Fusion Web User Manual

DNA Fusion™ is a trademark of Open Options, L.P.

The DNA Fusion™ Access Control and Security Management System uses equipment that generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause harmful interference, in which case the user will be required to correct the interference at the user's expense.

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

This manual is proprietary information of Open Options, L.P.

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

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

Open Options, L.P. assumes no responsibility for incorrect or outdated information that may be contained in this publication.

This manual has been written for DNA Fusion™ version 6.0 or higher

Print Date: October 11, 2017

Manual Number: FW-1.0

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, L.P. Software License Agreement and Warranty

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

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

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

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

LIMITED WARRANTY: Open Options warrants that it has the sole right to license the Software to licensee. Open Options further warrants that the media on which the Software is furnished will be free from defects in materials and workmanship under normal use for a period of ninety (90) days following the delivery of the Software to the licensee. Open Options' entire liability and your exclusive remedy shall be the replacement of the Software if the media on which the Software is furnished proves to be defective. This warranty is void if the media defect has resulted from accident, abuse, or misapplication. Open Options does not warrant that the Software will meet the end user customer requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTIES ARE THE ONLY WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. NEITHER OPEN OPTIONS, NOR ITS VENDORS SHALL BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS, NOR FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND WHETHER UNDER THIS AGREEMENT OR OTHERWISE.

IN NO CASE SHALL OPEN OPTIONS' LIABILITY EXCEED THE PURCHASE PRICE OF THE SOFTWARE.

The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

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

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

Table of Contents

Chapter 3: Hardware

Chapter 4: Events and Alarms

Appendix A: Glossary

Appendix B: Process Diagrams

This Page Intentionally Left Blank

Introduction 1

In This Chapter	
√	Opening & Logging In to Fusion Web
√	Setting Operator Permissions
√	Navigating the Fusion Web Environment

Overview

Fusion Web is an Internet-based extension of the DNA Fusion access control software. It allows users to securely and remotely manage their DNA Fusion system through Internet Explorer.

From the Fusion Web interface, system operators can perform the following tasks:

- Manage Personnel
- Configure Card Access
- Control Hardware
- Generate Personnel and Hardware Reports
- Monitor Real-time Events and Alarms

> *The Flex API application must be installed and configured on the computer hosting the DNA Fusion driver (DNAdrvr32) prior to accessing the Fusion Web interface. For more information on Flex API installation and setup, see the Flex API Installation Manual.*

Fusion Web Access

Setting Operator Permissions

The system administrator must grant web access to the operator profile before a DNA Fusion operator can log in to Fusion Web.

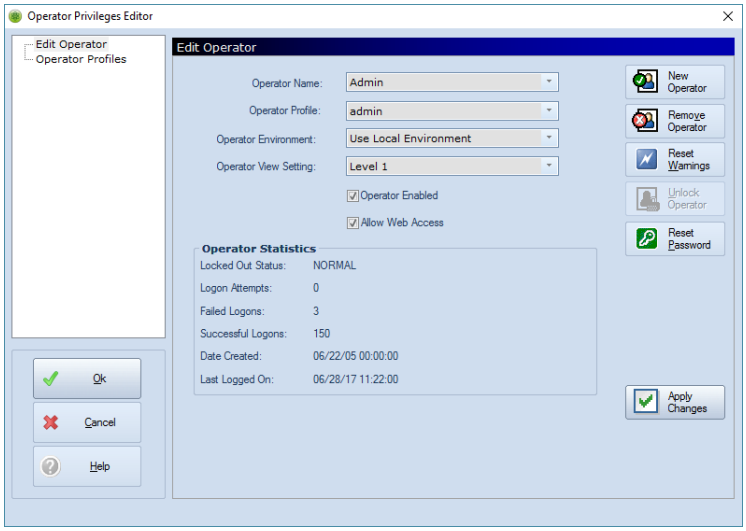
1. In DNA Fusion, open the Operators Privileges Editor dialog.

   See page 4-5 in the DNA Fusion User Manual for more information.

2. **Select** the desired Operator Name from the drop-down list.

3. **Check** the Allow Web Access checkbox.

   The designated operator(s) will be able to log in to the Fusion Web application using their Operator Name and Password.

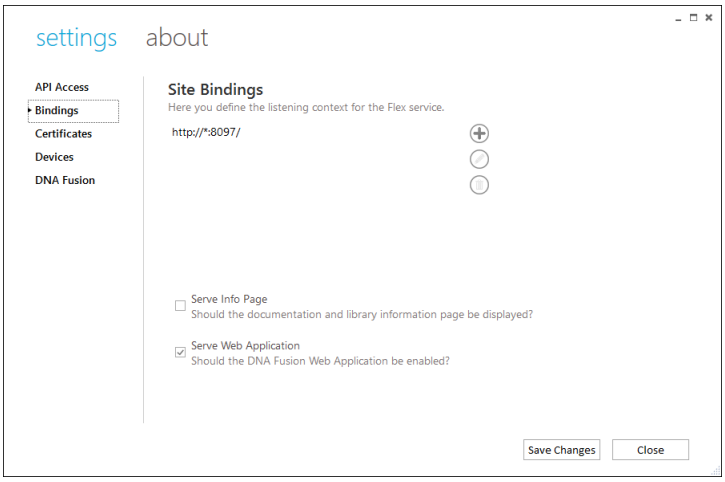


Obtaining the Site Binding

The Site Binding, which is configured by the system administrator in the Flex API application, is required to access the Sign In screen for Fusion Web. For more information on setting up site bindings, see page 2-5 in the Flex API Installation Manual.

1. **Open** the Flex API application and **select** Bindings from the Settings menu.

   The Site Bindings screen appears.



2. **Replace** the asterisk (*) in the configured Site Binding with localhost.

   In the example above, http://*:8097/ would be entered as http://localhost:8097/ in the address bar.

Signing In to Fusion Web

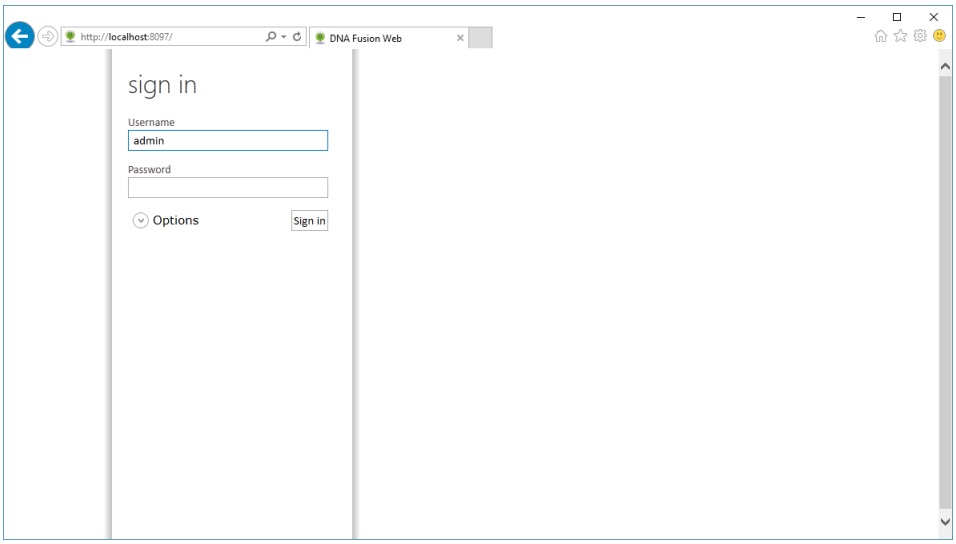
1. **Open** the Internet Browser.

   The web browser must be fully compatible with Microsoft Silverlight in order to access Fusion Web.

2. **Enter** the configured DNA Fusion address in the address bar.

   This information will need to be obtained from the system administrator.

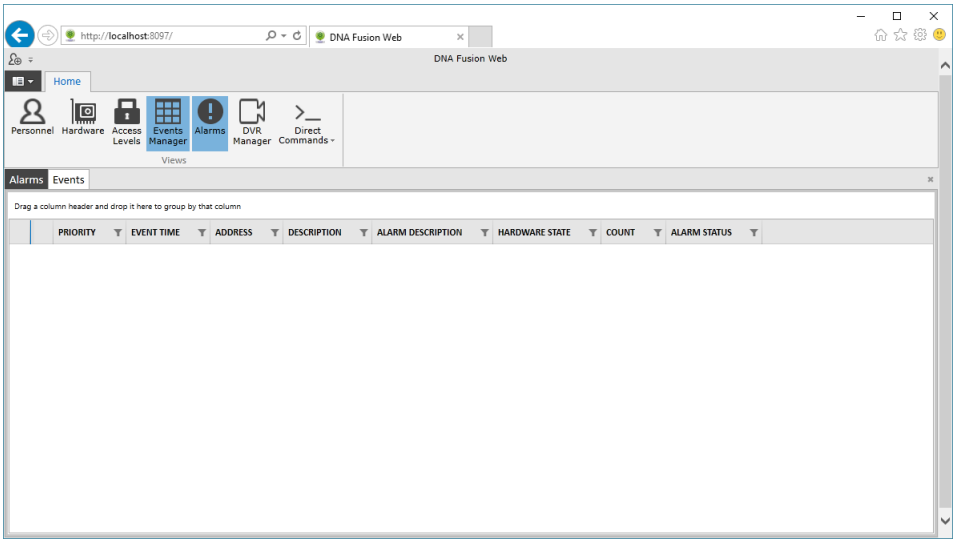
   The Fusion Web Sign In screen appears in the browser.



3. **Enter** the Username and Password and **click** Sign In.

   These are the operator credentials used to log in to the DNA Fusion software client.

   The Fusion Web main screen appears.



The Flex API account determines the Operator Privileges *in Fusion Web. A list of operator permissions and access rights is located in the* Privileges *tab of the* Settings Menu*.* *See page 1-8 for more information.*

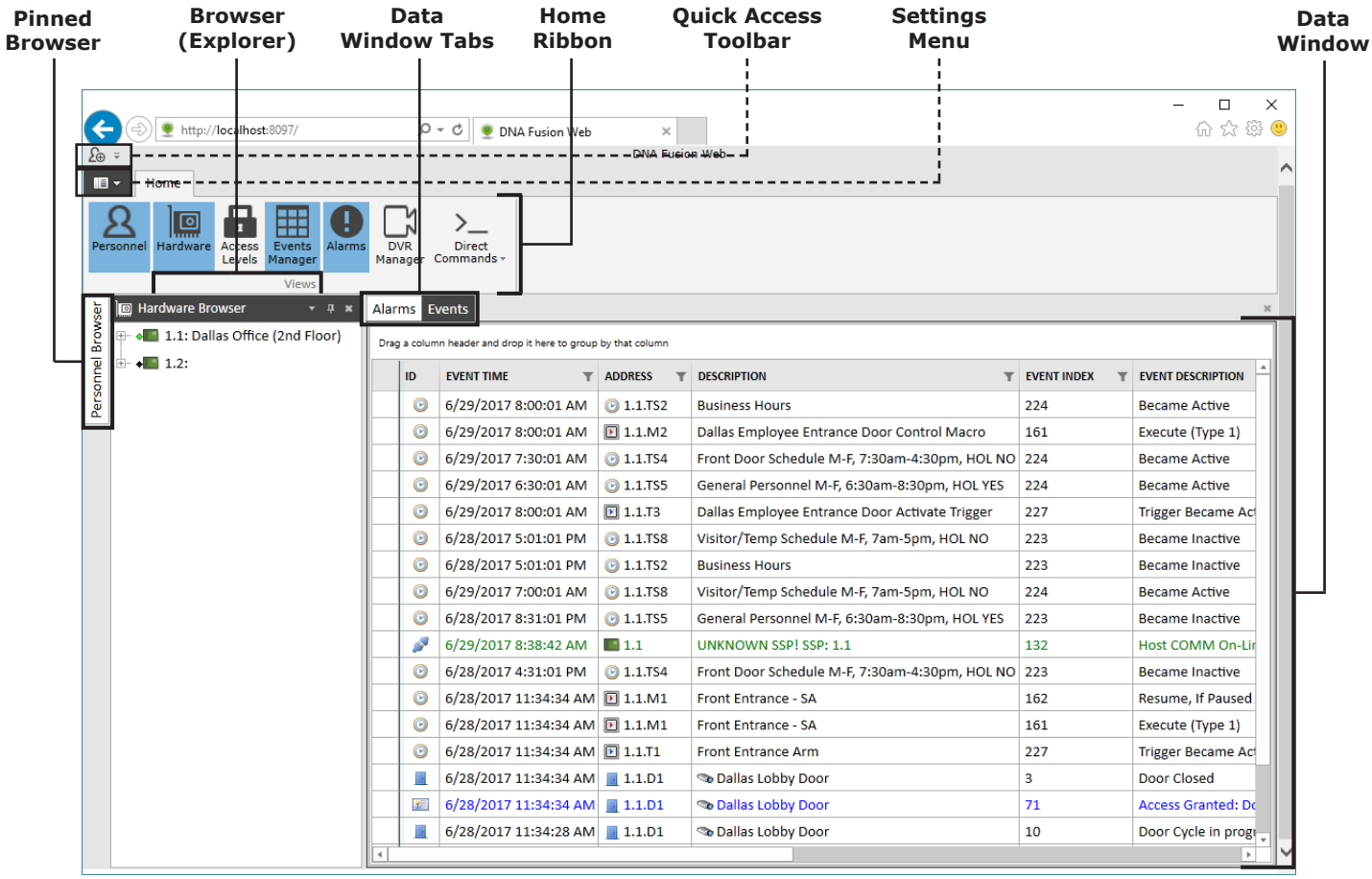
NOTES:

Fusion Web Environment

The Fusion Web interface is designed for user operability and navigation. Like DNA Fusion, the majority of operator actions are performed in the main screen and follow standard Windows conventions. The Fusion Web environment also uses many of the same customization features, including floating and dockable objects, pinned browsers, and resizable columns.

The main screen consists of seven principal elements:

- Home Ribbon
- Browsers (Explorers)
- Data Windows
- Data Window Tabs
- Pinned Browsers
- Quick Access Toolbar
- Settings Menu



Although the Fusion Web interface is designed to mirror the DNA Fusion application, it does not contain all of the features used in the software client. Programming functions, such as adding or removing hardware, designating card formats, and configuring properties, are not available in Fusion Web.

NOTES:

Home Ribbon

The Home Ribbon is the equivalent of the Standard Toolbar in DNA Fusion. It consists of seven options that open browsers and data windows in the main screen or display a list of commands. The Home Ribbon is the primary source of operator action in the Fusion Web environment.

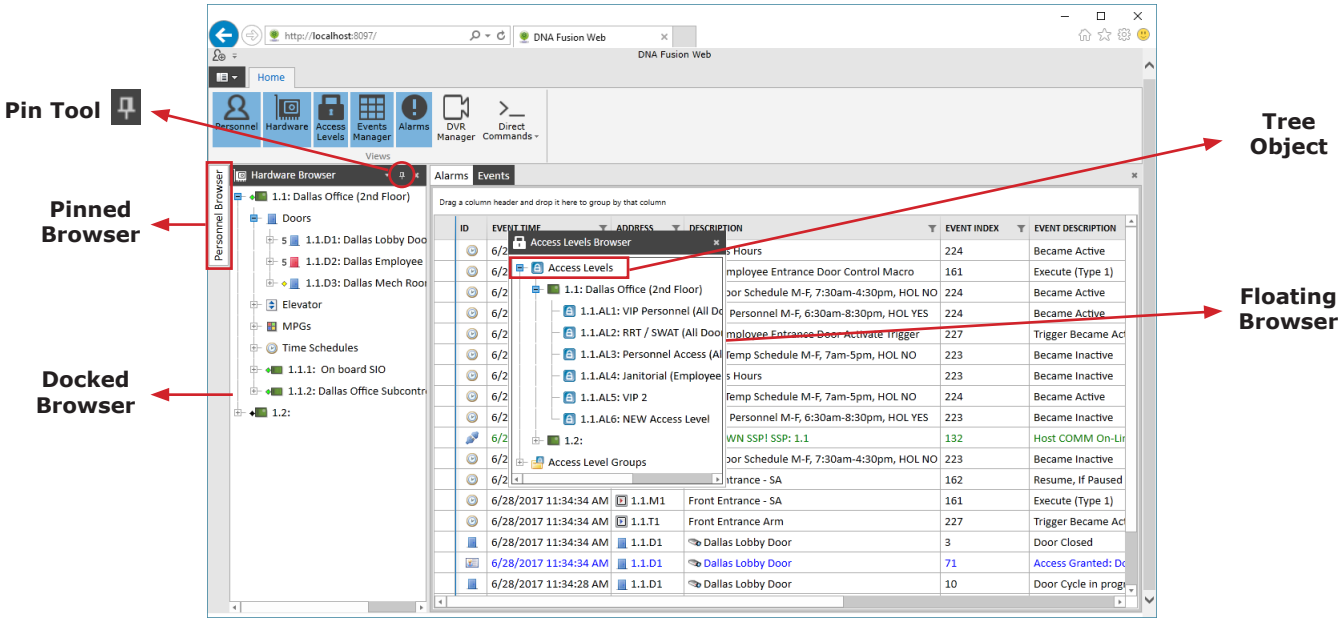
The following options are available from the Home Ribbon:

Personnel	Personnel Icon	Toggles the Personnel Browser. See page 2-1.
Hardware	Hardware Icon	Toggles the Hardware Browser. See page 3-1.
Access Levels	Access Levels Icon	Toggles the Access Levels Browser. See page 2-11.
Events Manager	Events Manager Icon	Toggles the Events Grid in a data window. See page 4-1.
Alarms	Alarms Icons	Toggles the Alarm Grid in a data window. See page 4-5.
DVR Manager	DVR Manager Icon	Toggles the DVR Browser. See page 3-6.
Direct Commands	Direct Commands Icon	Populates a drop-down menu to execute a Direct Command.* See page 3-5.

* Direct Commands are configured in DNA Fusion using the User Commands Editor dialog. See Chapter 8 in the DNA Fusion User Manual for more information.

Browsers (Explorers)

Browsers, sometimes referred to as explorers, are adjustable windows that populate when the user selects the Personnel, Hardware, Access Levels, or DVR Manager Icon(s) from the Home Ribbon. Browser information is organized in a hierachical "tree" view, where tree objects represent nodes that the operator can expand to view subgroups of related information.



By default, browsers are docked on the left or right side of the main screen. However, users 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, or, if desired, in the data window.

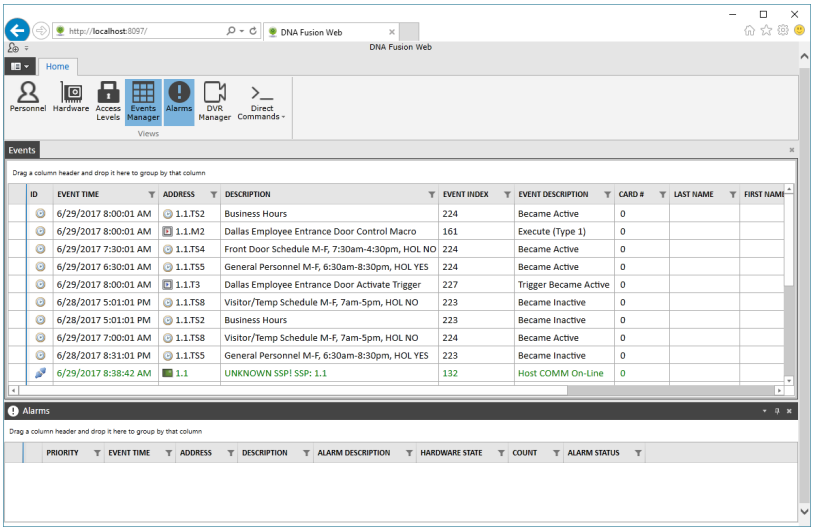
Alternatively, users can select the Pin Tool to hide the browser in the form of a document tab. To recall the window, hover the mouse cursor over the pinned tab; the browser will automatically hide when the user moves the cursor outside of the browser's edges. Toggle the Pin Tool to dock the browser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

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 item in the browser tree, click the minus (-) sign.

Data Windows

Data windows are adjustable windows that populate when the user selects the Alarms or Events Manager Icon(s) from the Home Ribbon. Like browsers, data windows can be docked on any location of the main screen or resized according to the operator's preference.

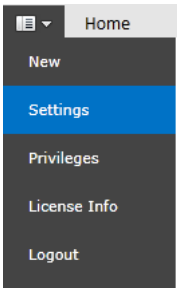
By default, when the user opens multiple data windows, they are separated by tabs; however, if the user docks the window on the left, right, top, or bottom section of the main screen, they behave similarly to browsers.



Settings Menu

The Settings Menu, located to the left of the Home Ribbon tab, opens a drop-down menu to configure the settings, view operator privileges, display license information, or log out of Fusion Web.

Select from the following options:

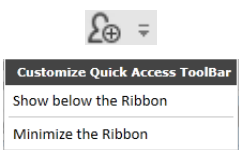


- New - Displays a Personnel icon that, when selected, opens a new Personnel Record in the data window.
- Settings - Displays a menu to configure the Fusion Web settings. See page 1-7 for more information.
- Privileges - Displays a read-only list of Operator Privileges based on the operator's DNA Fusion profile.
- License Info - Displays the Fusion Web license information, including the Licensed To name, License Type, License ID, and System ID.
- Logout - If selected, the operator is signed out of Fusion Web.

Quick Access Toolbar

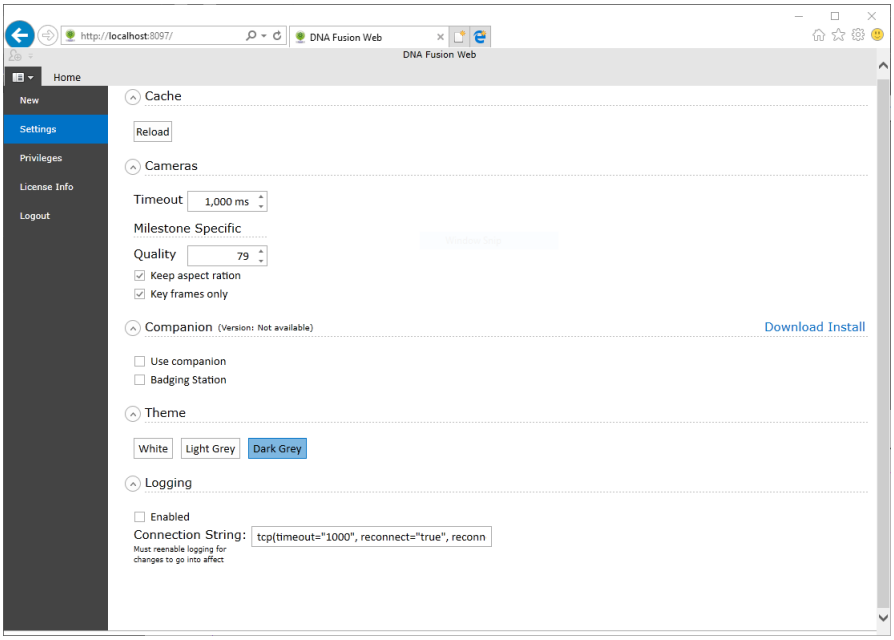
The Quick Access Toolbar is located above the Settings Menu. By default, the Add Personnel icon is the only function available from the toolbar. If selected, a new Personnel Record appears in the data window.

To customize the toolbar, click on the arrow to the right of the Add Personnel icon and select one of the following items:



- Show Below the Ribbon - Moves the Quick Access Toolbar below the Home Ribbon.
- Minimize / Restore the Ribbon - Toggles the Home Ribbon.

Fusion Web Settings



Cache

- Reload - Refreshes the browser cache.

Cameras

- Timeout - The number of milliseconds between retreiving each camera frame. The lower the number, the closer the camera footage will appear to real time. (Maximum setting = 1,000 ms)
- Milestone Specific - The following settings only apply to Milestone DVRs:
  - Quality - The JPEG image quality of each frame.
  - Keep Aspect Ratio - If selected, maintains proportional frames and prevents image stretching.
  - Key Frames Only - If selected, DNA Fusion will return key frames only.

Companion

The companion application allows Fusion Web users to perform badging functions and biometric enrollment.

- Use companion - If selected, the web application will attempt to communicate with the local, client-stored companion application.
- Badging Station - If enabled, Fusion Web operators will be able to use the web application to preview and print badges.

Theme

The theme setting changes the color scheme of Fusion Web. Select from three options: White, Light Grey, or Dark Grey.

Logging

- Enabled - If selected, the Fusion Web application will send logging information directly to the SmartInspect console.

This Page Intentionally Left Blank

Personnel 2

In This Chapter	
√	Opening a Personnel Record
√	Adding Cardholders and Credentials
√	Adding Cardholders to a Personnel Group
√	Generating Personnel Reports
√	Capturing and Uploading Photos

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. Information about cardholders is stored and managed in the Personnel Browser.

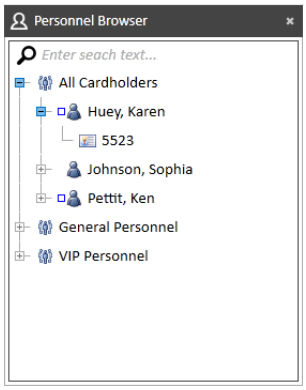
Using the personnel features in Fusion Web, operators can:

- Add and Remove Cardholders
- Activate and Deactivate Cards
- Assign and Remove Card Access Levels
- Capture and Upload Cardholder Photos
- Add Cardholders to a Personnel Group
- Run Trace History Reports

Personnel Browser

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

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



To open the Personnel Browser:

1. **Select** the Personnel Icon **from the** Home Ribbon.

   The Personnel Browser **appears.**

> *The* Enter Search Text *field is specific to Fusion Web. Operators can use this feature to search for individual cardholders by name.* *See page 2-3 for more information.*

This Page Intentionally Left Blank

Managing Personnel

Fusion Web retains many of the personnel management features offered by the DNA Fusion software client. For example, operators are able to add, edit, and remove cardholders, add cardholders to a personnel group, and generate reports.

In addition to the Personnel Browser, operators can use the Edit or Reports Ribbon to perform specific personnel actions in Fusion Web. The ribbons will only appear if a Personnel Record is open and active in the main screen.

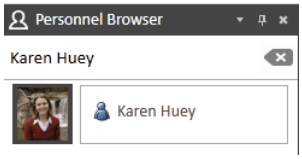
Opening a Personnel Record

1. In the Personnel Browser, **expand** the All Cardholders tree object and **double-click** on the desired cardholder's name.

   OR

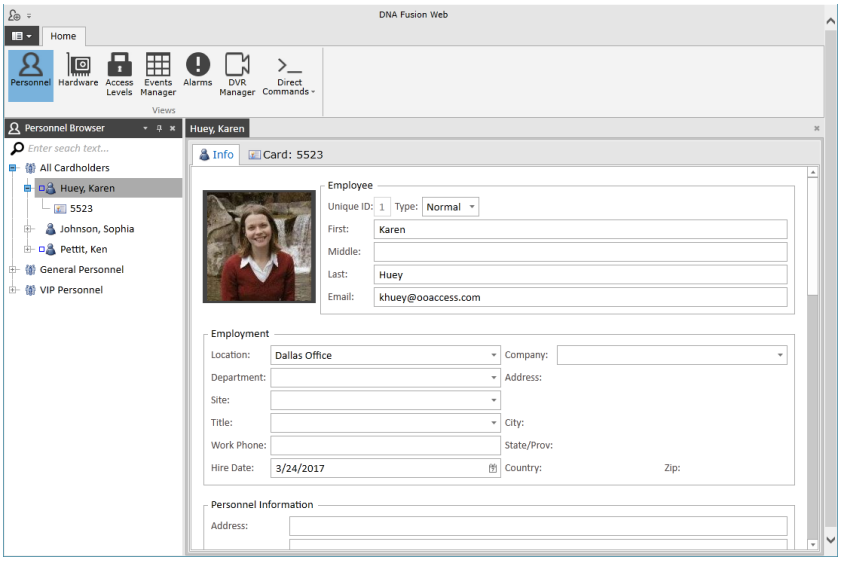
   In the Personnel Browser, type the cardholder's name in the Enter Search Text field and **select** the cardholder from the drop-down list. Enter seach text...

   The cardholder's photo will appear next to his or her name in the search results.



2. **Double-click** on the cardholder's name or photo.

   The associated Personnel Record opens in the data window.



For more information on the Personnel Record, see page 2-7.

> *Operators can also use the* Events Grid *to populate an existing* Personnel Record*. See page 4-3 for more information.*

Edit Ribbon

The Edit Ribbon is a toolbar used to perform basic edit functions for cardholders and credentials. It contains two toolsets: Personnel and Credentials.

Personnel		
Delete	Delete Icon	Deletes the selected personnel record. See page 2-4 for more information.
Save	Save Icon	Saves the current personnel record.
Take Photo	Take Photo Icon	Opens the Take Photo screen to take a photo with a connected camera. See page 2-17 for more information.
Upload Photo	Upload Photo Icon	Displays the Open dialog to upload a photo file (.png, .jpg, etc.) to the active personnel record. See page 2-17 for more information.

Credentials		
Add	Add Icon	Adds a new card to the existing personnel record. See page 2-5 for more information.
Delete	Delete Icon	Deletes the selected card from an existing personnel record. See page 2-5 for more information.
Add Access Level	Add Access Level Icon	Assigns an access level to the card. See page 2-11 for more information.

Reports Ribbon

The Reports Ribbon is a toolbar that the operator can use to generate Info Ready personnel reports.

Has Access To	Has Access To Icon	Generates a report that displays the cardholder's assigned access levels. See page 2-16 for more information.
Trace History	Trace History Icon	Opens the Trace History Dialog to run a trace history report for the cardholder. See page 2-15 for more information.

> *The* Edit Ribbon and Reports Ribbon *are only available if a* Personnel Record *is active in the data window.*

Adding a Cardholder

Operators can add cardholders in Fusion Web by using the Quick Access Toolbar or Settings Menu.

Quick Access Toolbar

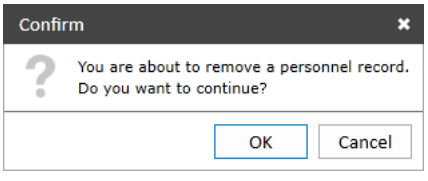
1. **Select** the Add Personnel Icon from the Quick Access Toolbar.
   A new Personnel Record appears.
2. **Populate** the desired fields in the Personnel Record tab(s).
   For more information, see page 2-7.
3. **Click** the Save Icon in the Edit Ribbon. Save
   The new cardholder is added to the Personnel Browser.

Settings Menu

1. **Select** the Settings Menu button from the main screen.
   A drop-down menu appears.
2. **Select** New from the drop-down menu.
3. **Click** the Personnel Icon under Available Items. Personnel
   A new Personnel Record appears.
4. **Populate** the desired fields in the Personnel Record tab(s).
   For more information, see page 2-7.
5. **Click** the Save Icon in the Edit Ribbon. Save
   The new cardholder is added to the Personnel Browser.

Removing a Cardholder

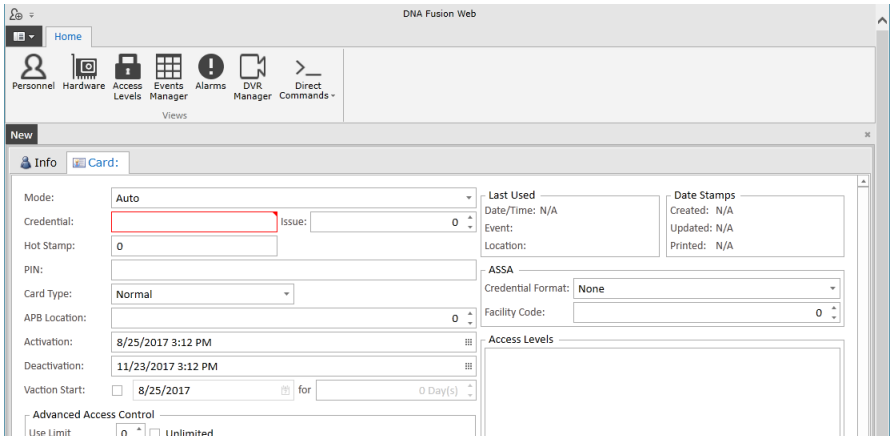
1. **Open** the desired Personnel Record.
2. **Click** the Delete Icon in the Personnel section of the Edit Ribbon. Delete
   A confirmation dialog appears.
3. **Click** OK to confirm the delete action.
   The cardholder is removed from the Personnel Browser.



Adding a Card

1. In an active Personnel Record, **click** the Add Icon in the Edit Ribbon.

   A new Card Tab appears in the data window.



2. **Enter** a card number in the Credential field. (Required)
3. If desired, **configure** the remaining fields in the Card Tab.

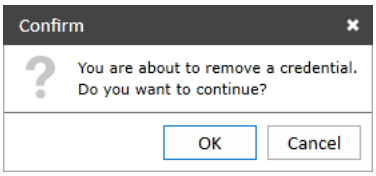
   See page 2-8 for more information.
4. **Click** the Save Icon in the Edit Ribbon.

   The new card object is saved and added to the Personnel Browser.

Removing a Card

1. **Open** the desired Personnel Record.
2. **Select** the Card Tab.
3. **Click** the Delete Icon in the Credentials section of the Edit Ribbon.

   A confirmation dialog appears.



4. **Click** OK to confirm the delete action.

   The card object is removed from the Personnel Browser.

Adding a Cardholder to a Personnel Group

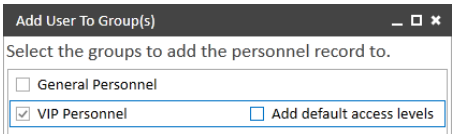
Personnel groups logically organize cardholders, and assign one or more default access levels to members of the group. When new cardholders are added to a personnel group, they receive all of the group's assigned access levels.

> *While it is possible to add cardholders to existing personnel groups in Fusion Web, users must create, configure, and remove personnel groups in the DNA Fusion software client. For more information, refer to Chapter 7 in the DNA Fusion User Manual.*

To add a cardholder to an existing personnel group(s):

1. **Right-click** on the Cardholder in the Personnel Browser and **select** Add Personnel to Group(s) from the context menu.

   The Add User to Group(s) dialog appears.



2. **Check** the desired Personnel Group(s).
3. If desired, **check** Add Default Access Levels to assign all of the personnel group's Legacy Access Levels to the cardholder.

   This setting does not apply to Legacy or Global Access Level Groups.

4. **Click** OK.

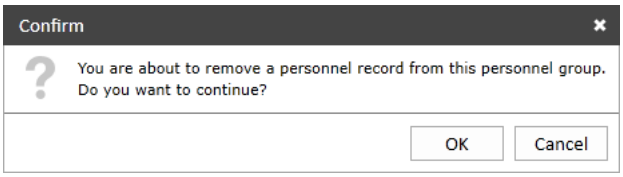
   The cardholder is added to the selected personnel group(s) and default access levels are applied.

> *The* Add Personnel to Group(s) *option is also available when the operator uses the* Search Tool *in the* Personnel Browser*.* **Right-click** *on the cardholder's search result and* **select** Add Personnel to Group(s)*.*

Removing a Cardholder from a Personnel Group

1. In the Personnel Browser, **expand** the desired Personnel Group.
2. **Right-click** on the desired Cardholder and **select** Remove Personnel from Group.

   A confirmation dialog appears.



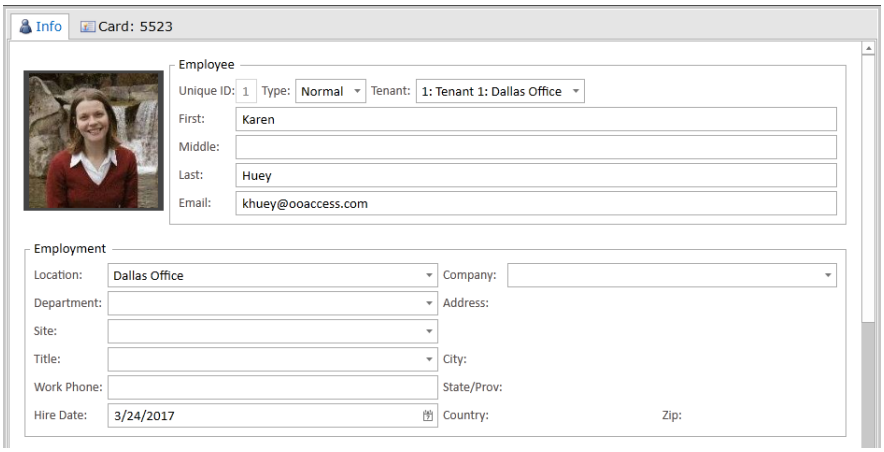
3. **Click** OK to confirm the delete action.

   The cardholder is removed from the selected personnel group.

Personnel Record

The Personnel Record in Fusion Web consists of two tabs: the Info Tab and the Card Tab. Each tab contains data entry fields and predefined drop-down lists that store information about cardholders and their credential(s). Drop-down list options must be configured in DNA Fusion; see page 7-5 in the DNA Fusion User Manual.

Info Tab



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).
- Tenant - Select the cardholder's Tenant Group from the drop-down list. For more information, see Chapter 13 in the DNA Fusion User Manual.
- First / Middle / Last - Enter the cardholder's first, middle, and last names.
- Email - Enter the cardholder's e-mail address.

Employment

- Location - Select the cardholder's employment location from the predefined drop-down list.
- Department - Select the cardholder's department from the predefined drop-down list.
- Site - Select the cardholder's site from the predefined drop-down list.
- Title - Select the cardholder's job title from the predefined drop-down list.
- Work Phone - Enter the cardholder's work phone number.
- Hire Date - Enter a cardholder's hire date or select the date from the calendar. (m/dd/yyyy) This field is populated by default with the addition of a cardholder.
- 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 under the Employment section of the Info Tab.

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.
- Zip - Enter the cardholder's zip code.
- Home Phone - Enter the cardholder's home phone number.
- 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)

Custom Fields

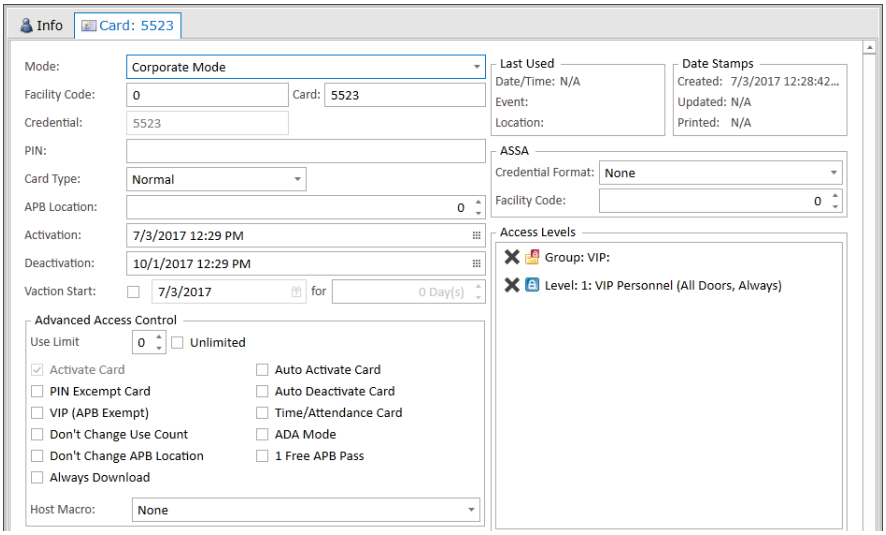
- Custom String (1-16) - Enter alphanumeric text in the field(s).
- Custom Value (1-3) - Enter a numeric value in the field(s).

> Custom Fields must be defined in DNA Fusion through the Host Settings / Personnel Properties / Custom Fields and Types dialog. For more information, see Chapter 3 in the DNA Fusion User Manual.

Other Personal Information

This section contains a text-entry field to store supplementary information about the cardholder.

Card Tab



Card Information

- Mode - Identifies the card format mode for the cardholder.
  - Auto - The default mode; uses the controller-stored card formats configured in DNA Fusion. See page 3-13 in the DNA Fusion User Manual for more information.
  - Corporate Mode - If selected, the operator must enter the card's Facility Code and Card Number. Fusion Web will calculate the Credential number based on the Multiplier specified in DNA Fusion through the DNA Properties dialog.
  - Multi - XX Bit Card - Provides the same functionality as Corporate Mode.
- Issue - Indicates the number of times a magstripe card has been issued to the cardholder, e.g., as a replacement for a lost card. See Chapter 8 in the DNA Fusion User's Manual for more information on storing issue codes.
- Credential - The hard-coded credential number that the system will read from the card. Users can add personnel records in the access control system without assigning a card to the record.
- PIN - The cardholder's personal identification number (PIN).
- Card Type - Identifies the card classification: Normal, Visitor, Temporary, Disabled, Contractor, Vendor, Custom (1-5). If Disabled is selected, a Why? drop-down appears and the card is deactivated.

The following fields require the operator to set a Controller Flag in DNA Fusion through the Controller Properties / Stored Quantities dialog. See Chapter 8 in the DNA Fusion User Manual for more information.

- APB Location - A number indicating the cardholder's anti-pass back (APB) area.
- Activation - The card's activation date and time.
- Deactivation - The card's deactivation date and time. By default, the date is set for one (1) year after the Activation date; however, it can be modified in Fusion Web.
- Vacation Start/For - The date range used to temporarily deactivate the card while the cardholder is on vacation.

Advanced Access Control

The following items are advanced features and may require the operator to configure additional settings in DNA Fusion. For more information, see page 7-10 in the DNA Fusion User Manual.

- Use Limit - Determines the maximum number of card uses. By default, this setting is Unlimited.
- Activate Card - Activates the card if checked and deactivates the card if unchecked. By default, all cards are active.
- 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 database even if the SSP controller did not receive an access request from the card. This feature overrides the Download on Personnel Demand setting in the DNA Site (Driver) Configuration dialog, which must be accessed through DNA Fusion.
- Auto Activate Card - If checked, automatically activates the card when the cardholder presents the card to an Auto Activate Door.
- Auto Deactivate Card - If checked, automatically deactivates the card when the cardholder presents the card 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 8-55 in the DNA Fusion User Manual.
- ADA Mode - If checked, the card uses the ADA settings in the door properties when presented to a door, thereby granting additional time to the designated cardholder(s).
- 1 Free APB Pass - Permits one anti-pass back (APB) infraction before denying card access.
- Host Macro - If desired, select a Host-Based Macro from the drop-down to associate with the card.

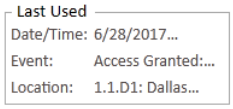
> *Operators can also* Activate *and* Deactivate *cards using the* Events Grid*. See page 4-3 for more information.*

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 7-10 in the DNA Fusion User Manual for more information.

Last Used

- Date/Time - The date and time that the card was last used. (Read-only)
- Event - The event associated with the card's last use. (Read-only)
- Location - The hardware address where the card was last used. (Read-only)



Date Stamps

- Created - The date and time that the card was added to the system. (Read-only)
- Updated - The date and time that the Card Tab was last updated. (Read-only)
- Printed - The date and time that the card was last printed. (Read-only)

Access Levels

The Access Levels panel contains a list of access levels assigned to the card. Users can remove an access level(s) or right-click in the personnel record to view additional options. For more information on access levels in Fusion Web, see page 2-11.

NOTES:

Access Levels

Access levels, when assigned to a card or credential, determine where and when the cardholder has access to secured areas. They represent the combination of entry points, such as doors or elevators, and time schedules. Each card contains a maximum of 6, 32, or 128 access levels per controller, depending on the Controller Properties / Stored Quantities setting in DNA Fusion. See page 8-49 in the DNA Fusion User Manual.

This section focuses on the access level features available in Fusion Web. For example, the operator can:

- View existing access levels in the Access Levels Browser
- Add access levels to a specific card
- Copy existing card access levels to a new card
- Remove all access levels from a card or member of a personnel group

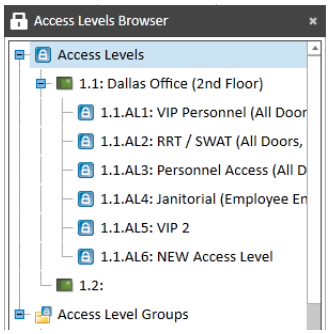
> *Operators must use DNA Fusion to configure access levels in the system. For more information, see Chapter 6 in the DNA Fusion User Manual.*

Access Levels Browser

The Access Levels Browser is an explorer window that contains information regarding a system's access levels and access level groups. Operators can expand the browser tree to display the access levels available from individual controllers or view the doors and elevators assigned to global access level groups.

The browser uses the following icons to designate the access level type:

- - Legacy Access Level
- - Global Access Level Group (Red)
- - Legacy Access Level Group (Blue)

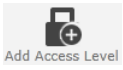


To open the Access Levels Browser:

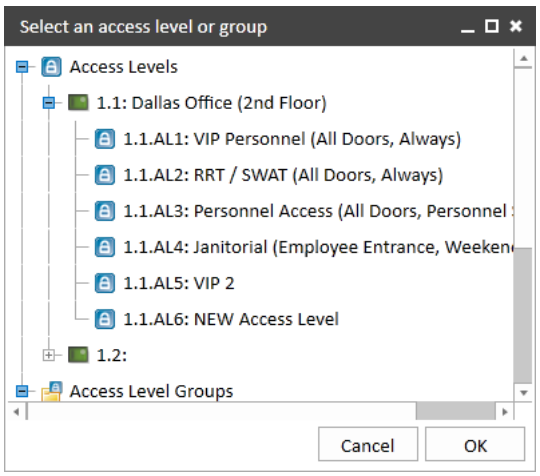
1. **Select** the Access Levels Icon from the Home Ribbon.
   

   The Access Levels Browser appears.

Adding an Access Level to a Card

1. With a Personnel Record open, **click** the Add Access Level Icon in the Edit Ribbon.
   

   The Select An Access Level or Group dialog opens.



2. **Select** the desired Access Level(s) or Access Level Group(s).
   Use the Ctrl or Shift key to select multiple access levels.
3. **Click** OK.
   The Access Level(s) or Access Level Group(s) is assigned to the card.

Removing an Access Level from a Card

1. With a Personnel Record open, **select** the desired Card Tab.
2. In the Access Levels panel, **click** the ✖ icon to the left of the desired Access Level(s) or Access Level Group(s).

   The Access Level(s) or Access Level Group(s) is removed from the card.
3. If desired, **click** the ↶ icon to restore a deleted Access Level or Access Level Group.

   This step must be performed prior to saving the Personnel Record.
4. **Click** the Save Icon in the Edit Ribbon to save the Personnel Record. 

> *The operator can also remove an access level from a card using the* Assigned To *report.* *See page 2-15 for more information.*

Removing All Access Levels from a Card

Operators can quickly remove all access levels from a card. This action can be performed using a right-click option in the Personnel Record or Personnel Browser.

From the Personnel Record

1. With a Personnel Record open, **select** the desired Card Tab.
2. **Right-click** in the Card Tab and **select** Access Levels / Remove All Access Levels.

   A confirmation dialog appears.

3. **Click** OK to confirm.

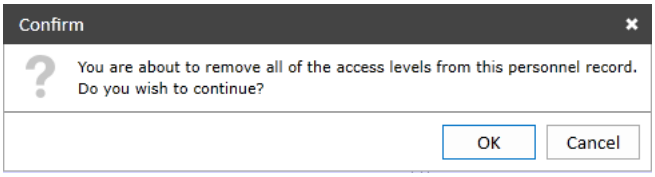
   All access levels are removed from the card.

From the Personnel Browser

1. In the Personnel Browser, **right-click** on the desired Cardholder or Card object and **select** Access Levels / Remove All Access Levels.

> If this action is performed on a cardholder with multiple cards, ALL of their cards' access levels will be removed.

A confirmation dialog appears.



2. **Click** OK to confirm.

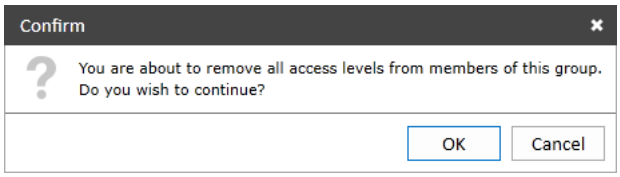
   All access levels are removed from the card(s).

> *The* Remove All Access Levels *option is also available when the operator uses the* Search Tool *in the* Personnel Browser*.* **Right-click** *on the cardholder's search result and* **select** Access Levels / Remove All Access Levels*.*

Removing All Access Levels from Personnel Group Members

1. In the Personnel Browser, **right-click** on the desired Personnel Group and **select** Access Levels / Remove All Access Levels from Group Members.

   A confirmation dialog appears.



2. **Click** OK to confirm.

   All access levels are removed from the members of the selected personnel group.

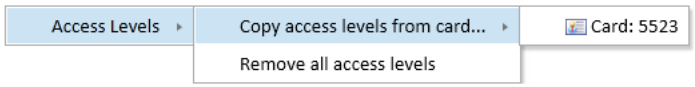
Copying Access Levels From a Card

Operators can copy access levels from an active card and distribute them to another card in the same personnel record. This action can be performed using a right-click option in the Personnel Record or Personnel Browser.

> *By default, when a new card is added and saved to a personnel record in Fusion Web, the new card will receive all access levels assigned to the cardholder's personnel group(s), if any.*

From the Personnel Record

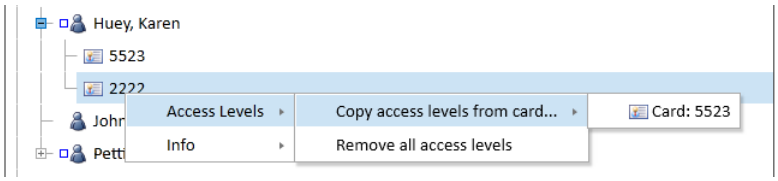
1. With a Personnel Record open, **select** the Card Tab to which the access levels will be copied.
2. **Right-click** in the Card Tab and **select** Access Levels / Copy Access Levels from Card.
3. **Select** an existing Card from the context menu.



   The access levels are copied from the existing card to the new card.

From the Personnel Browser

1. In the Personnel Browser, **expand** the desired Cardholder object.
2. **Right-click** on the Card to which the access levels will be copied and **select** Access Levels / Copy Access Levels from Card.
3. **Select** an existing Card from the context menu.



   The access levels are copied from the existing card to the new card.

Assigning Access Levels from the Access Levels Browser

In addition to the Personnel Record and Personnel Browser, operators can use the Access Levels Browser to drag and drop access levels to a cardholder or card.

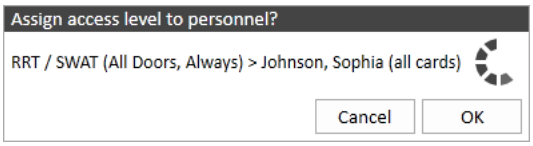
Drag and Drop to a Cardholder (All Cards)

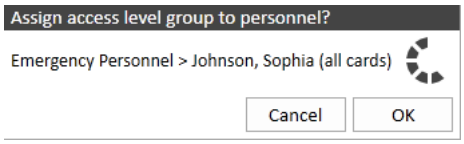
1. In the Access Levels Browser, **expand** the tree to the desired Access Level or Access Level Group.
2. **Drag** and **drop** the Access Level or Access Level Group to the desired Cardholder object in the Personnel Browser.

   OR

   Drag and **drop** the Access Level or Access Level Group to the Info Tab of the desired Personnel Record.

   A timed confirmation dialog appears.





3. **Click** OK to confirm.

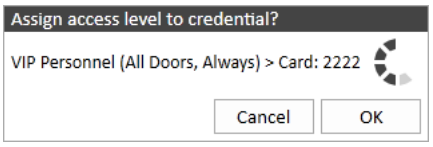
   The Access Level or Access Level Group is added to all cards in the Personnel Record.

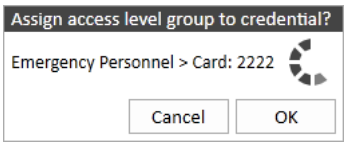
> *If the operator does not complete this step before the timer runs out, the dialog will disappear and cancel the action.*

Drag and Drop to an Individual Card

1. In the Access Levels Browser, **expand** the tree to the desired Access Level or Access Level Group.
2. **Drag** and **drop** the Access Level or Access Level Group to the desired Card object in the Personnel Browser.

   A timed confirmation dialog appears.





> *Alternatively,* **drag** *and* **drop** *the* Access Level *or* Access Level Group *to the desired* Card Tab *in the* Personnel Record *to immediately assign the access level(s) to the card.*

3. **Click** OK to confirm.

   The Access Level or Access Level Group is added to the selected Card.

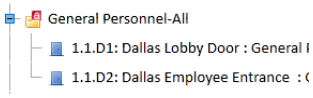
> *If the operator does not complete this step before the timer runs out, the dialog will disappear and cancel the action.*

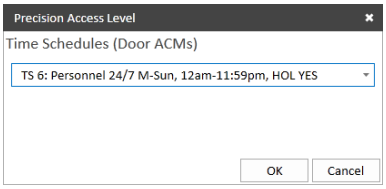
Assigning Precision Access Levels

Precision Access Levels allow the operator to assign individual doors to a cardholder or card. This feature must be configured in DNA Fusion through the Controller Properties. See page 6-17 in the DNA Fusion User Manual.

1. In the Access Levels Browser, **expand** a Global Access Level Group.
2. **Drag** and **drop** the desired Door to a Cardholder or Card object in the Personnel Browser.

   The Precision Access Level dialog opens.





3. **Select** a Time Schedule from the Time Schedules (Door ACMs) drop-down menu.
4. **Click** OK.

   The Precision Access Level is added to the selected Cardholder or Card.

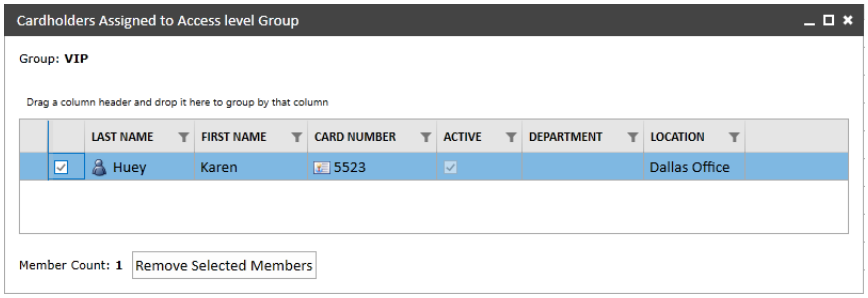
Personnel Reports

Operators can use Fusion Web to generate Info Ready reports about the system's cardholder activity. Five types of reports are available: Assigned To, Trace History, Has Access To, Non-Use, and Last Used.

Assigned To

The Assigned To feature generates a report of all the cardholders assigned to a Legacy or Global Access Level Group. The report includes each cardholder's first and last names, card number, active status, department, and work location.

1. In the Access Levels Browser, **expand** the Access Level Groups object.
2. **Right-click** on the desired Access Level Group and **select** Assigned To from the context menu.
   The Cardholders Assigned to Access Level Group dialog appears.

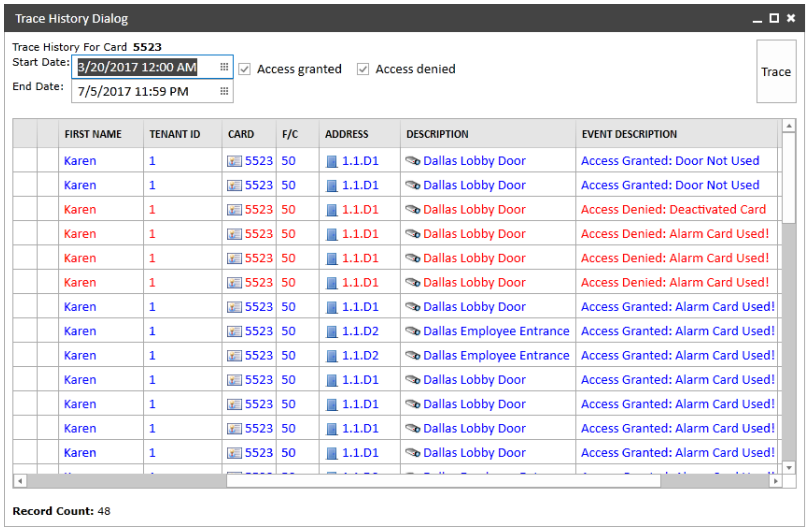


3. If desired, **select** one or more cards and **click** Remove Selected Members.
   The Access Level Group is removed from the selected card(s).

Trace History

The Trace History report displays the transaction history for an individual cardholder or card.

1. In the Personnel Browser, **right-click** on the desired Cardholder or Card and **select** Info / Trace History.
   The Trace History Dialog appears.
2. **Enter** a Start Date and End Date or **select** the dates from the calendar.
3. If desired, **toggle** the Access Granted or Access Denied checkbox(es) to filter the report.
   The report will only display events with the selected transaction type(s).
4. **Click** Trace to run the report.
   The results populate in the grid.

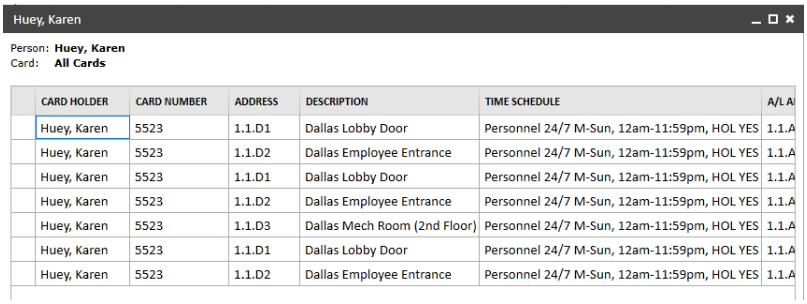


Has Access To

The Has Access To report displays all entry points to which a selected cardholder or card has access.

1. In the Personnel Browser, **right-click** on the desired Cardholder or Card and **select** Info / Has Access To.

   The Has Access To dialog appears.

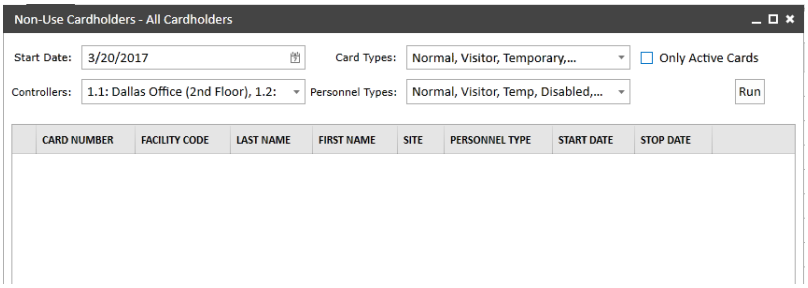


Non-Use

The Non-Use report displays cards that have not been used for a specified amount of time.

1. In the Personnel Browser, **right-click** on the All Cardholders object or an individual Personnel Group and **select** Info / Non-Use.

   The Non-Use Cardholders dialog appears.



2. **Enter** a Start Date or **select** the date from the calendar.
3. **Select** the desired Controller(s) from the drop-down.
4. **Select** the desired Card Type(s) from the drop-down.
5. **Select** the desired Personnel Type(s) from the drop-down.
6. If desired, **check** the Only Active Cards checkbox.

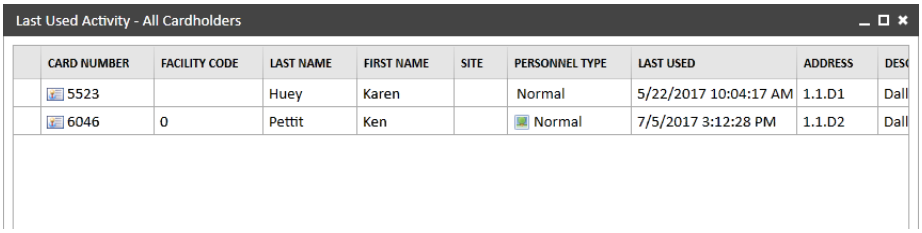
   This will remove deactivated cards from the report results.
7. **Click** Run to generate the report.

Last Used

The Last Used report displays the last used activity of cardholders in a selected personnel group(s), including the card number, date and time, hardware address, and hardware description.

1. In the Personnel Browser, **right-click** on the All Cardholders object or an individual Personnel Group and **select** Info / Last Used.

   The Last Used Activity dialog appears.



Photos

Fusion Web allows the user to capture ID photos using a connected web camera and upload photos to a personnel record.

Taking a Photo

1. With a Personnel Record open, **click** the Take Photo Icon in the Edit Ribbon. 

   The Take Photo window opens and displays the camera feed.
2. **Click** Capture to take the photo.
   The photo appears in the Image Preview.
3. If needed, **select** a Zoom percentage from the drop-down or **move** the sliding scale to alter the Image Preview dimensions. 

4. If desired, **edit** the photo using the Transform, Adjust, and Effects menus to the left of the Image Preview.
   See Editing a Photo instructions below for a list of edit options.
5. **Click** Done to save the photo.
   The photo appears in the Personnel Record.

> *The photo will also display in the form of a tooltip when the operator hovers the mouse over an event associated with the cardholder. See page 4-2 for more information.*

Uploading a Photo

1. With a Personnel Record open, **click** the Upload Photo Icon in the Edit Ribbon. 

   The Open dialog appears.
2. **Browse** to the desired file location and **click** Open.
   The photo appears in the Image Preview.
3. If needed, **select** a Zoom percentage from the drop-down or **move** the sliding scale to alter the Image Preview dimensions. 

4. If desired, **edit** the photo using the Transform, Adjust, and Effects menus to the left of the Image Preview.
   See Editing a Photo below for a list of edit options.
5. **Click** Done to save the photo.
   The photo uploads to the Personnel Record.

Editing a Photo

The Transform, Adjust, and Effects menus contain a variety of photo editing options, such as Resize, Crop, Rotate, Contrast, and Sharpen. Use the Undo and Redo buttons to reverse or reapply an edit action.

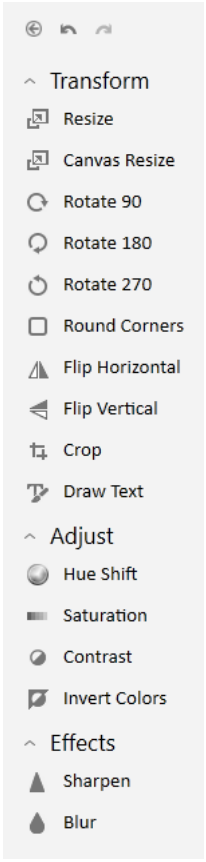
Transform

Resize

- Image Size - **Enter** the desired Width and Height dimensions (in pixels).
- Relative Size - **Enter** the desired Width and Height dimensions (as a percentage).
- Preserve Aspect Ratio - If checked, the ratio of the width to the height of the image remains proportional when the operator resizes the image dimensions.

Canvas Resize

- Canvas Size - **Enter** the desired Width and Height dimensions (in pixels).
- Image Alignment - **Select** a square in the grid to adjust the image's alignment on the canvas.
- Background - **Select** a canvas background color from the drop-down menu.



Rotate

- Rotate 90 - Rotates the image clockwise by 90 degrees.
- Rotate 180 - Rotates the image clockwise by 180 degrees.
- Rotate 270 - Rotates the image clockwise by 270 degrees.

Round Corners

- Radius - **Slide** the scale or **enter** a numeric value to adjust the curvature of the rounded corners.
  - Background - **Select** a radius background color from the drop-down menu.
- Border Thickness - **Slide** the scale or enter a numeric value to adjust the border thickness.
  - Border Color - **Select** a border color from the drop-down menu.

Flip

- Flip Horizontal - Horizontally flips the image.
- Flip Vertical - Vertically flips the image.

Crop

- Crop - **Adjust** the rectangular selection tool to the desired crop dimensions.

Draw Text

- Text - **Enter** the desired text.
- Font Size - **Slide** the scale or **enter** a numeric value to change the font size.
  - Text Color - **Select** a text color from the drop-down menu.
- Horizontal Position - **Slide** the scale or **enter** a numeric value to adjust the text's horizontal position on the image canvas.
- Vertical Position - **Slide** the scale or **enter** a numeric value to adjust the text's vertical position on the image canvas.
- Rotation - **Slide** the scale or **enter** a numeric value to adjust the text's rotation degree on the image canvas.

Adjust

Hue Shift

- Hue Shift - **Slide** the scale or **enter** a numeric value to adjust the hue of the image.

Saturation

- Saturation - **Slide** the scale or **enter** a numeric value to adjust the saturation of the image.

Contrast

- Brightness - **Slide** the scale or **enter** a numeric value to adjust the brightness of the image.
- Contrast - **Slide** the scale or **enter** a numeric value to adjust the contrast of the image.

Invert Colors

- Invert Colors - If selected, **inverts** the color values of the image.

Effects

Sharpen

- Amount - **Slide** the scale or **enter** a numeric value to adjust the sharpness of the image.

Blur

- Amount - **Slide** the scale or **enter** a numeric value to adjust the blur effect of the image.

Hardware 3

In This Chapter	
√	Controlling Hardware and Time Schedules
√	Executing Direct Commands
√	Using the DVR Manager
√	Generating Hardware Reports

Hardware refers to the physical field devices that comprise an access control system, such as controllers, subcontrollers, and card readers. Using Fusion Web, operators can remotely manage a number of hardware functions that are available in the DNA Fusion software.

This chapter highlights the following Fusion Web hardware features:

- The Hardware Browser
- Direct Controls
- Direct Commands
- The DVR Browser
- Hardware Reports

> *Operators must use DNA Fusion to add or remove system hardware, and configure object properties. See Chapter 8 in the DNA Fusion User Manual for more information.*

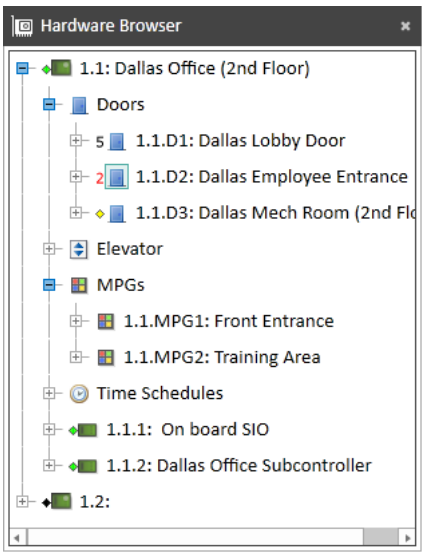
Hardware Browser

The Hardware Browser is an explorer window that displays a hierarchical layout of system field devices. It is the primary tool for controlling hardware in Fusion Web. The browser tree contains colored icons to indicate the status and condition of hardware objects.

To open the Hardware Browser:

1. **Select** the Hardware Icon from the Home Ribbon. 

   The Hardware Browser appears.



Status Indicators:

- Green Diamond - Inactive
- Red Diamond - Active
- Yellow Diamond - Fault
- Black Diamond - Offline

Object Colors:

- Black - Normal condition
- Gray - Offline object
- Red - Alarm condition
- Blue - Acknowledged alarm
- Green - Returned to normal (but not acknowledged)
- Red Door - Alarm door
- Blue Door - Normal door

This Page Intentionally Left Blank

Controlling Hardware

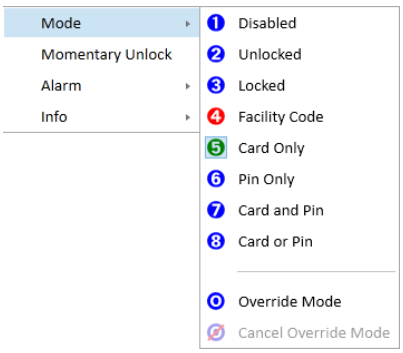
Operators can use Fusion Web to control doors, elevators, inputs and outputs, as well as monitor point groups (MPGs). Control options vary based on the selected hardware object.

Doors

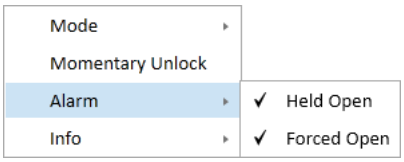
Direct control options for doors include changing the door's mode, momentarily unlocking the door, and arming or disarming the Door Forced and Door Held alarm states.

1. From the Hardware Browser, **right-click** on the desired Door object and **select** from the following menu options:

   - Mode - Changes the reader mode based on the operator's selection.
     - Disabled - Disables the reader and all associated door hardware. The door remains locked with no request-to-exit (REX) capability.
     - Unlocked - Unlocks the selected door and grants access to all cardholders.
     - Locked - Locks the selected door and disables card access. The REX button remains functional on the inside of the door.
     - Facility Code - Verifies that the card's facility code(s) match the facility code(s) stored in the SSP controller.
     - Card Only - Grants access to the selected door if a cardholder presents a card with the correct card format and access level.
     - Pin Only - Requires the cardholder to enter a valid PIN code. PIN numbers are set in the Personnel Record.
     - Card and Pin - Requires the cardholder to present a valid card AND enter a valid PIN code.
     - Card or Pin - Requires the cardholder to present a valid card OR enter a valid PIN code.
     - Override Mode - Opens the Temporary Door Override dialog. See page 3-5 for more information.
     - Cancel Override Mode - Cancels the Temporary Override command and returns the door to its normal state.



   - Momentary Unlock - Unlocks the door for the programmed strike trime. This is configured in DNA Fusion through the Door Properties / Door Objects dialog. See page 8-57 in the DNA Fusion User Manual for more information.
   - Alarm - Arms or disarms the Door Forced and Door Held alarm states.
     - Held Open - If checked, arms the Door Held alarm. If unchecked, disarms the Door Held alarm.
     - Forced Open - If checked, arms the Door Forced alarm. If unchecked, disarms the Door Forced alarm.



   If an Alarm option is selected, a colored mask may appear over the door icon in the Hardware Browser. See the table below for examples.

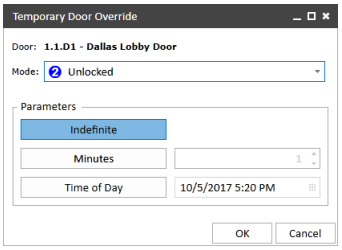
	Blue Mask	The Door Held alarm is disarmed (Held Open is unchecked).
	Green Mask	The Door Forced alarm is disarmed (Forced Open is unchecked).
	Red Mask	The Door Held and Door Forced alarms are both disarmed (Held Open and Forced Open are unchecked).

Door Override Mode

The Override Mode can be used to override a door for a specified amount of time. The operator selects which Mode to use during this time; once the time expires, the door reverts to its normal mode.

Example: A door is set to be temporarily unlocked for five minutes to grant access without a card. If an event occurs that affects 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 expired.

The Temporary Door Override dialog allows the operator to set the override using one of three Parameters:

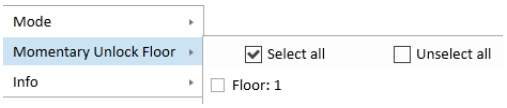


- Indefinite - Overrides the the door's normal mode and sets the reader to the specified mode permanently. The operator must cancel the override to return the door to its normal state.
- Minutes - Sets the selected door mode for the specifed number of minutes. (Max = 16383) The door will return to normal when the time expires.
- Time of Day - Sets the selected door mode until a specified end time. See page 8-5 in the DNA Fusion User Manual for more information.

Elevators

Direct control options for elevators include changing the elevator's mode and momentarily unlocking one or more floors.

1. From the Hardware Browser, **right-click** on the desired Elevator object and select an option:
   - Mode - Changes the reader mode based on the operator's selection. See Doors section on page 3-4 for a description of each reader mode.
   - Momentary Unlock Floor - Unlocks the selected floor(s) for the amount of time specified in the Elevator Objects dialog. See page 8-65 in the DNA Fusion User Manual.



Input Points

Use the Hardware Browser to arm or disarm an input point. Armed inputs generate alarms in the access control system; disarmed (or masked) inputs do not.

1. From the Hardware Browser, **right-click** on the Input Point.
2. **Select** one of the following control options:
   - Arm - Arms the input point and reports state changes to the Alarm Grid.
   - Disarm - Disarms (masks) the input point. Activity will not be reported to the Alarm Grid, but the system will still generate an event.

Output Points

Use the Hardware Browser to activate (turn on), deactivate (turn off), or momentarily activate an output point.

1. From the Hardware Browser, **right-click** on the Output Point.
2. **Select** one of the following control options:
   - Activate - Activates the output point and reports state changes to the Alarm Grid.
   - Deactivate - Deactivates the output point. Activity will not be reported to the Alarm Grid, but the system will still generate an event.
   - Momentary - Activates the output point based on the Momentary Time setting in the Output Properties dialog. See page 8-76 in the DNA Fusion User Manual for more information.

MPGs

If MPGs have been configured in the system, use the Hardware Browser to arm and disarm the secured area.

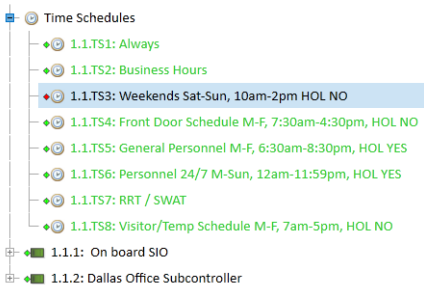
1. From the Hardware Browser, **right-click** on the desired MPG object and **select** Control.
2. **Select** from the following direct control options:
   - Access - Grants access to the secured area if the MPG points are not masked (disarmed).
   - Arm - Arms all points in the MPG.
   - Disarm - Disarms all points the MPG.
   - Force Arm - Arms the secured area even if the MPG contains one or more fault points.
   - Standard Arm - Arms the secured area if none of the MPG points are active.
   - Override Arm - Arms the secured area and overrides any fault points in the MPG.

Controlling Time Schedules

Fusion Web operators can access direct control options for time schedules using the Hardware Browser. Time schedules are commonly associated with access levels and doors; however, they serve numerous other purposes.

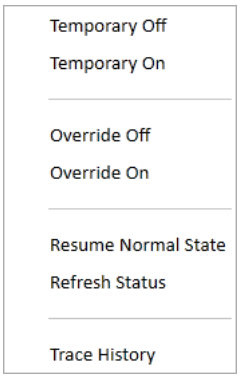
The browser tree uses colored icons to indicate the status of each time schedule:

- Green Diamond - The Time Schedule is currently active. If it is linked to a cardholder through an access level, the system will grant access to the cardholder. If it is linked to a door, the door will follow the mode that is programmed for the Active state of the time schedule.
- Red Diamond - The Time Schedule is currently inactive. If it is linked to a cardholder through an access level, the system will deny access to the cardholder and an Access Denied: Time event will populate in the Events Grid. If it is linked to a door, the door will follow the mode that is programmed for the Inactive state of the time schedule.



Direct Control Options

1. From the Hardware Browser, **expand** the Time Schedules object to view the controller's time schedules.
2. **Right-click** on the desired Time Schedule and **select** from the following menu options:
   - 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 anything associated with the time schedule will not be affected. Overrides the Scan Mode and ignores the effects of time intervals. Use the Resume Normal State command to restore the time schedule to the time based control.



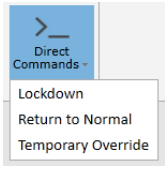
   - Override On - Sets the time schedule mode to ON and anything associated with the time schedule will be affected. Overrides the Scan Mode and ignores the effects of time intervals. Use the Resume Normal State command to restore the time schedule to the time-based control.
   - Resume Normal State – Returns the time schedule to its "normal" state. The system will evaluate the time schedule to determine whether it should be ON or OFF. Use this command to remove the Temporary On/Off and Override On/Off commands.
   - Refresh Status – Logs the current time schedule modes into the transaction log. Use this command to test triggers that are activated based on time schedule events.

> *Time schedule intervals are configured in DNA Fusion. For more information, see Chapter 5 in the DNA Fusion User Manual.*

Direct Commands

Operators can execute Direct Commands in Fusion Web; however, the commands must be programmed and managed in DNA Fusion.

1. **Select** the Direct Commands Icon from the Home Ribbon.
   A drop-down list of predefined commands appears.
2. **Select** the desired Command.
   The direct command executes.



For more information on configuring direct commands, see Chapter 8 in the DNA Fusion User Manual.

DVR Manager

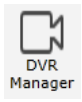
Fusion Web allows the operator to view and control cameras attached to a DVR/NVR server using the DVR Browser. The web application supports all of the DVR/NVR manufacturers supported by DNA Fusion.

> *Users can also launch cameras from the* Events Grid*. For more information, see page 4-3.*

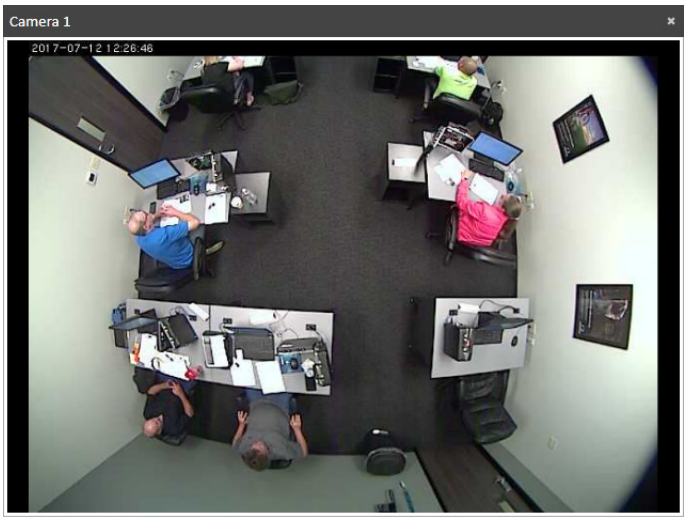
DVR Browser

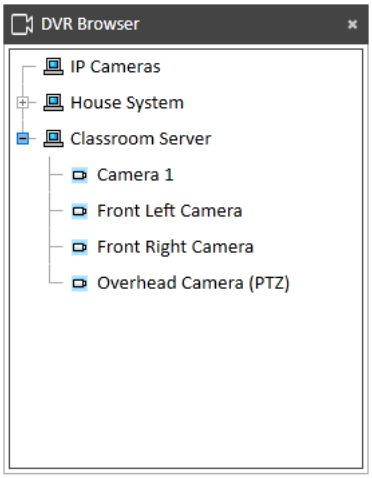
The DVR Browser contains the DVR and NVR servers as well as the cameras associated to each server.

1. **Select** the DVR Manager Icon from the Home Ribbon.
   The DVR Browser appears.



2. **Double-click** on the desired camera.
   The camera launches in a new window.





PTZ Controls

If the camera has PTZ (pan, tilt, and zoom) functionality, hover the mouse over the window to access the controls. The blue directional arrows will adjust the camera position, and the blue magnifying glasses will increase or decrease the zoom level.

Icon	Function
	Moves the camera in the selected direction.
	Increases or decreases the camera's zoom level.

> *The directional arrows will not move the camera if the zoom level is magnified.*

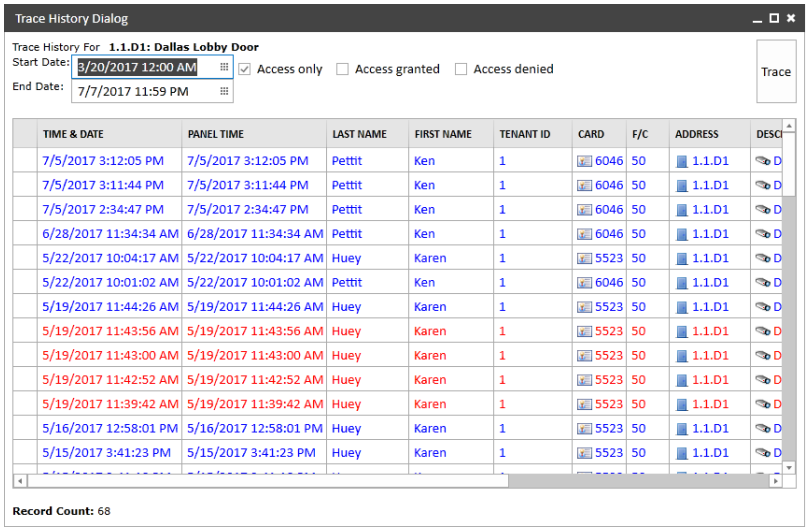
Hardware Reports

Operators can use Fusion Web to generate Info Ready reports about their system's hardware. Three types of reports are available: Trace History, Who Has Access, and Who Does Not Have Access.

Trace History

The Trace History report displays a transaction history for a selected hardware object or time schedule.

1. **Open** the Hardware Browser using the steps outlined on page 3-1.
2. **Right-click** on the desired Object or Time Schedule and **select** Info / Trace History.
   The Trace History Dialog appears.
3. **Enter** a Start Date and End Date or **select** the dates from the calendar.
4. If desired, **toggle** the Access Only, Access Granted, or Access Denied checkbox(es) to filter the report.
   This option is only available for doors.
5. **Click** Trace to run the report.
   The results populate in the grid.

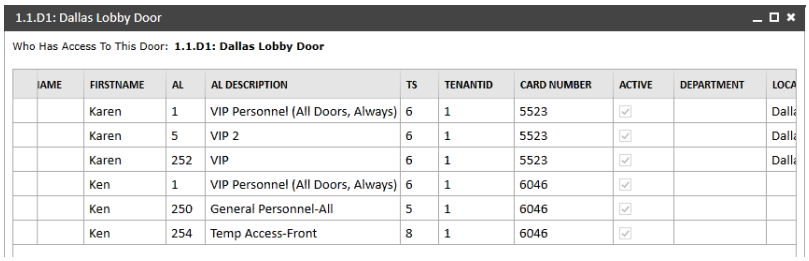


TIME & DATE	PANEL TIME	LAST NAME	FIRST NAME	TENANT ID	CARD	F/C	ADDRESS	DESC
7/5/2017 3:12:05 PM	7/5/2017 3:12:05 PM	Pettit	Ken	1	6046	50	1.1.D1	D
7/5/2017 3:11:44 PM	7/5/2017 3:11:44 PM	Pettit	Ken	1	6046	50	1.1.D1	D
7/5/2017 2:34:47 PM	7/5/2017 2:34:47 PM	Pettit	Ken	1	6046	50	1.1.D1	D
6/28/2017 11:34:34 AM	6/28/2017 11:34:34 AM	Pettit	Ken	1	6046	50	1.1.D1	D
5/22/2017 10:04:17 AM	5/22/2017 10:04:17 AM	Huey	Karen	1	5523	50	1.1.D1	D
5/22/2017 10:01:02 AM	5/22/2017 10:01:02 AM	Pettit	Ken	1	6046	50	1.1.D1	D
5/19/2017 11:44:26 AM	5/19/2017 11:44:26 AM	Huey	Karen	1	5523	50	1.1.D1	D
5/19/2017 11:43:56 AM	5/19/2017 11:43:56 AM	Huey	Karen	1	5523	50	1.1.D1	D
5/19/2017 11:43:00 AM	5/19/2017 11:43:00 AM	Huey	Karen	1	5523	50	1.1.D1	D
5/19/2017 11:42:52 AM	5/19/2017 11:42:52 AM	Huey	Karen	1	5523	50	1.1.D1	D
5/19/2017 11:39:42 AM	5/19/2017 11:39:42 AM	Huey	Karen	1	5523	50	1.1.D1	D
5/16/2017 12:58:01 PM	5/16/2017 12:58:01 PM	Huey	Karen	1	5523	50	1.1.D1	D
5/15/2017 3:41:23 PM	5/15/2017 3:41:23 PM	Huey	Karen	1	5523	50	1.1.D1	D

Who Has Access

The Who Has Access report displays which cards have access to a selected door. It includes the cardholder's name, card number, and access level description.

1. **Open** the Hardware Browser using the steps outlined on page 3-1.
2. **Right-click** on the desired Door and **select** Info / Who Has Access.
   The Who Has Access dialog appears.



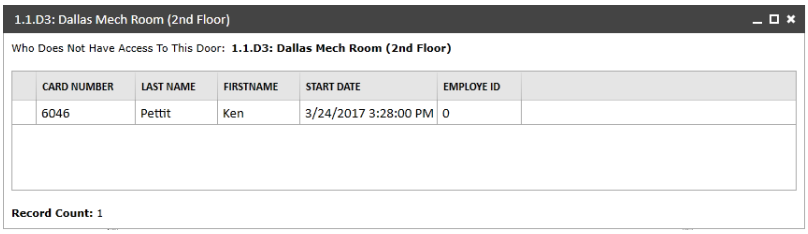
NAME	FIRSTNAME	AL	AL DESCRIPTION	TS	TENANTID	CARD NUMBER	ACTIVE	DEPARTMENT	LOCA
	Karen	1	VIP Personnel (All Doors, Always)	6	1	5523	☑		Dalla
	Karen	5	VIP 2	6	1	5523	☑		Dalla
	Karen	252	VIP	6	1	5523	☑		Dalla
	Ken	1	VIP Personnel (All Doors, Always)	6	1	6046	☑		
	Ken	250	General Personnel-All	5	1	6046	☑		
	Ken	254	Temp Access-Front	8	1	6046	☑		

Who Does Not Have Access

The Who Does Not Have Access report displays which cards do not have access to a selected door. It includes both the cardholder's name and card number.

1. **Open** the Hardware Browser using the steps outlined on page 3-1.
2. **Right-click** on the desired Door and **select** Info / Who Does Not Have Access.

   The Who Does Not Have Access dialog appears.



Events & Alarms 4

In This Chapter	
√	Using the Events Grid
√	Controlling Hardware and Personnel Events
√	Using the Alarm Grid
√	Managing Alarms

Fusion Web operators can use the Events and Alarm Grids to monitor real-time events and alarms that occur in the access control system. The grids are nearly identical to those used in DNA Fusion, and they maintain the settings configured in the DNA Properties dialog. For more information, see page 3-5 in the DNA Fusion User Manual.

Events

An event is an activity or incident that the system logs and reports in the Events Grid. For example, when a cardholder presents an access card to a reader, 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.

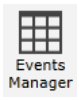
Events Grid

The Events Grid is the primary data window in Fusion Web. It consists of twelve resizable columns and displays events in chronological order from top to bottom, beginning with the most recent events.

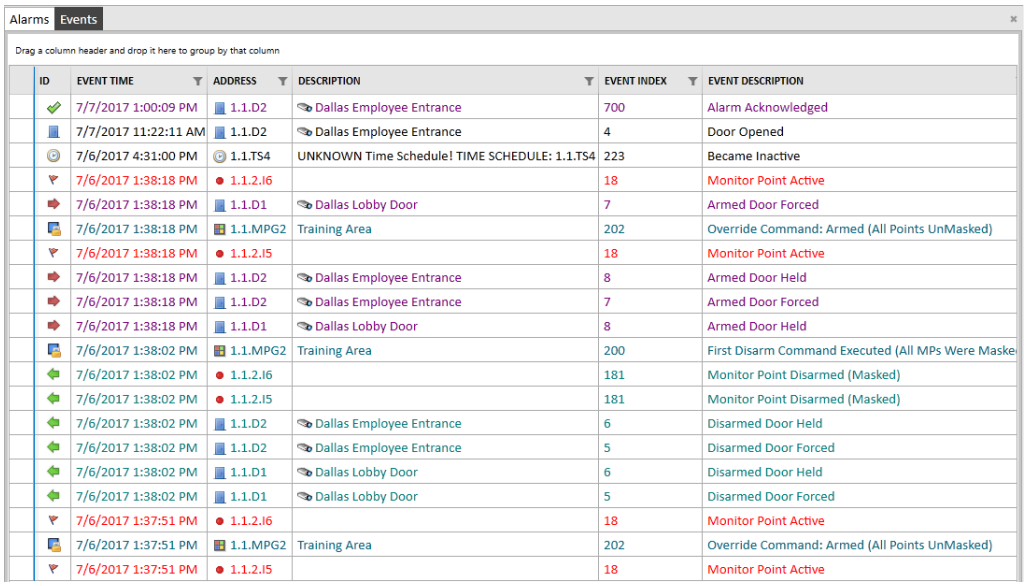
> *The* Events Grid *only displays events for an active operator session. The grid resets when the user logs out of Fusion Web.*

To open the Events Grid:

1. **Select** the Events Manager Icon **from the** Home Ribbon.

   The Events Grid **appears.**



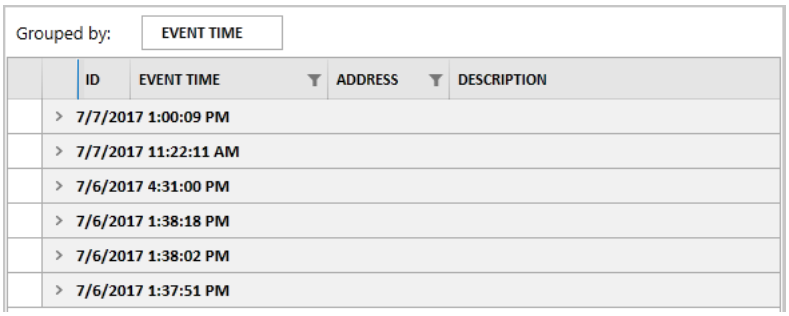
ID	EVENT TIME	ADDRESS	DESCRIPTION	EVENT INDEX	EVENT DESCRIPTION
	7/7/2017 1:00:09 PM	1.1.D2	Dallas Employee Entrance	700	Alarm Acknowledged
	7/7/2017 11:22:11 AM	1.1.D2	Dallas Employee Entrance	4	Door Opened
	7/6/2017 4:31:00 PM	1.1.TS4	UNKNOWN Time Schedule! TIME SCHEDULE: 1.1.TS4	223	Became Inactive
	7/6/2017 1:38:18 PM	1.1.2.I6		18	Monitor Point Active
	7/6/2017 1:38:18 PM	1.1.D1	Dallas Lobby Door	7	Armed Door Forced
	7/6/2017 1:38:18 PM	1.1.MPG2	Training Area	202	Override Command: Armed (All Points UnMasked)
	7/6/2017 1:38:18 PM	1.1.2.I5		18	Monitor Point Active
	7/6/2017 1:38:18 PM	1.1.D2	Dallas Employee Entrance	8	Armed Door Held
	7/6/2017 1:38:18 PM	1.1.D2	Dallas Employee Entrance	7	Armed Door Forced
	7/6/2017 1:38:18 PM	1.1.D1	Dallas Lobby Door	8	Armed Door Held
	7/6/2017 1:38:02 PM	1.1.MPG2	Training Area	200	First Disarm Command Executed (All MPs Were Maske
	7/6/2017 1:38:02 PM	1.1.2.I6		181	Monitor Point Disarmed (Masked)
	7/6/2017 1:38:02 PM	1.1.2.I5		181	Monitor Point Disarmed (Masked)
	7/6/2017 1:38:02 PM	1.1.D2	Dallas Employee Entrance	6	Disarmed Door Held
	7/6/2017 1:38:02 PM	1.1.D2	Dallas Employee Entrance	5	Disarmed Door Forced
	7/6/2017 1:38:02 PM	1.1.D1	Dallas Lobby Door	6	Disarmed Door Held
	7/6/2017 1:38:02 PM	1.1.D1	Dallas Lobby Door	5	Disarmed Door Forced
	7/6/2017 1:37:51 PM	1.1.2.I6		18	Monitor Point Active
	7/6/2017 1:37:51 PM	1.1.MPG2	Training Area	202	Override Command: Armed (All Points UnMasked)
	7/6/2017 1:37:51 PM	1.1.2.I5		18	Monitor Point Active

Grouping the Events Grid

Users can group the Events Grid by individual columns.

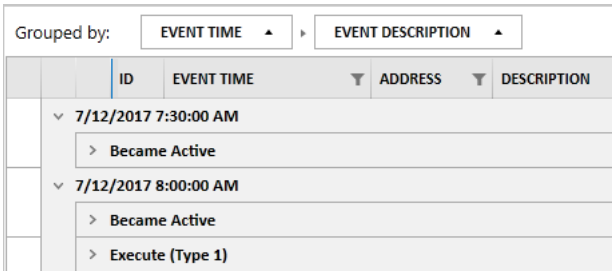
1. In the Events Grid, **drag** and **drop** a column header into the white space above the grid.

   The grid is grouped by the selected column.



2. **Expand** the desired group to display a list of events.

3. If desired, **drag** and **drop** an additional column header(s) to add a subgroup.



   In the example above, the Event Description column is a subgroup of the Event Time column.

   The sequence of the column headers determines the subgroup's position in the grid.

4. To **remove** a column group, **drag** and **drop** the column header away from the Grouped By field.

Displaying Photo Tooltips

Personnel photos appear in the form of a tooltip when the operator hovers the mouse over a cardholder-related event in the Events Grid.

1. In the Events Grid, **hover** the mouse over a cardholder-related event, e.g. Access Granted or Access Denied.

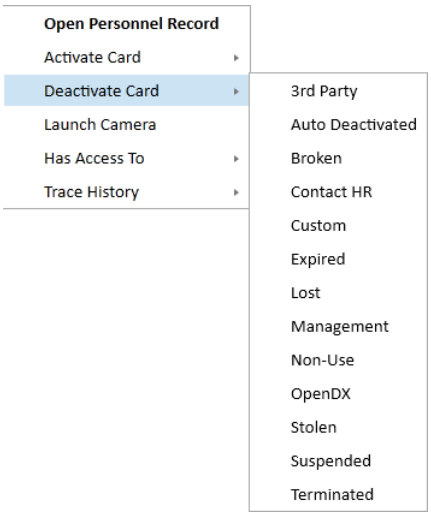
   The cardholder's photo populates in the form of a tooltip.

Controlling Hardware and Personnel Events

The operator can perform a number of hardware and personnel tasks directly from the Events Grid.

1. **Right-click** in the Events Grid and **select** an option from the context menu:

- Open Personnel Record - Opens the Personnel Record if the event is associated with a cardholder. See page 2-7 for more information.
- Activate Card - Activates the card associated with the event and applies the selected Card Type.
- Deactivate Card - Deactivates the card based on the selected reason.
  - 3rd Party - The operator is using a third-party system (such as an HR application).
  - Auto Deactivated - The card is an Auto Deactivate Card. See page 2-9 for more information.
  - Broken - The card is broken.
  - Contact HR - The cardholder must contact the HR department.
  - Expired - The card is expired.
  - Lost - The card is lost.
  - Management - The card has been disabled per management request.
  - Non-Use - The card has been deactivated through the Non-Use Report. This report allows the operator to view cards that has not been used for a predetermined amount of time. See page 2-16 for more information.
  - OpenDX - OpenDx has been configured and the card has been deactivated due to an OpenDX event.
  - Stolen - The card has been stolen.
  - Suspended - The card is suspended from use.
  - Terminated - The cardholder has been terminated from employment.



If the operator created Custom Card Types *or* Disable Reasons *in DNA Fusion, custom options will appear in the* Activate Card *and* Deactivate Card *menus. See page 3-24 in the DNA Fusion User Manual for more information.*

- Launch Camera - Opens the Camera associated with the event's hardware point. See page 3-6 for more information.
- Has Access To - Generates a Has Access To report for the selected hardware or personnel object. See pages 2-16 and 3-7 for more information.
- Trace History - Generates a Trace History report for the selected hardware, personnel, or card object. See pages 2-15 and 3-7 for more information.

NOTES:

Alarms

Alarms signal a specific, user-defined change in hardware state, e.g., forced or held doors. The system reports these state changes in the Alarm Grid. While grid properties and alarm priorities must be configured in the DNA Fusion software client, operators are able to use Fusion Web to acknowledge, clear, and dismiss alarms that appear in the grid.

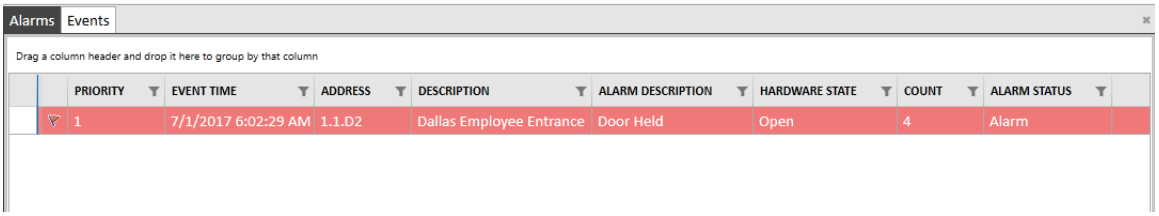
Alarm Grid

The Alarm Grid is a data window that contains a spreadsheet record of active system alarms. The operator can use the grid to monitor and respond to alarms.

To open the Alarm Grid:

1. **Select** the Alarms Icon from the Home Ribbon. 

The Alarm Grid appears.



The grid consists of the following resizable columns:

Column	Description
Priority	The user-defined alarm priority. See page 14-25 in the DNA Fusion User Manual for more information on setting priorities.
Event Time	The date and time when the alarm event occurred (based on the operator's time zone).
Address	The hardware location of the alarm point.
Description	The user-defined address description for the alarm point.
Alarm Description	The system-defined description of the alarm event.
Hardware State	The current hardware status.
Count	The number of times that the alarm point has changed state since the operator acknowledged and cleared the alarm.
Alarm Status	The current alarm status.

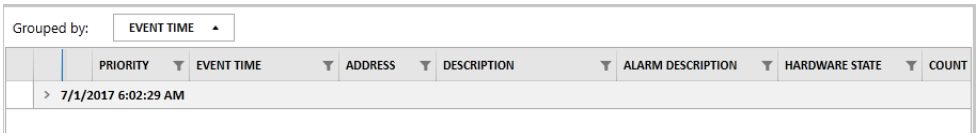
Additionally, the grid contains a color-coded flag to represent the Alarm Status. The operator can use this icon to determine how to respond to the alarm.

Icon Color	Alarm Status	Description	Operator Response
Red	Alarm	The alarm is active.	Acknowledge and clear or dismiss the alarm.
Green	Returned-to-Normal (RTN)	The alarm point has returned to its normal state.	Acknowledge the alarm.
Yellow	Acknowledged (ACK)	The operator has acknowledged the alarm, but the point has not returned to its normal state.	No action required; however, the operator may need to change the physical condition of the alarm point to return it to normal.
Blue	Clear	The operator has acknowledged the alarm and the point has returned to its normal state, but the alarm has not been cleared.	Clear the alarm.

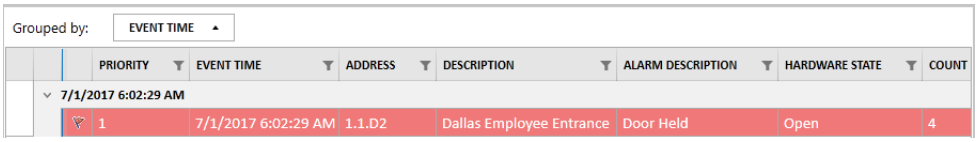
Grouping the Alarm Grid

Users can group the Alarm Grid by individual columns.

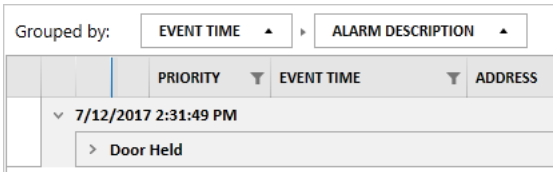
1. In the Alarm Grid, **drag** and **drop** a column header into the white space above the grid.
   The grid is grouped by the selected column.



2. **Expand** the desired group to display a list of alarms.



3. If desired, **drag** and **drop** an additional column header(s) to add a subgroup.



   In the example above, the Alarm Description column is a subgroup of the Event Time column.
   The sequence of the column headers determines the subgroup's position in the grid.

4. To **remove** the column group, **drag** and **drop** the column header away from the Grouped By field.

Alarm Management

The system operator is responsible for recognizing and responding to an alarm condition. This section explains how to manage an alarm in the Alarm Grid.

Like DNA Fusion, alarms in Fusion Web are either active or inactive:

- 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.

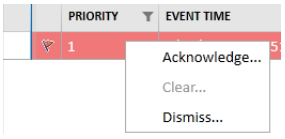
Depending on the operator's action, the alarm has four possible conditions:

- Unacknowledged Alarm – The operator has not acknowledged the alarm.
- Acknowledged Alarm – The operator has acknowledged the alarm.
- Cleared Alarm – The operator has acknowledged and cleared the alarm from the grid.
- Dismissed Alarm – The operator has dismissed the alarm.

Under normal operations, the alarm response process is 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 its normal state.	Inactive	Acknowledged
4.	The operator clears the alarm.	Inactive	Cleared

Responding to an Alarm



1. **Right-click** on the desired Alarm in the Alarm Grid.
2. **Select** an Action from the context menu: Acknowledge, Clear, or Dismiss.
   Use the Alarm Status table on page 4-5 to determine the appropriate operator response.

> *If the* Dispatch Text *feature is used in DNA Fusion, Fusion Web will prompt the user to enter custom dispatch text or select from a predefined list. See page 4-7 for details.*

Dispatch Text

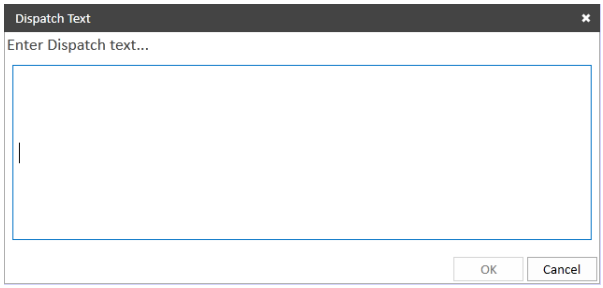
The Dispatch Text feature requires the operator to enter a comment or select predefined text from a drop-down list when responding to alarms. It must be configured in DNA Fusion; however, Fusion Web retains the DNA Fusion settings. See page 14-21 in the DNA Fusion User Manual for more information.

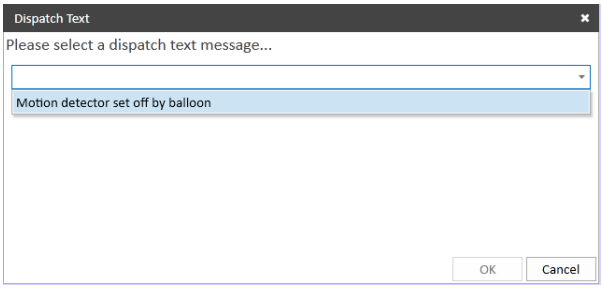
To enter Dispatch Text:

1. **Right-click** on the desired Alarm in the Alarm Grid.
2. **Select** an Action from the context menu: Acknowledge, Clear, or Dismiss.

   Use the Alarm Status table on page 4-5 to determine the appropriate operator response.

   The Dispatch Text dialog appears.





3. **Enter** the custom Dispatch Text.

   OR

   Select the Predefined Dispatch Text from the drop-down menu.
4. **Click** OK to complete the action.

> *Fusion Web only requires predefined dispatch text if the operator checks* Use Predefined Dispatch Text *in the* DNA Properties *dialog of DNA Fusion. See page 3-6 in the DNA Fusion User Manual for more information.*

This Page Intentionally Left Blank

Glossary A

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.

Access Level
A logical pairing of a door and time schedule that is used to determine when and where a card is granted access in the system.

Acknowledge
An action performed by an operator to indicate that he or she is aware of a specific alarm or tamper state.

ADA Mode
Indicates that a setting or access card is compliant with the American Disabilities Act, which provides specific access parameters for personnel with disabilities. Cards set to ADA Mode cause ADA parameters to take effect when someone badges at a reader.

Administrator
The person responsible for adding operators, assigning the privileges specific to an operator's profile, and designating station levels.

Alarm
A system-generated signal that populates in the Alarm Grid and alerts the operator about a user-defined change of state in hardware.

Anti-Passback (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.

Brightness
The overall luminance of a photo or graphic; an adjustment to brightness equally affects the highlights and shadows of an image.

Browser
Adjustable windows that organize information in a hierarchical "tree" view, where tree objects represent nodes that the operator can expand to view subgroups of related information. Browsers can be docked, resized, or pinned depending on the operator's preference.

Cache
A portion of memory in the computer's hard drive where the web browser stores data from previously visited web pages to increase future processing speeds for the same data.

Cardholder
A person, frequently referred to as personnel, who possesses a valid access credential.

Clear
An action performed by an operator to clear an acknowledged alarm from the Alarm Grid.

Client
A computer application, such as a web browser, that runs on the operator's local computer or workstation and accesses a service made available by a server.

Context Menu
A menu in a graphical user interface (GUI) that populates on a specific user interaction, such as a right-click mouse operation. The contents of the menu vary based on the location and context of the interaction.

Contrast
The difference in luminance between the highlights and shadows of an image; an increase in contrast darkens shadows and brightens highlights.

Controller
The data-gathering panel, also referred to as an SSP, that makes local access decisions.

Credential
A medium such as an access card, key fob, biometric signature, or smart chip that contains encoded information. When recognized by a reader, it allows the user to enter secured areas in an access control system.

Data Window
Adjustable windows that populate grids in the main screen; like browsers, they can be docked or resized according to the operator's preference. Multiple data windows are separated by tabs.

Dialog
A contextual window that appears when the operator performs an action in the Fusion Web application; it communicates information to the operator and prompts them for a response.

Direct Command
An operator-initiated event that causes a change or action within the access control system.

Driver
The service that establishes the connection between the DNA Fusion application and the field controllers to manage system settings and system events.

Event
An activity or transaction that the system recognizes and logs in the Events Grid.

Explorer
Synonymous with browser. See Browser on page A-1.

Facility Code
A numeric code stored in each access credential that uniquely identifies the facility at which the card is valid.

Hardware
The physical field devices that comprise the access control system, such as controllers, subcontrollers, and card readers.

Host
The machine on which the driver generally resides, such as a client.

Hue
The shade or tint of a color.

Input Point
The connections on a subcontroller that sense whether a circuit is open or closed and monitor the status of a hardware device, such as a motion detector or request-to-exit (REX) button. Also referred to as a monitor point.

Masking
Hiding or suppressing an alarm that the operator does not wish to be visible.

Monitor Point Group (MPG)
A collection of monitor points, or inputs, that are managed as a group.

Operator
A person with access to an access control application, such as DNA Fusion or Fusion Web. The administrator is also an operator; however, they do not share the same responsibilities or permissions.

Output Point
The connections on a subcontroller that act as a switch controlled by the SSP controller. They are typically used to control strikes (locks), but can also control elevators, lighting, etc. Also reffered to as a control point.

Personnel Group
A logically organized set of cardholders that shares one or more default access levels.

Privileges
The permissions assigned to an operator profile that determine what actions the operator can perform in the access control application. Privileges must be configured in DNA Fusion.

Reader
A device that reads the encoding on a card or badge to process an access request.

Ribbon
A user interface element (and standard Microsoft convention) that contains a set of contextual toolbars to help the operator navigate the application and locate specific controls or commands.

Saturation
The intensity or purity of a color.

Save
An operator action that records new or updated information in the database.

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 operator-initiated commands. Typically used to define Monitor Point Groups.

Security System Processor (SSP)
Synonymous with panel and controller. See Controller on page A-2.

Server
A computer or device on a network that processes requests and delivers data to client machines.

Site Bindings
A binding that defines the ports on which the Flex API application will accept communication.

Subcontroller
One of a series of circuit boards that communicates information about field devices upstream to the SSP controller.

Time Schedule
A predetermined time block that is associated with days and holidays to control access, trigger an event, and manage automated operators in the the system.

Tooltip
An message that appears when the cursor hovers over an item in the application interface. In Fusion Web, tooltips are used to display a cardholder photo when the operator hovers the cursor over a cardholder event in the Events Grid.

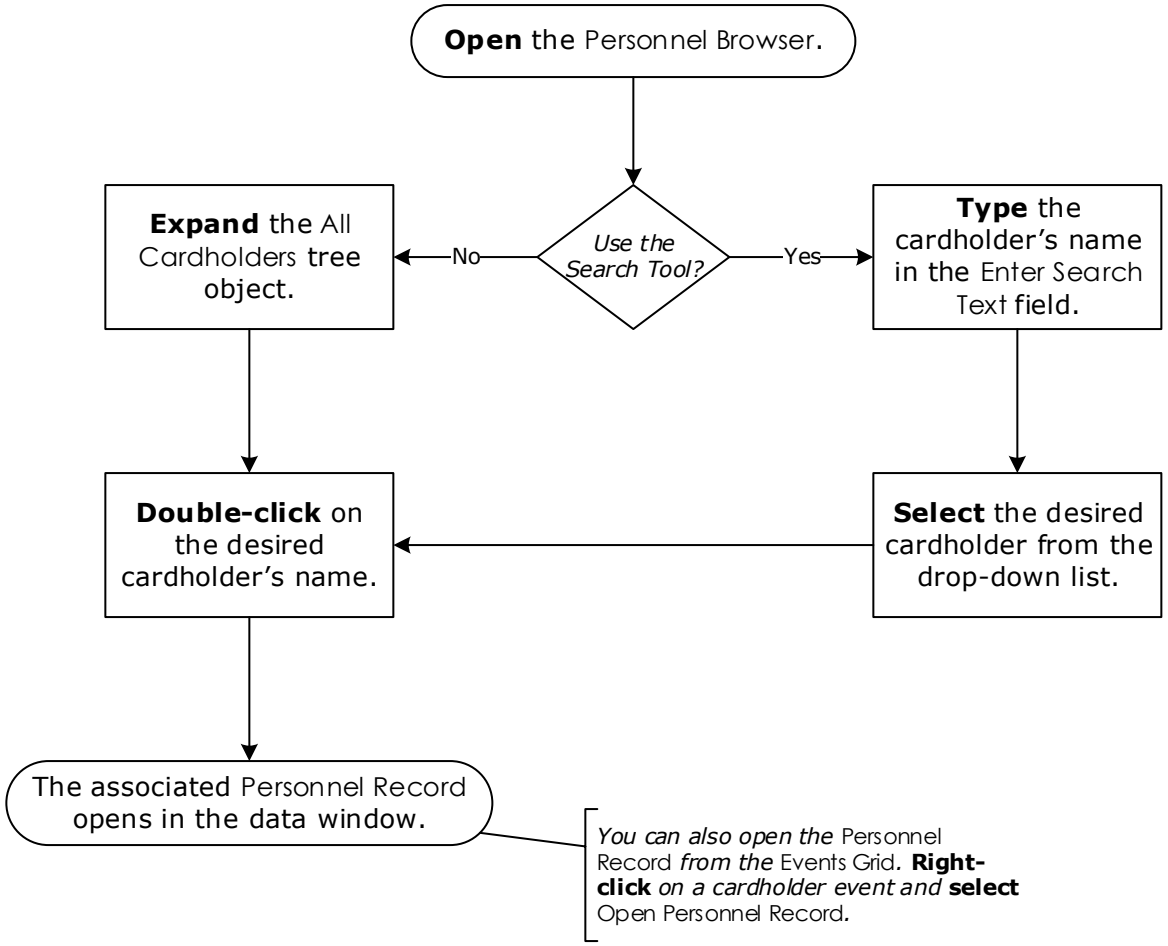
Workstation
A computer connected to the Fusion Web application that the operator uses to manage and monitor the access control system. Also referred to as a station or client.

This Page Intentionally Left Blank

Process Diagrams B

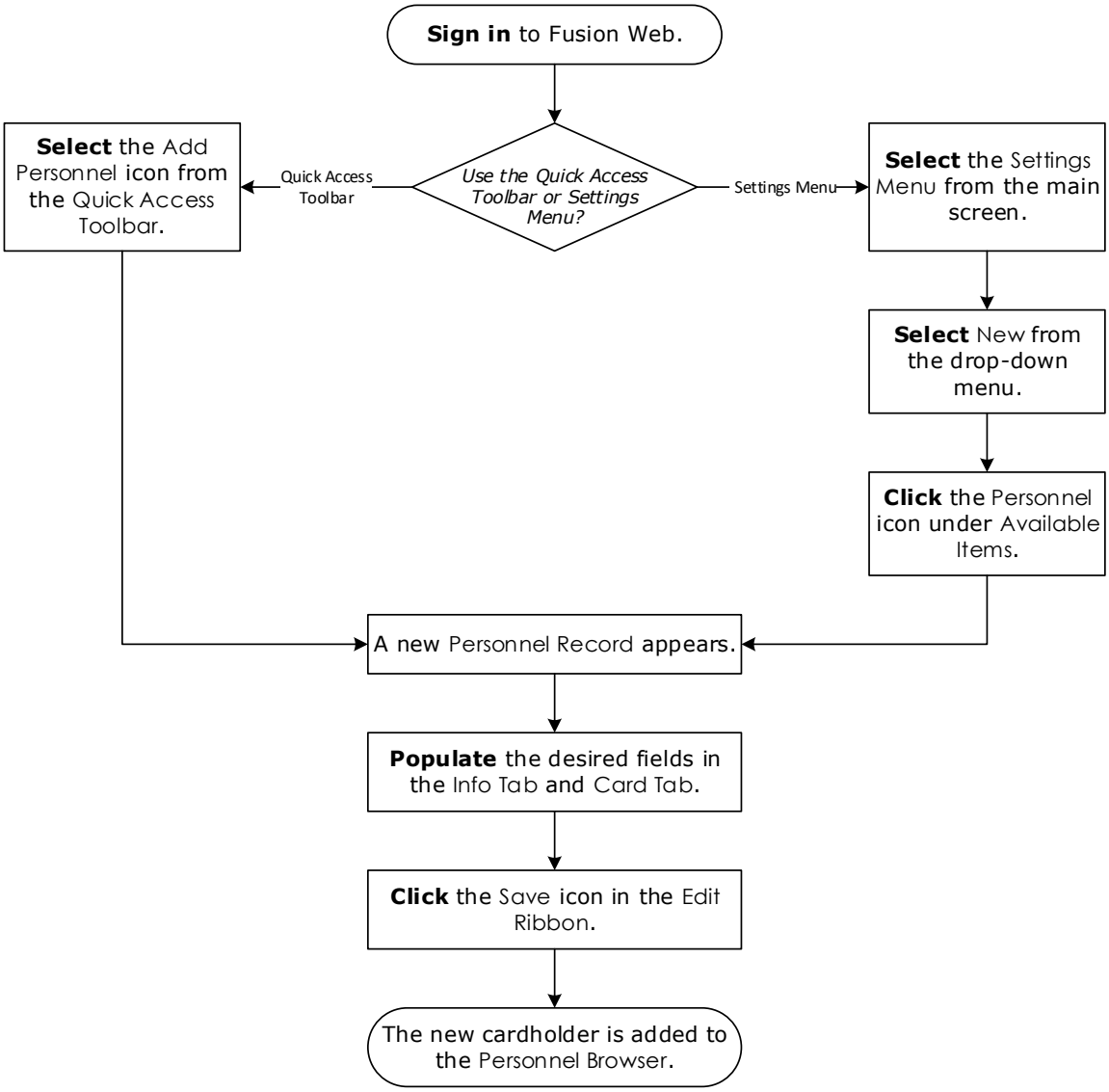
Opening a Personnel Record

See page 2-3 for more information.



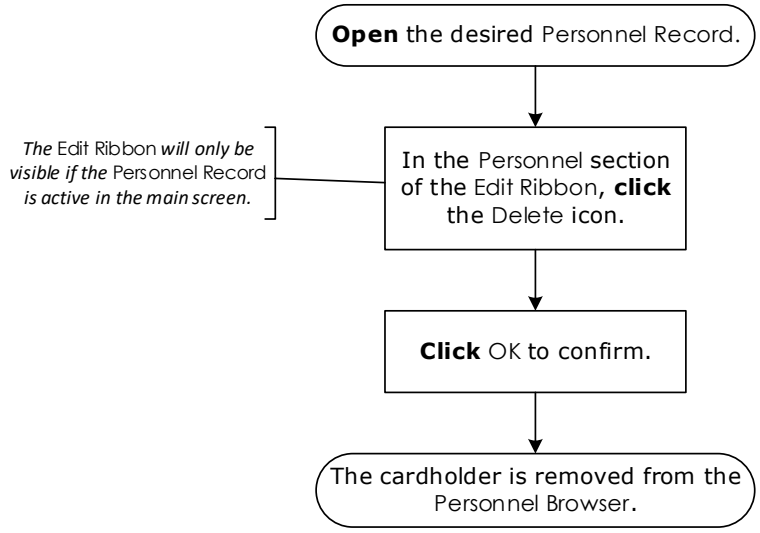
Adding a Cardholder

Add cardholders by using the Quick Access Toolbar or Settings Menu. See page 2-4 for more information.



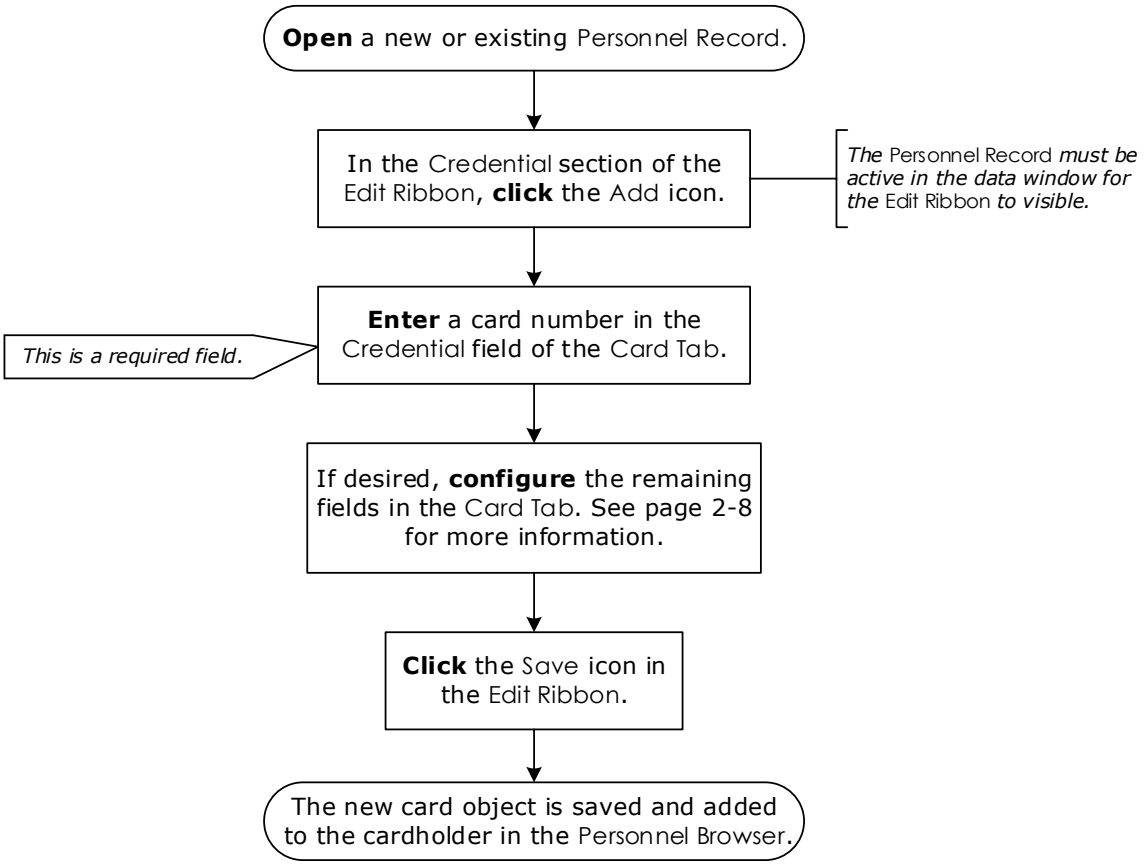
Removing a Cardholder

See page 2-4 for more information.



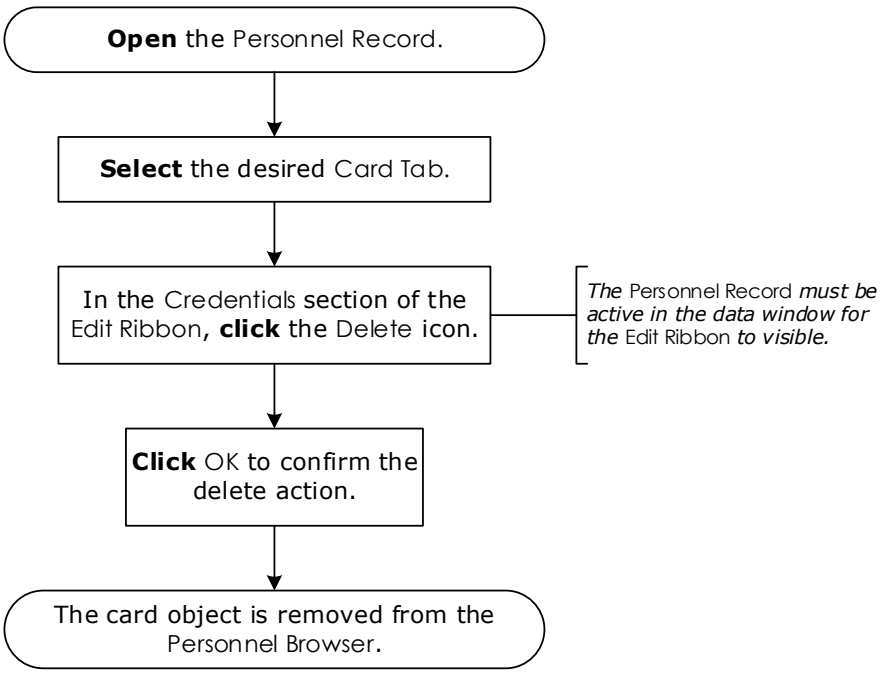
Adding a Card

See page 2-5 for more information.



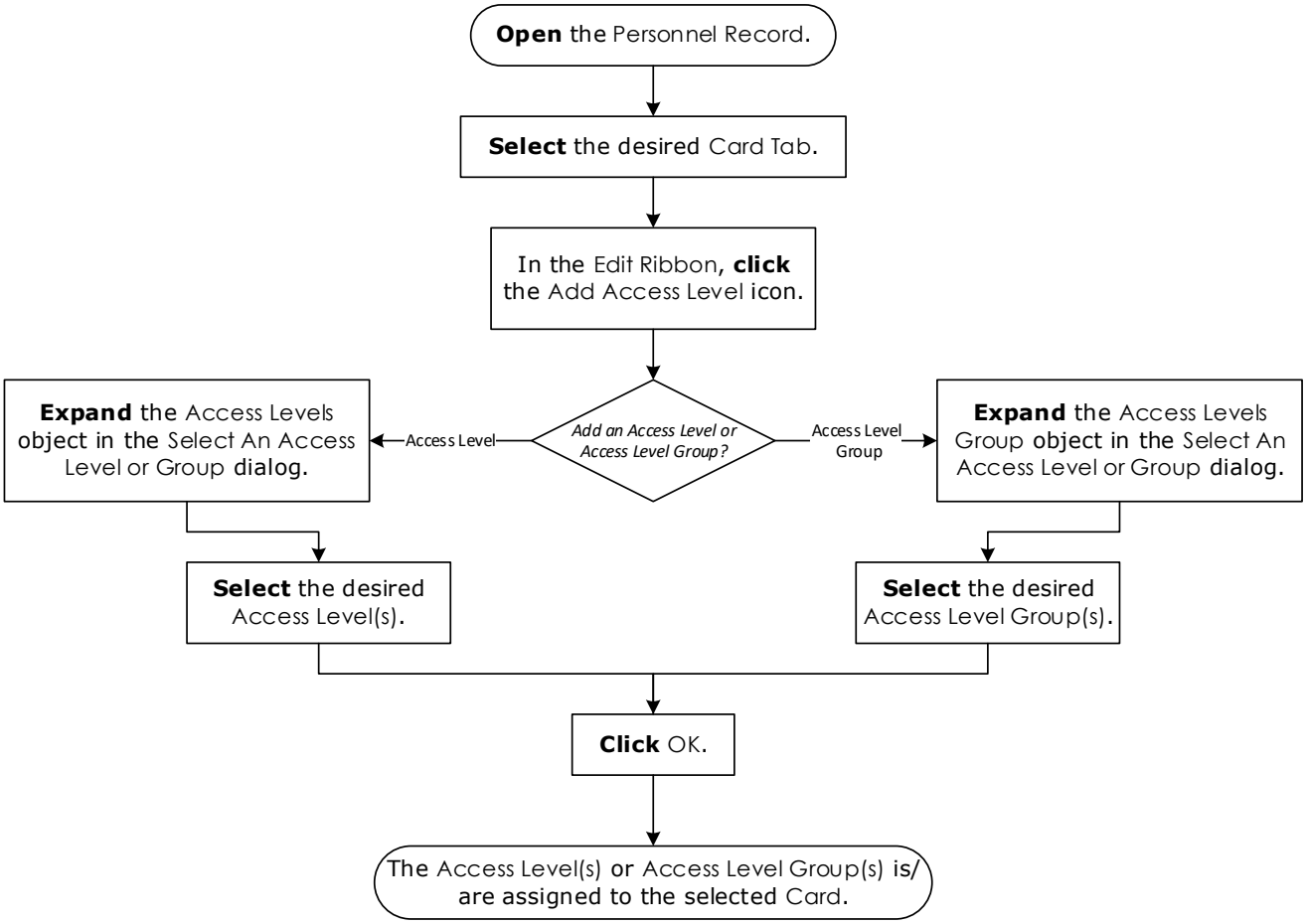
Removing a Card

See page 2-5 for more information.



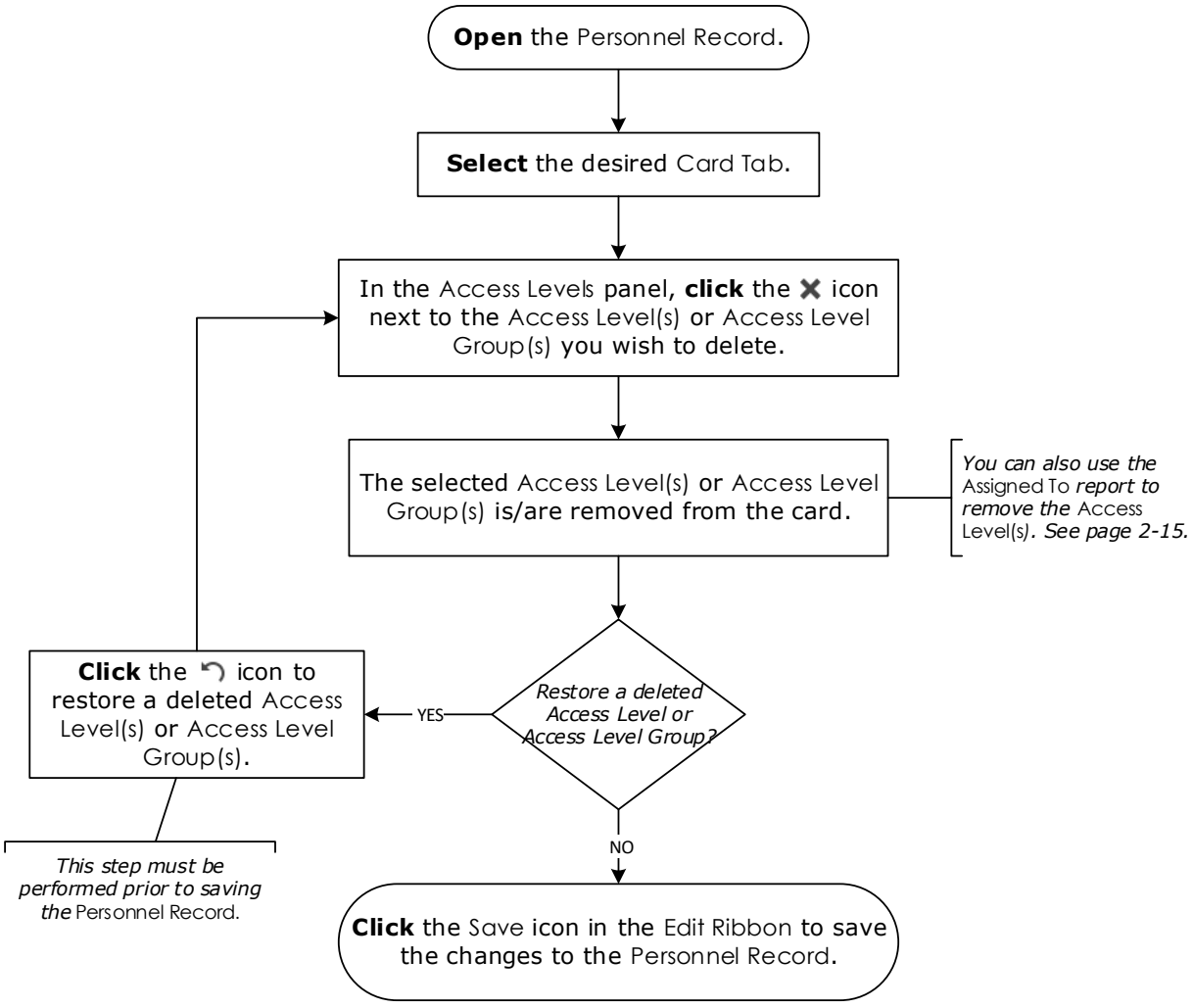
Adding an Access Level to a Card

See page 2-5 for more information.



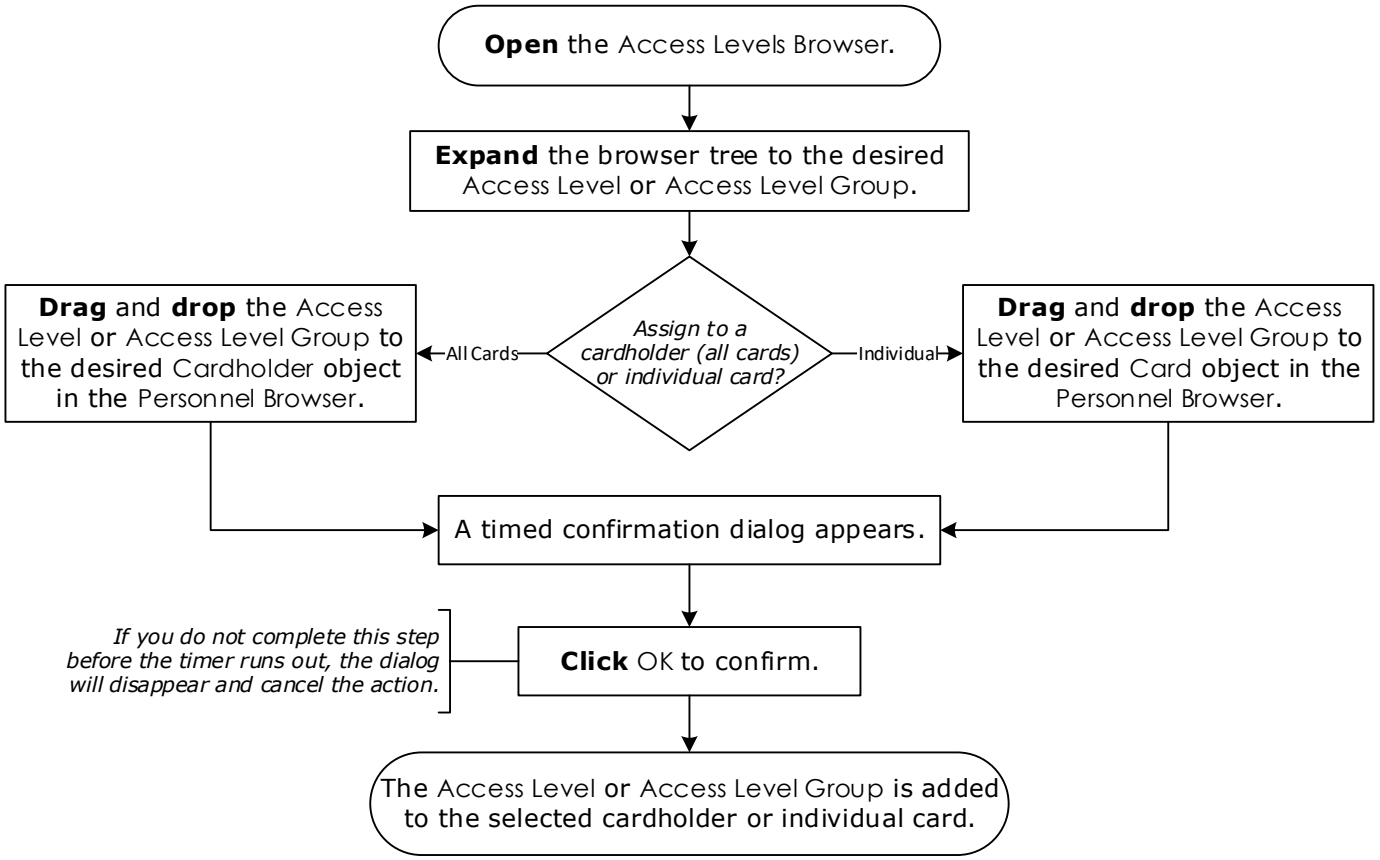
Removing an Access Level from a Card

See page 2-12 for more information.



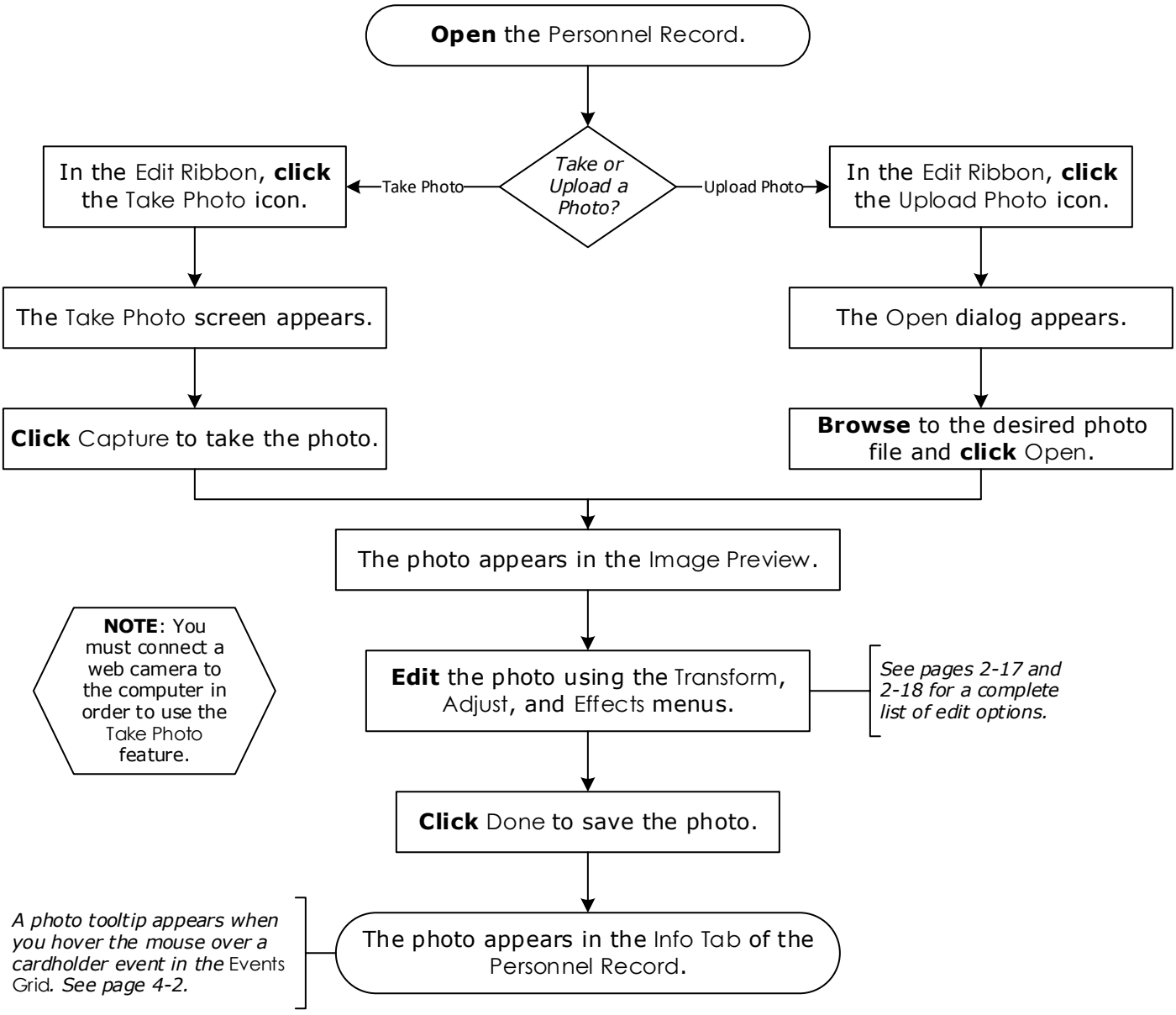
Assigning Access Levels from the Access Levels Browser

See page 2-14 for more information.



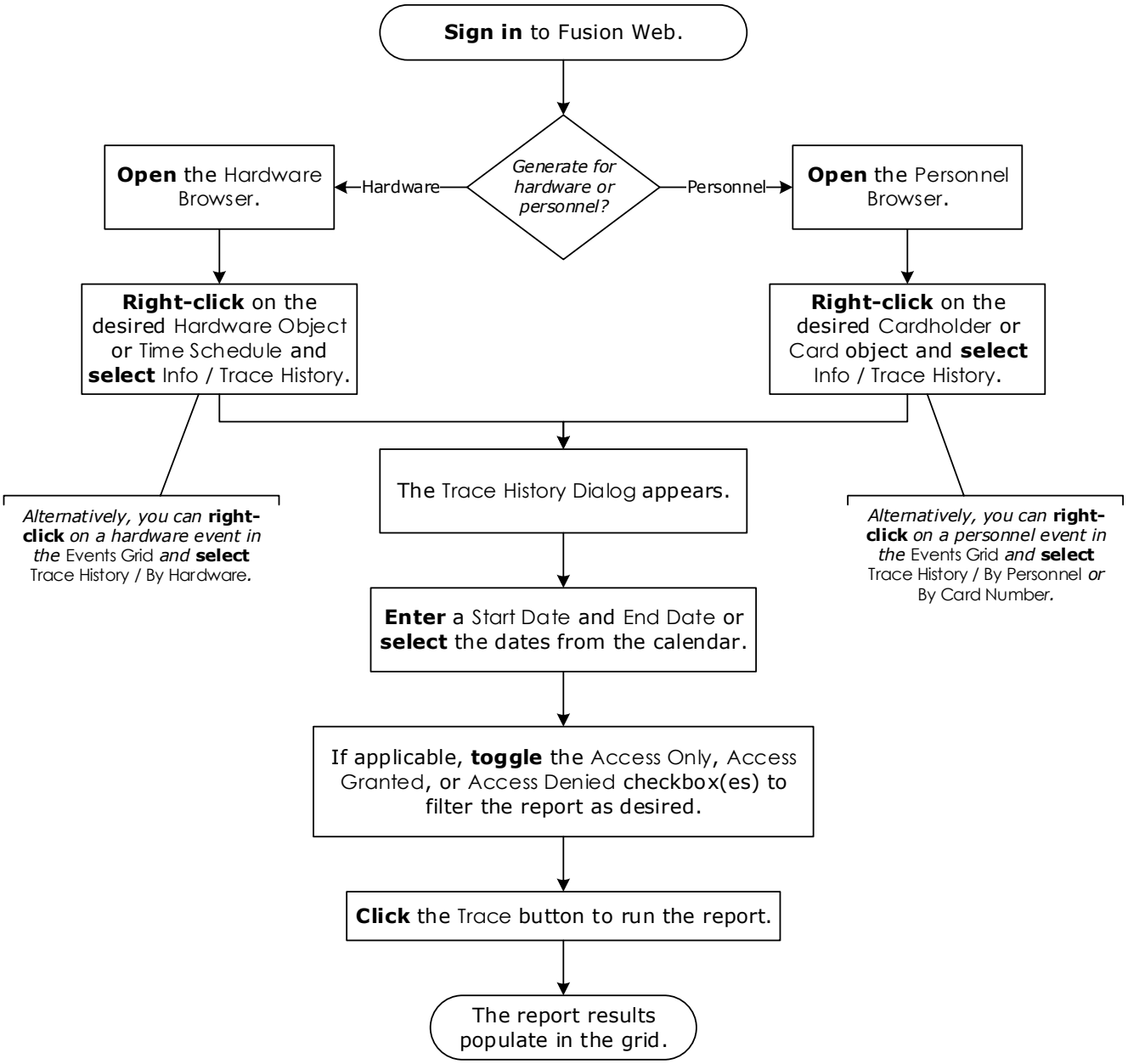
Taking or Uploading a Photo

See page 2-17 for more information.



Generating a Trace History Report

You can generate a Trace History report for personnel or hardware. See pages 2-15 and 3-7 for more information.



This Page Intentionally Left Blank


OPEN OPTIONS®
ACCESS TECHNOLOGY