



Access control

OPTIMA®

ONE Blue



ONE **BLUE**

Copyright: © Eden Innovations

No part of this publication may be reproduced, transmitted, transcribed or translated in any form or by any means without the consent of the copyright holder. Unauthorized copying can not only break the laws of copyright but also reduce the ability of Eden Innovations to provide accurate information.

Contents

1- Specifications.....	4
1.1 Virtual badge concept.....	4
1.2 Cost of virtual badges	5
2- Requirements for managing Premium badges.....	5
3- ONE Blue module.....	5
4- Requirements	6
4.1 Setting up Smartphone	6
4.2 Steps for improving responsiveness on readers	7
4.2.1 Badge Mode with Contact	7
4.2.2 Remote control mode on smartphone	7
4.2.3 Widget shortcut (ANDROID & IPHONE)	8
4.2.4 IWatch shortcut (IPhone only)	8
4.2.5 Payment card: why is it displayed?	8
4.2.6 List of smartphones tested by STid	8
4.2.7 STid Mobile ID account	8
4.2.8 Internet connection	9
5- Secard Configuration.....	9
5.1 Logging into the software	9
5.2 Reader configuration	9
5.3 Reader and virtual badge settings.....	11
5.4 Blue/NFC Mobile ID configuration	12
5.5 Configuring badge reading and key Configuration.....	12
5.6 Saving the pse file.....	13
6- STid mobile ID portal configuration.....	14
6.1 STid Mobile ID account	14
6.2 Creation of the site	14
6.3 Configuration of readers.....	15
6.4 Card layout	17
6.5 Generation of API parameters	17
6.6 Configuring readers for ONE Blue	18

6.7 Email personalization.....	19
6.8 Configuring OPTIMA for ONE Blue	20
7- Operation	21
7.1 Access virtual card	21
7.2 Premium card	22
7.3 Delete virtual badge	24
7.4 Revocation.....	25
7.5 Status update	26
8- Display credits.....	26
9- STid Mobile ID API configuration.....	27

1- Specifications

The ONE Blue module allows you to synchronize the OPTIMA data with the STid Mobile ID account.

Features:

- Compatible with proximity readers, U&Z and wireless electronic handles
- Management of green virtual badge (**Access card**), blue virtual badges (**Premium card**)
- Transmission of access virtual badges to smartphones

This module allows you to:

- Associate existing users of your choice with STid Mobile Id virtual badges
- Revoke/ Delete Premium cards
- Find out the current number of credits

1.1 Virtual badge concept

A virtual badge enables the dematerialization of your access control badges within a mobile application. Your virtual badge carries an identifier and behaves like an RFID badge.

The virtual badge is associated with a single device. STid offers 2 types of access badges adapted to your need:

Access card:

- Available directly in the STid Mobile ID smartphone app
- Standard configuration, no third-party software/portal required
- No internet connection required for OPTIMA
- Badge number is provided by the app
- Contact mode only
- Remote deletion is not possible

Premium card:

- Available via email activation in the STid Mobile ID smartphone app
- Pre-configured "Eden Innovations" or custom configuration
- Third-party software if custom configuration is used
- Access to the STid mobile portal ID is required for configuration
- Internet connection required for OPTIMA
- Badge number is managed by OPTIMA
- Various identification methods available
- Remote deletion is possible

Note: The reader prioritizes the recognition of the Premium badge if it is configured with the expected properties.

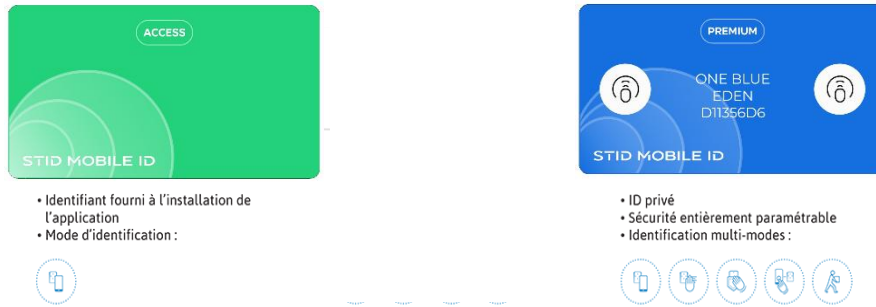


Fig. 1 : Types of virtual badges.

1.2 Cost of virtual badges

The virtual badges used have the following cost:

- Green badge (**Access**): free
- Blue badge (**Premium**): 5 credits

2- Requirements for managing Premium badges

- OPTIMA version 5.3.0 minimum connected to Internet (port **9092** must be accessible for OPTIMA to connect to the STid Mobile ID virtual badge server)
- STid Mobile account
- STid configuration pse file:
 - Generic configuration by Eden Innovations
 - Custom configuration by SECard software
 - Custom configuration provided by STid
- EDEN INNOVATIONS controllers
- Readers from STid Architect® Blue products range, OPTIMA ID BLE and U&Z BLE
- Access to emails on smartphone for end users
- SECard software if custom configuration

3- ONE Blue module

Activate the ONE Blue additional module from the Configuration menu / Installation administration / Additional modules:

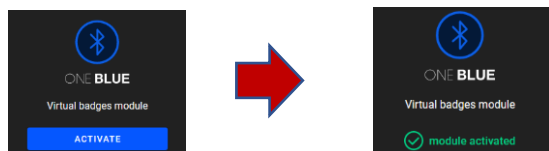
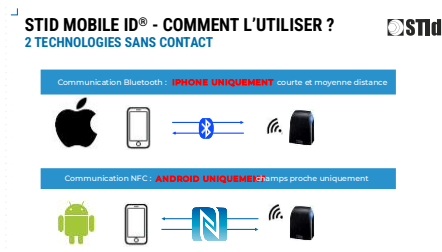


Fig. 2 : Activation of ONE Blue module.

4- Requirements

4.1 Setting up Smartphone

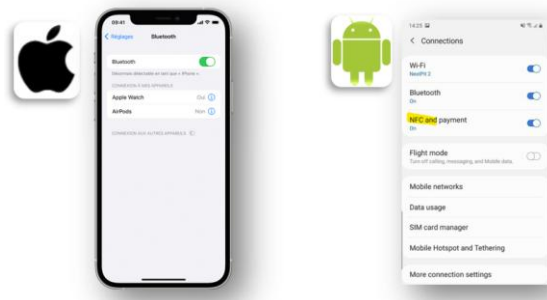
1. STid MOBILE ID Application launched
2. NFC® / Bluetooth® enabled
 - a. **NFC®** on **Android** (+ adapted + responsive)
 - b. **Bluetooth®** on **APPLE**
3. Virtuel badge created



Requirement :

IOS : **Bluetooth** activation

ANDROID : **NFC** and **Géolocalisation** activation



Why enable geolocation in Android?

STID MOBILE ID® - RÉUSSIR SON DÉPLOIEMENT

ANDROID VS IOS – PRINCIPALES DIFFÉRENCES



- v8 OREObu+
- Le mode "Badge" fonctionne en "champ proche" (NFC), permettant une authentification rapide
- L'application STid Mobile ID fonctionne même si "fermée"
- Les distances de détection du Bluetooth peuvent différer en fonction des marques et modèles de smartphone
- **L'activation de la géolocalisation est obligatoire** pour assurer le bon fonctionnement de l'app **en Bluetooth (ce comportement est imposé par Android des versions 8 à 11)**



- v12 ou+
- Le mode "Badge" fonctionne en Bluetooth, technologie couvrant une plus grande distance que le NFC, impliquant donc une authentification moins rapide
- L'application STid Mobile ID doit être ouverte pour fonctionner (sans forcément être au premier plan)

4.2 Steps for improving responsiveness on readers

4.2.1 Badge Mode with Contact

- I unlock my smartphone
- I activate my bluetooth® on IPHONE or NFC on ANDROID (before arriving at the secure point)
- I launch/see my STid Mobile ID® application as well as my badge (no need to click on the badge to select it)
- I present my smartphone to the reader (as below)



If that doesn't work:

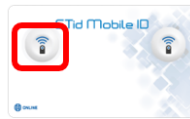
1. close the application, I relaunch it and I try again
2. close the application, I turn off Bluetooth® / NFC® and I restart, I activate NFC/BLUE and I try again
3. If still not operational I restart my phone

4.2.2 Remote control mode on smartphone

Warning: Bluetooth® must be activated and the application must be launched

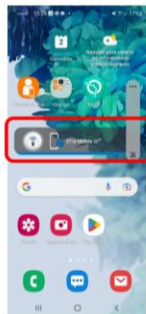
The remote control (RemoteObu+ mode) must be activated by the user – manual action

Through the STid application directly, press the left button

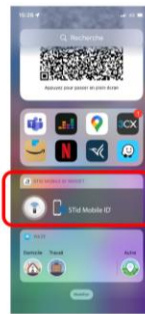


4.2.3 Widget shortcut (ANDROID & IPHONE)

Android



IPhone



4.2.4 IWatch shortcut (IPhone only)

Warning : this mode requires your iPhone connected to your watch (Bluetooth enabled)



4.2.5 Payment card: why is it displayed?

Your iPhone automatically displays your credit card when it approaches an ARCHITECT reader, which are readers operating at 13.56 MHz (same frequency as the NFC used for contactless payment).

To avoid the automatic display of your credit card on the screen of your smartphone, please launch the STid MOBILE ID application beforehand in order to make it visible in the foreground.

4.2.6 List of smartphones tested by STid

You will find below a link leading you to a document listing the smartphones tested by STid: [Tested-smartphones-list.pdf \(stid-security.com\)](https://stid-security.com/Tested-smartphones-list.pdf)

4.2.7 STid Mobile ID account

A STid Mobile ID account is required (<https://secure.stidmobile-id.com/>)

It must be activated and configured with sufficient credits to operate your virtual badges.

For more information, please consult the page <https://stid-security.com/fr/outils-support>

4.2.8 Internet connection

OPTIMA must have a permanent internet connection to interact with the STid Mobile ID server.

Port **9092** must be accessible for OPTIMA to connect to the STid Mobile ID virtual badge server.

Please check the OPTIMA's default gateway in the *Configuration/Software Administration/Network Settings menu*.

5- Secard Configuration

The following steps involve customizing the configuration of security keys and virtual badge reading by generating a PSE configuration file.

In this case, SECard software is required.

If you wish to use the generic EDEN PSE configuration file, skip directly to the STid Mobile ID Portal Configuration section.5.1 Connection to SECard software and encoder.

5.1 Logging into the software

To log in to the software in Configuration mode: log in with the Administrator login and the password STidA (default).

To log in to the software in Operation mode (Badge encoding only): log in with the User login and the password STidU (default).

5.2 Reader configuration

Go to the reader settings  and click



Then click to  Paramètres configure the reader.

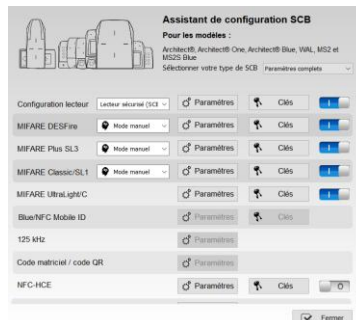


Fig. 3 : Reader settings.

Step 1 and 2:

Choose **Wiegand** or **Data/Clock (R31)**. Check the **Blue/NFC Mobile ID** box.

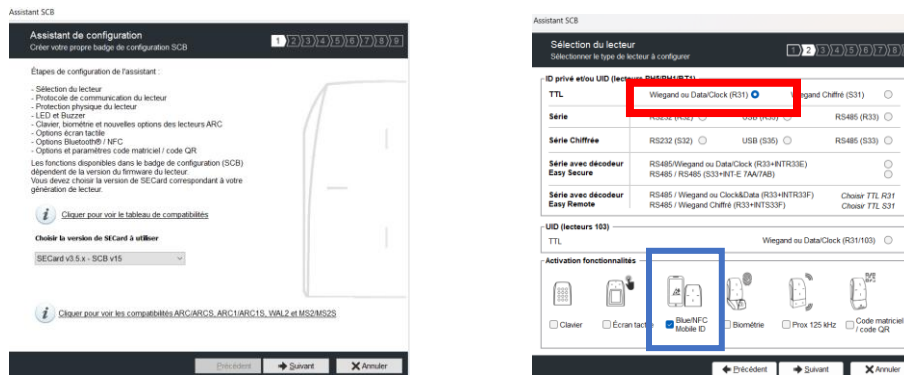


Fig. 4 : "Blue/NFC" settings.

Step 3:

Choose **Wiegand 32bits - 3La**, check the box "Save user keys in memory" (for proximity readers) and Next for all other steps.

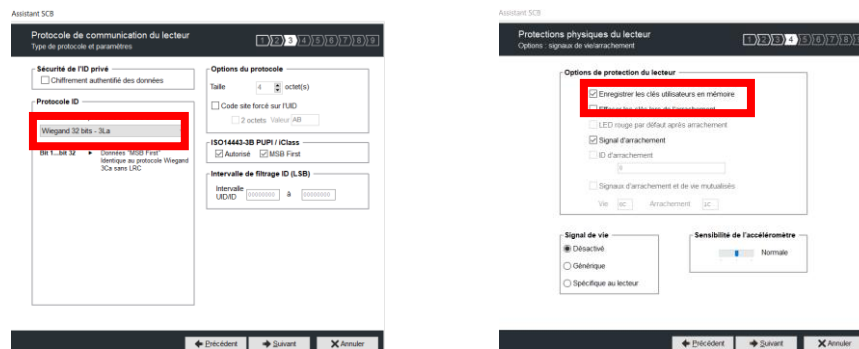


Fig. 5 : Reading settings.

Step 8: BLE settings

Enter the name of the desired configuration (in this case, EDEN) and the [Site code](#).

Check the boxes corresponding to the desired identification types:

SCB wizard

Blue/NFC Mobile ID options
Settings and Reading options

Blue mode: STid Mobile ID

Designation

Configuration Name (max 14 characters) * EDEN

Site code * 1

Identification modes and communication distances

- Card
- Hands free
- Slide/External detection
- Remote
- TapTap

Reader options

Unlocking smartphone required by the reader

NFC SAK/ATQA values adding

Back Next Cancel

Fig. 6 : Blue/NFC Mobile ID options.

5.3 Reader and virtual badge settings

Then click on the Settings button in the Blue/NFC Mobile ID section to configure the badge reading management of the virtual badge settings.

SCB wizard

Configuration wizard

For models: Architect®, Architect® One, Architect® Blue, WAL, MS2 and MS2S Blue

Select your SCB type: Full settings

Reader configuration: Secure reader (SCB) Settings Keys

MIFARE DESFire: Manual mode Settings Keys

MIFARE Plus SL3: Manual mode Settings Keys

MIFARE Classic/SL1: Manual mode Settings Keys

MIFARE UltraLight/C: Settings Keys

Blue/NFC Mobile ID: Settings Keys

Apple Wallet Access: Settings Keys

125 kHz: Settings

Matrix code / QR code: Settings

Citizen Multiservice Application (AMC): Settings

Close

SCB wizard

Blue/NFC Mobile ID

STid Mobile ID

Reader parameters

Read mode

- Private ID
- From DESFire
- Private ID else CSN

Key type

- One key (RW)
- Two keys (R and W)

Data

Size: 4

Offset: 0

Reverse:

Virtual access card parameters

Virtual access card name (max 14 characters) * ONE BLUE

Card preview

ONE BLUE
EDEN
XXXXYYZ

Settings

- ID
- Site code
- Configuration name
- Prohibit Deletion
- Remote 1
- Remote 2
- Unlock required
- Bio unlock required

Validate Cancel

Fig. 7 : Virtual badge settings.

5.4 Blue/NFC Mobile ID configuration

Click the “Keys” button in the Blue/NFC Mobile ID section to configure the key for reading virtual badges.

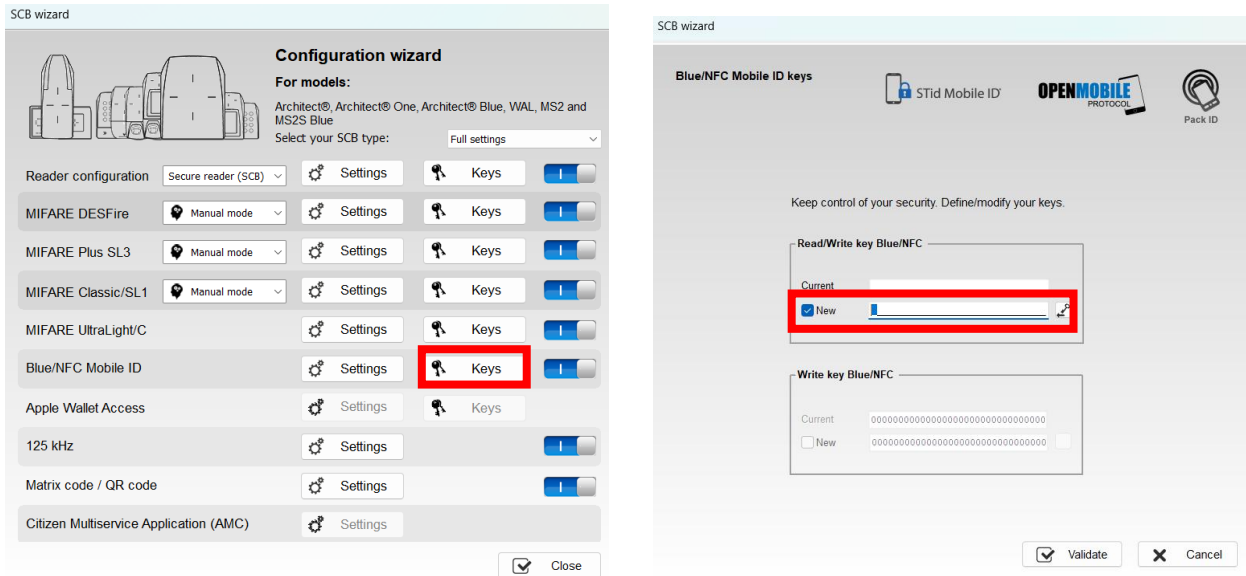


Fig. 8 : Blue NFC key.

5.5 Configuring badge reading and key Configuration

Click MIFARE DESFire *Settings*



Select the following options:

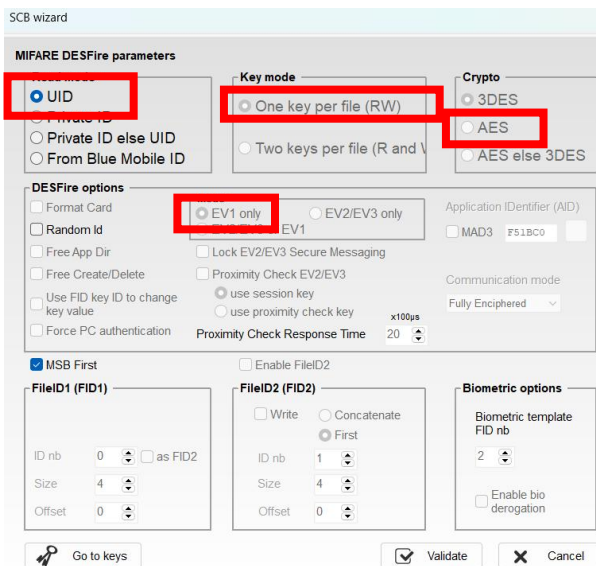



Fig. 9 : Reading settings.

Select **UID** to read the CSN number of the Mifare badge, or **Private ID** to read only the private ID (DESfire and virtual badges).

If DESFire badge reading, click on the “Go to keys”  to go directly to the 2nd “Files settings” tab to enter the keys.

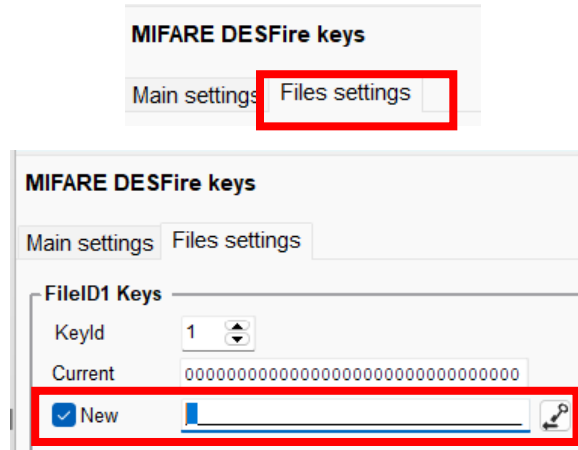


Fig. 10 : DESFire key.

Fill in the key or check the “New” box to enter a new key (use the shortcut CTRL R to generate randomly).

5.6 Saving the pse file

Go to Settings / Files to save the configuration in pse format.

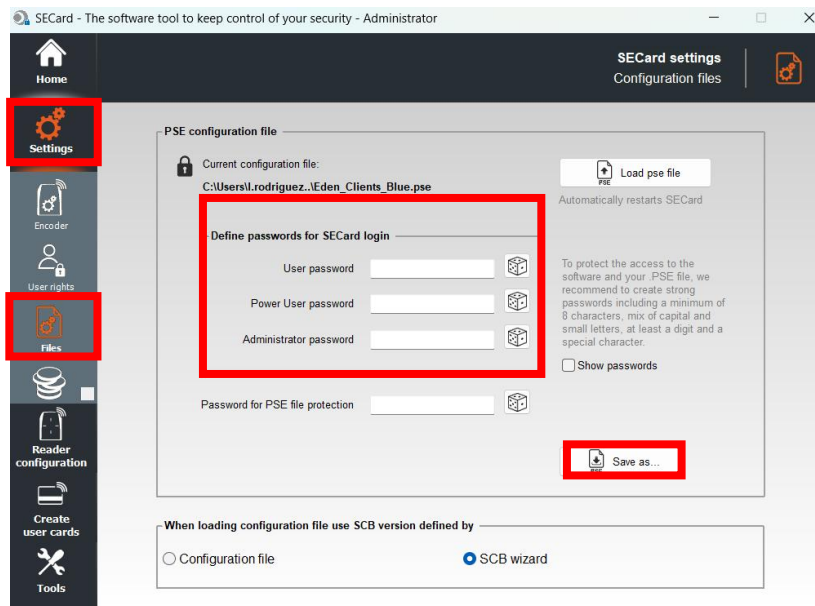


Fig. 11 : Saving the pse file.

6- STid mobile ID portal configuration

The STid mobile ID portal is required (<https://secure.stidmobile-id.com/>) for configuring blue virtual badges. It allows you to associate your configuration with your customer site by importing the PSE file.

6.1 STid Mobile ID account

It must be activated and configured with sufficient credits to use your virtual badges.

Please log in to your STid Secure ID account using the provided login and password (<https://secure.stidmobile-id.com/>) and follow these instructions:

6.2 Creation of the site

Create a site each installation using the OPTIMA ONE Blue module in order to assign them the number of credits necessary for the use of virtual badges (use credit transfer).

Go to Settings / Sites: press *Add*, fill in the fields, activate transferable mode on site's virtual cards if necessary, then validate by pressing *Add*:



Fig.12 : Creating a site.

Then go to “Access and rights” and Add, fill in the necessary fields, then press *Next*:

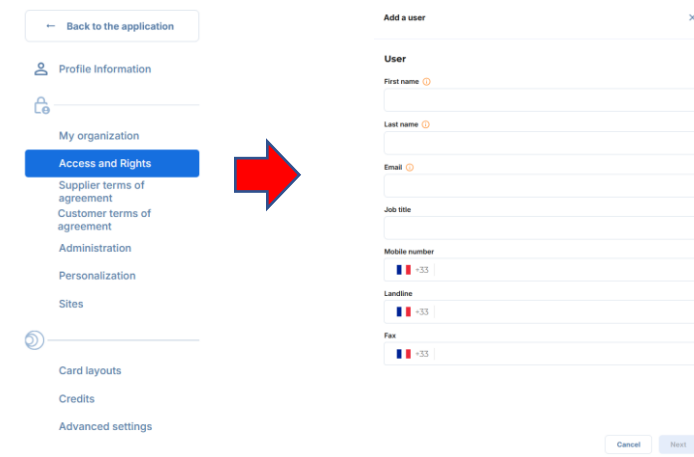


Fig.13 : Adding account.

6.3 Configuration of readers

A configuration file (pse) is required; this can be provided by:

- Custom configuration provided by STid: contact your sales department
- Custom configuration using SECard software: see the SECard Configuration chapter
- Generic Eden Innovations configuration: Eden_Clients_Blue.pse file, available below.

Configuration Name: **EDEN** with Private ID reading or CSN

Identification modes and communication distances:

- Badge: Enabled (contact)
- Slide: Disabled
- Tap Tap: Enabled (3m)
- Hands-Free: Disabled
- Remote: Enabled on button 1 (3m)

https://www.optimabox.fr/doc/produits/eden/ONE_BLUE/Eden_Clients_Blue.pse

To modify a reader already configured with Eden_Clients_Blue.pse:

Configuration name: **EDEN1** with Private ID reading otherwise CSN

Identification modes and communication distances:

- Badge: Activated (contact)
- Slide: Activated (Very close)
- Tap Tap: Activated (3m)
- Hands-free: Deactivated
- Remote: Activated on button 1 (3m)

https://www.optimabox.fr/doc/produits/eden/ONE_BLUE/Config_Eden_Clients_Blue_Update1.pse

To modify a reader already configured with Eden_Clients_Blue.pse, with hands-free mode only:

Configuration name: **EDEN2** with Private ID reading or CSN

Identification modes and communication distances:

- Badge: disabled
- Slide: disabled
- Tap Tap: disabled
- Hands-free: enabled
- Remote: disabled

https://www.optimabox.fr/doc/produits/eden/ONE_BLUE/Config_Eden_Clients_Blue_Update2.pse

To modify a reader already configured with Eden_Clients_Blue.pse, to activate all modes except "Hands-free" mode:

Configuration name: **EDEN3** with Private ID reading or CSN

Identification modes and communication distances:

- Badge: enabled
- Slide: enabled
- Tap Tap: enabled
- Hands-free: disabled
- Remote: enabled

https://www.optimabox.fr/doc/produits/eden/ONE_BLUE/Config_Eden_Clients_Blue_Update3.pse

Alternatively, use your own PSE file generated by the SECard software.

Go to Reader / Card Profiles to import the pse file.

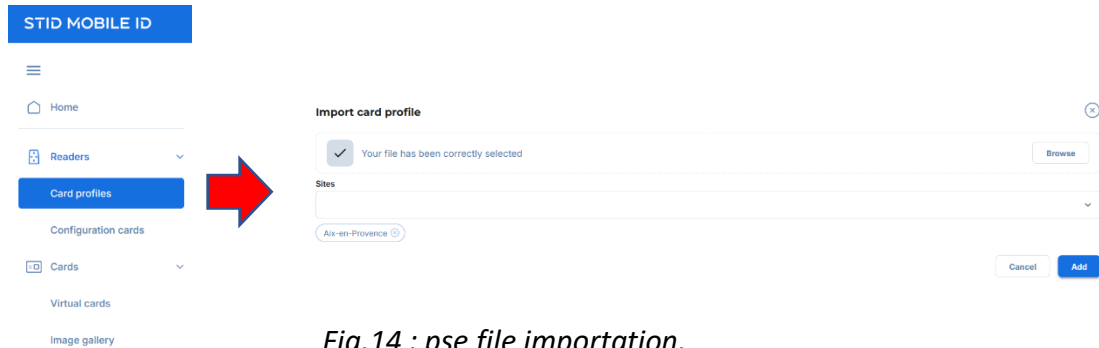


Fig.14 : pse file importation.

6.4 Card layout

Go to *Settings / Card layouts* to create the desired card layout for the front and back (optional) to personalize the virtual badge:

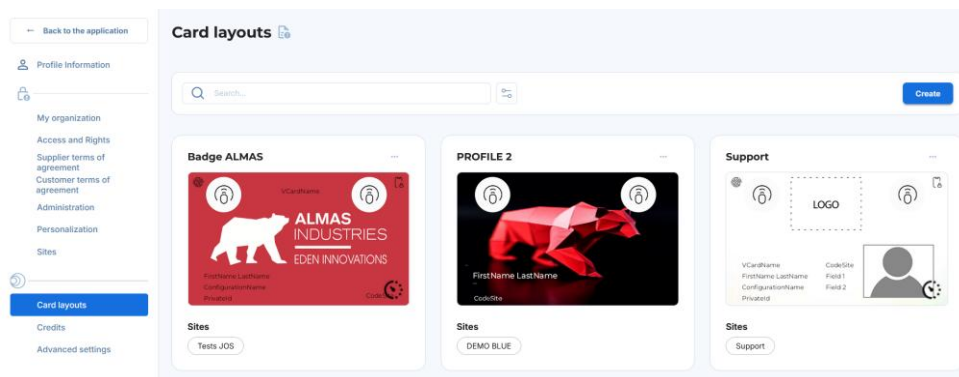


Fig. 15: Creation of card layout.

6.5 Generation of API parameters

Go to *Settings / Administration / API* to activate it, then press *Generate* the **Client secret**.

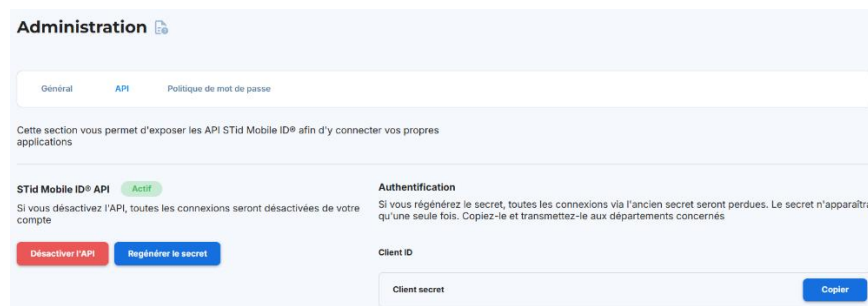


Fig. 16: API Settings.

Please copy the "Client ID" and "Client secret" identifiers which will be requested in the ONE Blue virtual badge management interface in OPTIMA (STid Mobile ID API configuration).



These identifiers must be kept because the Secret Client is permanently hidden after its creation.

For more information, please visit the page <https://stid-security.com/en/tools-support>



Connection from the OPTIMA Box to the STid Mobile ID account is not possible if configuration parameters of the STid Mobile ID portal are missing.

6.6 Configuring readers for ONE Blue

Two methods are available: by swiping a physical configuration badge to be encoded using the SECard software, or by using a smartphone with the STid Settings software.

- Physical configuration badge: Swipe the configuration badge over each reader for a few seconds until you hear a continuous beep. Reboot the reader electrically
- Virtual configuration badge:
 - Install the STid Settings application (Android or IOS).
 - Go to *readers / Card profiles*, select the appropriate configuration, select “Share” action

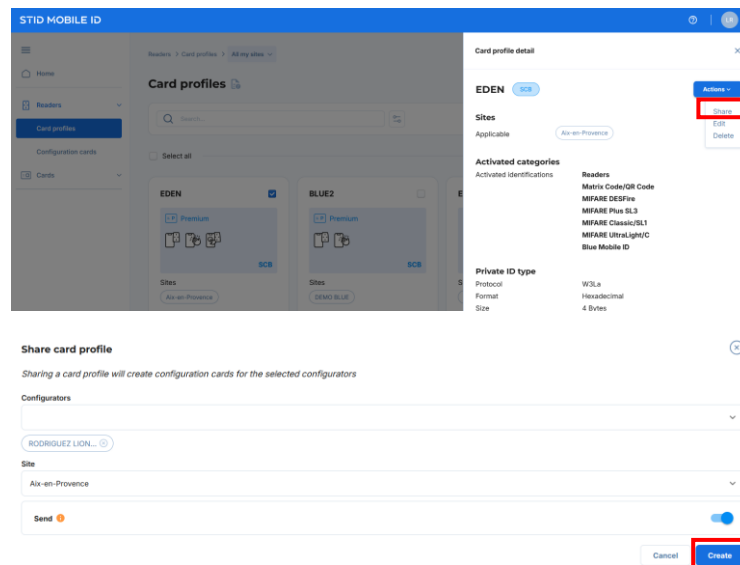
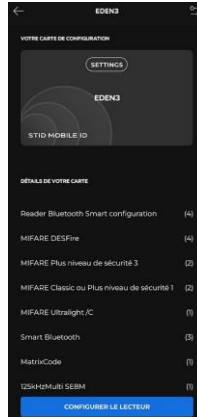


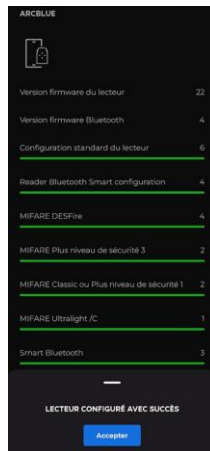
Fig. 17 : Sharing a configuration.

- Select the assigned configuration and click on the “Create” button.

- Open the email from the smartphone containing the STid Settings application and click on the newly created configuration badge
- If necessary, modify the configuration of reading modes and distances: click on “View Thresholds” at the top right



- Present the smartphone to each reader to configure them



- Restart the reader electrically

6.7 Email personalization

The content of emails sent for the following actions:

- Send Virtual card
- Virtual card revoked
- Virtual card deleted

can be customized from the *Settings/Personalization/Emails/Virtual Cards category* menu.

6.8 Configuring OPTIMA for ONE Blue

The One Blue module is available from the Operation menu / Access management / Virtual badges menu (badges management rights are required).

If no account has ever been configured, directly enter the identifiers (Client ID and Client secret) of your main administration STid Mobile Id account.

They are available from the "API Settings" tab of the STid Mobile ID Account Settings menu (<https://secure.stidmobile-id.com/Settings/Settings>)



Fig. 18 : Configuration of API identifiers.

Then choose the STid Mobile ID site to synchronize:

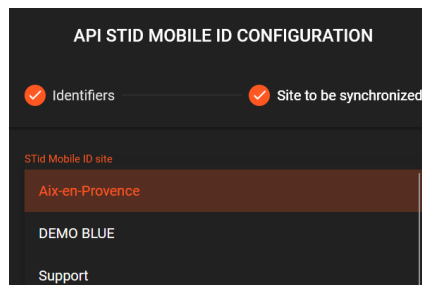


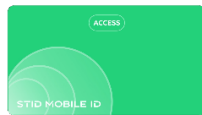
Fig. 19 : Site to synchronize.

7- Operation

In the ONE Blue interface located in the Operation / Access management / Virtual badges menu, find the list of users with their access groups, the badge number, but above all their association with a virtual badge, the type of virtual badge and their status.

VIRTUAL BADGES MANAGEMENT					
OWNER ↑	ACCESS GROUP	BADGE NUMBER	VIRTUAL	TYPE	STATUS
<input type="checkbox"/>	ALONSO Léo	8205	✔	📱	Activated
<input type="checkbox"/>	AMANI Sophia	3507705558	✘	📱	
<input type="checkbox"/>	AUDIBERT Elie	2568985594	✘	📱	
<input type="checkbox"/>	BOTARI Pedro	59587	✘	📱	
<input type="checkbox"/>	BUSCEMA Franck	8794336	✘	📱	
<input type="checkbox"/>	FERGUSON Samantha	41512	✘	📱	
<input type="checkbox"/>	TUTTLE Richard	1	✘	📱	

Fig. 20 : Virtual badges management.



7.1 Access virtual card

A badge of this type is provided automatically and free of charge when installing the STid Mobile ID application.

Ask the user to give you the ID of his badge to create the user with the corresponding ID.

Note: Having no interaction with the STid Mobile ID platform, these users appear as standard access control users (like physical badges).

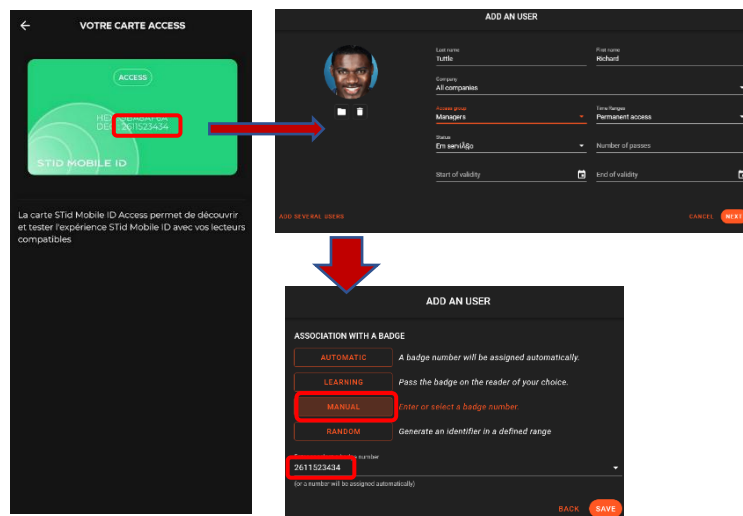


Fig. 21 : Add a user with an Access card.



7.2 Premium card

To associate a user with a new virtual badge, click on the corresponding line to enter the e-mail (mandatory), the telephone number (optional) of the person with the STid Mobile application on their smartphone.

The cost of activating a Premium card is **5 credits**. It is revocable (restitution of credits if cancellation).

Also select the Blue Mobile ID configuration and the card design.

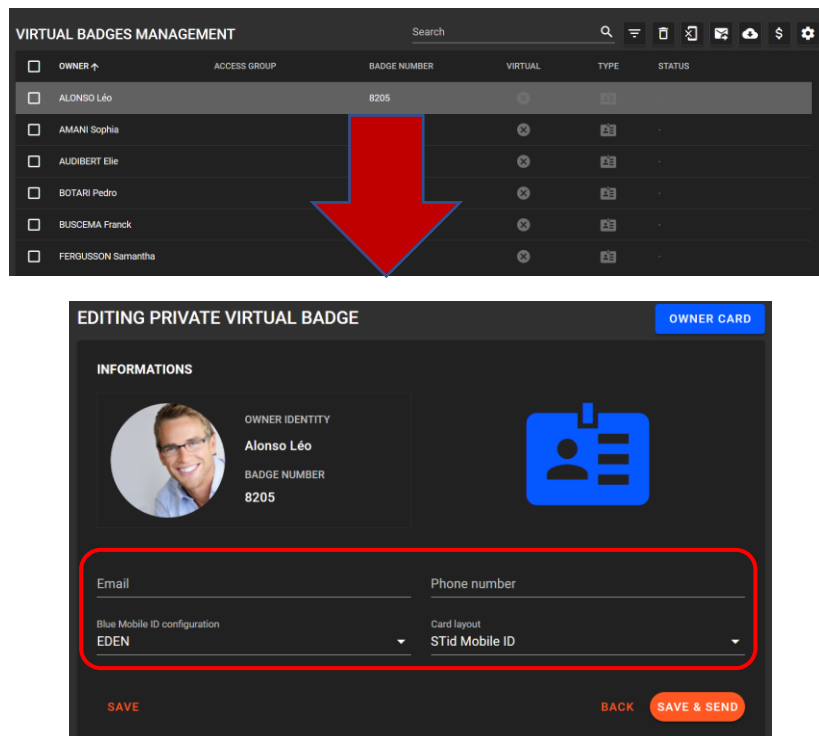


Fig. 22 : Add a blue virtual badge (Premium).

You have two options: Click the "**Save and send**" or "**Save**" button.

Save and send: An email is sent directly to the user.

The status of the virtual badge will change to "**Activation email sent**" while the user waits for the activation of the email received by the user on their smartphone.

Upon receipt of the email, the virtual badge is created by clicking on the link contained in the email received by the user.

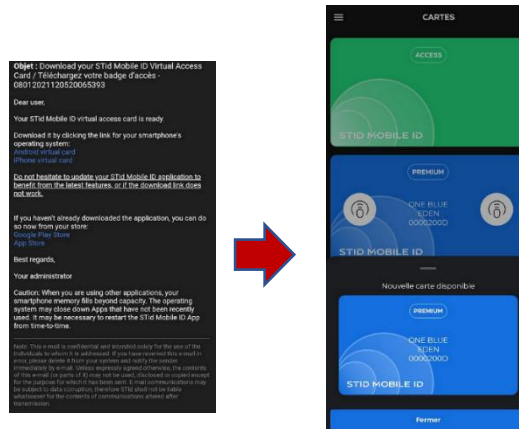


Fig. 23 : Virtual badge on user smartphone.

Save: The status of the virtual badge will change to "**Created**" while waiting for the activation of the email received by the user on their smartphone.

VIRTUAL BADGES MANAGEMENT						
OWNER	ACCESS GROUP	BADGE NUMBER	VIRTUAL	TYPE	STATUS	
<input type="checkbox"/>	ALONSO Léo		8205	<input checked="" type="checkbox"/>		Created

Fig. 24 : Creation of the blue virtual badge.

Once the users have been associated with virtual badges, select them to send confirmation emails.

OWNER	ACCESS GROUP	BADGE NUMBER	VIRTUAL	TYPE	STATUS
<input type="checkbox"/>	ALONSO Léo	8205	<input checked="" type="checkbox"/>		Activation email sent
<input type="checkbox"/>	AMANI Sophia		<input type="checkbox"/>		
<input type="checkbox"/>	AUDIBERT Elie		1		Activation emails sent
<input type="checkbox"/>	BOTARI Pedro		0		Activation sending errors
<input type="checkbox"/>	BUSCEMA Franck				
<input type="checkbox"/>	FERGUSSON Samantha				

5 credits have been reserved. They will be consumed when the badge is activated.

CLOSE

Fig. 25 : Request to send activation email.

The cost of the credit associated with the virtual badge is deducted from the activation of the virtual badge operated by the smartphone user.

OWNER	ACCESS GROUP	BADGE NUMBER	VIRTUAL	TYPE	STATUS
<input checked="" type="checkbox"/>	ALONSO Léo	8205	<input checked="" type="checkbox"/>		Activation email sent

Fig. 26 : Sending confirmation email(s).

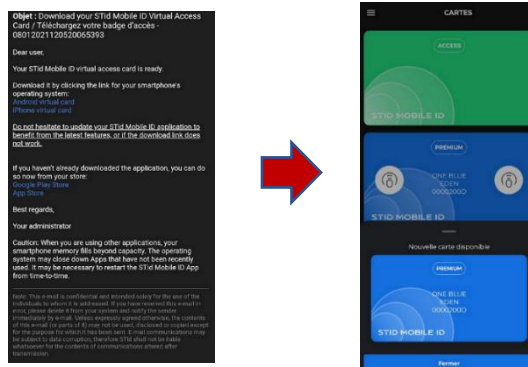


Fig. 27 : Adding the virtual badge.

Note: once the virtual badge is activated, the activation link is no longer valid (**error 404 - File or directory not found**)

7.3 Delete virtual badge

You want to delete access to a user: delete the virtual badge directly in OPTIMA.

In the event that the email address entered for the activation of the virtual badge is incorrect or any other sending problem, the ONE Blue interface may report "*Email not sent*".

In this case, or for any request to delete a virtual badge, you have the opportunity to delete the virtual badge.

If the phone is unreachable (loss, theft, Airplane mode, reset, etc.), refer to the following paragraph.

Select the virtual badge and press the button "*Trash bin*" .

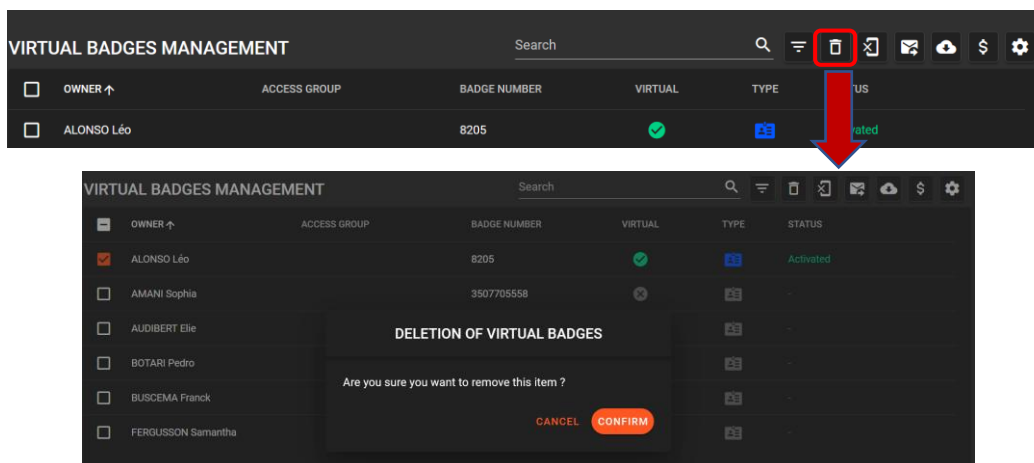



Fig. 28: Removal of virtual badge.

7.4 Revocation

If the phone is unreachable (loss, theft, Airplane mode, reset, etc.), revoke the virtual badge by pressing “Revocate”  after selecting it.

Then finalize its deletion by pressing the “Delete” button .

- A revoked blue virtual badge is automatically **suspended** to block its passage through access control.
- A deleted virtual badge remains in the phone if it is unreachable loss, theft, Airplane mode, reset, etc): the passage on a reader will be blocked on the access control since it is in "Suspended" state. It is advisable to generate a new badge in access control if you want to create a virtual badge for a phone that already has a deleted virtual badge.
- The time taken to remove the virtual badge depends on the connection quality of the user's smartphone.
- A blue virtual badge is revocable with restitution of the credit.
- You can no longer create a virtual badge from a revoked badge.

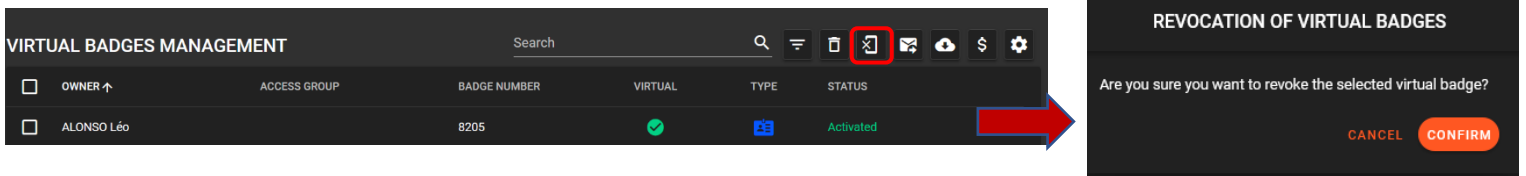


Fig. 29 : Revocation of virtual badges.

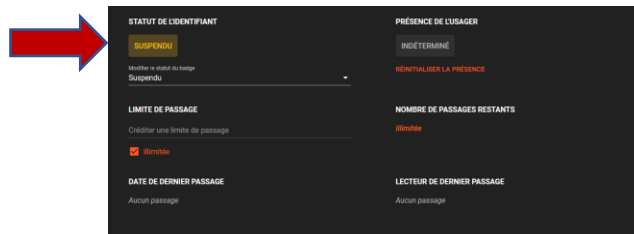



Fig. 30 : Suspended user (Premium card only).

Check revocation status by “Synchronizing STid data online”  ONE_Blue

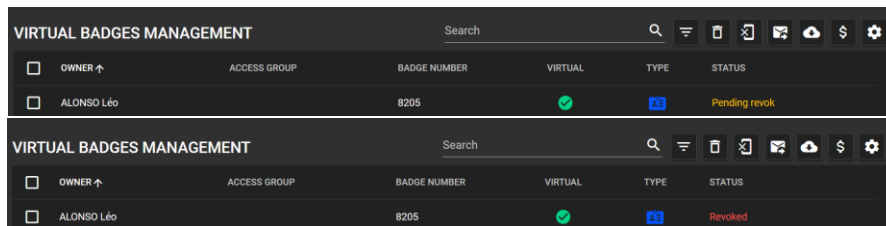


Fig. 31: User effectively revoked (depends on the state of the smartphone's network).

7.5 Status update

Updating the activation status of virtual badges is done by clicking on the button .

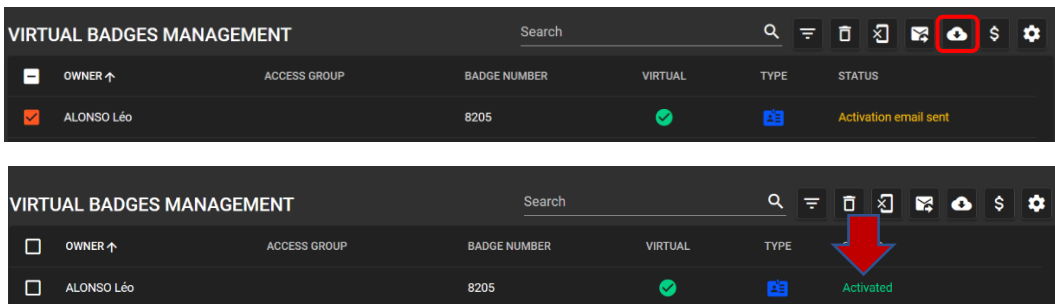


Fig. 32 : Status update: virtual badge activated (if the user opened the link in their email).

We strongly recommend that you use the data synchronization functionality of the STid server first.

It will allow you to make the virtual badges consistent with your OPTIMA database.

Indeed, in the case of shared use of the STid Mobile Id account, the users of the OPTIMA will be correlated with the existing virtual badges of the STid account.

The status of virtual badges is also updated according to the actions of users from their smartphones (activation of the virtual badge).

In the event of a conflict (presence of a virtual badge with the same number as an OPTIMA user's badge number), no modification will be made to the existing user.

For them to be synchronized, the first and last names must match.

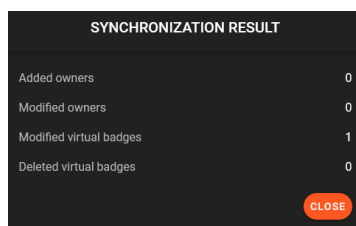


Fig. 33 : Synchronisation result.

8- Display credits

Find out the number of reserved and available credits by pressing the button "Display credits"



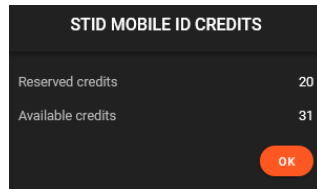



Fig.34 : Reserved and available credits.

9- STid Mobile ID API configuration

Access the configuration of the STid Mobile Id account by clicking on the "Gear"  .



Zone Commerciale et Artisanale

670, route de Berre

13510 EGUILLES

France

www.eden-innovations.com