

Table of Contents

How to issue smart cards 1

Configure a smart card format 1

Applying the configured smart card format to the devices 4

Formatting a card 4

Issuing a smart card 5

[System Configuration](#), [BioStar 2](#), [Smart](#), [Card](#)

How to issue smart cards

The BioStar 2 system is designed to authenticate users matching the template stored inside the device with the scanned fingerprint template. However, there are needs for securing personal information including fingerprint templates. In BioStar 2, the administrator can use a concept called smart card which will allow issuing cards to store users' fingerprint templates inside a card and carry it for authentication. This will lead to a more secure environment since the devices don't have to store the user information inside the device.

To issue a smart card, such as Access on Card and Secure Credential card, you will have to configure the smart card format first and apply it to the device.

Access on Card doesn't need any user information transferred to the device. Secure Credential Card needs basic user information stored inside the device.
Secure Credential Card is used when only to store the fingerprint template inside the card.

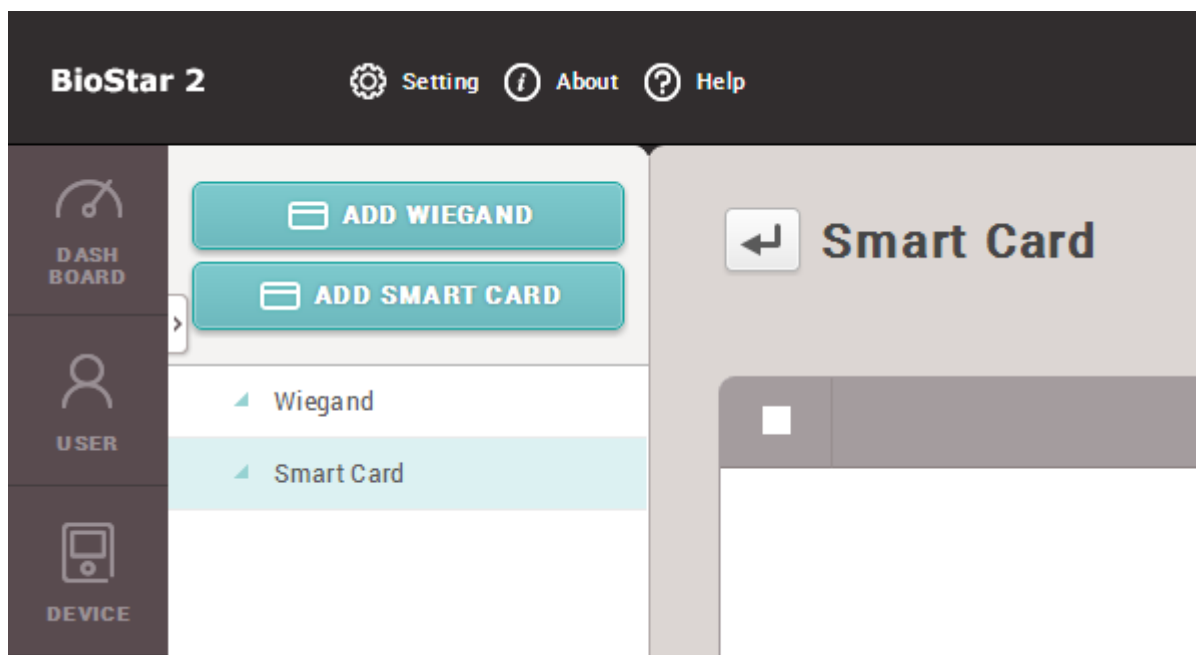
To delete the user fingerprint template information from BioStar 2 DB after writing Access On Card, enable [Delete personal & credential data when issuing an AoC].
Direction>Settings>Server> [Delete personal & credential data when issuing an AoC]

In addition, please disable Automatic User Synchronization. If not, the BioStar 2 server synchronizes the user information to the connected devices automatically.

To understand the benefits and difference between the two smart cards, refer to the following [FAQ](#)

Configure a smart card format

1) Go to **Setting** → **Card Format** → **Add Smart Card**.



2) Enter the name of the smart card format. There are 4 types of cards supported for the AoC card and the SC card, Mifare, iClass, DESFire, and iClass Seos (added in BioStar 2.6). Select the card that will be used for the smart card.

The screenshot shows the 'Add New Smart Card' form. At the top, there's a header with a back arrow and the title 'Add New Smart Card'. Below it is a tab labeled 'Information'. The form contains several fields: 'Name' (set to 'Mifare'), 'Secondary Key' (with a toggle switch set to 'Inactive'), 'Primary Key' (with a dropdown menu and a text input field containing 'abcd12345678'), 'Confirm New Primary Key' (a text input field), 'Secondary Key' (with a checkbox and a text input field containing 'New Secondary Key'), 'Confirm New Secondary Key' (a text input field), and 'Start Block Index' (a dropdown menu set to '4'). There are also tabs for 'MIFARE', 'ICLASS', 'DESFire', and 'ICLASS Seos', with 'MIFARE' selected. On the right side, there is a red warning message: 'The key values made with 2.5v or before need to be converted to HEX through the below before applying.' Below this message is a text input field and a 'Convert to HEX' button. At the bottom right, it says 'Converting Result : 35353535353535353535353535353535'.

You can use hexadecimal Keys starting in BioStar 2.6. Refer to the [How to Configure Hexadecimal Card Key](#)

DESFire cards are only supported if the encryption type is DES/3DES.

Refer to the [FAQ article](#) to check which devices/firmware support SEOS cards.

3) You can select to use up to 2 card keys for the card. To use the Secondary Key, you will have to activate it first. Check the checkbox if you need to use the key.

If you're trying to write a key to a blank card without a key, configure the primary key and turn on the secondary key but leave the secondary key blank.

Information

• Name

Mifare Layout

• Secondary Key



Active

MIFARE

iCLASS

DESFire / Mobile

iCLASS Seos

• Primary Key ☒

.....

.....

• Secondary Key ☒

New Secondary Key

Confirm New Secondary Key

• Start Block Index

4

The key values made with 2.5v or before need to be converted to HEX through the below before applying.

Convert to HEX

Converting Result :

Information

• Name

Test

• Secondary Key



Active

MIFARE

iCLASS

DESFire

• Primary Key ☒

....

....

• Secondary Key ☒

.....

.....

• Start Block Index

4

4) You can configure how many templates you want to store inside the card and which block to start on storing the information. You can also configure the template size, if you don't have enough space on the card to fit the template.

• Start Block Index

8

Layout

• Template Count

2

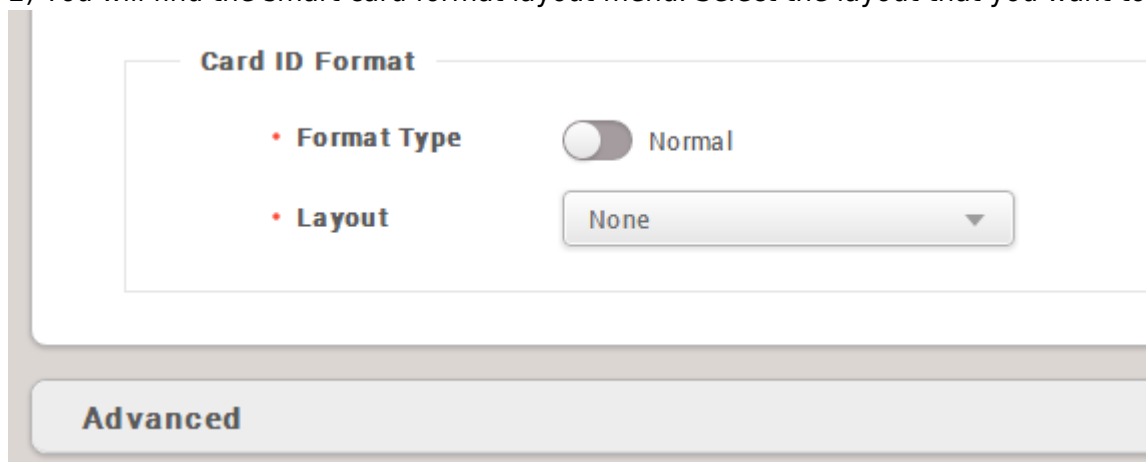
• Template Size

300

Applying the configured smart card format to the devices

To make the device read the smart cards, you will have to set the device to have the smart card format.

- 1) Go to **Device** → **Select the device** → **Authentication Tab** → **Card ID Format**.
- 2) You will find the smart card format layout menu. Select the layout that you want to apply.

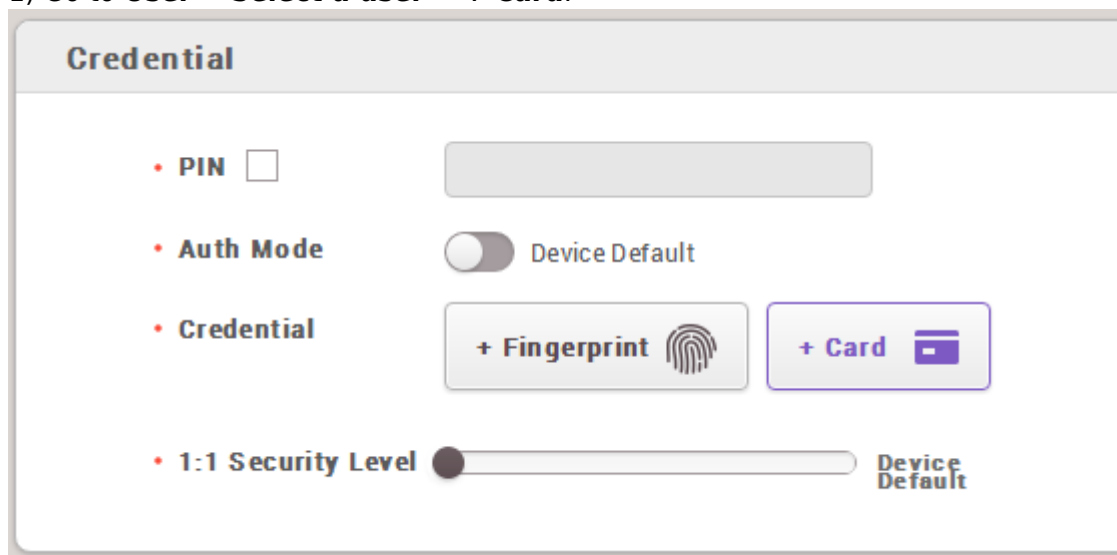


The screenshot shows the 'Card ID Format' configuration window. It has a title bar 'Card ID Format'. Inside, there are two settings: 'Format Type' with a toggle switch set to 'Normal', and 'Layout' with a dropdown menu currently showing 'None'. At the bottom of the window is a tab labeled 'Advanced'.

Formatting a card

The card needs to be formatted before being used as a smart card. The card information stored in the blocks will be deleted.

- 1) Go to **User** → **Select a user** → **+ Card**.



The screenshot shows the 'Credential' configuration window. It has a title bar 'Credential'. Inside, there are four settings: 'PIN' with an empty input field; 'Auth Mode' with a toggle switch set to 'Device Default'; 'Credential' with two buttons: '+ Fingerprint' (with a fingerprint icon) and '+ Card' (with a card icon); and '1:1 Security Level' with a slider set to 'Device Default'.

- 2) Select **Read Card** from the **Card Type** menu.

Enroll Card

• Card Type

Read Card

• Card Layout Format

• Device

None

• Smart Card Type

None

Information

• Card ID

• Access Group

• Fingerprint

1st Finger

Duress

2st Finger

Duress

• PIN

• Period

Format Card

Read Card

Cancel

3) Select the device to format the card.

4) Click **Format Card** and place the card on the device. If the format is successfully done, you will hear a sound from the device.

Issuing a smart card

1) From the same screen, please change the **Card Type** to **Enroll Smart Card**.

Enroll Card

• Card Type

Enroll Smart Card

• Card Layout Format

• Device

None

• Smart Card Type

Secure Credential Card

Information

• Card ID

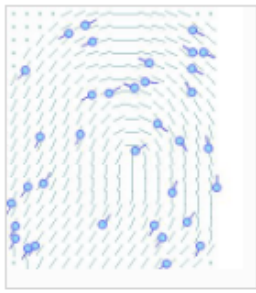
2

• PIN

• Fingerprint

1st

1st Finger



☐ Duress

Write Smart Card

Cancel

2) Select the device to enroll the smart card.

3) Select the smart card type. Access on Card and Secure Credential Card is supported.

3-1) The Access on Card will use the user ID same for the secure ID.

3-2) The Secure Credential Card's secure ID can be modified.

4) Select the fingerprint template to be written on the card. For example, click the **1st** button to select the 1st template to be written on the card. The template will get highlighted. A fingerprint must be added first to use the template.

Enroll Card

• Card Type

Enroll Smart Card

• Card Layout Format

• Device

None

• Smart Card Type

Secure Credential Card

Information

• Card ID

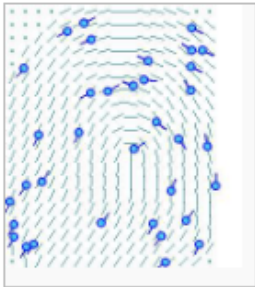
2

• PIN

• Fingerprint

1st

1st Finger



☐ Duress

Write Smart Card

Cancel

5) Click the **Write Smart Card** button.

From:
<http://kb.supremainc.com/knowledge/> -

Permanent link:
http://kb.supremainc.com/knowledge/doku.php?id=en:how_to_issue_a_smart_card&rev=1614036091

Last update: **2021/02/23 08:21**