SIEMENS

Access Control

SiPass integrated

Biometric Integration

MP 2.80

A-100062-1

Smart Infrastructure

07.09.2020

Copyright

Edition: 07.09.2020

Document ID: A-100062-1

Table of Contents

1 Introduction

The Bioscrypt functionality allows operators to capture fingerprint templates and encode the fingerprint template into the smart card during enrollment.

An optional feature allows operators to capture and store the fingerprint template into the SiPass integrated database. This feature is configurable based on the individual country regulations regarding fingerprint storage.

This functionality allows operators to encode fingerprint templates as cardholder data into the smart card, while enrolling the card at the same simultaneously.

It supports the 1K and 4K Mifare cards, and the 2K, 4K and 8K DESFire Card Technology.

It utilizes the Triple DES (also known as 3DES), mechanism for encryption.

The Bioscrypt reader can be connected to RIM devices (DRI, ERI and SRI) for Access Control.

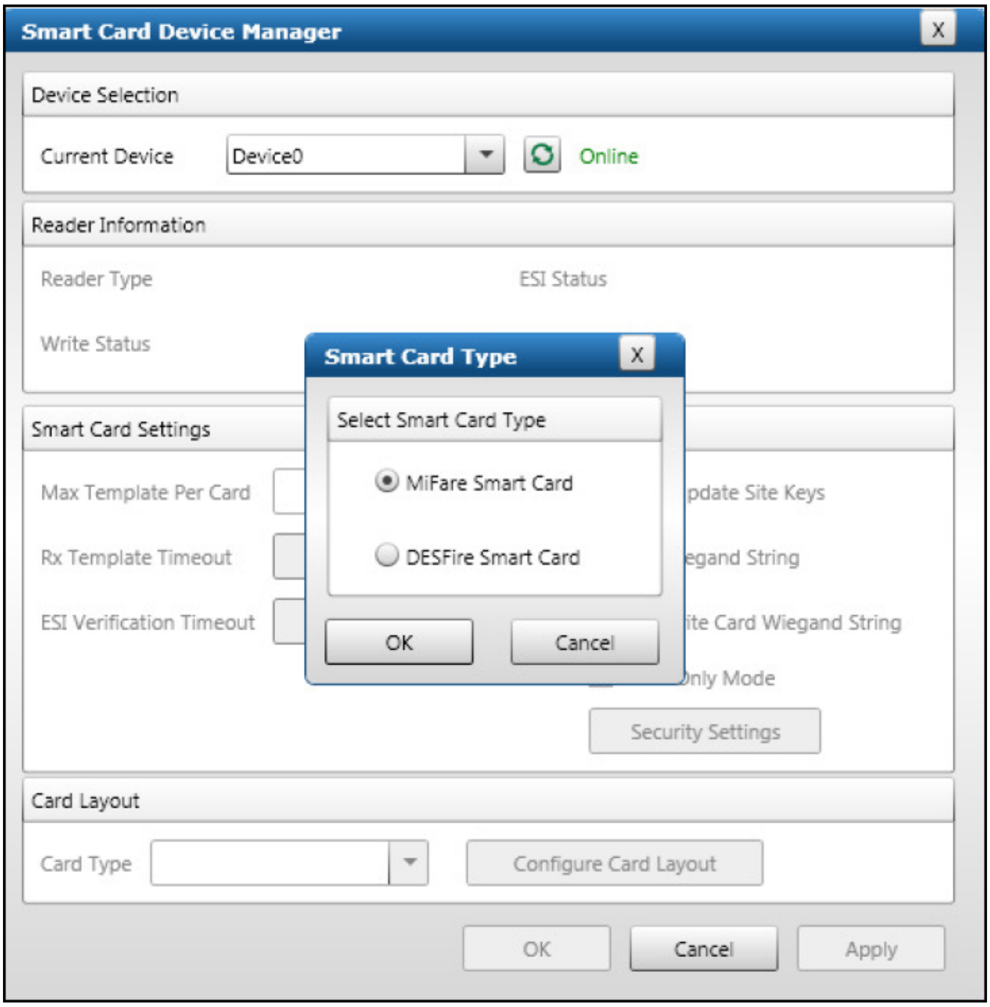
1.1 Pre-requisites

Before proceeding to create a Bioscrypt components in SiPass integrated, the operator must ensure that the following prerequisites are available with the SecureAdmin application.

- Install the Server and Client of the SecureAdmin version 4.1.9.

After the SecureAdmin applciation is installed, the documentation for the application should also be availble on your PC. Please refer the same for information on how to use the application

- Register the BIOSCRYPT V-Station reader in SecureAdmin. Please refer the Secure Admin documentation for detailed information on how to register.
- Ensure you select the smart card type (Mifare or DESFire) before you configure. Navigate to the Smart Card Device Manager dialog and select any one of the card type.



Smart Card Device Manager

Device Selection

Current Device: Device0 — Online

Reader Information

Reader Type | ESI Status

Write Status

Smart Card Settings

Max Template Per Card

Rx Template Timeout

ESI Verification Timeout

Smart Card Type

Select Smart Card Type

● MiFare Smart Card

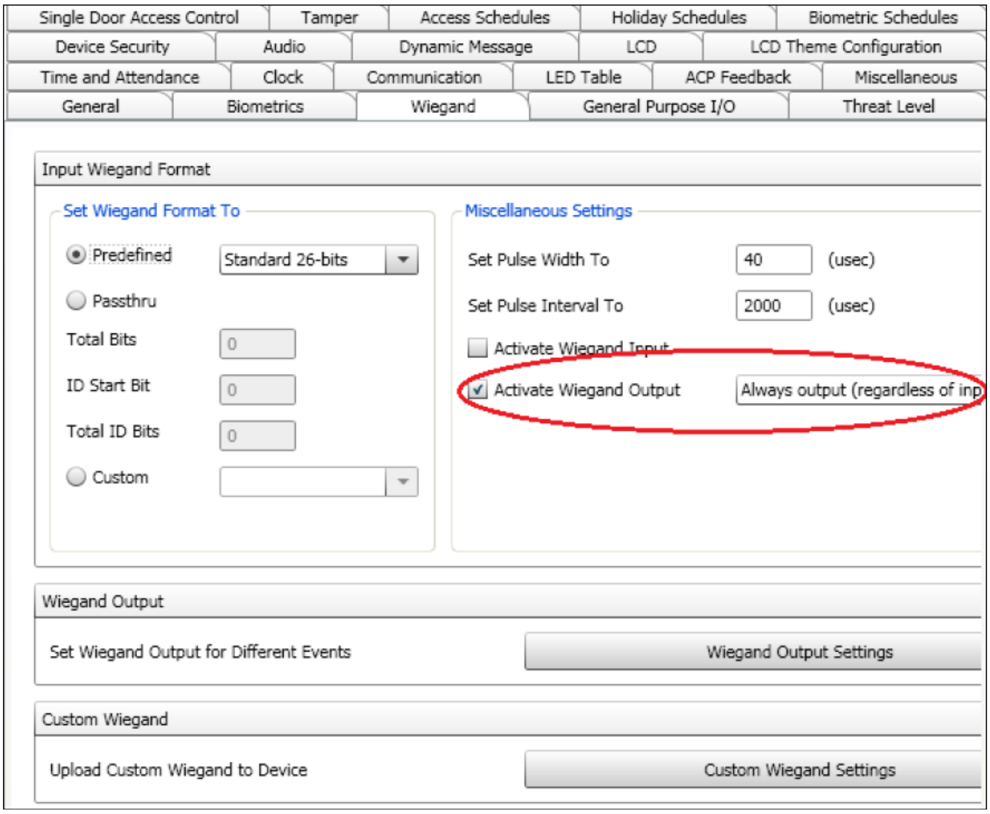
○ DESFire Smart Card

Card Layout

Card Type

Configure the **Wiegand** output for the BIOSCRYPT V-Station reader. This can be done through the following steps:

1. Navigate through Device Settings to locate the *Wiegand* tab of the BIOSCRYPT V-Station device.



● Predefined: Standard 26-bits

○ Passthru

Total Bits: 0

ID Start Bit: 0

Total ID Bits: 0

○ Custom

Set Pulse Width To: 40 (usec)

Set Pulse Interval To: 2000 (usec)

□ Activate Wiegand Input

☑ Activate Wiegand Output: Always output (regardless of inp

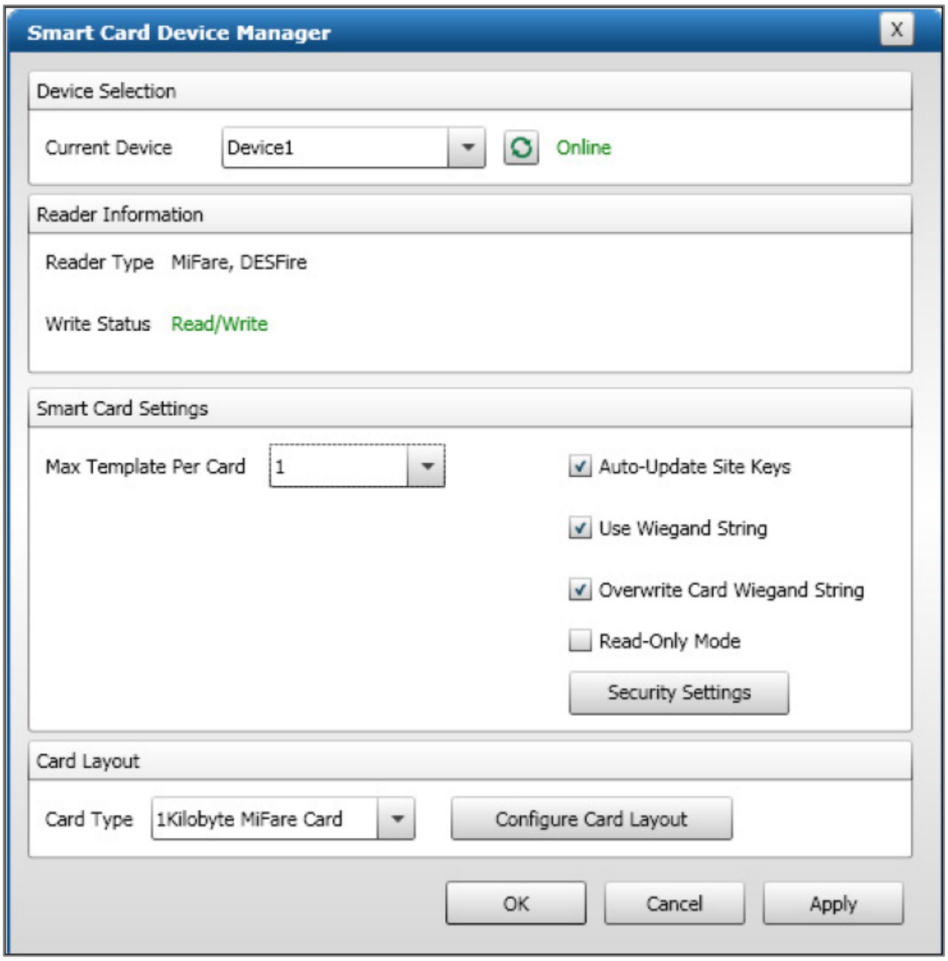
Set Wiegand Output for Different Events

Upload Custom Wiegand to Device

Figure 1:

2. In the *MiscellaneousSettings*section of this tab, check the **ActivateWiegandOutput**checkbox.
3. Select **AlwaysOutput**in the adjacent dropdown field.
4. Click the **WiegandOutputSettings**button. Set **VerificationOutput.**To set the Verification Output for a specific smart card type see the sections that follow
5. Proceed to create a **SiteKey**to authenticate the Mifare Smart Card. A de- tailed guide for the same can be found in the **SecureAdmin**documentation.
6. Set the **SiteKey**and **SmartcardLayout**on the BIOSCRYPT V-Station reader. Refer the SecureAdmin documentation to set the Site Key.

7. Open the **SmartCardDeviceManager**and ensure that the Use Wiegand String option is ticked for every device integrated into the system. **OverwriteCard WeigandString**should also be ticked for Mifare DESFire card.



Smart Card Device Manager

Device Selection

Current Device: Device1 — Online

Reader Information

Reader Type: MiFare, DESFire

Write Status: Read/Write

Smart Card Settings

Max Template Per Card: 1

☑ Auto-Update Site Keys

☑ Use Wiegand String

☑ Overwrite Card Wiegand String

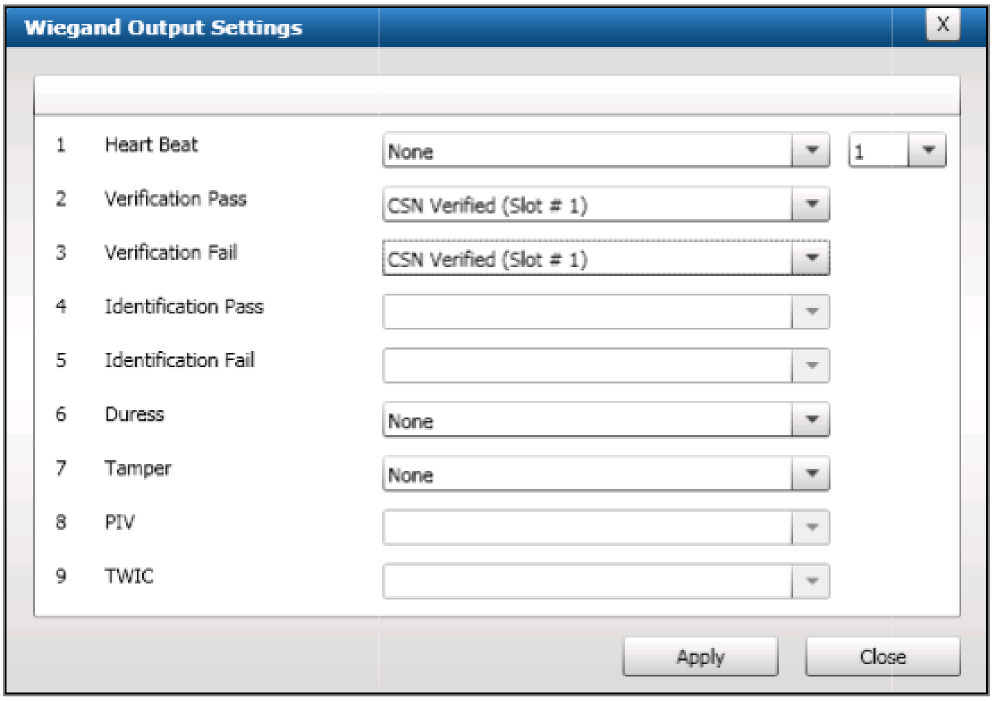
☐ Read-Only Mode

Card Layout

Card Type: 1Kilobyte MiFare Card

1.1.1 To configure the Mifare Classic card template

- The custom format is used to send the CSN number of cards that use the Mifare Classic card technology.
- To set Verification Output, Click Wiegand Output Settings button in the Wiegand tab.

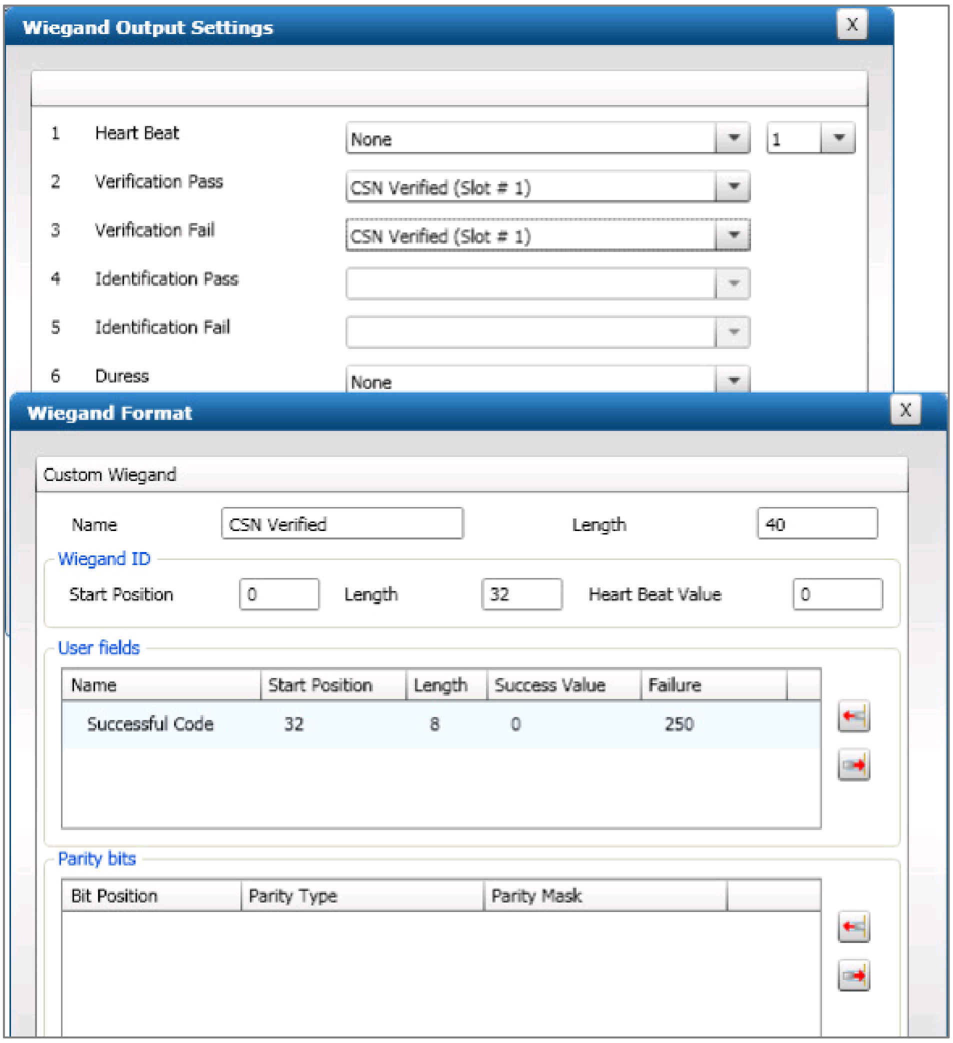


Wiegand Output Settings

1	Heart Beat	None	1
2	Verification Pass	CSN Verified (Slot # 1)	
3	Verification Fail	CSN Verified (Slot # 1)	
4	Identification Pass		
5	Identification Fail		
6	Duress	None	
7	Tamper	None	
8	PIV		
9	TWIC		

Figure 2:

- ◈ Click the Custom Wiegand Settings button, and configure the template in the Weigand Format dialog displayed.



Wiegand Output Settings

1	Heart Beat	None	1
2	Verification Pass	CSN Verified (Slot # 1)	
3	Verification Fail	CSN Verified (Slot # 1)	
4	Identification Pass		
5	Identification Fail		
6	Duress	None	

Wiegand Format

Custom Wiegand

Name: CSN Verified Length: 40

Wiegand ID

Start Position: 0 Length: 32 Heart Beat Value: 0

User fields

Name	Start Position	Length	Success Value	Failure
Successful Code	32	8	0	250

Parity bits

Bit Position	Parity Type	Parity Mask

1. Enter the **Name** of the configuration.
2. Enter **Length** as 40.
3. In the **Weigand ID** settings, Enter **Start Position** as 0, **Length** as 32, **Heart Beat Value** as 0.
4. In the **User fields** settings, specify the following information:

Name - Successful code

Start Position - 32

Length - 8

Success Value - 0

Failure - 250

- ◈ Click **Apply**.

This configuration is required only if the system is required to configure the Mifare Classic card.

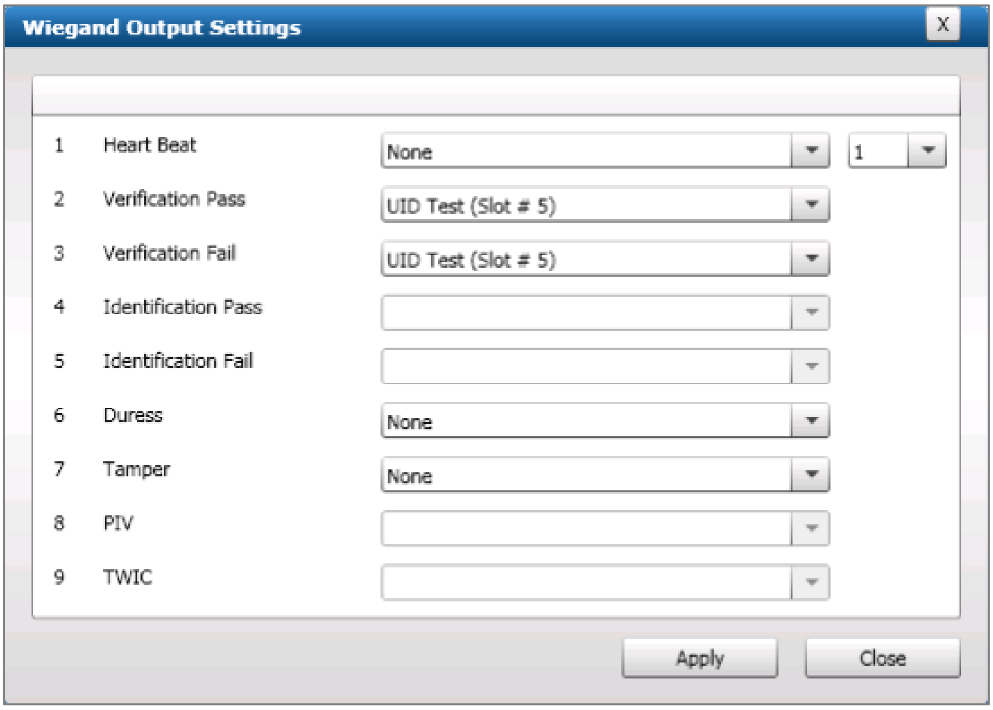
1.1.2 To configure the Mifare DESFire card template

The Card Type has to be set to DESFire to configure a DESFire card. To select the card type as DESFire, perform the following steps:

1. Click the Smart Card tab from SecureAdmin to open the Smart Card Device Manager dialog.
2. Select DESFire Smart Card from the Smart Card Type pop-up.

The custom format is used to send the UID number of cards that use the Mifare DESFire card technology.

To set Verification Output, Click Wiegand Output Settings button in the Wiegand tab.

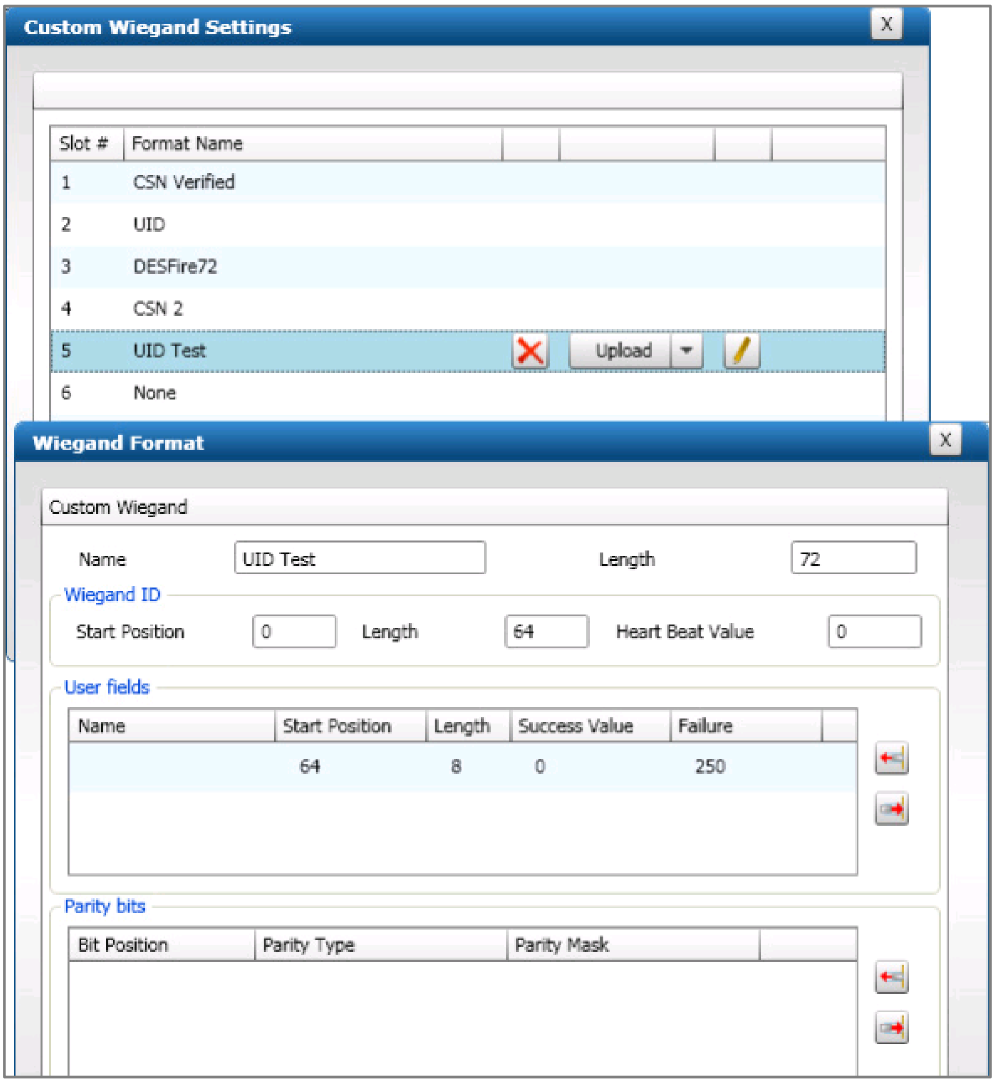


Wiegand Output Settings

1	Heart Beat	None	1
2	Verification Pass	UID Test (Slot # 5)	
3	Verification Fail	UID Test (Slot # 5)	
4	Identification Pass		
5	Identification Fail		
6	Duress	None	
7	Tamper	None	
8	PIV		
9	TWIC		

Figure 3:

1. Click the Custom Wiegand Settings button, and configure the template in the Weigand Format dialog as displayed.



Slot #	Format Name
1	CSN Verified
2	UID
3	DESFire72
4	CSN 2
5	UID Test
6	None

Custom Wiegand

Name: UID Test   Length: 72

Wiegand ID

Start Position: 0   Length: 64   Heart Beat Value: 0

User fields

Name	Start Position	Length	Success Value	Failure
	64	8	0	250

Parity bits

Bit Position	Parity Type	Parity Mask

Figure 4:

2. Enter the **Name** of the configuration.

3. Enter **Length** as 72.

4. In the **Weigand ID** settings, Enter **Start Position** as 0, **Length** as 64, **HeartBeat Value** as 0.

5. In the **User fields** settings, specify the following information:

Name

Start Position -64

Length-8

Success Value-0

Failure-250

◈ Click **Apply**.

This configuration is required only if the system is required to configure the Mifare Classic card

2 Configuring the Bioscrypt Bus

1. This section details the steps required to configure a Bioscrypt bus in SiPass integrated.
2. Select **System > Components** on the SiPass integrated main menu to open the *Components* dialog.
3. Select the SiPass integrated server as required.
4. Click the **New Bus** button, and select **Bioscrypt System**.
5. Enter a name for the bus in the **Name** field.
6. Enter the **Site Key**. The Site Key entered here should match the Site Key configured in SecureAdmin. The Site Key should be of 12 digits.
7. In the Biometric Quality Section, configure the expected quality of the fingerprint. Adjust the **Minimum Quality** and the **Minimum Content** of the fingerprint.

!	*NOTICE*
	In order to be accepted by the SiPass integrated system, fingerprints presented through the Bioscrypt reader must meet the minimum standards set in the Minimum Quality and Minimum Content fields. By default the **Minimum Quality** and **Minimum Content** is 50.

8. Click **Save**.

⇨ The Bioscrypt bus will be saved with the configured settings.
⇨ The ACC should be initialized for changes to take effect

3 Saving the Custom Card Configuration

1. Select System > FLN Configuration from the SiPass integrated main menu to open the FLN Configuration dialog.
2. Expand the Global Settings item in the tree hierarchy on the left hand pane.
3. Select the Custom Card Format tab.
4. Click the Add button.
5. The Custom Card Configuration dialog appears with a default configuration.
6. Change the default configuration of the Custom Card Configuration according to the below steps.
7. Enter a new Name for the custom card to be used for the Bioscrypt functionality.
8. Set the Total Length field from 1 to 40 for Mifare smart card and 1 to 72 for DESFire smart card.
9. Set the Number field from 1 to 32 for Mifare smart card and 1 to 64 for DESFire smart card.
10. Un-tick the Facility field checkbox.
11. Tick the Revision field checkbox, and set this field from 33 to 40 for Mifare smart card and 65 to 72 for DESFire Smart Card.
12. Un-tick the Even Parity and Odd Parity fields.
13. Click OK to save the custom card configuration.
14. The newly created custom card configuration is added to the Custom Card Format list.
15. Navigate to the door reader device being used in the FLN Configuration dialog from the tree hierarchy.
16. Click the Configuration tab for the device.
17. Ensure that Custom Card (Wiegand) is selected in the Technology field.
18. In the Configuration field, select the newly created custom card (Mifare/DESFire) format from the drop down list.
19. Click the Save Configuration button to save the custom card configuration.
20. Click the Close button.

4 Creating a Bioscrypt Credential Profile

1. Select **Program > Credential Profile** from the SiPass integrated main menu to display the Credential Profile dialog.
2. Select the **Base** card profile.
3. Verify if **Bioscrypt Credential** is checked for this profile.
4. Click **OK** to save this profile.

5 Determining the Bioscrypt / Enrolment Reader Configuration

The Bioscrypt reader and the Enrollment reader can be configured in SiPass integrated for the Bioscrypt functionality. The operators can decide if they require an enrollment reader, apart from the Bioscrypt reader; in which case, they will need to configure an enrollment reader in the Enrollment Configuration dialog. The enrollment reader must be configured to import a Bioscrypt Profile.

The steps required to configure a Bioscrypt and Enrollment reader in SiPass integrated are explained in the sections that follow.

Please note that the configuration explained in this section is client-specific.

5.1 Configuring the Bioscrypt Reader in SiPass integrated

1. Select Options > Enrollment Reader Configuration on the SiPass integrated main menu.
2. Click the Add button.
3. From the Select Type drop down list, select Bioscrypt Reader Configuration.

Please note that the **Encode** button of the Cardholder dialog will be disabled if the Bioscrypt reader configuration is the only card reader added in the **Select Type** field of the Enrollment Reader Configuration dialog.

4. Tick the Reading checkbox if you wish to use the Bioscrypt Reader only to read the card.
5. Or else, tick the Encoding checkbox if you wish to use the Bioscrypt Reader to encode the card. Ticking the Encoding checkbox ticks the Reading checkbox by default.

The options available in the Fingerprint Enrollment section of this dialog, determine the various functionalities that can be configured. The table below explains the options.

Configuration Option	Expected Configuration Action
Prompt to encode the fingerprint on card	When this option is ticked, the Bioscrypt device is used to encode the fingerprint template on the card. When this option is un-ticked, the system saves the acquired fingerprint to be stored in the SiPass database.
Use Card Serial Number as Template Identifier	When this option is ticked, the fingerprint template will be identified by the Card Serial Number (CSN) of the card. When this option is un-ticked, the fingerprint template will be identified by the card number given in the Definition tab of the Cardholder dialog. If no card number was specified, the user is notified that a card number is required to complete the card assignment operation.
Store the fingerprint for encoding later	When this option is ticked, the fingerprint will be saved to the database as part of the enrollment process.

!

NOTICE

For **Configuration Type A: Card Assignment - Prompt to encode the fingerprint on card** and **Use Card Serial Number as Template Identifier** options should be checked.

For **Configuration Type B: Fingerprint Accquisition - Use Card Serial number as Template Identifier** and **Store the fingerprint for encoding later** options should be checked.

1. In the Communication Settings section of this dialog, do the following:
2. Enter an appropriate value for the Bioscrypt device in the **Device ID** field. The Device ID value for Bioscrypt reader shall match the Device ID value set in the Communication tab of SecureAdmin.
3. Specify the type of connection to the Bioscrypt reader in the **Connect Using** field.
4. Enter the IP address of the Bioscrypt device in the **IP Address** field.
5. Click **Save** to save this configuration.

5.2 Configuring an Enrollment Reader for the Bioscrypt functionality

If you wish to use an enrollment reader as part of the Bioscrypt functionality, the reader needs to be configured in the Enrollment Reader configuration dialog.

ℹ The option to use the enrollment reader to read, search and assign cards will be enabled in the Cardholder dialog,only when the enrollment reader is configured to the Reading mode in the Enrollment Reader Configuration dialog. This action ensures that the Read, Assign and Read & Search buttons of the Cardholder dialog will be made drop-down buttons, to allow selection of the reader device to be used.

1. Select **Options > Enrollment Reader Configuration** on the SiPass integrated main menu.
2. Click the **Add** button.
3. From the **Select Type** drop down list, select the enrollment reader to be used for this functionality.
4. Tick the **Reading** checkbox of the **Operation Mode** field.
5. In the **Profile Name** field, select the Bioscrypt profile from the drop down list.
6. Set the **Sector / Application** in the fields.
7. Select the port to be used for the enrollment reader in the **Port Name** field.
8. Click **Save** to save this configuration.

6 Importing the Bioscrypt Reader Configuration

The user can import a Bioscrypt profile into SiPass integrated by using the Profile Configuration dialog.

Ensure that the Bioscrypt Reader has been configured in SiPass integrated. Refer Configuring the Bioscrypt reader in SiPass integrated [→ 1-14] on how to configure a Bioscrypt Reader.

1. Click System > Profile Configuration from the SiPass integrated main menu.
2. Enter a new Profile Name for the Bioscrypt profile.
3. Select a Card Type.
4. Click the Import dropdown button, and select Bioscrypt Reader Configuration to import the Bioscrypt reader configuration into this dialog.
   - ⇨ The reader configuration layout gets automatically imported from the reader into SiPass integrated, and is displayed on this dialog. After importing the Bioscrypt profile, the user can change or add new fields to the profile as needed.

Next, a new Sector Key needs to be configured for this configuration.

1. Click the drop down arrow of the Keys button.
2. Select between Mifare Key or DESFire Key.

ℹ Each profile created by SiPass integrated can have only one Bioscrypt binary data.

- ⇨ This action displays the Keys Configuration dialog.

3. Enter a new Key Name.
4. Enter the transport keys of the Mifare card in the Smart Card Keys section of this dialog.
5. Tick the Overwrite the Sector Key checkbox if you want to overwrite the sector key.
   - – The Site Keys entered here must match the Site Key entered in the Components dialog while creating the Bioscrypt bus.
   - – If the length of the Site Key is less than 32 digits, it should be appended with zeroes to fill 32 digits if DESFire key is used.
   - – The File ID should be the same that has been configured in the Bioscrypt system. Refer the section Configuring Bioscrypt bus for more information.

1. Next, each sector of the Bioscrypt Profile needs to be configured with the newly created Site Key.
2. To do this, double-click each Key icon corresponding to a sector of the profile. A drop-down list is displayed.
3. Select the new Site Key for the Bioscrypt profile from this list, and continue to configure this key to all the remaining sectors of this profile.
4. Click the Save button to save this configuration.
5. For detailed information on configuring a card profile, please refer the section Creating a Smart Card Profile do this, double-click each Key icon corresponding to a sector of the profile.

7 Configuring the Bioscrypt profile to a Work Group

This section details the steps required to configure a new workgroup with the Bioscrypt profile.

1. Select **Operation > Work Group** on the SiPass integrated main menu to open the Work Group dialog.
2. Configure a New Work Group.
3. Click the drop down arrow of the Profile field, and select the Bioscrypt smart card profile created.
4. Click **Save**.

8 Types of Bioscrypt Configuration in SiPass

SiPass integrated can be configured to work with the Bioscrypt reader in two ways, each providing a different functionality. A brief explanation of each configuration type follows.

Card Assignment

This configuration type allows operators to use the SiPass integrated interface to select cardholders for whom fingerprints are required. The Bioscrypt reader is then used to obtain the cardholder's fingerprint, and assign a card with fingerprint details written to it.

In this case, the fingerprint template is not saved to the database. In is only saved to the card assigned.

Fingerprint Acquisition

The functionality of this configuration builds on the result of Configuration Type 1, where a cardholder is assigned a card containing their fingerprint information.

However, in this type of configuration, SiPass integrated also saves the fingerprint to the database for future use.

8.1 Configuration Type A: Card Assignment

Through this configuration, the operator selects a cardholder in SiPass integrated, whose card will then be assigned and written with their fingerprint data using the Bioscrypt reader device. A summary of the configuration stages required for this scenario is detailed below.

8.1.1 Summary of Configuration Stages for Type I

- Ensure that you have installed the SecureAdmin client and server software.
- Ensure that you have created a Bioscrypt bus in SiPass integrated.
- Ensure that you have saved the custom card configuration in SiPass integrated.

1. Configure the Bioscrypt Enrollment Reader in SiPass integrated through the Enrollment Reader Configuration dialog. For further information, refer the section Configuring the Bioscrypt Reader for Configuration
2. Use the Cardholder dialog to begin scanning a fingerprint on the Bioscrypt reader, and assigning a card with the fingerprint. For further information, refer the section Assigning Fingerprints and Cards with the Bioscrypt Reader.

The sections that follow explain each of these configuration stages in detail.

8.2 Configuring the Bioscrypt Reader for Configuration I

The Bioscrypt reader can be configured to read and encode the fingerprint template onto a card in this type of configuration, without saving the card template to the database.

Follow the steps described in the section Configuring the Bioscrypt reader in SiPass integrated.

Ensure that **Prompt to encode the fingerprint on card** option is checked on Enrollment Reader Configuration dialog.

8.3 Assigning Fingerprints and Cards with the Bioscrypt Reader

Once operators have created a Bioscrypt bus, and the enrolled a Bioscrypt reader in SiPass integrated, they can proceed to assign cards with fingerprints using the Bioscrypt reader. This is done on the Cardholder dialog. The instructions that follow explain this process.

1. Select **Operation > Cardholder** on the main menu to display the Cardholder dialog.
2. Click the **Assign** drop down button, and select **Assign fingerprint from Bioscrypt** reader. The drop-down appears only if multiple readers have been connected to SiPass integrated.
3. Register Card with Fingerprint dialog will be displayed.
4. Follow the instructions of the dialog to acquire a fingerprint.
5. When a satisfactory fingerprint has been obtained, the Cardholder dialog prompts to register the fingerprint with a card.
6. Place the card on the Bioscrypt reader to assign the fingerprint to the card.
7. The card number will be displayed on the Cardholder dialog. And an icon is displayed on the definition tab of the cardholder indicating that fingerprint is on the card.
8. Configure all other required cardholder details.
9. Click the **Access Privileges** button, and define the access items for the cardholder and click **OK**.
10. Click **Save**.
    - ⇨ As a result of this configuration, the acquired fingerprint gets physically assigned to a card using the Bioscrypt reader. This is also indicated by an icon.

You can inspect the card after acquiring the fingerprint.

In the Cardholder dialog, click **Read** drop-down and select **Inspect Bioscrypt Card**. Read Card dialog shows up. Place the card on the Bioscrypt reader.

The Bioscrypt reader reads the card and shows the biometrics stored on the card.

You can verify the card details by doing the following steps:

1. Badge the card on the Bioscrypt reader; follow the instruction on the reader and present fingerprint.
2. If the card is valid then it is notified to the user by an audit trail message which says Valid. If the card is invalid then it is notified to the user through an audit trail message which says Invalid.

8.4 Configuration Type B: Fingerprint Acquisition

This functionality allows the operator to use SiPass integrated to encode a card that has already been assigned fingerprints through the Bioscrypt reader.

A summary of the configuration stages required for this scenario is detailed below.

Summary of Configuration Stages for Type I

- Ensure that you have installed the SecureAdmin client and server software.
- Ensure that you have created a Bioscrypt bus in SiPass integrated.
- Ensure that the Bioscrypt Reader Configuration has been imported for the purpose of configuring the smart card profile. For more information, refer the section Importing the Bioscrypt Reader Configuration.
- Ensure that a Bioscrypt profile has been configured for a work group. For more information, refer the section Configuring the Bioscrypt profile to a Work Group.

Make sure, in the Enrollment Reader Configuration dialog, under the **Finger Enrollment** section, the **Use Card Serial Number as Template Identifier** is unchecked and **Store the fingerprint for encoding later** option is checked for this configuration.

Configure the Bioscrypt Enrollment Reader in SiPass integrated through the Enrollment Reader Configuration dialog. For further information, refer the section Configuring the Bioscrypt Reader for Configuration.

Use the Cardholder dialog to begin scanning a fingerprint on the Bioscrypt reader, and assigning a card with the fingerprint. For further information, refer the section Card Enrollment with Bioscrypt Details.

The sections that follow explain each of these configuration stages in detail.

8.5 Configuring an Enrollment Reader for Configuration II

The Bioscrypt reader must be configured in SiPass integrated. This section details the steps required to do this.

It is important to note that the configuration explained in this section is client-specific.

1. Select **Options > Enrollment Reader Configuration** on the SiPass integrated main menu.
2. Click the **Add** button.
3. From the **Select Type** drop down list, select **Profile Reader – OmniKey Card-Man 5×21**. Ensure that the **Bioscrypt Reader Configuration** is also added as part of this drop down list. Ensure that the **Encoding** is checked.

Note that on selecting this reader type, the **Encoding** checkbox gets ticked by default and the **Profile** section of this dialog becomes enabled. The OmniKey CardMan 5*21 reader is used to read both Mifare and DESFire cards.

4. From the **Profile Name** drop down list, select the card profile to be used for the bioscrypt card enrollment.
5. Enter the **Sector/ Application** for the profile selected. (Sector is entered for Mifare card. Application is entered for DESFire card)
6. From the **Port Name** drop down list, specify the port name of the card reader.
7. Click **Save** and **Close**.
   ⇨ The enrollment reader will be now be enrolled in SiPass integrated.

8.5.1 Card Enrollment with Bioscrypt Details

Once operators have created a Bioscrypt bus, enrolled the Bioscrypt reader, and imported a Bioscrypt Profile in SiPass integrated, they can proceed to assign cards with fingerprints using the Bioscrypt reader. This is done on the Cardholder dialog.

The instructions that follow will explain this process

Ensure that the Bioscrypt smart card profile is selected in the **Profile** field of the Personal tab on the Cardholder dialog.

8.5.1.1 Assigning a fingerprint to the card

The fingerprint details of the cardholder are displayed on the Personal tab of the Cardholder dialog.

This tab contains a section called Finger Prints where finger print details can be configured and displayed.

Note: A maximum of 2 fingerprints can be saved for each cardholder.

1. Select Operation > Cardholder on the main menu to display the Cardholder dialog.
2. To assign a finger print to a card, place the card on the Enrollment Reader.
3. Click Assign to get the CSN number. The CSN number is displayed in the Card Number field of on the Cardholder dialog.
4. Enter the required cardholder details like the First Name, Last Name, Work-group, etc.
5. Click the Access Privileges button, select the access items for the cardholder and click OK.
6. Click the Assign drop down button, and select Acquire fingerprint for basecard from Bioscrypt reader.
7. Follow the instructions on the dialog to acquire a fingerprint.
8. You can repeat this step to capture additional fingerprints. However, only 2 of these prints can be saved in the system.
9. The Finger Prints section of the Advanced tab will display a new row for the captured fingerprint. If you have captured multiple fingerprints, select the rows that you do not require, and click the Delete button to remove these rows.
10. In the Index field, click to select the finger name was used for the fingerprint capture.
11. In the Credential Profile field, select a credential profile to which this fingerprint should be saved.
12. Click Save. The fingerprint/s will be saved in the SiPass integrated system. This system indicates this by displaying a ticked Saved checkbox for the fingerprint that was saved.
13. Click Read & Search button to read the contents of the card placed on the reader. An icon is displayed on the cardholder dialog which depicts fingerprint is on the card as well as on the disk.
14. Click Encode. The fingerprint/s will be encoded to the card. This system indicates this by displaying a ticked Encoded checkbox for the fingerprint that was encoded to a card.

   ⇨ Smart Card encoding successful message is displayed to the user.
   ⇨ As a result of this configuration, the fingerprint gets encoded to a card using the Bioscrypt reader.

You can inspect the card after acquiring the fingerprint.

- In the Cardholder dialog, click Read drop-down and select Read card from Profile Reader – OmniKey CardMan 5×21. Read Card dialog shows up. Place the card on the Bioscrypt reader.

The Bioscrypt reader reads the card and shows the biometrics stored on the card.

You can verify the card details by doing the following steps:

1. Badge the card on the Bioscrypt reader; follow the instruction on the reader and present fingerprint.
2. If the card is valid then it is notified to the user by an audit trail message which says Valid. If the card is invalid then it is notified to the user through an audit trail message which says Invalid.

Issued by
Siemens Switzerland Ltd
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies