Suprema Biometric Reader Configuration and User Guide

9.9.0 v1

Symmetry™ Security Management

9600-0261

Suprema Biometric Reader Configuration and User Guide
9600-0261

Issue 9.9.0v1 (for Symmetry software version 9.9.0) – 30th September 2024

Contents

About this Guide

This guide explains how to integrate a Suprema biometric reader into the Symmetry™ Security Management System.

This guide is intended to be of use to:

- Personnel who are responsible for configuring, using or supporting Symmetry systems.
- Sales and management personnel.

This document is supported by context-sensitive online help available from the Symmetry software.

It is assumed that you understand the basic concepts of security management and the Symmetry software. If you do not have this knowledge, please read the *Symmetry User's Guide* first.

Chapter 1: Introduction

Overview of the Integration

Symmetry integrates with the following Suprema™ biometric readers:

- BioLite N2 biometric fingerprint readers
- FaceStation F2 biometric fingerprint/face readers

The readers can be used as enrollment readers and access-control readers.

For enrollment, the reader allows fingerprint or face images to be captured and smart cards to be encoded from the Symmetry "Home/Identity/Card Holders" and "Home/Identity/Visitors" screens. Symmetry communicates with enrollment readers over the network.

When used for access control, the reader connects directly to a Symmetry M2150 or M4000 node using standard Wiegand connections. Optionally, a Symmetry monitor point can be set up for each reader to monitor for duress conditions at the reader.

When encoding a card, Symmetry can encode the card number, PIN and fingerprint(s) or face image (not both). When the card is presented to a Suprema access-control reader, the reader compares the presented fingerprint(s) or face image and PIN with the data stored on the card, signals the result and passes the card data to the Symmetry controller. Symmetry then decides whether to grant or deny access, based on the result from the reader and the card holder's access rights set up in Symmetry.

Since key information is stored on the card and checked by the reader, the card must be re-encoded if the card holder's card number, fingerprint, face image or PIN is changed in Symmetry.

About the BioStar 2 Configuration Application

It may be necessary to configure each reader using the Suprema BioStar 2 application, which is available from the Suprema web site. This configuration is necessary before you can use the reader for enrollment or access control. Configuration takes place over the network.

Note: If the reader firmware has been supplied by AMAG, configuration may not be required. Please check with your local support representative.

BioStar 2 configures settings such as the card format, fingerprint template format, smart-card layout and reader mode. Once configuration is complete, the application does not need to be running for encoding or access control.

System Requirements

- Symmetry v9.4.9 or later (earlier versions support only the BioLite N2).
- One standard Symmetry reader license for each biometric access-control reader.
- Suprema BioLite N2 or FaceStation F2 biometric readers (for access control or enrollment). **Note:** Only one Symmetry client can connect to the same reader for enrollment. FaceStation F2 readers require firmware version 2 (file name "fstf2-all_v22.0.1_20221215_171612c_hidnewhw.bin") or later.
- If M4000 nodes are being used, M4000 firmware version 1.8 or later is required.
- Private Authentication configuration files may be needed from Suprema to change the Private Authentication mode (see below).
- For FaceStation F2 biometric readers, a separate power supply is required for each reader. FaceStation F2 readers must not be powered directly from the M2150 or M4000 node.
- Suprema BioStar 2, available from the Suprema web site (see page 8).
- Supported smart-card layout: MIFARE and MIFARE DESFire. (**Note:** A sentinel is not needed for DESFire.) Required card memory:
  - 1kB minimum when encoding one fingerprint.
  - 2kB minimum when encoding two fingerprints.
  - 4kB minimum when encoding face images (for FaceStation F2).
- Supported fingerprint template format: ISO 19794-4, ANSI378 and Suprema.
- Supported card formats (all supported for encoding and access control):

  Symmetry 32-bit CSN format

  Symmetry 62-bit smartMAX Wiegand format

  Symmetry 63-bit Wiegand format

About Private Authentication Mode

The Private Authentication mode determines how readers authenticate an access-control transaction. One of the following authentication modes can be selected:

- **Private Authentication Disabled** (default) – If a reader is set to Private Authentication Disabled, it takes the authentication mode configured in the reader using BioStar 2 (see page 18). With this authentication mode, all cards must be encoded with what is required for authentication, otherwise the reader will deny access. For example, if a reader is configured to require a face, card and PIN, all cards must be encoded with this information.
- **Private Authentication Enabled** – If a reader is set to Private Authentication Enabled, it takes the authentication mode from what has been encoded on the card in Symmetry (see page 35) and ignores what is set in the reader using BioStar 2. This authentication mode allows for a hybrid environment where different card holders can have different levels of authentication. One card may need the face, card and PIN, whereas another may require only the card for access.

To change the mode, an appropriate Private Authentication configuration file will need to be obtained from Suprema and installed (page 37).

The "Card Only" and "Card & PIN" commands/modes in Symmetry have no effect.

Chapter 2: Connecting Suprema Readers

Connecting a BioLite N2 Reader

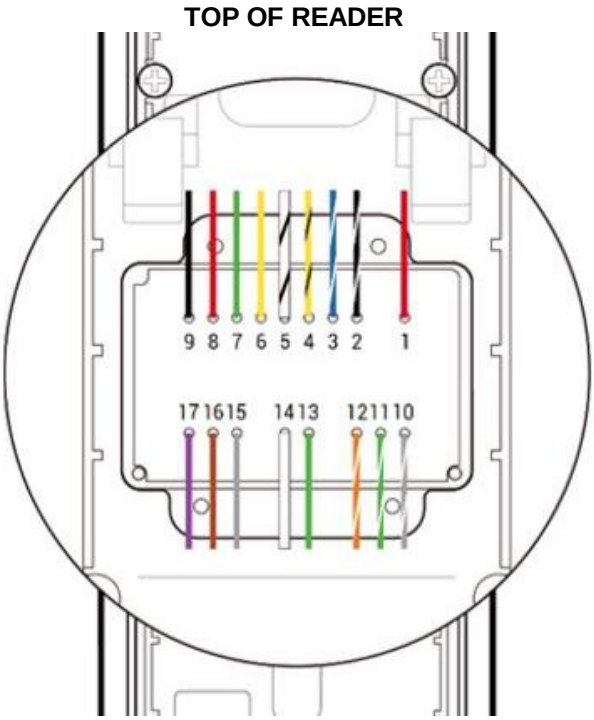


Figure 1 BioLite N2 Reader Rear Wiring

BioLite N2 – Connections for Enrollment or BioStar 2

When using the reader as an enrollment reader, or when using BioStar 2:

1. Connect the Ethernet port (attached via a cable to the back of the reader) to:
   - The same network as BioStar 2 while you are using BioStar 2.
   - The same network as Symmetry when the reader is added to Symmetry, and during Symmetry card enrollment and encoding.
2. Connect the following pins on the back of the reader (see Figure 1) to a 12Vdc power supply:

Pin	Wire Color	Power Supply
1	Red	12Vdc
2	Black with white stripe	0V

Note: Please refer to the reader's installation instructions for details of the power supply required.

BioLite N2 – Connections for Access Control

When the reader is used as an access-control reader, connect the following pins on the back of the reader to the reader terminal on the Symmetry controller. The reader port on the Symmetry controller must be set to "Wiegand", as described in the *M2150 Installation Instructions*.

BioLite N2		Symmetry Controller	
Pin	**Wire Color**	**M2150**	**M4000**
1	Red	12Vdc	12Vdc
2	Black with white stripe	0V	0V
11	Green with white stripe	Monitor point (optional for duress alarm)	
12	Orange with white stripe		
13	Green	Reader: 0	Reader: Rx+
14	White	Reader: 1	Reader: Rx-
16	Brown	Reader: RED	Reader: Tx+
17	Purple	Reader: GRN	Reader: Tx-

Connecting a FaceStation F2 Reader

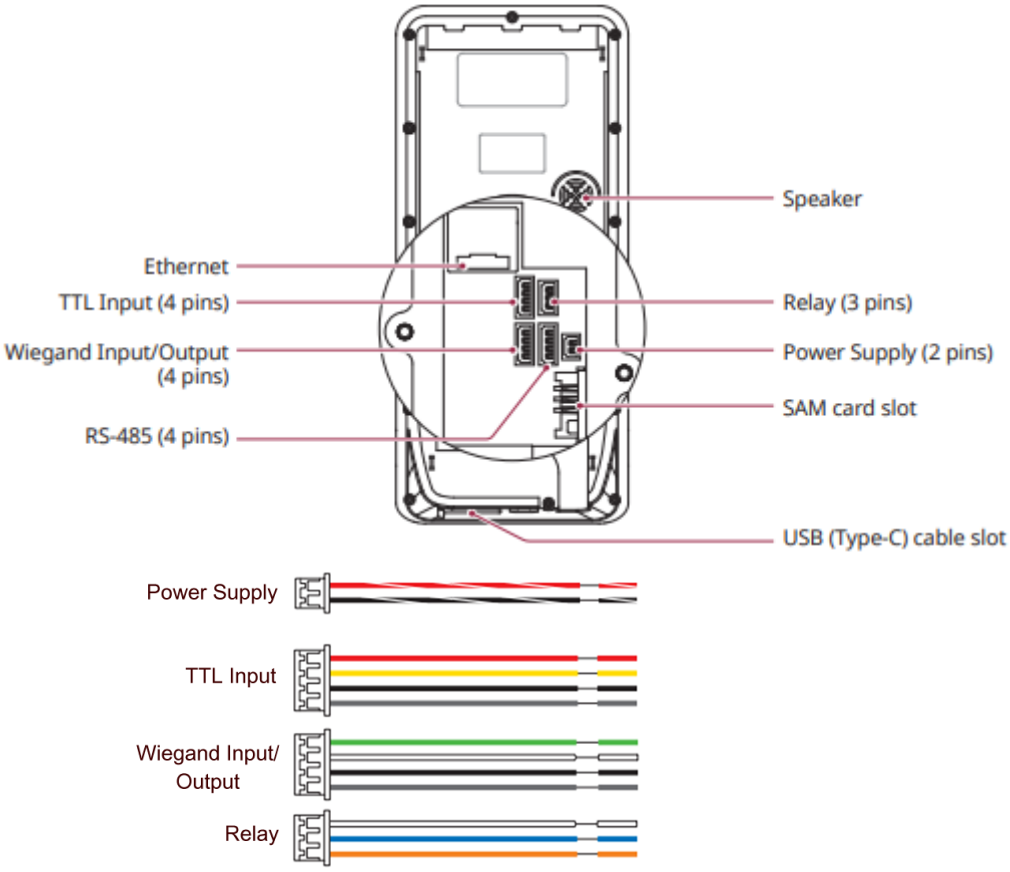


Figure 2 FaceStation F2 Reader (Rear) and Cables

FaceStation F2 – Connections for Enrollment or BioStar 2

When using the reader as an enrollment reader, or when using BioStar 2:

1. Connect the Ethernet port to:
   - The same network as BioStar 2 while you are using BioStar 2.
   - The same network as Symmetry when the reader is added to Symmetry, and during Symmetry card enrollment and encoding.
2. Connect the power terminals on the back of the reader to a power supply:

Pin	Wire Color	Power Supply
1	Red with white stripe	12Vdc (minimum 1.5A) or 24Vdc (minimum 0.8A)
2	Black with white stripe	0V

FaceStation F2 – Connections for Access Control

When the reader is used as an access-control reader, connect the following pins on the back of the reader to the reader terminal on the Symmetry controller. The reader port on the Symmetry controller must be set to "Wiegand", as described in the *M2150 Installation Instructions* or M4000 Commissioning Guide.

FaceStation F2				Symmetry Controller	
Connector	**Pin**	**Name**	**Color**	**M2150**	**M4000**
Power Supply	1	PWR +VDC	Red with white stripe	Do not connect. A separate 12Vdc (minimum 1.5A) or 24Vdc (minimum 0.8A) power supply is required (12Vdc/24Vdc to "PWR +VDC", and 0V to "PWR GND")	
	2	PWR GND	Black with white stripe		
TTL Input	1	TTL IN0	Red	Reader: GRN	Reader: Tx-
	2	TTL IN1	Yellow	Reader: RED	Reader: Tx+
Wiegand Input/Output	1	WG D0	Green	Reader: 0	Reader: Rx+
	2	WG D1	White	Reader: 1	Reader: Rx-
	3	WG GND	Black	Reader: 0V	Reader: 0V
	4	SH GND	Gray	Reader: 0V	Reader: 0V
Relay	1	RLY NO	White	Monitor point (optional for duress alarm)	
	2	RLY COM	Blue		

Chapter 3: Configuring BioStar 2 and the Suprema Readers

Resetting a Reader

If a reader has been used previously, you can reset it to factory defaults as follows.

For a BioLite N2:

1. Press **ESC**.
2. Press **2** several times until **DEVICE** is selected, then press **6**.
3. Press **2** several times until **Restore Default** is selected, then press **6**.
4. Press **2** several times until **Factory Default** is selected (or **Reset All Settings** if **Factory Default** is not available), then press **6**.
5. Press **OK** to confirm.

For a FaceStation F2:

1. On the FaceStation F2 main screen, press and authenticate with the Admin level credential.
2. Select **Device, Restore Default**.
3. Select **Factory Default**.

For further information, please refer to the *FaceStation F2 User Guide*.

Step 1 – Install the BioStar 2 Software

Install BioStar 2 as follows:

1. Download the latest application from the Suprema web site.
2. Double-click the installer exe, and follow the prompts to install the application.
3. Start the application. You may need to use the **Advanced** option to start without a secure connection.

Note: In steps 2 to 5 described next, you will define common settings in BioStar 2, such as the fingerprint template format, card layout and smart-card layout to use for the Suprema readers. During these steps,

there is no need to be connected to any readers. Once you have completed steps 2 to 5, you will need to connect and configure each individual reader using the common settings already defined.

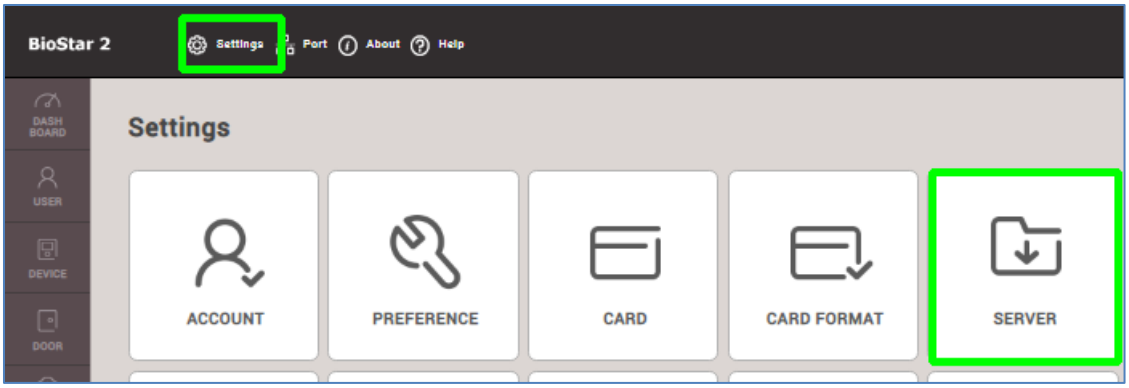
Note: By default, the M4000 multiNODE API uses the same port that BioStar 2 uses for communications to the reader (port 443). Therefore, either use different machines for BioStar 2 and the multiNODE API, or when installing the multiNODE API, specify a different port number, as described in the *M4000 Commissioning Guide*.

Step 2 – Specify the Fingerprint Template Format to use

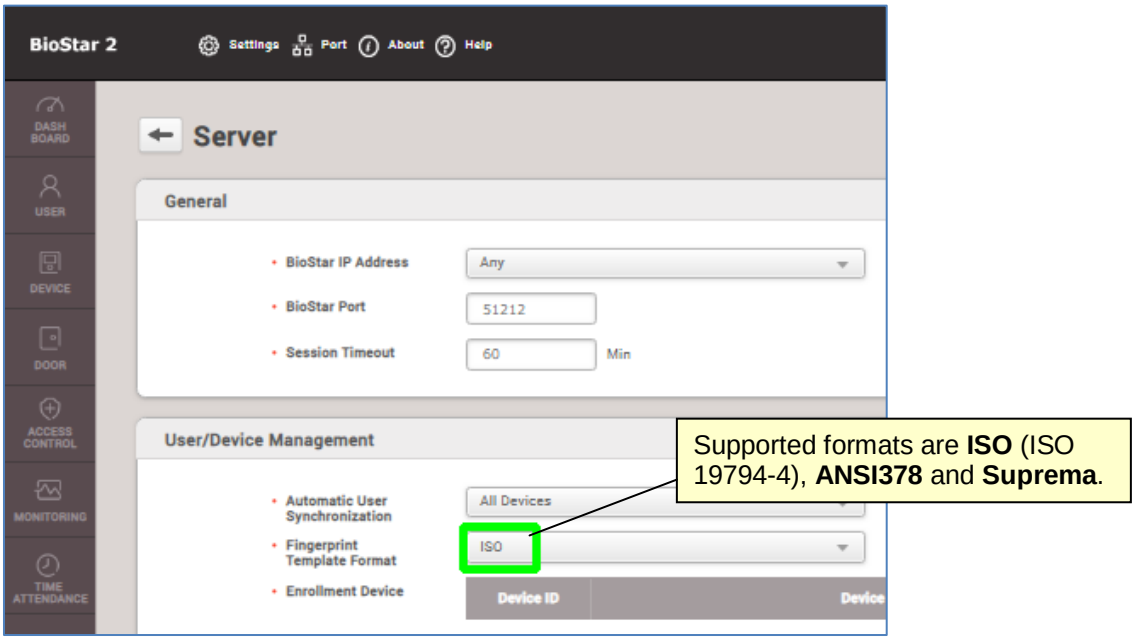
Note: This step is relevant only if fingerprints are to be used for access and the readers have a fingerprint reader.

In the BioStar 2 application:

1. Click **Settings** in the top bar, followed by the **SERVER** icon:



2. Select the required fingerprint template format from the menu:



Note: If Symmetry is going to be used to encode cards, you will need to select the same format in the "Maintenance/User & Preferences/System Preferences" screen in Symmetry.

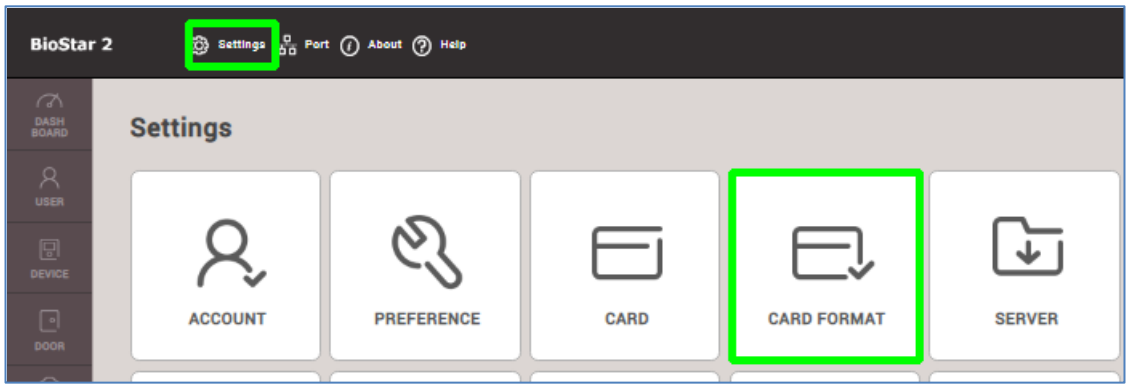
3. Click **Apply** to save changes, and click **Yes** when prompted to continue.

Step 3 – Create the Card Format

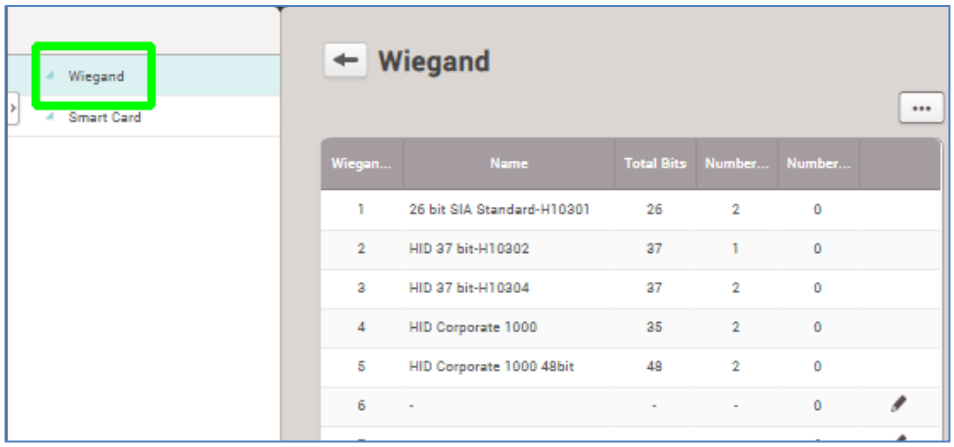
This step allows you to create a Symmetry 32-bit, 62-bit or 63-bit card format.

To create a card format:

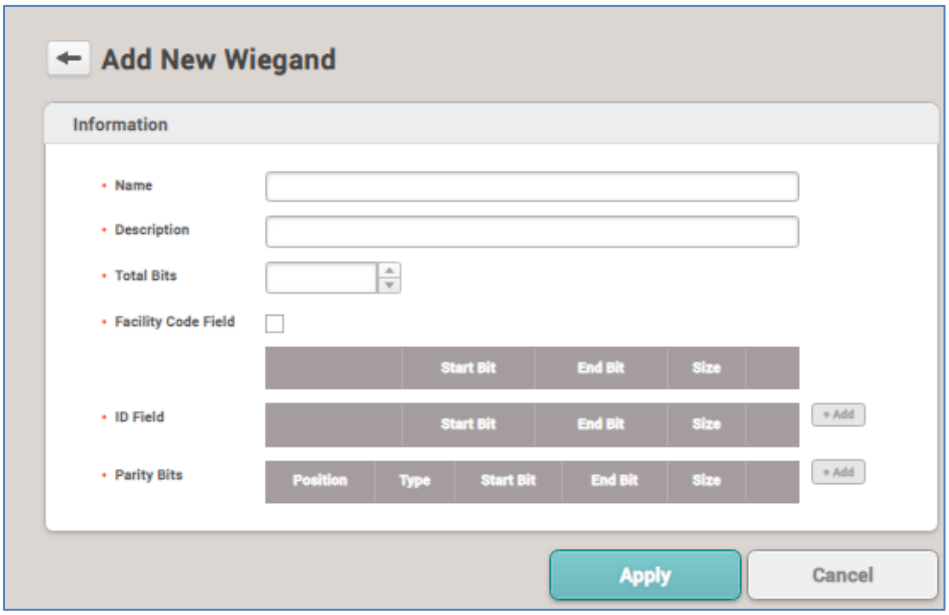
1. Click **Settings** in the top bar, followed by the **CARD FORMAT** icon:



2. Select **Wiegand** on the left side of the page:



3. Create a new card format by clicking the button at the end of the first unused row. The following page is displayed:

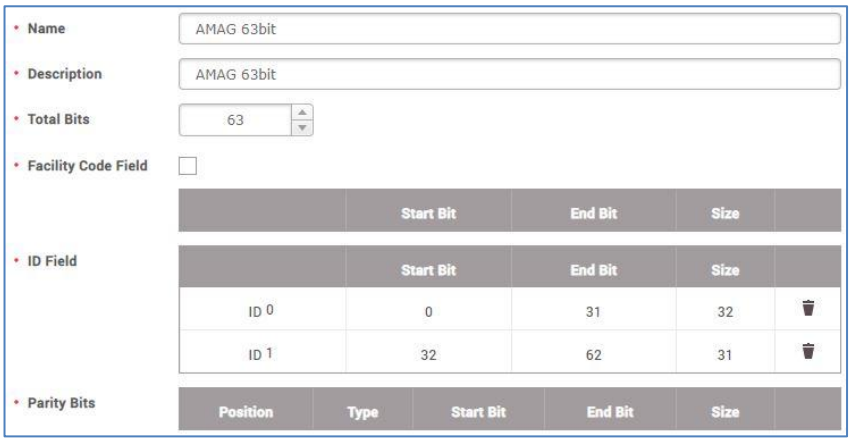


4. Specify the following:

- **Name** – A meaningful name for the card format (e.g. "AMAG 62-bit").
- **Description** – A meaningful description (e.g. "62-bit Card Format").
- **Total Bits** – The number of bits the format uses. Symmetry encoding supports 32, 62 and 63 bits.
- **Facility Code Field** – Leave unchecked.
- **ID Field** – Click **Add** to specify the **ID 0** start and end bits (e.g. 0 and 31). If you are defining a 62-bit or 63-bit format, click **Add** again to specify the **ID 1** start and end bits (e.g. 32 and 61 for a 62-bit format).
- **Parity Bits** – Leave undefined.

Example of 32-bit configuration:

Example of 63-bit configuration:



5. Click **Apply** to save changes.

Step 4 – Create a Smart Card Layout

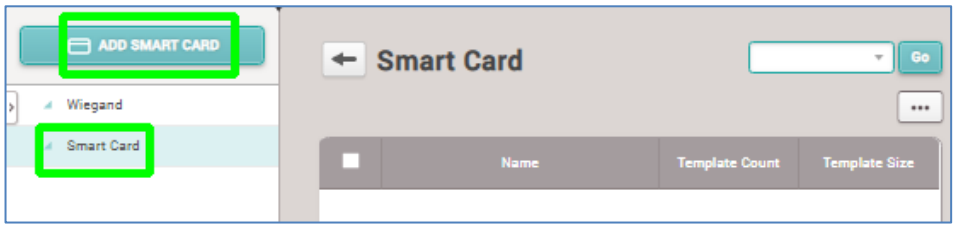
Configure a smart card layout (for MIFARE and/or MIFARE DESFire) as follows.

Note: Each reader uses only one smart card layout. You can configure the layout to support MIFARE format only, MIFARE DesFire format only, or both. If you specify both formats, the reader will accept cards that use either format.

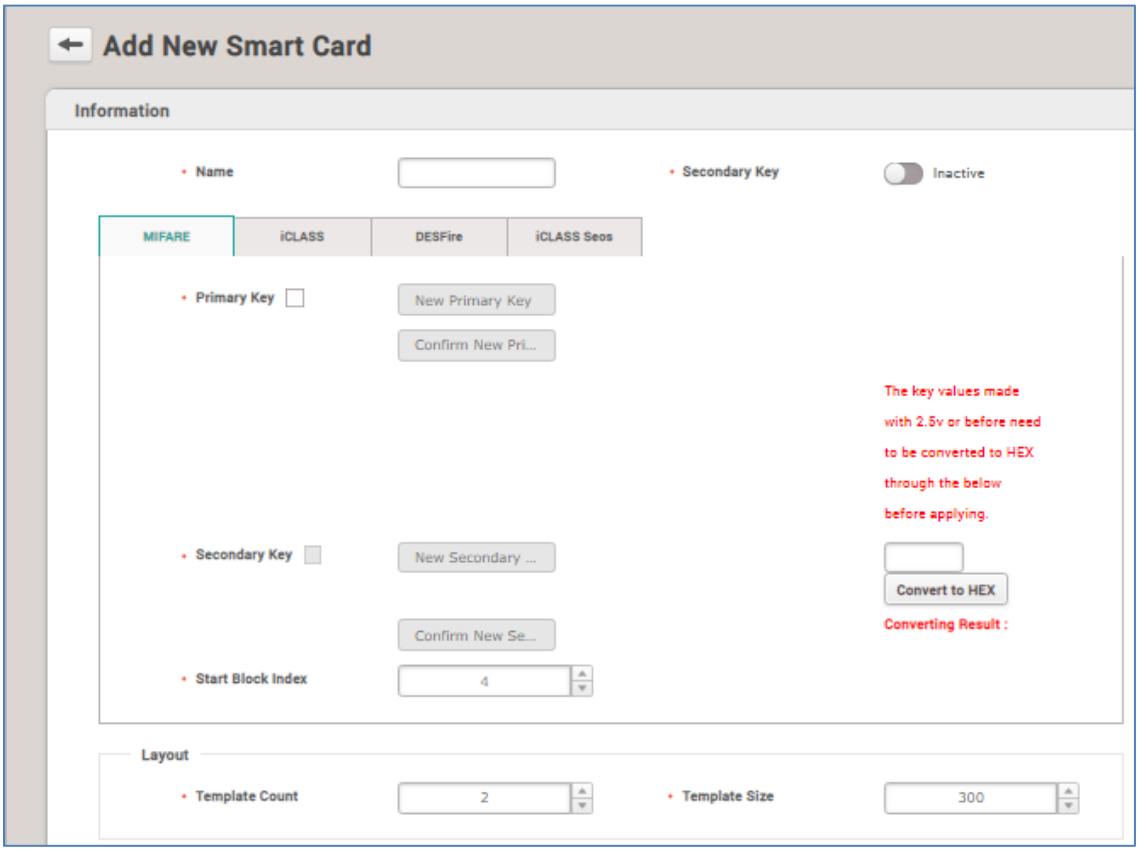
1. Click **Settings** in the top bar, followed by the **CARD FORMAT** icon.

2. Select **Smart Card** on the left side of the page.

3. Click **ADD SMART CARD**:



The following page is displayed.

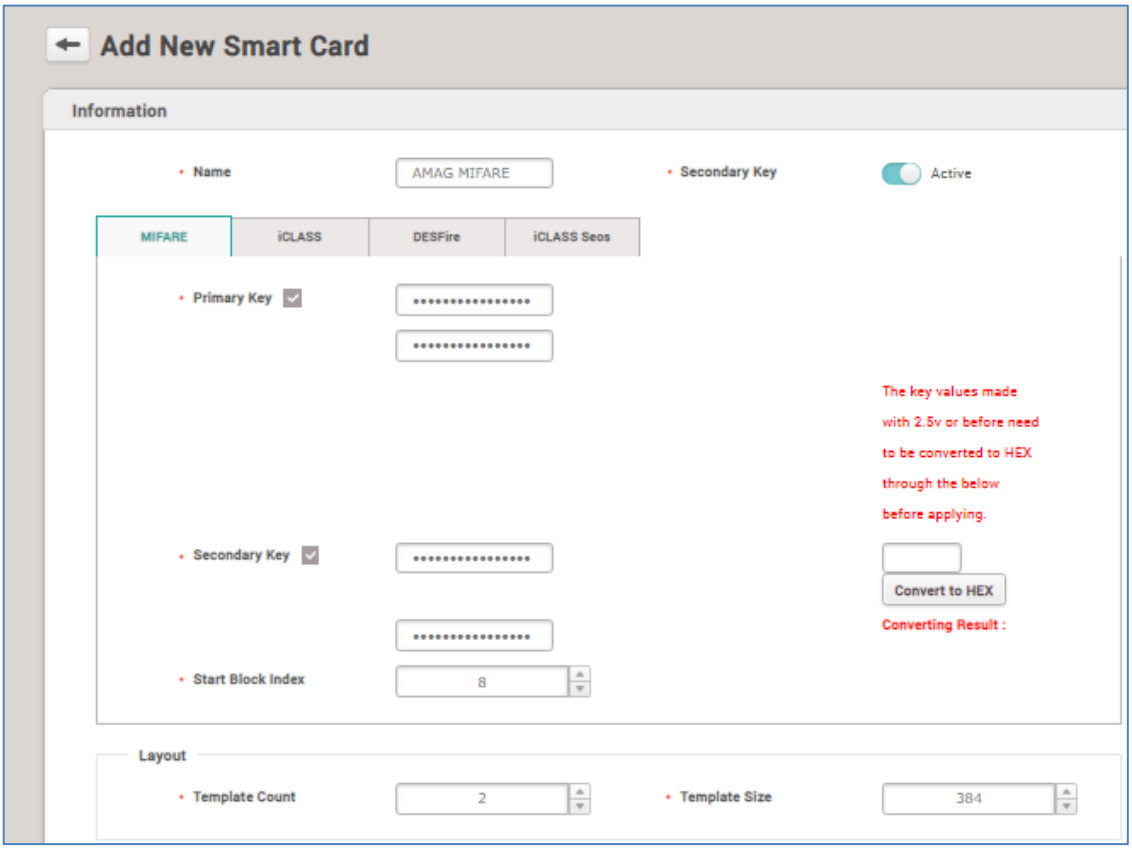


4. In the **Name** field, specify a meaningful name for the smart card layout (e.g. "AMAG DESFire").

5. Set **Secondary Key** to **Active**.

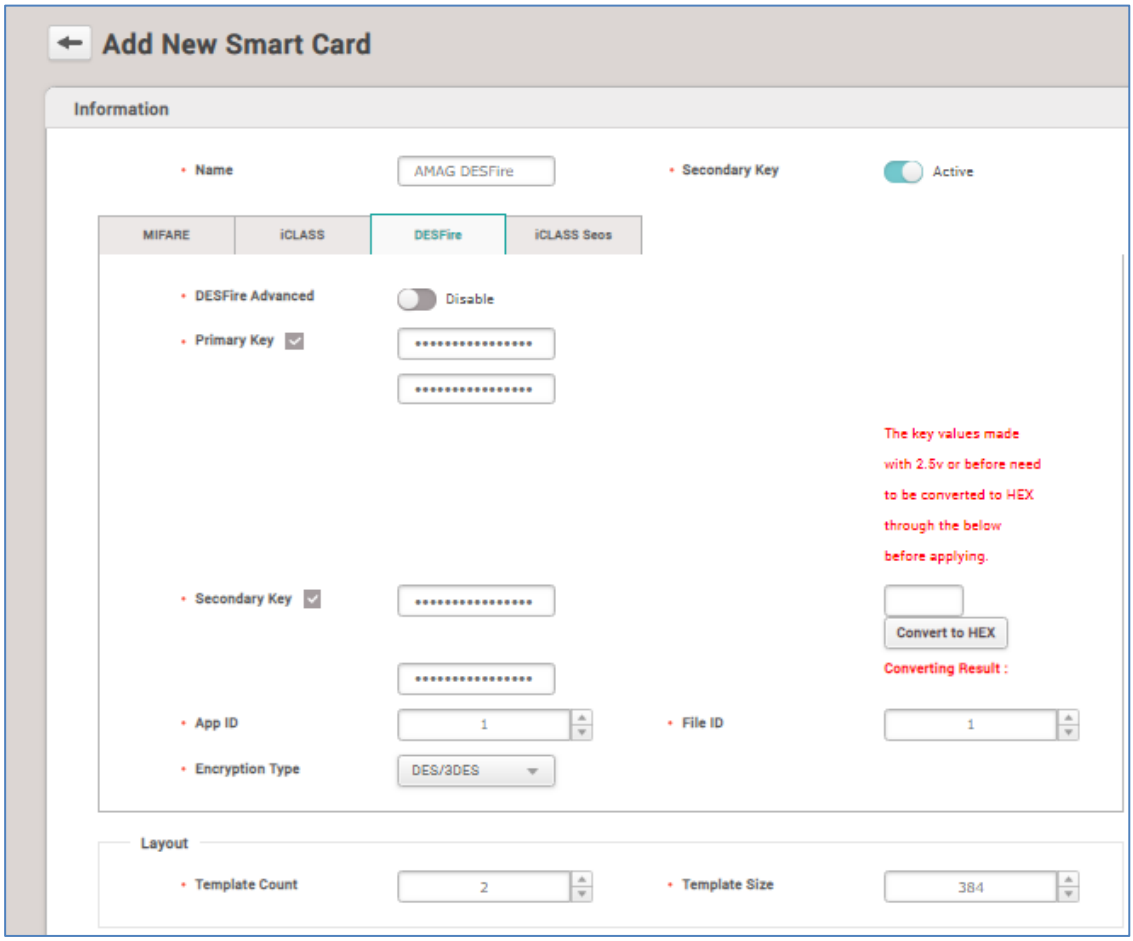
6. Configure one or both of the following tabs:
   - **MIFARE** – For MIFARE format.
   - **DESFire** – For MIFARE DESFire format.

   For **MIFARE** (non-DESFire), use the following settings:
   - **Primary Key** – Select **Primary Key** and specify the primary key to use for encoding. This can be a customer-specific value of 12 characters. **Note:** If you have already encoded cards, and change the keys, those existing cards will not be recognized at access-control readers.
   - **Secondary Key** – Set to a customer-specific value of 12 characters.
   - **Start Block Index** – Set to 8.
   - **Template Count** – Set to 2.
   - **Template Size** – Set to 384.



For MIFARE DESFire, use the following settings:

- **DESFire Advanced** (if available) – Set to **Disable**.
- **Primary Key** – Select **Primary Key** and specify the primary key to use for encoding. This can be a customer-specific value of 32 characters. **Note:** If you have already encoded cards, and change the keys, those existing cards will not be recognized at access-control readers.
- **Secondary Key** – Set to a customer-specific value of 32 characters.
- **App ID** – Set to 1.
- **File ID** – Set to 1.
- **Encryption Type** – Select **DES/3DES**.
- **Template Count** – Set to 2.
- **Template Size** – Set to 384.



7. Click **Apply**.

Step 5 – Enable Encoding Encryption

This step, which is mandatory, configures encryption between the Suprema biometric enrollment reader and any Symmetry PCs that are used for encoding. Encryption protects user data, such as fingerprints and PINs.

Step 5a – Create your own Certificates (Optional)

Note: For maximum security, it is recommended that each site has its own certificates. However, you can skip this section and continue to Step 5b if you want to use the default certificates provided with Symmetry.

To create your own certificates:

1. Download and install the **Windows OpenSSL** application. Make a note of the installation folder (default is C:\Program Files (x86)\GnuWin32\bin).

2. Copy **CreateSupremaCertificate.bat** (located in the "Setup\Packages\Suprema Certificates\Certificate Creation" folder on the Symmetry installation media) to a local folder on your computer.

3. If OpenSSL is not installed in the default folder, open CreateSupremaCertificate.bat using a text editor, and change the path to OpenSSL.

4. Open a Command Prompt on your computer and run CreateSupremaCertificate.bat.

5. Follow the prompts.

6. Check that the batch file has created three files named **ssl_server_root.crt**, **ssl_server.crt** and **ssl_server.pem** in the same folder as the batch file.

   Note: You will need to copy ssl_server_root.crt, ssl_server.crt and ssl_server.pem to the "Security Management System\Certificates" folder on any Symmetry client that is going to be used to encode cards for Suprema readers. The files must replace any existing files with the same name.

Step 5b – Add the Certificates to BioStar 2

Now that you have created the certificates, or have decided to use the default certificates provided with Symmetry, you need to add them in BioStar 2 as follows:

1. If you are using the default certificates provided with Symmetry, locate the files named **server_root.crt**, **server.crt** and **server.pem** in the "Setup\Packages\Suprema Certificates\Certificates" folder on the Symmetry installation media.

2. Click **Settings** in the top bar, followed by the **SERVER** icon.

3. Configure the **Advanced Security Settings** section:
   - **Secure communications with device** – Enable (set to **Use**), and confirm the warning message.
   - **Use external certificates** – Enable (set to **Use**).
   - **Root certificate** – click **Upload** and open **ssl_server_root.crt** (created in Step 5a) or **server_root.crt** (the default Symmetry certificate).
   - **Public key certificate** – click **Upload** and open **ssl_server.crt** (created in step 5a) or **server.crt** (the default Symmetry certificate).
   - **Private key** – click **Upload** and open **ssl_server.pem** (created in step 5a) or **server.pem** (the default Symmetry private key).

4. Click **Apply**.

Step 6 – Add and Configure the Suprema Readers

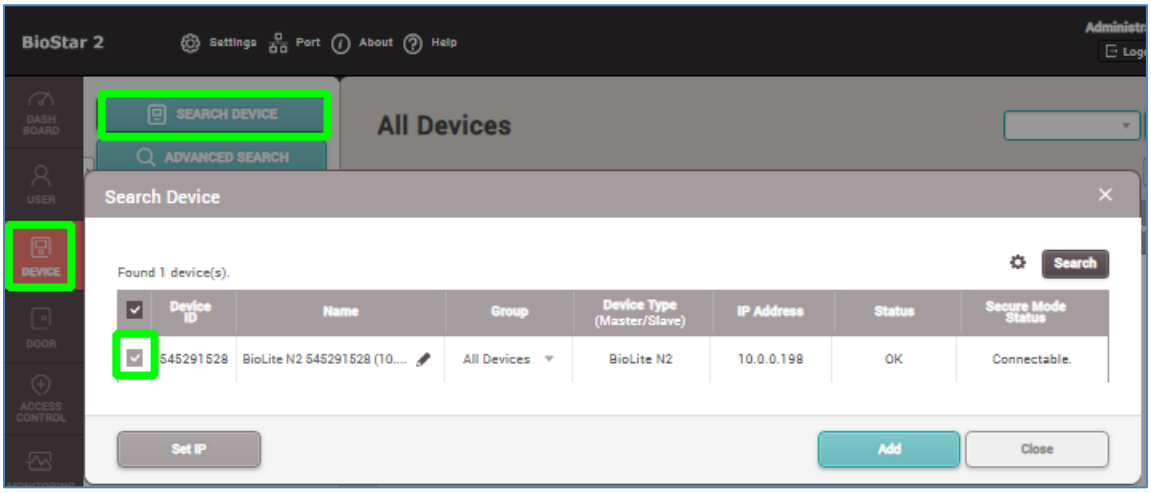
Configure each Suprema access-control and enrollment reader as follows:

1. Connect the reader to the network and power supply (refer to Chapter 2 for connection details), then switch on the power supply. Wait until the device has started.

2. Click **DEVICE** on the left side of the page.

3. Click **SEARCH DEVICE**. All readers on the network are listed.

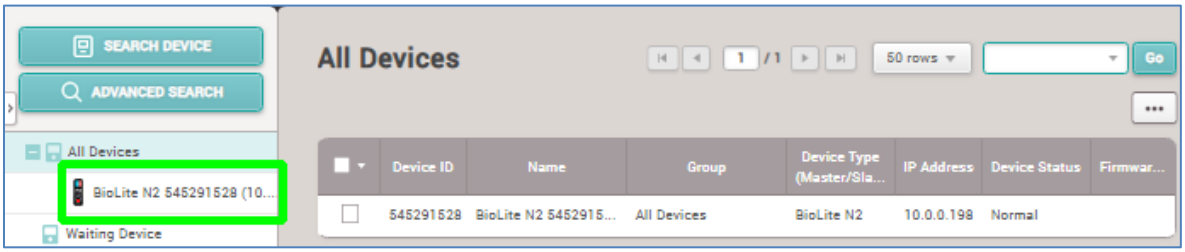
4. Select the checkbox of the device you want to configure:



Note: Check that the status is "Connectable". If it is not, you may need to factory reset the reader (see page 8).

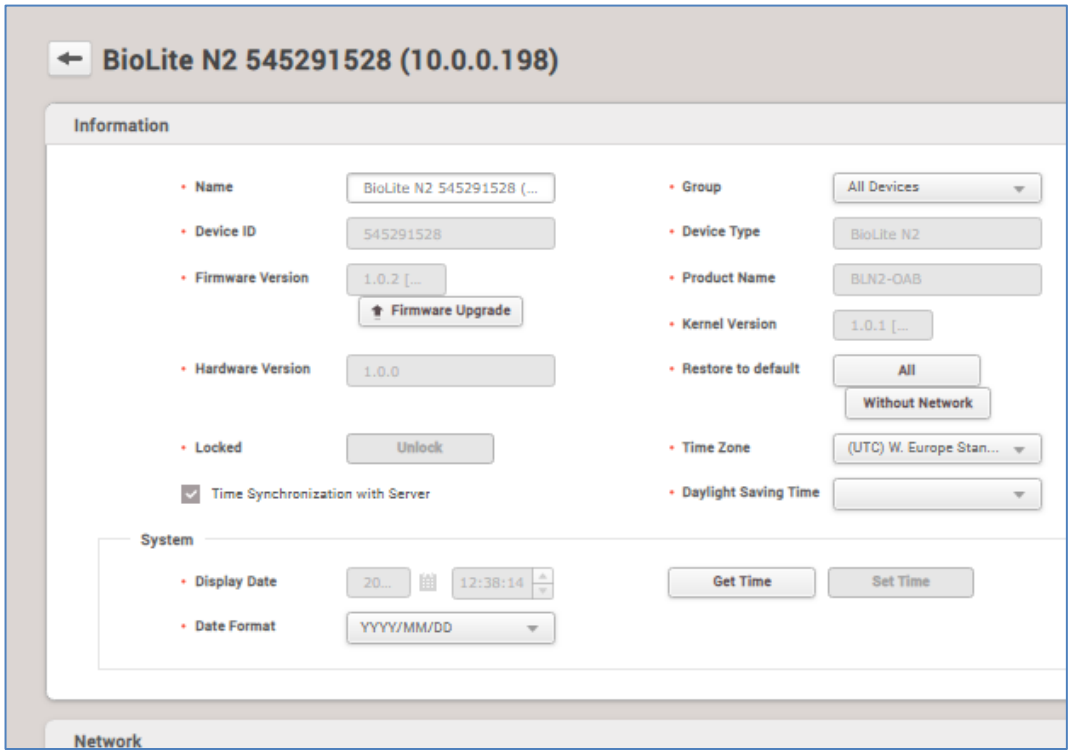
5. Click **Add**, and confirm when prompted. You should see the device listed under **All Devices** on the left side of the page.

6. Under **All Devices**, select the reader you want to configure:



If you are prompted to erase existing data, click **Yes** and try again.

The reader configuration settings are displayed, as shown next.



7. Check the **Firmware Version** field to determine whether the firmware is up to date and whether Private Authentication Mode (page 2) is enabled or disabled (disabled is the default). You may need to make the window bigger to see the whole field. If you need to update the firmware or change the authentication mode, please refer to Appendix A on page 37.

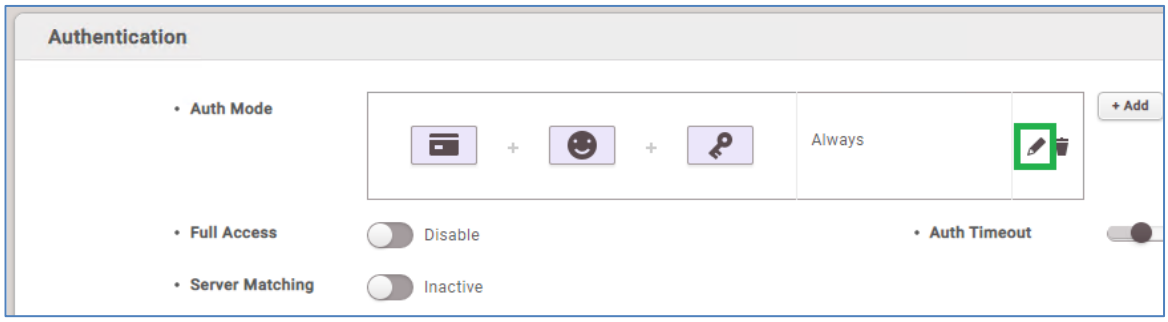
8. Scroll down to the **Authentication-CSN Card Format** section, and configure as follows:

   - **Format Type** – Enable (set to **Wiegand**, and confirm when prompted).
   - **Wiegand Format** – Select the card format from the menu, such as the card format you created previously (page 10).
   - **Byte Order** – Leave as the default (**MSB**).

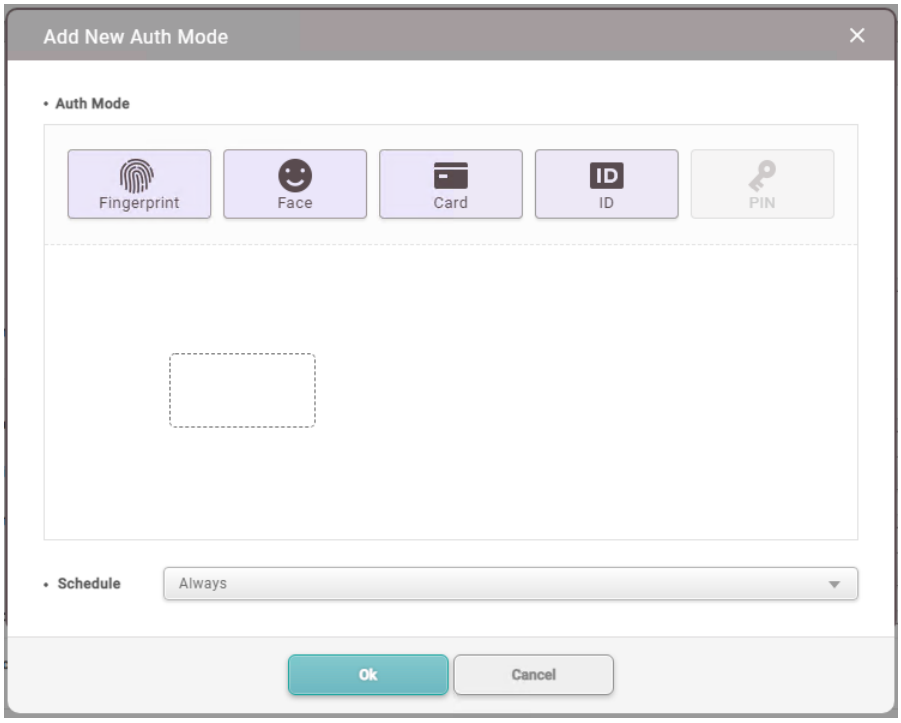
   DO NOT change **Wiegand Format** under the **Wiegand Card Format** section.

9. In the **Smart Card Layout** section, use the **Layout** menu to select the smart card layout you created previously (page 12).

10. If Private Authentication mode (see page 2) is disabled, scroll down to the **Authentication** section. **Auth Mode** shows the method the reader uses to authenticate access when Private Authentication mode is disabled:



If you need to change the authentication method, click the pen icon, drag and drop the credentials that you require for authentication:



The **Schedule** menu (shown above) specifies the times of the day that the authentication method will apply. Click **OK** to save changes.

Note:

- If you select **PIN**, the reader will authenticate using the PIN encoded on the card. If you change the PIN in Symmetry, you should re-encode the card to make sure that the PIN in Symmetry and on the card are the same to avoid any confusion.
- Do not select both **Fingerprint** and **Face**, as Symmetry allows only one of these to be enrolled and encoded on the card.

If you want to use different authentication methods for different times of the day, use the **Add** button in the **Authentication** section to add a new authentication method and select the required option from the **Schedule** menu.

11. If you are configuring an enrollment reader, **Device Port** in the **Network** section specifies the port number that Symmetry will use to communicate with the reader (default 51211).

12. Click **Apply**.

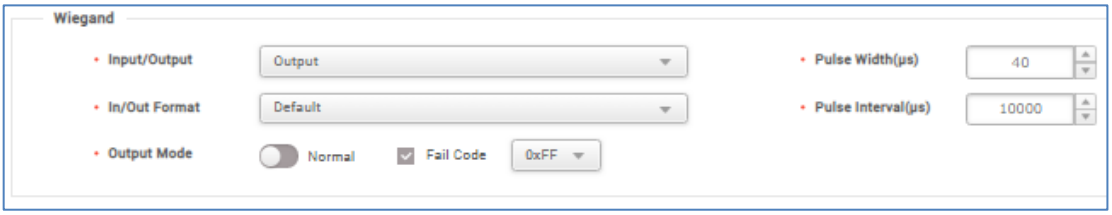
If you are configuring an enrollment reader, configuration is complete, and you can skip to Step 9.

Step 7 – Configure the Output Mode (for Access Control Readers Only)

Note: Skip this step if you are configuring an enrollment reader.

You need to set output mode for an access-control reader as follows:

1. Under **All Devices**, click the reader you want to configure.
2. Scroll down to the end of the page and click **Advanced**.
3. In the **Advanced-Wiegand** section:
   a) Set **Input/Output** to **Output**.
   b) Select **Fail Code**, and choose **0xFF** from the menu:



4. Leave the reader settings page open for the next step.

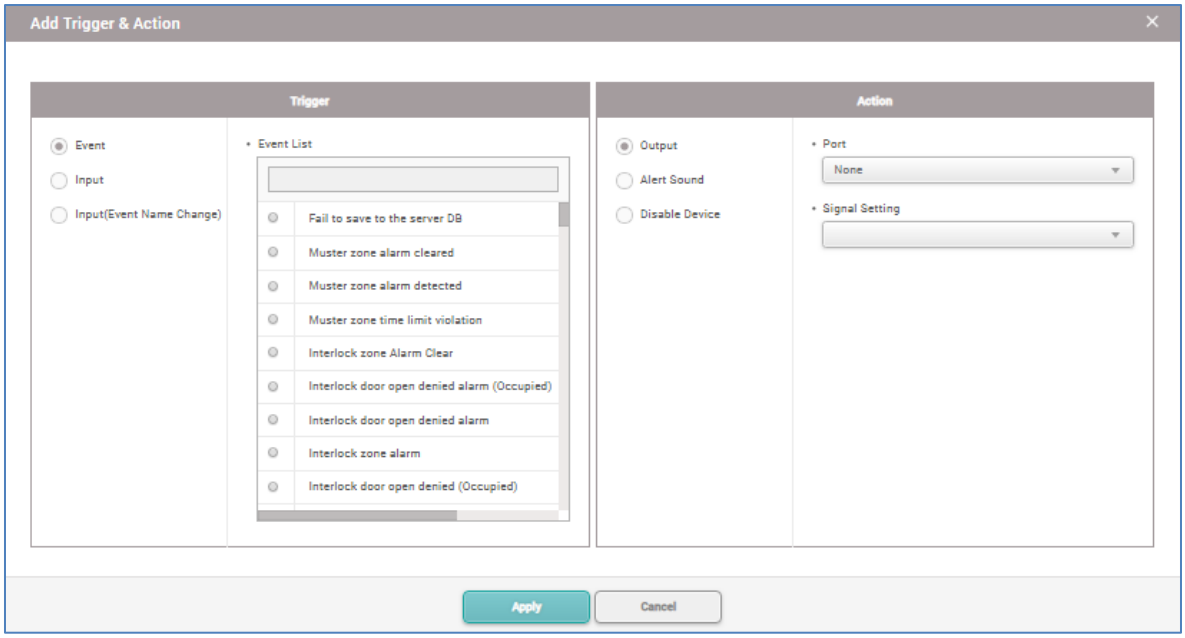
Step 8 – Set up Trigger and Action for Duress (Access Control Readers Only)

Note: Skip this step if you are configuring an enrollment reader.

Optionally, you may want to set up a trigger and action to enable a fingerprint reader to signal duress alarms to the Symmetry controller.

To set up a trigger and action for duress:

1. Scroll to the **Trigger & Action** section and click **Add**. The following page is displayed:



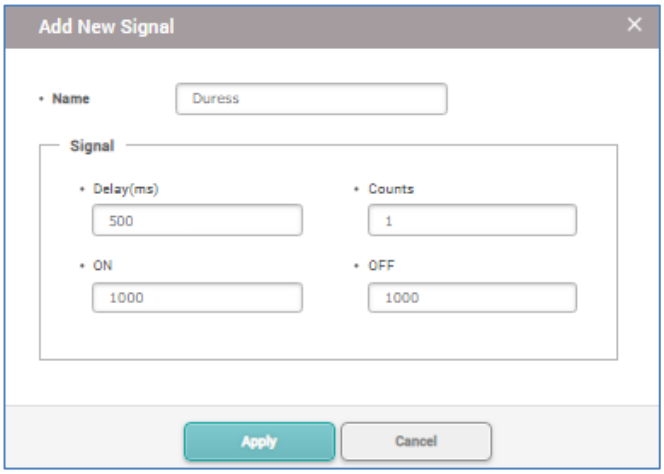
2. Use the following settings to configure a trigger for duress:

Trigger:

- Select the **Event** radio button.
- **Event List** – Select **1:1 duress authentication succeeded (Card + Fingerprint)**.

Action:

- Select the **Output** radio button.
- **Port** – Select **Relay 0**.
- **Signal Setting** – In the menu, click **Add Signal**. In **Name**, enter a meaningful name (e.g. "Duress"), and use the settings shown next.



Note: A duress transaction signals duress but still allows access (access rights permitting).

3. Click **Apply**.
4. From the **Signal Setting** menu, select the signal you have just created.
5. Click **Apply**.
6. Click **Apply** to save changes.

Step 9 – Configure Other Readers

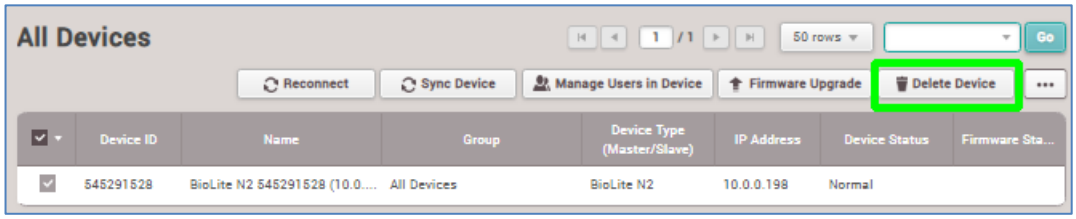
Repeat steps 6 to 8 for any other Suprema enrollment or access-control readers you are using.

Step 10 – Remove the Enrollment Readers from BioStar 2

Configuration of the Suprema readers is now complete. However, you should remove any enrollment readers defined in BioStar 2, since Symmetry cannot communicate with enrollment readers while BioStar 2 is communicating with them. If you do not delete the enrollment readers and BioStar 2 is started at a later date, it may interfere with the correct operation of Symmetry.

To remove an enrollment reader:

1. Click **DEVICE** on the left side of the page.
2. Select the checkbox of the device you want to delete.
3. Click **Delete Device**:



You can discover and add an enrollment reader back into BioStar 2 if you need to make any changes to the device configuration. You do not need to remove the enrollment reader from Symmetry before adding the reader back into BioStar 2, but you will not be able to use the reader in Symmetry while it is connected to BioStar 2.

Note: Make sure the Symmetry "Home/Identity/Card Holders" and "Home/Identity/Visitors" screens are closed before adding the reader back into BioStar 2.

Chapter 4: Configuring Symmetry

Step 1 – Install the Symmetry Software

Install Symmetry as described in the *Symmetry Software Installation Manual*.

Step 2 – Install the Certificates

Carry out the following if you are using encryption and created your own certificates (page 15):

1. Locate the created ssl_server_root.crt, ssl_server.crt and ssl_server.pem files.

2. Copy the files to the "Security Management System\Certificates" folder on any Symmetry client that is going to be used to encode cards for Suprema readers. The files must replace any existing files with the same name.

Default certificates are installed in the same folder as part of the installation of Symmetry.

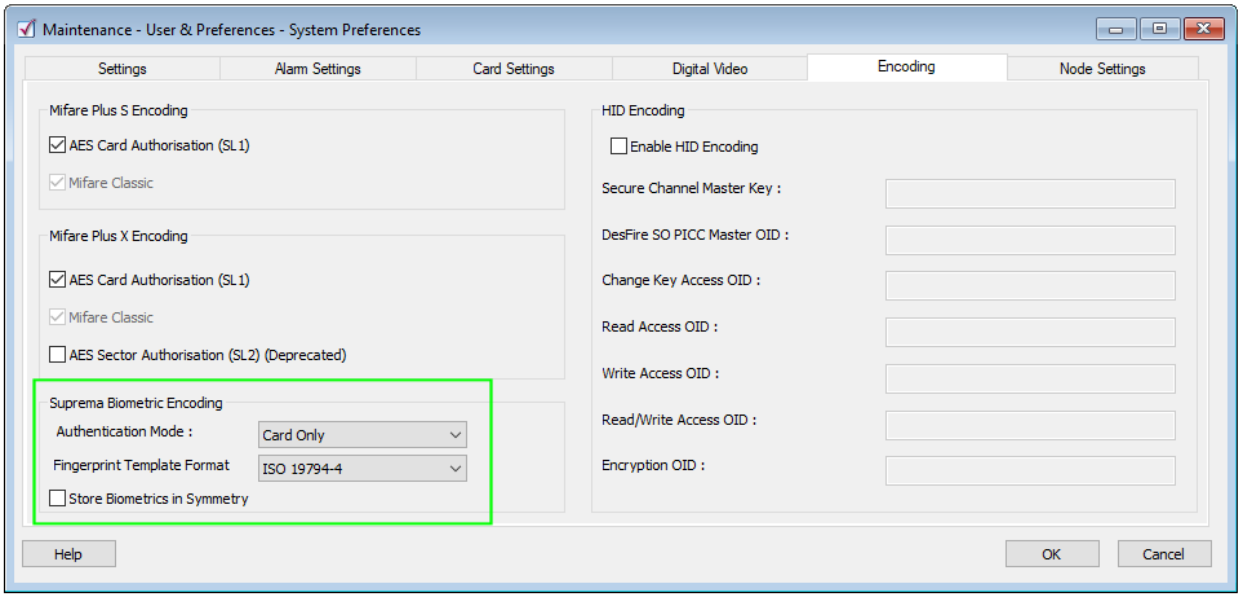
Step 3 – Add the Symmetry Encoding License

If you are going to encode cards from within Symmetry, open the "Maintenance/Licensing/System Licenses" screen in Symmetry, and add a license for the Card Encoding Module.

To obtain the new options in the user interface, log out of Symmetry, then log back in.

Step 4 – Configure the System Preferences

Open the "Maintenance/User & Preferences/System Preferences" screen in Symmetry, and configure the **Suprema Biometric Encoding** settings:

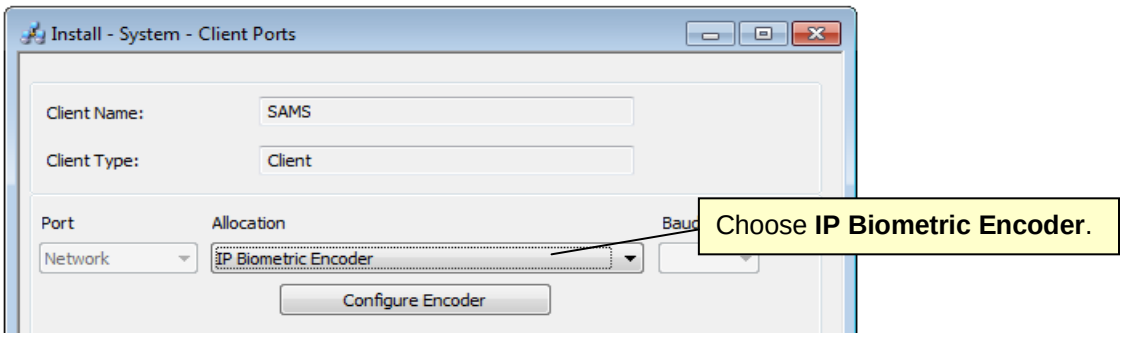


- **Authentication Mode** − This sets the default state of the same option in the Encode a Smart Card screen (page 35).
- **Fingerprint Template Format** − Select the fingerprint template that you configured the reader to use in BioStar 2, if fingerprints are used (see page 9).
- **Store Biometrics in Symmetry** − Select this option if you want to allow Symmetry to store fingerprints or face images if enrolled in the Symmetry Card Holders or Visitors screen (both a fingerprint and face image cannot be enrolled). If this option is not selected, card holders will need to re-enroll their fingerprints or face images if, for example, a new card needs to be encoded.

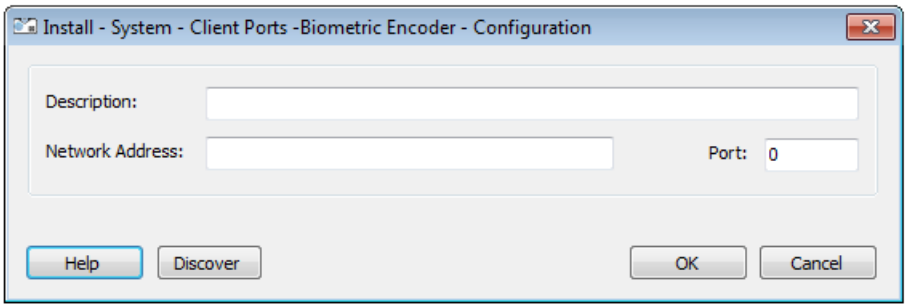
Step 5 – Add Each Enrollment Reader

Note: Make sure that the reader is connected to the network and powered up. See Chapter 2 for connection details.

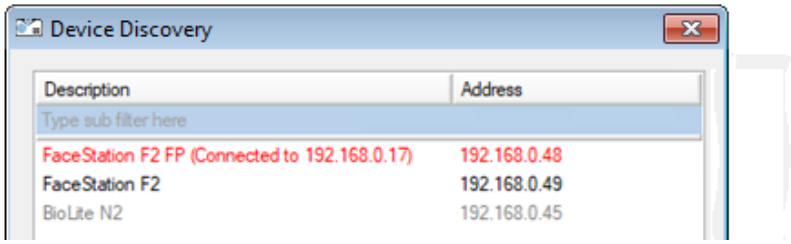
1. Open the "Install/System/Client Ports" screen in Symmetry, and create a new network port:



2. Click **Configure Encoder**. The following dialog is displayed:

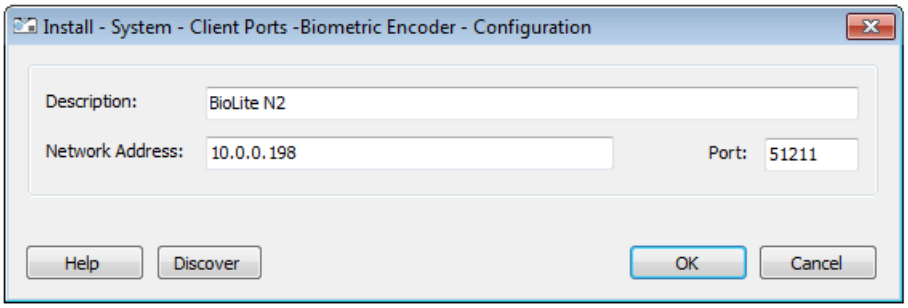


3. Click **Discover**. The Suprema enrollment readers are listed:



Encoders listed in black text are available to add to Symmetry. Encoders listed in red text are connected to another device, such as BioStar 2. Encoders listed in gray are already discovered and assigned to a client port in Symmetry.

4. Double-click the enrollment reader you want to add. The reader details are displayed in the Configuration dialog:



The **Port** number is the port on the encoder Symmetry will use to communicate with the encoder. On discovery, it reflects the port set up in BioStar 2 (page 19). Do not change it to be different from the port number configured in BioStar 2 (51211 is the default).

5. Click **OK** twice to save the client port definition.

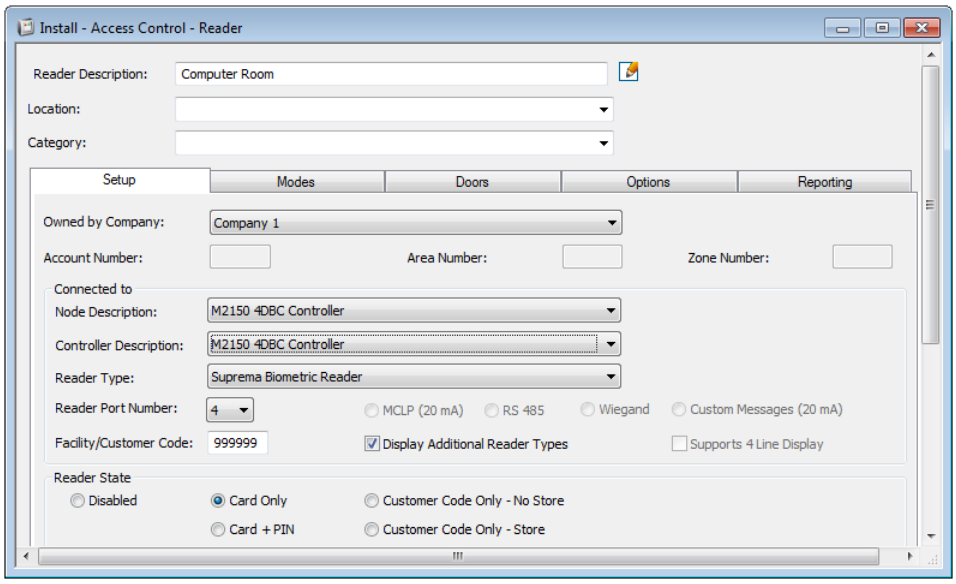
Step 6 – Add the Access-Control Readers

Note: See Chapter 2 for details of how to connect the reader to a Symmetry node.

Adding Readers when Using M2150 Nodes

To add the Suprema access-control readers to Symmetry when M2150 nodes are used:

1. Open the "Install/Access Control/Reader" screen in Symmetry, and create a new reader definition.
2. Complete standard details, such as selection of the node and reader port.
3. Select the **Display Additional Reader Types** checkbox.
4. From the **Reader Type** menu, select the appropriate reader/card format. For standard Symmetry 32-bit, 63-bit or 64-bit format, select **Suprema Biometric Reader**:



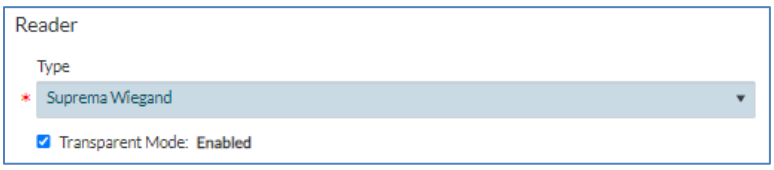
Note: The **Duress** setting in the Modes tab is not relevant for Suprema readers.

5. Click **OK**.

Adding Readers when Using M4000 Nodes

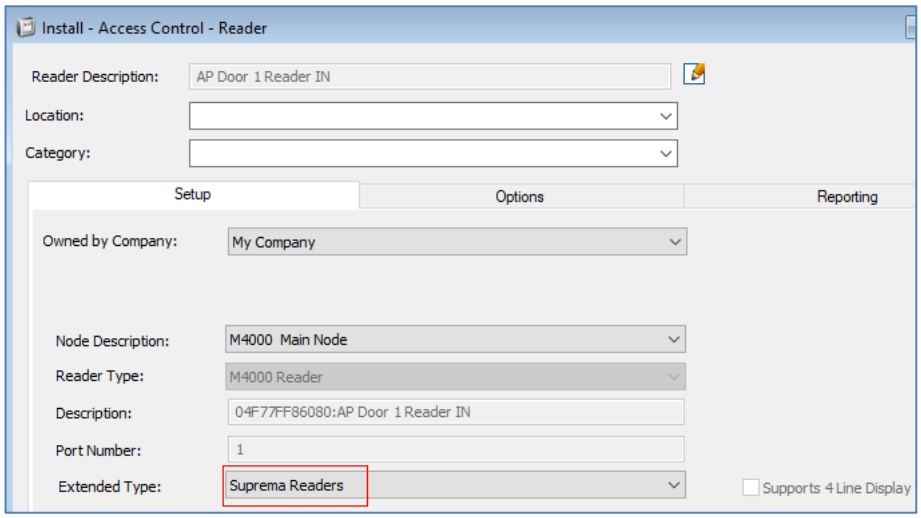
To add the Suprema access-control readers to Symmetry when M4000 nodes are used:

1. Using the web interface, configure the M4000 as described in the *M4000 Commissioning Guide*.
2. In the **Install, Access, Reader** screen of the web interface, configure the reader by setting **Type** to **Suprema Wiegand**, and by selecting **Transparent Mode**:



3. If you have not already done so, discover and add the M4000 node in Symmetry (as described in the *M4000 Commissioning Guide*).

4. Open the reader in the Symmetry "Install/Access Control/Reader" screen, and in the **Extended Type** menu, select **Suprema Readers**:



Selecting **Suprema Readers** for **Extended Type** allows Symmetry to report extended events such as "Fingerprint Mismatch" (see Appendix B on page 39). Extended events are available only when using M4000 nodes. Note that if you do not select this option, Symmetry will report all Suprema BioLite N2 and FaceStation F2 reader extended events as "Unknown Card".

Step 7 – Add a Monitor Point to Detect Duress

Each reader you configured in BioStar 2 to signal duress (see page 21) must have a monitor point defined in Symmetry to monitor for the duress event.

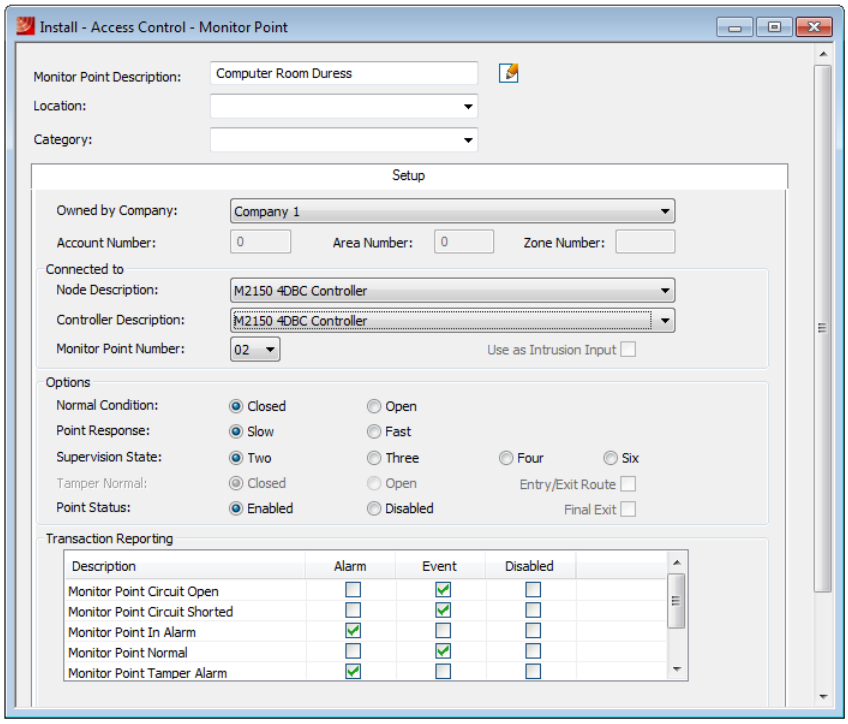
Note: Please refer to Chapter 2 for details of how to connect a reader to the monitor-point inputs of a node.

To define the Symmetry monitor point:

1. Open the "Install/Access Control/Monitor Point" screen in Symmetry, and create a new monitor point definition.

2. Complete standard details, such as selection of the node and monitor point number. For **Monitor Point Description**, use a name that easily identifies the monitor point with the reader, as this name will be displayed in any alarm or activity screens.

3. Make sure that **Normal Condition** is set to **Closed**, as shown next.



4. Click **OK**.

Adding a Trigger Command (Optional)

You can configure a trigger command in Symmetry to signal a duress event by. The trigger command could, for example, operate a sounder or light.

To define a Symmetry trigger command:

1. Open the "Operation/Commands/Trigger" screen in Symmetry, and create a new trigger command.

2. In the **If** part of the trigger command, select the monitor point that monitors for the duress condition at the reader.

3. Set the **Then** part of the trigger command to operate the output device (such as a sounder or light).

Chapter 5: Using Symmetry

Defining Card Holders/Visitors

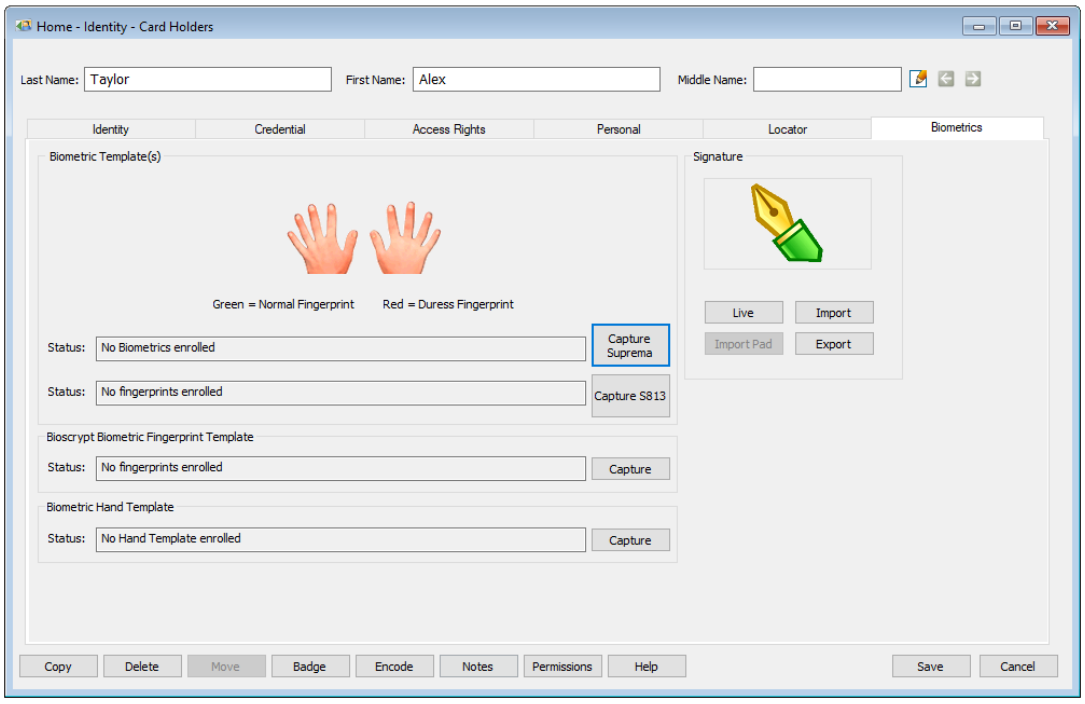
In Symmetry, for each card holder and visitor who needs to use a Suprema biometric access-control reader:

1. Open the "Home/Identity/Card Holders" or "Home/Identity/Visitors" screen, and create a new card holder/visitor or open an existing record.

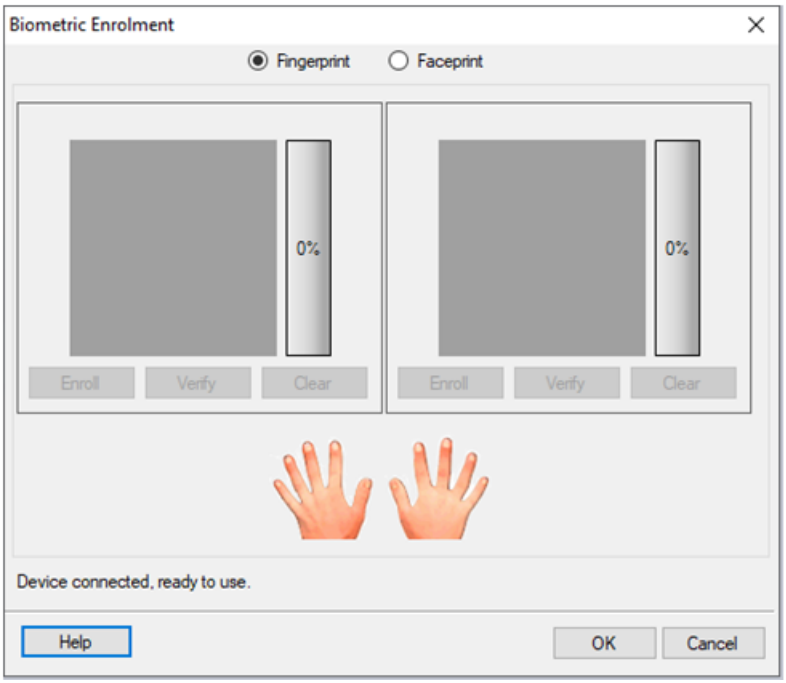
2. Define all standard details for the card holder, including the name, card number, PIN (if required), access rights, etc.

3. In the Credential tab, select **AMAG - 32**, **AMAG - 62** or **AMAG - 63** from the **Credential Format** menu, depending on the format used by the Suprema readers, as configured in BioStar 2 using the **Wiegand Format** setting (see page 18). **Note:** This selection is required irrespective of the Symmetry node type being used.

4. Display the Biometrics tab:



5. Click **Capture Suprema**. The following is displayed.



6. Enroll fingerprints or a face image, as described in the next sections.

   Note: You can enroll only fingerprint(s) or a face image, not both. If you have already enrolled fingerprint(s), these will need to be cleared before you can enroll a face image, and vice versa.

Enrolling Fingerprint(s)

To enroll fingerprint(s):

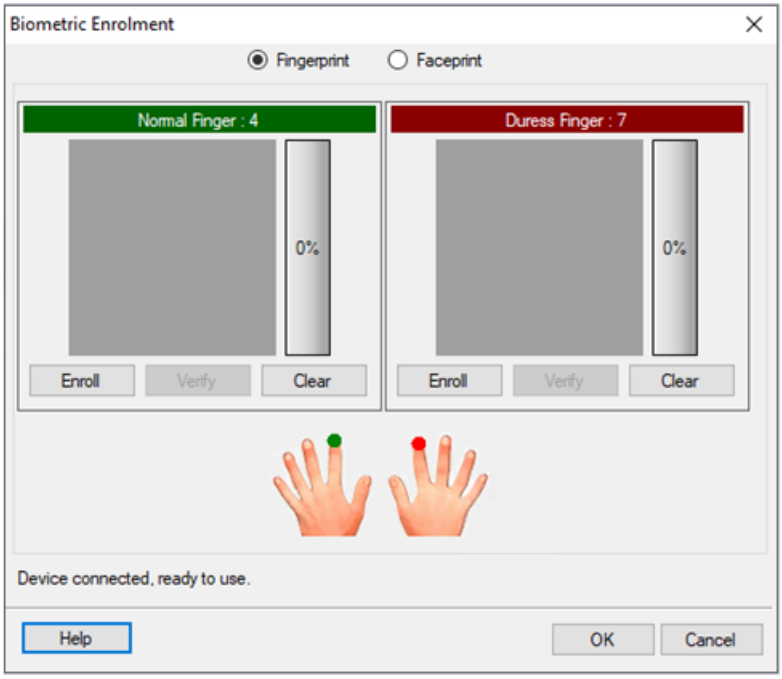
1. Select **Fingerprint** in the Biometric Enrolment dialog. (This radio button is grayed out if you are using a FaceStation F2 enrollment reader that does not support fingerprint capture.)

2. In the picture of the hands:

   - Left-click any fingertip to specify the finger is to be used to gain access. The fingertip is highlighted in green.
   - Right-click any fingertip to specify the finger is to be used to signal duress. The fingertip is highlighted in red.

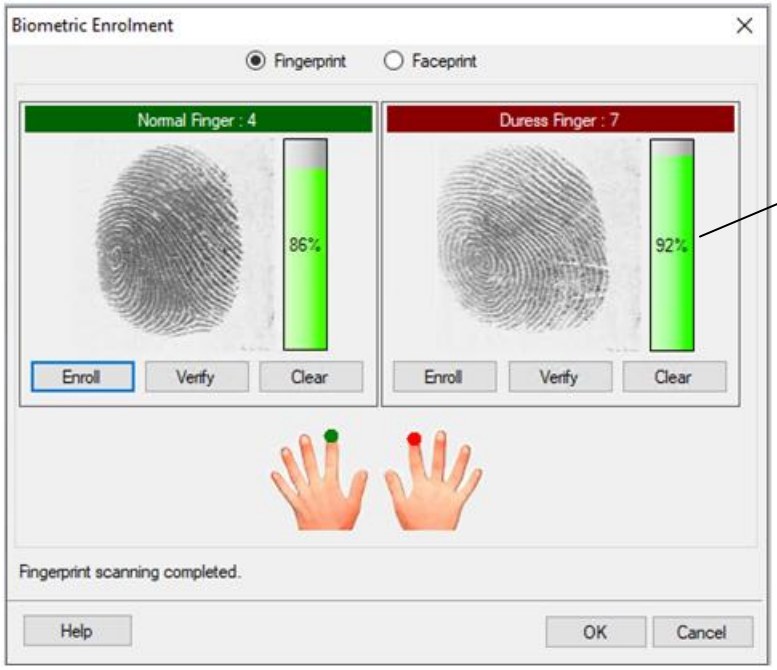
   You can enroll up to two fingerprints, either both for access, or one for access and another for duress.

   The headers near the top of the window show the selected finger numbers and their selected purpose. The following shows an example.



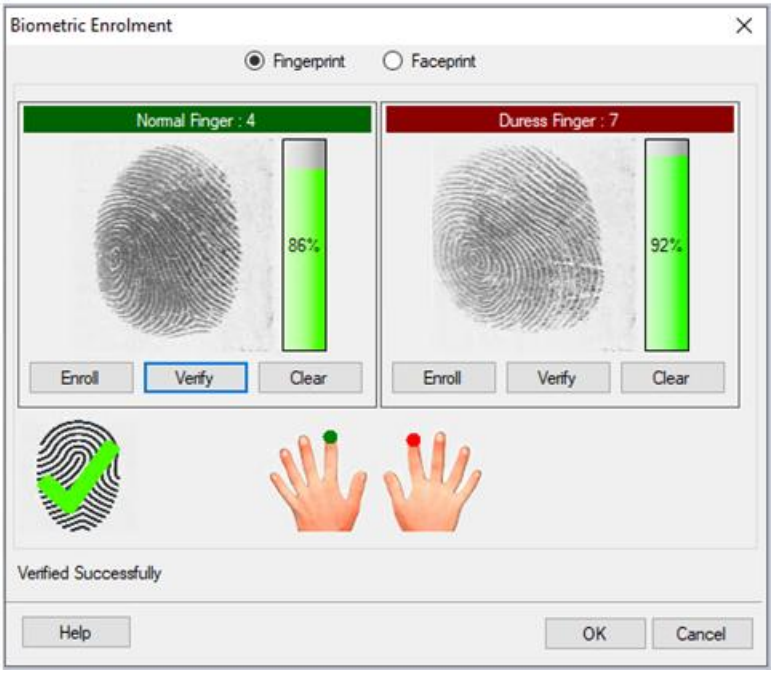
3. For each finger, click **Enroll** and present the selected fingerprint to the enrollment reader.

   The fingerprint(s) are displayed, with a percentage score to the right. For example:



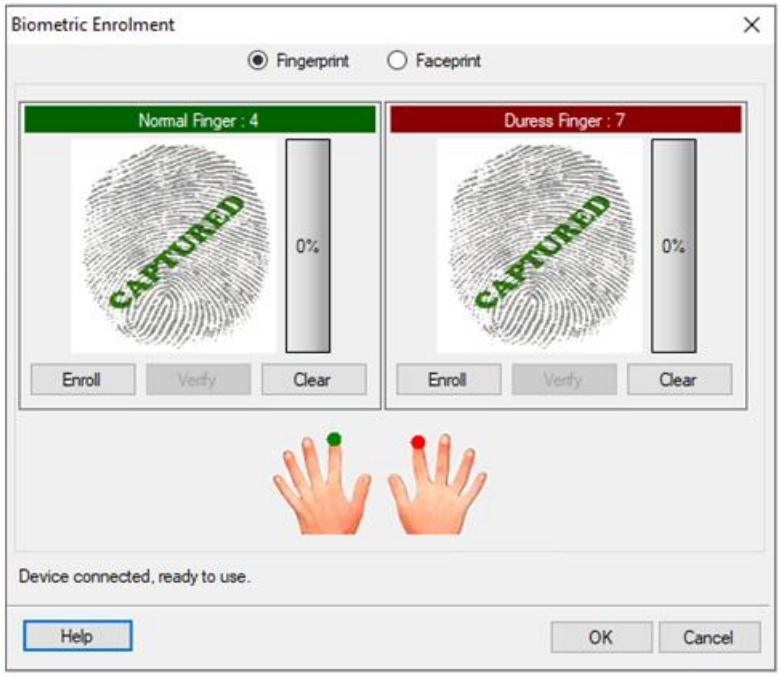
Aim for a score in excess of 80% for each finger to ensure reliable operation and good security.
If you do not reach a score of 80%, click **Enroll** and try again.

4. Click **Verify** to check that when you present the same finger again, the reader is able to confirm that it is the same finger as the one enrolled. This gives confidence that the finger has been positioned normally on the sensor during enrollment.



5. Click **OK**.

6. If you click **Capture Suprema** again, you should see that the fingerprint(s) have been captured successfully:

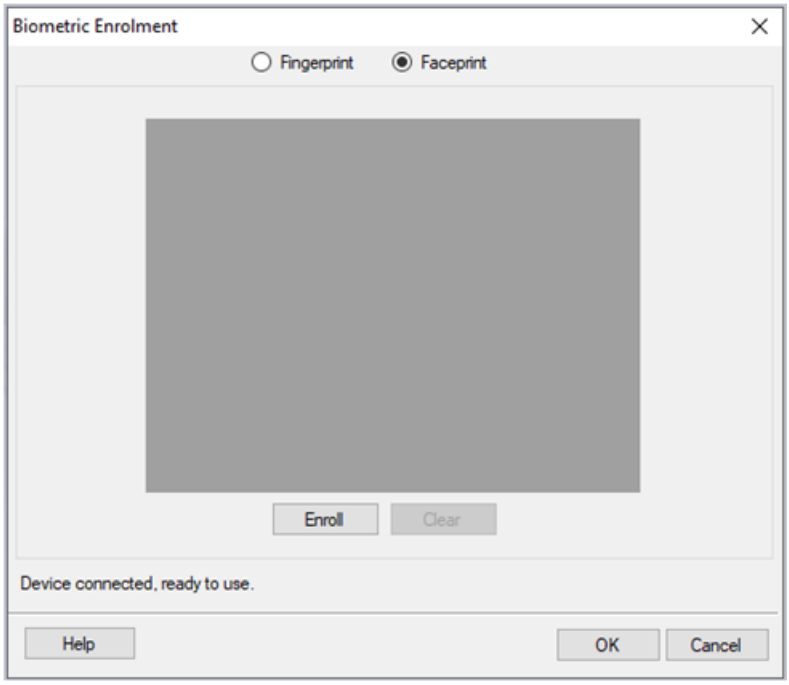


7. Click **Save** to save the card holder or visitor details, or proceed to encode a card (page 35).

Enrolling a Face Image

To enroll a face image:

1. Select **Faceprint** in the Biometric Enrolment dialog. The following is displayed:

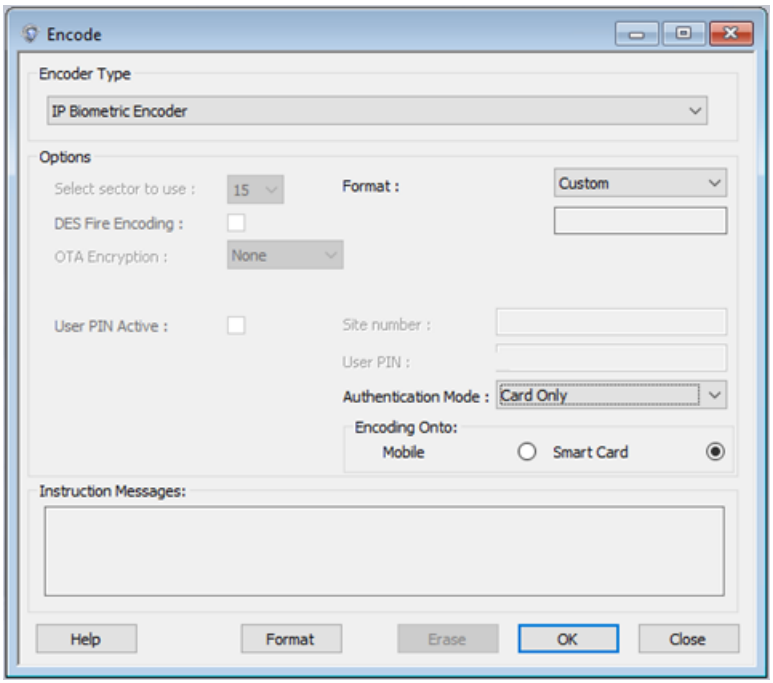


2. Click the **Enroll** button and present the face to the reader when prompted.
3. The face image is displayed in the window when the reader has captured a suitable image.
4. If the image is not as you require, click **Enroll** and try again.
5. Click **OK** to save the image.

Encoding Cards

To encode a card for a card holder or visitor:

1. In the "Home/Identity/Card Holders" or "Home/Identity/Visitors" screen, click the **Encode** button (located at the bottom of the screen). The following is displayed:



2. Choose one of the following for **Authentication Mode**:
   - **Card Only** – The card number will be encoded on the card. This option is available only if the card holder has the **Executive Card, PIN Exempt** option set.
   - **Card + PIN** – The card number and card holder's PIN will be encoded on the card
   - **Card + Biometrics** – The card number and any enrolled fingerprint(s) or face image will be encoded on the card.
   - **Card + Biometric or PIN** – The card number, any enrolled fingerprint(s) or face image and the PIN will be encoded on the card. If Private Authentication Enabled is used (page 2), the card holder will be able to use fingerprint(s)/face biometric data **OR** a PIN.
   - **Card + Biometric and PIN** – The card number, any enrolled fingerprint(s) or face image and the PIN will be encoded on the card. If Private Authentication Enabled is used (page 2), the card holder will need to use fingerprint(s)/face biometric data **AND** a PIN. Choose this option if Private Authentication Disabled is used and access-control readers are configured in BioStar2 to require all three items of data.
3. For **Encoding Onto**, select **Smart Card**.
4. If you want to re-format the card, click the **Format** button, and follow the prompts.
5. Click **OK** to encode the card, and follow the prompts.
6. Click **Save** to save the card holder or visitor details.

Using an Access-Control Reader

To gain access at a Suprema access-control reader:

1. Present your card to the reader.

2. Depending on how the reader is configured in BioStar 2 (page 2), the reader may, for example, give you the choice to present a finger or enter a PIN. If you want to enter your PIN, choose the relevant option.

3. Present your enrolled finger or face, and enter a PIN if required. If you want to signal duress, present your duress finger (if you have a duress finger enrolled).

4. If you have access rights to the reader in Symmetry, and the card and fingerprint\face image\PIN are valid, you will see "Access Granted" at the reader and the door will unlock. The door unlocks even if you used your duress finger. If your access rights set up in Symmetry are not valid, you will see "Access Denied" (FaceStation F2) or “Verify Fail” (BioLite N2).

Sending Commands

You can send commands to a Suprema access-control reader from, for example, the "Home/Monitoring/Command Centre" screen. The following commands are supported:

Automatic Door Controlled Enabled
Card Only
Card + PIN
Disable Reader
Disable Push Button
Enable Reader
Enable Push Button
Grant access
Keycard In
Keycard Mode Off
Keycard Mode On
Keycard Out
Lock door
Manual Door Control Enabled
Random Search On
Random Search Off
Re-enable Stopped Cards
Return to Schedule
Unlock door

Note: Other commands may be listed, but these will not function.

Appendix A: Upgrading the Firmware or Updating the Authentication Mode

Introduction

This appendix describes how to upgrade the reader firmware to obtain the latest updates from Suprema, and how to change the Private Authentication mode. See page 2 for an overview of the Private Authentication mode.

The firmware version and Private Authentication mode used by a Suprema reader is displayed in the **Information** page when configuring the reader in BioStar 2 (see page 17).

Upgrade / Authentication Mode Change Procedure

To upgrade the firmware (minimum 2.0.0 is needed) and/or to change the Private Authentication mode:

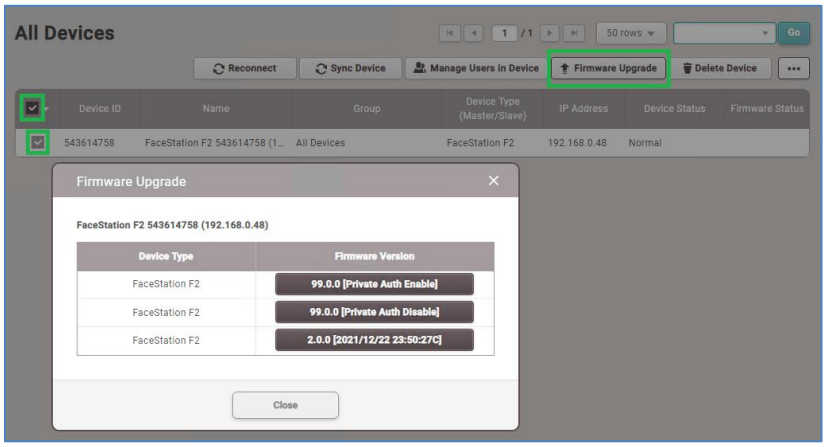
1. Download the latest Symmetry compatible firmware and/or Private Authentication configuration files and place them in the firmware folder on your BioStar 2 machine. For example:

   C:\Program Files\ BioStar 2(x64)\firmware

2. Under **All Devices** (page 17), select the reader(s) you want to upgrade/configure and click **Firmware Upgrade**.

   Alternatively, in the Information page of the reader you are configuring (page 17), click **Firmware Upgrade**. You can use this route only to upgrade the reader you are currently configuring.

3. The firmware and Private Authentication configuration versions are listed. For example:



4. Click the firmware version (e.g. **2.0.0 [2021/12/22 23:50:27C]** in the above example) or Private Authentication configuration version (e.g. **99.0.0 [Private Auth Enable]** in the above example). When prompted, confirm to start the upgrade process.

Appendix B: M4000 Alarm/Event Mapping

Standard Events

The following table shows the mapping between standard Suprema BioLite N2 or FaceStation F2 events and Symmetry alarms/events when an M4000 node is used.

Suprema Event	Symmetry Alarm/Event	Default Type
PIN_VERIFY_FAIL	Wrong PIN	Alarm
CARD_VERIFY_FAIL	Unknown Card	Alarm
IDENTIFY_FAIL	Unknown Card	Alarm
NOT_YET_VALID	Unknown Card	Alarm
EXPIRED	Card Expired	Alarm
CANNOT_FIND_ACCESS_GROUP	Unknown Card	Alarm
CANNOT_FIND_ACCESS_LEVEL	At Wrong Door	Alarm
CANNOT_FIND_ACCESS_SCHEDULE	At Wrong Time	Alarm
CANNOT_FIND_HOLIDAY_GROUP	At Wrong Time	Alarm
AUTH_UNEXPECTED_USER	At Wrong Door	Alarm
AUTH_UNEXPECTED_CREDENTIAL	At Wrong Time	Alarm
CANNOT_FIND_FLOOR_LEVEL	At Wrong Door	Alarm
HARD_APB_VIOLATION	Anti-Passback Hard	Alarm
SOFT_APB_VIOLATION	Anti-Passback Soft	Alarm
HARD_TIMED_APB_VIOLATION	Anti-Passback Hard	Alarm
SOFT_TIMED_APB_VIOLATION	Anti-Passback Soft	Alarm
FORCED_LOCK_VIOLATION	Door Forced	Alarm

INACTIVE_ZONE	Zone Disabled	Event
HARD_ENTRANCE_LIMIT_TIME_VIOLATION	At Wrong Time	Alarm
SOFT_ENTRANCE_LIMIT_TIME_VIOLATION	At Wrong Time	Alarm
AUTH_LIMIT_SCHEDULE_VIOLATION	At Wrong Time	Alarm

Extended Events

The following table shows the mapping between Suprema BioLite N2 or FaceStation F2 events and Symmetry alarms/events when an M4000 node is used and **Suprema Readers** is selected from the reader's **Extended Type** menu (see page 28).

Suprema Event	Symmetry Alarm/Event	Default Type
FINGERPRINT_VERIFY_FAIL /NOT_SAME_FINGERPRINT	Fingerprint Mismatch	Alarm
HIGH_TEMPERATURE_VIOLATION	High Temperature Violation	Alarm
UNMASKED_FACE_VIOLATION	Unmasked Face Violation	Alarm
EXTRACTION_FAIL	Biometric Features Extraction Failed	Event
FINGERPRINT_CAPTURE_FAIL	Fingerprint Capture Failed	Event
FINGERPRINT_SCAN_TIMEOUT	Fingerprint Scan Timeout	Event
FINGERPRINT_SCAN_CANCELLED	Fingerprint Scan Cancelled	Event
EXTRACTION_LOW_QUALITY	Fingerprint Quality Issue	Event
CANNOT_FIND_FINGERPRINT	Fingerprint Not Found	Event
FAKE_FINGER_DETECTED/ FAKE_FINGER_TRY_AGAIN/ FAKE_FINGER_SENSOR_ERROR	Fake Fingerprint	Alarm
CANNOT_FIND_FACE/ MATCH_FAIL	Face Not Found	Event
FAKE_FACE_DETECTED	Fake Face	Alarm
FACE_CAPTURE_FAIL/ FACE_SCAN_FAILED	Face Capture Failed	Alarm
FACE_SCAN_TIMEOUT	Face Capture Timed out	Event
FACE_SCAN_CANCELLED	Face Scan Cancelled	Event
UNMASKED_FACE_DETECTED	Unmasked Face Detected	Event

CANNOT_ESTIMATE/ NORMALIZE_FACE/ SMALL_DETECTION/ LARGE_DETECTION/ BIASED_DETECTION/ ROTATED_FACE/ OVERLAPPED_FACE/ UNOPENED_EYES/ NOT_LOOKING_FRONT/ OCCLUDED_MOUTH/ INCOMPATIBLE_FACE/	Error Verifying Face	Event
ACCESS_RULE_VIOLATION	Reader Access Rule Violation	Alarm
DISABLED	Reader Disabled	Alarm
BLACKLIST/ CANNOT_FIND_BLACKLIST	Blacklist Credential	Alarm
AUTH_SERVER_MATCH_REFUSAL	Reader Server Match Refused	Alarm
ANTI_TAILGATE_VIOLATION	Tailgating	Alarm
CANNOT_MEASURE_TEMPERATUR E	Unable To Measure Temperature	Event
CANNOT_FIND_ZONE	Invalid Zone	Event
INTRUSION_ALARM_VIOLATION	Intrusion Alarm Violation	Event
HARD_ENTRANCE_LIMIT_COUNT_VI OLATION/ SOFT_ENTRANCE_LIMIT_COUNT_VI OLATION	People Count Violation	Event
CAMERA_INIT_FAIL/ JPEG_ENCODER_INIT_FAIL/ CANNOT_ENCODE_JPEG/ JPEG_ENCODER_NOT_INITIALIZED/ JPEG_ENCODER_DEINIT_FAIL/ CAMERA_CAPTURE_FAIL	Reader Camera Failed	Event
AUTH_TIMEOUT/ DUAL_AUTH_TIMEOUT	Authentication Timed out	Event
INVALID_AUTH_MODE	Invalid Authentication Mode	Event
DUAL_AUTH_FAIL	Authentication Failed	Event
APB_ZONE_FULL	Anti-Passback Zone Full	Event
TIMED_APB_ZONE_FULL	Anti-Passback Timed Zone Full	Event
FIRE_ALARM_ZONE_FULL	Fire Alarm Zone Full	Event
FORCED_LOCK_UNLOCK_ZONE_FU LL	Forced Lock Unlock Zone Full	Event
INTRUSION_ALARM_ZONE_FULL	Intrusion Alarm Zone Full	Event

CANNOT_ARM/ CANNOT_DISARM	Unable To Arm/Disarm	Event
CANNOT_FIND_ARM_CARD/ CANNOT_FIND_DISARM_CARD	Unable To Find Arm/Disarm Card	Event
INTERLOCK_ZONE_DOOR_VIOLATION	Interlock Zone Door Violation	Event
INTERLOCK_ZONE_INPUT_VIOLATION	Interlock Zone Input Violation	Event
INTERLOCK_ZONE_FULL	Interlock Zone Full	Event
AUTH_LIMIT_SCHEDULE_VIOLATION	Authentication Limit Schedule Violation	Event
AUTH_LIMIT_COUNT_VIOLATION	Authentication Limit Count Violation	Event
AUTH_LIMIT_USER_VIOLATION	Authentication Limit User Violation	Event
SOFT_AUTH_LIMIT_VIOLATION	Soft Authentication Limit Violation	Event
HARD_AUTH_LIMIT_VIOLATION	Hard Authentication Limit Violation	Event
LIFT_LOCK_UNLOCK_ZONE_FULL	Lift Lock/Unlock Zone Full	Event
LIFT_LOCK_VIOLATION	Lift Lock Violation	Event
OCCUPANCY_LIMIT_COUNT_VIOLATION	Occupancy Limit Count Violation	Event
OCCUPANCY_LIMIT_NETWORK_VIOLATION	Occupancy Limit Network Violation	Event
OCCUPANCY_LIMIT_ZONE_FULL	Occupancy Limit Zone Full	Event
CANNOT_DETECT_FACE	Unable To Detect Face	Event
FAILED_ON_1TO1_VERIFICATION	Failed on 1:1 verification	Alarm