

EXgarde Suprema W2 ACU

User Manual
UM0123_1

Foreword

Copyright © 2021 TDSi. All rights reserved.

Time and Data Systems International Ltd operate a policy of continuous improvement and reserves the right to change specifications, colours or prices of any of its products without prior notice.

Guarantee

For terms of guarantee, please contact your supplier.

Copyright © 2021 Time and Data Systems International Ltd (TDSi). This document or any software supplied with it may not be used for any purpose other than that for which it is supplied nor shall any part of it be reproduced without the prior written consent of TDSi.

Trademarks

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other brands and product names are trademarks or registered trademarks of their respective owners.

Cautions and Notes

The following symbols are used in this guide:



CAUTION! This indicates an important operating instruction that should be followed to avoid any potential damage to hardware or property, loss of data, or personal injury.



NOTE: This indicates important information to help you make the best use of this product.

Document Control

Issue	Date Issued	Change Summary	Issued by
1	11/03/2021	Initial Release	TBA

Table of Contents

1.	Overview	5
	1.1 Compatibility	5
2.	Prerequisites	5
3.	Setting Up Suprema.....	6
4.	Suprema W2 service	9
	4.1 Suprema W2 Service Configuration.....	10
	4.2 SSL (Secure Socket Layer) control	11
	4.2.1 Enable SSL	11
	4.2.2 Disable SSL.....	11
	4.3 DESFire Card Configuration	12
5.	Setting up Suprema in EXgarde	13
	5.1 Suprema W2 Readers connected to controllers.	13
	5.2 Suprema W2 as a standalone ACU.....	18
	5.3 Adding a Secure I/O 2 module.....	22
6.	BIOstar 2 reader door setup.....	23
	6.1 Associate Doors to an Access Area	23
	6.2 Fire door setup.....	24
	6.3 Door access area setup.....	24
	6.4 Reader Location	24
	6.5 Door Functions	24
	6.6 Door Schedule	25
	6.7 Manual Door Control.....	25
	6.7.1 Release Door.....	26
	6.7.2 Unlock Door for Free Access.....	26
	6.7.3 Lock Door to Stop All Access.....	26
	6.7.4 Set Door to Controlled Access	26

7.	Alarms	27
8.	Schedules	34
	8.1 Relay Schedules	34
	8.2 Biometric Schedules.....	37
9.	Biometric Enrolment Reader	39
10.	Adding a Keyholder to EXgarde	41
11.	Adding a Keyholder Biometric Template.....	42
12.	Reloading templates to readers.....	44
13.	Commissioning Mode.....	45
14.	Troubleshooting	46
	Connection Issues	46
	Distribution Error	46
	Reader Shown Offline	46

1. Overview

The EXgarde Suprema W2 ACU integration module allows the latest Suprema Biometric technology to integrate with the latest EXgarde access control software, providing a high level of security with confidence.

The integration module provides the following features.

- Ability to use Suprema W2 reader as standalone ACU
- Biometric Enrolment using Suprema W2 readers
- Template distribution to readers
- Monitor reader tamper input
- Monitor reader online/offline status.
- Display reader events in EXgarde including template download progress

1.1 Compatibility

The EXgarde Suprema integration module is compatible with all Suprema readers running the Suprema SDK 2 interface.

2. Prerequisites

The follow criteria must be met in order for the integration to function correctly.

- EXgarde 4.6 PRO or higher installed
- .Net 4.5 installed
- An additional network user
- Suprema BioEntry finger License feature enabled (required for both Standalone and TDSi ACU integration)
- Suprema W2 ACU License feature enabled (Standalone mode only)
- Adequate Biometric Users License added (amount of enrolled Keyholders required)
- All connections to Suprema readers have been established and all IP addresses recorded
- All reader serial numbers recorded
- BioStar2 software installed for reader configuration.

3. Setting Up Suprema

This part of the setup will need to be carried out in accordance with the Biostar2 software provided. The screenshot below is an example of the All Devices page of the Biostar2 software.

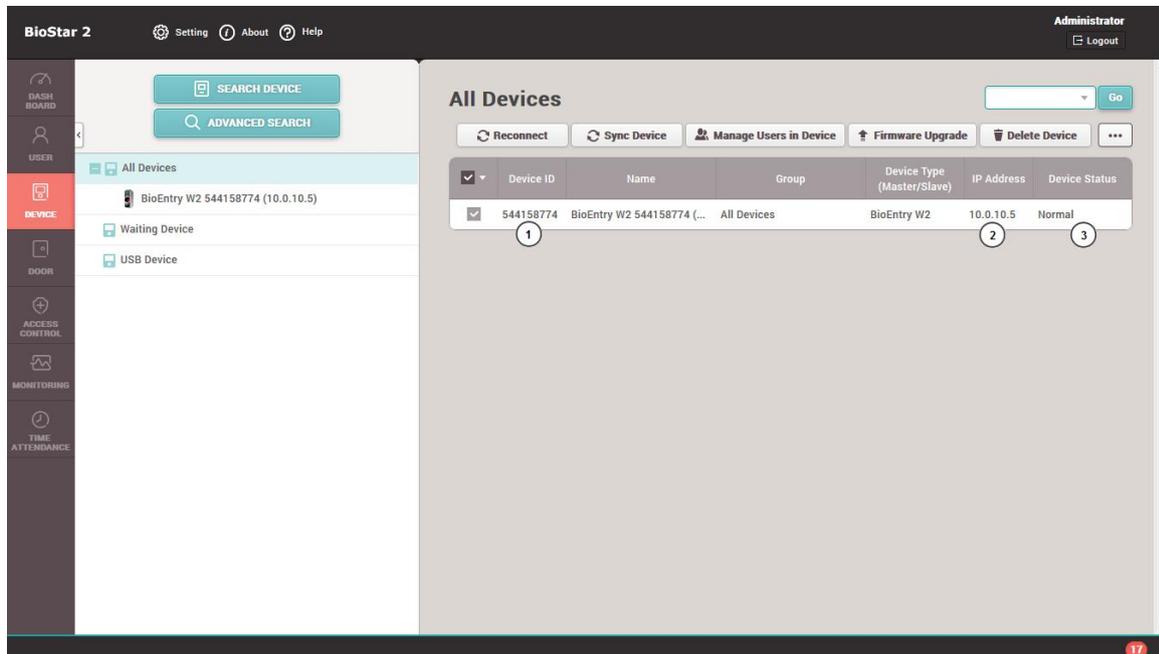


Figure 1

The numbered item is required by EXgarde to complete the setup.

- 1- Serial number of the reader
- 2- IP address of the reader
- 3- Status of the reader



CAUTION! Ensure the Wiegand Input / Output mode in the reader advanced settings is set to OUTPUT



NOTE: Ensure all readers have been added in the BioStar2 software and are all online

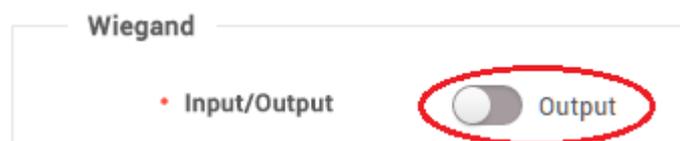


Figure 2

In the following example we are setting the output to 37-bit Wiegand.

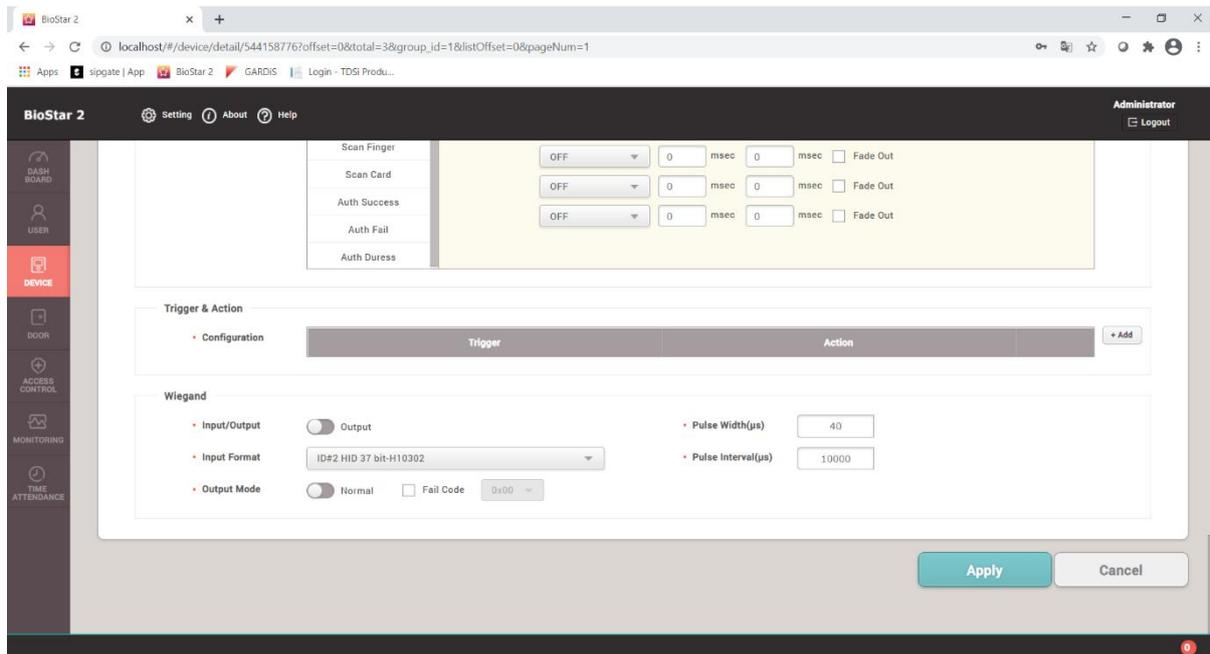


Figure 3

Go to Setting -> Card Formats in the Biostar Software. Take note of the format used for the output.

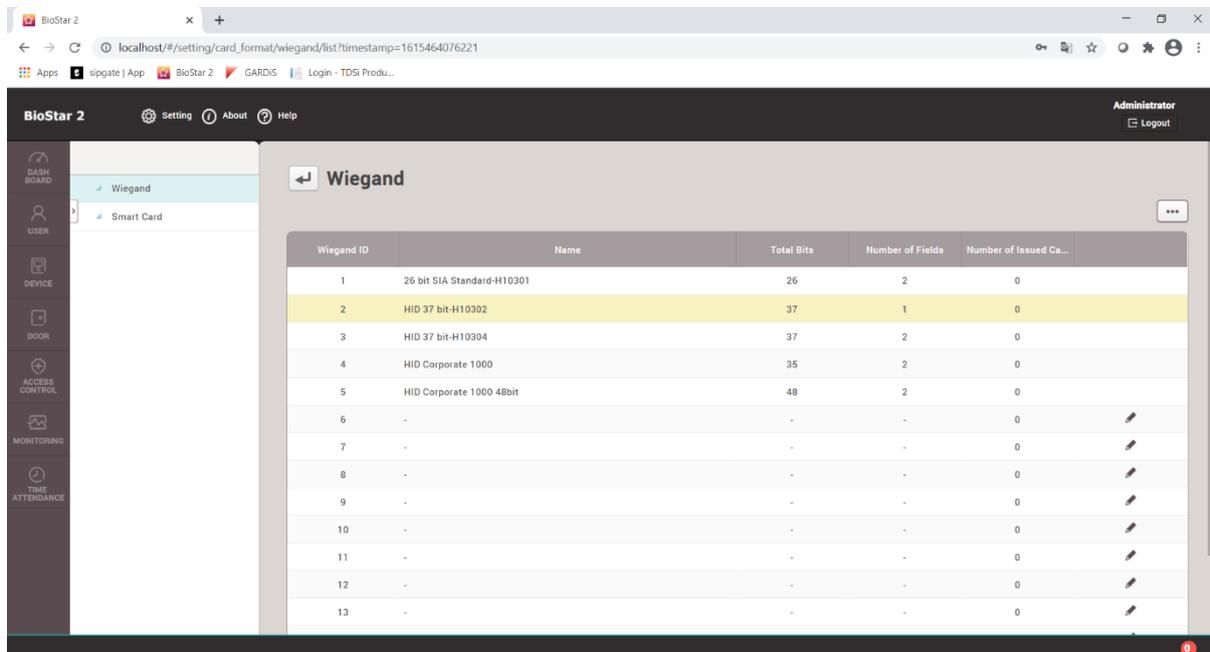


Figure 4

Go into the TDSi Suprema folder and edit the following configuration file :- SupremaW2Integration.exe.config. Ensure the SetTDSiWiegandConfig value equals the 37-bit Wiegand format in Figure 4 e.g. in the following example it is set to 2.

```

SupremaW2Integration.exe.config - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSec
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
  </startup>
  <connectionStrings>
    <add name="EXgarde" connectionString="Server={0}; Database={1}; User ID={2}; Password={3}" prov
  </connectionStrings>
  <appSettings>
    <add key="AccessControlSystem" value="EXgarde" />
    <add key="DatabaseServer" value=".\EXGARDE" />
    <add key="Database" value="EXGARDE" />
    <add key="DatabaseUserId" value="ExgardeUser" />
    <add key="DatabasePassword" value="GV72JPry6YzICxowhREkpa3E4U+u0tb3400QKJer6ys=" />
    <add key="KeyType" value="6" />
    <add key="SetTDSiWiegandConfig" value="2" />
    <add key="WiegandFormatId" value="42" />
    <add key="DesfirePrimaryKey" value="5WT7QuLQ30y4YudepuemT8WY5mV3YD2kJrx/dpXs1PYxTVZ+3hk+etNre8a
    <add key="DesfireAppId" value="1" />
    <add key="DesfireFileId" value="1" />
    <add key="TCMClientType" value="11" />
    <add key="SSLEnabled" value="0" />
    <add key="RootCertificatePath" value="Certificates/ca.cert.pem" />
    <add key="ServerCertificatePath" value="Certificates/server.cert.pem" />
  </appSettings>
</configuration>
Ln 20, Col 49      100%  Windows (CRLF)  UTF-8 with BOM

```

Figure 5

Once the readers have been configured correctly, ensure the BioStar 2 Services has been stopped. Failure to do so will prevent EXgarde from connecting to the biometric readers.

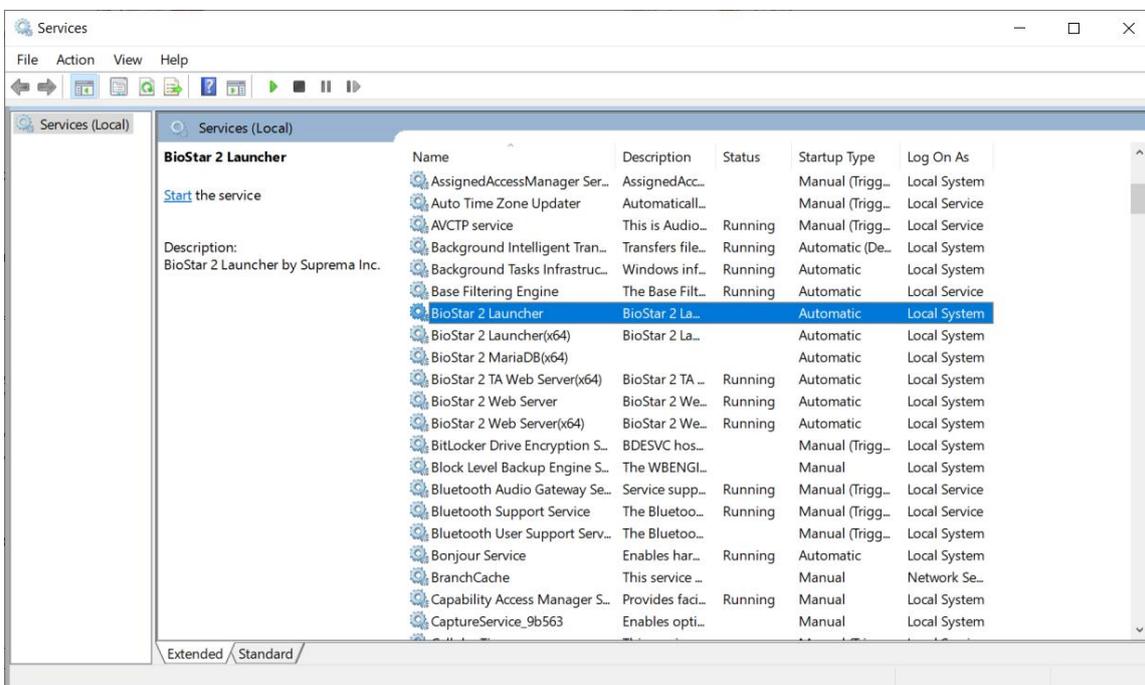


Figure 6



CAUTION! Ensure the BioStar 2 Service has been STOPPED before running EXgarde Communications

4. Suprema W2 service

To enable communications between EXgarde and the Suprema W2 readers, the Suprema W2 Service installed must be running.

The Suprema W2 Service Manager can be used to install the service and set the start-up method. This can be found in C:\Program Files (x86)\TDSi\Exgarde\Suprema W2\SupremaW2IntegrationServiceManager.exe

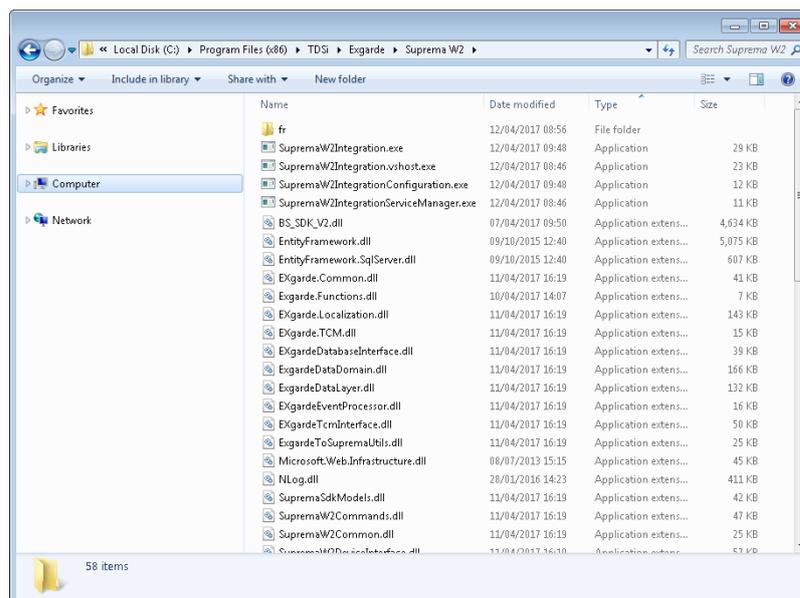


Figure 7

The Suprema Service Manager can be used to control/configure the Suprema Service; the start/stop buttons can be used to start or stop the service. When you first run EXgarde, the Suprema Service will be set to run in manual mode by default. This can be changed to run in Automatic mode by right clicking on the shortcut you have just created and selecting Run as administrator, click yes on the next screen to accept running as Administrator.

The Suprema Service Manager will open and 'Start-up type' will default to Manual. To enable Automatic start-up of the service, click Stop then Uninstall, then select Automatic from the drop-down list and click Install, next click on Start. From now on every time the PC running EXgarde is started the Suprema Service will start.

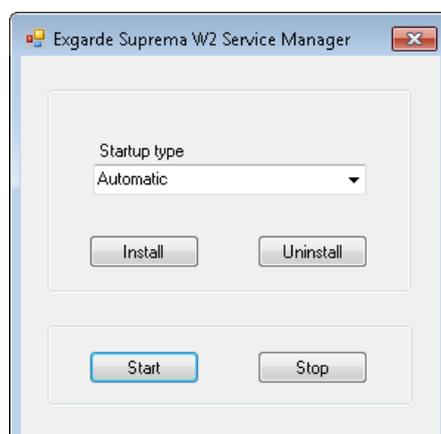


Figure 8

4.1 Suprema W2 Service Configuration

If a client installation of EXgarde is being used or if EXgarde is connecting to a custom database, the connections will need to be set up for the service to function correctly.

This can be found in C:\Program Files (x86)\TDSi\Exgarde\Suprema W2\SupremaW2IntegrationConfiguration.exe



NOTE: The configuration tool will need to be run as administrator

To access the service configuration tool, complete the login details

The screenshot shows a 'Login' dialog box with the following fields and values:

Tenant	Landlord
Operator	Admin
Password	*****

There is a 'Login' button at the bottom of the dialog.

Figure 9

The screenshot shows the 'EXgarde Suprema W2 Service Configuration' dialog box with the following fields and values:

Database Server	.\EXGARDE
Database Name	EXGARDE
Database User	ExgardeUser
Database User Password	*****
DESfire Key	*****
DESfire App Id	1
DESfire File Id	1

There are 'Update' and 'Enable SSL' buttons at the bottom of the dialog.

Figure 10

Database server – This needs to be the address of the server.

Database Name – This needs to be the name of the server .

Database User – This need to be the user login.

Database User Password – This needs to be the database password.

DESfire Key – Encrypton key used to access the DESfire cards

DESfire App ID – Location of data stored on DESfire card

DESfire File ID – Location of file store within the application

Once the information entered is correct click on **Update**

4.2 SSL (Secure Socket Layer) control

The SSL control feature will allow the data communicated between the service and the readers using a 4096 bit encrypted RSA key. This can also be configured to use custom certificates.

4.2.1 Enable SSL

To enable SSL between readers and the service, login in to the service configuration tool and click on the **Enable SSL** button at the bottom of the page.

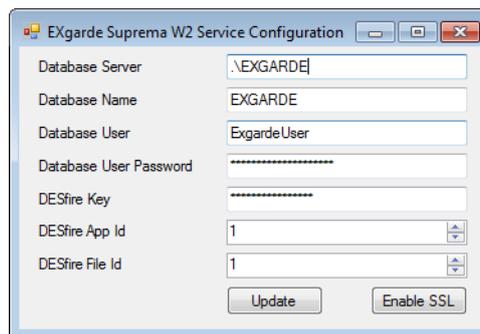


Figure 11

A message box will appear informing that the service will need to be restarted.

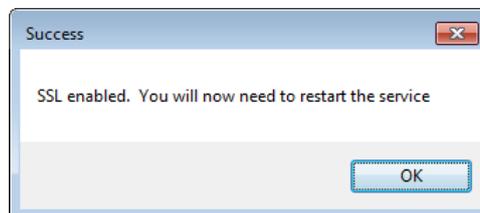


Figure 12

Click on the **OK** button and restart the service to complete the process.

4.2.2 Disable SSL

To disable the SSL feature, log in to the configuration tool and click on the **Disable SSL** button.

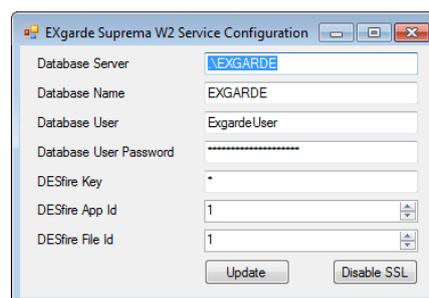


Figure 13

A message will appear informing of disabled readers and the requirement to restart the service

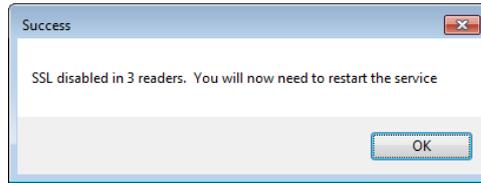


Figure 14

4.3 DESFire Card Configuration

The current encryption method use by Suprema is the Triple DES format, therefore the Suprema Service Configuration tool can also be used to allow the readers to operate with the Triple DES card technology.

For the Triple DES cards to function with the Suprema readers, the Master key, Application ID and the File ID must be available.

To set the application and file id's, log in to the configuration tool.

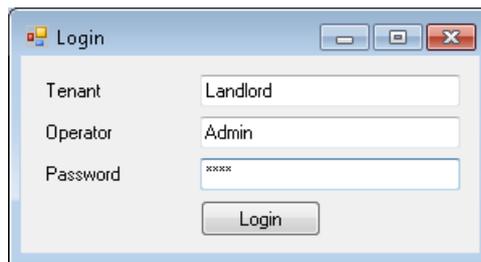


Figure 15

The DESFire Key application and file ID's will now be available to amend.

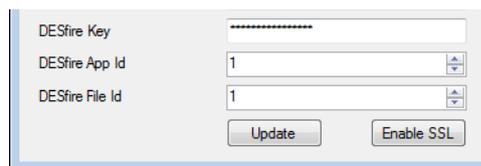


Figure 16

Perform the necessary changes and click on the **Update** button



NOTE: The service will need to be restarted and an ACU reset will need to be performed

5. Setting up Suprema in EXgarde

5.1 Suprema W2 Readers connected to controllers.

Log into the EXgarde using the default password **tdsi**. This can be changed later if required.

Once logged in, you will be presented with the EXgarde Home Page. From here you will be able to add the Suprema readers to the system.

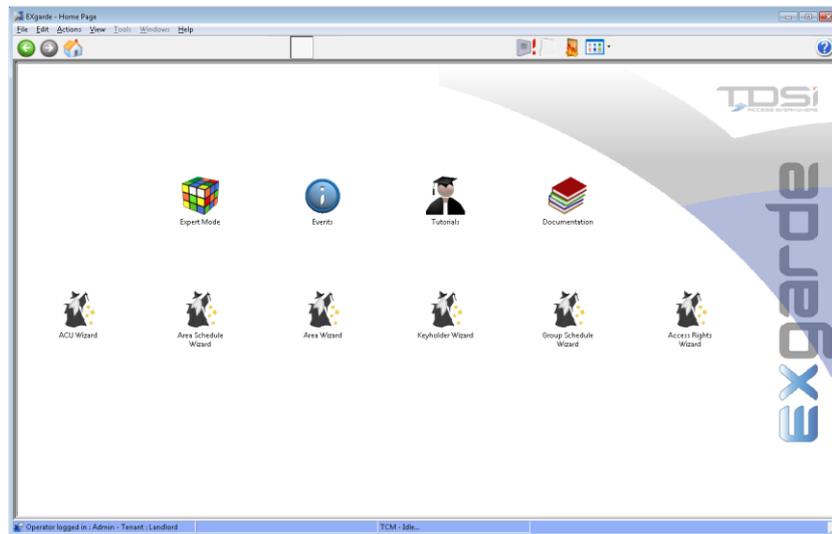


Figure 17

To begin adding the first reader, click on the ACU Wizard icon. This will guide to through the necessary steps for you to get the first reader online.

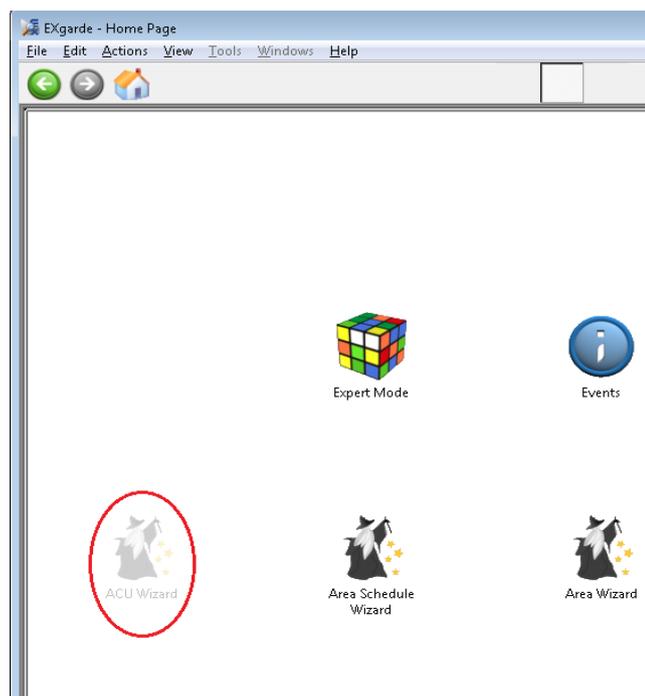


Figure 18

Follow the step through the process and when prompted to select the type of reader, select Suprema from the list.

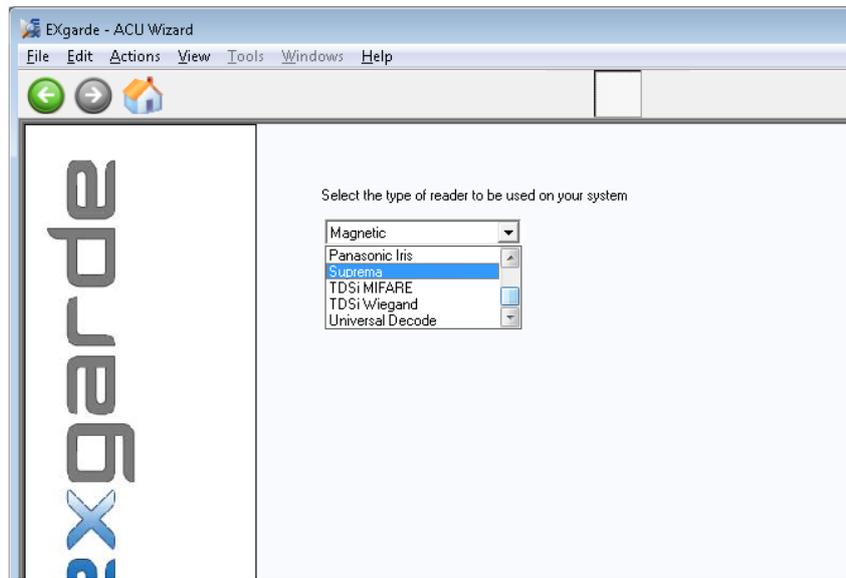


Figure 19

To add further door controllers as required, click the Start Again button. When all the readers have been added, click on the finished button.

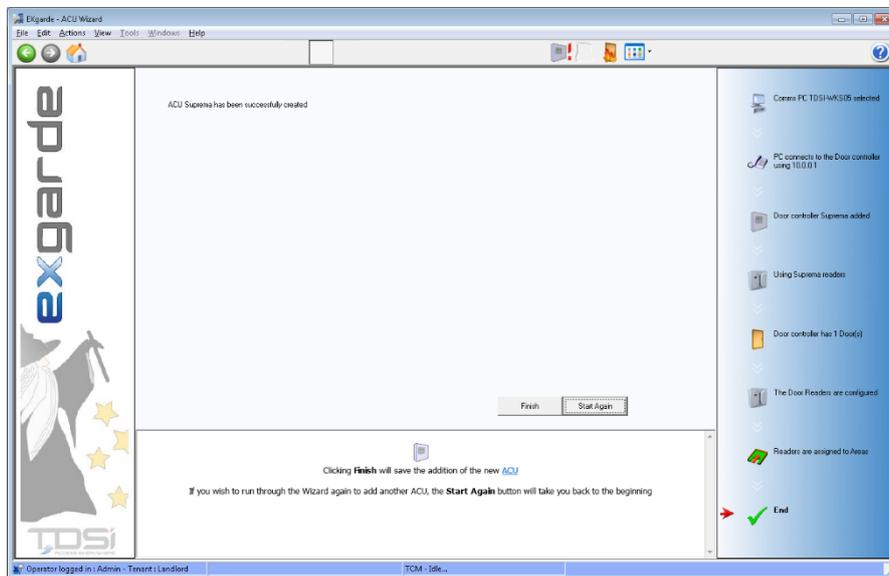


Figure 20

You will now need to set up the readers in the system. Click on the Expert Mode icon on the home page.

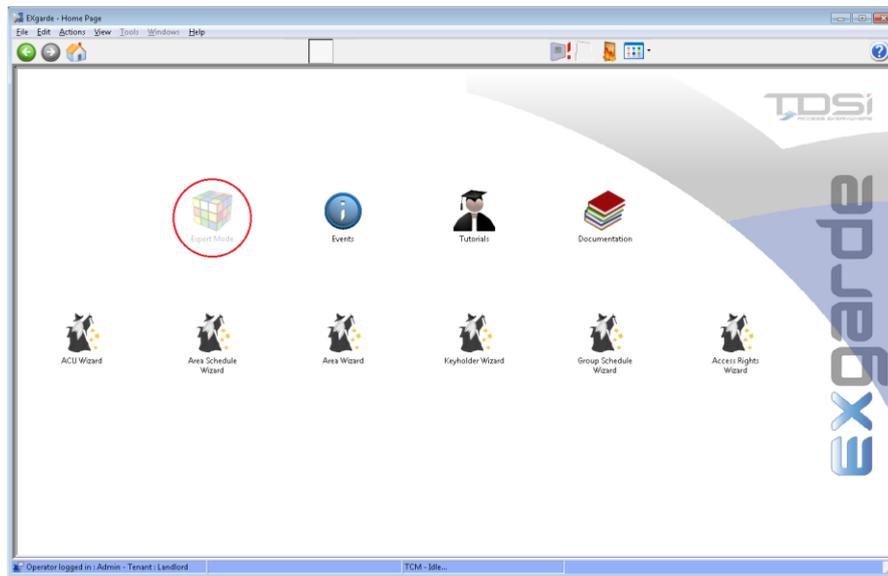


Figure 21

From the Shortcut bar on the left-hand side, click on the **Equipment** button.



Figure 22

To create a portal for the Suprema BioEntry W2 or BioStation readers, click on the Summary button and the select **Portals**.

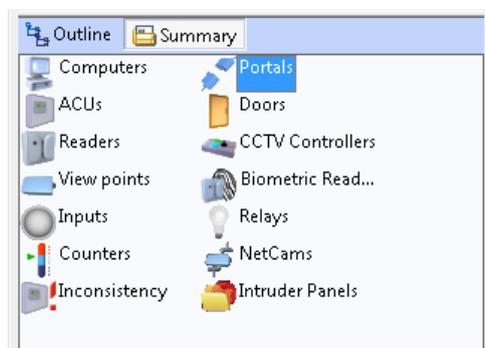


Figure 23

In the middle of the screen, click on the **New** button. Enter the name of your portal in the Name field

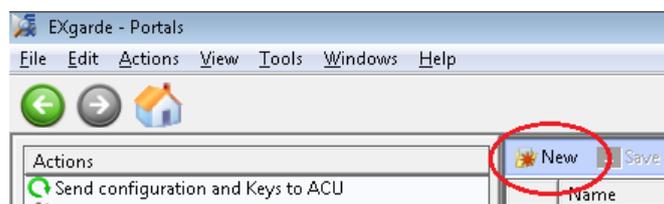


Figure 24

Select the Type of Portal to be Biometric

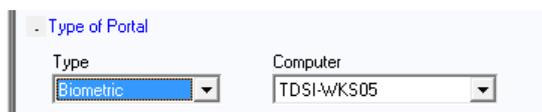


Figure 25

Select the Biometric Reader Model to be Suprema W2.

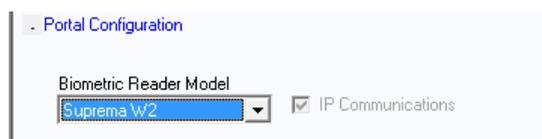


Figure 26

Check the IP communications Box and the click on **Save**.

Next in the Summary List on the left-hand side of the screen, select the Biometric Readers from the list.

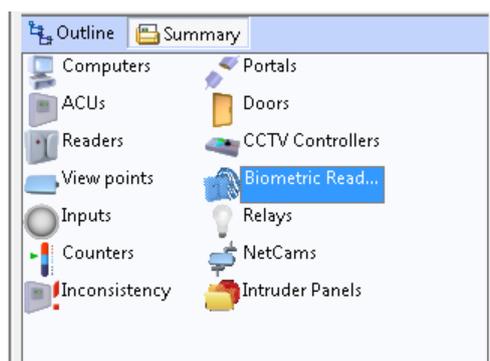


Figure 27

Click on the **New** button to create a new Biometric reader.

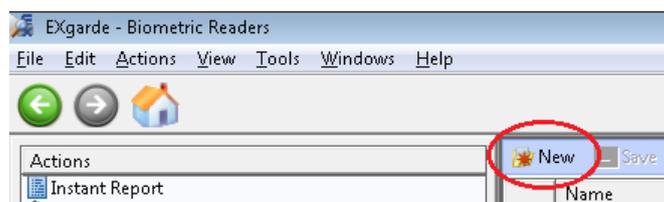
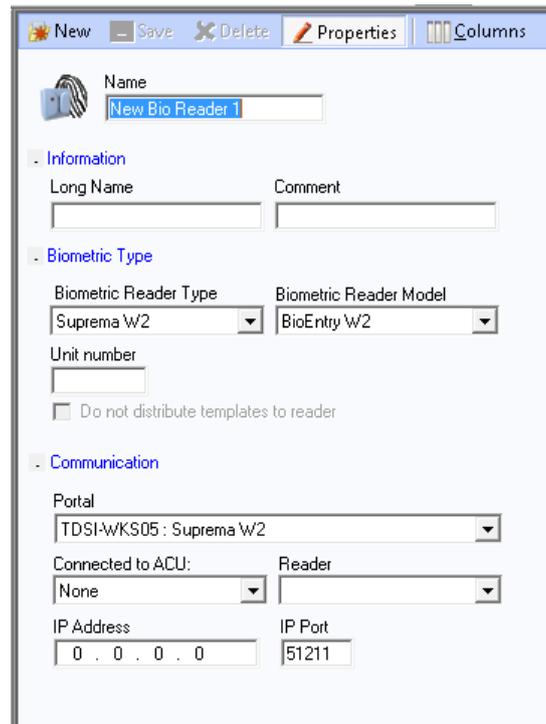


Figure 28

In the Reader properties window, complete the following fields.



The screenshot shows a software window titled 'Reader properties' with a toolbar containing 'New', 'Save', 'Delete', 'Properties', and 'Columns'. The main area is divided into sections:

- Name:** A text field containing 'New Bio Reader 1'.
- Information:** Two empty text fields labeled 'Long Name' and 'Comment'.
- Biometric Type:** Two dropdown menus: 'Biometric Reader Type' (set to 'Suprema W2') and 'Biometric Reader Model' (set to 'BioEntry W2'). Below them is an empty 'Unit number' field and a checkbox labeled 'Do not distribute templates to reader' which is unchecked.
- Communication:** A dropdown menu for 'Portal' (set to 'TDSI-WKS05 : Suprema W2'), two dropdown menus for 'Connected to ACU:' (set to 'None') and 'Reader' (empty), and two text fields for 'IP Address' (set to '0 . 0 . 0 . 0') and 'IP Port' (set to '51211').

Figure 29

- Type the name for the reader into the Name field.
- Select the Biometric Type as Suprema W2 and the model as BioEntry W2.
- Enter the Unit Serial Number as specified in the Suprema BioStar2 software.
- Select the Controller and reader to which the reader is physically connected to.
- Finally, enter the IP address for the Suprema reader and the port to 51211
- Once done, click **Save**.

To add more readers to the system, repeat this process until finished.

Finally, Start the EXgarde Communications application to establish connect to the door controllers and readers.

5.2 Suprema W2 as a standalone ACU

The new Suprema W2 integration can also operate as standalone access controllers, eliminating the requirement for access control units.

To setup a BioEntry W2 or BioStation W2 access reader, login to EXgarde and select the expert function from the home page.

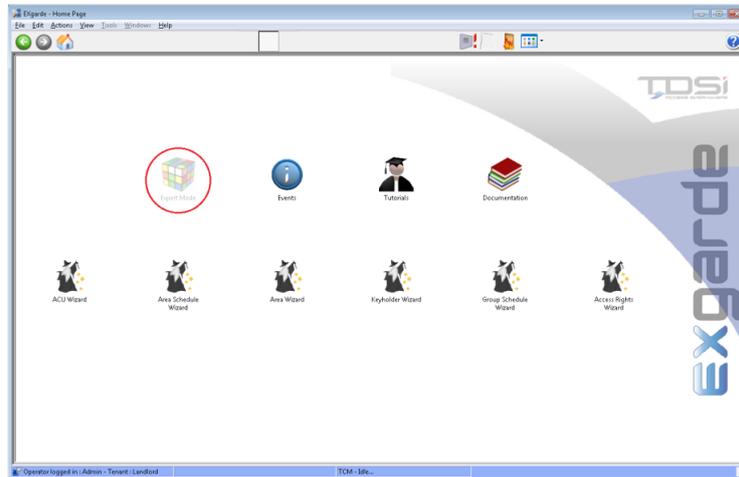


Figure 30

From the Shortcut bar on the left-hand side, click on the **Equipment** button.



Figure 31

To create a portal for the Suprema BioEntry W2 or BioStation readers, click on the Summary button and the select **Portals**.

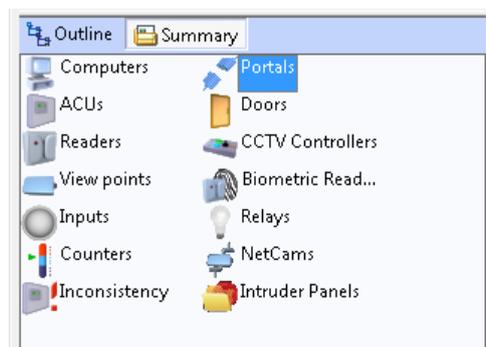


Figure 32

In the middle of the screen, click on the **New** button. Enter the name of your portal in the Name field



Figure 33

Select the Type of Portal to be Biometric



Figure 34

Select the Biometric Reader Model to be Suprema W2.

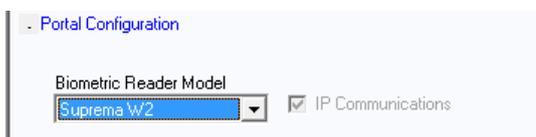


Figure 35

Check the IP communications Box and the click on **Save**.

Next in the Summary List on the left-hand side of the screen, select the ACUs from the list.

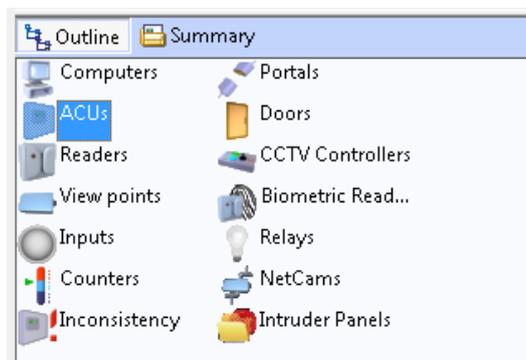


Figure 36

Click on the **New** button to create a new Biometric reader.

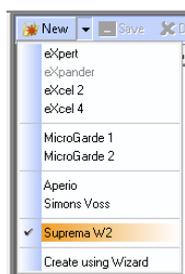


Figure 37

With the new ACU created, give it an appropriate name and click on the Save button.

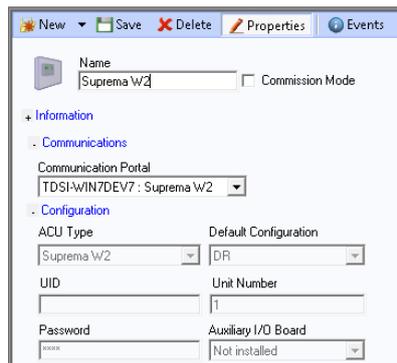


Figure 38

Next, click on the Outline button in the left hand menu to access the outline view.

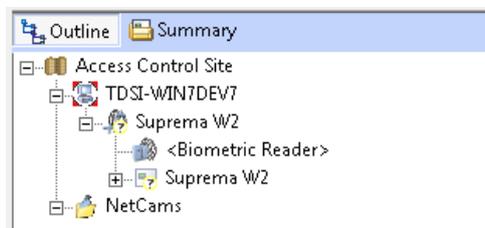


Figure 39

Select the New Bio Reader 1 from the list.

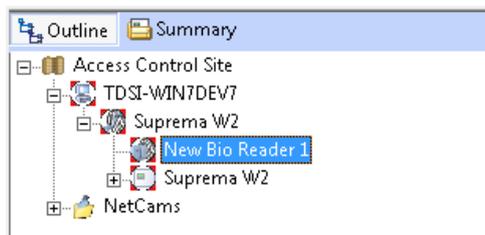
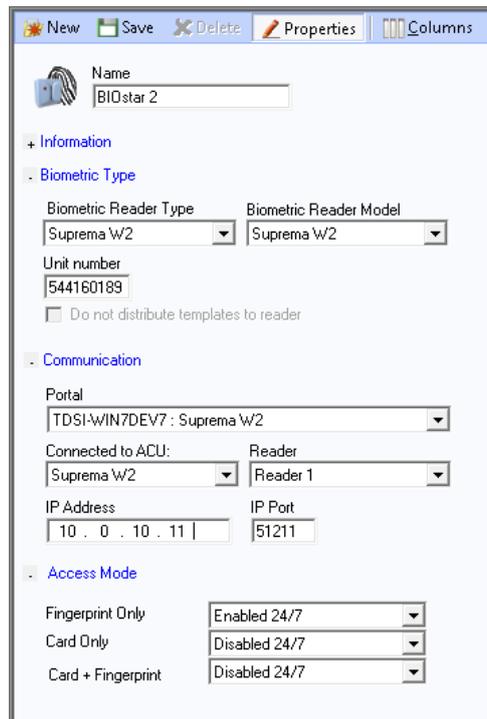


Figure 40

Select the Properties tab and complete the required fields



The screenshot shows a software configuration window with the following fields and values:

- Name: BI0star 2
- Information section:
 - Biometric Type section:
 - Biometric Reader Type: Suprema W2
 - Biometric Reader Model: Suprema W2
 - Unit number: 544160189
 - Do not distribute templates to reader:
 - Communication section:
 - Portal: TDSI-WIN7DEV7 : Suprema W2
 - Connected to ACU: Suprema W2
 - Reader: Reader 1
 - IP Address: 10 . 0 . 10 . 11 |
 - IP Port: 51211
 - Access Mode section:
 - Fingerprint Only: Enabled 24/7
 - Card Only: Disabled 24/7
 - Card + Fingerprint: Disabled 24/7

Figure 41

- **Biometric Reader Type** – Select Suprema W2
- **Biometric Reader Model** – Select Suprema W2
- **Unit Number** – Enter the reader serial number (*found on the back of the reader*)
- **Portal** – Select the Portal the reader is attached too
- **Connected to ACU** – Select the ACU reader is attached too
- **Reader** – Select Reader 1
- **IP Address** - Enter the reader IP address
- **IP Port** - this should be set to default 51211 unless user defined

5.3 Adding a Secure I/O 2 module

If a secure I/O module has been added to the BIOstar2 ACU door entry system, it will need to be set up in EXgarde.

To set up the Secure I/O module, select the ACU the module will be attached too and open the properties menu.

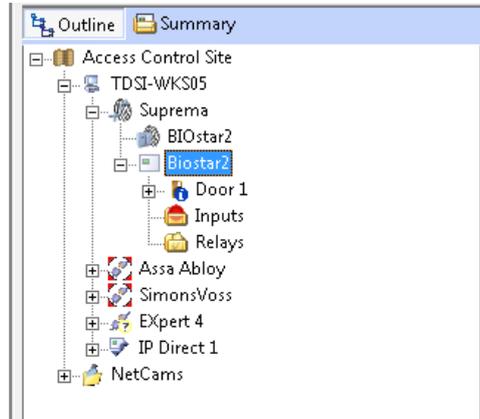


Figure 42

Enter the serial number of the I/O module found on the back of the unit into the Comments field, under the Information tab and click save. The IO unit will now be operational.

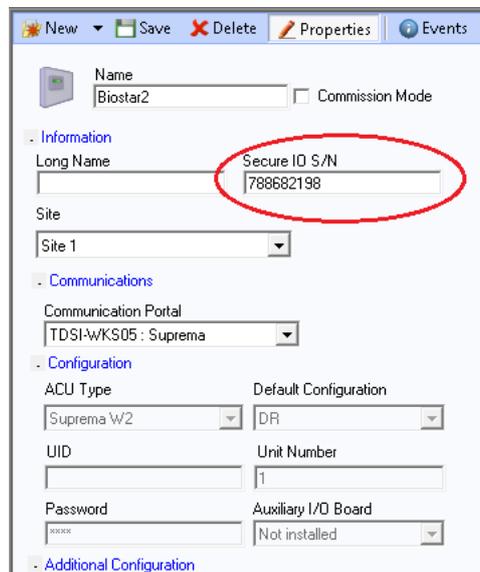


Figure 43

Complete the process by clicking **Save**. The Suprema reader will now be updated to recognise the I/O module.

6. BIOstar 2 reader door setup

6.1 Associate Doors to an Access Area

Click on Equipment in the Navigation Window

Click on Summary

Click on Doors

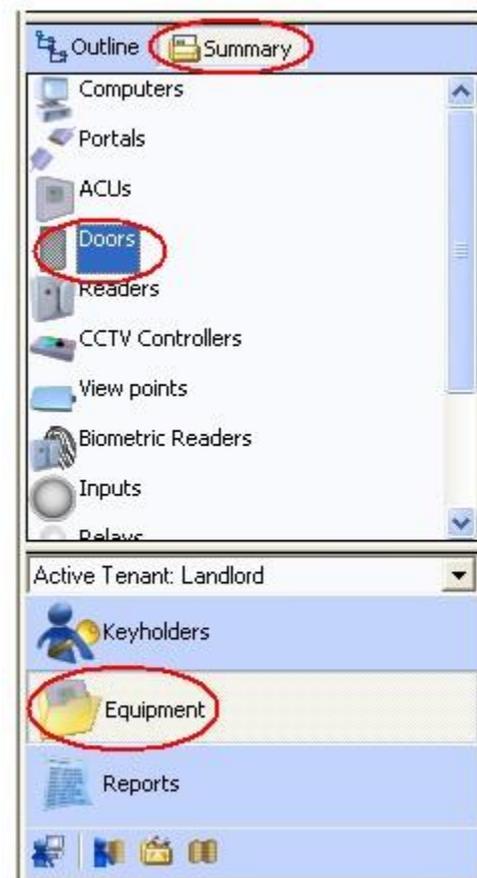


Figure 44

In the main window select the door you wish to define

Click on the Properties button in the Toolbar

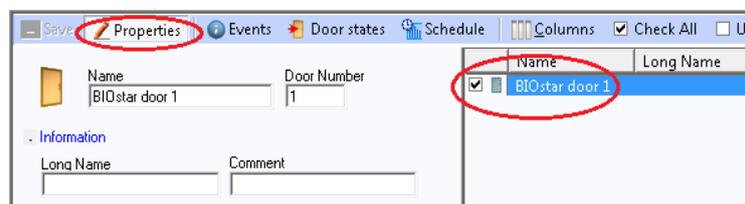


Figure 45

6.2 Fire door setup

To enable the door as a Fire Door expand the Options section and tick the Fire Door option. If the associated inner or outer area for the door is configured as a fire door area, then the door will become unlocked when the fire input is activated

The screenshot shows a configuration panel titled 'Options'. It contains three main elements: a checked checkbox for 'Enabled', a checked checkbox for 'Fire Door' which is circled in red, and a 'Display as' dropdown menu currently set to 'Door'.

Figure 46

6.3 Door access area setup

To setup the Door's access areas expand the Access Areas section (Figure 32) In the Outer & Inner Area drop downs, select the 2 Access Areas which are either side of the door

The screenshot shows a configuration panel titled 'Access Areas'. It features two dropdown menus: 'Outer Area' and 'Inner Area', both of which are currently set to 'Public'.

Figure 47

6.4 Reader Location

Expanding the Additional tab will select where the reader or readers are located with respect to the Inner area.

The screenshot shows a configuration panel titled 'Additional' with several tabs: 'Readers', 'I/O', 'Functions', 'Schedule', and 'Events'. The 'Readers' tab is active. It contains a 'Readers' dropdown menu set to 'Reader 1' and a 'Located' section with radio buttons for 'Outside' (selected) and 'Inside'.

Figure 48

6.5 Door Functions

Expanding the Functions tab will allow you to edit the Local & Remote Alarms and Lock Off Condition

The screenshot shows the 'Functions' tab within the 'Additional' configuration panel. It includes two input fields: 'Local Alarm Delay (seconds)' with the value '15' and 'Remote Alarm Delay (minutes)' with the value '45'. Below these is a 'Lock Off Condition' dropdown menu set to 'Door Opened'. At the bottom, the 'Man Trap' section has a 'Group' dropdown set to 'None' and a 'Type' dropdown set to 'Inside Door'.

Figure 49

Local Alarm Delay

Once the time (in seconds) has been configured, the Door may stay open for defined time before the ACU generates a Local Alarm by the operating the on-board sounder.

Remote Alarm Delay

Once the time (in minutes) has been configured, the Door may stay open for a defined time before the ACU generates a Remote Alarm.

Local and remote alarms will generate an event after the door has been left ajar for the specified time.

Lock Off Condition

The Lock Off Condition determines when the door lock strike relay will turn off after the relay has been energized.

Door Opened - Lock strike relay will turn off as soon as the door is opened.

Door Closed - Lock strike relay will turn off as soon as the door is closed.

Lock strike Timed Out - Lock strike relay will turn off after the lock strike time has elapsed.

6.6 Door Schedule

Expanding the Schedule tab will allow you to apply a Door Schedule (i.e., doors unlocked 9am to 5pm).

Select an available schedule from the drop-down list. Selecting Relay Off 24/7 means that the door will be locked all day, every day for normal access.

Selecting Relay On 24/7 means that the door will be unlocked all day, every day.

The Apply Schedule option determines how the schedule should be applied during days defined as holidays.

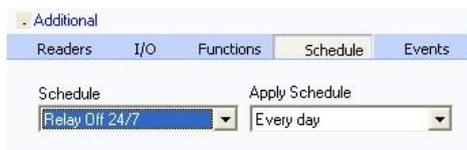


Figure 50

6.7 Manual Door Control

If you wish to manually select the door to follow an action (overriding the door schedule), then you can do this by selecting the door in the list view and selecting one of the following actions located in the Actions Window:



Figure 51

6.7.1 Release Door

Releases the Door manually (as when the Egress Button is pressed) which will follow the relay opening time (default of 4 seconds).

6.7.2 Unlock Door for Free Access

Unlocks the Door (it will remain unlocked until another manual or scheduled event causes it to become locked).

6.7.3 Lock Door to Stop All Access

When a door is barred, the readers and egress buttons are disabled, preventing all access via the door.

6.7.4 Set Door to Controlled Access

Will cancel all manual overrides and allow the door to follow the schedule it has been attached to. Doors can also be triggered by a Fire Input. This specifies if the door is to be automatically released on an input designated as a fire input becoming active. So, when the ACU receives an input from the fire panel, if selected as a Fire Door, it will remain unlocked until the fire panel has been reset and the Fire Input processed.

7. Alarms

To create an alarm (using Door Forced as an example) select the Equipment Button in the Shortcut window and then select Summary from the Navigation Window



Figure 52

In the main window, select your door you wish the alarm to be applied to and click on the **Properties** button.

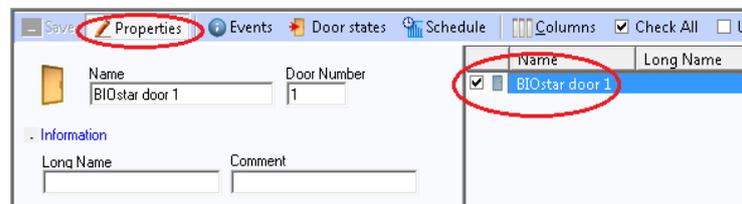


Figure 53

Next click on the Additional Drop-Down header and then on the **Events** tab.

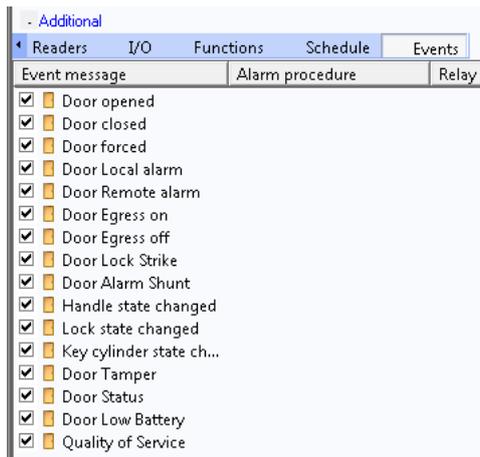


Figure 54

Right-click on the event you wish the alarm to apply to and select **Properties** from the menu that appears .

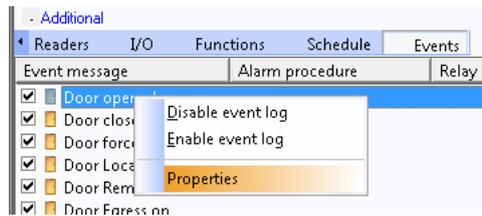


Figure 55

In the Event Action Details window, tick on the **Generate Operator Alarm** option box.

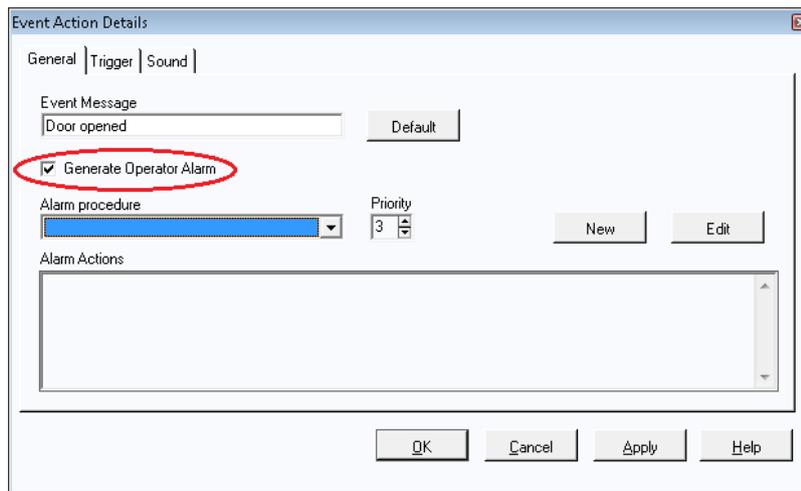


Figure 56

If there are no Alarm Procedures or you wish to create a new one, click on New

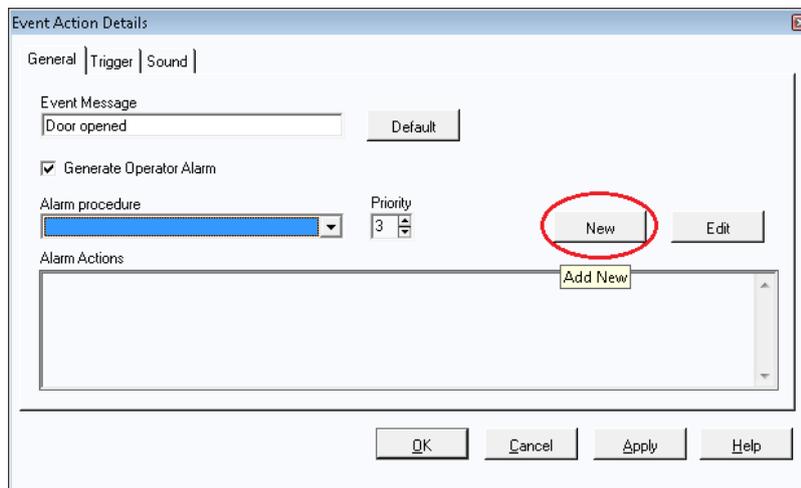


Figure 57

Name the procedure an in the Operator Actions box, every line entered becomes a task the operator must acknowledge and take responsibility for

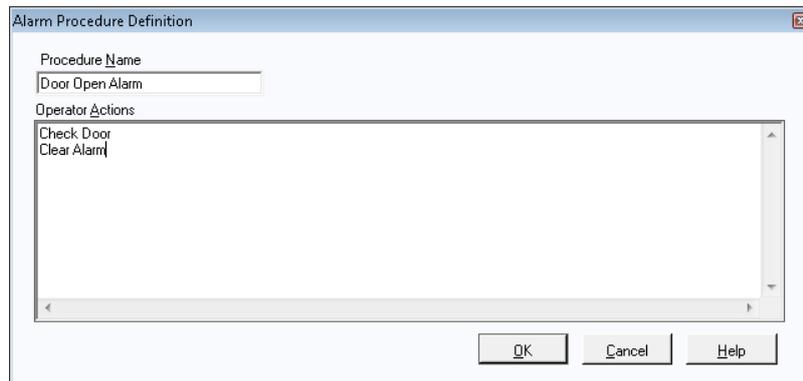


Figure 58

Once complete Click OK

If the event will be activating a relay or 3rd party, click on the **Trigger** tab.

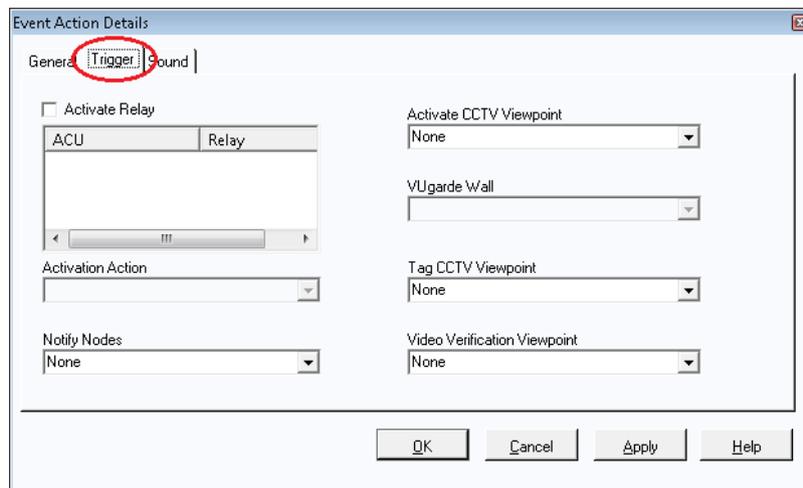


Figure 59

For the event procedure to activate a relay (a spare relay must be available on the system) then highlight it in the relay window and select the relay from the list.

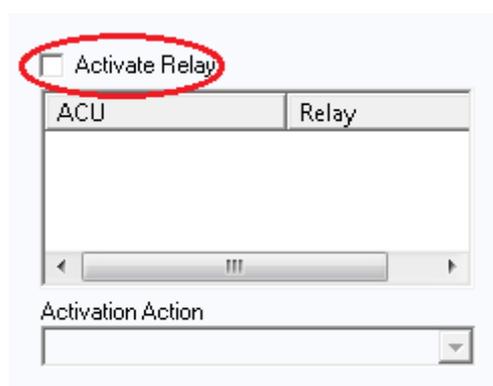


Figure 60

If the action will be triggering a CCTV operation, select the item from the desired CCTV options.



A screenshot of a configuration window showing four dropdown menus. The first menu is labeled 'Activate CCTV Viewpoint' and has 'None' selected. The second menu is labeled 'VUgarde Wall' and is empty. The third menu is labeled 'Tag CCTV Viewpoint' and has 'None' selected. The fourth menu is labeled 'Video Verification Viewpoint' and has 'None' selected.

Figure 61

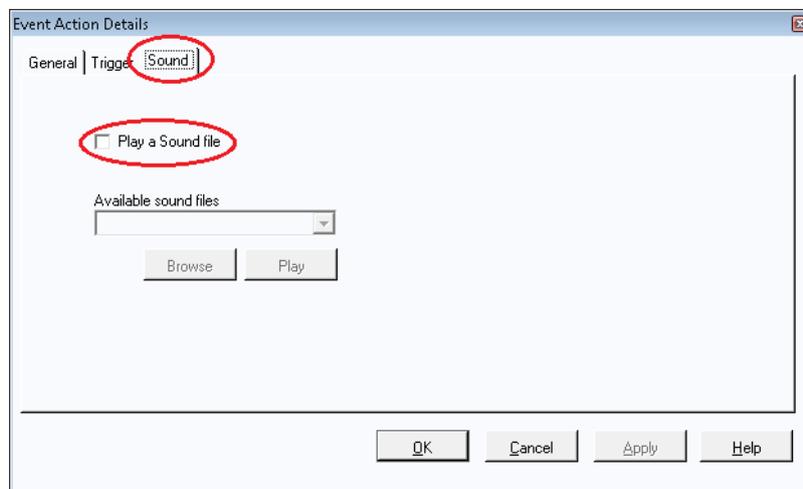
If remote notifications are setup, select the node from the Notify Nodes dropdown.



A screenshot of a 'Notify Nodes' dropdown menu with 'None' selected.

Figure 62

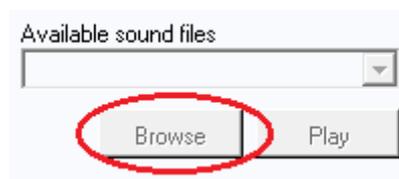
If the event will be activating a sound file, click on the **Sound** tab.



A screenshot of the 'Event Action Details' dialog box. The 'Trigger' tab is selected and circled in red. Below it, the checkbox 'Play a Sound file' is also circled in red. Underneath, there is a section for 'Available sound files' with a dropdown menu, 'Browse', and 'Play' buttons. At the bottom of the dialog are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Figure 63

If you wish a WAV file to be sounded on the PC when the alarm occurs, then click on browse and select your sound file and click OK.



A close-up screenshot of the 'Available sound files' section, showing the 'Browse' button circled in red.

Figure 64

When you are happy with the alarm procedure, click **OK** and you will see the event icon in the door properties change to a red explanation mark

Event message	Alarm procedure	Relay
  Door opened	Door Open Alarm	
<input checked="" type="checkbox"/>  Door closed		

Figure 65

When ready to save changes, you will be prompted to associate this with an Alarm Zone

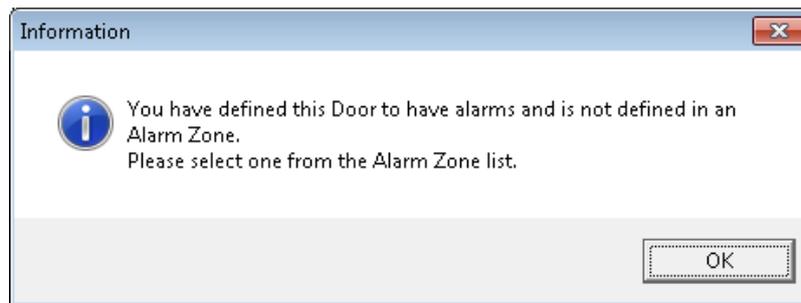


Figure 66

From the drop down menu, select the Alarm Zone you wish this procedure to follow and click ok

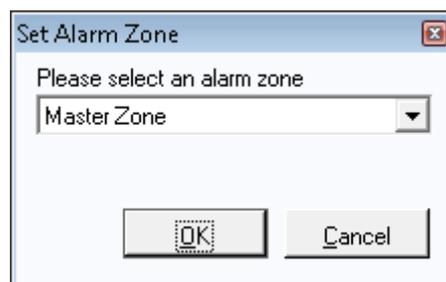


Figure 67

When the action is triggered the Alarm Monitor window will pop up.

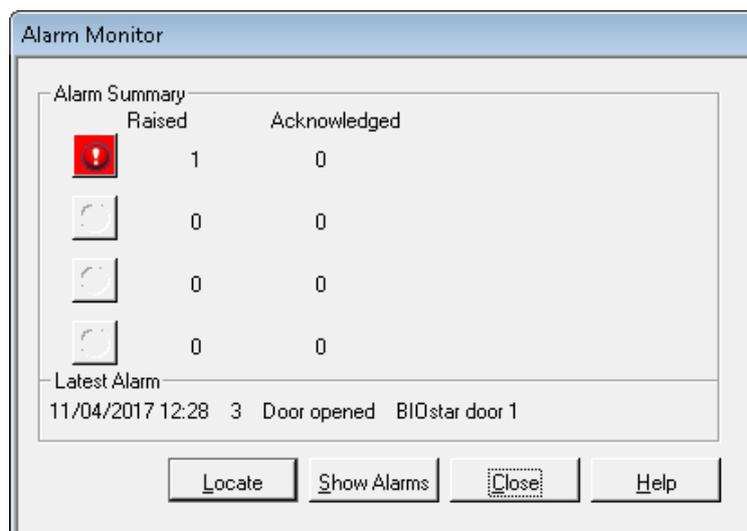


Figure 68

Next click on the **Show Alarms** button, this will bring up the Alarm window.

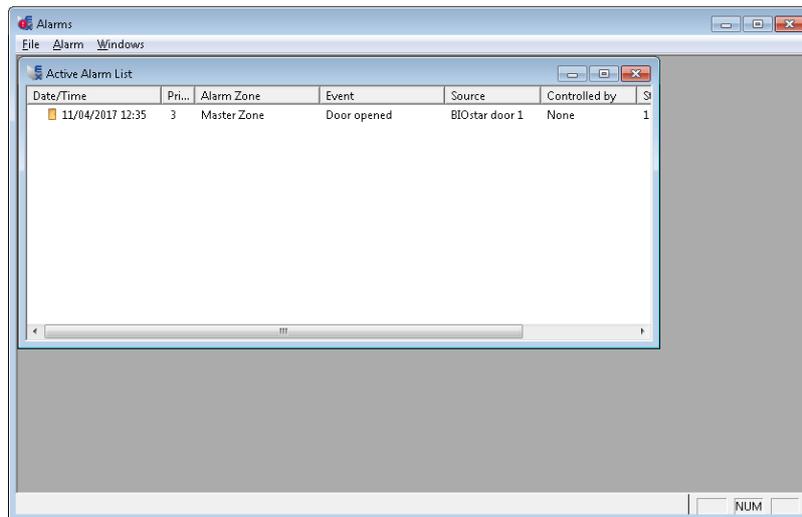


Figure 69

To view the alarm, double click on the alarm to bring up the Alarm Control window. This window will allow the user to action the alarms and perform the required tasks by clicking on the **Take Control** button.

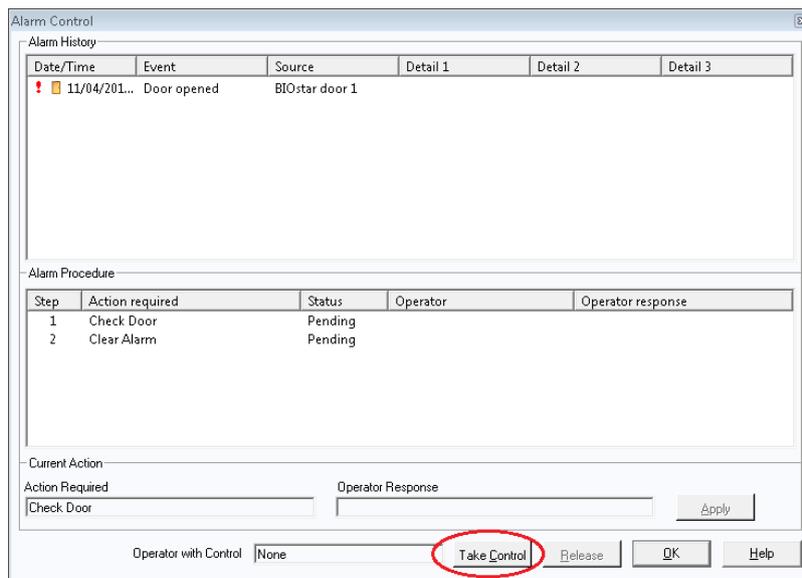


Figure 70

The Operator Response window will become live and the Apply button will now be enabled to perform the response required by the Action.

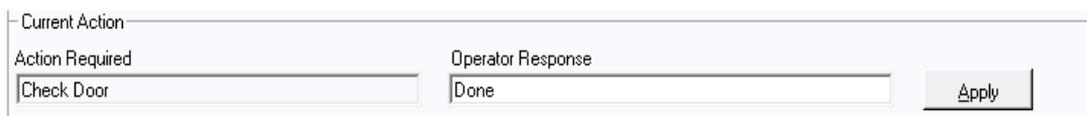


Figure 71

8. Schedules

The Suprema EXgarde integration will allow custom schedules to be applied to the readers providing greater levels of access capabilities.

8.1 Relay Schedules

Click on System Settings in the Shortcut Window and select Schedules. Then click on Relay Schedules.

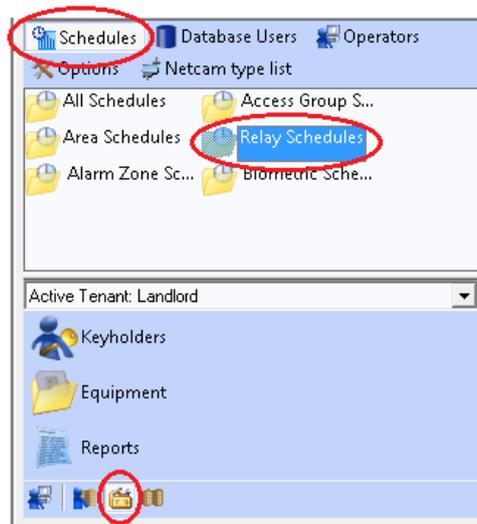


Figure 72

Click on New on the Tool Bar or click the arrow and select Relay Schedule from the drop down list.

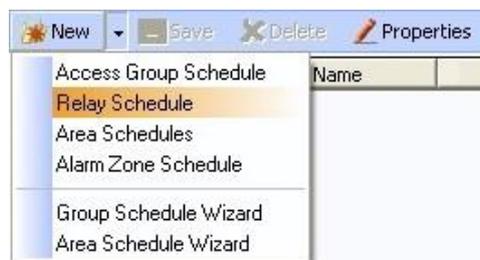


Figure 73

A new schedule will now appear in the main window.

Next select the new schedule and click on the **Editor** in the Tool Bar and using your left mouse button, select the Access Mode you desire and drag & drop it onto the Single Day grid.



Figure 74

Then by hovering the mouse pointer over the edge of the box, expand it to your desired time. To fine tune the period starts, and period ends times you can use the up and down arrows in the 'hh mm' boxes

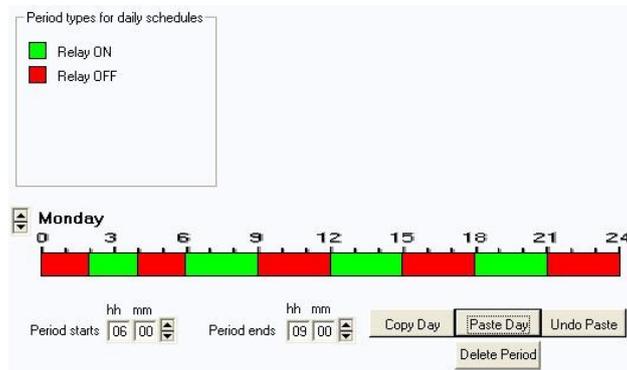


Figure 75

If your days are going to be following the same time, then you can copy & paste the mode and time to other days in the week.

To select the different days, use the Up & Down arrows

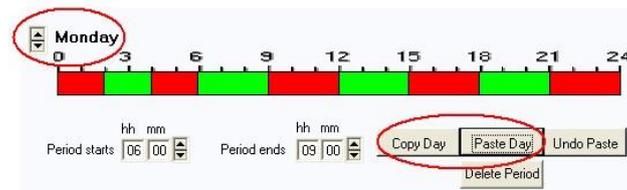


Figure 76

When the time schedules have been set up, click on Save

Now you can associate the Schedule with your Relay

In the same window, expand the List Menu

Select what relays you wish to follow the schedule by ticking them



Figure 77

Click on **Save** once the setup is complete.

The new schedule will now be displayed in the Lock Strike properties menu under the **Additions, Schedules** tab

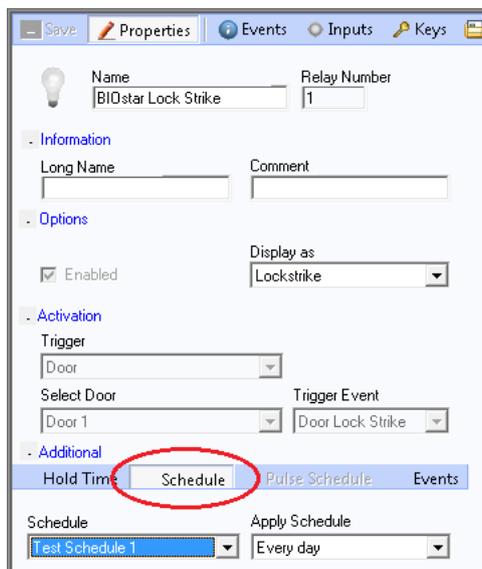


Figure 78

If you have more schedules configured, these will be displayed in the drop-down menu.

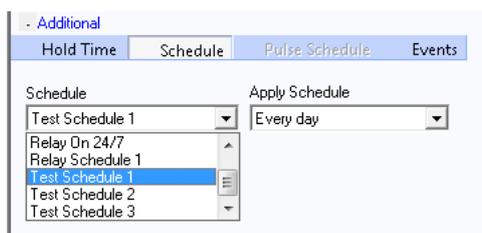


Figure 79

The selected schedule can also be apply with conditions. Three pre-set conditions are available.

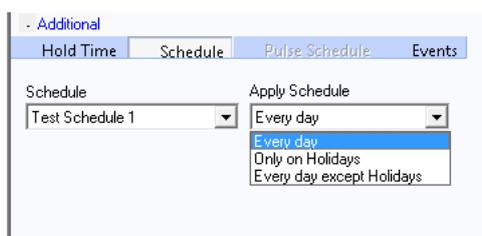


Figure 80

- Every day** – Schedule will apply to everyday
- Only on Holidays** – Schedule will only apply on holidays
- Every day except Holidays** - Schedule will apply to every day except Holiday periods

8.2 Biometric Schedules

As with the relay schedules, biometric schedules can be applied with the principles. Click on System Settings in the Shortcut Window and select Schedules. Then click on Biometric Schedules.

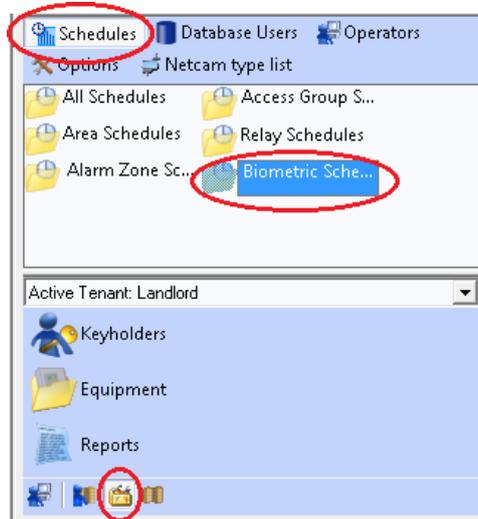


Figure 81

Click on New on the Tool Bar or click the arrow and select Biometric Schedule from the drop down list

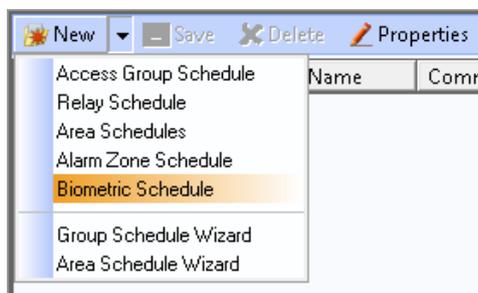


Figure 82

A new schedule will now appear in the main window.

	Name	Long Name	Comment	Type
<input checked="" type="checkbox"/>	Biometric Sche...			Biometric Schedule
<input type="checkbox"/>	Disabled 24/7			Biometric Schedule
<input type="checkbox"/>	Enabled 24/7			Biometric Schedule

Figure 83

Next select the new schedule and click on the **Editor** in the Tool Bar and using your left mouse button, select the Access Mode you desire and drag & drop it onto the Single Day grid.

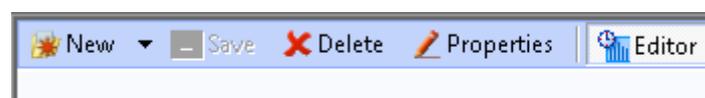


Figure 84

Then by hovering the mouse pointer over the edge of the box, expand it to your desired time. To fine tune the period starts, and period ends times you can use the up and down arrows in the 'hh mm' boxes

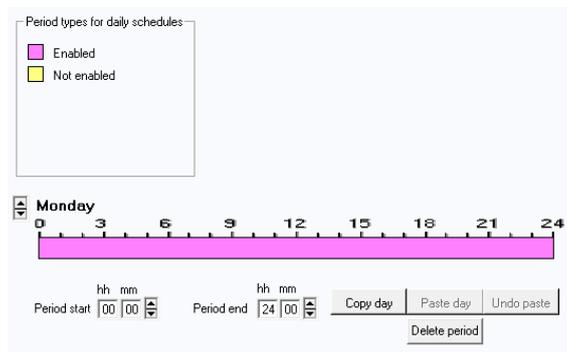


Figure 85

If your days are going to be following the same time, then you can copy & paste the mode and time to other days in the week. To select the different days, use the Up & Down arrows

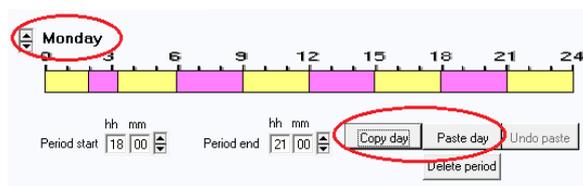


Figure 86

When the time schedules have been set up, click on **Save**. The new schedule will now be displayed under each of the Access Mode

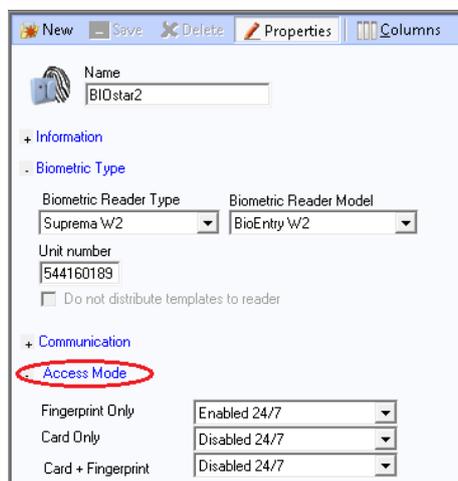


Figure 87

If you have more schedules configured, these will be displayed in the drop down menu against each method of entry.

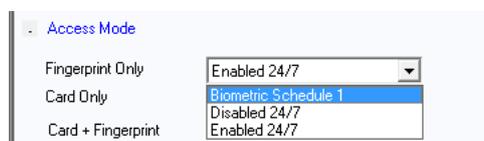


Figure 88

9. Biometric Enrolment Reader

To specify a reader for enrolment, Click on **Tools** and select **Options**

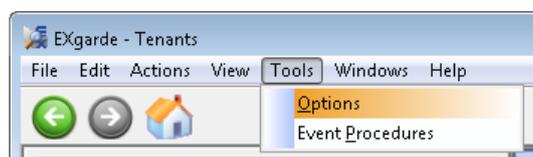


Figure 89

From the options, select **Biometric Enrolment**.

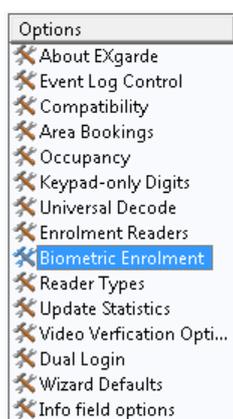


Figure 90

Next, scroll the top bar until the **Suprema BioEntry Finger** option appears.

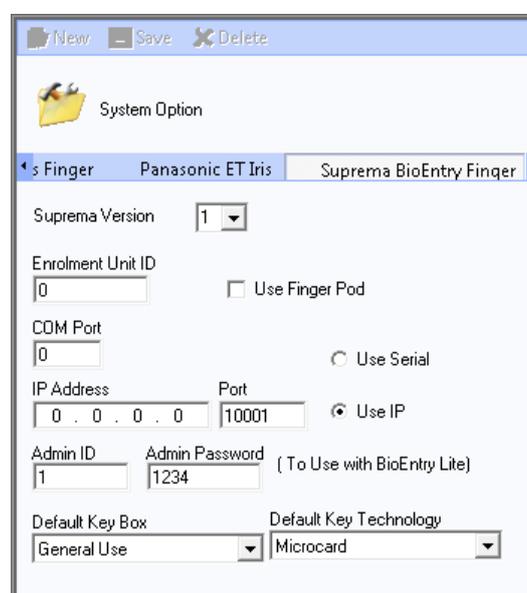


Figure 91

Enter the following details into the fields

- Suprema Version - Set to 2
- Enrolment Unit ID – Reader Serial number
- IP address – Reader IP Address
- Port – set to 51211

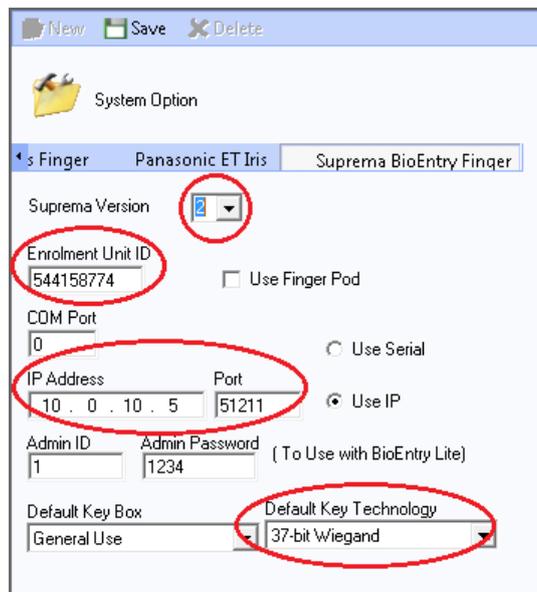


Figure 92

10. Adding a Keyholder to EXgarde

To set up and keyholder on the EXgarde system, click on the **Keyholders** button on the Shortcut Bar.



Figure 93

Click on the **Keyholders** tab and select the **All keyholders** from the list

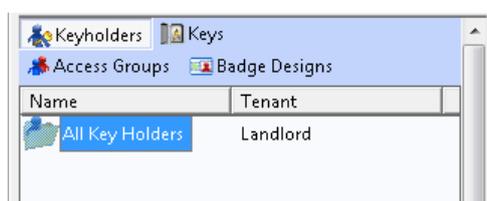
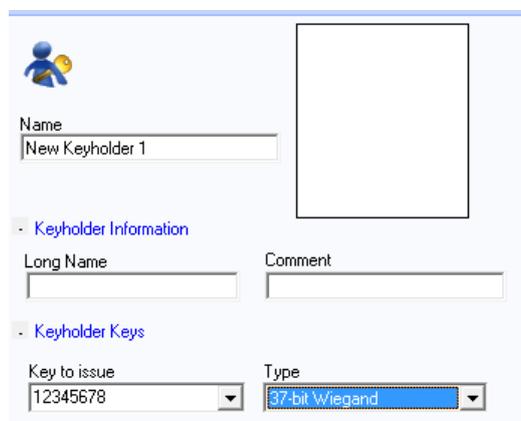


Figure 94

Click on the **New** button to create a new Keyholder. This will allow full access to the Biometric integration features of the software.

- Enter the user's name into the **Name** field.
- Enter **Key to issue** number in the **Keyholder Keys** section.
- Change the **Type** to 37-bit Wiegand and type in a key number. This is the number used to identify that keyholder in both the fingerprint template and also door controller.

Click on the **Save** button when done.



Name
New Keyholder 1

Keyholder Information

Long Name
Comment

Keyholder Keys

Key to issue
12345678

Type
37-bit Wiegand

Figure 95

11. Adding a Keyholder Biometric Template

With the Keyholder entered into the system, click on the **Biometrics** tab at the top of the screen.



Figure 96

With the Biometric window now open, click on the **Type of biometrics** and select **Suprema Finger** and from the **Associate Key** drop down, select the keyholders 37-bit Wiegand key

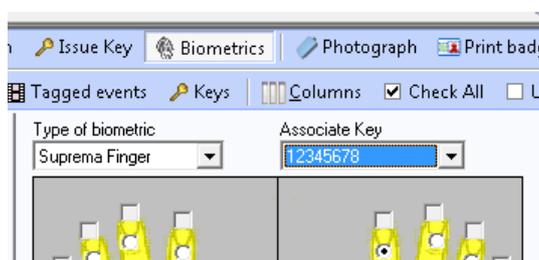


Figure 97

Next, click on the radial button of the finger to be enrolled and then click **Capture**.

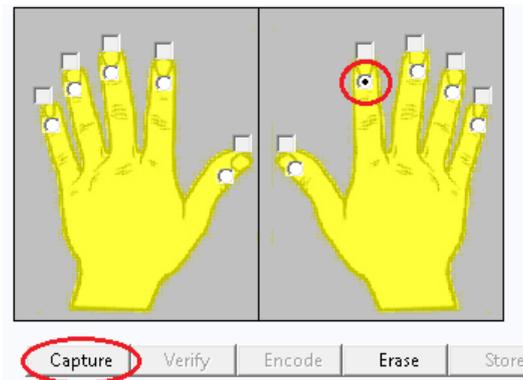


Figure 98

The window below will pop up prompting you to present the finger twice on the reader to enrol

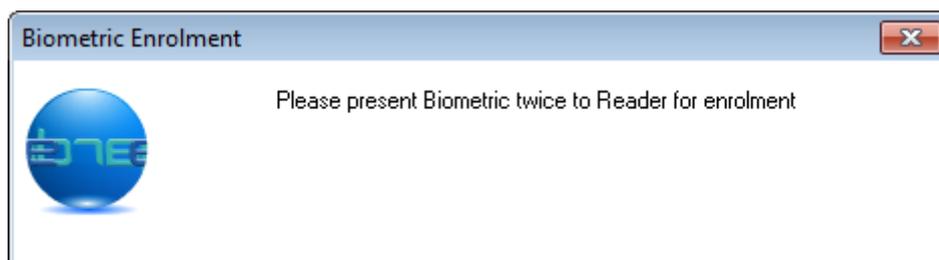


Figure 99

If the template has been captured successfully, the below message box will appear.

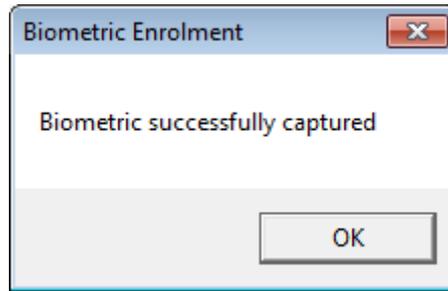


Figure 100

If however, the template was not successfully captured, the below message will appear and you will have to recapture the template.

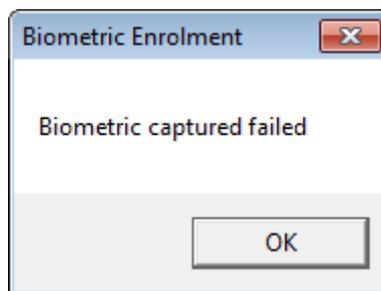


Figure 101

With the template now captured, click on the **Store** button to save the template to the database. This will also send the template to all applicable readers.

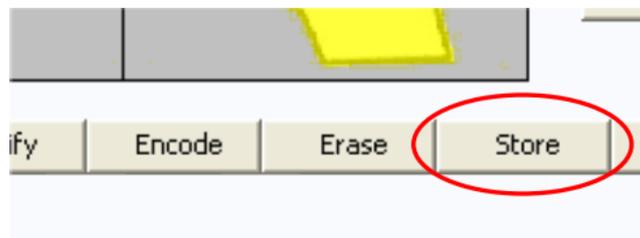


Figure 102

To test the system, present your finger to the reader. If the system is operating correctly the reader will indicate that the print has been accepted.

12. Reloading templates to readers

To reload templates to readers firstly select the reader from either the Outline View *figure 92* or the main window *figure 63*

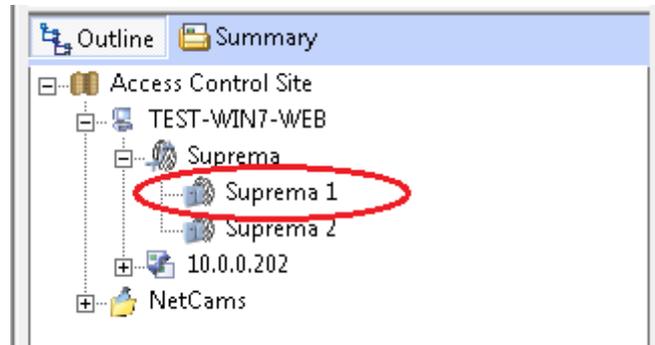
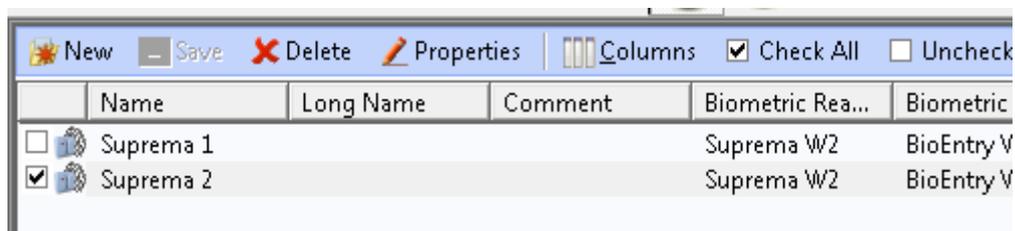


Figure 103



	Name	Long Name	Comment	Biometric Rea...	Biometric
<input type="checkbox"/>	Suprema 1			Suprema W2	BioEntry V
<input checked="" type="checkbox"/>	Suprema 2			Suprema W2	BioEntry V

Figure 104

Next click on **Reload Templates** from the Actions windows.

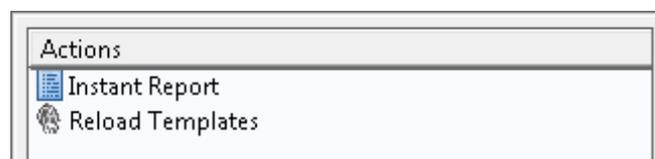


Figure 105

The action will display **Action Processed** while the templates are being loaded

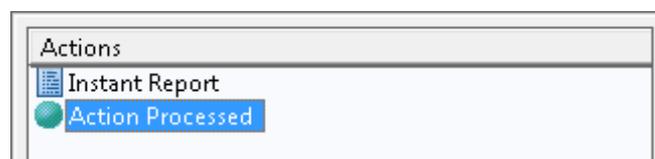
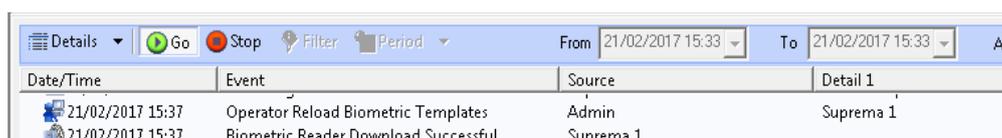


Figure 106

The action will also be displayed in the event window.



Date/Time	Event	Source	Detail 1
21/02/2017 15:37	Operator Reload Biometric Templates	Admin	Suprema 1
21/02/2017 15:37	Biometric Reader Download Successful	Suprema 1	

Figure 107

13. Commissioning Mode

When creating a new Biometric ACU in EXgarde, you can tick Commission Mode to delay communications to the reader during database configuration.

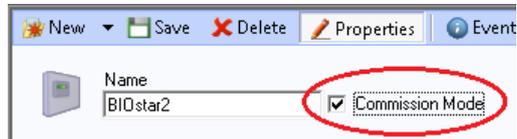


Figure 108

Once you have fully configured the ACU and its child objects you can turn off configuration mode and this will tell EXgarde Suprema W2 service to start communication to that ACU.

14. Troubleshooting

Connection Issues

- Check RJ45 is connected, and unit is powered.
- Check unit can be pinged.
- Check correct IP address has enter and matches unit settings.
- Check Suprema service has correct firewall rights

Distribution Error

- Check serial number entered matches unit.
- Check unit is displayed online in EXgarde.

Reader Shown Offline

- Check IP address and port are correct.
- Check the EXgarde Suprema service is running.
- Check conflicting services are not running I.E. BIOstar service
- Check connection I.E., can you ping unit?



TDSi UK, Unit 10, Concept Park, Innovation Close, Poole, Dorset, BH12 4QT, UK

WWW.TDSi.CO.UK

 +44(0)1202 723 535

 sales@tdsi.co.uk

 +44(0)1202 724 975