

SGSE

Soluciones Globales de Seguridad Electrónica

WBT-AEOS ENROLL

Installer and User Manual

Content

1. Document versions	2
2. Introduction	3
3. Solution architecture.....	4
4. WBT configuration	5
Configure newly installed SPEEDFACE-Devices.....	7
5. SPEEDFACE (Facial recognition) Configuration.....	9
6. AEOS Settings	17
Enable option 44.36 in Aeos	17
Add the biometric settings to the aeos.properties file.....	17
Secure the HTTPS connection.....	18
7. Configure AEOS server for the enrollment process.....	19
Build the configuration in Aemon.....	19
Enroll the Carrier	21
8. Licensing.....	23
A. Getting a UID.....	23
B. Applying the license.....	23
9. Troubleshooting.....	24
Integrated systems	24
Required equipment.....	24
Other.....	24
More info.....	24

1. Document versions

Version	Date	Author	Changes in the version
1.0	16/12/2020	JCR	First version (English)
1.1	22/10/2020	JCR/JHC	Aeos settings, SPEEDFACE settings
1.2	22/10/2020	JCR/JHC	Aeos settings, SPEEDFACE settings
1.3	22/12/2020	JCR/JHC	Aeos settings, SPEEDFACE settings
1.4	22/01/2021	JCR/JHC	ZKteco settings

2. Introduction

The purpose of this document is to explain the operation, installation and use of the software solution called "WBT" for use Aeos biometric interface for both identification and verification user from AEOS System.

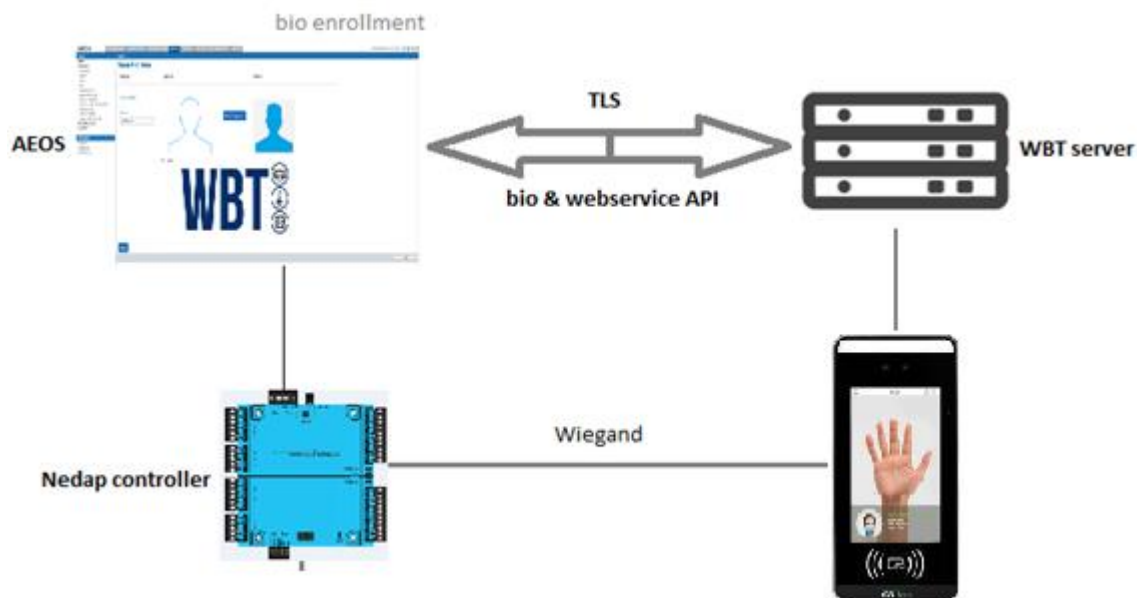
This solution consists of a web server that allows to monitor and interact with Aeos software included in the solution, from the user interface and the working environment of the Aeos platform® of [NEDAP](#).

The WBT application is designed specifically to provide the enrolment procedure from Aeos software to ZKTECO's SPEEDFACE terminals (Face recognition, Contactless, mask & Temperature) . It's the bridge between Aeos system and SPEEDFACE Biometric devices from ZKTECO.

In this way, the enrolment of a person begin in the Aeos system and ending in the SPEEDFACE devices, the software send the relevant data (card id, face,...) to SPEEDFACE terminals to permit the interaction between two systems Aeos-ZKTECO creating a unique environment system.

3. Solution architecture

The architecture of the solution is described in the scheme below:



Through the Ethernet network, the WBT service establishes communication with configured devices (SPEEDFACES).

Once the communication is established, it imports the data and keeps the communication channel open to:

- Send commands & data to the devices (enrolment features)
- CRUD (Create, read, Update, delete) data from Nedap interface over Nedap software and ZKTECO terminals.

4. WBT configuration

To check that the application has been correctly launched, please check that you can connect to the VMS server URL. In this case:

Connect to the server: <https://localhost:5001>

Log in from to the home page.

WBT Home Commissioning Eventlog Enrollment

Log in

Use a local account to log in.

Email

Password

Remember me?

[Log in](#)

[Forgot your password?](#)

[Register as a new user](#)

[Resend email confirmation](#)

Default parameters are user admin@sgse.eu and password sgse2017.

After correct log in go to Commissioning page.

License

The first time you run the software, you need to contact SGSE (sat@sgse.eu) in order to obtain a license file. You need to provide them with the number shown in your screen.

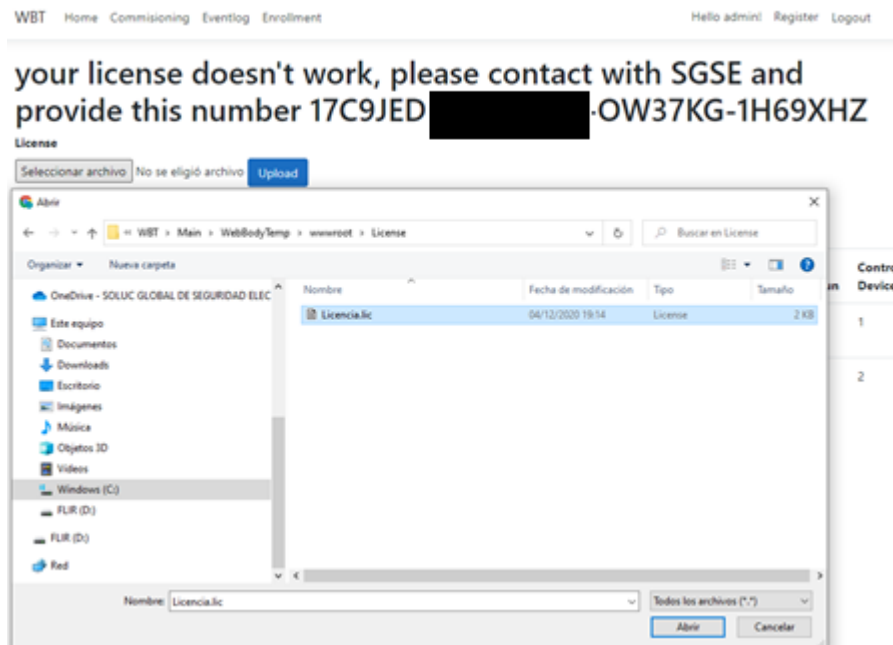
WBT Home Commissioning Eventlog Enrollment

License

[Browse license file](#) Chosen file: None [Upload](#)

your license doesn't work, please contact with SGSE and provide this number 1E0DEZT [REDACTED]-1GGFDZ3-1FR7P5L

After receiving the license, please select the path where you have the license file and select it.



You can see the selected file.

Click Upload and the licensing process is complete.

Configure the Soap Settings in the application

WBT Home Commissioning Eventlog Enrollment Hello admin! Register Logout

License
Browse license file Chosen file: None Upload

your license doesn't work, please contact with SGSE and provide this number 1E0DEZT [redacted] 1GGFDZ3-1FR7P5L

Soap Settings

Soap Server Ip:

Soap Server Port:

Aeos Soap User:

Aeos Soap User Password:

Save

Create New

Name devices	Description	idDevice	Icon	Position X	Position Y	Ip	Second Ipport	Alarm	Prealarm	Max	Min	Control Device	Active	Start Date	Aux data
BT1	TempAccess	U:25658982401FB	icono.ico	254	100	192.168.1.13		38	37,3	39,8	34	1	<input checked="" type="checkbox"/>	10/04/2020 11:11:00	38,5 Edit Delete
BT2	ZKteco device	Z:6254202900025	icono.ico	215	132	192.168.1.14	4370	39	38	40	32	2	<input checked="" type="checkbox"/>	26/11/2020 14:18:00	35,2 Edit Delete

On the commissioning page, fill in the following fields:

Soap Server IP: Soap Server IP or Soap Server Name.

Soap Server Port : Communication port. Default is 8443.

Aeos Soap User: Aeos user for the webservice connection.

Aeos Soap Password: Aeos user password for the webservice connection.

Click Save button.

Configure newly installed SPEEDFACE-Devices

Click over '**Create new**' and fill the following menu.

WBT Home Commissioning Eventlog Enrollment Hello admin! Register Logout

License

[Browse license file](#) Chosen file: None [Upload](#)

your license doesn't work, please contact with SGSE and provide this number 1E0DEZT [REDACTED] 1GGFDZ3-1FR7P5L

Soap Settings

Soap Server Ip:

Soap Server Port:

Aeos Soap User:

Aeos Soap User Password:


[Save](#)

[Create New](#)

Name devices	Description	idDevice	Icon	Position X	Position Y	Ip	Second lpport	Alarm	Prealarm	Max	Min	Control Device	Active	Start Date	Aux data
BT1	TempAccess	U:25658982401FB	icono.ico	254	100	192.168.1.13		38	37.3	39.8	34	1	<input checked="" type="checkbox"/>	10/04/2020 11:11:00	38.5 Edit Delete
BT2	ZKteco device	Z:6254202900025	icono.ico	215	132	192.168.1.14	4370	39	38	40	32	2	<input checked="" type="checkbox"/>	26/11/2020 14:18:00	35.2 Edit Delete

WBT Home Commisioning Eventlog Enrollm

Create device

name	<input type="text" value="BT2"/>	min	<input type="text"/>
description	<input type="text"/>	controldevice	<input type="text"/>
iddevice	<input type="text"/>	<input type="checkbox"/> active	
icon	<input type="text"/>	startdate	<input type="text" value="dd/mm/aaaa --:--"/> 
positionx	<input type="text"/>	aux	<input type="text"/>
positiony	<input type="text"/>	<input type="button" value="Create"/>	
ip	<input type="text"/>	Back to List	
alarm	<input type="text"/>		
prealarm	<input type="text"/>		
max	<input type="text"/>		

© 2020 - WBT - SGSE

The fields in yellow are mandatory to fill in by the installer.

Name: Write a unique name for the device.

Iddevice: Unique number to identify the terminal from the rest, you can use the mask address. **You must include the keyword Z: before the iddevice identification !**. Ex (Z:1457895456)

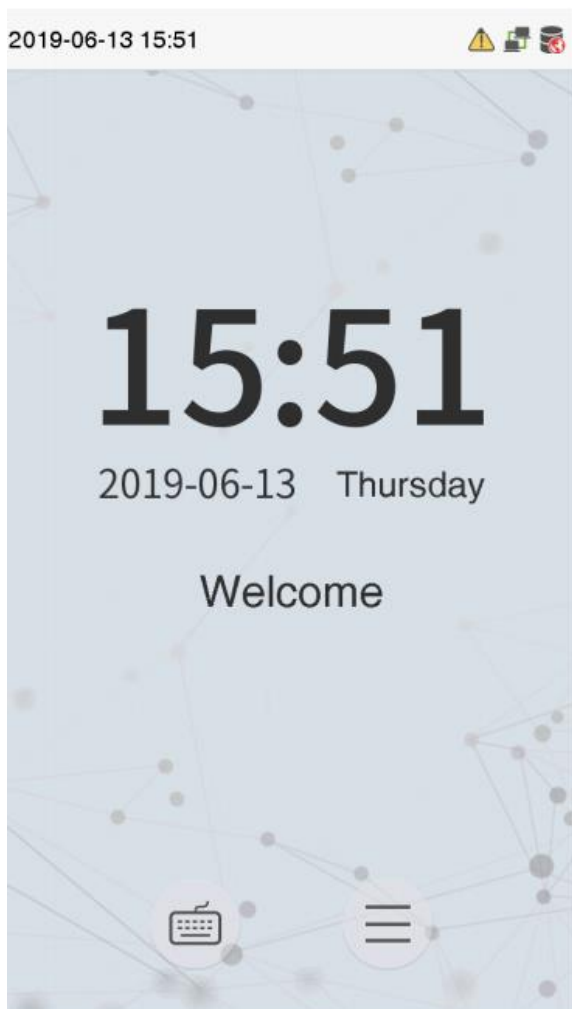
Ip: Ip address and port if the port is not 80. Ex: 172.16.25.145:8001


Active: If this field is selected the device will be included in the system.

Finally, click on create to create the device.

5. SPEEDFACE (Facial recognition) Configuration

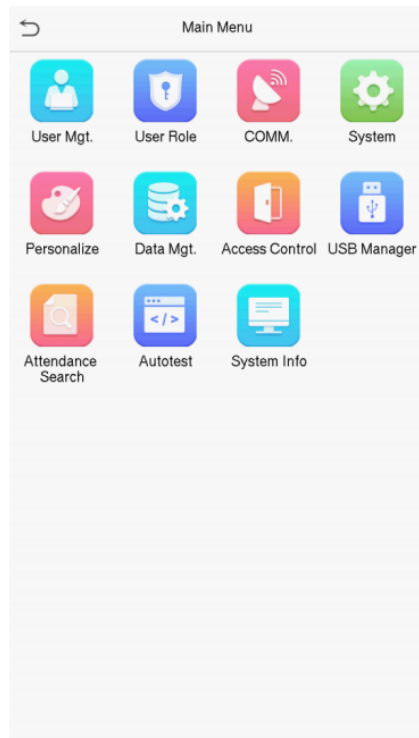
After connecting the power supply, you will see the following standby interface:



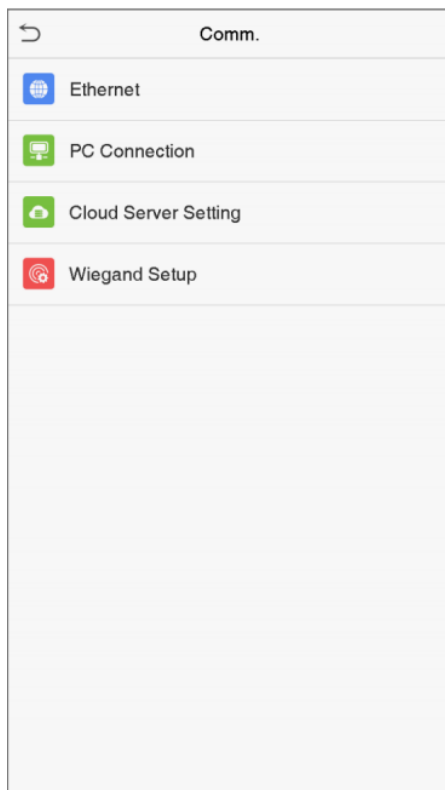
When there is no super administrator set in the device (default), click  to enter the menu.

After setting the super administrator, it requires the super administrator's verification before entering the menu operation. For the security of the device, it is recommended to register super administrator the first time you use the device.

Using the touch screen, select the initial interface and press the **Main Menu**, as shown below:



Select COMM. To set the relevant parameters of network, PC connection, cloud server and Wiegand. We need to configure Ethernet, Cloud Server Settings and Wiegand Setup.



You need to configure network settings (Ethernet, PC connection & Cloud Server) and ensure that the device and the PC are connecting to the same network segment.

1. Ethernet

Click Ethernet on the Comm. Settings interface

Ethernet	
IP Address	192.168.163.150
Subnet Mask	255.255.255.0
Gateway	192.168.163.1
DNS	0.0.0.0
TCP COMM.Port	4370
DHCP	<input type="checkbox"/>
Display in Status Bar	<input checked="" type="checkbox"/>

The default static IP address of the device is **192.168.1.201**. The device also supports simple login using the IP address of **192.168.1.201** and subnet mask of 255.255.255.0. Gateway factory default is 0.0.0.0.

Item Descriptions IP Address The factory default value is 192.168.1.201. Please adjust them according to the actual network situation.

Subnet Mask The factory default value is 255.255.255.0. Please adjust them according to the actual network situation.

Gateway The factory default address is 0.0.0.0. Please adjust them according to the actual network situation.

DNS The factory default address is 0.0.0.0. Please adjust them according to the actual network situation. TCP COMM.

Port The factory default value is 4370. Please adjust them according to the actual network situation. Critical, it's necessary to establish communication between Aeos & device.

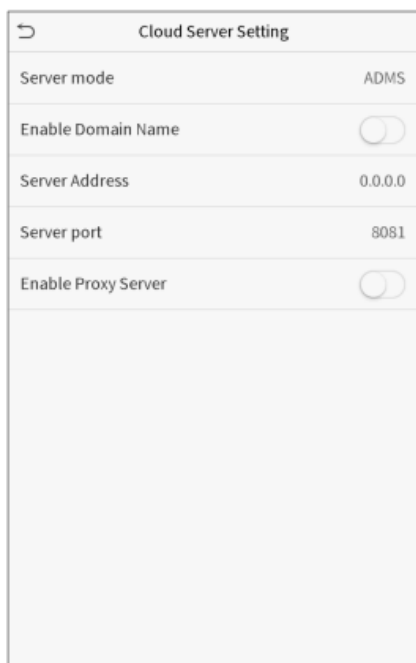
DHCP Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server.

Display in Status Bar To set whether to display the network icon on the status bar.

2. Cloud Server Setting

This represents settings used for connecting with the ADMS-WBT server. Click Cloud Server Setting on the Comm. Settings interface.

Click Cloud Server Setting on the Comm. Settings interface.



The screenshot shows a mobile application interface titled "Cloud Server Setting". It contains a list of settings:

Setting	Value
Server mode	ADMS
Enable Domain Name	<input type="checkbox"/>
Server Address	0.0.0.0
Server port	8081
Enable Proxy Server	<input type="checkbox"/>

Enable Domain Name Server Address When this function is enabled, the domain name mode "http://..." will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON.

Server Address: Please fill in the Aeos server address where the device needs to connect.

Disable Domain Name (Default) Server Address IP address of the WBT (AEO-WBT server) server. Ex. WBT service is installed in the same Aeos machine Ip address 172.16.25.85

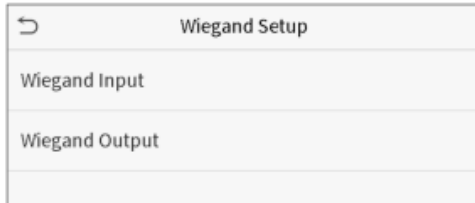
Server Port used by the WBT server (Default 8081)

Enable Proxy Server when you choose to enable the proxy, you need to set the IP address and port number of the proxy server.

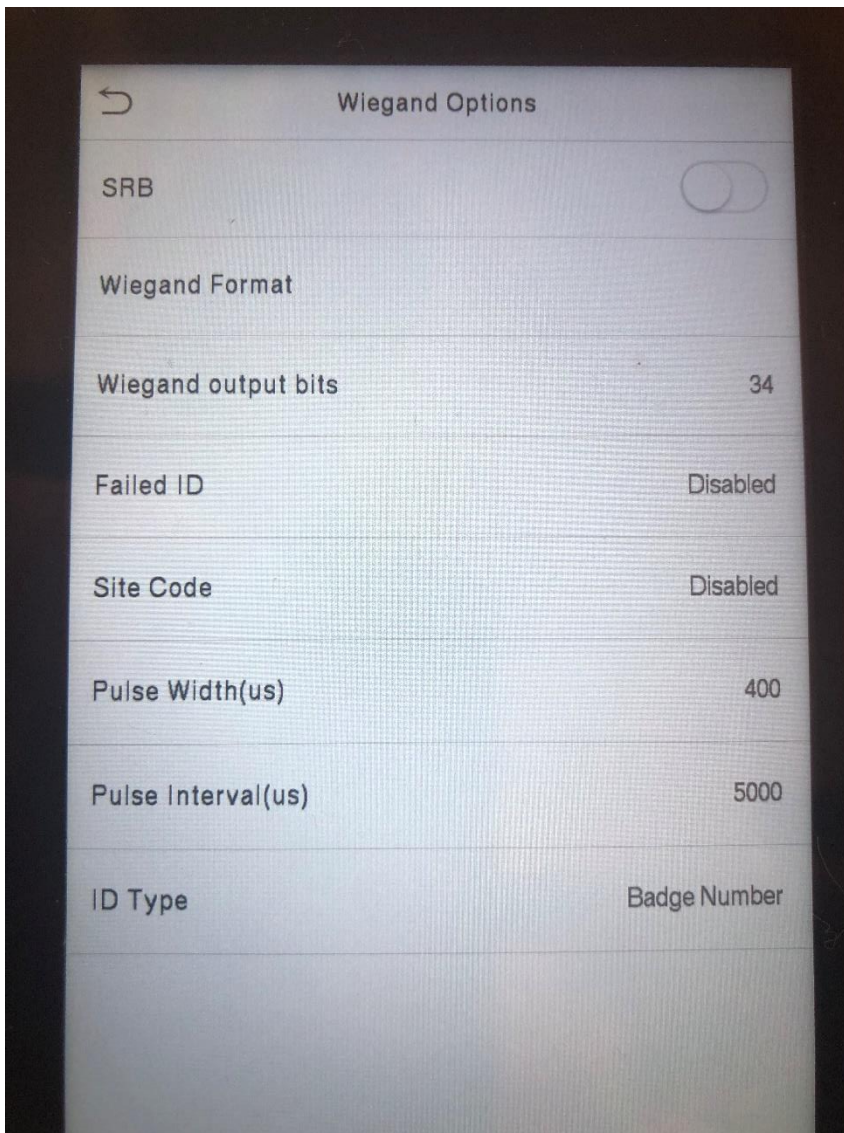
3. Wiegand Setup

To set the Wiegand input and output parameters.

Click Wiegand Setup on the Comm. Settings interface and click Wiegand Output



Select the wiegand format you are going to use. With this integration we use 34 wiegand output. It is very important to select the **ID Type** field as badge number.



You only need to change the values from the Wiegand format to 34 bits, in the "Wiegand outputs bits" menu!

Wiegand Format Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits.

Wiegand output bits After choosing the Wiegand format, you can select 34 bits of the corresponding output digits in the Wiegand format.

Failed ID If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new ones.

Site Code It is similar to the device ID. The difference is that a site code can be set manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default.

Pulse Width(us) The time width represents the changes of the quantity of electric charge with high-frequency capacitance regularly within a specified time.

Pulse Interval (us) The time interval between pulses.

ID Type Select between User ID and badge number.

[Create an admin user to access the devices](#)

****Before starting the enrollment process, please do the following:**

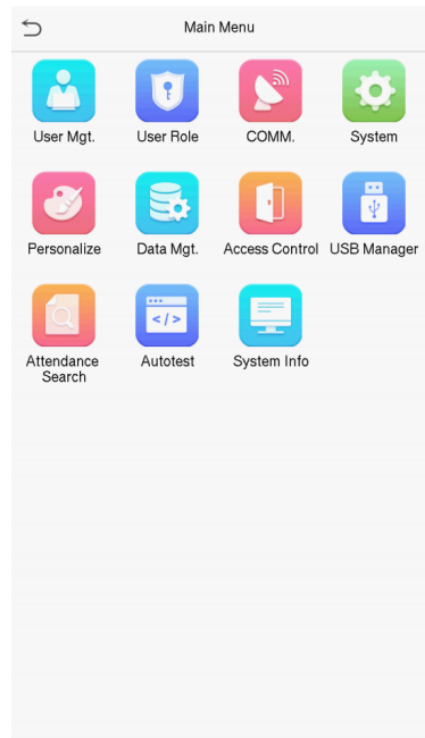
- 1.- Tap the reader screen, and click on 'User Mgt.' icon.
- 2.- Then click on 'new user'
- 3.- Edit the name of the user and select the 'Super admin' role for this user.
- 4.- You can select several verification options:
 - 4.1.- For palm or face options, you will need to present either of those to the reader.
 - 4.2.- For card number you will need to present a valid card to the reader.
 - 4.3.- If you want to use a password you will need to enter a password.

After you have finished enrolling the admin user, click on save.

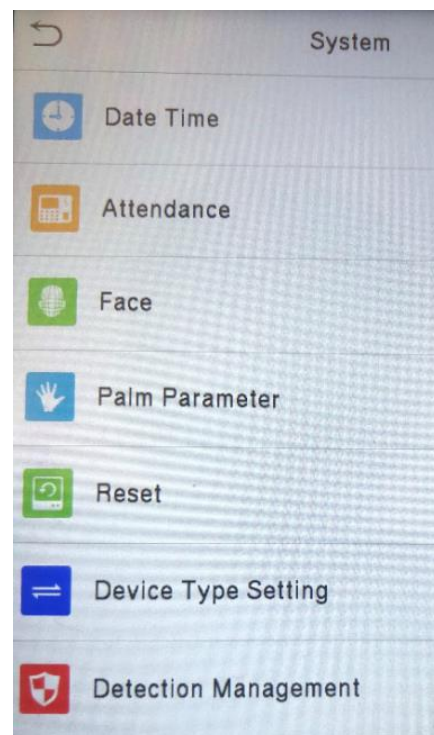
Close all windows and try the user. In the standby screen, tap on the top right corner and present your verification option. You will get access to the reader menus again.

Select mask detection (optional)

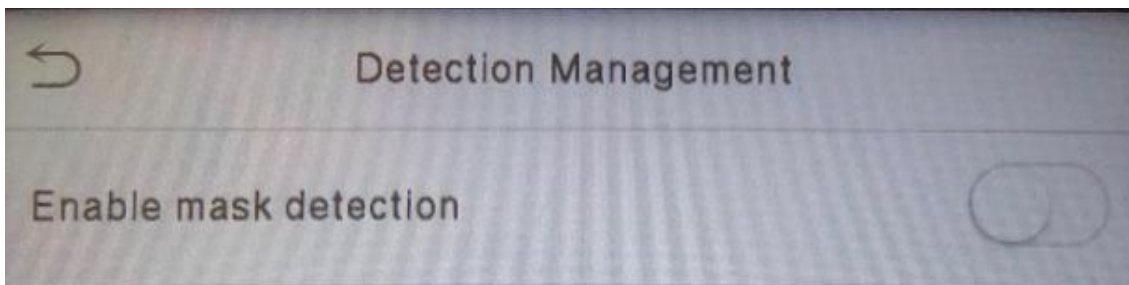
1.- Tap the reader screen, and click on 'System' icon.



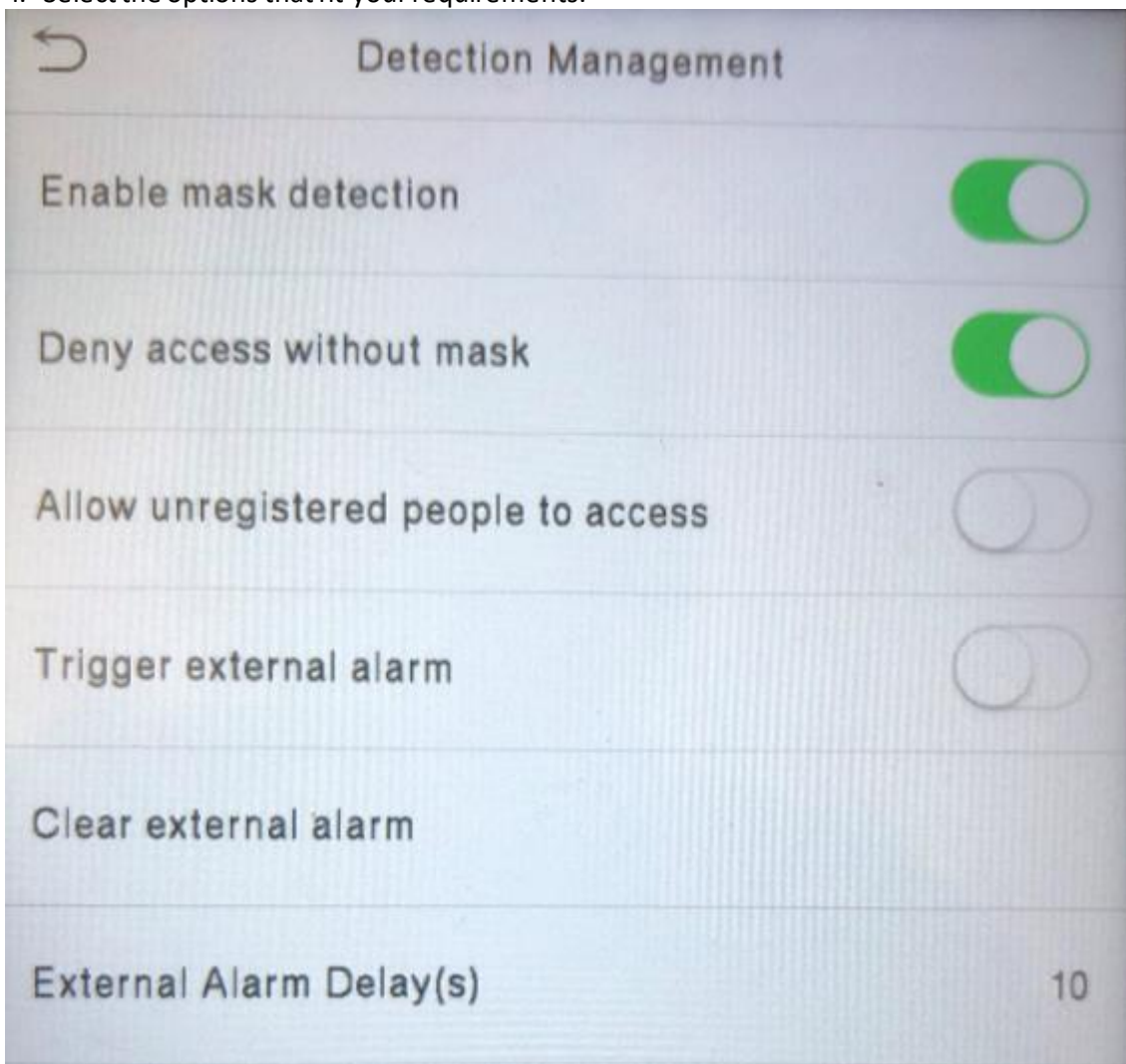
2.- Then click on 'detection management'



3.- Enable the option 'mask detection'



4.- Select the options that fit your requirements.



6. AEOS Settings

Enable option 44.36 in Aeos

Go to administration->maintenance->system properties-> Enable Biometric API

44.36	Enable biometric API	<input checked="" type="checkbox"/>
-------	----------------------	-------------------------------------

Add the biometric settings to the aeos.properties file

1. Browse to the ...\\AEOS\\AEserver\\jboss\\standalone\\configuration folder
2. Open the aeos.properties file.
3. Add the biometric settings to the file.

Below you find the configuration example:

Example settings:

```
#bioapi.settings.server.bms0.name=Test0
#bioapi.settings.server.bms0.uri=http://testserver0:844/bms/
bioapi.settings.server.bms1.name=Facial_Recognition
bioapi.settings.server.bms1.uri=https://localhost:5001/
#bioapi.settings.server.bms1.api.service.username=admin
#bioapi.settings.server.bms1.api.service.password=password
#bioapi.settings.server.bms1.optional.carrierName=false
bioapi.settings.server.bms1.optional.cards=false
bioapi.settings.server.bms1.optional.PIN=false
bioapi.settings.server.bms1.Content-Security-Policy=default-src 'self' https://localhost:5001
bioapi.settings.server.bms1.optional.carrierName=true
```

```
# Example settings:
#bioapi.settings.server.bms0.name=Test0
#bioapi.settings.server.bms0.uri=http://testserver0:844/bms/
bioapi.settings.server.bms1.name=Facial_Recognition
bioapi.settings.server.bms1.uri=https://localhost:5001/
#bioapi.settings.server.bms1.api.service.username=admin
#bioapi.settings.server.bms1.api.service.password=password
#bioapi.settings.server.bms1.optional.carrierName=false
bioapi.settings.server.bms1.optional.cards=false
bioapi.settings.server.bms1.optional.PIN=false
bioapi.settings.server.bms1.Content-Security-Policy=default-src 'self' https://localhost:5001
bioapi.settings.server.bms1.optional.carrierName=true
```

Please, note that no blank spaces must be left after each line!

The yellow fields are mandatory fields to edit by the installer.

Also note that the name configured in the line below will be the name of the identifier created in AEOS.

```
bioapi.settings.server.bms1.name=Facial_Recognition
```

'Send cards' option

Optionally, AEOS can send card numbers to the biometric management system server when it enrolls carriers. Note that when cards are used for identification and biometric data are used for verification, and the biometric reader reads both cards and biometric data, the card option must be enabled (i.e. set to 'true'):

```
bioapi.settings.server.bms1.optional.cards=true
```

Content security policy

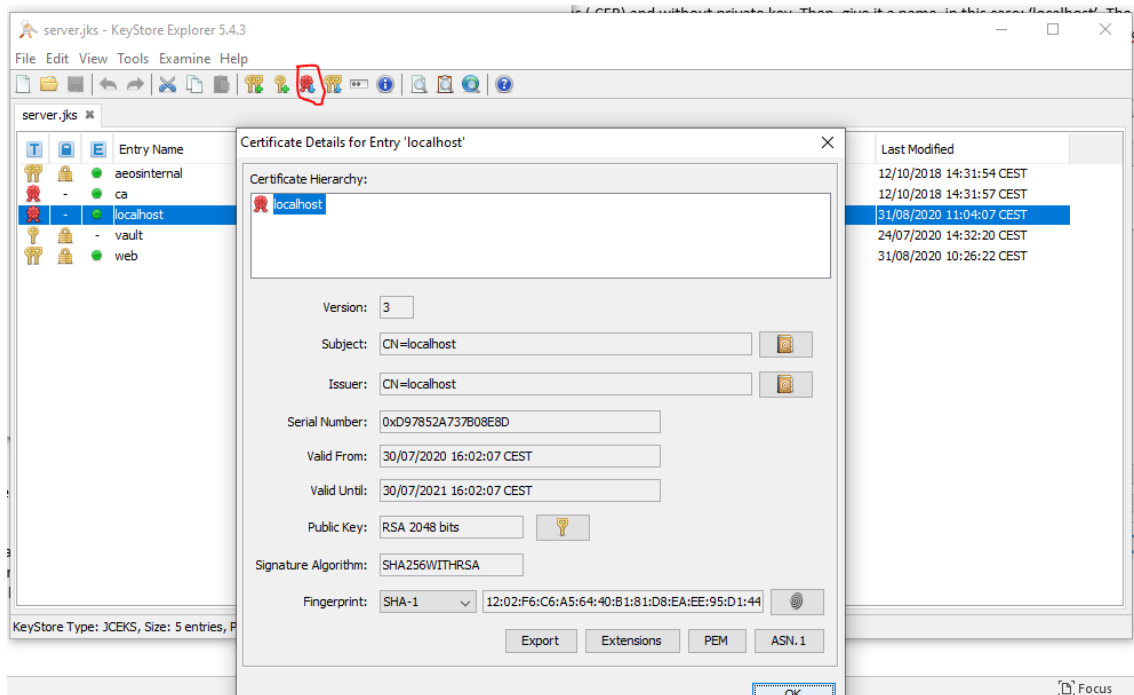
Browsers apply a strict security check. This means that to be able to load the enrollment page in the AEOS server software, you must add the content security policy to the browser where the AEOS server software is loaded. Depending on the implementation, the exact field that needs to be added here may be different. The required fields can be checked in the browser's developers console window. Please note that the IP address (or host name) must match the name in the signed certificate.

4. Save and close the the aeos.properties file.

Secure the HTTPS connection

To secure the HTTPS connection, import the certificate file (.crt) into the AEOS server keystore as (.CER) and without private key. Then, give it a name, in this case: 'localhost'. The AEOS server keystore is located at ... \AEOS\AEServer\jboss\standalone\certs, in the server.jks file. Use the red icon to import the certificate.

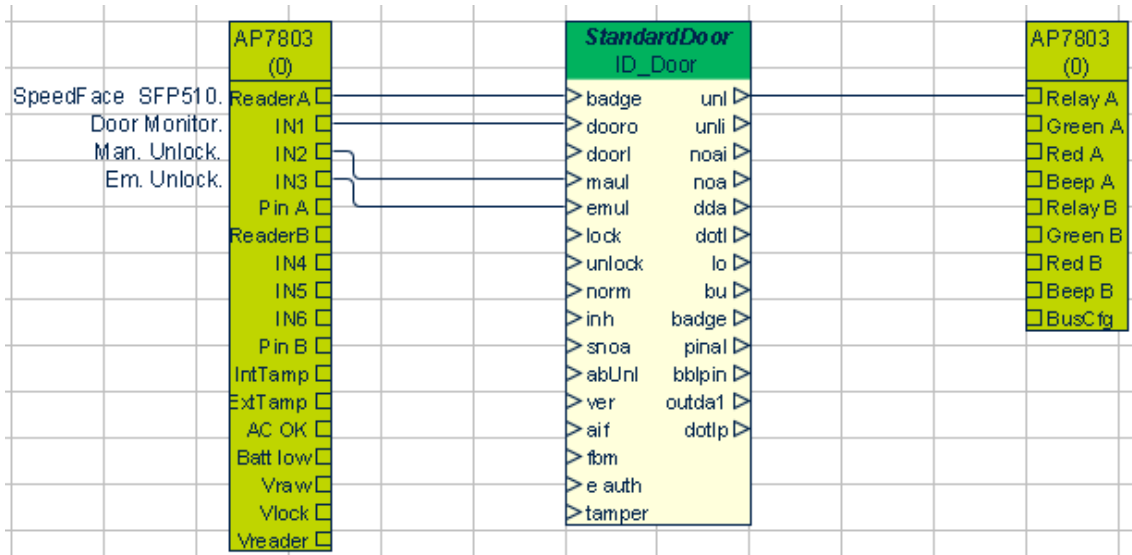
For more information on exporting and importing AEOS certificates, see the AEOS SSL manual.



7. Configure AEOS server for the enrollment process

Build the configuration in Aemon

Please note that this is just one possible option that you can use with this solution.



The identifier configured for the door is:

Please note that this parameters may differ depending on the identifiers you want to use.

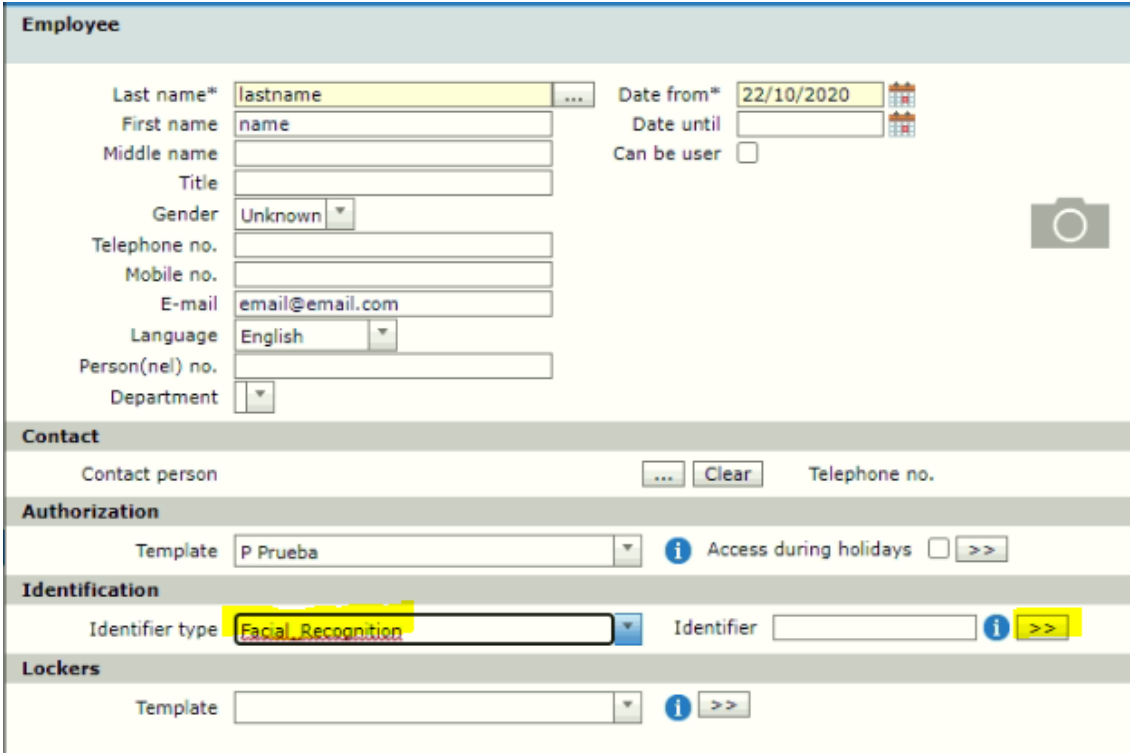
1. Right-click the AccessPoint and click Properties.
2. Open the Identifier type editor and select the identifier type as follows.
3. Click OK to save the new property settings.

Aeos Identifier:

Enroll the Carrier

The user interface to manage and issue biometric identifiers is only available in AEOS Maintenance & Configuration, not in AEOS Dashboard.

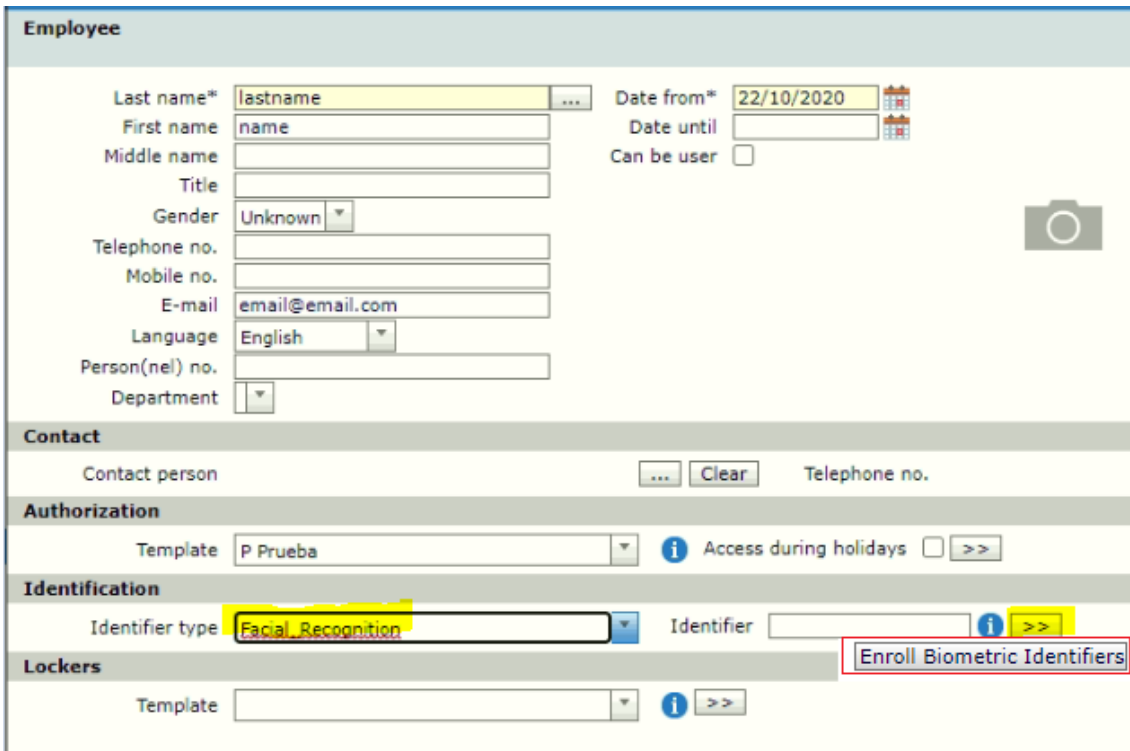
1. Go to Person > Announce.
2. Fill in the carriers data and click the [>>] button to assign the correct identifier type.
3. Select the identifier type, enter the correct id and click ok.



The screenshot displays the 'Employee' configuration form, organized into several sections:

- Employee:** Fields for Last name* (lastname), First name (name), Middle name, Title, Gender (Unknown), Telephone no., Mobile no., E-mail (email@email.com), Language (English), Person(nel) no., and Department.
- Contact:** Fields for Contact person (with a selection button), Telephone no., and a Clear button.
- Authorization:** Fields for Template (P Prueba), Access during holidays (checkbox), and a >> button.
- Identification:** Fields for Identifier type (Facial_Recognition), Identifier (with an info icon and a yellow >> button), and a selection button.
- Lockers:** Fields for Template and a >> button.

- 4.- After that you will have available the enroll button.



Employee

Last name* lastname Date from* 22/10/2020
 First name name Date until
 Middle name
 Title
 Gender Unknown
 Telephone no.
 Mobile no.
 E-mail email@email.com
 Language English
 Person(nel) no.
 Department

Contact

Contact person Telephone no.

Authorization

Template P Prueba Access during holidays

Identification

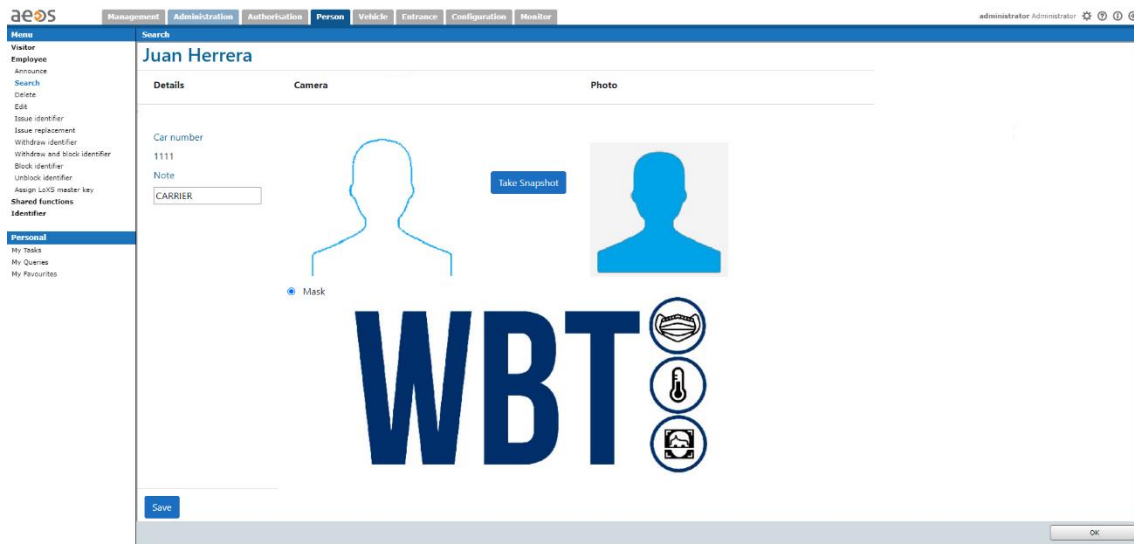
Identifier type Facial Recognition Identifier Enroll Biometric Identifiers

Lockers

Template

5.- Click on it to start the enrollment process.

6.- You will be taken to the enrollment application. (Image may differ due to upgrades in the app)



7. Take the snapshot to enroll your facial biometric data and click on Save.

8. Click Ok to go back to Aeos announce person menu.

9. Click Ok to finish the process.

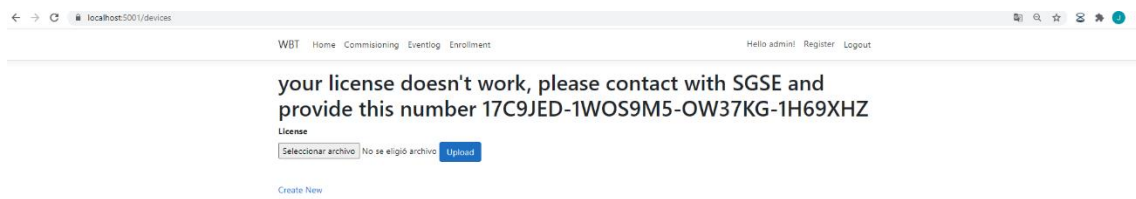
8. Licensing

The WBT needs a license to run. Each WBT must be licensed. These licenses are generated by SGSE. Every license means a device that can be configured in the application. The procedure to obtain the license is described below.

A. Getting a UID

In order to generate the license, you must provide the corresponding UID. This UID is a unique identifier to which the license is bound.

In the commissioning tab, you will get a message asking for the UID.



Please provide this UID to SGSE, and you will get your license file generated.

B. Applying the license

After applying the license, WBT must be restarted so that changes take effect.

9. Troubleshooting

Integrated systems

In case the integration does not work, please confirm that all parameters and configurations are correct as described in this manual.

SPEEDFACE devices Compatibility is not granted if a different firmware version is used. Although later firmware versions should work properly, compatibility with each specific firmware version must be tested.

Required equipment

In order to communicate with the devices SPEEDFACE, Ethernet connection must be established.

Other

In case of communication failure, check SPEEDFACEs IP address .

More info

For more info, please visit [plugin online information](#) or contact SGSE in the email address info@sgse.eu.