Bosch Manual

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

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

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

Warranty

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

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

Open Options Software License Agreement

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

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

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

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

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

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

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

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

Table of Contents

This Page Intentionally Left Blank

Introduction 1

In This Chapter
√ Requirements √ Supported Panel Models

This section is designed to introduce you to DNA Fusion™ and the Bosch Mode 2 integration.

How This Section is Organized

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

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

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

Chapter 3, "DNA Fusion Configuration," provides information on configuring Bosch hardware in the DNA Fusion application.

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

Icons and Conventions Used in This Manual

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

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

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

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

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

This Page Intentionally Left Blank

DNA Fusion/Bosch Overview

DNA Fusion can serve as the primary or secondary monitoring application for the Bosch Mode 2 alarm panels with a single interface for displaying and monitoring your intrusion detection system.

Available with DNA Fusion version 7, the Bosch Mode 2 integration features a clean user interface and simple configuration as well as a broader range of support. Operators can continue to receive alarm panel events and arm/disarm zones in DNA Fusion, but can also take advantage of extended capabilities such as programming users within the panel and controlling points from the graphics maps.

Minimum Requirements

The DNA Fusion and Bosch Server can reside on a single Windows workstations as well as on independent workstations or VM sessions.

Parameter	Minimum Software Requirements
Server Operating System	Win 7 Pro 32/64 bit, Win 8 SP1, Win 8/8.1, Win 10, Win 2012/16/19 Server
Client Operating System	Win 7 Pro 32/64 bit, Win 8 SP1, Win 8/8.1, Win 10, Win 2012/16/19 Server
DNA Fusion Version	7.0.0.1 or higher
Bosch Products	B Series G Series (B9512G and B8512G)
Bosch Firmware Version	v3.03.014
• Requires the Open Options Bosch Alarms Integration license	

The Bosch alarm panel can monitor multiple sites with each site consisting of multiple zones. A zone can consist of a single alarm/monitoring point, such as glass break, or may include multiple monitor points, such a numerous glass breaks and motion detectors placed in a contiguous area. If one point goes in to an alarm state within the zone, then the user is notified that the zone is in alarm.

The Bosch panel can also be used as a dialer with alarm notifications being sent to a monitoring station for first responder notification.

The Bosch panel must be configured via the Bosch remote programming software prior to the integration with DNA Fusion.

Supported Bosch Panel Models

Model	Areas Supported	Points (Zones) Supported
B6512	6	96
B5512	4	48
B4512	2	28
B9512G	32	599
B8512G	8	99

Fusion-Bosch Integration 2

In This Section
√ Bosch Installation and Configuration √ Bosch Integration Installation √ Service Permissions

The Bosch integration is supported by DNA Fusion version 7.0.0.1 or higher. The integration requires the proper licensing to be in place prior to the installation of the integration software.

DNA Fusion™ interfaces with the Bosch Mode 2 alarm panels allowing for the interaction with both access control and intrusion detection from a single, common user interface. Alarms and transactions from the Bosch panels are blended seamlessly into DNA Fusion, becoming part of the standard Fusion alarm monitoring and reporting system. Bosch points and zones can be armed and disarmed directly from within DNA Fusion. The result is an access control system that is ideally suited to meet the needs of any organization.

Features and Functionality

- DNA Fusion™ can monitor single points and multiple zones status received from the Bosch panels
- Receive alarm panel events in DNA Fusion Event Manager, Alarm Grid or both
- Arm and disarm zones via DNA Fusion through host-based macros or direct control commands
- Monitor access control and intrusion detection from single user interface
- The Bosch panels can function as a dialer
- DNA Fusion auto discovers Bosch configured panels, points, areas and zones
- Add and control Bosch zones and areas through Fusion's graphic maps
- Configure users (PIN's) to provide arming and disarming capability at keypads

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

> ! *SSL encryption must be enabled on the Bosch panels.*

The following steps should be performed to complete the integration:

1. **Install** the Bosch components.
2. **Configure** the Bosch system through the Remote Programming Software (RPS).
3. **Run** the DNA Fusion-Bosch Integration application.
4. **Add** the Bosch panel(s) in DNA Fusion.
   See Chapter 3: DNA Configuration of more information.
5. Auto discover the areas, points and outputs.

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

This Page Intentionally Left Blank

Bosch Installation and Configuration

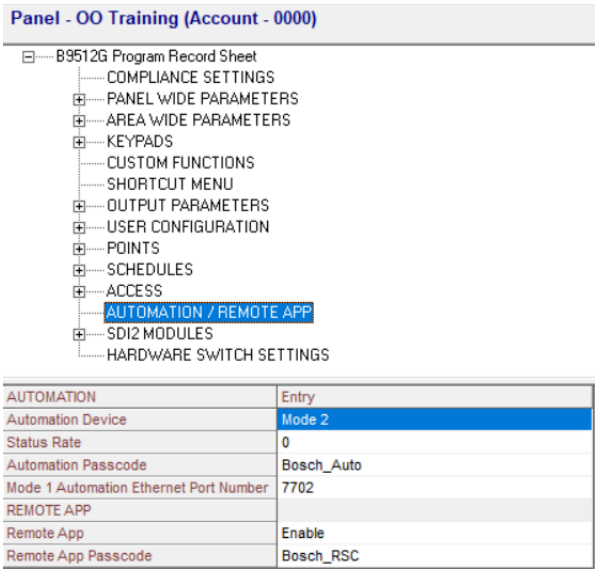
The following tasks must be completed before the DNA Fusion-Bosch integration will function properly.

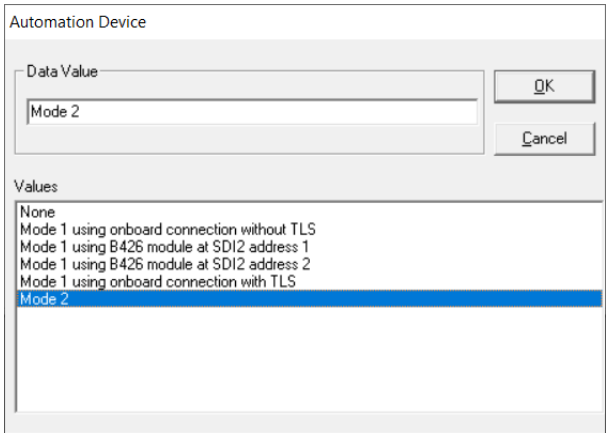
Installation and Configuration Steps

1. **Install** the Bosch Hardware including any keypads.
2. **Assign** an IP address to the unit.

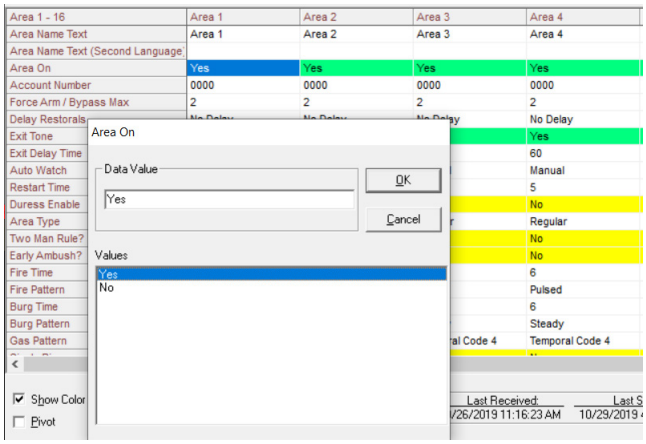
   This step can be configured through the keypad, see the Bosch documentation for more information.
3. **Configure** the system using the Bosch Remote Programming Software (RPS).

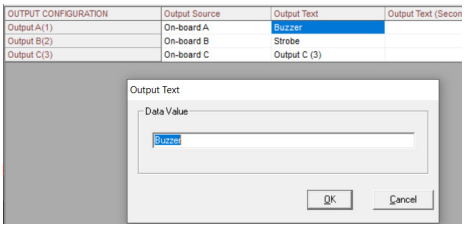
   This tool is used to configure the alarm panel as well as define areas. This step may require connection to the alarm panel via the supplied USB cable. The RPS Hardware Key must be in place to facilitate communication with the panel.
4. From the RPS, **connect**  to the desired Panel.
5. **Program** the panel to use the Mode 2 Automation Device.





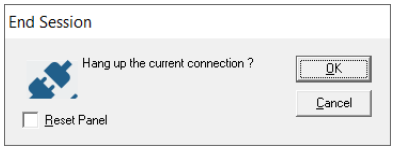
6. **Setup** the Areas in the Bosch Remote Programming Software.





7. If needed, **rename** the Outputs.
8. **Save** the information.
9. **Disconnect** from the Remote Programming Software (RPS).

   The End Session dialog will appear. If any changes have been made, **select** the Reset Panel checkbox.



NOTES:

DNA-Bosch Integration Installation

Once the Bosch equipment has been installed and configured, the DNA integration can be performed. The installation process is very straightforward and can be performed without any knowledge of the software.

1. **Obtain** the dnaFusion Bosch Install application from Open Options Technical Support.

   The setup procedure must be performed with an administrator login.

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

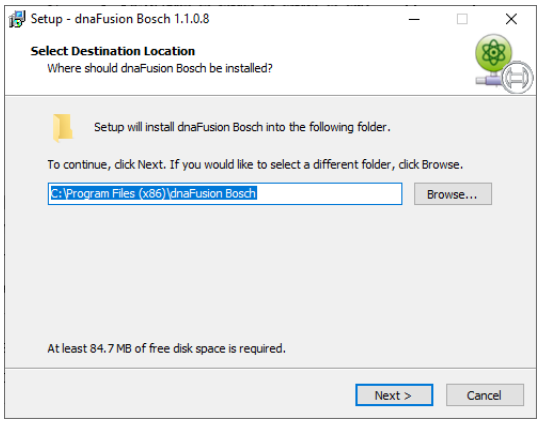
   The DNA driver and the Bosch driver need to run under the same identity. The account running the services will be used later in the installation process and should be noted for reference. For more information on DNA Fusion services, see page 2-7 and reference the DNA Fusion Technical Manual.

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

   The Introduction screen will open.

4. **Click** the Next button.

   The Destination Location dialog appears.

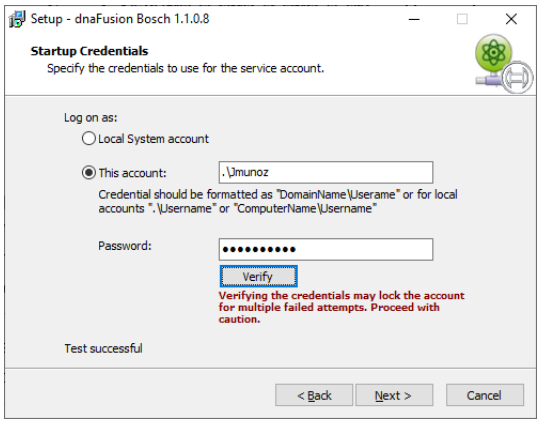


5. **Click** the Next button to continue the installation or **select** the Browse button and specify a different location.

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

   The Startup Credentials screen appears.

6. **Select** This Account, **enter** the credentials, and **click** Next.



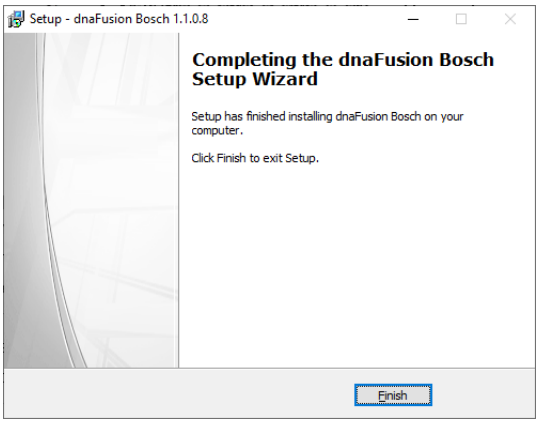
   The Bosch driver requires a service account to run the application; this account must be a local machine administrator in order to operate.

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

   The Ready to Install screen appears.

7. **Click** the Install button to start the process.
   When the installation is complete, the Install Complete screen opens.

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



9. **Configure** the Bosch panel within the DNA Fusion application.
   See Chapter 3: DNA Configuration for more information.

DNA Fusion Service Permissions

In order for the integration to function properly, the DNA Driver and COM+ objects, as well as the DNA User Group must be configured properly. This is imperative to the success of the integration.

COM+ Object

1. **Open** the Component Services menu on the server.

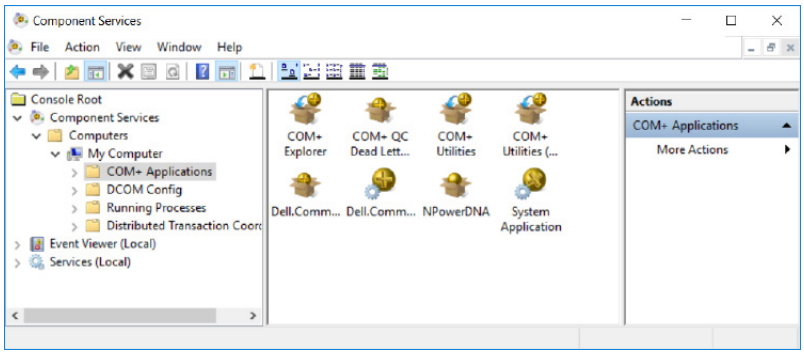
   To access Component Services, **type** the name in the Windows Start Search Bar and **select** the Component Services option from the list.

   The Component Services window opens.

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

3. **Double-click** the My Computer icon and **open** the COM+ Applications folder.

   The COM+ Objects dialog appears.



4. **Right-click** on the NPowerDNA object and **select** Properties.

   The NPowerDNA Properties dialog opens.

5. **Select** the Identity tab, **verify** This user is selected and the User and Password fields are completed.

   If the objects permissions have not been configured, **enter** a local machine Administrative login information and **click** the OK button.

   The DNA Fusion Bosch service will require the same information. This also applies to the DNA Driver (DNAdrvr32) service.

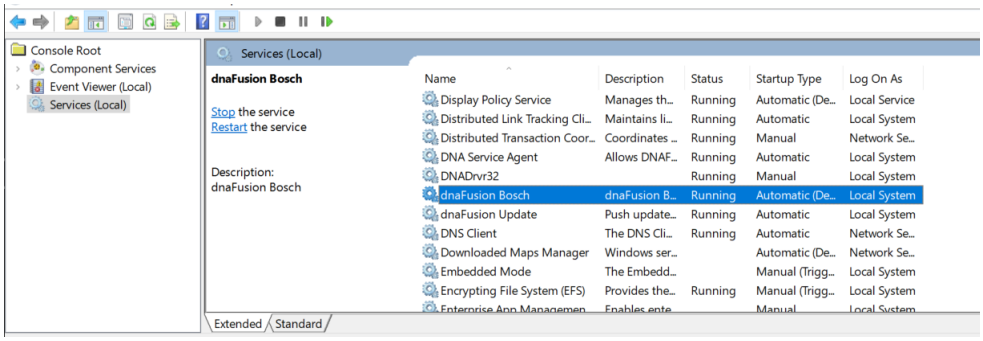
6. **Click** the OK button.

DNA Fusion Driver Service

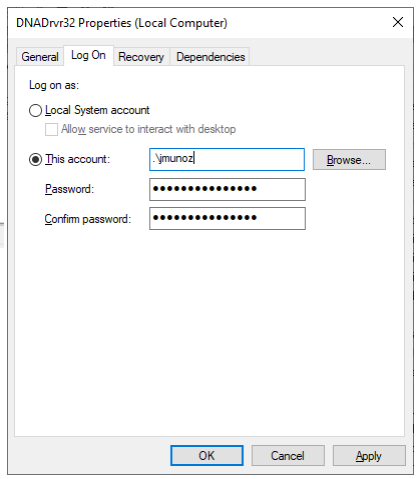
1. From the Component Services dialog, **select** the Services option or **open** the Services window.

   The Services dialog will populate.

2. **Locate** the DNADrvr32 service.



3. The DNADrvr32 Properties dialog will open.

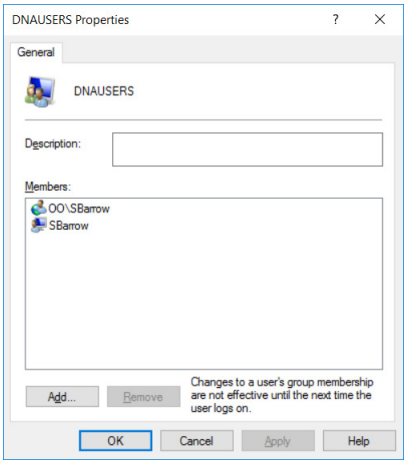


4. **Select** the Log On tab and **verify** the user configuration.

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

DNA Fusion User Group

1. **Right-click** on My Computer or This PC and **select** Manage from the menu.
   The Computer Management dialog appears.
2. **Expand** the Local Users and Groups option.
3. **Select** the Groups folder and **right-click** on the DNAUSERS group.
4. **Select** Add to Group from the menu.
   The DNAUSERS Properties dialog appears.
5. **Verify** the service account is listed in the dialog.
   If the account is not listed, **click** the Add button and **enter** the account's information.



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

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

DNA Fusion Configuration 3

In This Section
√ Adding the Bosch Panel to DNA Fusion √ Discovering Areas and Outputs √ User and Level Creation

The Bosch B and G series intrusion panel integration enables DNA Fusion clients to monitor and interact with the Bosch B and G series intrusion panels. The Bosch integration is a licensed feature. If the Bosch option is unavailable, contact Open Options Technical Support.

Adding the Bosch Panel to DNA Fusion

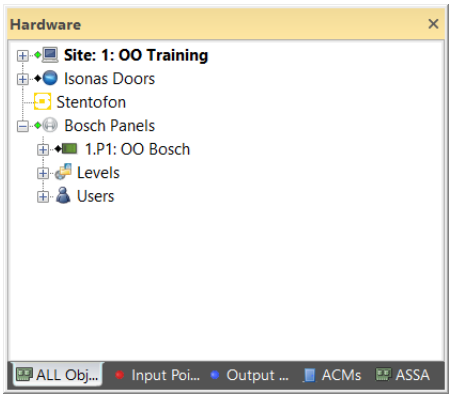
Once the Bosch equipment has been installed and the integration complete, the panel(s) will need to be added to DNA Fusion.

1. With DNA open, **select** the Hardware Browser 

button on the Standard toolbar.

   The Hardware Browser opens.

   The Bosch Panels option must be green to proceed to the step. This diamond icon represents the state of the dnaFusion Bosch driver.



Status Indicators:

- Green Diamond - The dna Fusion Bosch driver is running
- Black Diamond - The dna Fusion Bosch driver is inactive. Verify the DNADrvr32 and dnaFusion Bosch services are running under the correct identity. See page 2-7 for more information on service accounts.

2. **Right-click** on the Bosch Panels option and **select** Add Bosch Panel from the menu.

   The Bosch Panel Properties dialog will open.

3. **Enter** a Name for the Bosch Panel.
4. **Enter** the panel's IP Address.

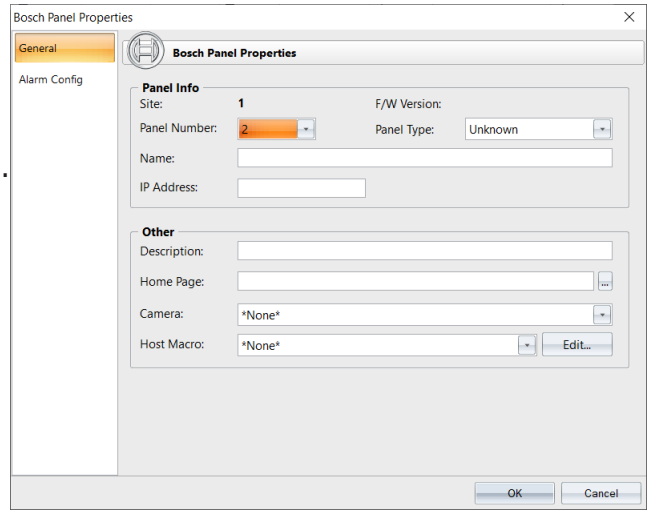
   This was configured during the panel programming.

5. If desired, **enter** a Description and **select** a Home Page.
6. If desired, **select** a Camera from the drop down list.
7. **Click** the OK button.

   The Bosch Panel is added to the Hardware Browser.

8. **Right-click** on the Bosch Panels option.
9. **Select** Discover Configuration from the menu.

   The Hardware Browser will auto populate the Bosch programmed areas and outputs into the DNA Fusion system.



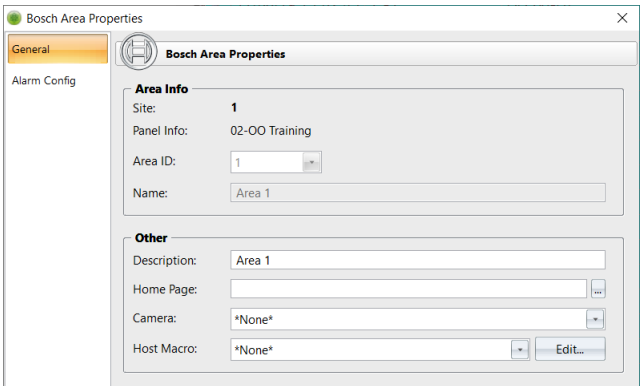
This Page Intentionally Left Blank

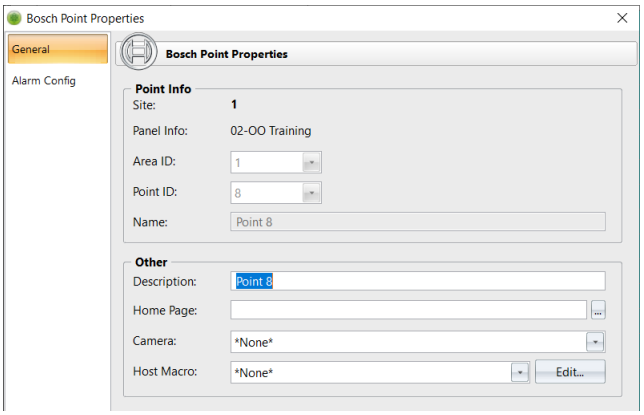
Configuring the Areas and Outputs

The Fusion software is able to upload details of the panels, zones, areas and outputs configured on Bosch panel. The current status of devices is conveniently displayed in the Hardware Browser. Once the Bosch panel has been discovered in DNA Fusion, the area and output settings can be configured.

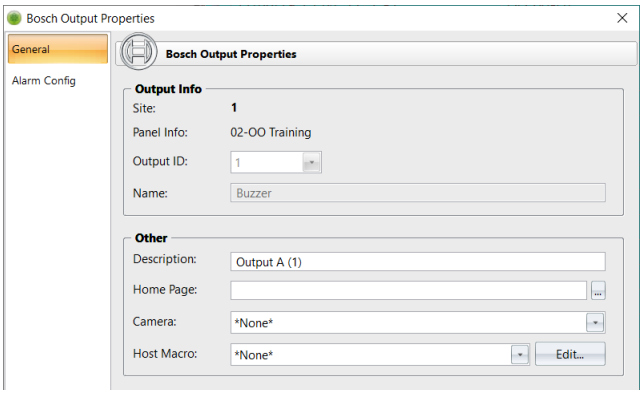
1. From the Hardware Browser, **right-click** on the Bosch Area, Point or Output and **select** Properties from the menu.

   The Bosch Object Properties dialog opens.





   Depending on the object selected, the properties dialog will vary slightly.



2. If desired, **enter** a Description for the point.

   The default name was pulled from the RPS configuration. The Description will appear in the Events Grid as well as any references to the point. The Description is auto-populated when the device is auto-added.

3. If desired, **select** the correct Home Page using the Browse button.

4. If needed, **select** a Camera from the drop-down list.

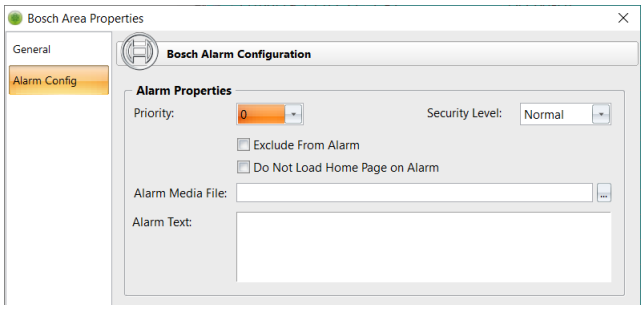
   Once selected the camera will be associated with the point and will provide viewing capabilities from the Event and Alarm grid.

5. If configured, **select** a Host Based Macro from the drop-down list or **click** the Edit button.

   If the Edit option is selected, the Host Based Macro Editor will open. For more information on Host Based Macros, see Chapter 10 the DNA Fusion User Manual.

6. **Select** the Alarm Config option from the menu on the left.

   The Alarm Config dialog opens. This dialog is common to all objects.



   Priority - If selected, overrides the default event-specific Alarm Priority set in DNA / Administrative / Alarms and Events / Logging. The alternate ID will be displayed in the Alarm Grid.

   Security Level - Category designation. Allows administrator to restrict operator use. See page 4-8 in the User Manual for more information.

   Do Not Load Home Page - If the associated point goes into alarm, the Home Page will not load.

   Exclude From Alarm - If selected, the point will not be displayed in the Alarm Grid. Events will still be recorded in the Event Grid.

   Alarm Media File - Audio file to be played when the associated door goes into alarm.

   Alarm Text - Additional text to be displayed with the alarm reason when the associated door goes into alarm.

7. **Click** the OK button to save the object changes.

NOTES:

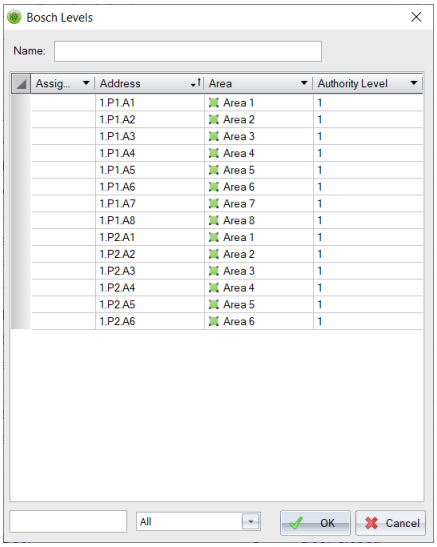
Creating Levels

A Bosch level is an area combined with an authority level that, when assigned to a cardholders, determines where the cardholder has access within the Bosch system.

The Address and Area Number identifies the areas of the Bosch security system If selected, the assigned cardholders will have access to the areas. The authority level determines what system functions the passcode can access. The authority level is configured in the Bosch Remote Programming Software (RPS).

1. From the Hardware Browser, **right-click** on the Levels option under the Bosch header and **select** Add New Level from the menu.

   The Bosch Levels dialog opens.

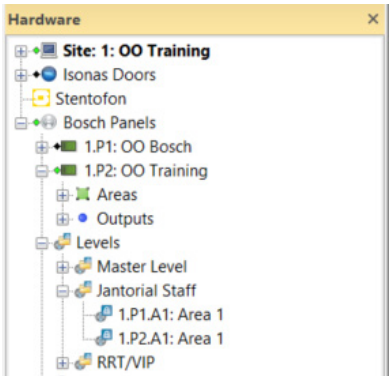


2. **Enter** a Name for the global access level group.
3. **Select** the Assigned column next to the desired areas.

   A ✚ appears in the Assigned column.
4. **Select** the user's Authority Level.

   The Authority level determines the features and functions the user can access in the Bosch system. Authority levels are configured in the RPS.
5. **Click** the OK button to save the level.

   The level is added to the Hardware Browser.

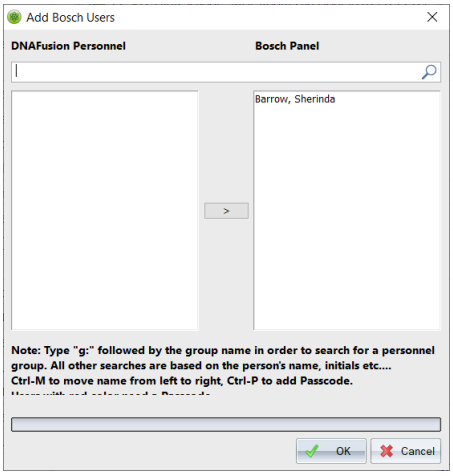


Creating Users

A Bosch user must be present in the DNA Fusion system to be added as a user under the Bosch header. If the user does not have an associated Passcode, the system will prompt for a passcode prior to adding the user.

1. From the Hardware Browser, **right-click** on the Users option under the Bosch header and **select** Add/ Remove Bosch Users from the menu.

   The Add Bosch Users dialog opens.

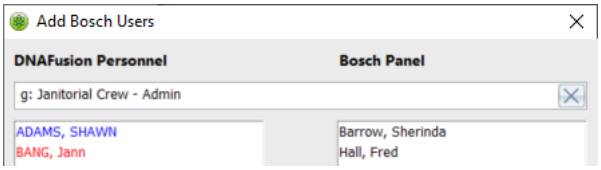


2. **Enter** the Users name and **click** the Search button.

   Users can also be added by Personnel Group. This provides a simple method to add multiple users in a group to the Bosch panels.

   To search a Personnel Group, **enter** the following:

   g: Name of Personnel Group and **click** the Search button.



   The DNAFusion Personnel will appear in the window

   The Ctrl or Shift keys may be used to select multiple users.

   Users with a Passcode will be blue and may be moved to the Bosch Panel pane by **selecting** the arrow or **double-clicking** the user. If the user does not have a Passcode, they will appear red in the dialog. These users will need to be assigned a Passcode prior to assigning the user.

3. If needed, **add** a Passcode to the User(s).

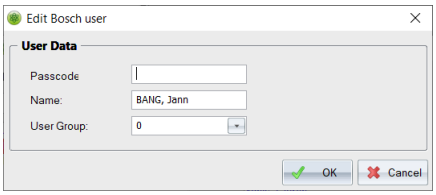
   Passcodes may be set for multiple user using the Ctrl or Shift keys.

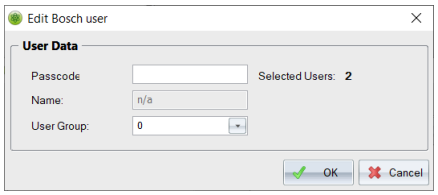
   Right-click on the User(s) and **select** Add Passcode.

   Or

   Press Ctrl P on the keyboard.

   The Passcode dialog opens.



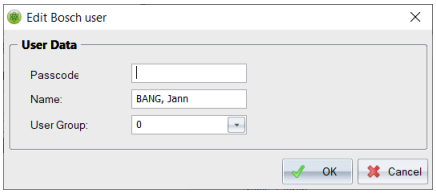


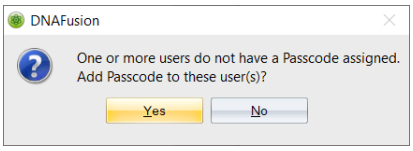
4. To add the user to the Bosch Panel, **right-click** on a red User and **select** Add Passcode.

   The Edit Bosch User dialog opens.

   Or

   Double-click on a red User and **click** Yes to open the DNAFusion Passcode dialog.



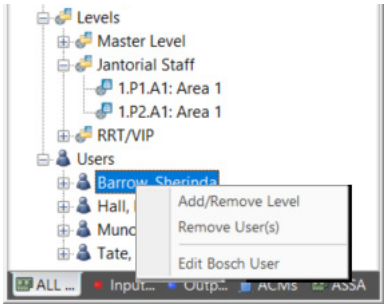


5. **Enter** the user(s) Passcode and **click** the OK button.

   The user is added to the Bosch Panels pane.

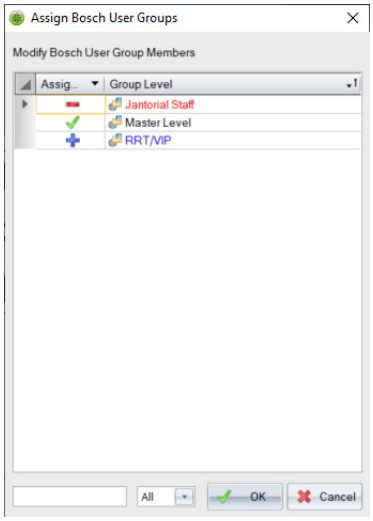
Assigning User Group Levels to Users

Once users and levels have been created, a user will be assigned a level that determines access and functions.



1. From the Hardware Browser, **right-click** on the User under the Bosch header and **select** Add/Remove Level the menu.

   The Assign Bosch User Groups dialog opens.

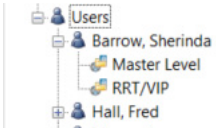


2. **Select** the Assigned column for the desired User Group Level.

   A ✚ will appear in the Assigned column. Existing User Groups will have a ✓ in the Assigned column.

3. **Click** the OK button.

   The User Group Level(s) is assigned to the User.

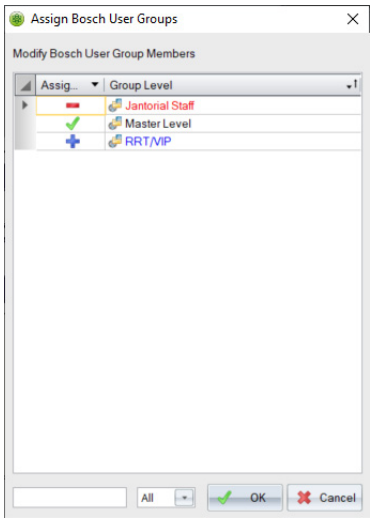


Removing User Group Levels from Users

To remove a previously assigned User Group Level:

1. From the Hardware Browser, **right-click** on the User under the Bosch header and **select** Add/Remove Level the menu.

   The Assign Bosch User Groups dialog opens.



2. **Select** the Assigned column for the desired User Group Level.

   A ▬ will appear in the Assigned column.

3. **Click** the OK button.

   The User Group Level(s) is removed from the User.

This Page Intentionally Left Blank

Bosch in DNA Fusion 4

In This Chapter
√ Controlling the Bosch Hardware √ Generating Reports √ Alarm Handling

A Bosch alarm panel can monitor multiple sites with each site consisting of multiple areas. An area can be a single alarm/monitoring point such as a glass break, or it can include input points such as glass breaks, motion detectors, etc. (usually in a contiguous area). If one point goes into an alarm state within the area, DNA Fusion will generate an alarm to notify the operator.

The hardware browser also offers varies control options. It provides the ability to arm and disarm the Bosch panel directly from DNA Fusion. There are also a number of different hardware features as well as the ability to generate Trace History and "Who Has Access" reports on the fly.

The Hardware Browser

The Hardware Browser is an explorer window that consists of a hierarchical layout of the field devices that make up the system. The tree also displays the status of objects by using status indicators to the left of the tree object.

To open the Hardware Browser:

1. **Select** the Hardware icon from the Standard Toolbar.
   Or
   Select View / Explorers / Hardware from the Main Menu.
   The Hardware Browser will open.
2. **Expand** the Bosch header to view the Bosch Panels, Levels, and Users.

Driver Status Indicators:

- Green Diamond - The Bosch driver is running and all systems are good.
- Black Diamond - The Bosch driver is not running. Verify the User Account running the service.

Area, Point, and Output Indicators:

- Green Diamond - The object is currently in a normal state; i.e., closed, inactive.
  - The Bosch Panels Area Points appear with a red circle and Outputs are represented with a blue circle. The diamond icon represents the state of the object.
- Red Diamond - The object is currently in an alarm or active state; i.e., point open, output active.
  - The Bosch Panels Area Points appear with a red circle and Outputs are represented with a blue circle. The diamond icon represents the state of the object.

Area Status Indicators:

- Armed Area - The area is currently armed and will report any defined alarms.
- Disarmed Area - The area is currently disarmed and not reporting alarms. It appears with a mask over the area.

> *Hovering over an object or area will show you the status in the form of a tooltip.*

This Page Intentionally Left Blank

Bosch Panel Object Options

The Bosch integration provides the ability to control the Bosch panel as well as monitor the status of Bosch hardware through the DNA Fusion system.

1. From the Hardware Browser, select the desired Area, Point, or Output to control.
2. **Right-click** on the desired object under the Bosch header.
   The Objects context menu appears.
3. **Select** the desired Control Option.

Area Control

An area is a number of points that are grouped together so that you can control them together as one object. For example, if a Bosch system has three (3) areas – an office, a laboratory, and a classroom – the points in each of those sections could be grouped together as an area. This allows the user to arm (turn on) and disarm (turn off) individually, in groups (office and laboratory), or all together. Fire, panic, and other 24-hour areas are considered always armed.

Disarm	Turns off alarm protection for the area. No alarms will be received by DNA Fusion.
Master Arm (Instant)	Immediately turns on alarm protection for the area. With the Instant command, no entry or exit delay is provided and an alarm will occur should an entry door be opened. When an area is armed and is tripped, an alarm will be generated in DNA.
Master Arm (Delay)	Turns on alarm protection for the entire system. With the Delay command, entry and exit delays are provided. When an area is armed and is tripped, an alarm will be generated in DNA. The delay period is specified at the intrusion system.
Master Arm (Instant Forced)	Immediately turns on alarm protection for the area. With the Instant command, no entry or exit delay is provided and an alarm will occur should an entry door be opened. When an area is armed and is tripped, an alarm will be generated in DNA. The forced portion relates to points that are typically faulted when arming the area. When the point returns to the normal state after being force armed, it automatically goes to the armed state with the other points in the area.
Master Arm (Delay Forced)	Turns on alarm protection for the entire system. With the Delay command, entry and exit delays are provided. When an area is armed and is tripped, an alarm will be generated in DNA. The delay period is specified at the intrusion system. The forced portion relates to points that are typically faulted when arming the area. When the point returns to the normal state after being force armed, it automatically goes to the armed state with the other points in the area.
Perimeter Arm (Instant)	Immediately turns on alarm protection for the perimeter points and leaves the interior points turned off. No entry or exit delay is provided and an alarm will occur in DNA should an entry door be opened. Perimeter arming allows for free movement inside without setting off any interior alarms.
Perimeter Arm (Delay)	Immediately turns on alarm protection for the perimeter points and leaves the interior points turned off while providing an entry and exit delay. When an area is armed and is tripped, an alarm will be generated in DNA. Perimeter arming allows for free movement inside without setting off any interior alarms. The delay period is specified at the intrusion system.
Perimeter Arm (Instant Forced)	Immediately turns on alarm protection for the perimeter points and leaves the interior points turned off. No entry or exit delay is provided and an alarm will occur in DNA should an entry door be opened. Perimeter arming allows for free movement inside without setting off any interior alarms. The forced portion relates to points that are typically faulted when arming the area. When the point returns to the normal state after being force armed, it automatically goes to the armed state with the other points in the area.

Perimeter Arm (Delay Forced)	Immediately turns on alarm protection for the perimeter points and leaves the interior points turned off while providing an entry and exit delay. When an area is armed and is tripped, an alarm will be generated in DNA. Perimeter arming allows for free movement inside without setting off any interior alarms. The delay period is specified at the intrusion system. The forced portion relates to points that are typically faulted when arming the area. When the point returns to the normal state after being force armed, it automatically goes to the armed state with the other points in the area.
Stay 1 Arm	Stay 1 points are armed all the time. They can be used for panic, medical, and police alerts.
Stay 1 Arm (Forced)	Stay 1 points are armed all the time. They can be used for panic, medical, and police alerts. The forced portion relates to points that are typically faulted when arming the area. When the point returns to the normal state after being force armed, it automatically goes to the armed state with the other points in the area.

Point Control

A point is a individual object connected to the Bosch system. Multiple points are typically assigned to an area so that all of their protection devices combined provide for the complete protection of the premises.

When a point is unbypassed, a change in its normal state causes the panel to activate an alarm.

1. **Right-click** on the desired Point in the DNA Fusion Hardware Browser under the Area.
2. **Select** the command from the list.
   - Bypass Point - Points that are bypassed will not send alarms to DNA Fusion. A point remains bypassed until it is unbypassed.
   - Unbypass Point - When a point is unbypassed, a change in its normal state causes the panel to activate an alarm.

Output Control

An output is a device that is controlled by the Bosch system. Outputs are generally programmed for automatic control or keypad control for devices such as premises lighting, buzzer, strobes or entry gates.

When an output is activated, it is in the ON state. While deactivated outputs are OFF.

1. **Right-click** on the desired Output in the DNA Fusion Hardware Browser under the Bosch header.
2. **Select** the command from the list.
   - Activate Output - The selected output point will become active or set to the On state.
   - Deactivate Output - The selected output point will deactivate or turn Off.

Bosch Object Features

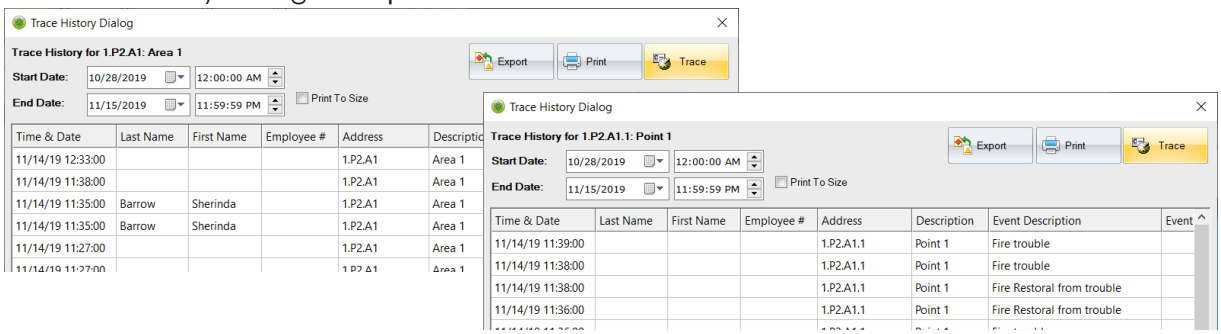
There are a number of features available for panels, areas, points, and outputs. For instance, you can see who has access to a specific area or trace the history for the selected point.

Trace History

The Trace History feature displays event transactions associated with the panel, area, point, or output for a specified date range.

1. **Right-click** on the Bosch Panel, Area, Point, or Output and **select** Trace History from the menu.

   The Trace History Dialog will open.



2. If a wider time or date range is needed, **enter** the Start and End Date/Time and **click** the Trace button.

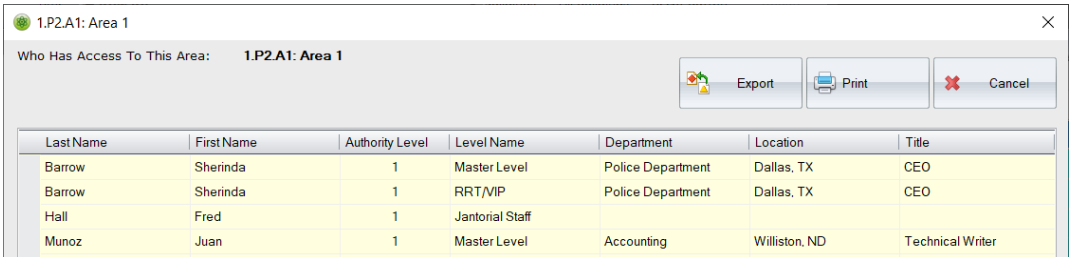
   The results can be exported or printed by selecting the appropriate button. **Select** the Print to Size checkbox to size the report so that all columns appear on the same page without forcing them to a new page.

Who Has Access

This feature allows you to generate an immediate report that details who has access to the selected area.

1. **Right-click** on the Area and **select** Who Has Access from the menu.

   The Who Has Access dialog appears.



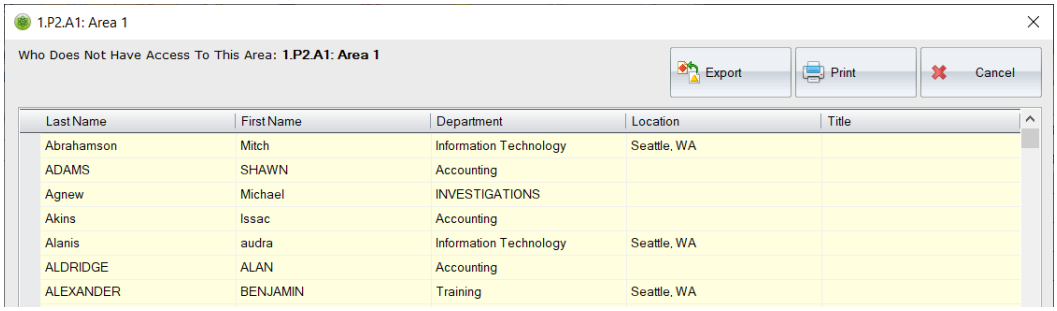
   The results can be exported or printed by selecting the appropriate button.

Who Does Not Have Access

This feature allows you to generate an immediate report that details who does not have access to the selected Bosch area.

1. **Right-click** on the ACM and **select** Who Does Not Have Access.

   The Who Does Not Have Access dialog appears.



   The results can exported or printed by selecting the appropriate button.

NOTES:

Configuring and Viewing Alarms

Alarms are configured and displayed in the same manner as all other DNA alarms. See page 14-9 in the DNA Fusion User Manual for more information on alarms.

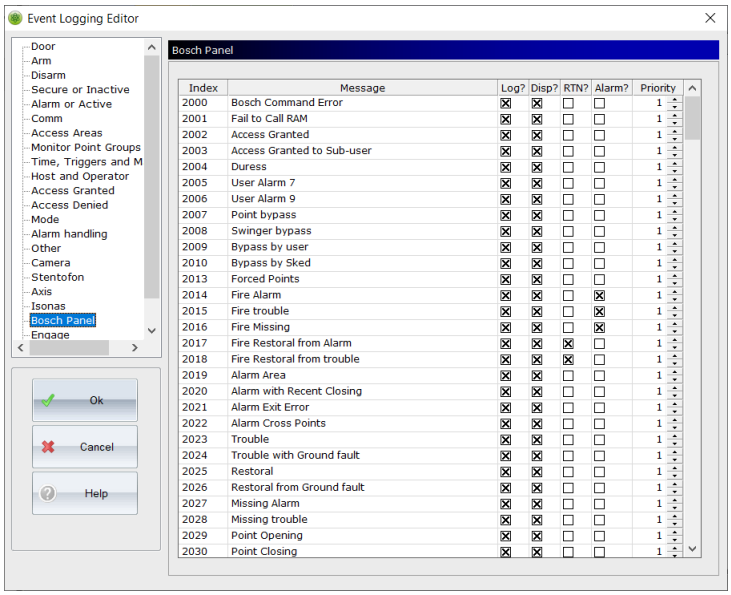
Configuring Alarm Logging

The system administrator will need configure which alarms will be reported to the Alarm gird. By default, no conditions are marked as alarms. To configure alarming properly, an Alarm event must be defined as well as a Return to Normal event.

1. **Select** DNA / Administrative / Alarms & Events / Logging from the Main Menu.

   The Alarms Routing Editor dialog box will open.

2. **Select** the Bosch item from the menu.



3. **Select** the parameters for each event for the selected object.
   - Log? - Log this event to the database.
   - Display? - Display this event in the Event Grid.
   - RTN? - Check if the event is a return to normal (RTN) from an alarm condition.
   - Alarm? - Display the event as an alarm in the Alarm Grid.

     NOTE: If an alarm event is identified, a RTN condition must be selected in order for alarm to be cleared, i.e., Area in Alarm is identified as an alarm (ALARM) condition then Area Normal would be the Return to Normal (RTN) condition.

   - Priority - Priority for the event.
4. **Click** OK to save the configuration.

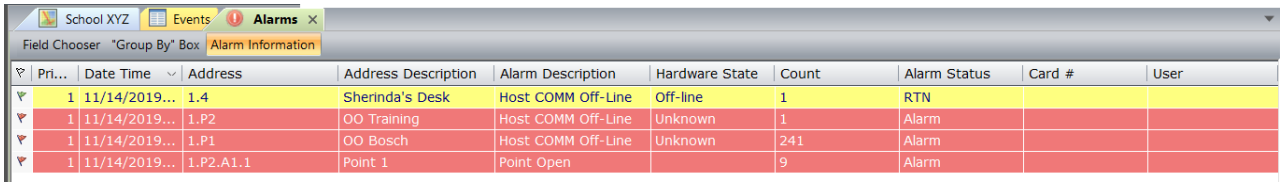
> *Bosch panel alarms can also be viewed from a graphic map. Graphic maps are flexible tools used to visually represent an external hardware platform. A map can depict various hardware states via graphic objects and provide quick access to user commands, such as alarm acknowledgement, direct control, and object properties.*

Viewing Alarms

The alarm grid is a data window comprised of a "matrix" or spreadsheet record of alarm events. There are several ways to display the alarm grid. The basic alarm grid can be viewed by a number of different methods:

- **Selecting** the Alarm button at the top of the screen in the Standard Toolbar.
- **Double-click** the Alarms status icon on the Status Bar.

Selecting the Alarm Grid (using any of the methods described) will bring it to the front of the operator interface and display any alarms that have not been acknowledged and cleared or dismissed.



Pri...	Date Time	Address	Address Description	Alarm Description	Hardware State	Count	Alarm Status	Card #	User
1	11/14/2019...	1.4	Sherinda's Desk	Host COMM Off-Line	Off-line	1	RTN		
1	11/14/2019...	1.P2	OO Training	Host COMM Off-Line	Unknown	1	Alarm		
1	11/14/2019...	1.P1	OO Bosch	Host COMM Off-Line	Unknown	241	Alarm		
1	11/14/2019...	1.P2.A1.1	Point 1	Point Open		9	Alarm		

The Alarm Grid presents the alarm information in a condensed format to conserve screen space, and organizes all pertinent data in an easy-to-read format. The grid consists of twelve adjustable columns to describe various alarm properties as well as options to toggle the Field Chooser dialog, "Group By" Box, and Alarm Information panel.

In DNA Fusion, alarms can exist in one of two states:

- Active – The point has changed from its normal state to an alarm state.
- Inactive – The point has not changed to an alarm state, or it has returned to its normal state.

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

- Unacknowledged Alarm (Alarm) – A new alarm message. A change of state was detected.
- Acknowledged Alarm (ACK) – An alarm that has been recognized by the operator.
- Cleared Alarm (Clear) – An alarm that has been acknowledged and cleared from the Alarm Grid.
- Dismissed Alarm – An alarm that has been dismissed by the operator whether or not the hardware object has returned to normal (RTN).

When handling alarms from the Alarm Grid, the operator can monitor (and must recognize) the current status of the alarm. The status is determined by a combination of the aforementioned states and conditions.

Under normal operations, the process for handling an alarm would be as follows:

Step	Action	State	Condition
1.	An alarm appears in the grid	Active	Unacknowledged
2.	The operator recognizes the alarm	Active	Acknowledged
3.	The alarm returns to normal state	Inactive	Acknowledged
4.	Operator clears alarm	Inactive	Cleared

The operator has three different avenues to work from when handling, monitoring and responding to alarms in the Alarms Grid:

- Alarms Toolbar
- Menus
  - Alarms option from the Main Menu
  - Context menu available by right-clicking on an alarm
- Keystroke / Shortcut Keys
  - Acknowledge F5 shortcut key
  - Clear F8 shortcut key
  - Custom keystroke combinations

See page 14-17 in the DNA Fusion User Manual for information on handling alarms.

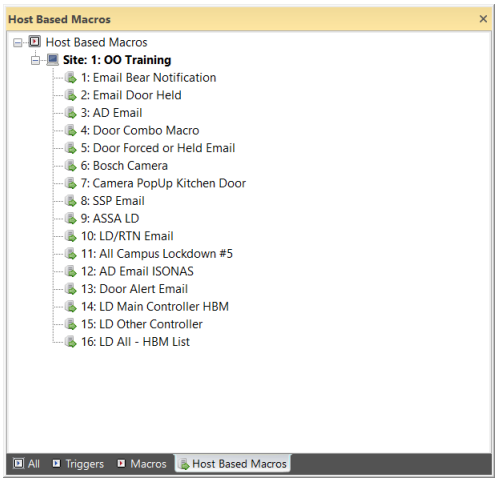
Host Based Macros

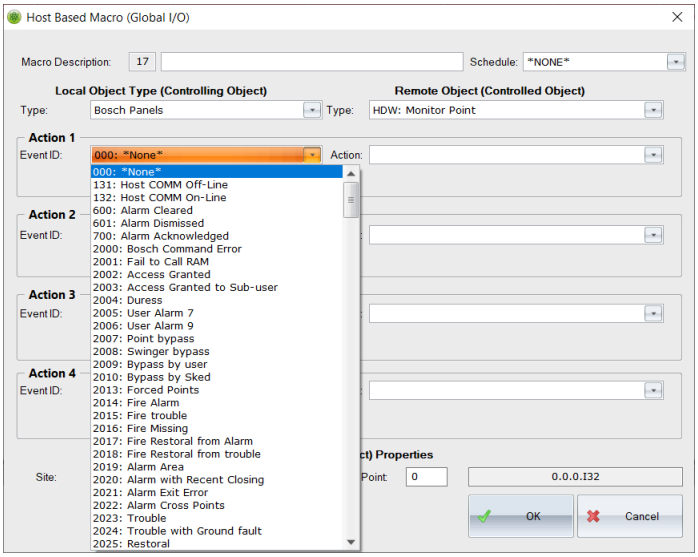
Automated operation is achieved using host based macros. For example, an area can be armed or disarmed automatically at specified times, or in response to an access-control transaction from a specified card holder, making the process of arming the system and locking doors as easy as swiping a card.

Host Based Macros allows for cause and effect relationships between points controlled by different controllers that wouldn't be possible with conventional trigger-macro configurations. For more information on Host Based Macros, see page 10-13 in the DNA Users Manual.

1. With the Triggers & Macros Browser open, **select** the Host Macros tab at the bottom of the browser.
2. **Right-click** on the Host Based Macros object in the browser and **select** Add Host Macro.

   The Host Based Macros dialog will appear.





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

   This description will appear in a drop-down menu later when the controlling object is configured.
4. **Select** the Bosch Panels option from the Local Object Type (Controlling Object) drop-down menu.

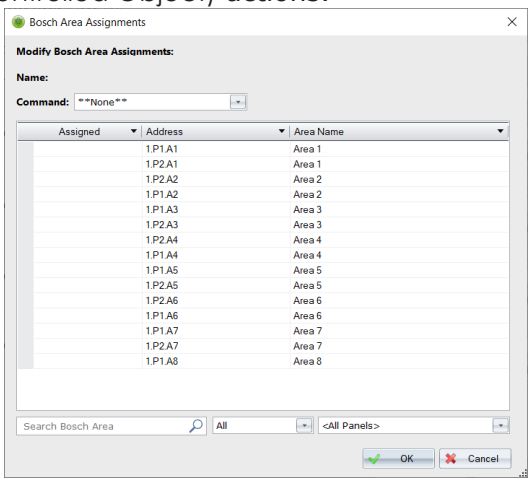
   This is the controlling object type that will cause the macro to execute. The selection of this object determines the choices available in the Action Event ID drop-down menus. The Actions below are based on this selection.
5. **Select** an Action(s) from the desired Action Event ID drop-down menu(s).

   Up to four separate actions can be configured.
6. **Select** Control Peripheral Object from the Remote Object Type (Controlled Object) drop-down menu.

   This is the controlled object that will receive the action as a result of the event being triggered.
7. **Select** Activate from the Action drop-down menu(s) corresponding to the selected Event ID(s).

   Up to four separate actions can be configured to match the Controlling Objects Actions.
8. **Click** the Build button to configure the Remote Object Type's (Controlled Object) actions.

   The Control Peripheral Devices Macro dialog opens. Depending on the panel and the type of object, different Actions may be displayed.



9. **Select** the Point and/or Area from the list.
10. **Select** the desired action from the list of Available Actions.
11. **Click** OK to close the Control Peripheral Devices Macro dialog.
12. **Click** OK to save the Host Based Macro.
13. **Add** the Host Based Macro to the appropriate Point or Area.

    See page 3-3 for more information or see the Triggers & Macros chapter in the DNA Users Manual.

This Page Intentionally Left Blank