



DNA Fusion/ISONAS Integration Guide

(for RC-03, RC-04, and IP Bridge)





DNA Fusion™ is a trademark of Open Options

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.

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

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

Open Options assumes no responsibility for incorrect or outdated information that may be contained in this publication.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: April 18, 2014

Manual Number: D-TI 6.0.1

©Copyright 2002-2016 Open Options, All rights reserved.

Warranty

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



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

Open Options, Inc. Software License Agreement and Warranty

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

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

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

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

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

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

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

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

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

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

Table of Contents

Chapter 1: Introduction

DNA Fusion/ISONAS Overview.....	1-3
Configuration Steps	1-3

Chapter 2: DNA Fusion/ISONAS Integration

ISONAS Configuration	2-1
Installation and Wiring	2-1
DNAFusion Integration Installation.....	2-1
ISONAS Driver Status	2-4
ISONAS Configuration in DNA Fusion.....	2-5
Configuring the IP Address	2-6
DNA Fusion Service Permissions	2-7
COM+ Object.....	2-7
DNA Fusion Driver Service	2-7
DNA Fusion User Group	2-8

Chapter 3: Fusion/ISONAS Integration and Installation

Adding the ISONAS Reader-Controller to DNA Fusion.....	3-1
Configuring the IP Address	3-2
Configuring the ISONAS Reader-Controller Doors.....	3-3
Configuring Access Levels in DNA Fusion.....	3-7
Creating a Global Access Level Group.....	3-7

Chapter 4: ISONAS in DNA Fusion

The Hardware Browser	4-1
Door Control Options	4-3
Door Control Dialog	4-3
Scheduling Commands.....	4-4
Configuring a Door to Follow a Time Schedule	4-5
ISONAS Door Features	4-7
Trace History	4-7
Who Has Access	4-7
Who Does Not Have Access.....	4-7
Where Used.....	4-7
ISONAS Reader-Controller Commands.....	4-9
Properties	4-9
Momentary Unlock.....	4-9
Modes.....	4-9
Control	4-9
Refresh Status	4-9
Download	4-9
Delete.....	4-9

Upgrade to Latest Firmware4-10

Reboot Controller4-10

Support Features.....4-11

Future Supported Features4-11

Introduction

1

In This Chapter

✓ Chapter Overview

This section is designed to introduce you to DNA Fusion™ and the ISONAS 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/ISONAS Integration and Installation," covers the ISONAS software installation.

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

Chapter 4, "ISONAS 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/ISONAS Overview

The ISONAS hardware utilizes network-based PowerNet™ reader-controllers. The IP reader-controller delivers power via Power Over Ethernet. The ISONAS integration brings a number of user-friendly features including InfoReady reporting and ease of configuration within the DNA Fusion software.

The following ISONAS hardware can be added to DNA Fusion:

- RC-03
- RC-04
- IP Bridge

The ISONAS integration is supported by DNA Fusion version 6.5.1 or higher; however, not all DNA Fusion features are fully supported. The integration also requires the ISONAS integration driver. See page 4-7 for more information on supported features.



Configuration Steps

To configure the ISONAS reader-controllers within the DNA Fusion application, complete the following steps:

1. **Install** the reader-controllers.
2. **Run** the ISONAS Integration installation.
For information see page 2-1.
3. **Connect** the ISONAS reader-controllers to the network.
See page 2-5 for information on adding the reader-controller.
4. **Configure** the ISONAS doors in DNA Fusion.
More information can be found on page 3-1.
5. **Add or modify** an Access Level(s).
More information on access levels can be found on page 3-7.

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

ISONAS Integration 2

In This Section

- ✓ ISONAS Integration Installation
- ✓ ISONAS Configuration in DNA Fusion

The ISONAS integration is supported by DNA Fusion version 6.5.1 or higher. The integration requires the proper licensing to be in place prior to the installation of the integration software.

The supported ISONAS hardware includes the two RC-03 PowerNet platforms, the various Pure IP RC-04 reader-controllers and the IP Bridge.

ISONAS Configuration

Before the ISONAS hardware can be integrated with DNA Fusion, the following key wiring tasks must be completed.

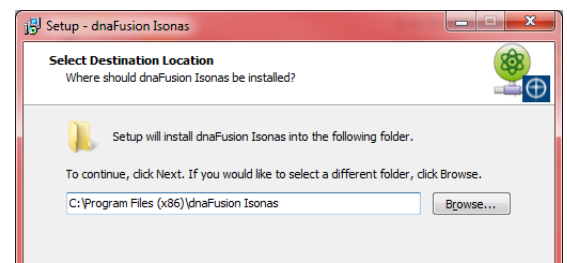
Installation and Wiring

1. **Install** and **supply power** to the ISONAS reader-controller unit.
This may be accomplished via Power over Ethernet (PoE) or through an external DC power source (12VDC or 24VDC).
2. **Wire** the door components to the ISONAS unit.
Readers, locks, and request to exit (REX) devices should be installed per the ISONAS Installation Manual.
For more information on installation and wiring, please see the ISONAS manual for the product being installed.
3. **Run** the DNAFusion ISONAS Integration.
See page 2-3 for more information.

DNAFusion Integration Installation

Once the ISONAS hardware has been installed and wired, the DNAFusion ISONAS Integration will need to be installed on the DNAFusion server. The ISONAS Integration installation process is very straightforward and can be performed without any knowledge of the software.

1. **Obtain** the ISONAS Integration application from Open Options Technical Support.
2. **Verify** the DNA Fusion DNADrvr32 Service Permissions.
The DNA driver and the ISONAS 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 ISONAS Integration installation.
The Select Destination Location dialog appears.
The default location is C:\Program Files (x86)\dnaFusion Isonas (64-bit) or C:\Program Files\dnaFusion Isonas (32-bit).

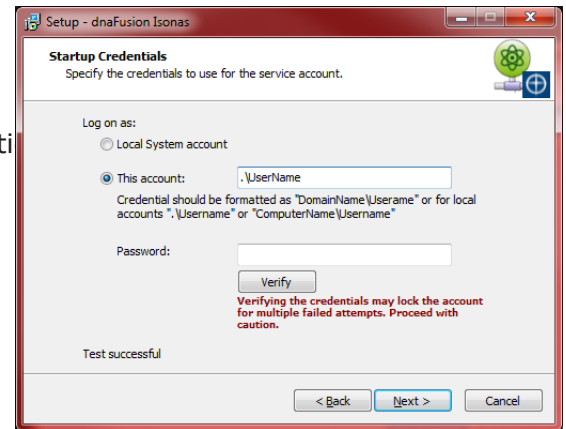


This Page Intentionally Left Blank

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

The Startup Credentials screen appears.

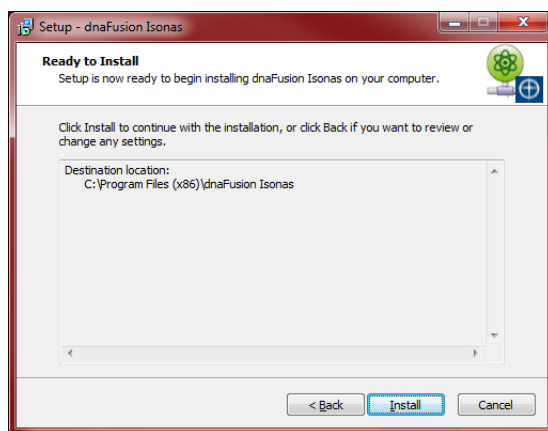
5. **Enter** the Service Account User Name and Password.
A local machine Administrative login information must be entered for the DNA Fusion ISONAS service to run. This information will need to be obtained from the System User and must match the credentials running the DNA Driver and the NPowerDNA COM+ object. The information was obtained in step 1 on page 2-1.
See page 2-7 for more information on the Services account.



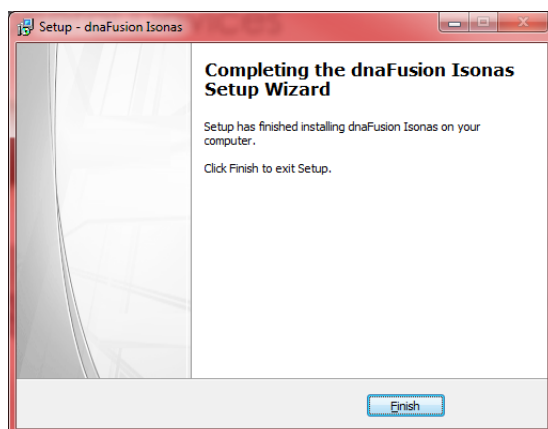
6. **Click** the Verify button.

Once successful, **click** the Next button.

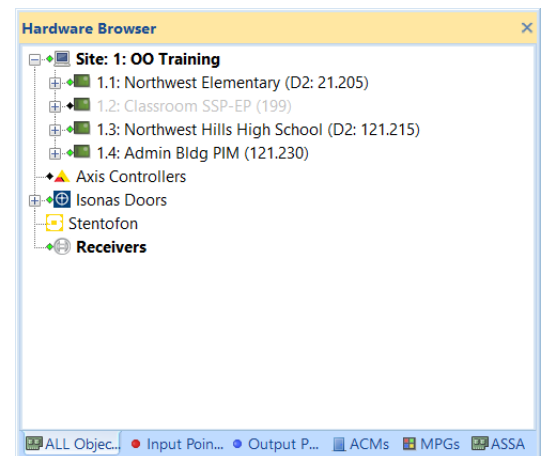
The Ready to Install screen will appear with a summary of the installation.



7. **Click** the Install button to start the installation process.
Installation will begin.
8. When the DNA ISONAS installation is complete, a dialog box will appear; **press** Finish to complete the setup.








The ISONAS driver icon will appear in the DNA Fusion Hardware Browser.



ISONAS Driver Status

The ISONAS driver status is reflected by the color of the diamond in the Hardware Browser. Below is a list of the various driver colors and states.

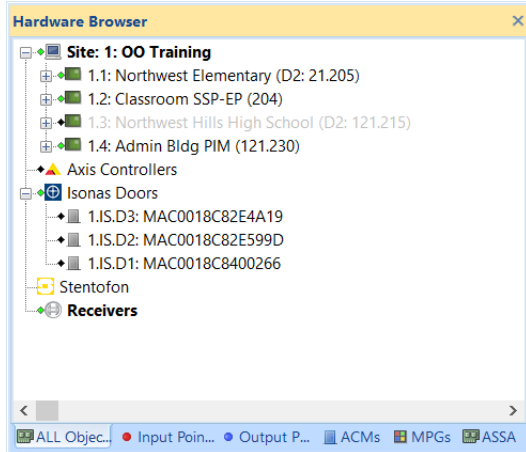
- ◆  • Green - The driver is running and all systems are functional. All is right in the world.
- ◆  • Black - The driver is not running.
 - ▣ Verify the DNADrvr32 and ISONAS services are running under the correct identity.
- ◆  • Yellow - The driver is running but unable to open the connection used to communicate status to DNA.
 - ▣ The oo.Isonas.status queue cannot be opened by the DNA Driver. Verify that the Isonas Driver is configured to run under a local administrators' group account.
- ◆  • Red - The driver is running but unable to open the connection used to relay events to DNA.
 - ▣ The oo.dnafusion.event queue cannot be opened by the DNA Driver.
- ◆  • Purple - The driver is running but unable to open either the events or status connections to DNA.
 - ▣ Both the oo.Isonas.staus or oo.dnafusion.event queues cannot be opened by the DNA Driver.

ISONAS Configuration in DNA Fusion

Once the integration installation has been completed, connect the hardware to the network and configure the doors within the DNA Fusion software.

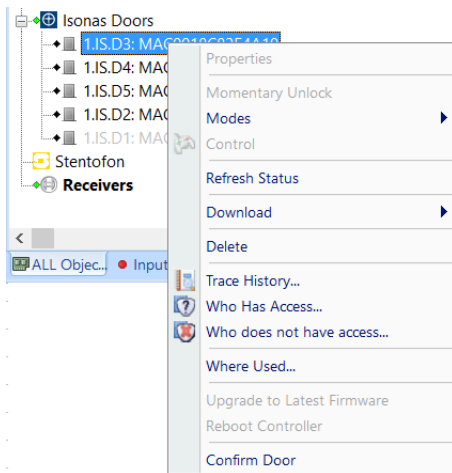
1. **Connect** the unit to the data network for communication with the DNA Fusion server.

When an ISONAS reader-controller is connected to the network, DNA will automatically add the device to the Hardware Browser. The service uses a UDP broadcast to connect to devices, and they appear in the Hardware Browser with the MAC Address as the description.



The devices will appear as gray doors until they are confirmed in DNA Fusion.

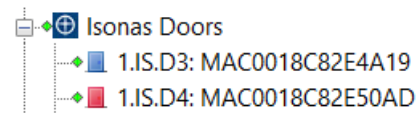
2. **Right-click** on the door and **select** Confirm Door from the drop-down menu.



A confirmation dialog will open.

3. **Click** OK to confirm the door.

The door state will change and the diamond color will change from black to green or red.



The color of the door in the Hardware Browser represents the door's current state. For more information on door properties, see page 3-3.

4. **Continue** to confirm the remaining ISONAS doors.

Once the door has been confirmed, the properties may be edited.

Configuring the IP Address

By default, the reader-controller will attempt to gain an IP address from the DHCP server. If the network does not have a DHCP server, the default IP address is 192.168.1.119.

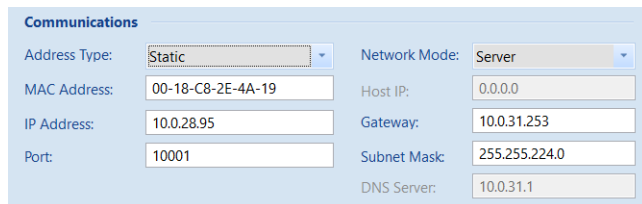
To set a static IP address:

1. **Right-click** on the ISONAS door and **select** Properties from the menu.

The ISONAS Door Properties dialog opens.

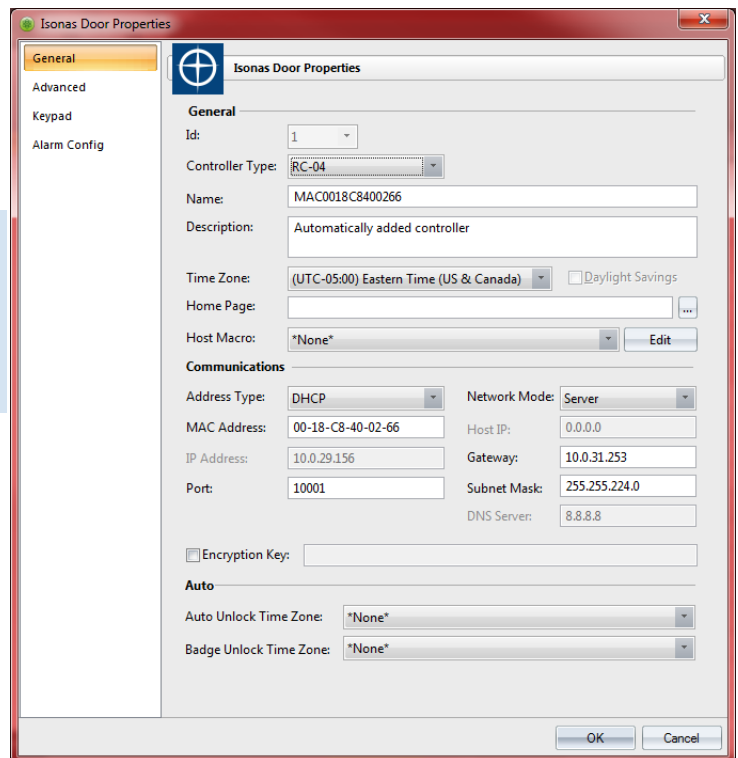
2. **Select** the Address Type drop-down in the Communications section and **select** the Static option.

The IP Address field can now be configured.



Communications	
Address Type:	Static
MAC Address:	00-18-C8-2E-4A-19
IP Address:	10.0.28.95
Port:	10001
Network Mode:	Server
Host IP:	0.0.0.0
Gateway:	10.0.31.253
Subnet Mask:	255.255.224.0
DNS Server:	10.0.31.1

3. **Enter** the IP Address and **click** the OK button.
If needed, **enter** the Subnet Mask and the Gateway information.



ISONAS Door Properties	
General	
Id: 1	
Controller Type: RC-04	
Name: MAC0018C8400266	
Description: Automatically added controller	
Time Zone: (UTC-05:00) Eastern Time (US & Canada) [Daylight Savings]	
Home Page: [...]	
Host Macro: *None [Edit]	
Communications	
Address Type: DHCP	
MAC Address: 00-18-C8-40-02-66	
IP Address: 10.0.29.156	
Port: 10001	
Network Mode: Server	
Host IP: 0.0.0.0	
Gateway: 10.0.31.253	
Subnet Mask: 255.255.224.0	
DNS Server: 8.8.8.8	
Encryption Key: []	
Auto	
Auto Unlock Time Zone: *None	
Badge Unlock Time Zone: *None	
OK Cancel	

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.

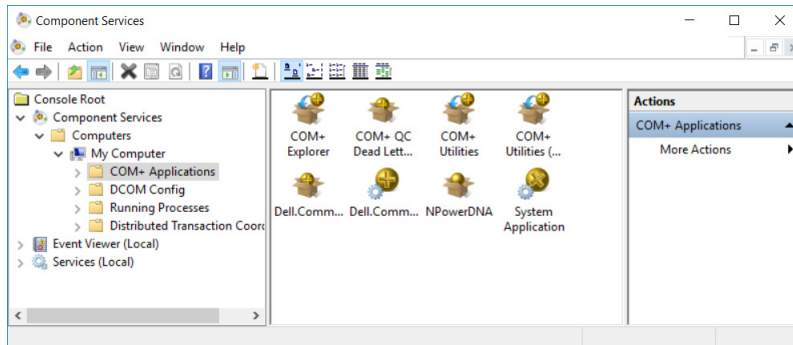
COM+ Object

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.

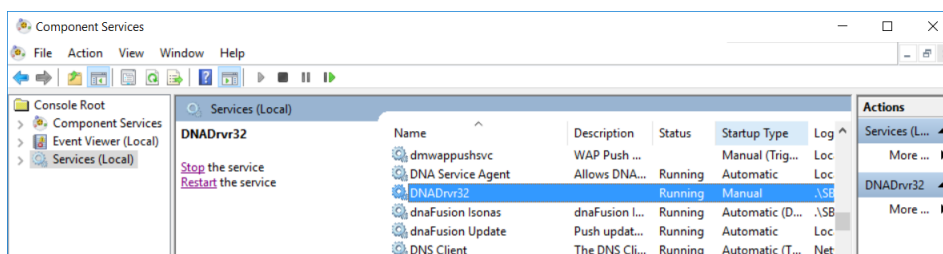
2. **Double-click** the Computers item.
 3. **Double-click** the My Computer icon and **open** the COM+ Applications folder.
- The COM+ Objects dialog appears.



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 ISONAS service will require the same information. This also applies to the DNA Driver (DNADrvr32) service.
6. **Click** the OK button.

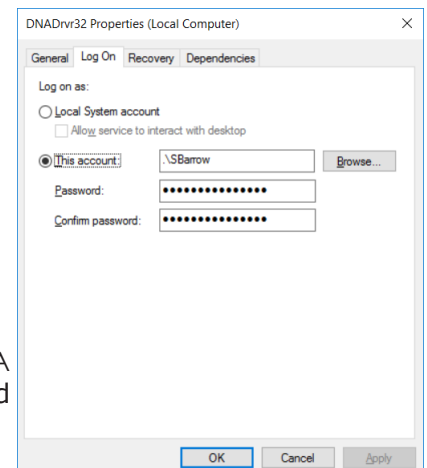
DNA Fusion Driver Service

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.



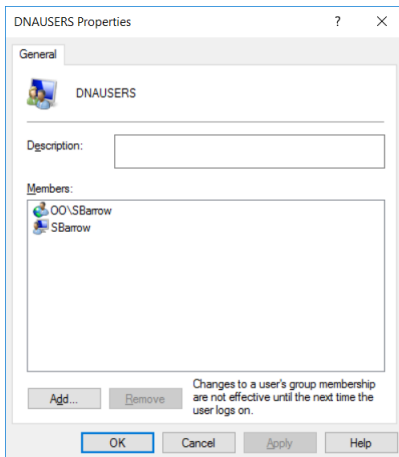
3. **Right-click** on the DNADrvr32 service and **select** the Properties option.
The DNADrvr32 Properties dialog will open.
4. **Select** the Log On tab and **verify** the user configuration.

Keep in mind this must be the same account used to run the NPowerDNA COM+ Object as well as the DNAFusion ISONAS 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 ISONAS Driver are in DNAUSERS group (or explicitly a local admin) to achieve communication via Microsoft Message Queues (MSMQ).

DNA Fusion Configuration 3

In This Section

- ✓ Adding the ISONAS Reader-Controller to DNA Fusion
- ✓ Configuring Doors
- ✓ Access Level Creation

Once the integration installation has been completed, connect the hardware to the network and configure the reader-controller within the DNA Fusion software.

Adding the ISONAS Reader-Controller to DNA Fusion

Once the devices are confirmed in DNA Fusion, the properties of the ISONAS door can be configured.

1. With DNA open, **select** the Hardware Browser button on the toolbar.

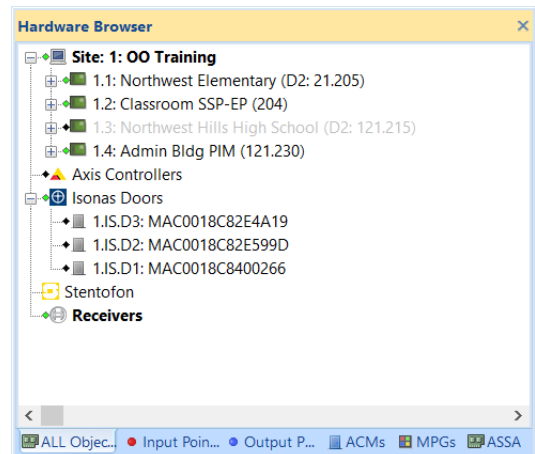
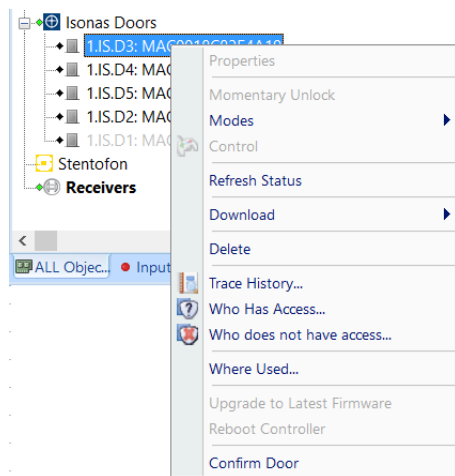
The Hardware Browser opens.

2. **Connect** the unit to the data network for communication with the DNA Fusion server.

When an ISONAS reader-controller is connected to the network, DNA will automatically add the device to the Hardware Browser. The service uses a UDP broadcast service to connect to devices. They appear in the Hardware Browser with the MAC Address as the description. If an IP Bridge is discovered, it will add the 2 or 3 door unit.

The devices will appear as gray doors until they are confirmed in DNA Fusion.

3. **Right-click** on the door and **select** Confirm Door from the drop-down menu.

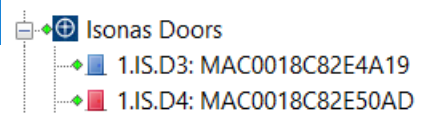
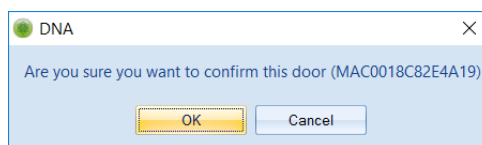


A confirmation dialog will open.

4. Click **OK** to confirm the door.

The door state will change and the diamond color will change from black to green or red.

The color of the door in the Hardware Browser represents the door's current state. For more information on door properties, see page 4-1.



5. **Continue** to confirm the remaining ISONAS doors.
Once the door has been confirmed, the properties may be edited.

Configuring the IP Address

By default, the reader-controller will attempt to gain an IP address from the DHCP server. If the network does not have a DHCP server, the default IP address is 192.168.1.119.

To set a static IP address:

1. **Right-click** on the ISONAS reader-controller and **select** Properties from the menu.

The ISONAS Door Properties dialog opens.

2. **Select** the Address Type drop-down in the Communications section and **select** the Static option.

The IP Address field can now be configured.

Communications			
Address Type:	Static	Network Mode:	Server
MAC Address:	00-18-C8-2E-4A-19	Host IP:	0.0.0.0
IP Address:	10.0.28.95	Gateway:	10.0.31.253
Port:	10001	Subnet Mask:	255.255.224.0
		DNS Server:	10.0.31.1

3. **Enter** the IP Address and **click** the OK button.
If needed, enter the Subnet Mask and the Gateway information.

The Door Properties are covered on page 3-3.

Isonas Door Properties

General

Id: 1

Controller Type: RC-04

Name: MAC0018C8400266

Description: Automatically added controller

Time Zone: (UTC-05:00) Eastern Time (US & Canada) ☐ Daylight Savings

Home Page:

Host Macro: *None

Communications

Address Type: DHCP

Network Mode: Server

MAC Address: 00-18-C8-40-02-66

Host IP: 0.0.0.0

IP Address: 10.0.29.156

Gateway: 10.0.31.253

Port: 10001

Subnet Mask: 255.255.224.0

DNS Server: 8.8.8.8

☐ Encryption Key:

Auto

Auto Unlock Time Zone: *None

Badge Unlock Time Zone: *None

Configuring the ISONAS Reader-Controller Doors

Once the reader-controller has been added to DNA Fusion and the device has been discovered by the driver, the door settings can be configured.

1. From the Hardware Browser, **right-click** on the ISONAS Door and **select** Properties from the menu. The ISONAS Door Properties dialog opens.

2. **Enter** a Name for the door and if desired, **edit** the Description.

The default name is the MAC Address of the device. This name will appear in the Events Grid as well as any references to the door. The Description is auto-populated when the device is auto-added.

3. **Select** the correct Time Zone from the drop-down list.

This selection will determine the time in for the reader-controller.

4. If needed, **click** the Browse button to select a Home Page.

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** DHCP or Static from the Address Type drop-down.

If Static is selected, see page 3-2 for more information on setting a static address.

7. **Select** the Network Mode from the drop-down list.

- Server Mode - The driver will open the connection to the reader-controller.
- Client Mode - The device will open the connection to the driver. Client Mode is only available for RC-03, IPBR-2 and IPBR-3 model reader-controllers.

❑ If Client Mode is selected, **enter** the Host IP Address and a valid DNS Server.

8. **Verify** the Port setting.

The IP reader controllers all come from the factory with port 10001 preset for all units except IPBridge. The port should only be changed under special cases. IPBridge units allow you specify a base port only. The second and third readers in the IPBridge will use the specified port +1 and +2 respectively.

9. If desired, **select** the Encryption Key checkbox and **enter** the desired 32 byte hex key.

The format of this key is a character string (64 characters maximum), using the characters 0-9, A-F.

10. If needed, **select** a preconfigured Time Schedule from the Auto Unlock Time Zone drop-down.

If a Time Schedule is selected, the door will unlock when the time schedule becomes active and will return to the door's default mode upon deactivation of the time schedule. For more information on Time Schedules, see Chapter 5: Time and Holiday Schedules in the DNA Fusion User Manual.

11. If needed, **select** a preconfigured Time Schedule from the Badge Unlock Time Zone drop-down.

If a Time Schedule is selected, the door will unlock when the time schedule becomes active and a valid credential is presented. The door will return to the default mode upon deactivation of the time schedule. For more information on Time Schedules, see page 5-1 in the DNA Fusion User Manual.

Open Options Integration Manual

12. **Select** the Advanced tab.

The ISONAS Advanced Properties dialog opens.

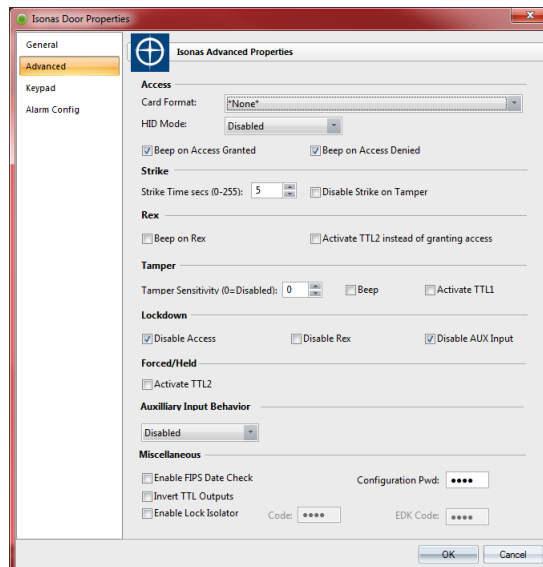
13. **Select** the Card Format from the drop-down list.

To create new card formats, see page 3-53 in the DNA Technical Manual or page 8-75 in the DNA User Manual.

14. If needed, **select** the correct HID Mode from the drop down.

The default mode is Disabled. There are two modes for HID badges:

- Enabled - The ISONAS reader uses all of the data that can be read from the card. It creates a unique 32 bit number that is used by the DNA Fusion system. This is a combination of the card number and the HID site/facility code.
- Advanced - The ISONAS reader uses a bit mask to select up to 32 bits from the card information. The bit mask is dependent on the Card Format. The bitmask can be configured to capture the HID Card number; this would make the ISONAS card number match the HID Card number. Alternatively, the HID Card number can be included in the selected bitmask. In this case the ISONAS card number will differ from the HID Card number.

15. If desired, **uncheck** the Beep on Access Granted and/or Beep on Access Denied options.16. **Configure** the Strike Time (0-255).

The number of seconds the door will remain unlocked when a valid credential is presented.

17. If desired, **check** the Disable Strike on Tamper option.

If selected, the strike will be disabled when a tamper condition exists.

18. **Check** the Beep on REX and/or Activate TTL2 instead of granting access options if needed.

If the Activate TTL2 option is selected, the TTL2 will activate instead of the strike.

19. **Set** the Tamper Sensitivity if needed.

The default is Off (0). The tamper count should be left at zero (0) for ISONAS reader-controllers equipped with optical tamper sensors. The tamper sensitivity determines the number of sequential tamper indications before the alarm is created. Higher settings allow for compensation for highly sensitive tamper conditions such as a location with a lot of physical vibration.

20. If desired, **select** the Beep and/or Activate TTL1 options.

If the Activate TTL1 option is selected, TTL1 will activate if a Tamper alarm is detected.

21. Under the Lockdown section, **check** or **uncheck** the desired options.

When the door is placed in Lockdown mode, no badges will be accepted except those flagged as VIP. This mode is intended as an emergency state and requires manual intervention by an operator to revert the point to normal the state.

- Disable Access - No access will be allowed when the unit is placed in Lockdown mode.
- Disable REX - If selected, the REX device will be disabled.
- Disable AUX Input - Disables the AUX input on the reader-controller and ignores any change of state.

22. Under the Forced/Held section, **check** Activate TTL2 if desired.

Once selected, the TTL2 output will be activated when the door is forced or held open.

23. **Select** the desired behavior of the Auxiliary Input when it changes state.

- Disabled - Default setting. The signal is ignored and the Auxiliary Input has no effect on other objects.
- Activate TTL1 - Activates TTL1 when a change in state is detected on the Auxiliary Input.

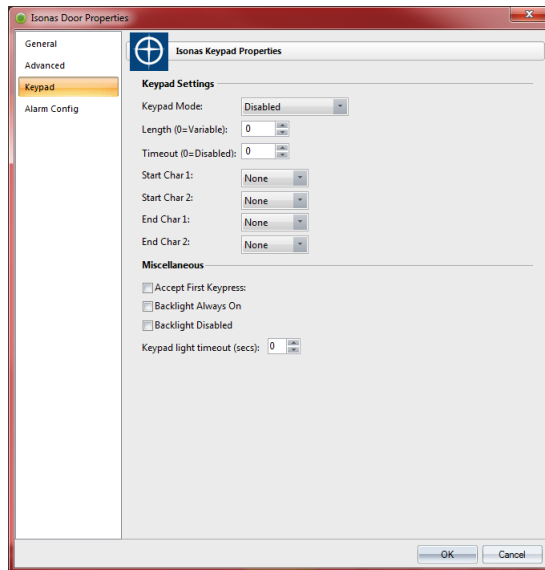
- Activate TTL2 - Activates TTL2 when the Auxiliary Input changes state.
- Grant Access - When a change of state is detected, the reader-controller will unlock the door for the predefined Strike Time.

24. If needed, **select** the desired options under the Miscellaneous section.

- Enable FIPS Date Check - Enables an additional verification of the date on FIPS 201-1 cards.
- Invert TTL Outputs - Reverses the state of the outputs.
- Enable Lock Isolator - Activates the Code and EDK Code fields.

25. **Select** the Keypad option on the menu if a keypad will be used at the reader-controller.

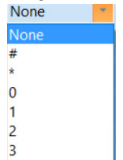
The ISONAS Keypad Properties dialog opens.



- **Select** the appropriate Keypad Mode: Enabled with Beep or Enabled without Beep.

If Enabled with Beep is selected, the unit will beep on every key press.

- **Set** the Length of the number of digits (0 = Variable). If set, the length of the entry will be fixed.
- **Set** the Timeout setting. This setting determines the amount of time for the keypad entry. (0 = Disabled)
- **Select** the Start Character 1 and 2.
- **Select** the End Character 1 and 2.
- If desired, **check** the Accept First Keypress option.
- If desired, **check** the Backlight Always On or Backlight Disabled options.
- **Enter** the Keypad Light Timeout.

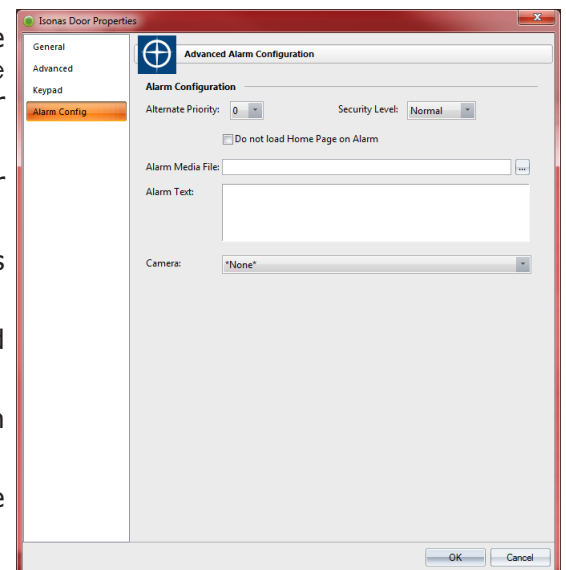


26. **Select** the Alarm Config tab to configure the Alarm Properties for the ISONAS door.

The Advanced Alarm Configuration dialog opens.

If desired, set the following options.

- Alternate Priority - The selected Alarm Priority overrides the default Event specific priority set in DNA / Administrative / Events & Alarms / Logging. See page 14-23 in the User Manual for more information.
- Security Level - Category designation. Allows administrator to restrict operator use in the Operator Profiles.
- Do Not Load Home Page on Alarm - If associated door goes into alarm, the Home Page will not load.
- Alarm Media File - Door specific alarm file to be displayed when an alarm occurs.
- Alarm Text - Point specific alarm text to be displayed when an alarm occurs in addition to the alarm reason.
- Camera - Camera associated with the door; allows it to be recalled in the Events Grid as well as in the Alarm Grid.

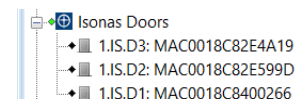


27. **Click** the OK button to add the door to the DNA Fusion system.

The door will appear in the Hardware Browser. If the door appears grayed out, it has not been confirmed.

To confirm the door, **right-click** on the door and **select** the Confirm Door option.

Doors must be confirmed before the ISONAS service will start to communicate with them.



Configuring Access Levels in DNA Fusion

An Access Level consists of an entry point (such as a ISONAS door) and an associated time schedule. When the access level is added to a card record, it determines where and when the cardholder has access within the system.

Access Levels can be added to individual cards or groups of cards in the system. Each card can be assigned 32 access levels per SSP controller in the system. This section shows you how to create and modify access levels.

For more information on access levels, see Chapter 6 in the DNA Fusion User Manual.

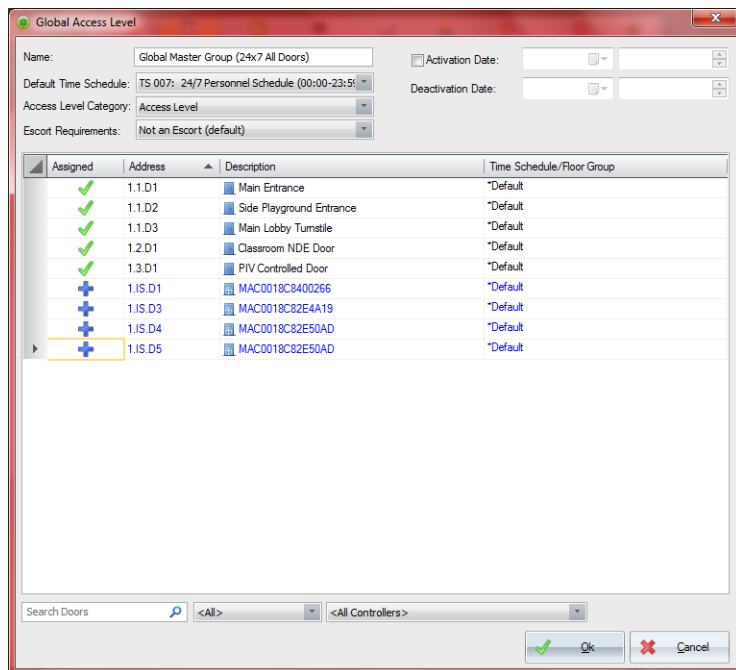
When using the ISONAS reader-controllers, Global Access Level Groups must be utilized.


Creating a Global Access Level Group

A Global Access Level Group provides an easy way for doors and elevators from multiple controllers to be grouped together in a common access level. This will allow a cardholder to have access to doors on multiple controllers with a single global access level group. See page 6-7 in the User Manual for more information.

1. With the Access Levels Browser open, **right-click** on Access Level Groups and **select** Add Global Access Level Group from the resulting menu.

The Global Access Level dialog opens.



2. **Enter** a Name for the global access level group.
3. **Select** the Assigned column for the desired ACMs (Doors & Elevators).
A **+** will appear in the Assigned column once the door(s) have been selected.
If the group has doors already assigned, a **✓** will appear in the Assigned column.
ISONAS doors appear with IS in the address as well as an identifying icon .
4. From the Default Time Schedule drop down, **select** a Time Schedule for the Access Level.
5. **Click** OK to close the Global Access Level dialog.

The Global Access Level Group will appear in the browser and is ready for distribution to cardholders. Global Access Level Groups can be identified by the folder with the red access level icon.

This Page Intentionally Left Blank

ISONAS in DNA Fusion4

In This Chapter

- ✓ Controlling the ISONAS Hardware
- ✓ Generating Reports

DNA Fusion offers a number of different hardware features as well as the ability to generate “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.

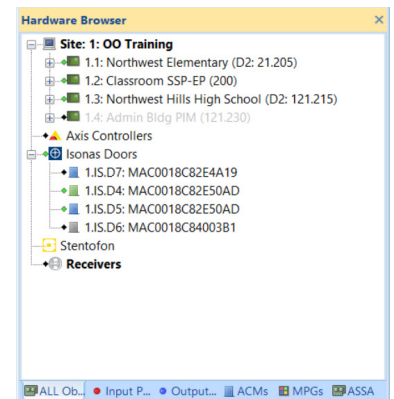
2. **Expand** the ISONAS Doors header.

Driver Status Indicators:

- Green Diamond - The ISONAS driver is running and all systems are good.  Isonas Doors
- Black Diamond - The ISONAS driver is not running.  Isonas Doors
- Yellow Diamond - The ISONAS driver is running but the oo.Isonas.status queue can't be opened by the DNA Driver.  Isonas Doors
- Red Diamond - The ISONAS driver is running but the oo.dnafusion.event queue can't be opened by the DNA Driver.  Isonas Doors
- Purple Diamond - The Isonas driver is running but neither the oo.Isonas.staus or oo.dnafusion.event queues can be opened by the DNA Driver.  Isonas Doors

Door Indicators:

-  • Blue Door - The door is currently in a normal state; i.e., closed.
-  • Red Door - The door is currently in an alarm state; i.e., door held open or door forced open.
-  • Gray Door - The door has not been confirmed or is offline.
-  • Green Door - The door is currently in an unlocked state.
-  • Yellow Door - The door is currently in the locked state.



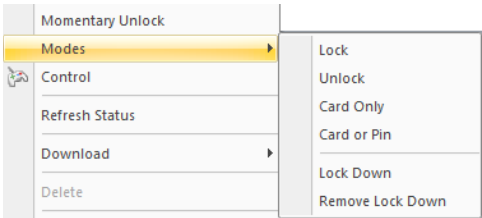
Hovering over a door will show you the status for the door in the form of a tooltip.

This Page Intentionally Left Blank

Door Control Options

The easiest way to control a door is to right-click on the door and select the option from the Door menu.

- 1. **Right-click** on the desired door in the Hardware Browser.
- 2. **Select** the Modes option and **select** the correct Mode.



Lock	Locks the selected door. All attempts to change the mode will be logged as an error.
Unlock	Unlocks the selected point and allows unlimited access.
Card Only	Requires a card with the correct format be presented.
Card or PIN	The door requires either a card be presented or a PIN code entered to gain access.
Lock Down	The door will ignore all badges except those flagged as VIP.
Remove Lock Down	Returns the doors to the normal state.

The Door Options menu also includes a Momentary Unlock option.

Door Control Dialog

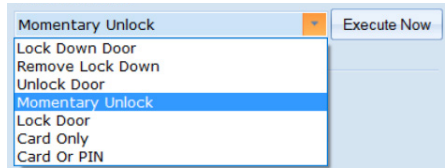
DNA allows the operator to directly perform various tasks on a selected door using the Door Control dialog. The dialog offers the following options:

- Change the Door Mode
- Issue a Momentary Unlock
- Schedule One Time Scheduled Commands

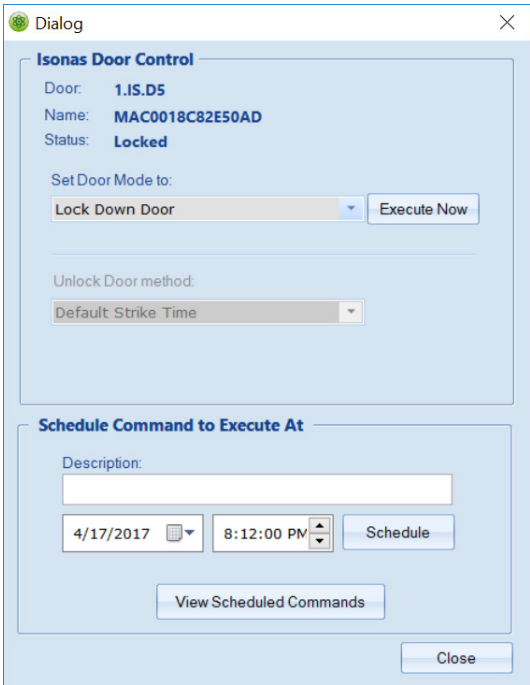
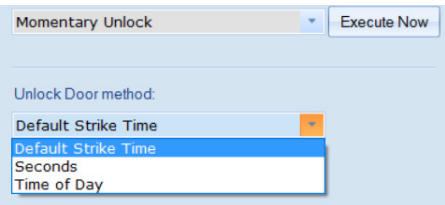
To open the Door Control dialog:

- 1. **Right-click** the door you wish to control and **select** Control from the context menu.
The Direct Control dialog will open.
- 2. **Select** the appropriate option from the Set Door Mode to: drop-down and **click** the Execute Now button.

Allows the operator to set the reader mode. This setting determines the type of access the reader will allow. See the table above for more door mode information.



If Momentary Unlock is selected, the Unlock Door Method drop-down becomes active. **Select** the desired method and **click** the Execute Now button.



- Default Strike Time - Unlocks the door for the programmed strike time.
- Seconds - **Enter** the time (in seconds) for the door to unlock.
- Time of Day - **Enter** the time for the Momentary Unlock command to be executed.

- 3. **Click** the Close button or the X icon to close the dialog box.

Scheduling Commands

The Schedule Command to Execute At option allows the operator to schedule door control.

A single event with defined start and end times as well as door modes. This type of scheduled control is stored in the host and is initiated from the host at the time of the event. Consequentiality, the host computer must be on at the time of the event.

1. From the Door Control dialog, **select** the Door Mode.
2. In the Schedule Command to Execute At section, **enter** a Description for the event.
This is a user-defined description for the action that will appear when the event is viewed in the future.
3. **Enter** a Date and Time.
4. **Click** the Schedule button.

A confirmation dialog will appear. **Click** OK to close the dialog. Keep in mind you may need to schedule multiple door mode events to return the door to a secured state.

To view any Scheduled Events, **click** the Schedule button.

The screenshot displays the 'Isonas Door Control' window. The 'Door' is '1.IS.D5', 'Name' is 'MAC0018C82E50AD', and 'Status' is 'Locked'. The 'Set Door Mode to:' dropdown is set to 'Lock Down Door' with an 'Execute Now' button. The 'Unlock Door method:' dropdown is set to 'Default Strike Time'.

The 'Schedule Command to Execute At' dialog is open, showing a 'Description:' field, a date/time picker set to '4/17/2017 8:12:00 PM', and a 'Schedule' button. Below the dialog is a 'View Scheduled Commands' button and a 'Close' button.

The 'Scheduled Commands Dialog' shows a table of scheduled commands for 'MAC0018C82E50AD (1.IS.D5)'. The table has columns: Date Time, Scheduled By, Explanation, and Action.

Date Time	Scheduled By	Explanation	Action
04/19/17 12:00:00	Admin @ Station 1	Meeting	Unlock Door
04/17/17 20:12:00	Admin @ Station 1		Momentary Unlock Duration 52 seconds
04/17/17 20:12:00	Admin @ Station 1		Momentary Unlock Duration 52 seconds

Below the table are 'Filters' for 'Action:' and 'Explanation:' both set to '<All>'. At the bottom are buttons for 'History', 'Print', 'Remove', and 'Cancel'.

If desired, **click** the History button to view previously scheduled events. Future events are displayed in green while events that have already occurred appear red.



If a door mode is changed, it may require scheduling two (2) events in order to return the door to a secured mode.

Configuring a Door to Follow a Time Schedule

The Unlock Schedule option provides a quick way to configure a door(s) to adhere to a specified unlock time schedule. The time schedule must be created prior to the setting up the unlock feature. The ISONAS reader-controller is capable of storing 32 time schedules. The first 32 default time schedules programmed in the DNA Fusion system will be available for selection.

1. **Right-click** on the Door and **select** the Properties option.

The Door Properties dialog opens.

2. **Select** the desired schedule from the Auto Unlock Time Zone drop-down list.

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



Time Schedule information can be found in the DNA User Manual in Chapter 5. Keep in mind the ISONAS unit is limited to 32 time schedules.

Open Options Integration Manual

ISONAS Door Features

There are a number of features available for doors and elevators. For instance, you can see who has access to a specific door or trace the history for the selected ACM.

Trace History

A trace history report can be run on a reader-controller to view the last transactions.

1. **Right-click** on the ISONAS Door and **select** Trace History from the menu.

The Trace History Dialog will open.

Time & Date	Panel Time	Last Name	First Name	Tenant ID	Card	F/C	Address	Description
04/13/17 17:21:16	04/13/17 17:21:16	ACCARDO	DAVID	6	6056	50	1.IS.D4	MAC0018C82E50AD
04/13/17 10:41:12	04/13/17 10:41:12				5482	115	1.IS.D4	MAC0018C82E50AD
04/12/17 17:19:30	04/12/17 17:19:30				5364	50	1.IS.D4	MAC0018C82E50AD
04/12/17 10:08:41	04/12/17 10:08:41				1204	50	1.IS.D4	MAC0018C82E50AD
04/11/17 16:20:37	04/11/17 16:20:37	Barrow	Sherinda	1	1002	115	1.IS.D4	MAC0018C82E50AD
04/11/17 09:44:11	04/11/17 09:44:11	Accurs	Bob	1	1205	50	1.IS.D4	MAC0018C82E50AD

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 printed or e-mailed by selecting the appropriate button. Select the Print to Size checkbox to size the report so that all columns appear on the same page 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 ACM.

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

The Who Has Access dialog appears.

Last Name	First Name	AL	AL Description	TS	Card Num...	Active	Department	Location	Title	Start Date
Barrow	Sherinda	2	Global Master ...	7	1218	Yes	Chemistry	Orlando		07/28/14
Barrow	Sherinda	2	Global Master ...	7	1002	Yes	Chemistry	Orlando		02/10/16
Beaty	Tom	2	Global Master ...	7	1876	Yes	Communications			01/01/00
Bob	Joe	2	Global Master ...	7	5004	Yes	Emergency Cr...			01/21/16

The results can be exported, printed or e-mailed 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 ACM.

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

The Who Does Not Have Access dialog appears.

The results can be exported, printed or e-mailed by selecting the appropriate button.

Where Used

The Where Used feature provides a grid displaying the door's associated relationships (i.e. Triggers, Macros, Access Levels, etc.).

1. **Right-click** on the ACM object and **select** Where Used.

The Where Used Report dialog opens.

The results can be exported to a CSV file or to the Clipboard.

Address	Description
DOOR: 1.IS.D4: MAC0018C82E50AD	
Access Levels	
Global Access Level - 2	Global Master Group (24x7 All Doors)
Global Access Level - 3	General Personnel

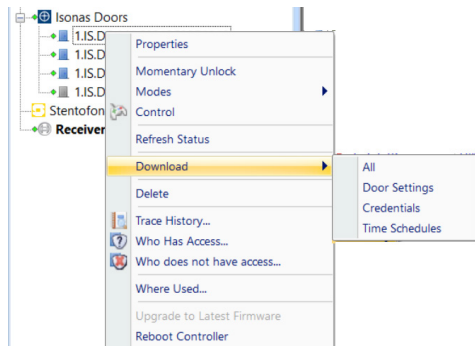
Open Options Integration Manual

ISONAS Reader-Controller Commands

The ISONAS Reader-Controllers features provide access to download options, perform a soft reset, and update firmware.

To access the reader-controller commands menu:

1. **Right click** on the ISONAS door.
The ISONAS reader-controllers context menu will open.
2. **Select** the desired option from the menu.



Properties

Opens the Properties dialog for the selected ISONAS Door (Reader-Controller). See page 3-3 for detailed information about ISONAS Reader-Controller Properties.

Momentary Unlock

When selected, the door will unlock for the programmed strike time.

Modes

Opens the Door Mode drop-down. See page 4-3 for more information on door modes.

Control

When selected, the Door Control dialog will open. See page 4-3 for more information on the door control dialog.

Refresh Status

Updates the ISONAS reader-controller's status in the DNA Fusion Hardware Browser.

Download

It is imperative that changes be downloaded to the ISONAS reader-controller in order for them to be saved to the panel. It is recommended that an actual download be performed when large amounts of information or changes have been entered.

1. **Select** the appropriate Download option from the menu.
If desired, **select** the All option to download all categories.
 - All - Downloads all door properties, cardholder information, and time schedules (32 maximum).
 - Door Settings - Pushes the door properties to the ISONAS unit.
 - Credentials - All of the cardholder's credential information will be downloaded.
 - Time Schedules - Downloads the first 32 default time schedules.

Delete

Removes the selected ISONAS reader-controller. Caution should be used when selecting this option since all information will be deleted.



Extreme caution should be used before selecting the Delete option. Once an ISONAS reader-controller has been deleted, there is no way to undo the action, the controller will have to be re-added to the system.

Upgrade to Latest Firmware

Firmware plays the middleman between the software and hardware. The most recent firmware updates will result in the best possible results for your system.

Reboot Controller

Deletes the information in the controller's memory and then a full download reloads the controller with updated information. During the process, the controller will lose communication with DNA; depending on the amount of information being downloaded, this process could take a while.

Firmware should be updated after any changes to the system, including the following:

- Installing a new system
- Upgrading to a new version of DNA Fusion
- Adding a new ISONAS reader-controller
- Replacing an existing ISONAS reader-controller
- Connecting to an ISONAS reader-controller for the first time

Supported Features

The following features are currently supported in a limited capacity.

- Host Based Macros

- Direct Commands

- Graphic Map Support
- Standard Crystal Reporting

Future Supported Features

The ISONAS platform is a new and developing solution. There will be some limited functionality in the following areas:

- Conventional Triggers and Macros
- Tenants, SSP Lists and Event Filtering
- API Support for the Mobile application and Web capabilities
- ACM Status Report
- View ISONAS doors on ACM tab
- ACM Sub Groups
- Operator Privilege Restrictions
- Multi Select/Edit
- Hardware Monitor Report

This Page Intentionally Left Blank