Code Icon - Inserts a bar code placeholder on the badge template. The bar code font must be installed on the workstation.
	Image Icon - Inserts an image placeholder on the badge template. The image will be determined by the database field assigned to the image object.
	Static Image Icon - Inserts an image that will remain the same for each badge.
	Shape Icon - Inserts a user-defined shape on the badge template.

Designing a Badge Template

The Badge Designer application can store an unlimited number of badge template designs. Templates define the physical layout of the badge. This includes the size and shape of the badge as well as the format of the various text, photos, and graphic data to be displayed on the badge.

Badge Designer gives you many design options. The key is to include the necessary elements and create an attractive badge. Achieving this balance may take some work. The following design elements should be considered.

- Photos – Color or Black & White
- Text – Names, ID Numbers, etc.
- Logos – Placement
- Type – Bar Codes, Magnetic Stripes, Smart Cards

Begin the design process by choosing the elements you want to include from the list above. Then sketch a few layouts in an area the size of a credit card. If you are including a magnetic stripe, design your badge so it can be swiped through a reader. If you are using bar codes, leave a 0.25-inch border on either side of the image.

To start a new design:

1. With Badge Designer open, **select** File / New.

   The New Template dialog opens.

2. **Specify** the Badge Orientation and Size.

3. **Select** One Sided or Two Sided.

4. If desired, **click** the Select Color button to set a Background Color.

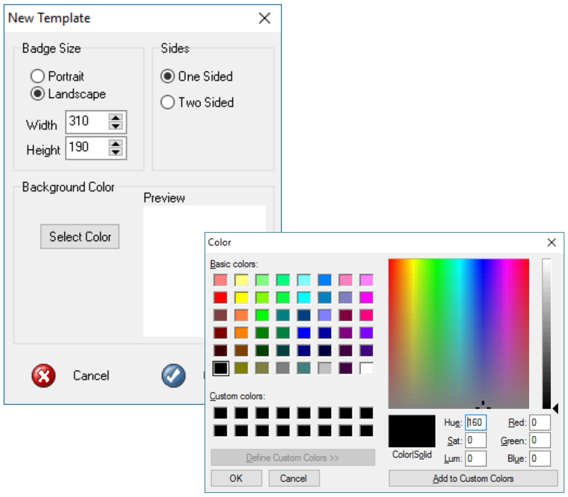
   The Color dialog opens.

   Select the desired color and **click** OK.

   To make the color visible, the Print Background must be set to True. See page 21-17 for more information.

5. **Click** OK.

   The blank template opens in the main screen.



New Template

Badge Size

○ Portrait

● Landscape

Width 310

Height 190

Sides

● One Sided

○ Two Sided

Background Color

Preview

Color

Hue: 160 Sat: 0 Lum: 0

Red: 0 Green: 0 Blue: 0

Adding a Background Image

An image can be used for the badge background with additional objects layered on top.

1. **Double-click** on the badge background.

   The Image Editor dialog opens. See page 21-13 for more information.

2. **Click** the Insert Image Icon .

   The Open dialog appears.

3. **Browse** to the desired image and **click** Open.

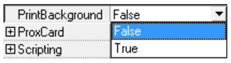
4. **Configure** the Image Editor as needed.

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

6. In the Object Inspector, **select** the PrintBackground field, **click** the drop-down arrow, and **select** True.

   The image appears on the badge.

   See page 21-15 for more information on the Object Inspector.



PrintBackground	False
⊞ProxCard	False
⊞Scripting	True

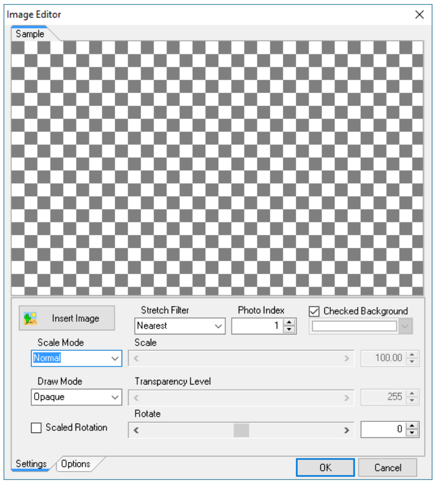


Image Editor

Sample

Stretch Filter: Nearest

Photo Index: 1

☑ Checked Background

Scale Mode: Normal

Scale: 100.00

Draw Mode: Opaque

Transparency Level: 255

Rotate: 0

☐ Scaled Rotation

Adding a Photo Placeholder

A photo placeholder is used to insert a photo (or other image) from a cardholder's record.

1. **Click** the Image Icon on the Insert Toolbar and **click** in the badge area.

   The Photo Placeholder appears.

2. **Move** and **resize** the Photo Placeholder as needed.

3. **Double-click** the Photo Placeholder.

   Or

   Right-click on the Photo Placeholder and **select** Image Config Dialog.

   The Image Editor dialog opens. See page 21-13 for more information.

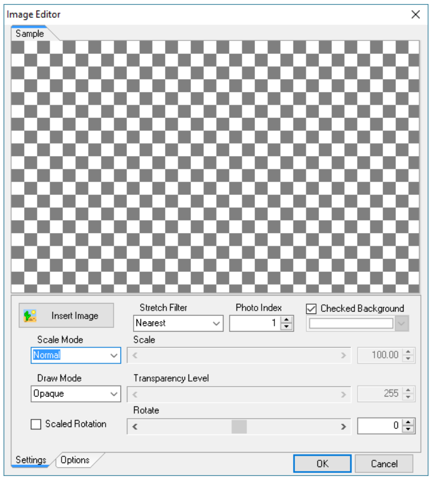


Image Editor

Stretch Filter: Nearest

Photo Index: 1

☑ Checked Background

Scale Mode: Normal

Scale: 100.00

Draw Mode: Opaque

Transparency Level: 255

Rotate: 0

□ Scaled Rotation

4. **Select** the Photo Index number.

   The Photo Index determines which photo database field (1-4) in the Cardholder's Record will be inserted as the badge photo.

5. **Configure** the Photo Placeholder as needed.

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

   When the badge is previewed in DNA Fusion, the specified image will appear in the placeholder.

Adding a Text Placeholder

A Text Placeholder can be used to insert any information from a Cardholder's Record onto the badge template. The operator can set various aspects of the placeholder's appearance during the design process, including the character font, character size, and character foreground and background colors.

1. **Click** the Text Icon on the Insert Toolbar and **click** in the badge area.

   The Text Placeholder appears.

2. **Move** and **resize** the Text Placeholder as needed.

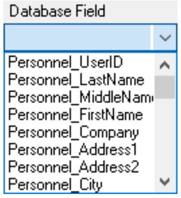
3. **Add** the Database Field to the Text Placeholder.

   - **Double-click** on the Text Placeholder OR **right-click** and **select** Text Config Dialog.

     When the Text Editor dialog opens, **select** the Database Field from the drop-down list. See page 21-11 for more information.

   - **Right-click** on the Text Placeholder and **select** Concatenate Wizard.

     When the Concatenate Wizard appears, **select** the Database Fields and Field Separators for each field. See page 21-12 for more information.



Database Field

Personnel_UserID
Personnel_LastName
Personnel_MiddleNam
Personnel_FirstName
Personnel_Company
Personnel_Address1
Personnel_Address2
Personnel_City

4. **Configure** the Text Placeholder as needed.

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

   The Caption text appears in the Text Placeholder.

Adding Static Graphics

Static graphics are images that will remain the same for each badge, such as a logo.

1. **Click** the Static Image Icon on the Insert Toolbar and **click** in the badge area.

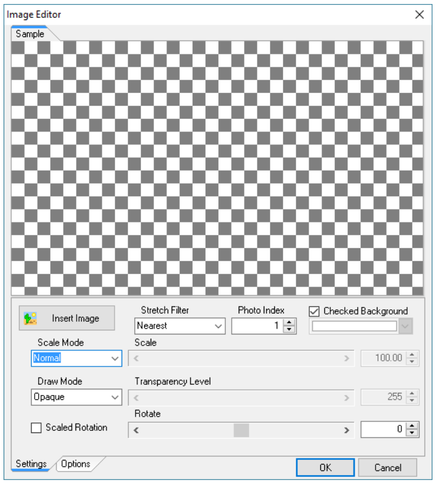
   The Graphic Placeholder appears.

2. **Move** and **resize** the Graphic Placeholder as needed.
3. **Double-click** on the Graphic Placeholder.

   Or

   Right-click on the Graphic Placeholder and **select** Image Config Dialog.

   The Image Editor dialog opens. See page 21-13 for more information.



Stretch Filter Nearest
Photo Index 1
☑ Checked Background
Scale Mode Normal
Scale 100.00
Draw Mode Opaque
Transparency Level 255
Rotate 0
□ Scaled Rotation

4. **Click** the Insert Image button.

   The Open dialog appears.

5. **Browse** to the desired graphic and **click** Open.
6. **Configure** the Image Editor as needed.
7. **Click** OK to save the settings.

   The selected image appears in the placeholder.

Adding Static Text

Like static graphics, static text remains the same for each badge.

1. **Click** the Static Text Icon A on the Component Toolbar and **click** in the badge background.

   The Text Placeholder appears.

2. **Move** and **resize** the Text Placeholder as needed.
3. **Double-click** on the Text Placeholder.

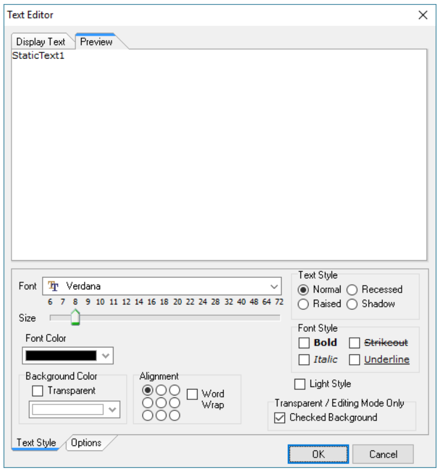
   Or

   Right-click on the Text Placeholder and **select** Text Config Dialog.

   The Text Editor diaog opens. See page 21-11 for more information.

4. **Select** the Display Text tab and **enter** the Text.
5. **Configure** the Text Placeholder as needed.
6. **Click** OK to save the settings.

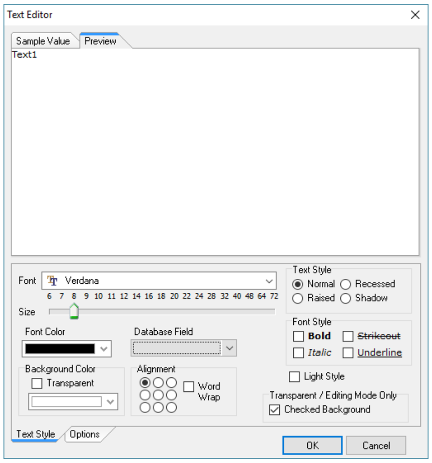
   The text appears in the placeholder.



StaticText1
Font Verdana
□ Transparent
□ Word Wrap
● Normal ○ Recessed
○ Raised ○ Shadow
□ Bold □ ~~Strikeout~~
□ *Italic* □ Underline
□ Light Style
Transparent / Editing Mode Only
☑ Checked Background

Adding a Bar Code

A Bar Code Placeholder can display text in a variety of bar code formats. Special leading and trailing characters, as required by each bar code, are added automatically.



Text1

Font: Verdana

Text Style: ● Normal ○ Recessed ○ Raised ○ Shadow

Font Style: □ Bold □ ~~Strikeout~~ □ *Italic* □ Underline

Background Color: □ Transparent

□ Word Wrap

□ Light Style

Transparent / Editing Mode Only: ☑ Checked Background

1. **Click** the Bar Code Icon on the Insert Toolbar and **click** in the badge area.

   The Bar Code Placeholder appears.

2. **Move** and **resize** the Bar Code Placeholder as needed.

3. **Double-click** the Bar Code Placeholder.

   Or

   Right-click on the Bar Code Placeholder and **select** Text Config Dialog.

   The Text Editor dialog opens. See page 21-11 for more information.

4. **Select** a Database Field from the drop-down list.

   The field will be used to pull information from a Cardholder's Record onto the badge.

5. **Select** the Bar Code Font from the drop-down list and **configure** the Bar Code Placeholder as needed.

> Badge Designer *does not come with a* Bar Code Font*. If using the* Bar Code *option, the required* Bar Code Font *will need to be loaded in the* Fonts *folder on the computer.*

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

   The bar code appears in the Bar Code Placeholder.

Adding a Color Block

A color block can be added to highlight an image or to incorporate the issuer's colors.

1. **Select** the Shape Icon from the Insert Toolbar and **click** in the badge area.

   The Shape Placeholder appears.

2. **Move** and **resize** the placeholder as needed.

3. **Configure** the object as needed using the Object Inspector. See page 21-15 for more information.

Configuration Dialogs

Text Editor

Text objects can be configured using the Text Editor dialog as an alternative to using the Object Inspector. The dialog provides a conventional dialog interface for the user to define the selected text object.

To display the Text Editor dialog:

1. **Double-click** on the desired Text Placeholder or Bar Code Placeholder.

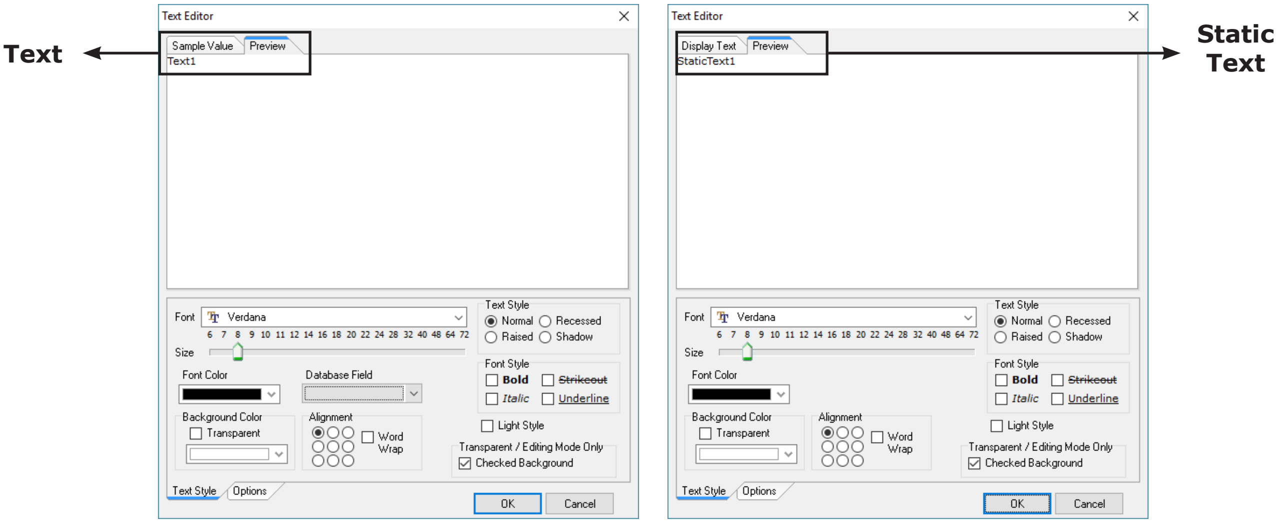
   Or

   Right-click and **select** Text Config Dialog.

   The Text Editor dialog opens. Two tabs are available: Sample Value/Display Text and Preview.

   - Sample Value/Display Text - User-defined text. This text serves as a placeholder in the badge template to be replaced later with text from the database field. For Static Text objects, the caption serves as the Display Text.
   - Preview - Displays sample of how the text object will appear on the badge template.

     Additionally, there are two tabs located at the bottom of the window: Text Style and Options. They are used to configure the text; see below for more information.



Text Style

- Font - Drop-down menu to select the font.
- Size - Sliding scale to select the font size.
- Font Color - Drop-down menu to select the font color.
- Database Field - Drop-down menu of database fields in the cardholder's record. Select the database field that will populate in the text object. (Only available for Text and Bar Code Placeholder objects)
- Background Color - Select the Background Color from the drop-down list.
  - ☐ Transparent - If checked, makes the background transparent.
- Alignment - Select an alignment radio button to position the text.
- Word Wrap - Wraps text in the Preview panel to allow the opeartor to view all text without scrolling.
- Text Style - Select a radio button to position the text.
- Font Style - Select the desired checkbox(es) to determine font attributes for the text.
- Light Style - If check, lightens the text during printing. This setting does not affect Badge Designer.
- Transparent/Editing Mode Only - If the Background Color is set to Transparent, this checkbox will display the transparent area with a checkerboard pattern.

Options

Borders

- Inner - Displays an inner border for edges selected in the Sides checkboxes.
- Outer - Displays an outer border for edges selected in the Sides checkboxes.
- Sides - Determines which border edges will be visible or hidden.

Rotation

- Restrict Angle - If checked, disables text rotation.

Options

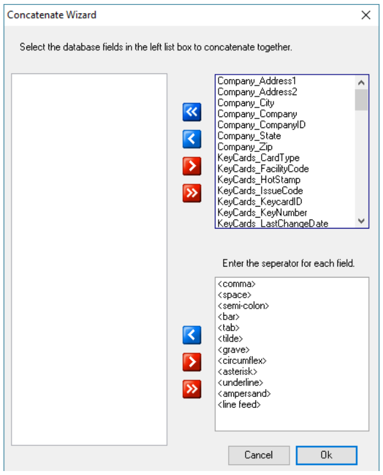
- Highlight Color - Drop-down menu to select the highlight color; only applies if the Raised or Recessed option is selected in Text Style tab.
- Shadow Color - Drop-down menu to select the shadow color; only applies if the Shadow option is selected in Text Style tab.
- Shadow - Increases or decreases the amount of shadow; only available if the Shadow option is selected in Text Style tab.

The Text Style tab for a Static Text object does not contain a Database Field drop-down menu; this is because the Static Text will not vary from badge to badge. The Static Text is determined by what is entered in the Caption field.

> *A number of configuration options are not available through the* Text Editor *dialog (such as* SizeToFit*) and must be set in the* Object Inspector*. See page 21-15 for more information.*

Concatenate Wizard

The Concatenate Wizard allows the operator to select multiple database fields to display on one line as well as separators.



Concatenate Wizard

Select the database fields in the left list box to concatenate together.

Company_Address1
Company_Address2
Company_City
Company_Company
Company_CompanyID
Company_State
Company_Zip
KeyCards_CardType
KeyCards_FacilityCode
KeyCards_HotStamp
KeyCards_IssueCode
KeyCards_KeycardID
KeyCards_KeyNumber
KeyCards_LastChangeDate

Enter the seperator for each field.

<comma>
<space>
<semi-colon>
<bar>
<tab>
<tilde>
<grave>
<circumflex>
<asterisk>
<underline>
<ampersand>
<line feed>

To open the Concatenate Wizard:

1. **Right-click** on the Text Placeholder and **select** Concatenate Wizard.

   The Concatenate Wizard appears.

2. **Select** the Database Fields and Separators to include in the text placeholder by **double-clicking** the name or **clicking** one of the Selection buttons. ◀

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

4. **Configure** the text by **double-clicking** the Concatenated Text.

   The Text Editor dialog opens.

   See page 21-11 for more information.

Image Editor

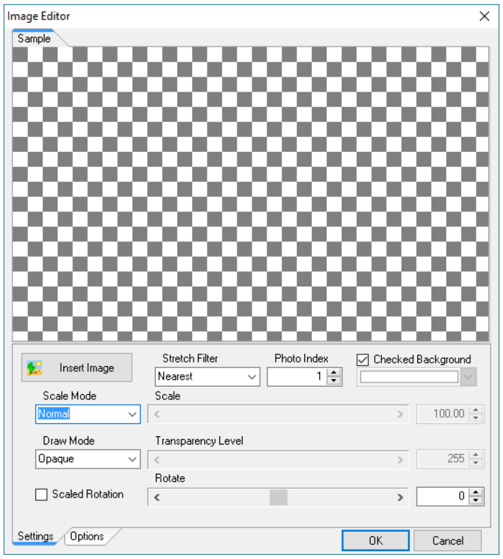
Image objects can be configured using the Image Editor dialog as an alternative to using the Object Inspector. The dialog provides a conventional dialog interface for the user to define the selected image object.

To display an Image Editor dialog:

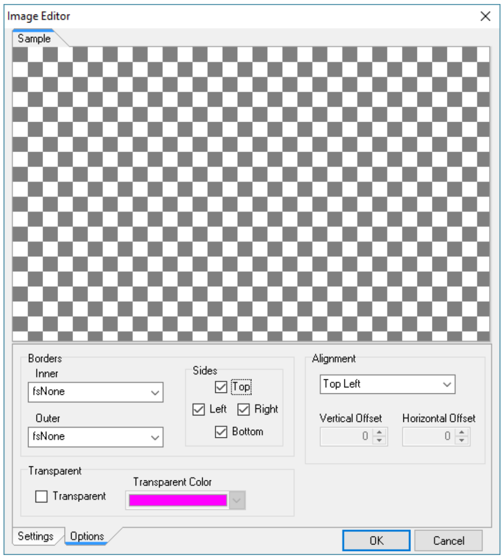
1. **Double-click** on the desired image object.

   The Image Editor dialog opens.

   Two tabs are located at the bottom of the window: Settings and Options.



Stretch Filter: Nearest
Photo Index: 1
☑ Checked Background
Scale Mode: Normal
Scale: 100.00
Draw Mode: Opaque
Transparency Level: 255
Rotate: 0
☐ Scaled Rotation



Borders
Inner: fsNone
Outer: fsNone
Sides: ☑ Top ☑ Left ☑ Right ☑ Bottom
Alignment: Top Left
Vertical Offset: 0
Horizontal Offset: 0
Transparent: ☐ Transparent
Transparent Color: 🟪

Settings

- Insert Image - Displays the Open dialog to browse for a desired graphic/photo file. The graphic/ photo serves only as a placeholder. The image on the badge will be determined by the Photo Index database field.

  To match the size of the preview graphic to the image placeholder, **right-click** on the Sample image and **select** Match Object Size.
- Stretch Filter - Drop-down menu of filter options that affect the graphic resolution.
- Photo Index - Numeric value that determines which photo database field to use from the cardholder's record.
- Background Color - Background color drop-down menu. **Check** the Checked Background checkbox to make the background transparent (displayed as checkerboard).
- Scale Mode - Drop-down menu that determines how the photo will display in the Preview panel and badge template.
  - □ Normal - Displays the photo without changing it.
  - □ Resize - Fits the photo to the preview window vertically, but maintains the photo's proportions.
  - □ Scale - Enables the slider to alter the photo size.
  - □ Stretch - Stretches the proportion of the photo to fit in the preview panel.
- Scale - If Scale is selected from the Scale Mode drop-down, the slider becomes active and increases the size of the picture in the preview panel as the slider is moved right. Use the SpinEdit buttons for more precise control.
- Draw Mode - Toggle menu that determines whether the transparency effect is active.
- Transparency Level - If Transparent is selected in the Draw Mode menu, the slider becomes active and increasingly fades the picture in the preview panel as the slider is moved to the right. Use the SpinEdit buttons for more precise control.
- Scaled Rotation - Scales the image during rotation, maintaining the aspect ratio of the image to fit the original boundaries of the image as it is rotated.
- Rotate - Rotates the image. Use the SpinEdit buttons for more precise control.

Options

- Inner Border - Displays inner border for edges selected in Sides checkboxes.
- Outer Border - Displays outer border for edges selected in Sides checkboxes.
- Sides Border - Determines which border edges will display or hide.
- Alignment - Drop-down menu to select the alignment setting.
- Vertical Offset - If Custom is selected in the Alignment drop-down menu, the Vertical Offset becomes active. Use the SpinEdit button to control vertical positioning of the picture.
- Horizontal Offset - If Custom is selected in the Alignment drop-down menu, the Horizontal Offset becomes active. Use the SpinEdit button to precisely control horizontal positioning of the picture.
- Transparent - Activates the Transparent Color drop-down.
- Transparent Color - Allows the operator to select a color in the image to become transparent.

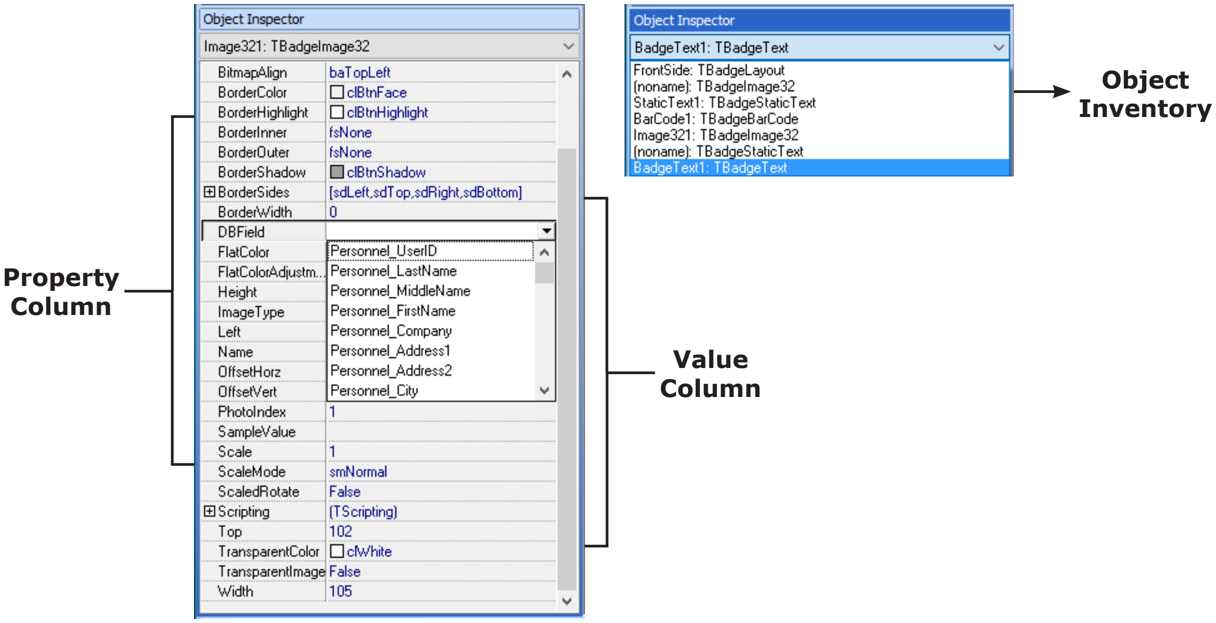
Object Inspector

The Object Inspector is a window containing the property settings that allow the user to configure the attributes of objects placed on the badge template.

> *The operator can elect to use the* Editor Dialogs *instead of the* Object Inspector*; however, some properties can only be configured through the* Object Inspector*. See page 21-11 and 21-13 for more information on the* Text Editor *and the* Image Editor*, respectively.*

The Object Inventory drop-down contains a list of all the objects currently placed on the badge template as well as the template background. Selecting an object from this list redefines the Property and Value columns for the object selected.

When an individual Property field is selected, the corresponding Value field will change to indicate the configuration options. Some of the properties are not configurable, such as Type and Name; the values for these properties are read-only.



Object Inspector

Image321: TBadgeImage32

BitmapAlign	baTopLeft
BorderColor	□ clBtnFace
BorderHighlight	□ clBtnHighlight
BorderInner	fsNone
BorderOuter	fsNone
BorderShadow	■ clBtnShadow
⊞ BorderSides	[sdLeft,sdTop,sdRight,sdBottom]
BorderWidth	0
DBField	
FlatColor	Personnel_UserID
FlatColorAdjustm...	Personnel_LastName
Height	Personnel_MiddleName
ImageType	Personnel_FirstName
Left	Personnel_Company
Name	Personnel_Address1
OffsetHorz	Personnel_Address2
OffsetVert	Personnel_City
PhotoIndex	1
SampleValue	
Scale	1
ScaleMode	smNormal
ScaledRotate	False
⊞ Scripting	(TScripting)
Top	102
TransparentColor	□ clWhite
TransparentImage	False
Width	105

Object Inspector

BadgeText1: TBadgeText

FrontSide: TBadgeLayout
(noname): TBadgeImage32
StaticText1: TBadgeStaticText
BarCode1: TBadgeBarCode
Image321: TBadgeImage32
(noname): TBadgeStaticText
BadgeText1: TBadgeText

If a property has more than one value option, the values are displayed via drop-down menu. This is true for properties that contain True/False values as well as properties that have multiple values. In the example above, the DBField property.

A plus sign indicates that the property field can be expanded to view sub-properties. **Click** the plus icon (+) to expand the property and display the additional options.

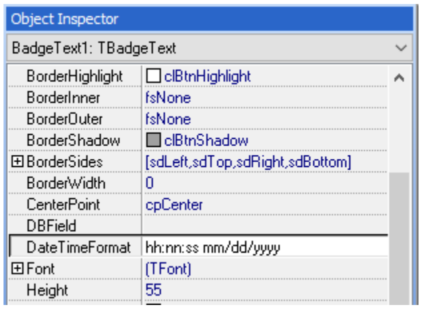
Date Time Format

If the information in the database field for a Text object or a Static Text object will be represented on the badge as a DateTimeFormat, the following will apply.

Click the DateTimeFormat property field to display a value field with a default string of hh:nn:ss mm/dd/yyyy, where hh = hours, nn = minutes, ss = seconds, mm = month, dd = day, and yyyy = 4-digit year.

The DateTimeFormat string is composed of specifiers that represent values to be inserted into the formatted string. Some specifiers (such as "d") simply format numbers or strings. Other specifiers (such as "/") refer to locale-specific strings from global variables.

The table on page 21-16 lists the specifiers available for DateTimeFormat strings. The specifiers are given in lower case. Case is ignored in formats, except for the "am/pm" and "a/p" specifiers.



Object Inspector

BadgeText1: TBadgeText

BorderHighlight	□ clBtnHighlight
BorderInner	fsNone
BorderOuter	fsNone
BorderShadow	■ clBtnShadow
⊞ BorderSides	[sdLeft,sdTop,sdRight,sdBottom]
BorderWidth	0
CenterPoint	cpCenter
DBField	
DateTimeFormat	hh:nn:ss mm/dd/yyyy
⊞ Font	(TFont)
Height	55

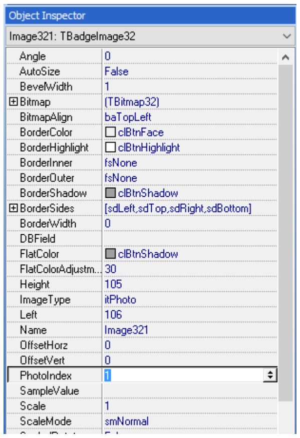
Specifier	Format
c	Displays the date using the format given by the ShortDateFormat global variable, followed by the time using the format given by the LongTimeFormat global variable. The time is not displayed if the date-time value indicates midnight precisely.
d	Displays the day as a number without a leading zero (1-31).
dd	Displays the day as a number with a leading zero (01-31).
ddd	Displays the day as an abbreviation (Sun-Sat) using the strings given by the ShortDayNames global variable.
dddd	Displays the day as a full name using the strings given by the LongDayNames global variable.
ddddd	Displays the date using the format given by the ShortDateFormat global variable.
dddddd	Displays the date using the format given by the LongDateFormat global variable.
e	Displays the year in the current period/era as a number without a leading zero (Japanese, Korean and Taiwanese locales only).
ee	Displays the year in the current period/era as a number with a leading zero (Japanese, Korean and Taiwanese locales only).
g	Displays the period/era as an abbreviation (Japanese and Taiwanese locales only).
gg	Displays the period/era as a full name. (Japanese and Taiwanese locales only).
m	Displays the month as a number without a leading zero (1-12). If the "m" specifier immediately follows an "h" or "hh" specifier, the minute rather than the month is displayed.
mm	Displays the month as a number with a leading zero (01-12). If the "mm" specifier immediately follows an "h" or "hh" specifier, the minute rather than the month is displayed.
mmm	Displays the month as an abbreviation using the strings given by the ShortMonthNames global variable.
mmmm	Displays the month as a full name using the strings given by the LongMonthNames global variable.
yy	Displays the year as a two-digit number (00-99).
yyyy	Displays the year as a four-digit number (0000-9999).
hh	Displays the hour with a leading zero (00-23).
n	Displays the minute without a leading zero (0-59).
nn	Displays the minute with a leading zero (00-59).
s	Displays the second without a leading zero (0-59).
ss	Displays the second with a leading zero (00-59).
z	Displays the millisecond without a leading zero (0-999).
zzz	Displays the millisecond with a leading zero (000-999).
t	Displays the time using the format given by the ShortTimeFormat global variable.
tt	Displays the time using the format given by the LongTimeFormat global variable.
am/pm	Uses the 12-hour clock for the preceding "h" or "hh" specifier, and displays "am" for any hour before noon, and "pm" for any hour after noon. The "am/pm" specifier can use lower, upper, or mixed case, and the result is displayed accordingly.
a/p	Uses the 12-hour clock for the preceding "h" or "hh" specifier, and displays "a" for any hour before noon, and "p" for any hour after noon. The a/p specifier can use lower, upper, or mixed case, and the result is displayed accordingly.
ampm	Uses the 12-hour clock for the preceding "h" or "hh" specifier, and displays the contents of the TimeAMString global variable for any hour before noon, and the contents of the TimePMString global variable for any hour after noon.
/	Displays the date separator character given by the DateSeparator global variable.
:	Displays the time separator character given by the TimeSeparator global variable.
'xx'/"xx"	Characters enclosed in single or double quotes are displayed as-is, and do not affect formatting.

Photo Index

An Image object can be configured to retrieve any of the four display photos associated with a personnel record.

To perform this function:

1. **Select** one of the four PhotoIndex listings in the PhotoIndex drop-down menu.



Object Inspector

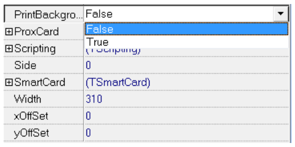
Image321: TBadgeImage32

Angle	0
AutoSize	False
BevelWidth	1
⊞ Bitmap	(TBitmap32)
BitmapAlign	baTopLeft
BorderColor	□ clBtnFace
BorderHighlight	□ clBtnHighlight
BorderInner	fsNone
BorderOuter	fsNone
BorderShadow	■ clBtnShadow
⊞ BorderSides	[sdLeft,sdTop,sdRight,sdBottom]
BorderWidth	0
DBField	
FlatColor	■ clBtnShadow
FlatColorAdjustm...	30
Height	105
ImageType	itPhoto
Left	106
Name	Image321
OffsetHorz	0
OffsetVert	0
PhotoIndex	1
SampleValue	
Scale	1
ScaleMode	smNormal

2. **Press** the Enter key after selecting the numeric value.

Print Background

If the badge's background will be an image or set to a specific color, the PrintBackground field will need to be set to True in order for the image or color to be visible.

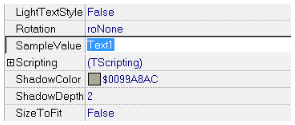


PrintBackgro...	False
⊞ ProxCard	False
⊞ Scripting	True
Side	0
⊞ SmartCard	(TSmartCard)
Width	310
xOffSet	0
yOffSet	0

Sample Value Property

Text, Image and Bar Code objects have a SampleValue property in the Object Inspector.

SampleValue properties allow the user to place a value to use as a placeholder. This has no effect on the template other than to allow the user to view the field with this placeholder sample to get an idea of what the badge will look like.



LightTextStyle	False
Rotation	roNone
SampleValue	Text1
⊞ Scripting	(TScripting)
ShadowColor	▨ $0099A8AC
ShadowDepth	2
SizeToFit	False

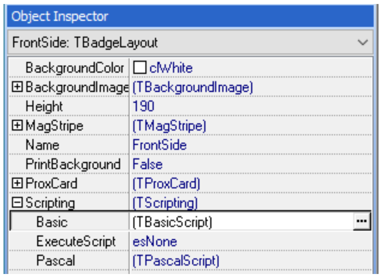
Text and Bar Code object values can be typed in the SampleValue field.

In the case of Image objects, the SampleValue requires a file. In such cases, the SampleValue field will display a Browse button. Clicking the Browse button displays the Open dialog, allowing the operator to navigate to the desired file.

Scripting

The Object Inspector provides a scripting feature that allows an operator to write program scripts.

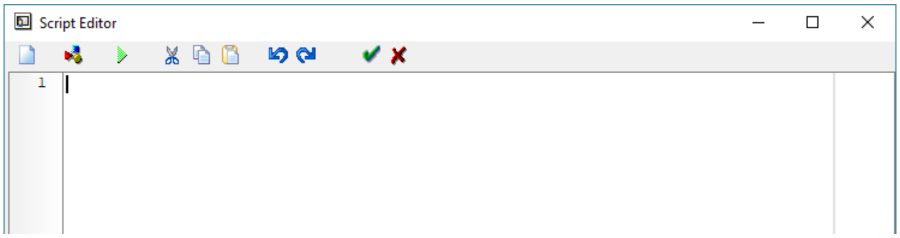
1. **Click** the plus (+) icon to expand the Scripting options.
2. **Select** the desired Scripting option.
3. **Click** the Browse button to display the Script Editor, where the operator can create scripts.



Object Inspector

FrontSide: TBadgeLayout

BackgroundColor	□ clWhite
⊞ BackgroundImage	(TBackgroundImage)
Height	190
⊞ MagStripe	(TMagStripe)
Name	FrontSide
PrintBackground	False
⊞ ProxCard	(TProxCard)
⊟ Scripting	(TScripting)
Basic	(TBasicScript)
ExecuteScript	esNone
Pascal	(TPascalScript)



Script Editor

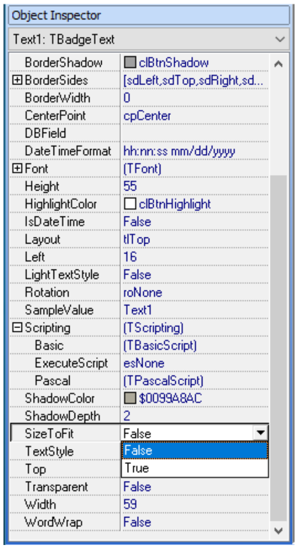
```
|
```

> ❗ *The* Scripting *functionality is an advanced feature of the* Badge Designer application*. For additional assistance regarding this feature, contact Open Options Technical Support or send an e-mail to support@ooaccess.com.*

Size To Fit

If enabled, the text in the selected object will either grow or shrink to fit the size of the object.

1. **Select** the SizeToFit property from the Object Inspector and **click** the drop-down arrow.



Object Inspector

Text1: TBadgeText

BorderShadow	▨ clBtnShadow
⊞BorderSides	[sdLeft,sdTop,sdRight,sd...
BorderWidth	0
CenterPoint	cpCenter
DBField	
DateTimeFormat	hh:nn:ss mm/dd/yyyy
⊞Font	(TFont)
Height	55
HighlightColor	□ clBtnHighlight
IsDateTime	False
Layout	tlTop
Left	16
LightTextStyle	False
Rotation	roNone
SampleValue	Text1
⊟Scripting	(TScripting)
Basic	(TBasicScript)
ExecuteScript	esNone
Pascal	(TPascalScript)
ShadowColor	▨ $0099A8AC
ShadowDepth	2
SizeToFit	False
TextStyle	False
Top	True
Transparent	False
Width	59
WordWrap	False

2. **Select** True to enable the feature.

Signature Settings

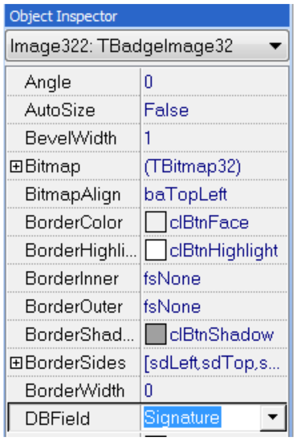
If a signature will be used on a badge, there are a number of settings that may need to be changed.

> *It may be easier to edit the badge template files in* Notepad *for some of the signature settings.*

1. **Insert** a Photo Placeholder.

   See page 21-8 for more information.

2. In the Object Inspector, **locate** DBField and **select** Signature from the drop-down list.



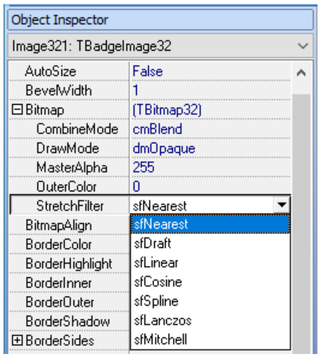
Object Inspector

Image322: TBadgeImage32

Angle	0
AutoSize	False
BevelWidth	1
⊞Bitmap	(TBitmap32)
BitmapAlign	baTopLeft
BorderColor	□ clBtnFace
BorderHighli...	□ clBtnHighlight
BorderInner	fsNone
BorderOuter	fsNone
BorderShad...	▨ clBtnShadow
⊞BorderSides	[sdLeft,sdTop,s...
BorderWidth	0
DBField	Signature

3. **Verify** that the AutoSize property is set to False.

4. **Expand** the Bitmap option and **select** the StretchFilter that best meets the project's requirements.



Object Inspector

Image321: TBadgeImage32

AutoSize	False
BevelWidth	1
⊟Bitmap	(TBitmap32)
CombineMode	cmBlend
DrawMode	dmOpaque
MasterAlpha	255
OuterColor	0
StretchFilter	sfNearest
BitmapAlign	sfNearest
BorderColor	sfDraft
BorderHighlight	sfLinear
BorderInner	sfCosine
BorderOuter	sfSpline
BorderShadow	sfLanczos
⊞BorderSides	sfMitchell

5. **Click** the ScaleMode drop-down arrow and **select** the desired resize option.

   See page 21-13 for more information on the scale options.

6. **Click** the Save button 💾 and **preview** the badge in DNA Fusion.

Configuring the Badge Type

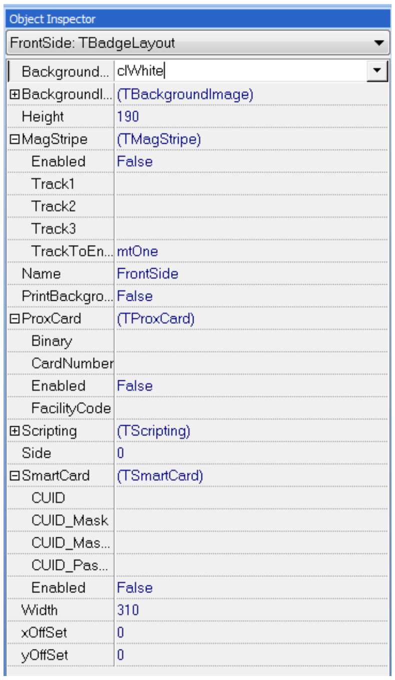
The Object Inspector contains three configurable card types:

- Magnetic Stripe Card (MagStripe)
- Proximity Card (ProxCard)
- Smart Card (SmartCard)

To configure a card:

1. In the Object Inspector and **select** Front Side TBadgeLayout from the drop-down list.

   The Badge Layout fields will change.

   Object Inspector

   FrontSide: TBadgeLayout

Background...	clWhite
⊞BackgroundI...	(TBackgroundImage)
Height	190
⊟MagStripe	(TMagStripe)
Enabled	False
Track1	
Track2	
Track3	
TrackToEn...	mtOne
Name	FrontSide
PrintBackgro...	False
⊟ProxCard	(TProxCard)
Binary	
CardNumber	
Enabled	False
FacilityCode	
⊞Scripting	(TScripting)
Side	0
⊟SmartCard	(TSmartCard)
CUID	
CUID_Mask	
CUID_Mas...	
CUID_Pas...	
Enabled	False
Width	310
xOffSet	0
yOffSet	0

2. **Enter** the values for the desired card type.

Saving a Badge Template

Badge template files will be saved as a .bdg file. The default location is C:\Users\Public\Public Documents\ Open Options, Inc\dnaFusion\Templates\.

Save the configured Badge Template by using one of the following methods:

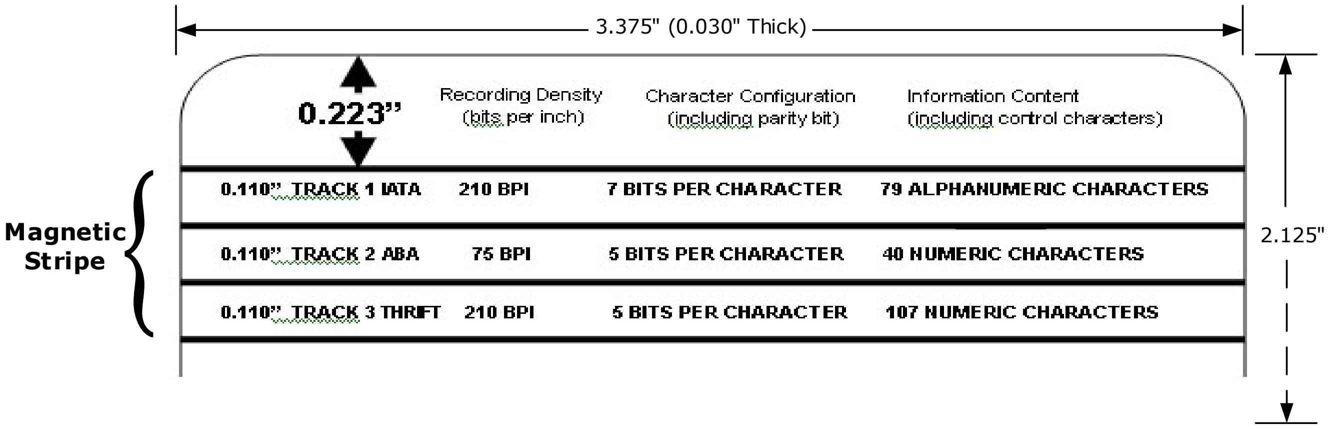
- **Click** File / Save from the Main Menu.
- **Click** the Save button. 💾
- **Click** Save As to change the file name and save the file to the default directory.

If a client workstation will be used for badging, create a shared directory for templates. This will allow the client to access the badge templates.

Magnetic Stripe Card

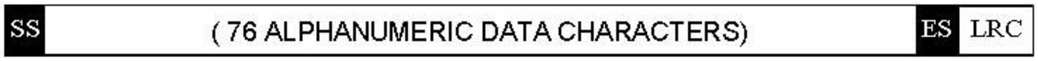
U.S. Standards

Magnetic Stripe Encoding



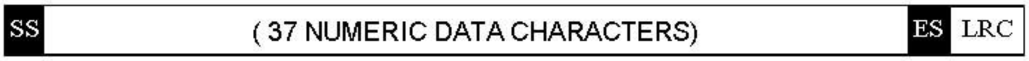
	Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110" TRACK 1 IATA	210 BPI	7 BITS PER CHARACTER	79 ALPHANUMERIC CHARACTERS
0.110" TRACK 2 ABA	75 BPI	5 BITS PER CHARACTER	40 NUMERIC CHARACTERS
0.110" TRACK 3 THRIFT	210 BPI	5 BITS PER CHARACTER	107 NUMERIC CHARACTERS

Card Data Format - Track 1



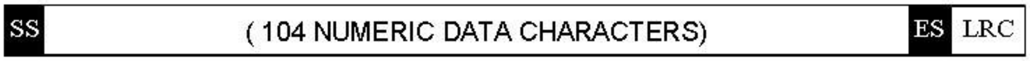
SS	Start Sentinel	%		
ES	End Sentinel	?	LRC	Longitudinal Redundancy Check character

Card Data Format - Track 2



SS	Start Sentinel	;		
ES	End Sentinel	?	LRC	Longitudinal Redundancy Check character

Card Data Format - Track 3



SS	Start Sentinel	;		
ES	End Sentinel	?	LRC	Longitudinal Redundancy Check character

Badge Manager

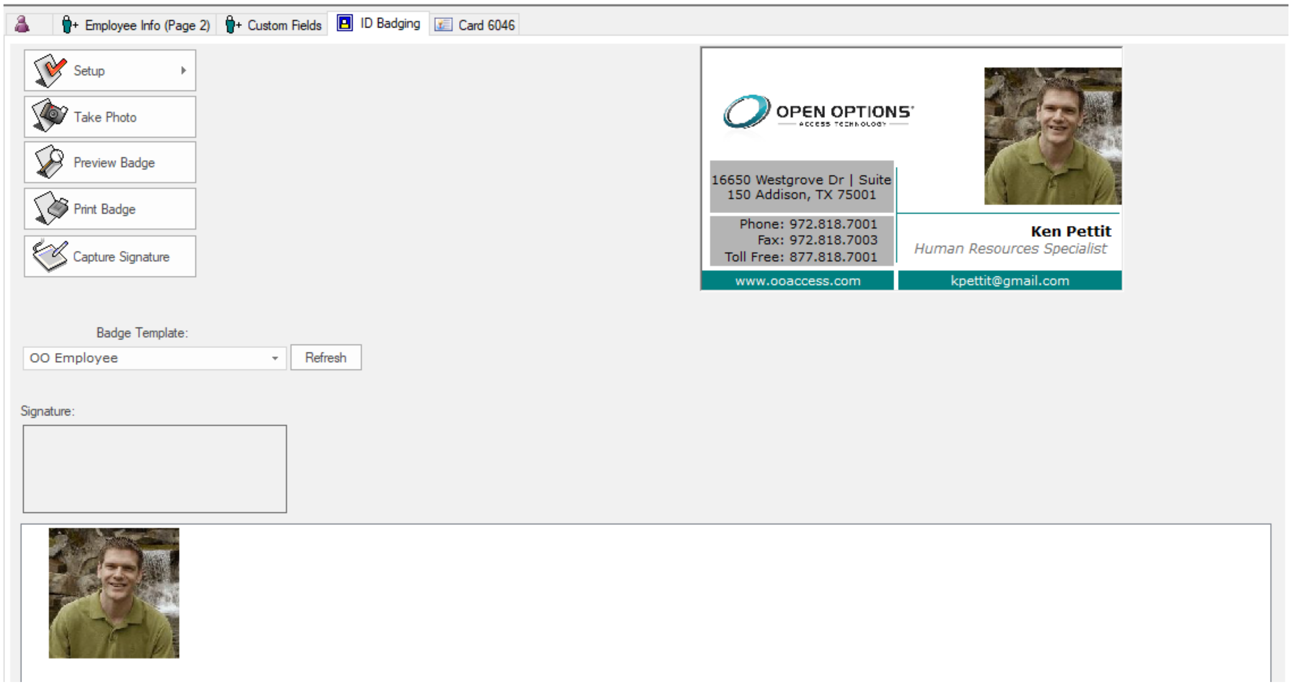
The badging functionality for DNA Fusion is located in the ID Badging tab of the Cardholder's Record. Open the tab to display the Badge Manager.

The Badge Manager is a user-friendly interface that allows the operator to take a photograph, apply the appropriate data from the cardholder's record to the selected badge template, and preview or print the badge as needed.

The Badge Manager Environment

The Badge Manager consists of the following elements:

- Five operation buttons
- The Badge Template selector
- The Static Preview Panel



Badge Template: OO Employee

16650 Westgrove Dr | Suite 150 Addison, TX 75001
Phone: 972.818.7001
Fax: 972.818.7003
Toll Free: 877.818.7001
www.ooaccess.com

Ken Pettit
Human Resources Specialist
kpettit@gmail.com

The elements function as follows:

- Setup - Displays a context menu: Printer Setup, Select Camera Type, and Advanced Setup. Depending on the selection, a setup dialog box will open. See page 21-23 for more information.
- Take Photo - Displays the camera interface (Capture Photo) dialog. See page 21-25 for more information.
- Preview Badge - Displays the interactive (zoom-able) preview window. Use the drop-down menu, and the plus and minus symbols along the top of the dialog to zoom in and out. See page 21-26 for more information.
- Print Badge - Prints the badge at the card printer. See page 21-26 for more information.
- Capture Signature - Opens the Capture Signature dialog and allows for the capturing of cardholders signatures. For use with ePad devices. See page 21-26 for more information.
- Badge Template - Drop-down list of pre-constructed badge templates. The Static Preview Panel will display a static preview of the template configured with the appropriate data of the current record.
- Static Preview Panel - Static badge preview that is automatically displayed after selecting a badge template. Unlike the Preview Badge window, it is not interactive.

NOTES:

Setup Dialogs

The Setup dialogs allow you to configure the different object parameters.

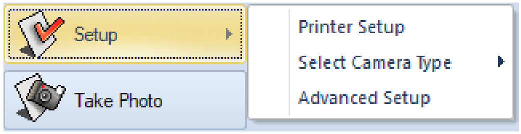
To open a dialog:

1. **Click** the Setup button in the ID Badging tab of the Cardholder's Record.

   A context menu appears.

2. **Select** the desired menu option.

   The Setup dialog opens for the selected object.



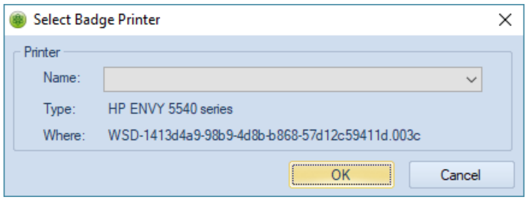
Printer Setup

1. **Select** Printer Setup from the context menu.

   The Select Badge Printer dialog appears.

2. **Select** the Printer from the drop-down list.

3. **Click** OK.


Select Badge Printer

Printer

Name:

Type: HP ENVY 5540 series

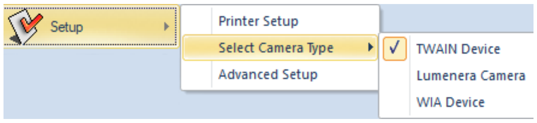
Where: WSD-1413d4a9-98b9-4d8b-b868-57d12c59411d.003c

OK Cancel

Camera Setup

1. **Select** the Camera Type from the sub-menu.

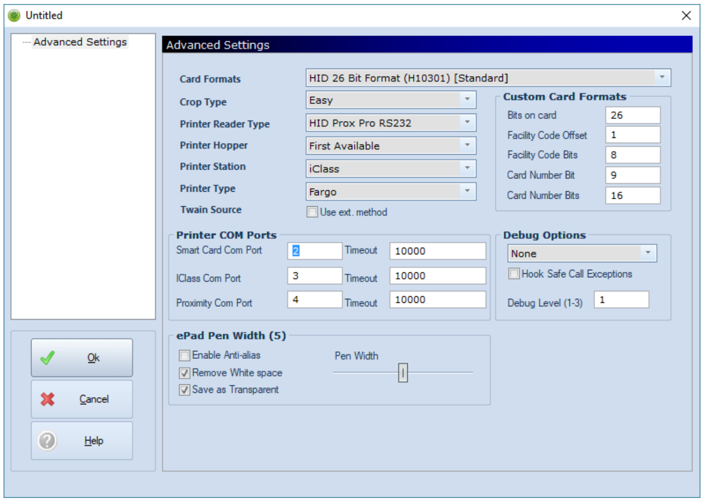
2. **Select** the Camera/Device from the list.



Advanced Setup

1. **Select** Advanced Setup from the context menu.

   The Advanced Settings dialog opens.


Untitled

Advanced Settings

Advanced Settings

Card Formats: HID 26 Bit Format (H10301) [Standard]

Crop Type: Easy

Printer Reader Type: HID Prox Pro RS232

Printer Hopper: First Available

Printer Station: iClass

Printer Type: Fargo

Twain Source: □ Use ext. method

Custom Card Formats

Bits on card: 26

Facility Code Offset: 1

Facility Code Bits: 8

Card Number Bit: 9

Card Number Bits: 16

Printer COM Ports

Smart Card Com Port: 2 Timeout: 10000

IClass Com Port: 3 Timeout: 10000

Proximity Com Port: 4 Timeout: 10000

Debug Options

None

□ Hook Safe Call Exceptions

Debug Level (1-3): 1

ePad Pen Width (5)

□ Enable Anti-alias

☑ Remove White space

☑ Save as Transparent

Pen Width

Ok Cancel Help

2. **Configure** the badge options.

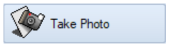
   - Card Formats - Select the Card Format from the drop-down list. If Custom is selected, the Custom Card Formats section must be completed.
   - Crop Type - Sets the crop option when a photo is taken with a camera attached to DNA Fusion. See page 21-25 for more information. The default Easy setting is recommended for operators that are inexperienced with graphic programs.
     - Easy - Simplest crop method. Crops the photo with a presized crop box.
     - Medium - Crops the photo using four configurable crop lines.
     - Advanced - Opens the Image Editor to allow photo cropping and editing.
   - Printer Reader Type - If the printer is equipped with a reader, select the Reader Type from the drop-down list.
   - Printer Hopper - If the printer is equipped with a hopper, select the hopper's physical location on the printer from the drop-down list. The default setting, First Available, will use the first available hopper.

- Printer Station - Select the printer device from the drop-down menu.
- Printer Type - Select the type of printer device from the drop-down menu.
- Twain Source - If Use Ext. Method is checked, the printer will check if a TWAIN driver will be used to communicate with the camera.
- Printer COM Ports - Specify the Printer COM Port for each device as well as the Timeout.
- Custom Card Format - If Custom was selected in the Card Formats drop-down, enter the format information for the custom card.
- Debug Options - Select the debug option from the drop-down list: Send to File, Send to Viewer, Send to Viewer and File.
  - Hook Safe Call Exceptions - For debugging, all call exceptions will be logged.
  - Debug Level (1-3) - If debug is selected, the level will provide diagnostic information. The higher the number, the more detailed information is collected. The more information, the larger the file size.
- Enable Anti-Alias - If checked, uses an anti-aliasing technique to smooth signature lines on the ePad.
- Remove White Space - If checked, removes the white space around the signature drawn on the ePad.
- Save as Transparent - If checked, saves the ePad signature with a transparent background.
- Pen Width - Adjust the slider to increase or decrease the thickness of the ePad pen.

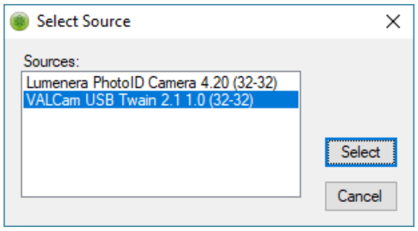
3. **Click** OK to save the settings.

Taking a Photo

The following instructions are intended for the VALCam 9000-628 camera model manufactured by Video Associates Labs. The camera driver must be installed on the host computer prior to using this feature.

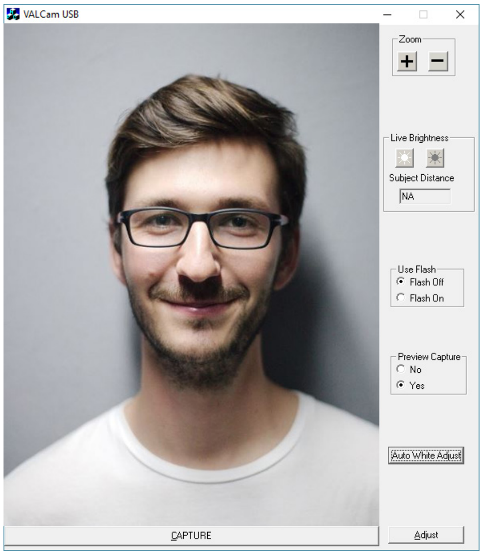
1. **Verify** that camera is ON and connected to a USB port.
2. In the ID Badging tab of the Cardholder's Record, **select** Setup / Select Camera Type / TWAIN Device.
3. **Click** the Take Photo button. 

   The Select Source dialog opens.


Select Source
Sources:
Lumenera PhotoID Camera 4.20 (32-32)
VALCam USB Twain 2.1 1.0 (32-32)
Select
Cancel

4. **Select** the appropriate Camera Source from the list and **click** the Select button.

   The VALCam USB dialog appears.



Subject Distance: NA

Use Flash: ● Flash Off ○ Flash On

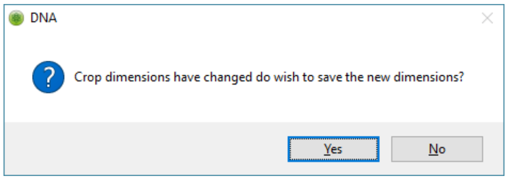
Preview Capture: ○ No ● Yes

5. **Adjust** the camera settings as desired:
   - Zoom - Increases or decreases the zoom level.
   - Live Brightness - Increases or decreases the brightness in the live preview.
   - Use Flash - Indicates whether the flash will be On or Off.
   - Preview Capture - Indicates whether a color-adjustable preview of the captured photo will appear before the photo is saved.
   - Auto White Adjust - If selected, automatically adjusts the white balance based on a white or gray object positioned in front of the camera.
   - Adjust - Opens the Adjust dialog, which allows the operator to alter additional photo settings. The dialog contains four tabs: Flesh Tones, Advanced, Capture Type, and Crop.
6. **Click** the Capture button to take the photo.

   If Preview Capture was set to Yes, **configure** the Red and Blue Color Adjust settings and **click** Save.

   The Photo Badging dialog appears.
7. If desired, **select** Crop Setting and **resize** the Crop Width and/or Crop Height dimensions.
8. **Drag** the blue outline to the desired crop position.
9. **Click** OK to save the settings.

   If the crop dimensions were changed, a confirmation dialog will appear. **Click** Yes.



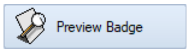
Crop dimensions have changed do wish to save the new dimensions?

10. The photo is added to the white space at the bottom of the ID Badging tab.
11. To edit the photo properties, **right-click** on the photo and **select** Photo Properties.

> *Photos should be limited to a size of 1 MB. DNA Fusion defaults the* Image Size *to small and sets the* Image Quality *to normal to achieve a high-quality photo while maintaining a manageable file size.*

Previewing a Badge

To view an interactive preview of the badge:

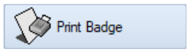
1. **Click** the Preview Badge button. 

   The Preview Badge viewer opens.

   - Use the forward/reverse arrows to move between pages of a two-sided badge.
   - Use the plus (+) and minus (–) signs and the drop–down menu to zoom in and out of the preview.
   - **Click** the Print Setup button to display the Print Setup dialog.

2. **Click** the X to close the dialog.

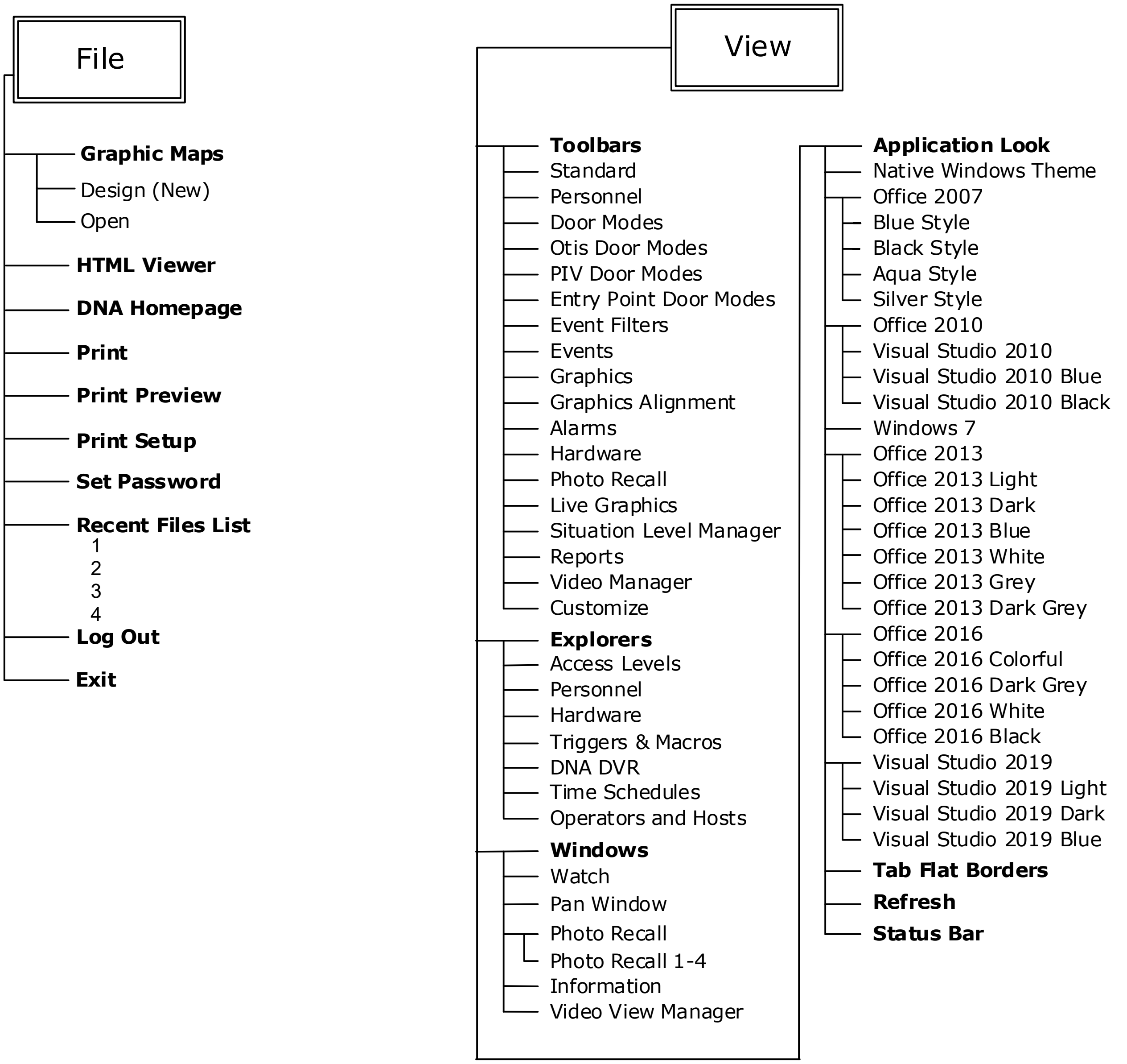
Printing a Badge

1. **Click** the Print Badge button. 

   The Page Setup dialog appears.

2. **Click** OK to print the badge.

Menu Structure A



- File
  - **Graphic Maps**
    - Design (New)
    - Open
  - **HTML Viewer**
  - **DNA Homepage**
  - **Print**
  - **Print Preview**
  - **Print Setup**
  - **Set Password**
  - **Recent Files List**
    - 1
    - 2
    - 3
    - 4
  - **Log Out**
  - **Exit**

- View
  - **Toolbars**
    - Standard
    - Personnel
    - Door Modes
    - Otis Door Modes
    - PIV Door Modes
    - Entry Point Door Modes
    - Event Filters
    - Events
    - Graphics
    - Graphics Alignment
    - Alarms
    - Hardware
    - Photo Recall
    - Live Graphics
    - Situation Level Manager
    - Reports
    - Video Manager
    - Customize
  - **Explorers**
    - Access Levels
    - Personnel
    - Hardware
    - Triggers & Macros
    - DNA DVR
    - Time Schedules
    - Operators and Hosts
  - **Windows**
    - Watch
    - Pan Window
    - Photo Recall
      - Photo Recall 1-4
    - Information
    - Video View Manager
  - **Application Look**
    - Native Windows Theme
    - Office 2007
      - Blue Style
      - Black Style
      - Aqua Style
      - Silver Style
    - Office 2010
      - Visual Studio 2010
      - Visual Studio 2010 Blue
      - Visual Studio 2010 Black
    - Windows 7
    - Office 2013
      - Office 2013 Light
      - Office 2013 Dark
      - Office 2013 Blue
      - Office 2013 White
      - Office 2013 Grey
      - Office 2013 Dark Grey
    - Office 2016
      - Office 2016 Colorful
      - Office 2016 Dark Grey
      - Office 2016 White
      - Office 2016 Black
    - Visual Studio 2019
      - Visual Studio 2019 Light
      - Visual Studio 2019 Dark
      - Visual Studio 2019 Blue
  - **Tab Flat Borders**
  - **Refresh**
  - **Status Bar**

- DNA
  - **Administrative**
    - **Properties**
    - **Operator Maintenance**
      - Save Operator Environment
      - Edit Operator Environment
      - Operator Privileges
    - **Alarms & Events**
      - Clear All Alarms
      - Dispatch Text
      - Logging
    - **Edit HTML Tree**
    - **Batch Processing**
    - **Tenants**
    - **Setup Filters**
    - **Setup Escalation**
    - **Setup Internal Schedules**
    - **Setup Custom Personnel Permissions**
    - **Driver Setup (Server Only)**
    - **DNA Directories**
    - **SSP Communications File**
      - Generate Capture File(s)
    - **DNA Data Management**
      - Archive Profiles
      - Restore Data
      - Export
    - **Scheduling**
      - Archive Data
      - Batch Files
      - Downloads
      - Reports
    - **Journal Entry Types**
    - **Station Statistics**
  - **Journal**
    - New Entry
    - View

- Hardware
  - **Download**
  - **Control**
  - **Direct Commands**
    - Manage
    - Execute
    - Custom Command(s)
  - **Properties**
  - **Promote SSP**
  - **Add**
    - Channel
    - Add Door
      - Use Default
      - Use Template
    - Elevator
    - MPG
    - Subcontoller
    - SSP
    - Keypad Command
  - **View Hardware**
  - **Status**
  - **ACM Status Report**
    - Open
    - New Report
  - **Hardware Monitor Report**
    - Open
    - New Report
  - **Defaults**
  - **Card Formats**
  - **Web Service Credentials**
  - **Trigger Codes**
  - **Add to Macro**
  - **Templates**
  - **Homepage**

Personnel

- **Properties**
- **Add Cardholder**
- **Remove Cardholder**
- **Update**
- **Add Record From Scanner**
- **Scanner Options**
  - Calibrate Scanner
  - Clean Scanner
- **Watch Item**
- **Add Personnel Group**
- **Download**
- **Set Use Limit**
- **Photo Recall**
  - Goto Photo (1-8)
  - Zoom In
  - Zoom Out
  - Stop Cycling
  - Personnel Record
  - Get Note
  - Pause
  - Other Photos
  - Remove
  - Clear
  - E-mail Photo
  - Set up

Reports

- **Alarms**
  - Alarms History
  - Acknowledged Alarms
  - Pending Alarms
- **Events**
  - Event History
  - DMP Receiver Transactions
  - Bosch Receiver Transactions
  - Thyssen Krupp Elevator Access
  - Event Log Settings
- **Restored Archive Data**
  - Acknowledged Alarms
  - Audit Trail
  - Event History
- **Access**
  - Access Levels by SSP
  - Access Level Descriptions
  - Legacy Access Level Groups
  - Global Access Level Details
  - Access Level Group Assignments
  - Floors
  - Door Access Profile
  - Who Has Access Door(s)
  - Access Level Last Used
  - Assa Access Levels
- **Personnel**
  - Companies
  - Personnel - Card Information
  - Personnel - General
  - Personnel - Access
  - Personnel - Groups
  - Personnel - Summary
  - Personnel - Daily Card Usage
  - Personnel - Printed Badges
  - Personnel - Schindler
- **Hardware Settings**
  - Sites
  - Channels
  - Controllers (SSP)
  - Controllers DST Settings
  - Sub-controllers (SIO)
  - Monitor Points
  - Control Points
  - Readers
  - Elevators
  - Cameras
  - Monitor Point Groups (MPG)
  - Card Formats
  - Doors
  - Door Contacts
  - Request To Exit (RTE)
  - Door Strikes
  - APB Doors
  - ASSA and Allegion Doors
  - Bosch Panel Reports
    - Bosch Panels
    - Bosch Areas
    - Bosch Panels
    - Bosch Points
    - Bosch Outputs
  - Engage Reports
    - Sites
    - Gateways
    - Doors
- **System**
  - Audit Trail
  - Holidays
  - Macros
  - Time Schedules
  - Triggers
  - Host Based Macros
  - Auto Armed Secured Areas
  - Door Follows Time Schedule Report
  - Station Status
- **Custom Reports**
  - Add
  - Manager
  - Custom 1-20

Events

- **Filters**
  - **Door**
    - Door
    - Mode Change
    - Access Granted
    - Access Denied
  - **Hardware**
    - Comm Events
    - Arm
    - Disarm
    - Secure or Inactive
    - Alarm or Active
    - Access Areas
    - MPG (Monitor Point Groups)
    - Time, Triggers, Macros
    - Miscellaneous
    - Camera Events
    - Stentofon Events
    - Axis Events
    - Isonas Events
    - Bosch Panel Events
    - Engage Events
  - **Operator**
    - Operator Commands
    - Alarm Handling
  - **Index**
  - **Secondary Filters**
    - Time and Date
    - Hardware Object
    - Operator
    - Tenant
    - Cardholder
    - Personnel Type
      - Contractor
      - Disabled
      - Normal
      - Temp
      - Visitor
      - Vendor
      - Custom 1-5
    - Card Type
      - Contractor
      - Disabled
      - Normal
      - Temp
      - Visitor
      - Vendor
      - Custom 1-5
    - Event Source
  - **Toggle Filter**
  - **Clear All Filters**
- **Hardware**
  - Object Properties
  - Control Point
  - Launch Camera
  - Show Archived Video
  - Export Video
  - Load Homepage
  - Trace History
  - Watch Item
- **Personnel**
  - Photo Recall
  - Personnel Record
  - Get/Set Note
  - Trace History
  - Activate Card
  - Deactivate Card
  - Set Use Limit
  - Free Pass
  - Watch Item
- **E-mail Event**
- **Reports**
  - Events History
  - DMP Receiver Transactions
  - Bosch Receiver Transactions
  - Thyssenkrupp Elevator Access
  - Logging
- **Grid**
  - Grid Properties
  - Save Settings
  - Load Settings
  - Pause Scrolling
  - Print Preview
  - Print
  - Auto Fit Grid
- **Events Grid**

Alarms

- **Acknowledge**
- **Clear**
- **Dismiss**
- **E-Mail**
- **Select All**
- **Alarm Information**
- **Hardware**
  - Point Properties
  - Control
  - Launch Camera
  - Show Archived Video
  - Export Video and Email
  - DVR Recordings
  - Load Homepage
- **Personnel – Personnel Records**
- **Grid Setup**
- **Field Chooser**
- **Group By Box**

Tools

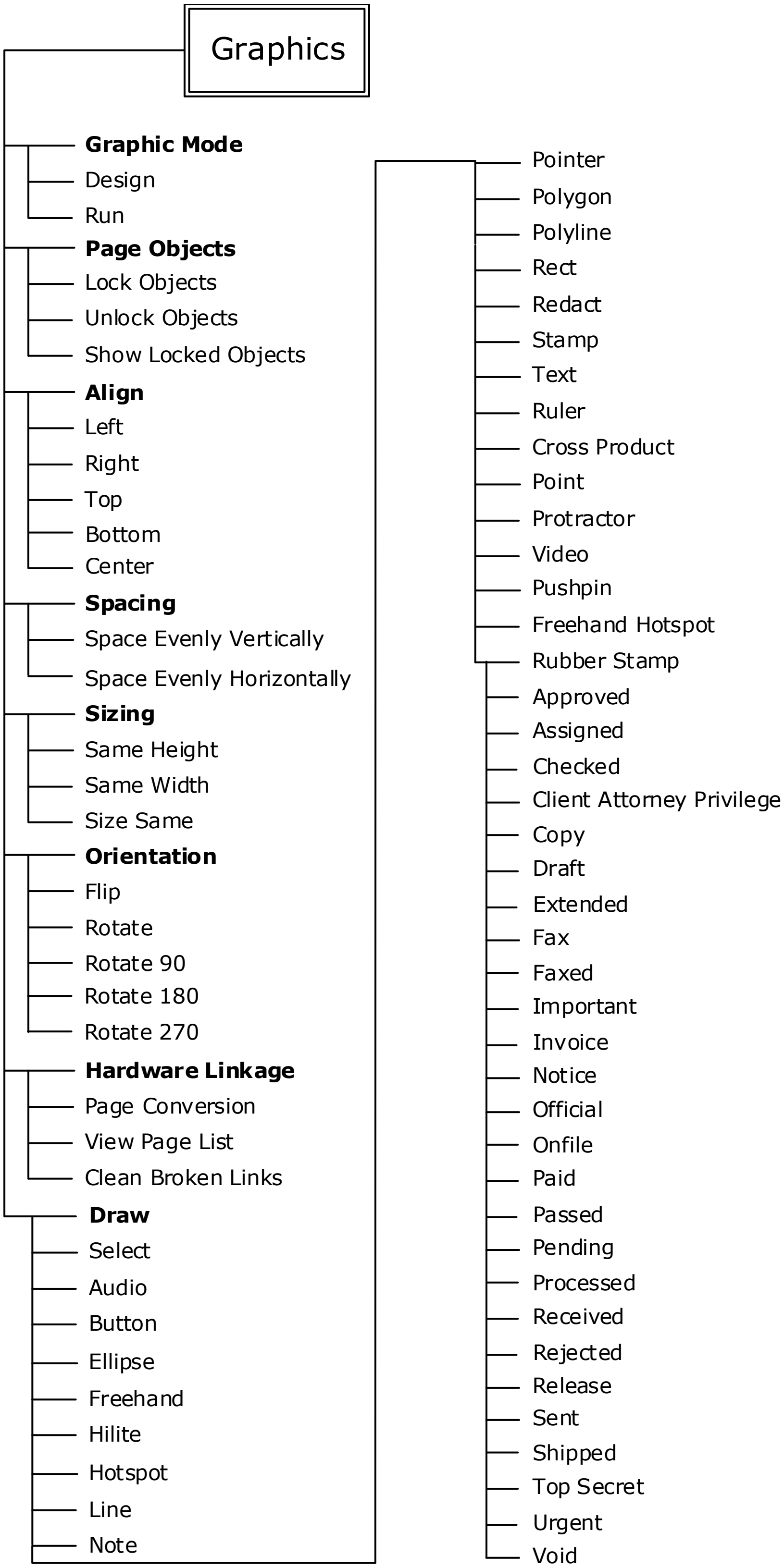
- **User Defined Tools**

Window

- **MDI Tab Groups**
- **Windows**

Help

- **DNA Directories**
  - Log Files
  - Backups
  - Graphic Maps
  - HTML Files
  - Photos
  - Reports
  - Templates
  - Video Exports
- **OpenOptions Help on the Web**
- **About DNA**

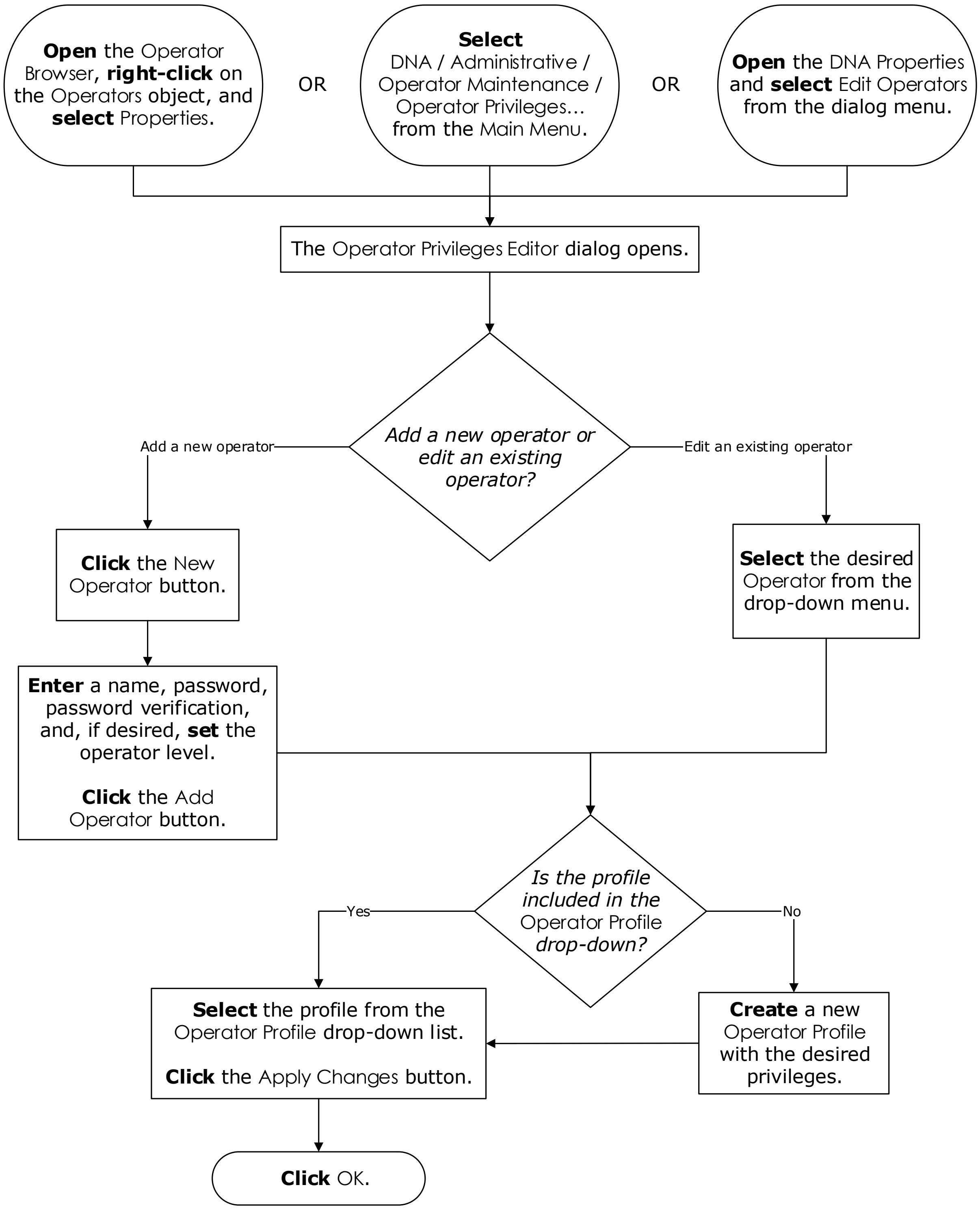

Graphics
Graphic Mode
Design
Run
Page Objects
Lock Objects
Unlock Objects
Show Locked Objects
Align
Left
Right
Top
Bottom
Center
Spacing
Space Evenly Vertically
Space Evenly Horizontally
Sizing
Same Height
Same Width
Size Same
Orientation
Flip
Rotate
Rotate 90
Rotate 180
Rotate 270
Hardware Linkage
Page Conversion
View Page List
Clean Broken Links
Draw
Select
Audio
Button
Ellipse
Freehand
Hilite
Hotspot
Line
Note
Pointer
Polygon
Polyline
Rect
Redact
Stamp
Text
Ruler
Cross Product
Point
Protractor
Video
Pushpin
Freehand Hotspot
Rubber Stamp
Approved
Assigned
Checked
Client Attorney Privilege
Copy
Draft
Extended
Fax
Faxed
Important
Invoice
Notice
Official
Onfile
Paid
Passed
Pending
Processed
Received
Rejected
Release
Sent
Shipped
Top Secret
Urgent
Void

This Page Intentionally Left Blank

Process Diagrams B

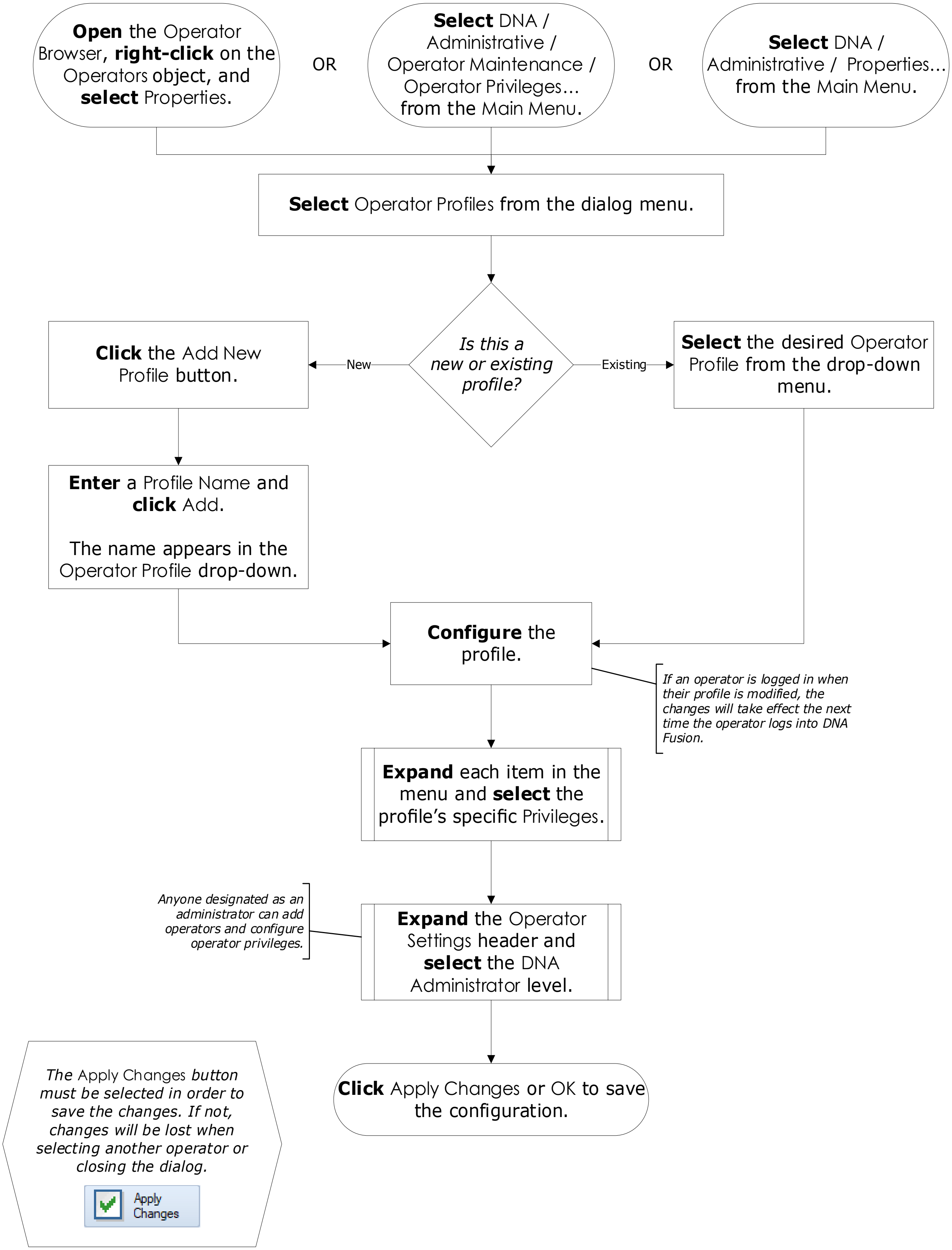
Adding a New Operator and Assigning a Profile

See Chapter 4 for more information on Operators and Operator Profiles.


Open the Operator Browser, **right-click** on the Operators object, and **select** Properties.
OR
Select DNA / Administrative / Operator Maintenance / Operator Privileges... from the Main Menu.
OR
Open the DNA Properties and **select** Edit Operators from the dialog menu.
The Operator Privileges Editor dialog opens.
Add a new operator or edit an existing operator?
Add a new operator
Edit an existing operator
Click the New Operator button.
Enter a name, password, password verification, and, if desired, **set** the operator level.
Click the Add Operator button.
Select the desired Operator from the drop-down menu.
Is the profile included in the Operator Profile *drop-down?*
Yes
No
Select the profile from the Operator Profile drop-down list.
Click the Apply Changes button.
Create a new Operator Profile with the desired privileges.
Click OK.

Configuring Operator Profiles

See Chapter 4 for more information on Operators and Operator Profiles.



Open the Operator Browser, **right-click** on the Operators object, and **select** Properties.

OR

Select DNA / Administrative / Operator Maintenance / Operator Privileges… from the Main Menu.

OR

Select DNA / Administrative / Properties… from the Main Menu.

Select Operator Profiles from the dialog menu.

Is this a new or existing profile?

Click the Add New Profile button.

Enter a Profile Name and **click** Add.

The name appears in the Operator Profile drop-down.

Select the desired Operator Profile from the drop-down menu.

Configure the profile.

If an operator is logged in when their profile is modified, the changes will take effect the next time the operator logs into DNA Fusion.

Expand each item in the menu and **select** the profile’s specific Privileges.

Anyone designated as an administrator can add operators and configure operator privileges.

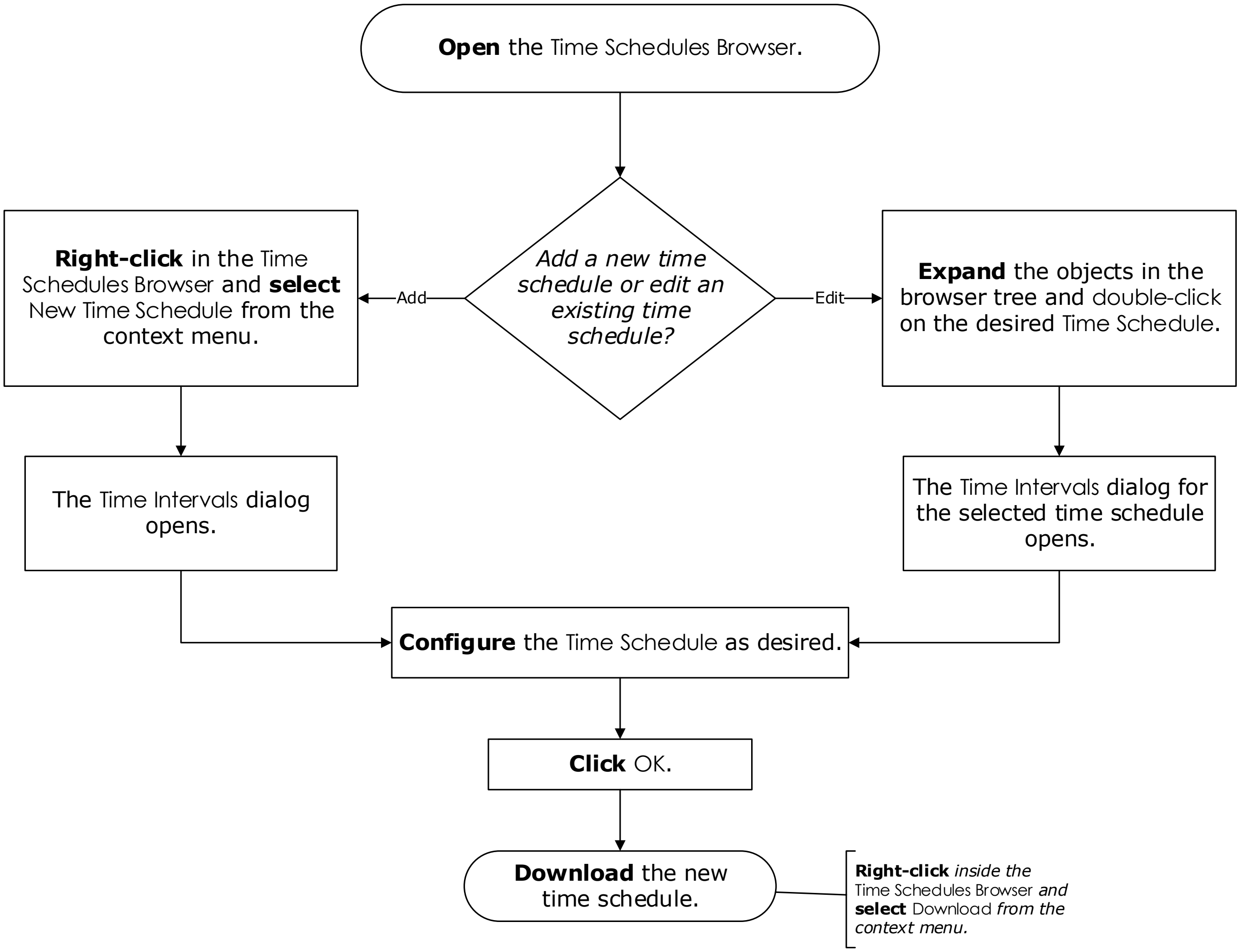
Expand the Operator Settings header and **select** the DNA Administrator level.

Click Apply Changes or OK to save the configuration.

The Apply Changes *button must be selected in order to save the changes. If not, changes will be lost when selecting another operator or closing the dialog.*

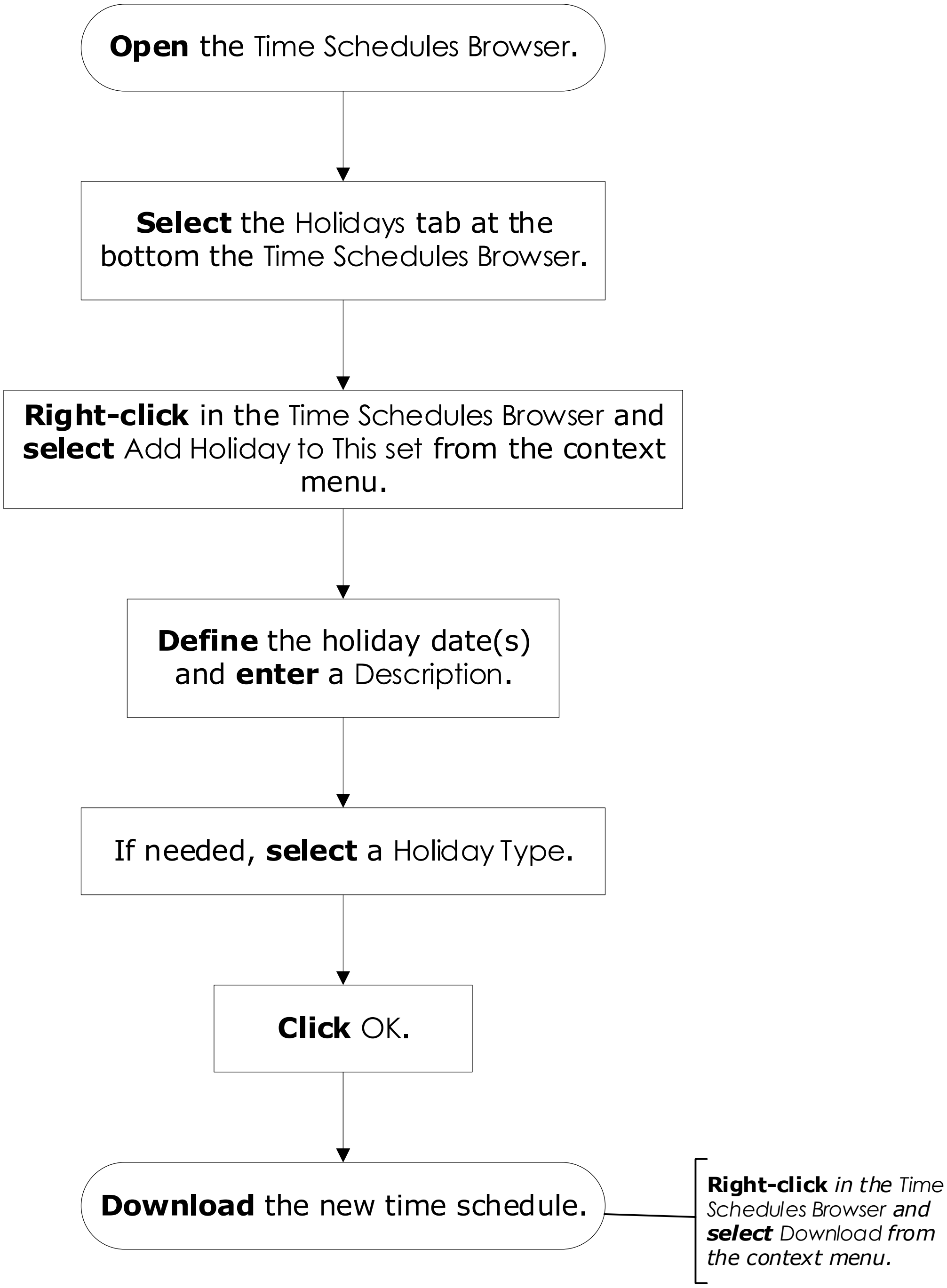
Adding and Editing Time Schedules

See Chapter 5 for more information on Time and Holiday Schedules.


Open the Time Schedules Browser.
Add a new time schedule or edit an existing time schedule?
Add
Edit
Right-click in the Time Schedules Browser and **select** New Time Schedule from the context menu.
Expand the objects in the browser tree and double-click on the desired Time Schedule.
The Time Intervals dialog opens.
The Time Intervals dialog for the selected time schedule opens.
Configure the Time Schedule as desired.
Click OK.
Download the new time schedule.
Right-click *inside the* Time Schedules Browser *and* **select** Download *from the context menu.*

Adding a Holiday

See Chapter 5 for more information on Time and Holiday Schedules.



Open the Time Schedules Browser.

Select the Holidays tab at the bottom the Time Schedules Browser.

Right-click in the Time Schedules Browser and **select** Add Holiday to This set from the context menu.

Define the holiday date(s) and **enter** a Description.

If needed, **select** a Holiday Type.

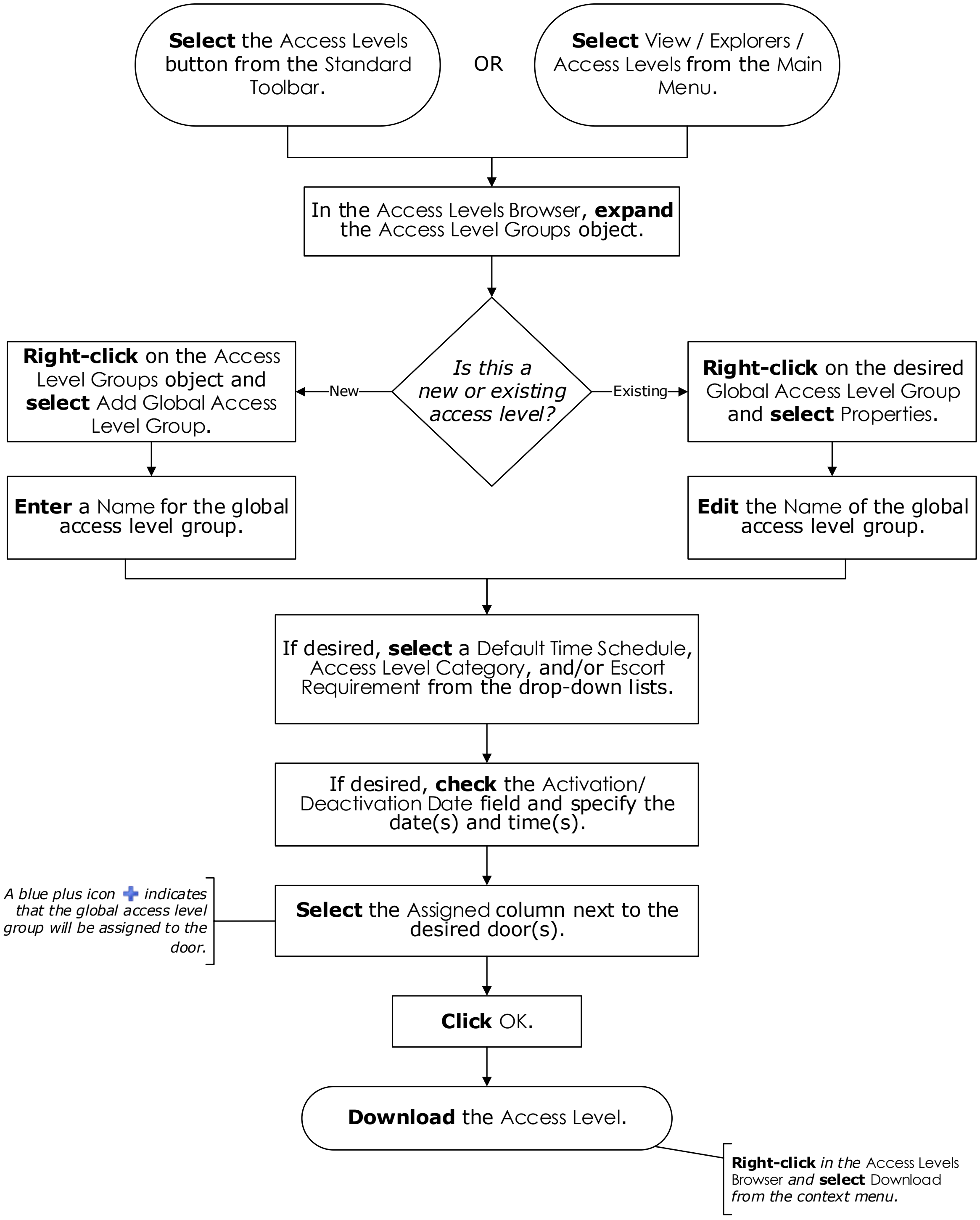
Click OK.

Download the new time schedule.

Right-click *in the Time Schedules Browser and* ***select*** *Download from the context menu.*

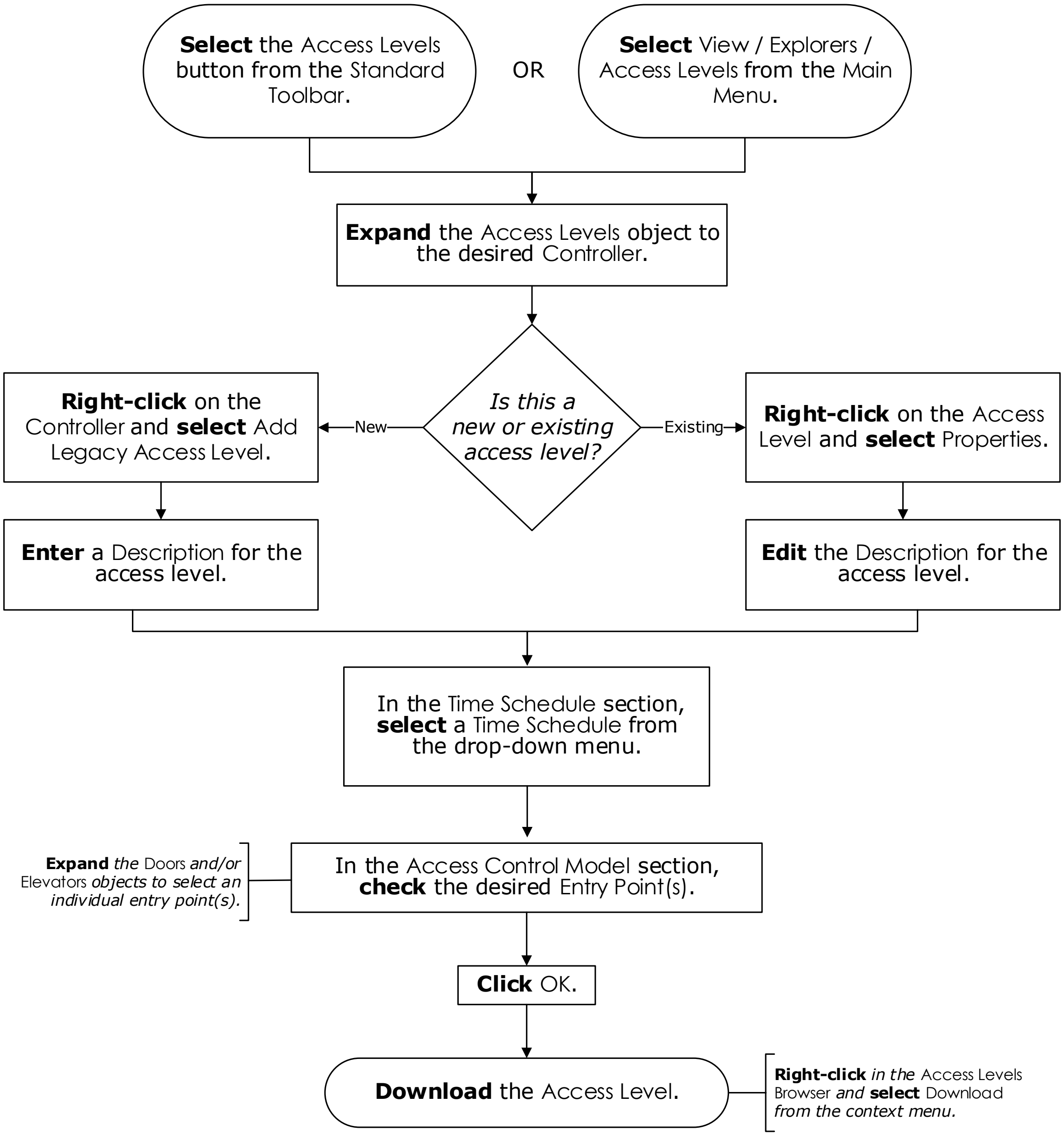
Creating a Global Access Level

See Chapter 6 for more information on Access Levels.


Select the Access Levels button from the Standard Toolbar.
OR
Select View / Explorers / Access Levels from the Main Menu.
In the Access Levels Browser, **expand** the Access Level Groups object.
Is this a new or existing access level?
New
Existing
Right-click on the Access Level Groups object and **select** Add Global Access Level Group.
Enter a Name for the global access level group.
Right-click on the desired Global Access Level Group and **select** Properties.
Edit the Name of the global access level group.
If desired, **select** a Default Time Schedule, Access Level Category, and/or Escort Requirement from the drop-down lists.
If desired, **check** the Activation/ Deactivation Date field and specify the date(s) and time(s).
A blue plus icon ✚ indicates that the global access level group will be assigned to the door.
Select the Assigned column next to the desired door(s).
Click OK.
Download the Access Level.
Right-click in the Access Levels Browser and **select** Download from the context menu.

Creating a Legacy Access Level

See Chapter 6 for more information on Access Levels.



Select the Access Levels button from the Standard Toolbar.

Select View / Explorers / Access Levels from the Main Menu.

Expand the Access Levels object to the desired Controller.

Is this a new or existing access level?

Right-click on the Controller and **select** Add Legacy Access Level.

Enter a Description for the access level.

Right-click on the Access Level and **select** Properties.

Edit the Description for the access level.

In the Time Schedule section, **select** a Time Schedule from the drop-down menu.

In the Access Control Model section, **check** the desired Entry Point(s).

***Expand** the Doors and/or Elevators objects to select an individual entry point(s).*

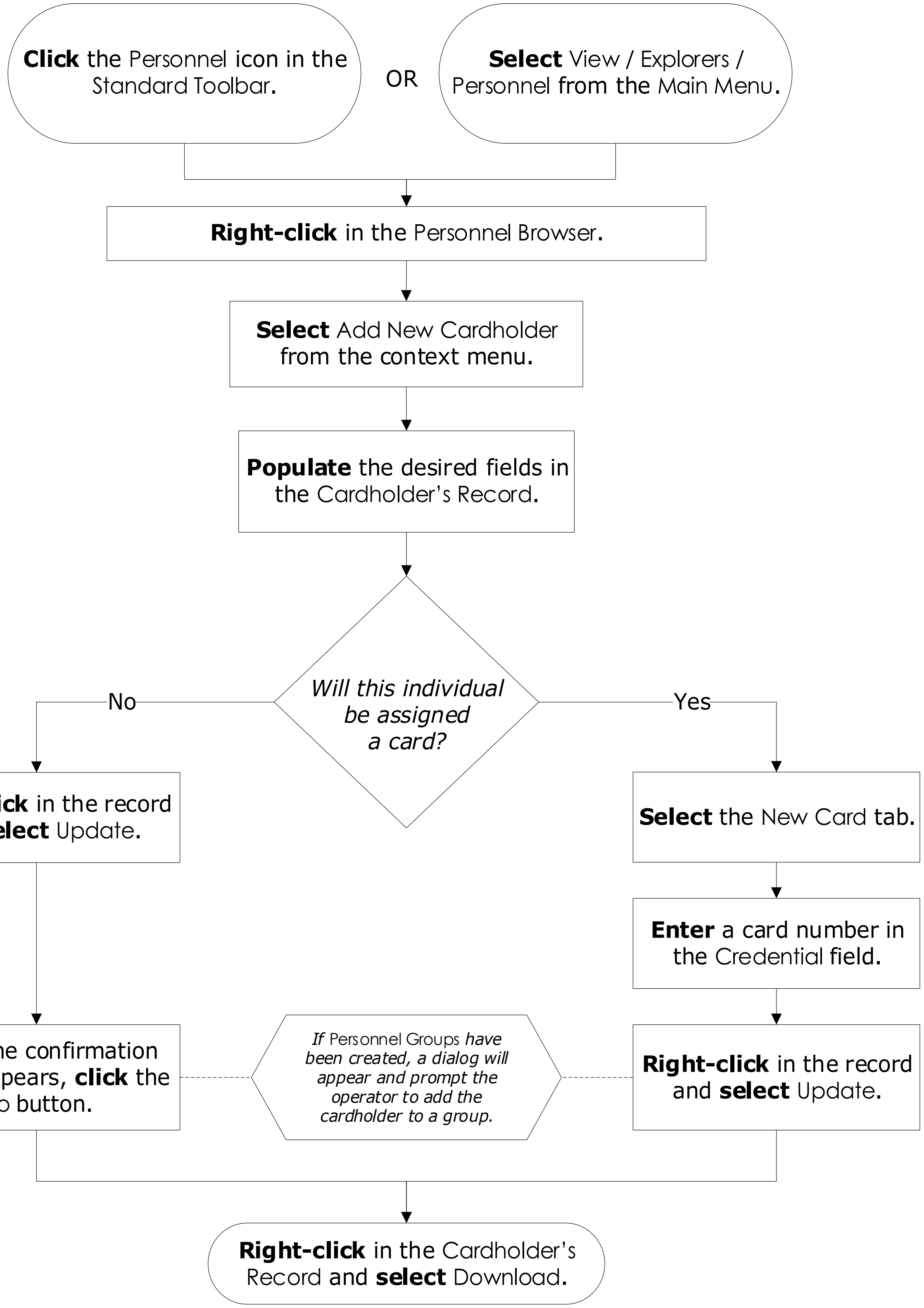
Click OK.

Download the Access Level.

***Right-click** in the Access Levels Browser and **select** Download from the context menu.*

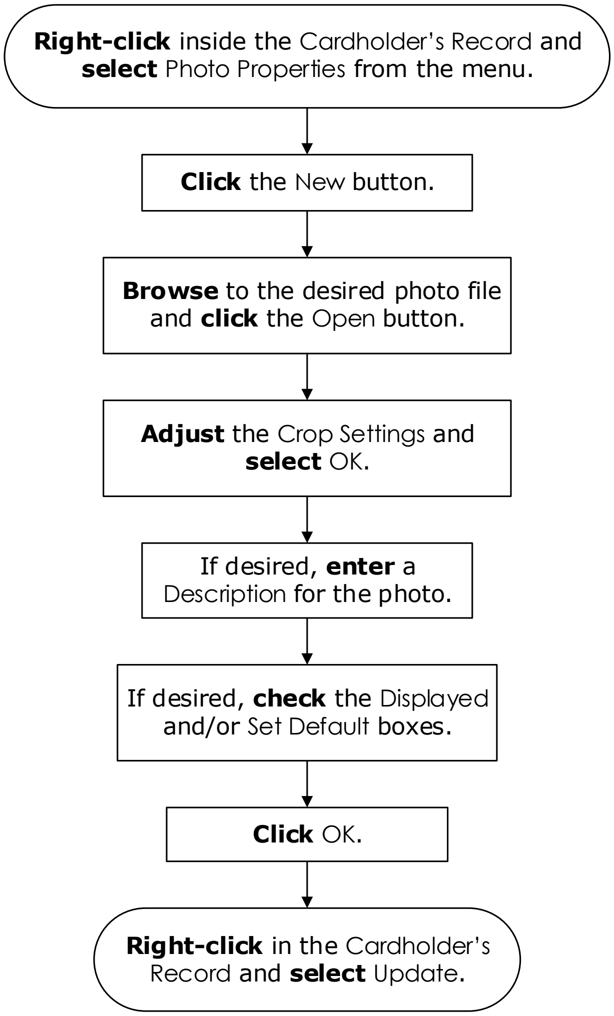
Adding a New Cardholder

See Chapter 7 for more information on Cardholders.


Click the Personnel icon in the Standard Toolbar.
OR
Select View / Explorers / Personnel from the Main Menu.
Right-click in the Personnel Browser.
Select Add New Cardholder from the context menu.
Populate the desired fields in the Cardholder's Record.
Will this individual be assigned a card?
No
Yes
Right-click in the record and **select** Update.
Select the New Card tab.
Enter a card number in the Credential field.
When the confirmation dialog appears, **click** the No button.
If Personnel Groups *have been created, a dialog will appear and prompt the operator to add the cardholder to a group.*
Right-click in the record and **select** Update.
Right-click in the Cardholder's Record and **select** Download.

Adding a Photo to a Cardholder’s Record

See Chapter 7 for more information on Cardholders.



Right-click inside the Cardholder’s Record and **select** Photo Properties from the menu.

Click the New button.

Browse to the desired photo file and **click** the Open button.

Adjust the Crop Settings and **select** OK.

If desired, **enter** a Description for the photo.

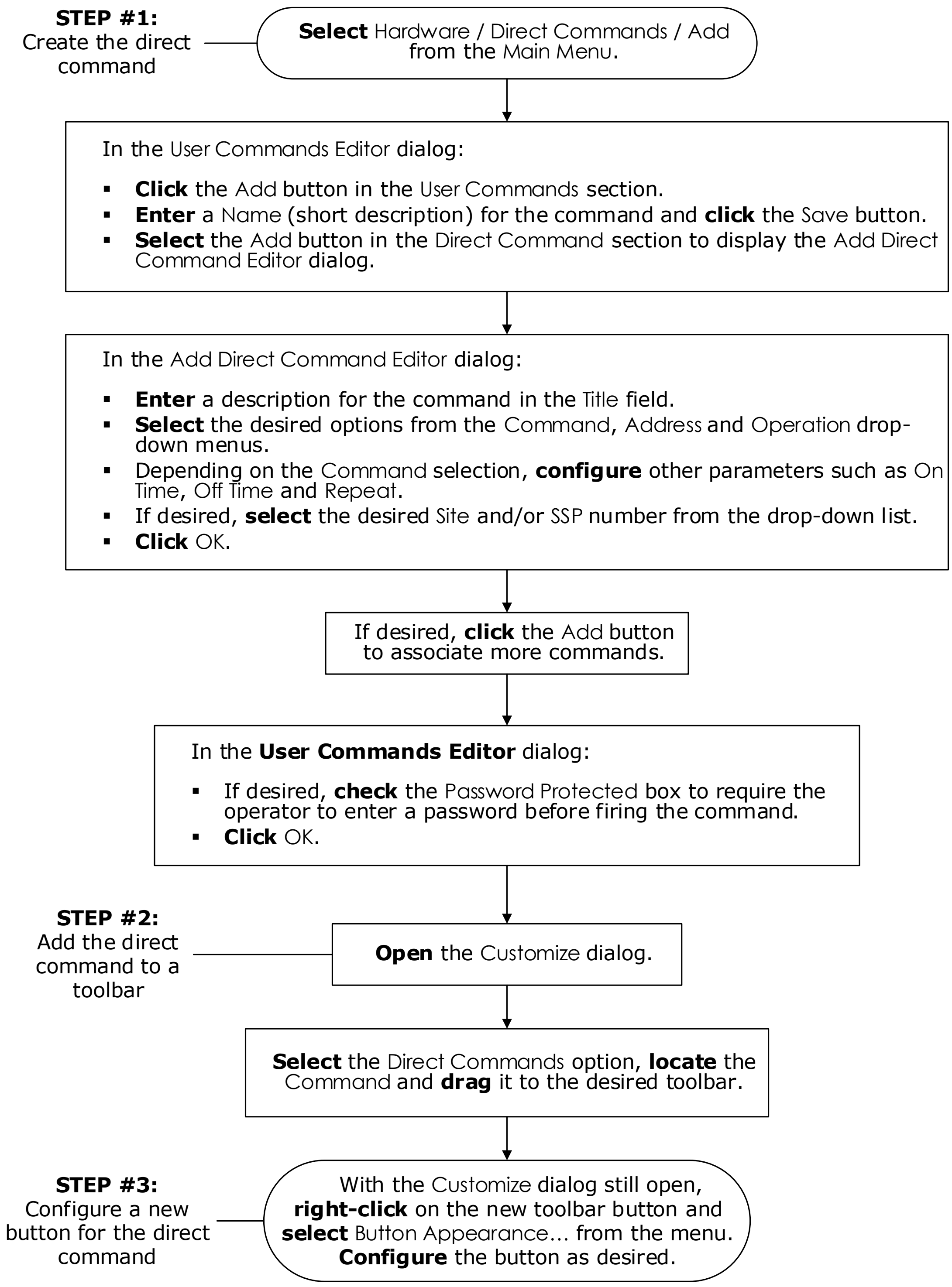
If desired, **check** the Displayed and/or Set Default boxes.

Click OK.

Right-click in the Cardholder’s Record and **select** Update.

Creating a Direct Command

See Chapter 8 for more information on Hardware



STEP #1:
Create the direct command

Select Hardware / Direct Commands / Add from the Main Menu.

In the User Commands Editor dialog:

- **Click** the Add button in the User Commands section.
- **Enter** a Name (short description) for the command and **click** the Save button.
- **Select** the Add button in the Direct Command section to display the Add Direct Command Editor dialog.

In the Add Direct Command Editor dialog:

- **Enter** a description for the command in the Title field.
- **Select** the desired options from the Command, Address and Operation drop-down menus.
- Depending on the Command selection, **configure** other parameters such as On Time, Off Time and Repeat.
- If desired, **select** the desired Site and/or SSP number from the drop-down list.
- **Click** OK.

If desired, **click** the Add button to associate more commands.

In the **User Commands Editor** dialog:

- If desired, **check** the Password Protected box to require the operator to enter a password before firing the command.
- **Click** OK.

STEP #2:
Add the direct command to a toolbar

Open the Customize dialog.

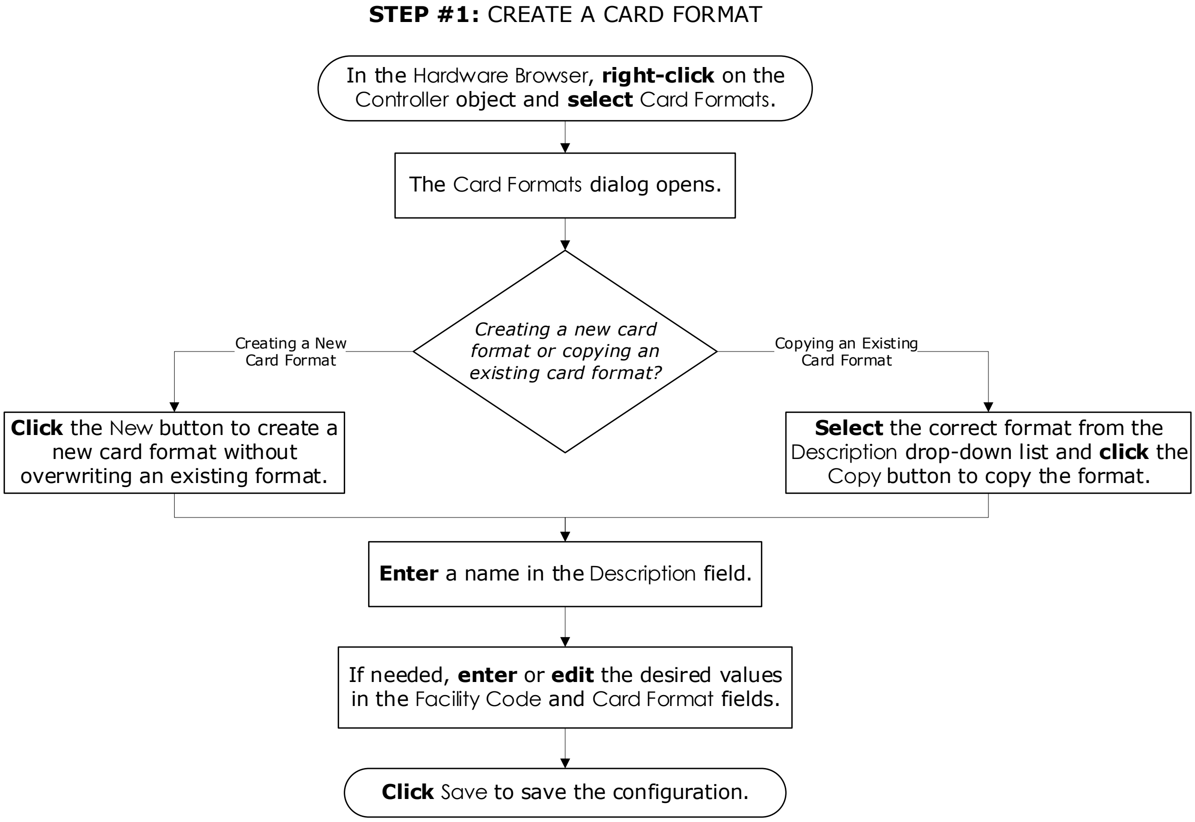
Select the Direct Commands option, **locate** the Command and **drag** it to the desired toolbar.

STEP #3:
Configure a new button for the direct command

With the Customize dialog still open, **right-click** on the new toolbar button and **select** Button Appearance... from the menu. **Configure** the button as desired.

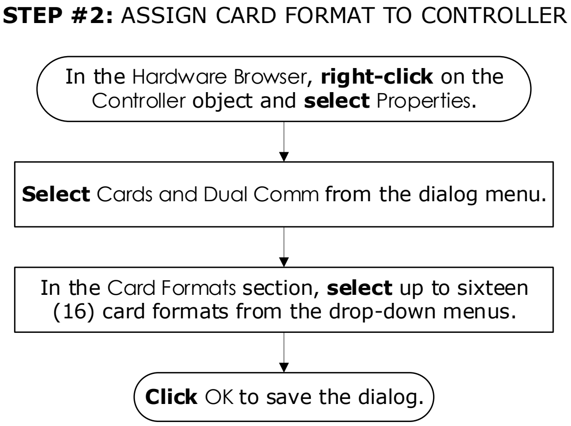
Configuring Card Formats

See Chapter 8 for more information on Hardware.



STEP #1: CREATE A CARD FORMAT
In the Hardware Browser, **right-click** on the Controller object and **select** Card Formats.
The Card Formats dialog opens.
Creating a new card format or copying an existing card format?
Creating a New Card Format
Copying an Existing Card Format
Click the New button to create a new card format without overwriting an existing format.
Select the correct format from the Description drop-down list and **click** the Copy button to copy the format.
Enter a name in the Description field.
If needed, **enter** or **edit** the desired values in the Facility Code and Card Format fields.
Click Save to save the configuration.

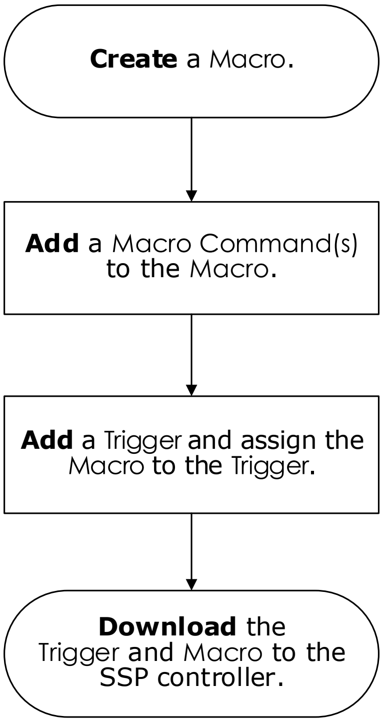
****



STEP #2: ASSIGN CARD FORMAT TO CONTROLLER
In the Hardware Browser, **right-click** on the Controller object and **select** Properties.
Select Cards and Dual Comm from the dialog menu.
In the Card Formats section, **select** up to sixteen (16) card formats from the drop-down menus.
Click OK to save the dialog.

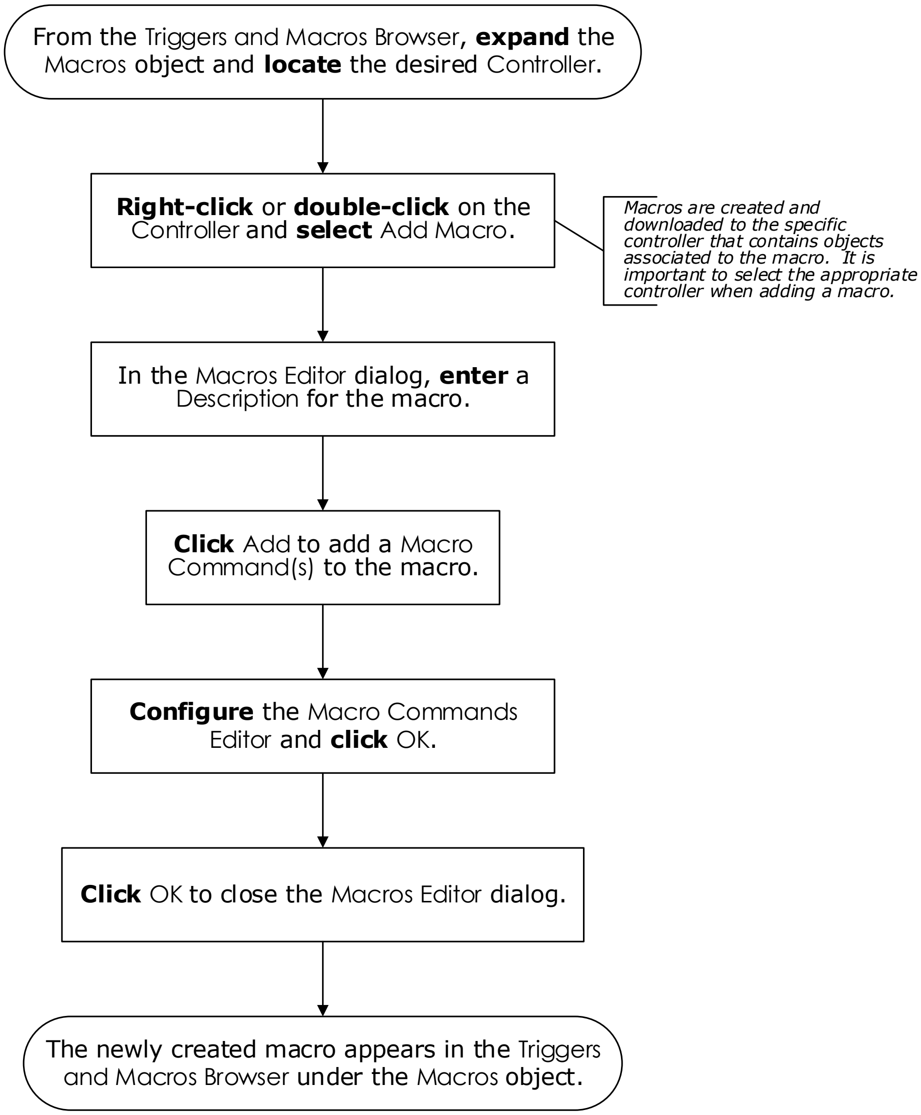
Basic Trigger and Macro Process

See Chapter 10 for more information on Triggers & Macros.


Create a Macro.
Add a Macro Command(s) to the Macro.
Add a Trigger and assign the Macro to the Trigger.
Download the Trigger and Macro to the SSP controller.

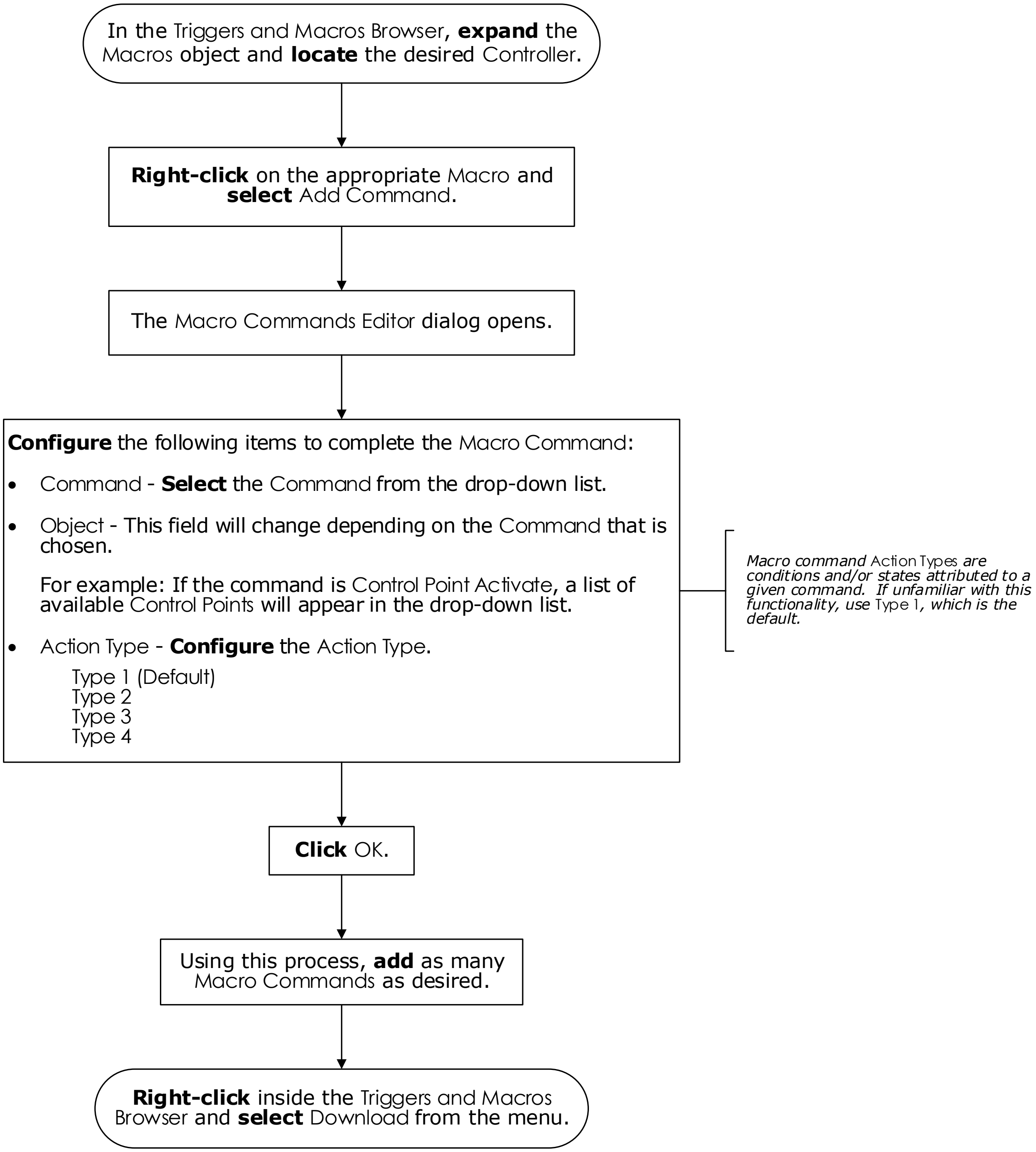
Creating a Macro

See Chapter 10 for more information on Triggers & Macros.


From the Triggers and Macros Browser, **expand** the Macros object and **locate** the desired Controller.
Right-click or **double-click** on the Controller and **select** Add Macro.
Macros are created and downloaded to the specific controller that contains objects associated to the macro. It is important to select the appropriate controller when adding a macro.
In the Macros Editor dialog, **enter** a Description for the macro.
Click Add to add a Macro Command(s) to the macro.
Configure the Macro Commands Editor and **click** OK.
Click OK to close the Macros Editor dialog.
The newly created macro appears in the Triggers and Macros Browser under the Macros object.

Adding a Macro Command

See Chapter 10 for more information on Triggers & Macros.



In the Triggers and Macros Browser, **expand** the Macros object and **locate** the desired Controller.

Right-click on the appropriate Macro and **select** Add Command.

The Macro Commands Editor dialog opens.

Configure the following items to complete the Macro Command:

- Command - **Select** the Command from the drop-down list.
- Object - This field will change depending on the Command that is chosen.

  For example: If the command is Control Point Activate, a list of available Control Points will appear in the drop-down list.
- Action Type - **Configure** the Action Type.

  Type 1 (Default)
  Type 2
  Type 3
  Type 4

Macro command Action Types are conditions and/or states attributed to a given command. If unfamiliar with this functionality, use Type 1, which is the default.

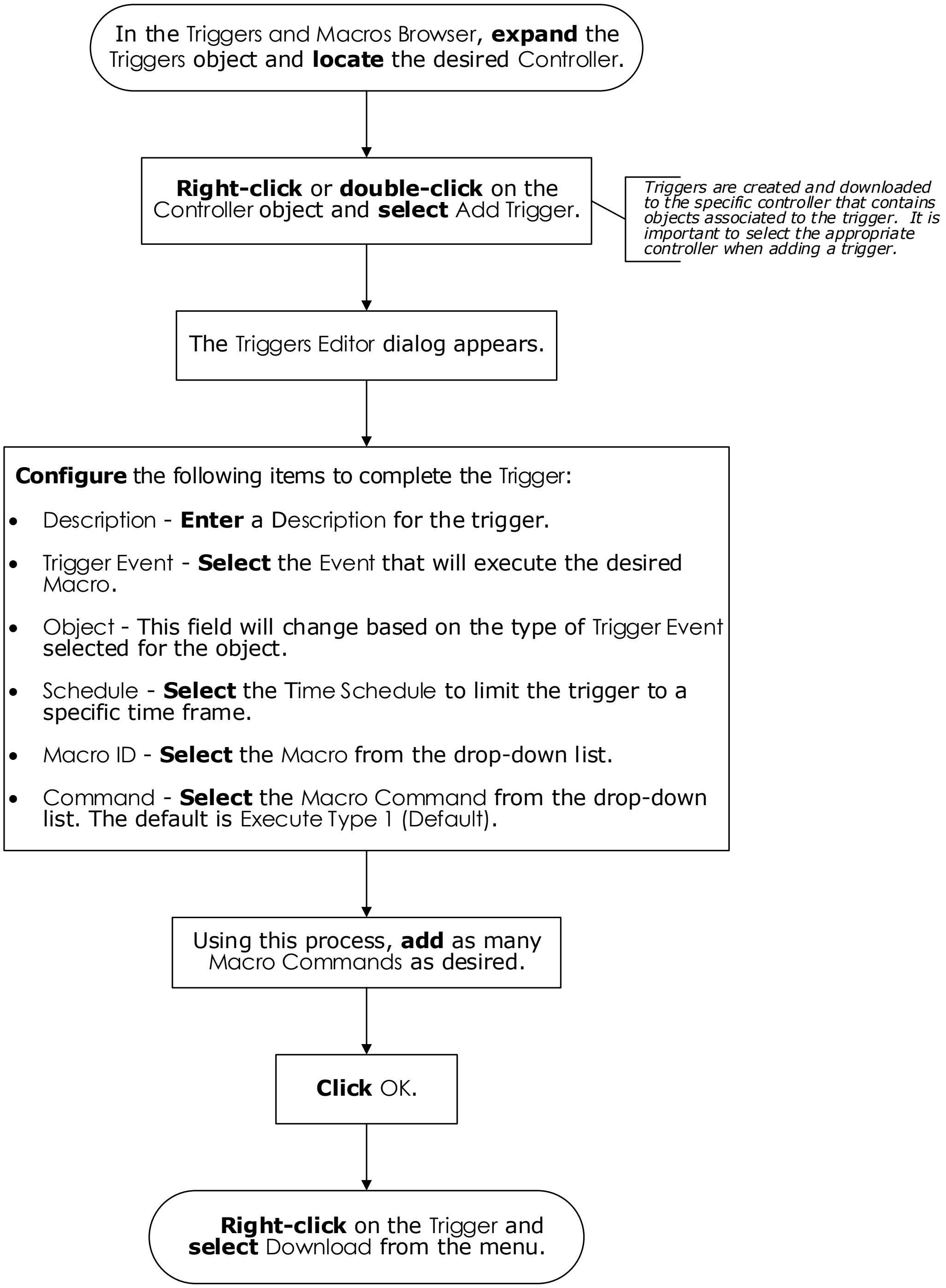
Click OK.

Using this process, **add** as many Macro Commands as desired.

Right-click inside the Triggers and Macros Browser and **select** Download from the menu.

Adding a Trigger

See Chapter 10 for more information on Triggers & Macros.



In the Triggers and Macros Browser, **expand** the Triggers object and **locate** the desired Controller.

Right-click or **double-click** on the Controller object and **select** Add Trigger.

Triggers are created and downloaded to the specific controller that contains objects associated to the trigger. It is important to select the appropriate controller when adding a trigger.

The Triggers Editor dialog appears.

Configure the following items to complete the Trigger:

- Description - **Enter** a Description for the trigger.
- Trigger Event - **Select** the Event that will execute the desired Macro.
- Object - This field will change based on the type of Trigger Event selected for the object.
- Schedule - **Select** the Time Schedule to limit the trigger to a specific time frame.
- Macro ID - **Select** the Macro from the drop-down list.
- Command - **Select** the Macro Command from the drop-down list. The default is Execute Type 1 (Default).

Using this process, **add** as many Macro Commands as desired.

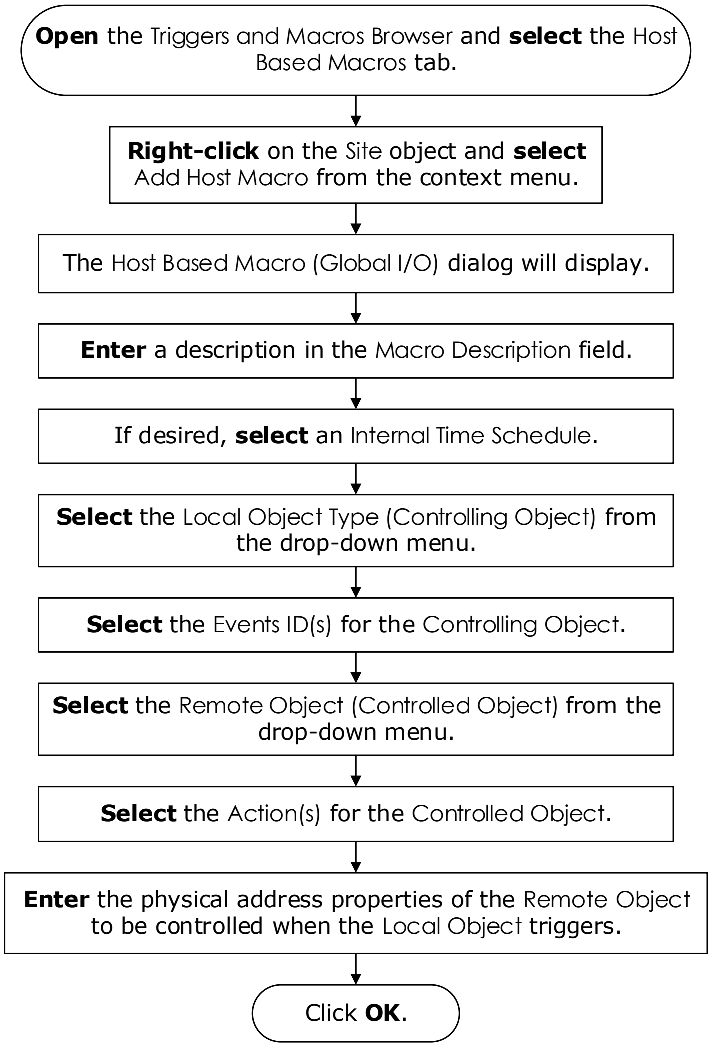
Click OK.

Right-click on the Trigger and **select** Download from the menu.

Configuring Host Based Macros

See Chapter 10 for more information on Triggers & Macros.

STEP #1: Select the macro object and configure object relationships.



Open the Triggers and Macros Browser and **select** the Host Based Macros tab.

Right-click on the Site object and **select** Add Host Macro from the context menu.

The Host Based Macro (Global I/O) dialog will display.

Enter a description in the Macro Description field.

If desired, **select** an Internal Time Schedule.

Select the Local Object Type (Controlling Object) from the drop-down menu.

Select the Events ID(s) for the Controlling Object.

Select the Remote Object (Controlled Object) from the drop-down menu.

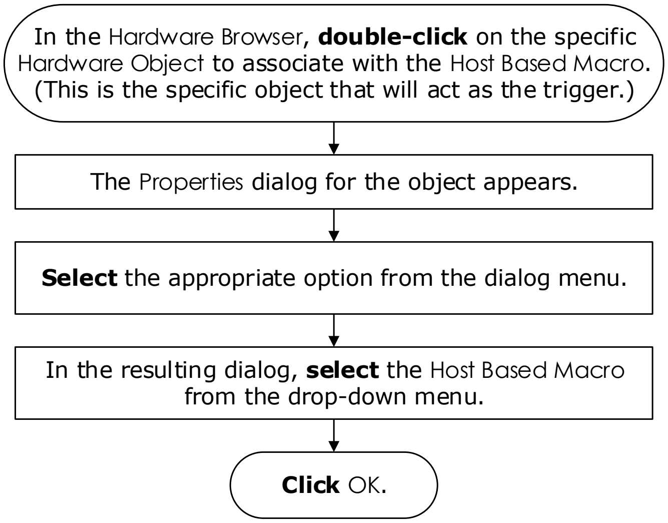
Select the Action(s) for the Controlled Object.

Enter the physical address properties of the Remote Object to be controlled when the Local Object triggers.

Click **OK**.

****

STEP #2: Select the trigger object and assign the macro.



In the Hardware Browser, **double-click** on the specific Hardware Object to associate with the Host Based Macro. (This is the specific object that will act as the trigger.)

The Properties dialog for the object appears.

Select the appropriate option from the dialog menu.

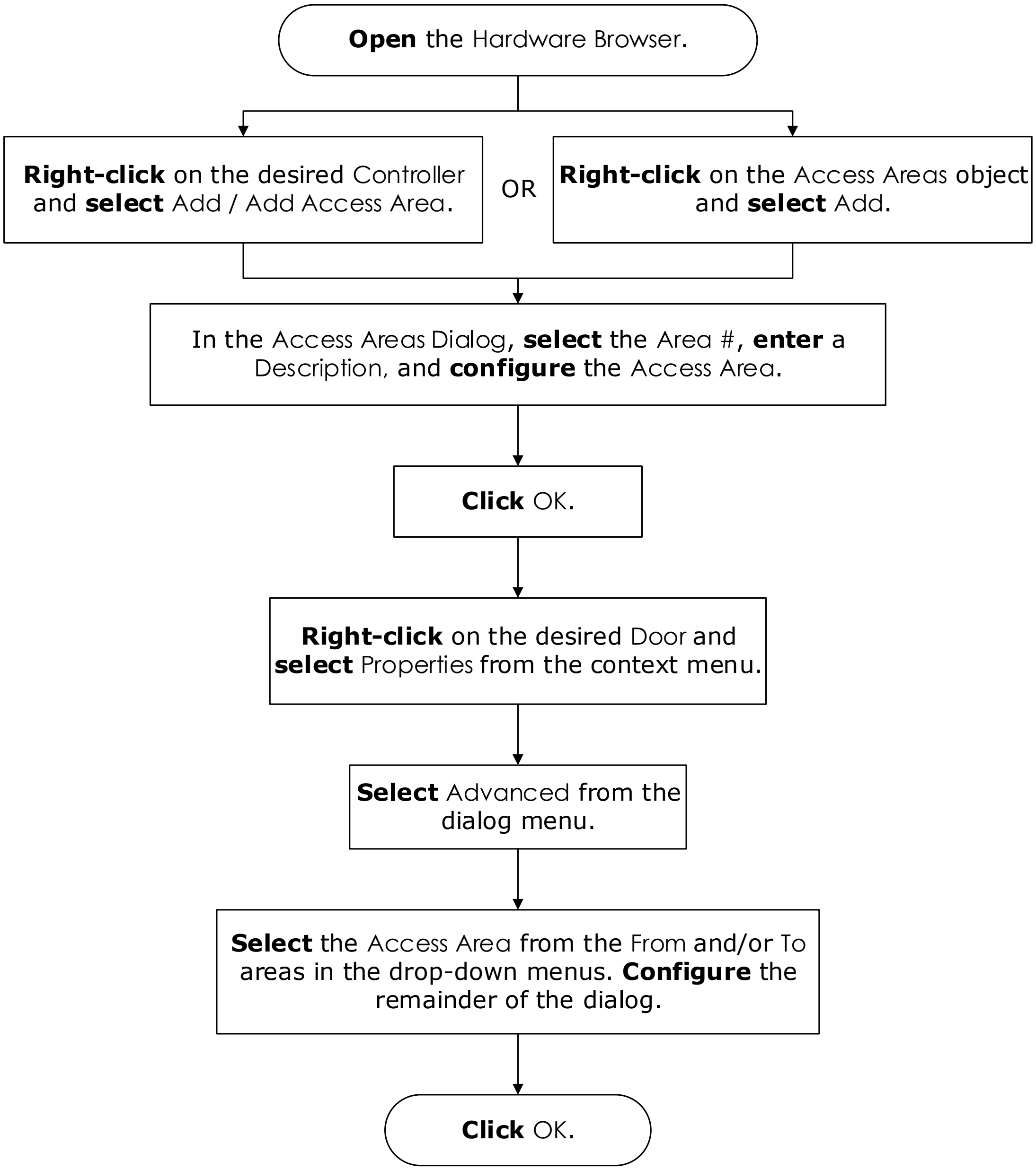
In the resulting dialog, **select** the Host Based Macro from the drop-down menu.

Click OK.

NOTES:

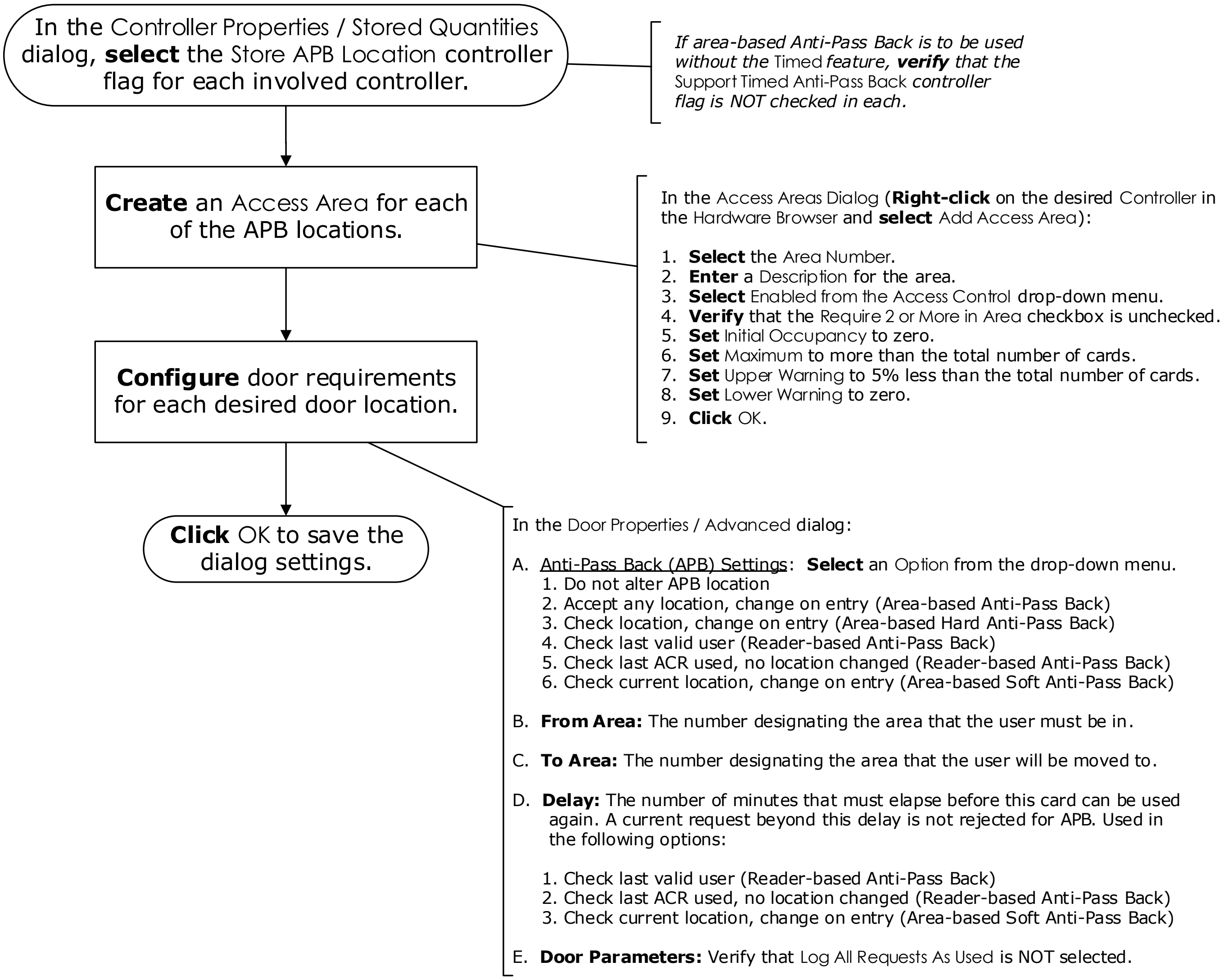
Create and Configure an Access Area

See Chapter 11 for more information on Access Areas and Anti-Pass Back.


Open the Hardware Browser.
Right-click on the desired Controller and **select** Add / Add Access Area.
OR
Right-click on the Access Areas object and **select** Add.
In the Access Areas Dialog, **select** the Area #, **enter** a Description, and **configure** the Access Area.
Click OK.
Right-click on the desired Door and **select** Properties from the context menu.
Select Advanced from the dialog menu.
Select the Access Area from the From and/or To areas in the drop-down menus. **Configure** the remainder of the dialog.
Click OK.

Configuring the System for Anti-Pass Back (APB)

See Chapter 11 for more information on Access Areas and Anti-Pass Back.



In the Controller Properties / Stored Quantities dialog, **select** the Store APB Location controller flag for each involved controller.

If area-based Anti-Pass Back is to be used without the Timed *feature,* ***verify*** *that the* Support Timed Anti-Pass Back *controller flag is NOT checked in each.*

Create an Access Area for each of the APB locations.

In the Access Areas Dialog (**Right-click** on the desired Controller in the Hardware Browser and **select** Add Access Area):

1. **Select** the Area Number.
2. **Enter** a Description for the area.
3. **Select** Enabled from the Access Control drop-down menu.
4. **Verify** that the Require 2 or More in Area checkbox is unchecked.
5. **Set** Initial Occupancy to zero.
6. **Set** Maximum to more than the total number of cards.
7. **Set** Upper Warning to 5% less than the total number of cards.
8. **Set** Lower Warning to zero.
9. **Click** OK.

Configure door requirements for each desired door location.

In the Door Properties / Advanced dialog:

A. Anti-Pass Back (APB) Settings: **Select** an Option from the drop-down menu.
   1. Do not alter APB location
   2. Accept any location, change on entry (Area-based Anti-Pass Back)
   3. Check location, change on entry (Area-based Hard Anti-Pass Back)
   4. Check last valid user (Reader-based Anti-Pass Back)
   5. Check last ACR used, no location changed (Reader-based Anti-Pass Back)
   6. Check current location, change on entry (Area-based Soft Anti-Pass Back)

B. **From Area:** The number designating the area that the user must be in.

C. **To Area:** The number designating the area that the user will be moved to.

D. **Delay:** The number of minutes that must elapse before this card can be used again. A current request beyond this delay is not rejected for APB. Used in the following options:

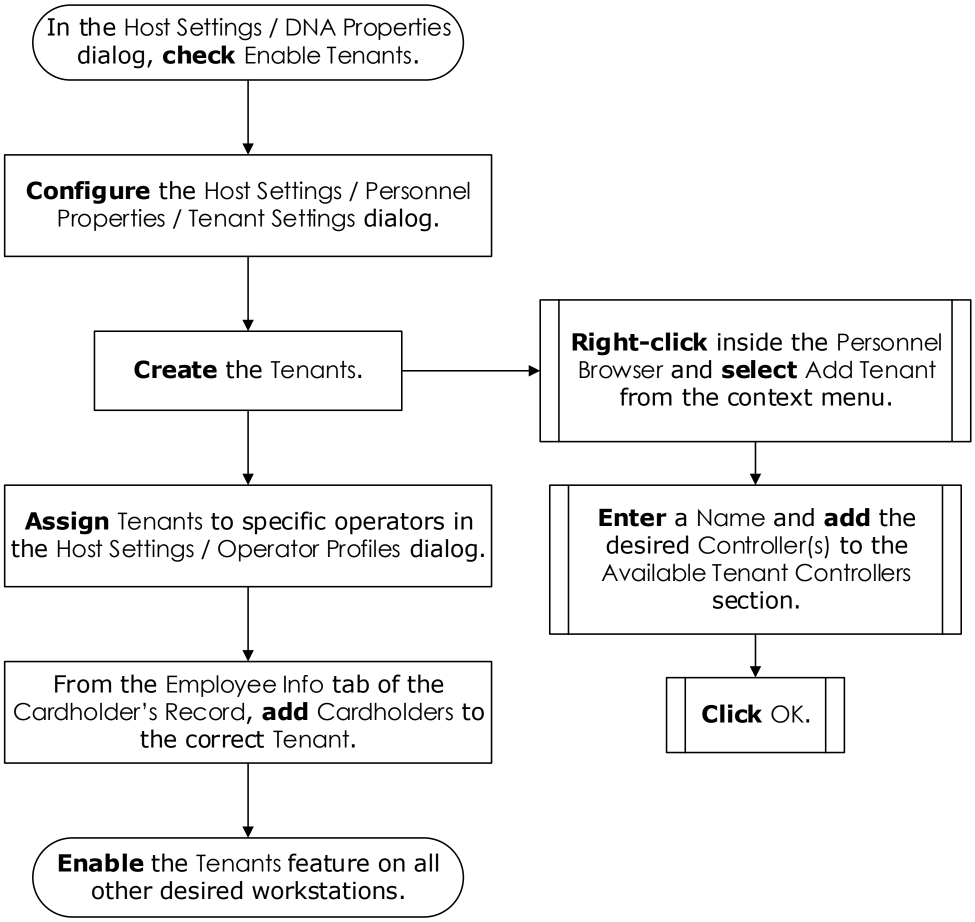
   1. Check last valid user (Reader-based Anti-Pass Back)
   2. Check last ACR used, no location changed (Reader-based Anti-Pass Back)
   3. Check current location, change on entry (Area-based Soft Anti-Pass Back)

E. **Door Parameters:** Verify that Log All Requests As Used is NOT selected.

Click OK to save the dialog settings.

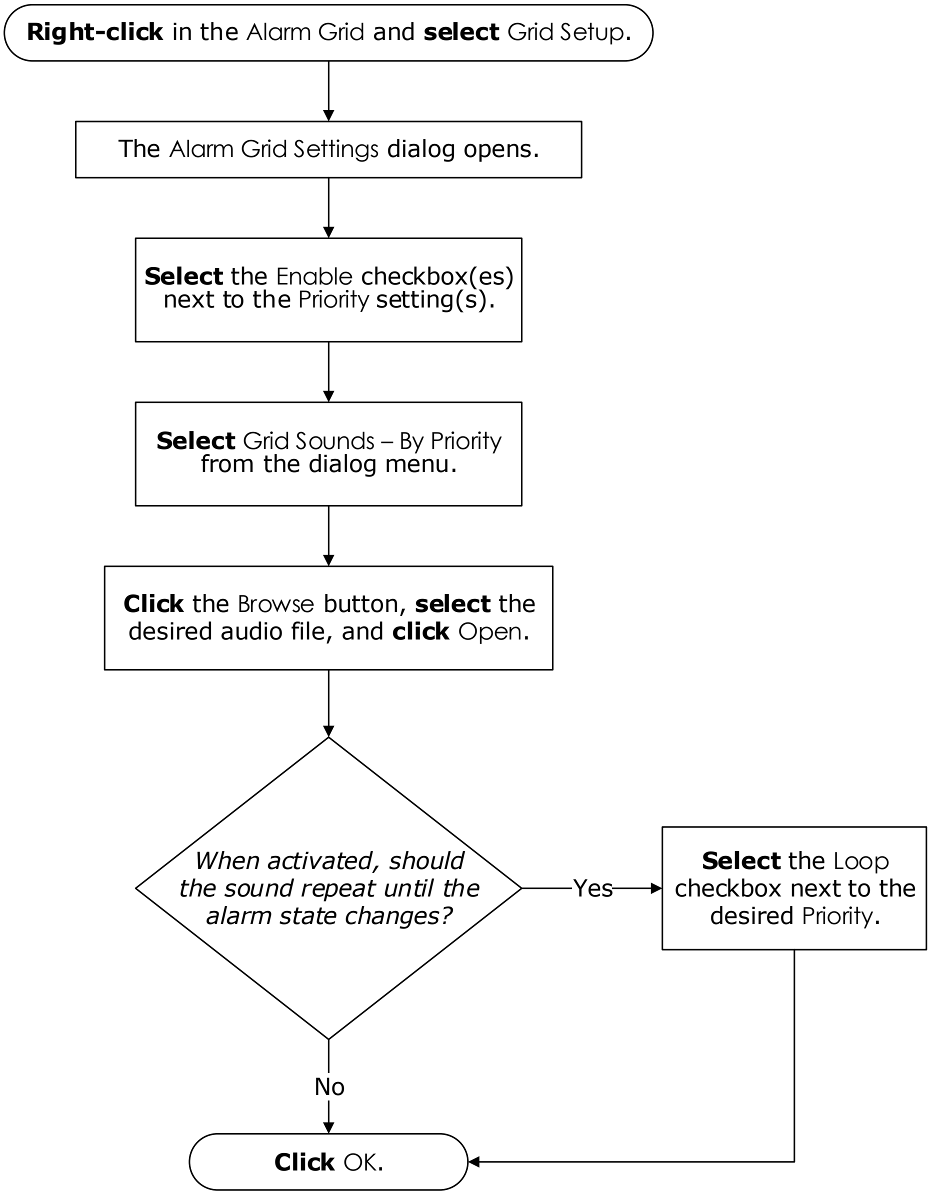
Configuring Tenants

See Chapter 13 for more information on Tenants.


In the Host Settings / DNA Properties dialog, **check** Enable Tenants.
Configure the Host Settings / Personnel Properties / Tenant Settings dialog.
Create the Tenants.
Right-click inside the Personnel Browser and **select** Add Tenant from the context menu.
Enter a Name and **add** the desired Controller(s) to the Available Tenant Controllers section.
Click OK.
Assign Tenants to specific operators in the Host Settings / Operator Profiles dialog.
From the Employee Info tab of the Cardholder's Record, **add** Cardholders to the correct Tenant.
Enable the Tenants feature on all other desired workstations.

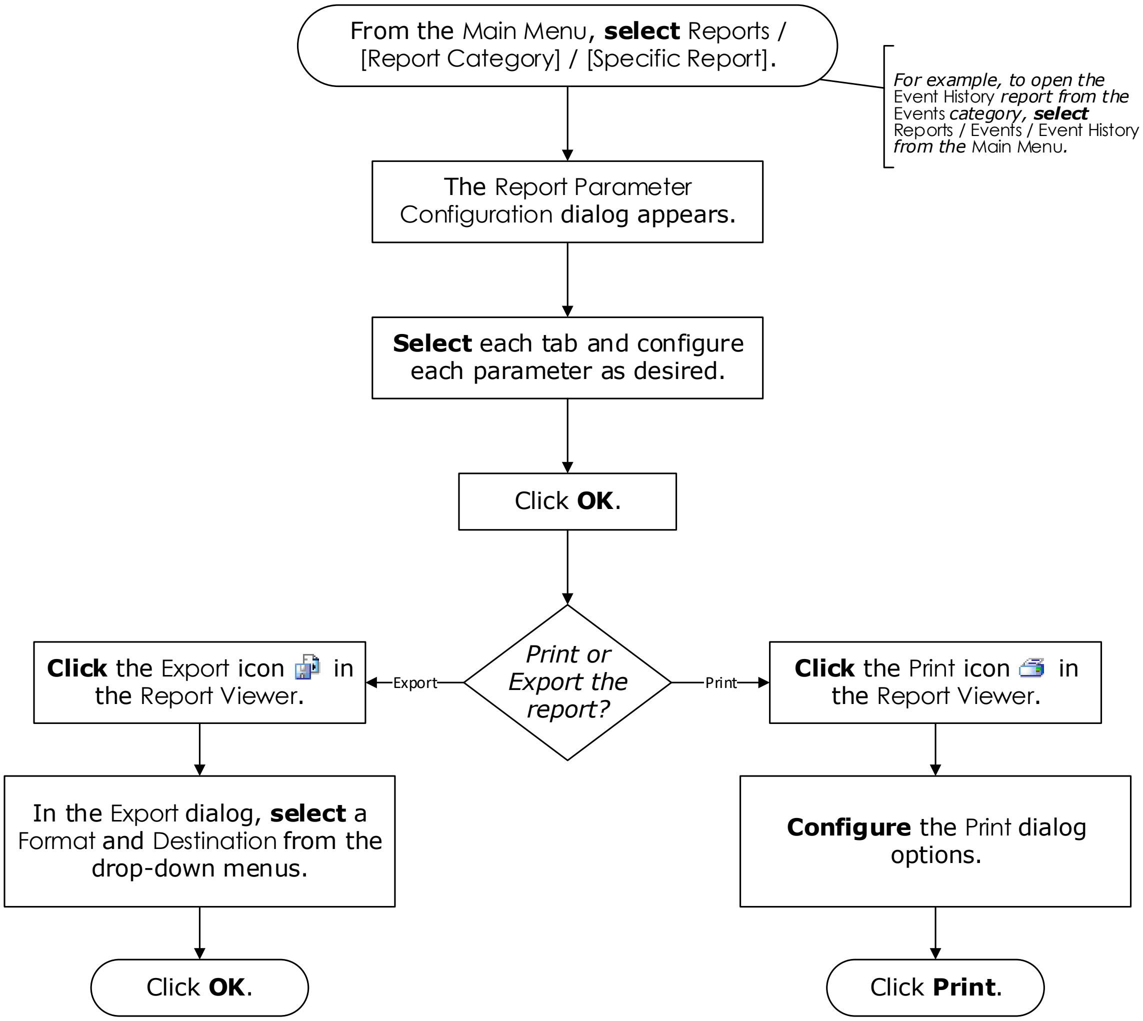
Assigning a Sound to an Alarm Priority

See Chapter 14 for more information on Events and Alarms.


Right-click in the Alarm Grid and **select** Grid Setup.
The Alarm Grid Settings dialog opens.
Select the Enable checkbox(es) next to the Priority setting(s).
Select Grid Sounds – By Priority from the dialog menu.
Click the Browse button, **select** the desired audio file, and **click** Open.
When activated, should the sound repeat until the alarm state changes?
Yes
Select the Loop checkbox next to the desired Priority.
No
Click OK.

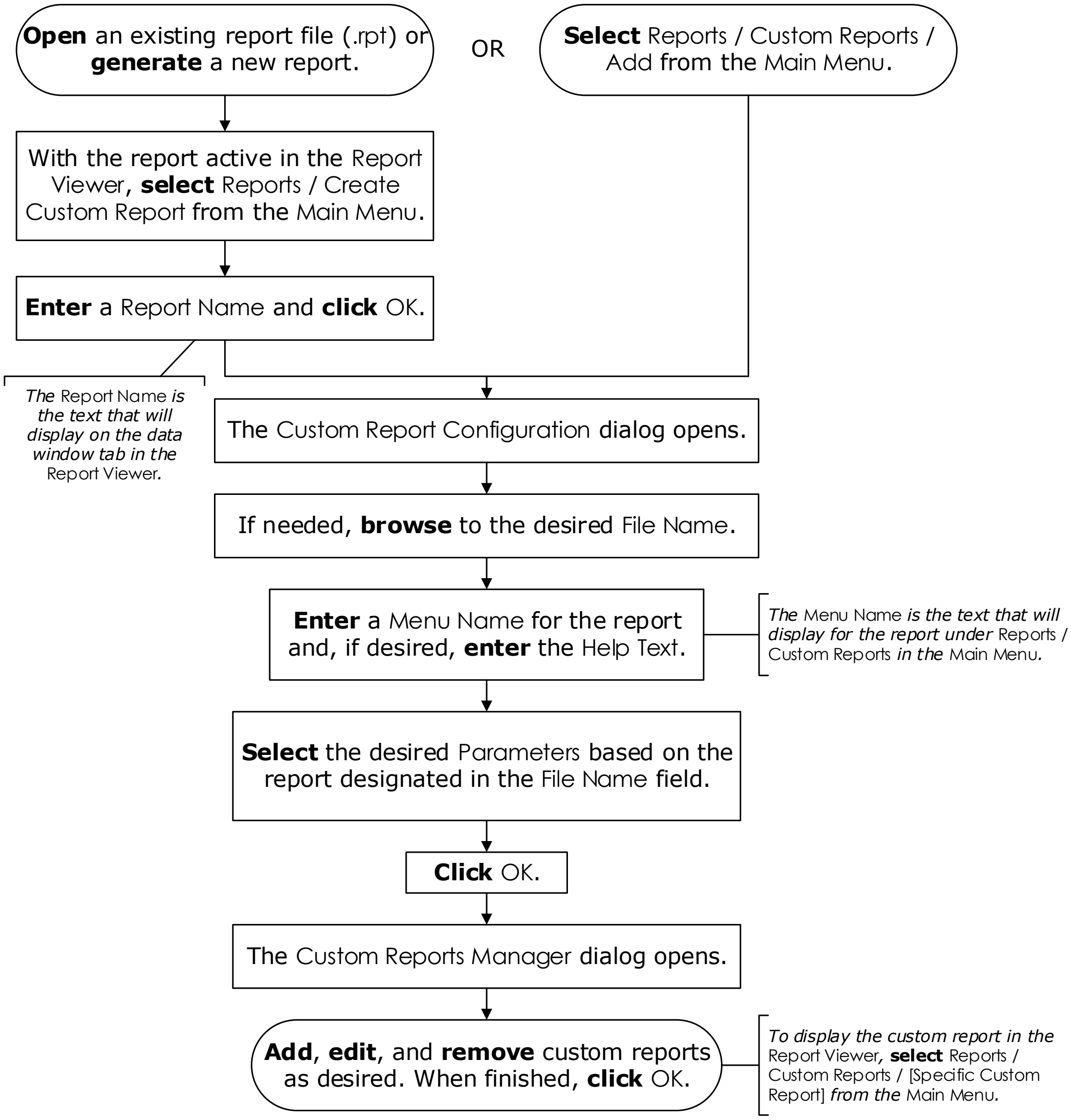
Configuring a Report

See Chapter 17 for more information on Reports.


From the Main Menu, **select** Reports / [Report Category] / [Specific Report].
For example, to open the Event History *report from the* Events *category,* ***select*** Reports / Events / Event History *from the* Main Menu.
The Report Parameter Configuration dialog appears.
Select each tab and configure each parameter as desired.
Click **OK**.
Print or Export the report?
Export
Print
Click the Export icon in the Report Viewer.
In the Export dialog, **select** a Format and Destination from the drop-down menus.
Click **OK**.
Click the Print icon in the Report Viewer.
Configure the Print dialog options.
Click **Print**.

Creating a Custom Report

See Chapter 17 for more information on Reports.



Open an existing report file (.rpt) or **generate** a new report.

OR

Select Reports / Custom Reports / Add from the Main Menu.

With the report active in the Report Viewer, **select** Reports / Create Custom Report from the Main Menu.

Enter a Report Name and **click** OK.

The Report Name *is the text that will display on the data window tab in the* Report Viewer*.*

The Custom Report Configuration dialog opens.

If needed, **browse** to the desired File Name.

Enter a Menu Name for the report and, if desired, **enter** the Help Text.

The Menu Name *is the text that will display for the report under* Reports / Custom Reports *in the* Main Menu*.*

Select the desired Parameters based on the report designated in the File Name field.

Click OK.

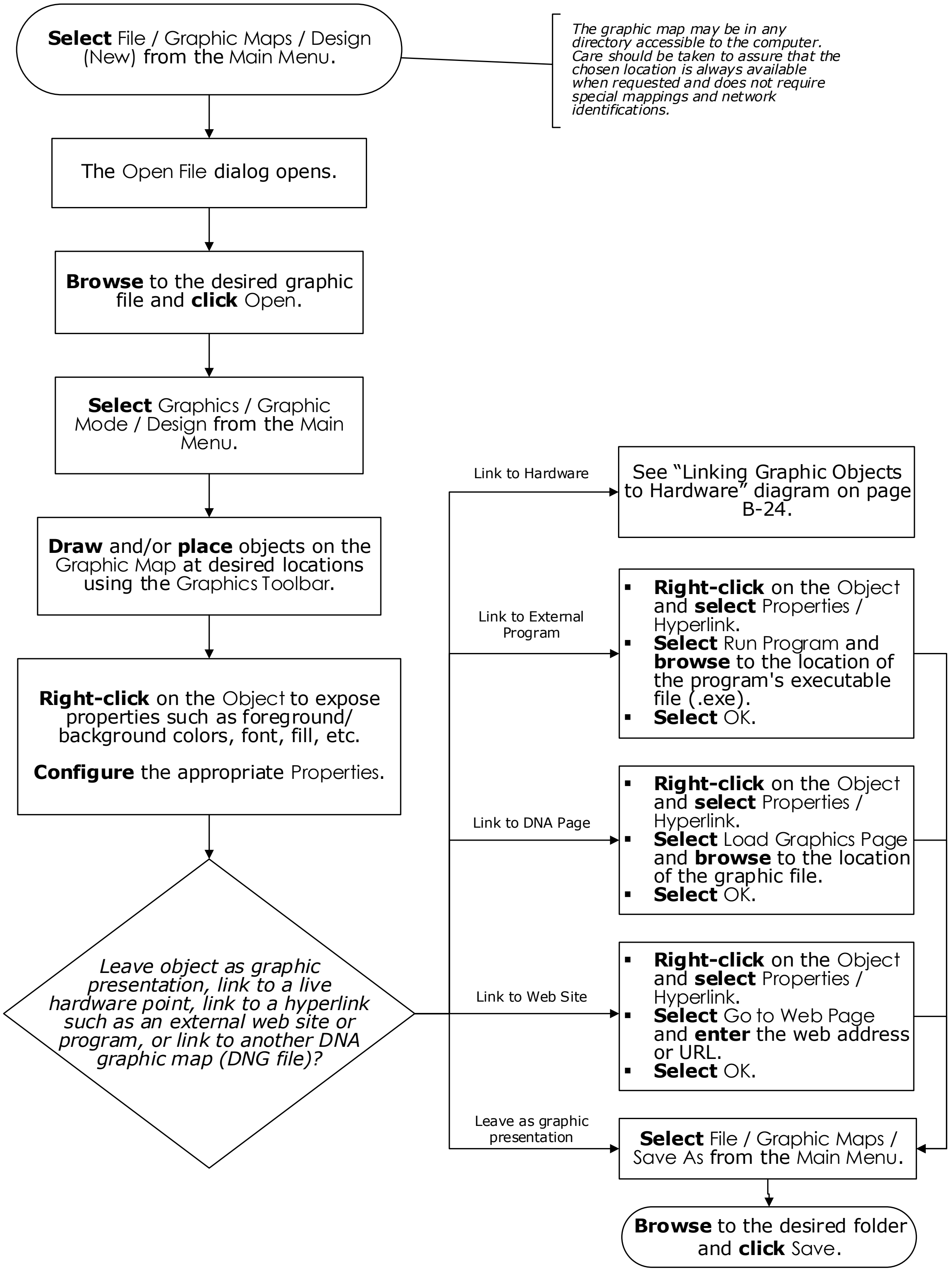
The Custom Reports Manager dialog opens.

Add, **edit**, and **remove** custom reports as desired. When finished, **click** OK.

To display the custom report in the Report Viewer*,* **select** Reports / Custom Reports / [Specific Custom Report] *from the* Main Menu*.*

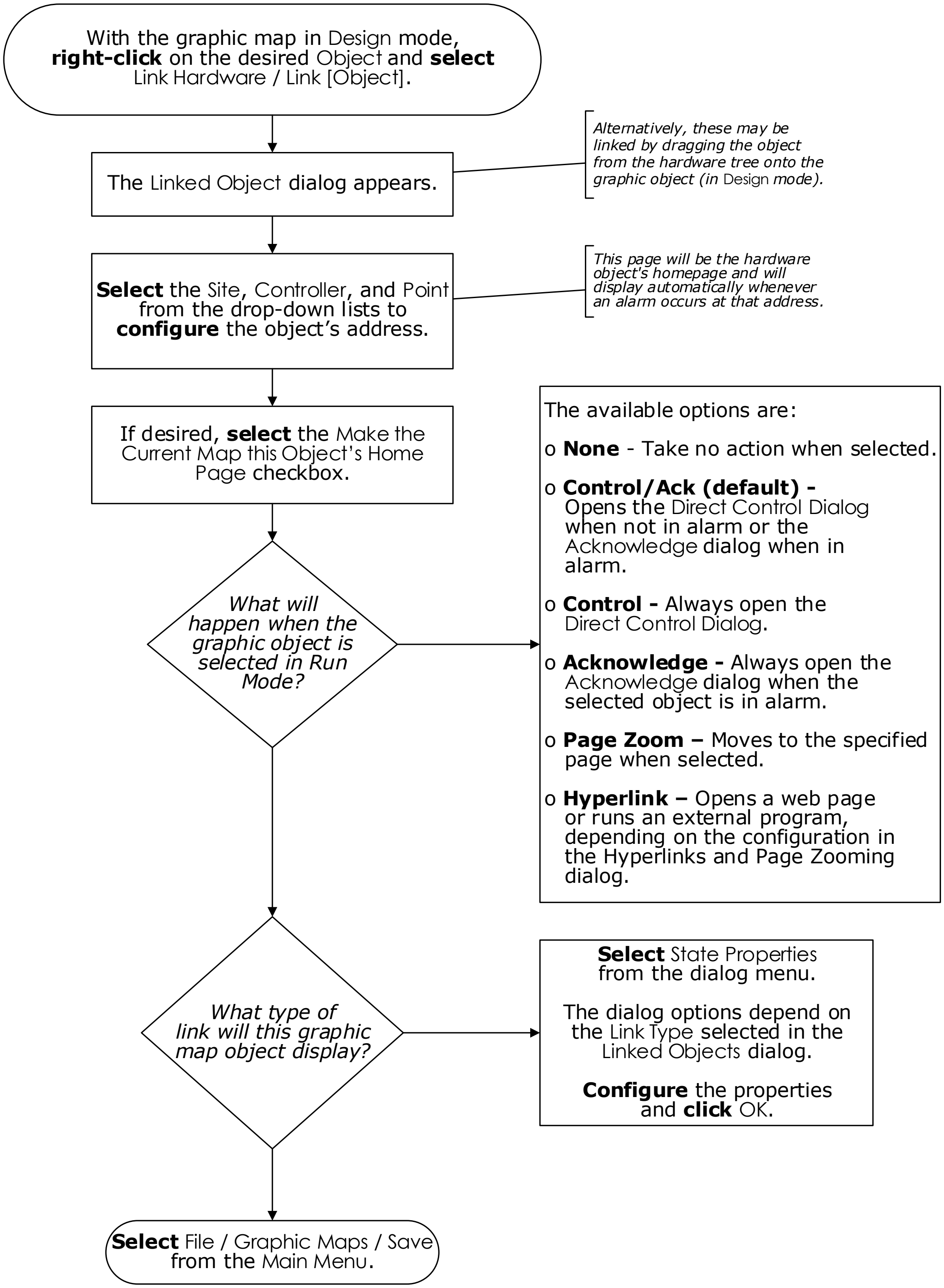
Creating Graphic Maps and Applying Graphic Objects

See Chapter 18 for more information on Graphic Maps.


Select File / Graphic Maps / Design (New) from the Main Menu.
The graphic map may be in any directory accessible to the computer. Care should be taken to assure that the chosen location is always available when requested and does not require special mappings and network identifications.
The Open File dialog opens.
Browse to the desired graphic file and click Open.
Select Graphics / Graphic Mode / Design from the Main Menu.
Draw and/or place objects on the Graphic Map at desired locations using the Graphics Toolbar.
Right-click on the Object to expose properties such as foreground/ background colors, font, fill, etc.
Configure the appropriate Properties.
Leave object as graphic presentation, link to a live hardware point, link to a hyperlink such as an external web site or program, or link to another DNA graphic map (DNG file)?
Link to Hardware
See "Linking Graphic Objects to Hardware" diagram on page B-24.
Link to External Program
Right-click on the Object and select Properties / Hyperlink.
Select Run Program and browse to the location of the program's executable file (.exe).
Select OK.
Link to DNA Page
Right-click on the Object and select Properties / Hyperlink.
Select Load Graphics Page and browse to the location of the graphic file.
Select OK.
Link to Web Site
Right-click on the Object and select Properties / Hyperlink.
Select Go to Web Page and enter the web address or URL.
Select OK.
Leave as graphic presentation
Select File / Graphic Maps / Save As from the Main Menu.
Browse to the desired folder and click Save.

Linking Graphic Objects to Hardware

See Chapter 18 for more information on Graphic Maps.



With the graphic map in Design mode, **right-click** on the desired Object and **select** Link Hardware / Link [Object].

The Linked Object dialog appears.

Alternatively, these may be linked by dragging the object from the hardware tree onto the graphic object (in Design mode).

Select the Site, Controller, and Point from the drop-down lists to **configure** the object's address.

This page will be the hardware object's homepage and will display automatically whenever an alarm occurs at that address.

If desired, **select** the Make the Current Map this Object's Home Page checkbox.

What will happen when the graphic object is selected in Run Mode?

The available options are:

o **None** - Take no action when selected.

o **Control/Ack (default) -** Opens the Direct Control Dialog when not in alarm or the Acknowledge dialog when in alarm.

o **Control -** Always open the Direct Control Dialog.

o **Acknowledge -** Always open the Acknowledge dialog when the selected object is in alarm.

o **Page Zoom –** Moves to the specified page when selected.

o **Hyperlink –** Opens a web page or runs an external program, depending on the configuration in the Hyperlinks and Page Zooming dialog.

What type of link will this graphic map object display?

Select State Properties from the dialog menu.

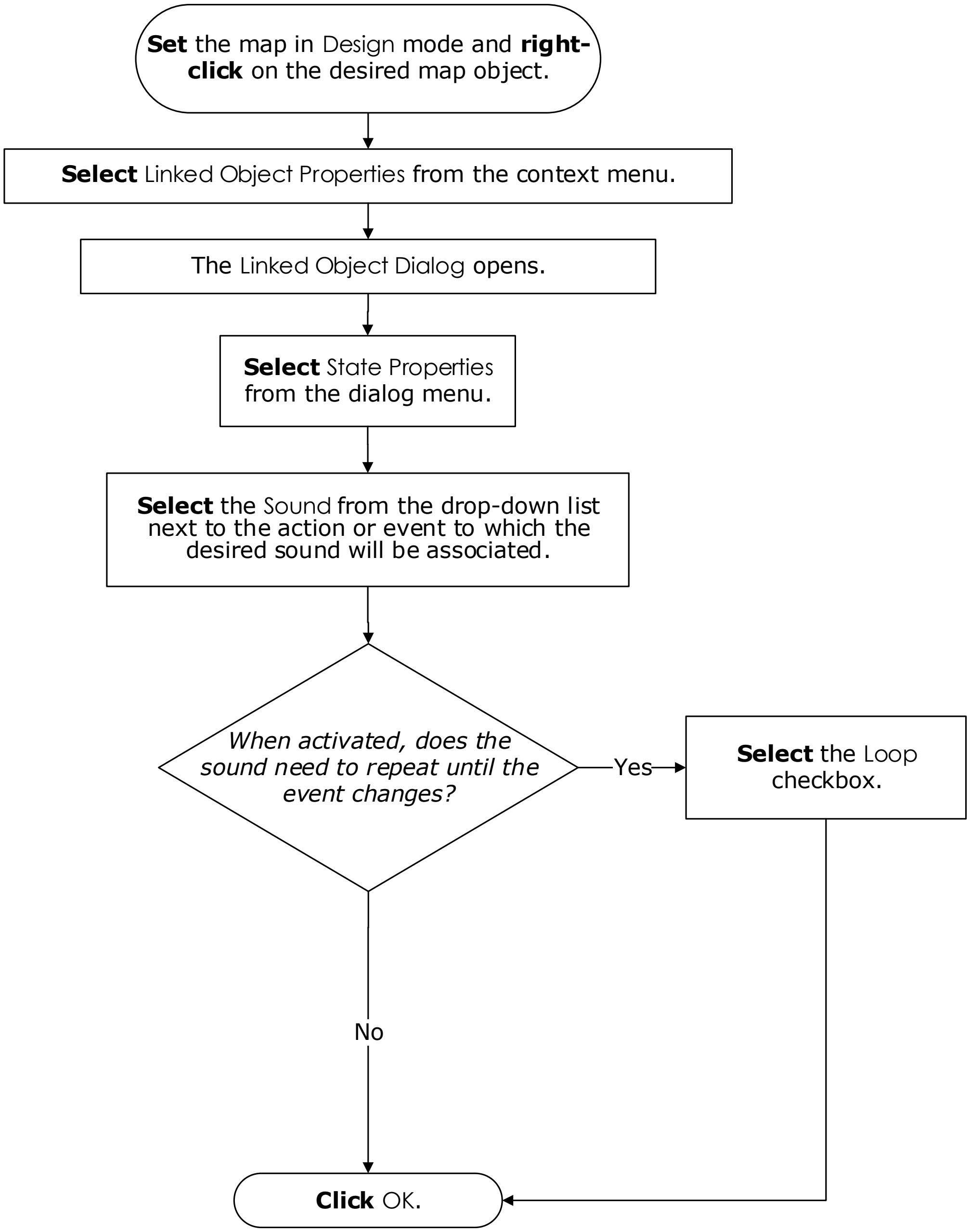
The dialog options depend on the Link Type selected in the Linked Objects dialog.

Configure the properties and **click** OK.

Select File / Graphic Maps / Save from the Main Menu.

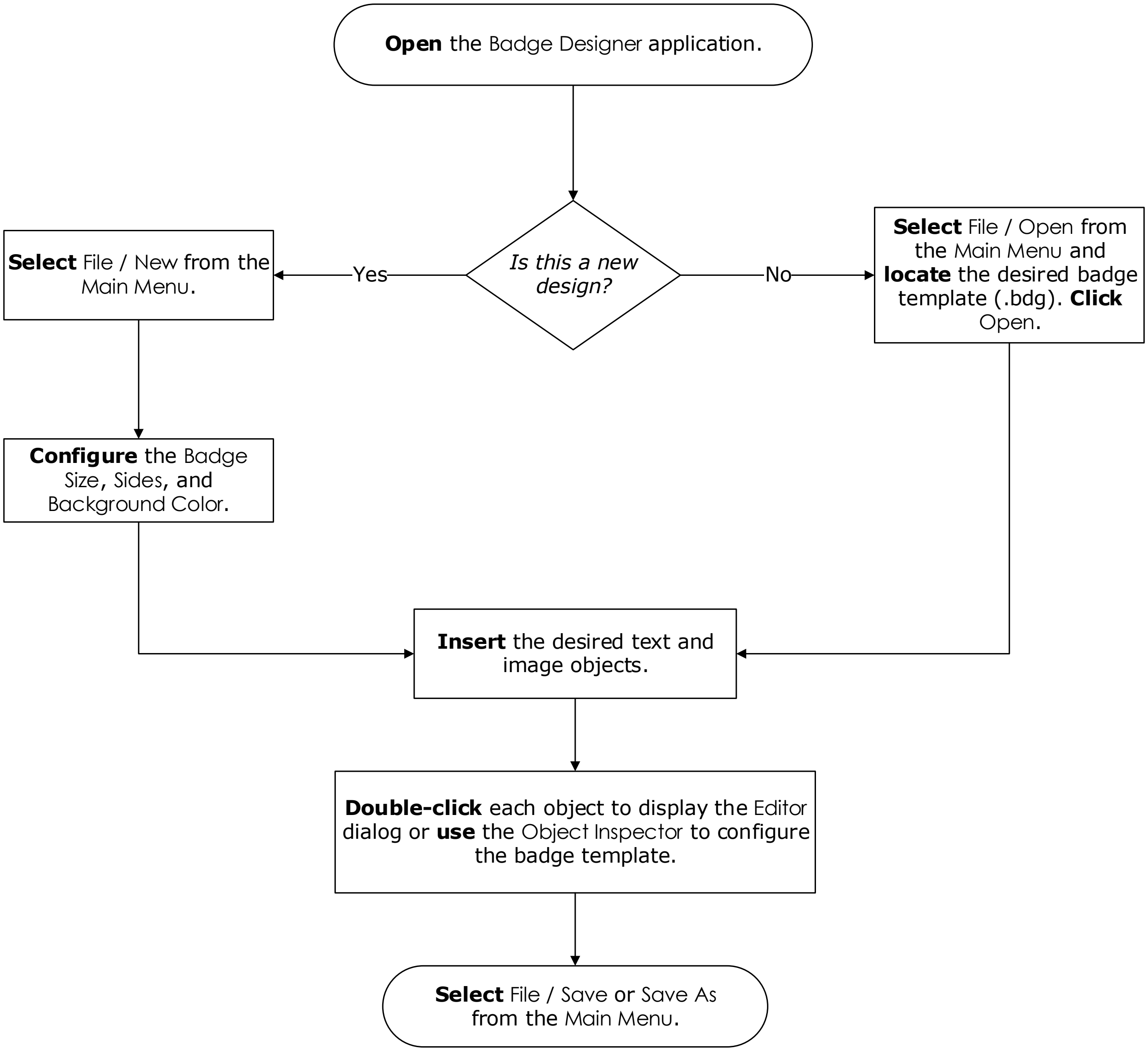
Assigning a Sound to a Graphic Map Object

See Chapter 18 for more information on Graphic Maps.


Set the map in Design mode and **right-click** on the desired map object.
Select Linked Object Properties from the context menu.
The Linked Object Dialog opens.
Select State Properties from the dialog menu.
Select the Sound from the drop-down list next to the action or event to which the desired sound will be associated.
When activated, does the sound need to repeat until the event changes?
Yes
Select the Loop checkbox.
No
Click OK.

Basic Badge Design Process

See Chapter 21 for more information on ID Badging.


Open the Badge Designer application.
Is this a new design?
Yes
No
Select File / New from the Main Menu.
Configure the Badge Size, Sides, and Background Color.
Select File / Open from the Main Menu and **locate** the desired badge template (.bdg). **Click** Open.
Insert the desired text and image objects.
Double-click each object to display the Editor dialog or **use** the Object Inspector to configure the badge template.
Select File / Save or Save As from the Main Menu.

Shortcut Keys C

Shortcut keys provide an easier and quicker method of navigating and using DNA Fusion. Shortcut keys are commonly used by selecting the Alt, Ctrl, and/or Shift keys in conjunction with a single letter or function key. Operators can also perform shortcuts designated by underlined letters in various DNA Fusion dialogs and menus.

The standard notation for a shortcut key includes a modifier key, a plus symbol, and a single character. For example, "ALT+S" instructs the operator to hold the Alt key and select the S key to perform the shortcut operation.

The table below includes additional space to add custom keyboard shortcuts. See page 2-9 for more information.

Operation	Shortcut Key
Access Level Browser	Shift+F7
Acknowledge Alarm	F5
Alarm Grid	F2
Clear Alarm	F8
Copy	Ctrl+C or Ctrl+Insert
Cut	Ctrl+X or Shift+Delete
DNA Homepage	Shift+F3
Events Grid	Shift+F2
Hardware Browser	F7
HTML Viewer	F3
IP Video 1	F12
IP Video 2	Shift+F12
IP Video 3	Ctrl+F12
IP Video 4	Alt+F12
New Journal Entry (for selected object)	F10
Paste	Ctrl+V or Shift+Insert
Personnel Browser	F9
Photo Recall 1	F11
Photo Recall 2	Shift+F11
Photo Recall 3	Ctrl+F11
Photo Recall 4	Alt+F11
Print	Ctrl+P
Save Settings (Active Document)	Ctrl+S
Select All Alarms	F4
View DNA Journal Entries	Shift+F10
Watch Window	Shift+F9

Operation	Shortcut Key

Replacement Text D

Replacement	Category	Description	Example
%ALARMCARD%	Event	Defines Alarm Card State	Alarm Card or NOT
%CARD%	Event	Card Number	256
%CARDFLAG%	Event	Card Flags	Watched, Alarm Card, etc.
%CARDTYPE%	Event	Card Type as Text	Visitor, Normal, etc.
%COMPANY%	Event	Cardholder’s Company	Open Options
%DATE%	Event	Event Date	2/24/2004
%DEPARTMENT%	Event	Cardholder’s Department	Marketing
%EVENTDATA%	Event	Event Data	MPG Controlled by Operator
%EVENTGROUP%	Event	Event Grouping	1, 2, 3, etc.
%FIRSTNAME%	Event	Cardholder’s First Name	John
%FLOOR%	Event	Elevator Floor	5
%FLOORNAME%	Event	Elevator Floor Description	Lobby
%LASTNAME%	Event	Cardholder’s Last Name	Smith
%LOCATION%	Event	Cardholder’s Location	Dallas
%MESSAGE%	Event	Event Message	Became Active
%MSG%	Event	Event Message Index	Index 18
%PERSON%	Event	Cardholder’s Name	Smith, John
%PERSONSITE%	Event	Cardholder’s Site	Dallas Office
%PERSONTYPE%	Event	Person Type as Text	Visitor, Normal, etc.
%PHOTO1%	Event	Cardholder’s Photo 1 Image	\\Server\Photos\JSmith1.jpg
%PHOTO2%	Event	Cardholder’s Photo 2 Image	\\Server\Photos\JSmith2.jpg
%PHOTO3%	Event	Cardholder’s Photo 3 Image	\\Server\Photos\JSmith3.jpg
%PHOTO4%	Event	Cardholder’s Photo 4 Image	\\Server\Photos\JSmith4.jpg
%PRIORITY%	Event	Alarm Priority	1, 2, 3, etc.
%SECURITYLEVEL%	Event	Hardware Object Security Level	High, Medium, Low, Normal
%SOURCENUMBER%	Event	Hardware Event Source Number	1, 2, 3, etc.
%SOURCETYPE%	Event	Hardware Event Source Type	1, 2, 3, etc.
%TENANT%	Event	Tenant Number	1
%TENANTNAME%	Event	Tenant Name	Student Hall
%TIME%	Event	Event Time	2:15:03 PM
%TIMEDATE%	Event	Event Date & Time	2/24/2004 14:15
%TITLE%	Event	Cardholder’s Title	Sales Engineer
%WATCH%	Event	Watched Status of Card	Watched or Clear
%ADDR%	Hardware	Hardware Object Address String	1.1.1.I6
%ADDRESS%	Hardware	Hardware Object Description	Front Entrance
%ALARM%	Hardware	Alarm Status in Text Form	Alarm, RTN, ACK, etc.
%ALARMINFO%	Hardware	Hardware Specific Alarm Text	If this is in alarm, call...

Replacement	Category	Description	Example
%AREA%	Hardware	Event's Area as Number	1
%ARMSTATE%	Hardware	Arm or Disarm State	Armed, Disarmed, etc.
%CAMERA%	Hardware	Camera Name	Motion1
%CAMERAID%	Hardware	Camera Number	1
%DOOR%	Hardware	Event's Door as Number	1
%FOREIGNACM%	Hardware	Door # of the Macros Associated Door Object	1
%FOREIGNADDR%	Hardware	Hardware Address of Macros Associated Hardware Object	1.4.D2
%FOREIGNADDRESS%	Hardware	Hardware Description of Macros Associated Hardware Object	Front Door
%FOREIGNAREA%	Hardware	Area # of the Macros Associated Area	1
%FOREIGNMACRO%	Hardware	Macro # of the Macros Associated Macro	1
%FOREIGNPOINT%	Hardware	Point # of the Macros Associated Hardware Object	1
%FOREIGNSIO%	Hardware	SIO # of the Macros Associated Hardware	1
%FOREIGNSITE%	Hardware	Site # of the Macros Associated Hardware	1
%FOREIGNSSP%	Hardware	SSP # of the Macros Associated Hardware Object	1
%FOREIGNSSPNAME%	Hardware	SSP Description of the Macros Associated Hardware Object	Main Building Controller
%FOREIGNTRIGGER%	Hardware	Trigger # of the Macro's Associated Trigger	1
%HOMEPAGE%	Hardware	Object's Homepage	C:\ProgramFiles\Map\Bldg1
%LASTCARD%	Hardware	Last Card Number Read at the Door	764319
%LASTCARDNAME%	Hardware	Last Cardholder to Badge at the Door	Smith, Bob
%LASTCARDTIME%	Hardware	Last Card Read at Door Time/Date	2/24/2004 14:15 PM
%LASTMESSAGE%	Hardware	Last Event Received at the Hardware Point	Access Granted: Door Used
%LASTMSG%	Hardware	Last Event Index Received at the Hardware Point	72
%LASTMSGTIME%	Hardware	Time and Date of Last Event	11/21/2018 4:11:00 PM
%LEDMODE%	Hardware	Door LED Mode	2
%LOWEROCCUPANCY%	Hardware	Area Lower Occupancy Warning	1
%MACRO%	Hardware	Event's Macro as Number	1
%MAXOCCUPANCY%	Hardware	Area MAX Occupancy	1
%MODE%	Hardware	Door Mode	Card Only
%MPG%	Hardware	Event's MPG as Number	1
%PDATE%	Hardware	Panel Transaction Date	2/12/2011
%POINT%	Hardware	Event's Point as Number	1
%PTIME%	Hardware	Panel Transaction Time	2:00:00 PM
%PTIMEDATE%	Hardware	Panel Transaction Date and Time	2/12/2011 2:00:00 PM
%OCCUPANCY%	Hardware	Area Occupancy	1

Replacement	Category	Description	Example
%SIO%	Hardware	Event’s SIO as Number	1
%SITE%	Hardware	Site Number	1
%SITENAME%	Hardware	Site Name	Oklahoma Office
%SSP%	Hardware	Event’s SSP Number	1
%SSPNAME%	Hardware	Event’s SSP Name	Main Building Controller
%STATE%	Hardware	Hardware Object State	Active, Inactive, etc.
%STATEOPEN%	Hardware	Door Open Status	Open, Closed, Unknown
%STATEFORCED%	Hardware	Door Forced Status	Forced, Normal, Unknown
%STATEHELD%	Hardware	Door Held Status	Held, Normal, Unknown
%STATUS%	Hardware	Hardware Object Status	Armed, Disarmed, etc.
%TRIGGER%	Hardware	Event’s Trigger as Number	1
%UPPEROCCUPANCY%	Hardware	Area Upper Occupancy Warning	1
%ALARMCOUNT%	System	Alarm Count Since Startup	12
%ALARMCOUNTOP%	System	Alarm Count Since Last Login	6
%EVENTCOUNT%	System	Event Count Since Startup	240
%EVENTCOUNTOP%	System	Event Count Since Last Login	120
%IPADDRESS%	System	Station’s Current IP Address	10.0.30.93
%OP%	System	Current DNA Operator	Admin
%OPTIME%	System	Time DNA Host Has Been Running Since Login	1:24:12
%RUNTIME%	System	Time DNA Host Has Been Running	2:08:52
%STATION%	System	Station Number	12
%STATIONNAME%	System	Station Name	Guard Station
%TRANSCOUNT%	System	Transaction Count Since Startup	70
%TRANSCOUNTOP%	System	Transaction Count Since Last Login	35

This Page Intentionally Left Blank

Glossary

E

Access Area

A defined area wherein all access points are secured by the system and can be configured and adjusted to set parameters on occupancy and permission attributes.

Access Control Model (ACM)

A group of objects that, when associated together, form an entry point that is frequently associated with a door or elevator.

ACM Mode (Door Mode)

The mode in which the ACM (door, elevator, gate, etc.) is programmed to grant access. This setting may be unlocked, card only, PIN, PIN and card, etc.

Access Credential

A medium, such as ID cards, key fobs, biometrics, or smart chips, that contains encoded information (which is recognized by the access control system).

Access Level

A logical group of doors paired with a time schedule that is used to determine when and where a card is granted access in the system.

Access Level Group

A group of access levels from multiple controllers associated together for easier distribution to cardholders.

Acknowledge Alarm

The action taken by an operator to indicate that he or she is aware of a specific alarm or tamper state.

Administrator

The person responsible for adding operators, assigning specific privileges to the operators' profiles, and designating operator levels.

Alarm Condition

Alarms signal a specific and "user-defined" state change in system hardware that is reported through the Alarm Grid.

ADA Mode

Indicates that a setting or card designation is compliant with the American Disabilities Act, which provides specific access parameters for personnel with disabilities. If the ADA setting is checked for a card, ADA parameters will take effect when the cardholder badges with the card.

Anti-Pass Back (APB)

A control feature that prohibits a card from entering an access area more than once unless the system recognizes that the card has first exited the access area.

Audit Trail

A record that accounts for all of the operator activity in the system.

Badge

An identification card that commonly includes the cardholder's photo, signature, and other identifying characteristics.

Badging Station

A hardware and software system used to obtain and save personal data about a cardholder, e.g., a photo or signature.

Bar Code

An array of machine-readable rectangular bars and spaces arranged in a specific way to represent letters, numbers, and other human-readable symbols.

Batch Processing

The execution of a series of programs (“jobs”) within DNA Fusion without manual intervention.

Battery Backup

A secondary energy source used to power devices in the event that the primary power supply fails.

Biometrics

Machine-readable technology that uniquely identifies individuals by reading their biological features (fingerprints, retina scans, etc.).

Bumping

The action of sending an alarm to an alternate site or workstation following a predefined time during which the alarm is unacknowledged.

Cardholder

A person who has been issued an access credential.

Channel

The path in which the SSP controller communicates with the host or driver.

Clear Alarm

The action taken by an operator to respond to an alarm condition after the alarm has been acknowledged, responded to, and cleared from the alarm grid.

Client

A computer connected to DNA Fusion that can be used to manage or monitor the system.

Command

An operator-initiated event that causes a change or action within the access control system.

Contact

An input point used to make or break an electrical circuit mechanically.

Controller

The data-gathering panel that makes local access decisions. Includes the SSP-D2, DController and SSP-EP.

Credential

See Access Credential.

Door Status Monitor (DSM)

A DSM is an input switch used to monitor whether a door is in an opened or closed position.

Door Forced

An alarm generated when a door is forced open. A Door Forced event may be generated for a number of reasons, such as when a key is used at the door or a DSM is not present on the door.

Door Held

An alarm generated when a door is held open past the programmed time.

Download

An “update” action to store saved information in a controller for the purposes of making access decisions or system actions without the intervention of the DNA server. See also: Save.

Driver

The service that establishes the connection between the DNA Fusion application and the field controllers to manage system settings and system events.

Egress

The act of exiting an access-controlled door, especially a door that leads out of a structure.

Facility Code

A numeric code stored in each access credential that uniquely identifies the facility at which the card is valid.

Fail Safe

If the power fails, the door will automatically unlock and allow entry or exit.

Fail Secure

If the power fails, the door will automatically lock and will not allow entrance, but it will still function as an exit.

Global Access Level Group

Allows an access level group to span multiple controllers without the need to create individual access levels.

Group

A logical set of common data objects such as cardholders or hardware points.

Held Time

The amount of time that an ACM (door, elevator, etc.) can be held open after receiving a valid access granted event or a request-to-exit is generated.

Host

The machine on which the driver generally resides. Sometimes refers to a given client machine, i.e. in reference to a host-based macro.

Host Settings

The settings that determine the behavior of the application at the host or workstation.

Input Point

Monitors the status of a device. This can be a DSM, motion detector or output from another device. Also referred to as a Monitor Point.

Keypad

An alphanumeric grid which allows a user to enter an personal identification number (PIN) to validate access.

Landscape

Horizontal orientation of pages, screen displays or badges.

Logging

Creating and storing a permanent record of the events.

Logo

A graphic symbol used to represent a company or organization.

Machine Readable

A code or string of characters that can be read by machines.

Magnetic Stripe

Magnetic material, usually applied as a stripe on a card, that is used to encode cardholder information.

Macro

A defined set of actions or commands based on a trigger event. Macros can also be manually executed.

Masking

Hiding or suppressing specific alarm points that the operator does not wish to be viewed while other points still report their status.

Monitor Point Group (MPG)

A collection of monitor points that typically have been grouped for common manageability.

Normally Closed

A circuit or switch in which the contacts are closed during normal operation.

Normally Open

A circuit or switch in which the contacts are open during normal operation.

Off-line

A condition in which a controller is not communicating with the DNA driver. In the off-line mode, the controller continues to make access decisions and process events according to the information stored in the local memory.

Operator

A person with access to the application. The administrator is also an operator, but is generally distinguished in the documentation due to the difference in responsibility and permissions.

Output

Supplies a contact or relay change of state to control a device, such as door locks, HVAC, etc. Also referred to as a Control Point.

Personal Identification Number (PIN) Code

A unique numerical code used to identify an individual.

Panel

Synonymous with an SSP. See also: Controller.

Password

A string of characters, symbols, and/or numbers associated with an operator’s account that is required to log in to DNA Fusion.

Personnel Group

A logical grouping of cardholders with a default access level(s).

Portrait

Vertical orientation of pages, screen displays or badges.

Pre-Alarm Held

An alert generated before an opened door reports a “held open” alarm.

Proximity

A non-contact system in which data are exchanged between card and reader by radio frequency, fiber optics, induction, laser or other non-mechanical contact technology.

Reader

A device that can read the encoding on a card or badge to process an access request.

Relay

A device that is capable of opening a normally closed circuit or closing a normally open circuit.

Request-to-Exit (REX)

A signal from an input programmed at the door that informs the controller that someone has requested to exit from a secured door.

Save

An action to record information in the database. See also: Download.

Secured Area

A physical location within a facility to which monitor points, control points and card readers can be grouped and controlled via card reads, keypad interaction or commands initiated by the operator. Typically used to define Monitor Point Groups.

Security System Processor (SSP)

Synonymous with panel and controller. See also: Controller.

Shunt

The length of time that an input will be ignored after it becomes active during an access granted event. This only applies to inputs that are specified as the Door Contact.

Smart Card

A plastic card with an embedded microchip that can be used to store information about the cardholder or record card transactions as they occur.

Strike Time

The time that a door (ACM) will be unlocked when a valid access granted or momentary unlock is received at the door.

Sub-controller

One of a series of circuit boards that communicates information about field devices like readers, contacts, motion detectors, etc., upstream to the SSP. (RSC-1, RSC-2, RSC-DT, ISC-16, NSC-100 and OSC-16)

Tamper1

A digital input that, if open, signals a cabinet tamper alarm at the device.

Tamper2

A digital input that signals power loss alarm at the device.

Time and Attendance

A report that consists of the arrival and departure card reads at identified readers.

Time Schedule

A predetermined time block that is associated with days and holidays to control access, trigger an event, and manage automated operations.

Trigger

A system event that causes another event or macro to occur.

Trouble

A condition within the circuitry of a monitored point that indicates that an equipment malfunction and/or a single break, a single fault or a wire-to-wire short exists. This only applies to supervised points.

Underwriters Lab

The UL label on a product signifies that the product has met the Underwriters Laboratories requirements and passed the stringent UL testing.

Workstation

A computer connected to the DNA system that can be used to manage and monitor the system. Also referred to as a Client.

OPEN OPTIONS®

ACCESS TECHNOLOGY