

Suprema Integration with Nedap AEOS

SETUP GUIDE

Version 1.1.1.3
English

Contents

Target Audience	3
Introduction	4
Features	4
System diagram.....	4
Installation	5
Prerequisites.....	5
Configuration procedure	5
Install Suprema Integration with Nedap AEOS.....	6
Suprema Integration with Nedap AEOS Setup file	6
Configuration	9
Suprema Integration with Nedap AEOS.....	9
Setting device administrator	9
Applying License.....	9
Online Activation.....	9
Offline Activation	10
AEOS	11
Configure AEOS properties for Suprema Integration.....	11
Configure AEOS for Suprema Integration	12
Install certificate (Client PC).....	13
Biometric Device	14
Configure biometric device's network settings.....	14
Configure biometric device's wiegand settings	15
Biometric Credential Enrollment	17
Enroll biometric credentials.....	17
Enroll Fingerprint	18
Enroll Face.....	19
Troubleshooting	21
When Suprema Integration with Nedap AEOS web service does not work normally	21
When the device can not connected to Suprema Integration with Nedap AEOS web service.....	21
Appendices	22

Target Audience

This document describes the integration between Suprema biometric devices and Nedap AEOS using Suprema Integration with Nedap AEOS.

This document is intended for system operators as well as system administrators. The system operators/administrators require basic knowledge of the Nedap AEOS system and Suprema biometric devices.

Introduction

Features

Suprema Integration with Nedap AEOS is a programming interface that allows the Nedap AEOS platform to communicate with the Biometric Management System, which is able to generate user biometric templates with Suprema biometric devices and manages user information from the AEOS on the devices. With Suprema Integration with Nedap AEOS, you can easily setup and build the Biometric Management System for the AEOS using Suprema biometric devices.

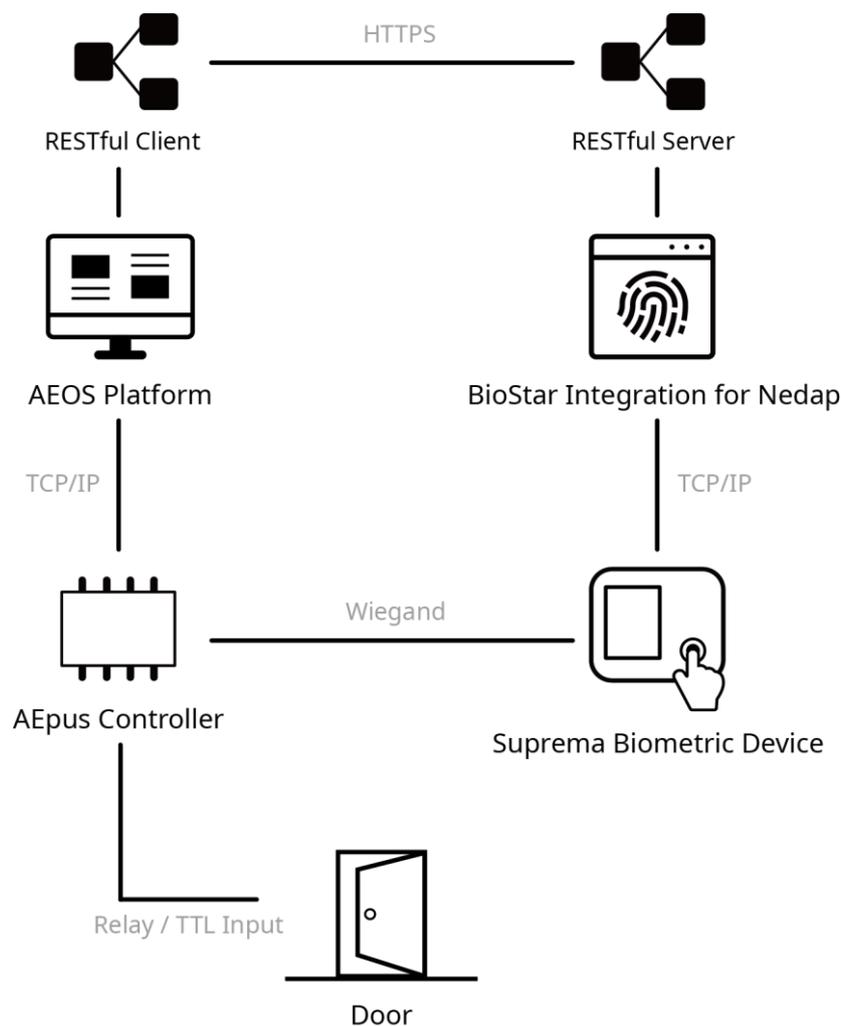
Suprema Integration with Nedap AEOS provides the following features:

- Allows to add, update, and delete users and Wiegand cards, as well as register each user's fingerprint templates.
- Offers a web page for enrolling fingerprint. It can add or delete 10 fingerprint templates for a user.
- Without installing an independent web server.
- Provides a service for user information synchronization among the devices connecting to the server of Suprema Integration with Nedap AEOS.
- Allows to connect and manage up to 1,000 Biometric Devices.

NOTE

- For more details on the functionality of AEOS platform, see the user manuals for Nedap AEOS.

System diagram



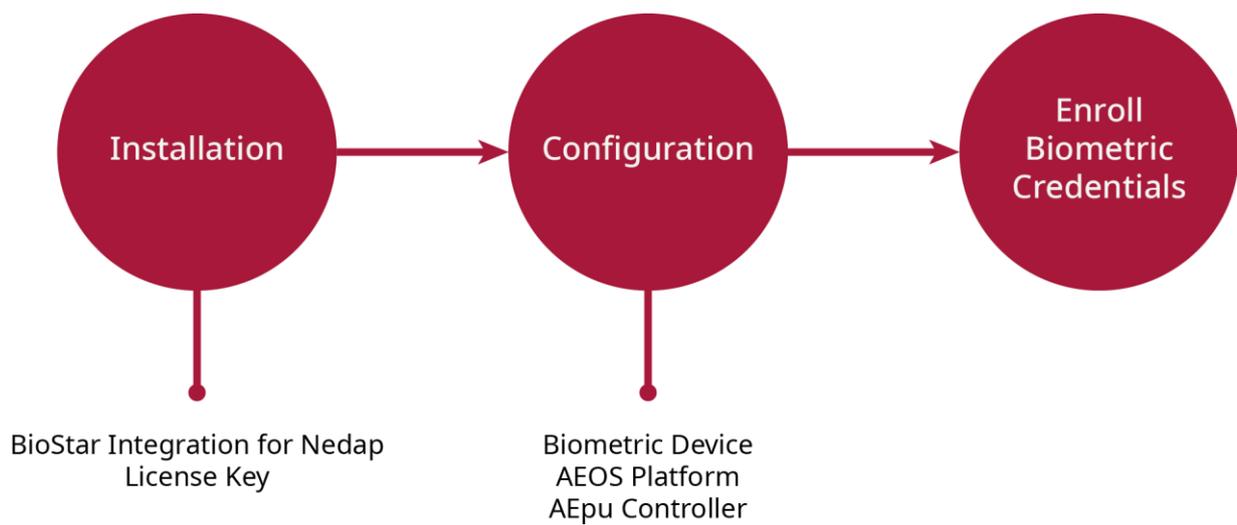
Installation

Prerequisites

The following prerequisites are required to use Suprema Integration with Nedap AEOS. Check the support conditions before installing the Suprema Integration with Nedap AEOS.

- Operating system
 - Microsoft Windows 7(x86 / x64), Microsoft Windows 10(x64)
- Web browsers
 - Chrome, New Microsoft Edge
- AEOS
 - AEOS 2020.1.1 or higher
- Biometric Device
 - BioStation 2, BioStation A2, BioStation L2, BioEntry W2, BioLite N2, XPass 2, FaceStation 2, FaceLite, FaceStation F2

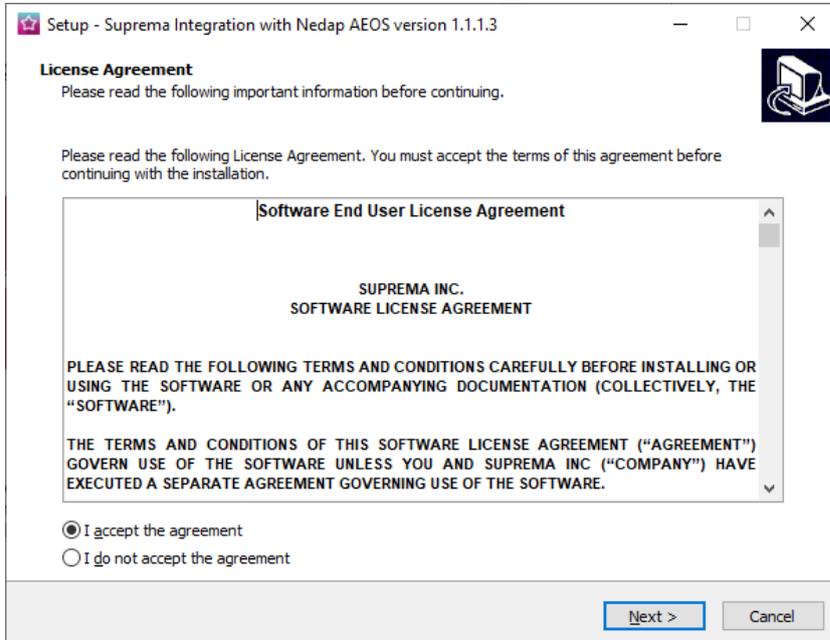
Configuration procedure



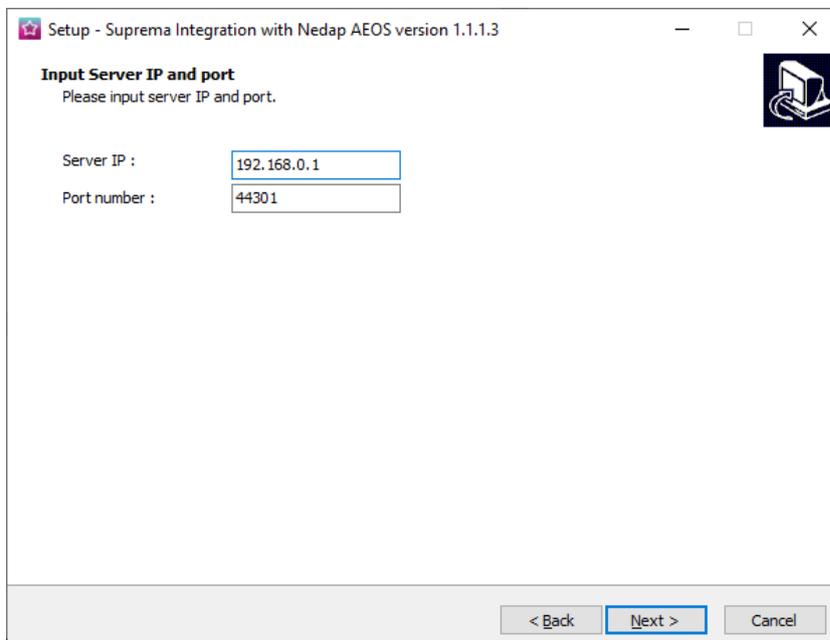
Install Suprema Integration with Nedap AEOS

Suprema Integration with Nedap AEOS Setup file

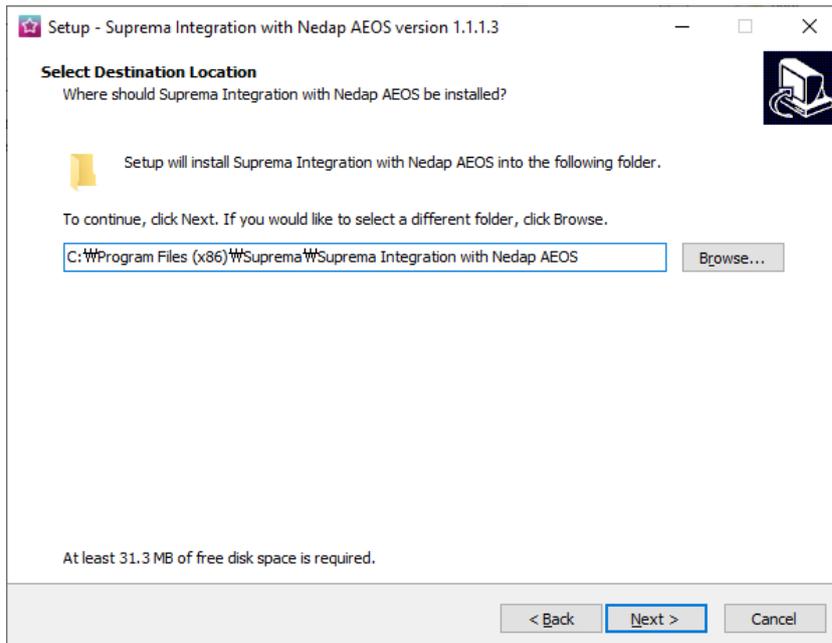
- 1 Run the Suprema Integration with Nedap AEOS 1.1.1.3 setup file.
- 2 To continue the installation, click **Next**.



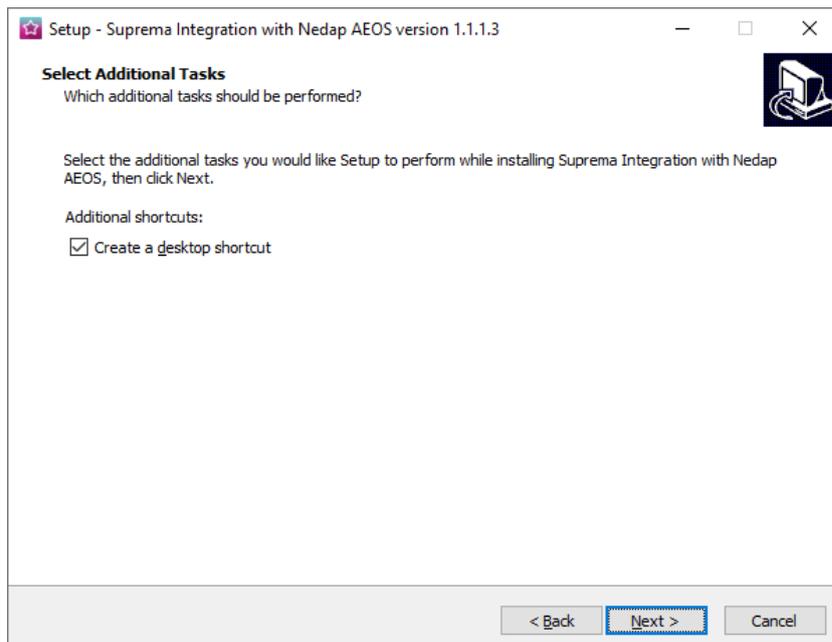
- 3 Enter the IP address of the server PC and click **Next**. The default port used is 44301.



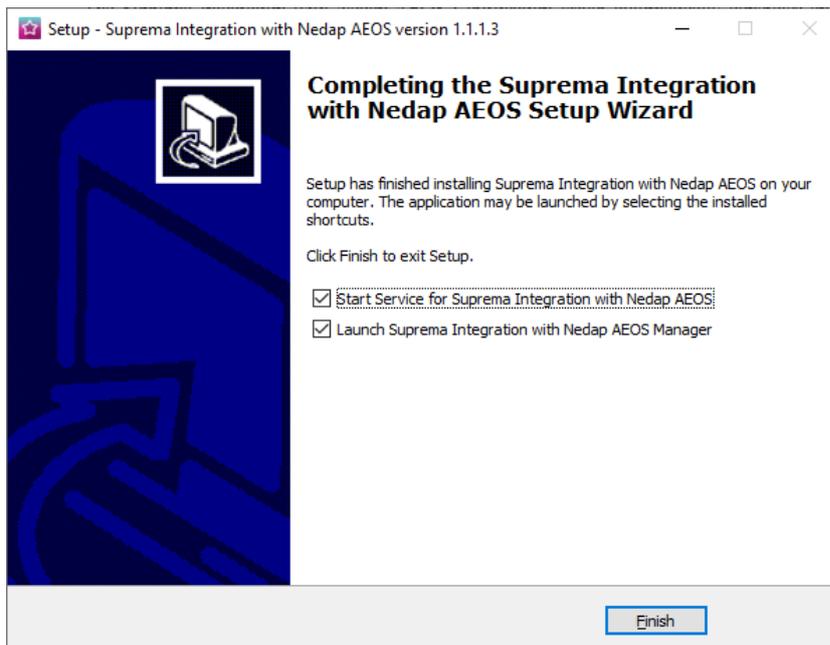
- 4 Select the installation path of the Suprema Integration with Nedap AEOS and click **Next**.



- 5 Select whether to create a desktop shortcut.



- 6 Click **Finish** to end the installation process



- 7 Click **Finish** to complete installing Suprema Integration with Nedap AEOS.

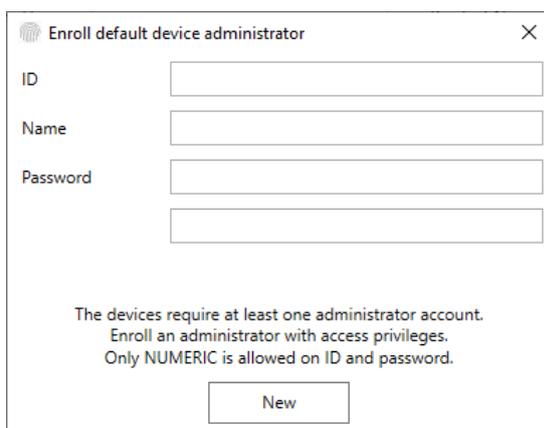
Configuration

Suprema Integration with Nedap AEOS

Setting device administrator

Suprema devices with LCD requires a device administrator to control access privilege to the device menu. The integration software will ask to create a device administrator on its first launch. Follow the instructions below to create and apply the device administrator

- 1 Launch the Suprema Integration with Nedap AEOS client.
- 2 Enter the ID, name, password of the device administrator. Only numeric is allowed on the ID and password.



Enroll default device administrator

ID

Name

Password

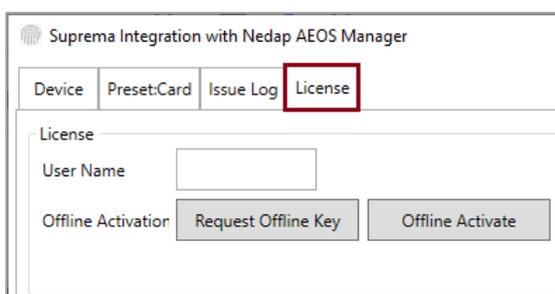
The devices require at least one administrator account.
Enroll an administrator with access privileges.
Only NUMERIC is allowed on ID and password.

Applying License

The Suprema Integration with Nedap AEOS offers a 30-day trial. After this period, a license needs to be applied. The license can be activated online and offline. If the network has restrictions on outbounds follow the steps for offline activation.

Online Activation

- 1 Launch the Suprema Integration with Nedap AEOS client.
- 2 Go to the **License** tab.



Suprema Integration with Nedap AEOS Manager

Device Preset:Card Issue Log **License**

License

User Name

Offline Activation

- 3 Enter the user name and received activation key then click **Online Activate**.

Suprema Integration with Nedap AEOS Manager

Device | Preset:Card | Issue Log | License

License

User Name Activation Key **Online Activate**

Offline Activation

Offline Activation

- 1 Launch the Suprema Integration with Nedap AEOS client.
- 2 Go to the **License** tab.

Suprema Integration with Nedap AEOS Manager

Device | Preset:Card | Issue Log | **License**

License

User Name

Offline Activation

- 3 Click **Request Offline Key** and save the request file. Send the request file to your distributor. A license file will be delivered within a few days.

Suprema Integration with Nedap AEOS Manager

Device | Preset:Card | Issue Log | License

License

User Name

Offline Activation

- 4 Click **Offline Activate** and select the license file received.

Suprema Integration with Nedap AEOS Manager

Device | Preset:Card | Issue Log | License

License

User Name

Offline Activation

AEOS

Configure AEOS properties for Suprema Integration

To launch the fingerprint enrollment page in AEOS platform, you must configure certain options in AEOS.

- 1 Open the `AEOS\WAEserver\standalone\configuration` folder.
- 2 Open `aeos.properties` file.
- 3 Set the Suprema Identifier type and the Suprema Integration web server URL as shown below. The 'serverIP' needs to be replaced to the actual IP address of the server PC.
- 4 The name of the biometric management system needs to be same with the AEOS identifier that will be used.
 - `bioapi.settings.server.bms1.id = 1`
 - `bioapi.settings.server.bms1.name = The name of the identifier from AEOS that will be used`
 - `bioapi.settings.server.bms1.uri = https://serverIP:44301/bioapi`
 - `bioapi.settings.server.bms1.optional.carrierName = true`
 - `bioapi.settings.server.bms1.optional.cards = true`
 - `bioapi.settings.server.bms1.optional.PIN = true`
 - `bioapi.settings.server.bms1.Content-Security-Policy=default-src 'self' https://serverIP:44301 https://serverIP:44301/WECClient 'unsafe-inline' 'unsafe-eval'; script-src 'self' https://serverIP:44301 https://serverIP:44301/WECClient https://serverIP:44301/bioapi/cmdfingers/scan 'unsafe-inline' 'unsafe-eval'; object-src 'self' https://serverIP:44301 https://serverIP:44301/WECClient 'unsafe-inline' 'unsafe-eval'; img-src 'self' data`

```
# Example settings:
#bioapi.settings.server.bms0.name=Test0
#bioapi.settings.server.bms0.uri=https://testserver0:8444/bms/
#bioapi.settings.server.bms1.name=Test1
#bioapi.settings.server.bms1.uri=https://testserver1:8443/bms
#bioapi.settings.server.bms1.api.service.username=myname
#bioapi.settings.server.bms1.api.service.password=mypassword
#bioapi.settings.server.bms1.optional.carrierName=true
#bioapi.settings.server.bms1.optional.cards=true
#bioapi.settings.server.bms1.optional.PIN=true

bioapi.settings.server.bms1.id=1
bioapi.settings.server.bms1.name=Suprema
bioapi.settings.server.bms1.uri=https://192.168.12.169:44301/bioapi
bioapi.settings.server.bms1.optional.carrierName=true
bioapi.settings.server.bms1.optional.cards=true
bioapi.settings.server.bms1.optional.PIN=true
bioapi.settings.server.bms1.Content-Security-Policy=default-src 'self' https://192.168.12.169:44301 https://192.168.12.169:44301/WECClient 'unsafe-inline' 'unsafe-eval';
script-src 'self' https://192.168.12.169:44301 https://192.168.12.169:44301/WECClient https://192.168.12.169:44301/bioapi/cmdfingers/scan 'unsafe-inline' 'unsafe-eval';
object-src 'self' https://192.168.12.169:44301 https://192.168.12.169:44301/WECClient 'unsafe-inline' 'unsafe-eval'; img-src 'self' data;
```

Sample with IP address

```
bioapi.settings.server.bms1.id = 1
bioapi.settings.server.bms1.name=Suprema
bioapi.settings.server.bms1.uri=https://192.168.0.1:44301/bioapi
bioapi.settings.server.bms1.optional.carrierName = true
bioapi.settings.server.bms1.optional.cards=true
bioapi.settings.server.bms1.optional.PIN=true
bioapi.settings.server.bms1.Content-Security-Policy=default-src 'self' https://192.168.0.1:44301 https://192.168.0.1:44301/WECClient 'unsafe-inline' 'unsafe-eval'; script-src 'self' https://192.168.0.1:44301 https://192.168.0.1:44301/WECClient https://192.168.0.1:44301/bioapi/cmdfingers/scan 'unsafe-inline' 'unsafe-eval'; object-src 'self' https://192.168.0.1:44301 https://192.168.0.1:44301/WECClient 'unsafe-inline' 'unsafe-eval'; img-src 'self' data
```

Configure AEOS for Suprema Integration

You can configure Suprema Integration on the Administration menu.

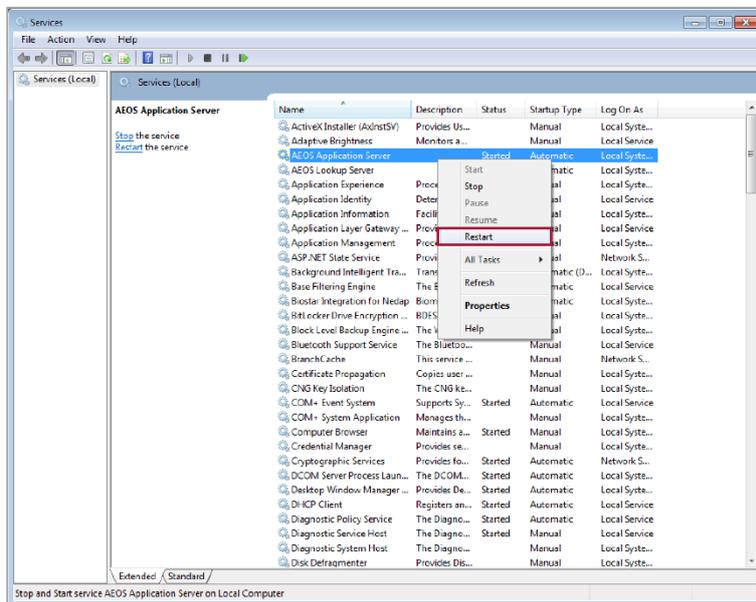
- 1 Run AEOS and click **Administration > Maintenance > Settings > System Properties**.
- 2 Select the biometric server name for the default verification type, then click **OK**. If the drop-down box is not enabled, enter the name used on the configuration from page 10.

12.04	Default verification method	<input type="text"/>
12.12	Default number of days for visitor verification validity	<input type="text"/>
12.13	Default number of days for employee verification validity	<input type="text"/>
12.14	Default number of days for contractor verification validity	<input type="text"/>
12.17	Holiday schedule overrules verification disabled schedule	<input type="checkbox"/>
12.36	Default BioAPI verification method (overrides default verification method)	Suprema <input type="text"/>
13.01	Export events, using eventfilter:	<input type="text"/>

- 3 Check **Enable biometric API**.

44.30	Enrollment Bioscript fingerprint	<input type="checkbox"/>
44.31	Document scanner	<input type="checkbox"/>
44.32	Enrollment Hitachi fingervein	<input type="checkbox"/>
44.33	Enrollment Kosmos weight	<input type="checkbox"/>
44.34	Enrollment Sagem fingerprint	<input type="checkbox"/>
44.36	Enable biometric API	<input checked="" type="checkbox"/>
44.37	4 eyes verification	<input type="checkbox"/>

- 4 Click **OK** and apply the changes.
- 5 Restart the AEOS Application Server service.



Install certificate (Client PC)

- 1** To access the Suprema biometric enrollment screen from AEOS at a client PC, the root certificate needs to be installed.
- 2** Open the **C:\Program Files (x86)\Suprema\Suprema Integration with Nedap AEOS\cert** folder from the server PC.
- 3** Copy the **SupremaIntegrationWithNedapAEOS.root.crt** to the client PC
- 4** Install the certificate.

NOTE

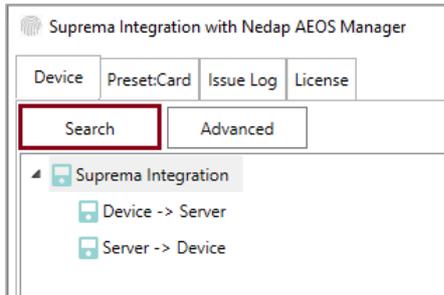
- The browser needs to be restarted for the certificate to be applied for usage.
-

Biometric Device

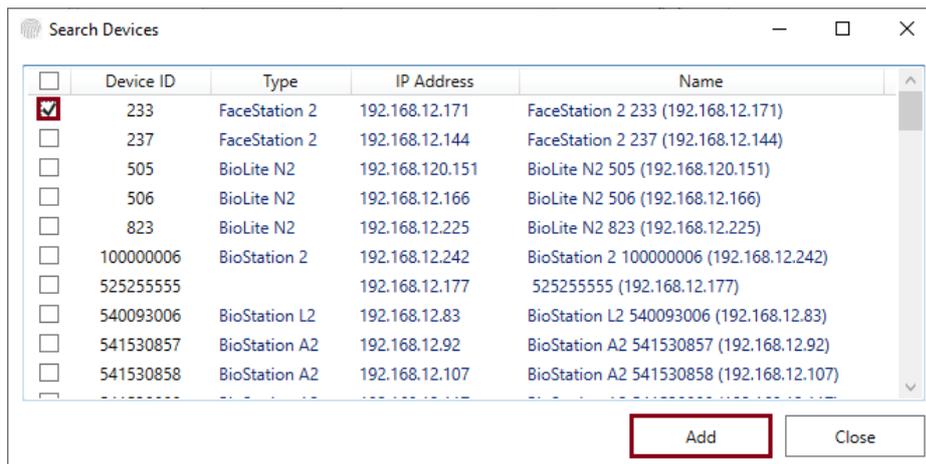
Configure biometric device's network settings

Biometric devices must be connected on the server of Suprema Integration with Nedap AEOS to be used as an enrollment device or a reader.

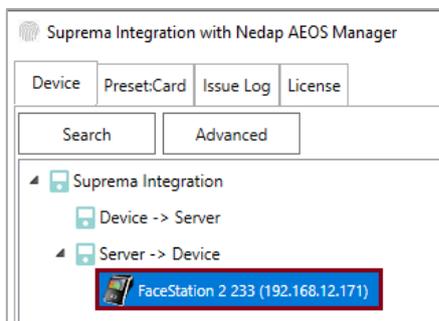
- 1 Run Suprema Integration with Nedap AEOS Manager and click **Search**.



- 2 Select the device for connecting to Suprema Integration with Nedap AEOS Manager and then click **Add**.



- 3 The added device will appear on the left panel.



NOTE

- If the connected device is not displayed on the panel, restart **Suprema Integration with Nedap AEOS Manager**.

Configure biometric device's wiegand settings

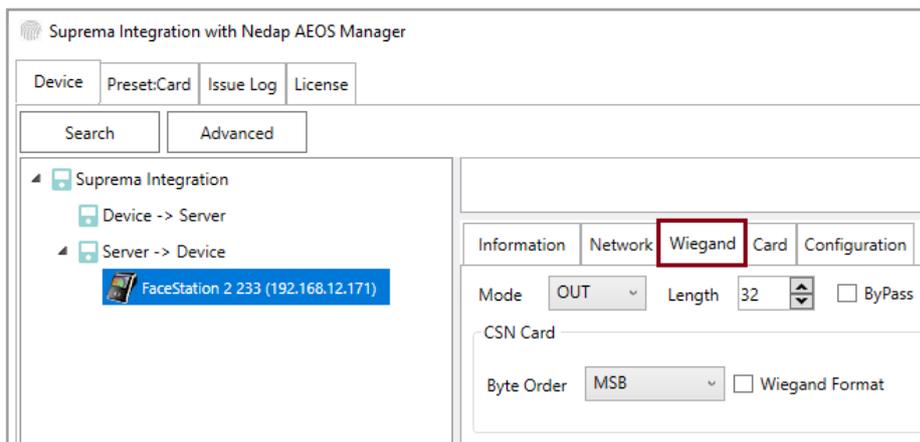
Biometric devices outputs data to the AEpu Controller by Wiegand. The device's wiegand format and other settings can be managed from the **Suprema Integration Manager**.

NOTE

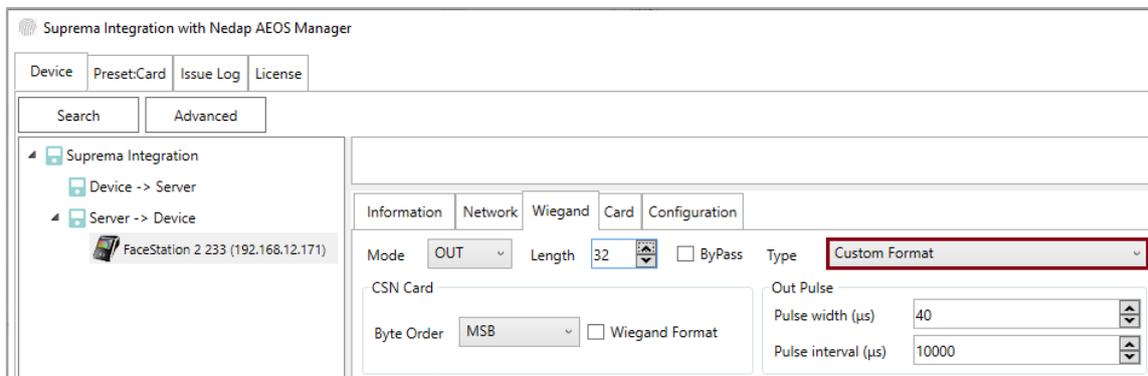
- The Suprema Integration with Nedap AEOS is set to work with Mifare Classic cards. The devices will need a specific configuration to be set to send out proper wiegand signals on a successful authentication.

1 Select the device to manage from the device panel.

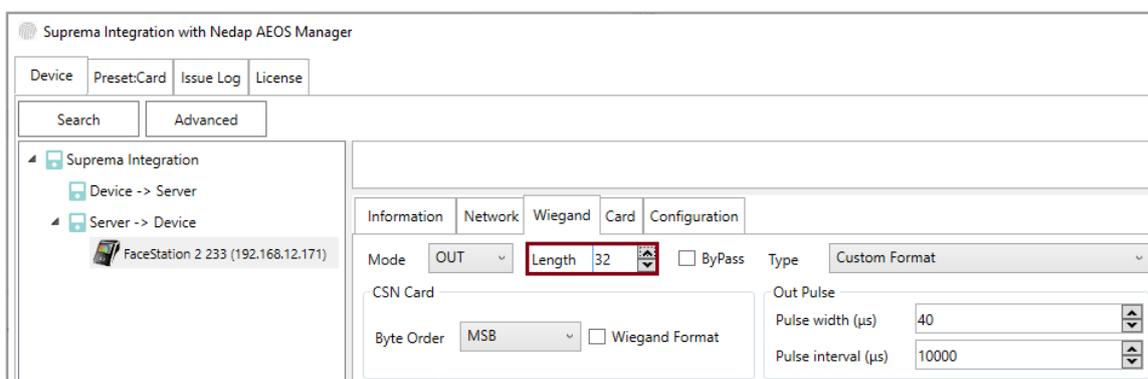
2 Click the **Wiegand** tab.



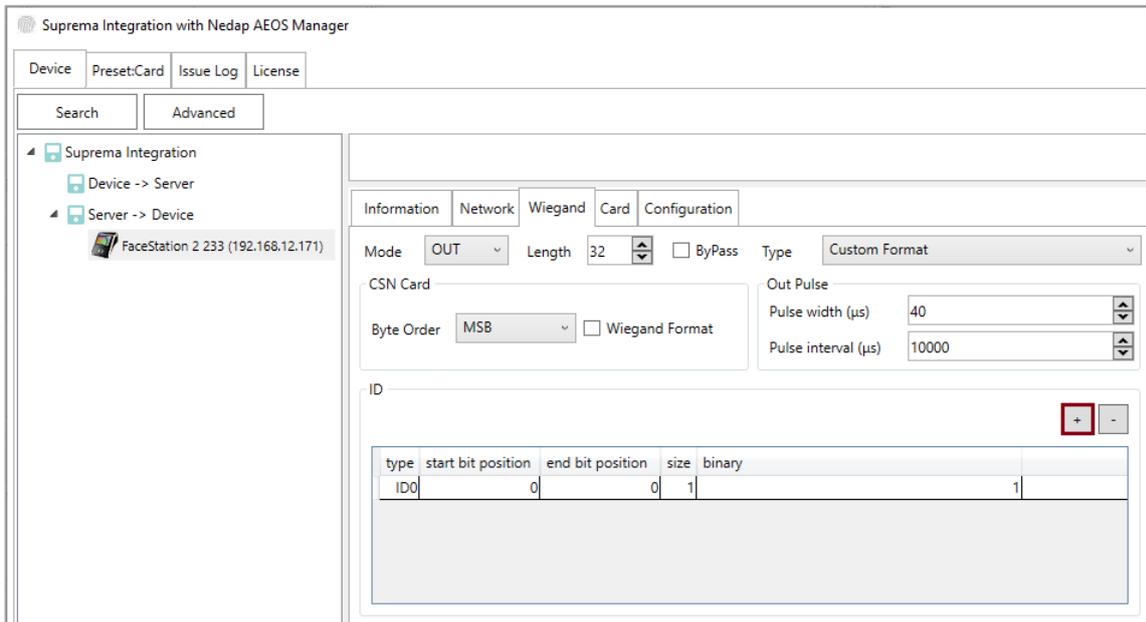
3 From the **Wiegand** tab, select **Custom Format** from the drop-down menu for **Type**.



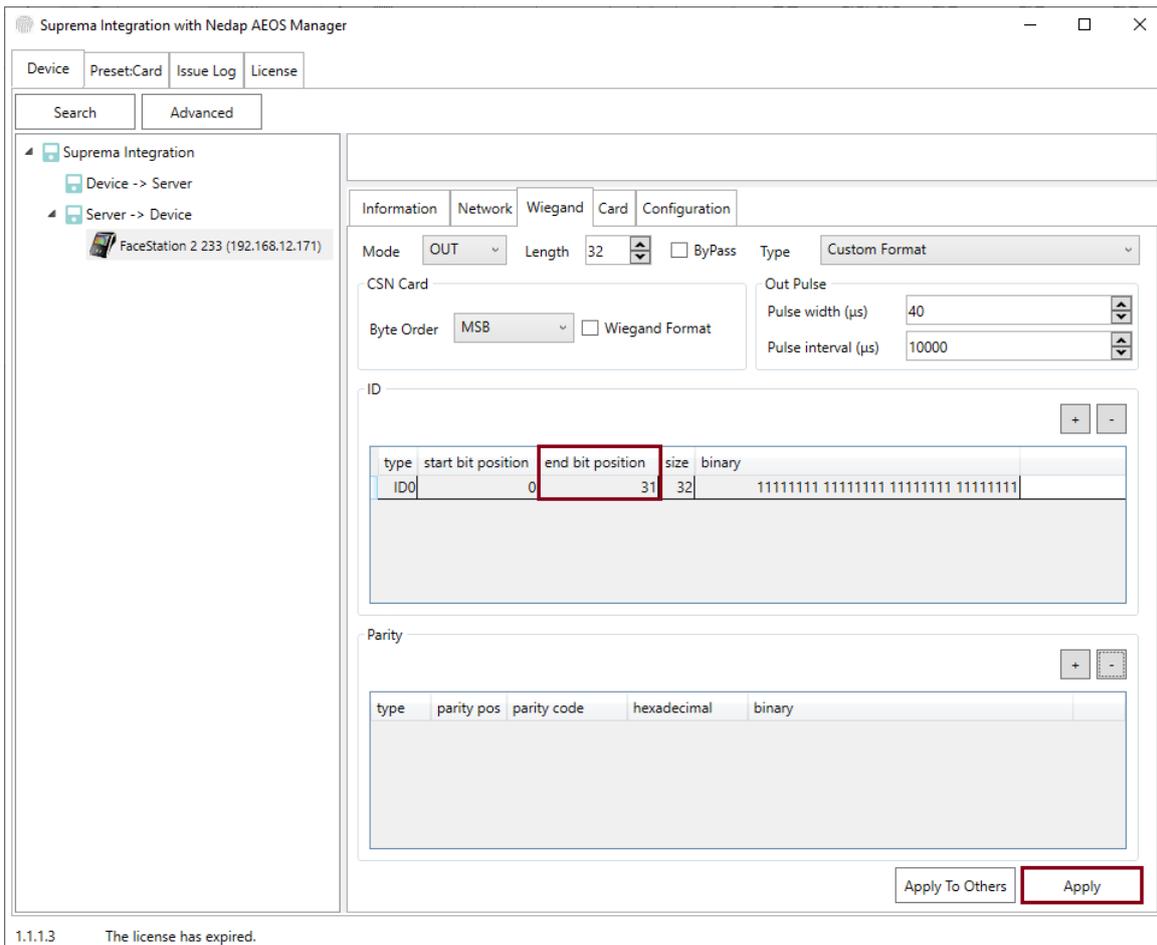
4 Set the **Length** to 32.



5 Click the **Add** button.



6 Set the **End Bit Position** to 31 and click **Apply**.



1.1.1.3 The license has expired.

Biometric Credential Enrollment

NOTE

- In order to enroll fingerprints on AEOS, users to enroll fingerprints, entrances and time schedules must be set in AEOS. This document describes how to set these conditions. For more information, refer to the AEOS manual.

Enroll biometric credentials

Once you have configured Suprema Integration with Nedap AEOS, you can enroll and manage fingerprints of user on the AEOS platform.

1 Enroll Biometric Identifiers button will appear when the cardholder has an identifier.

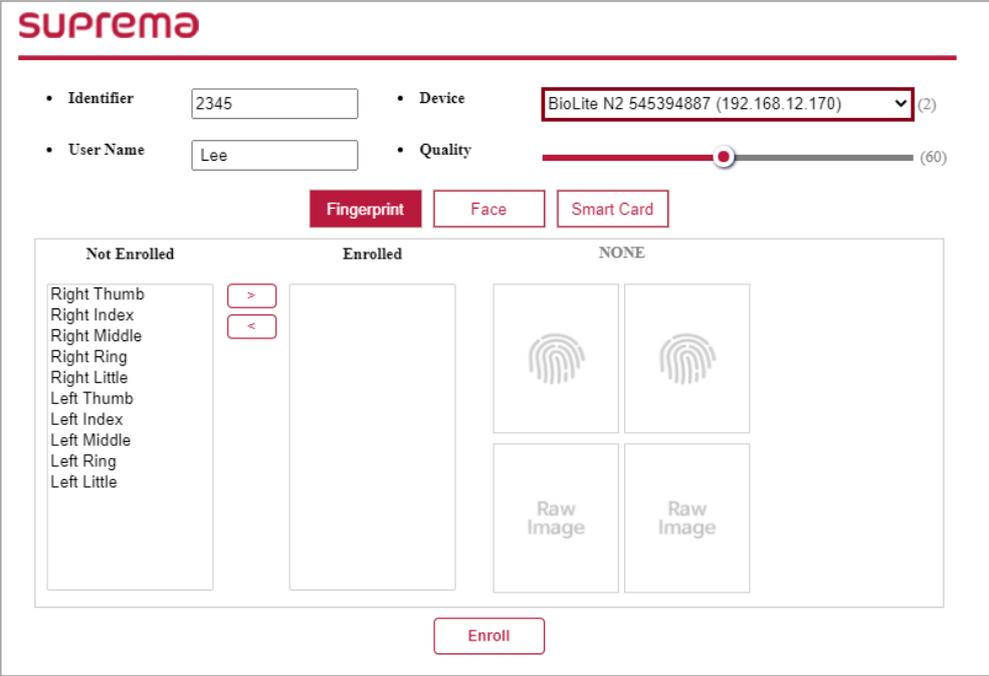
The screenshot shows an 'Employee' profile form. Fields include: Last name* (Suprema), First name, Middle name, Title, Gender (Unknown), Telephone no., Mobile no., E-mail, Language (English), Person(nel) no., and Department. On the right, there are date fields (Date from*, Date until), creation and modification dates, last time seen, last used entrance, last time denied (24/11/2020 17:13), last denied entrance (Door1), and a 'Can be user' checkbox. A camera icon is present. Below the employee info are sections for 'Contact', 'Authorization', and 'Identification'. The 'Identification' section shows 'Identifier type' (Suprema) and 'Identifier' (2345). A red box highlights the 'Enroll Biometric Identifiers' button.

2 Click the Enroll Biometric Identifiers button.

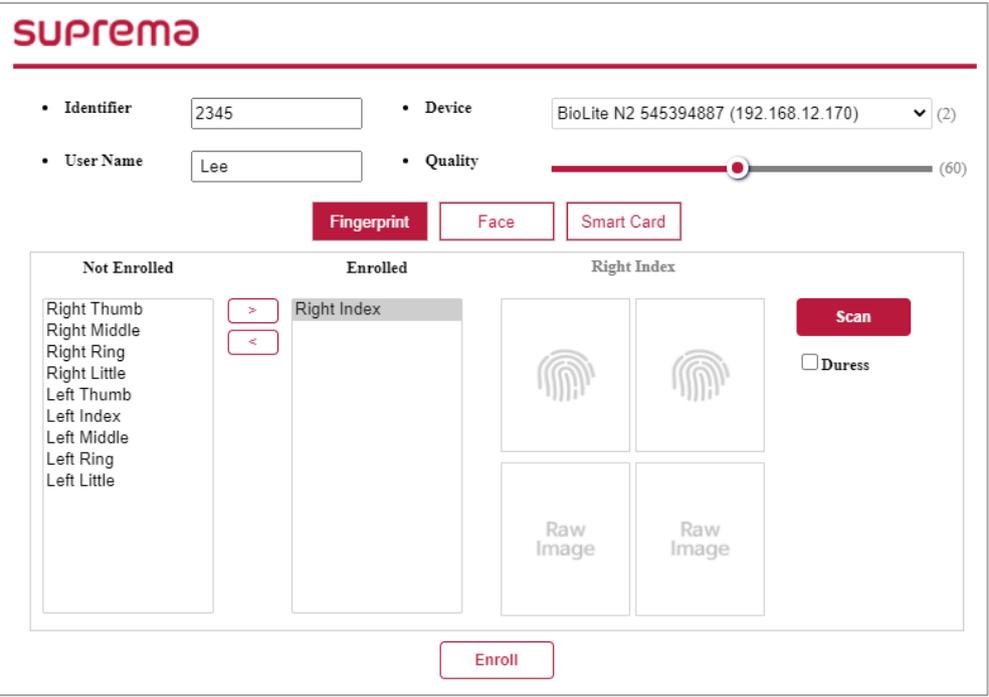
The screenshot shows the Suprema enrollment interface. At the top, there are fields for Identifier (2345), Device (BioLite N2 545394887 (192.168.12.170)), and User Name (Lee). A Quality slider is set to 60. Below these are three buttons: Fingerprint (highlighted in red), Face, and Smart Card. The main area is divided into three columns: 'Not Enrolled', 'Enrolled', and 'NONE'. Under 'Not Enrolled', there is a list of fingers: Right Thumb, Right Index, Right Middle, Right Ring, Right Little, Left Thumb, Left Index, Left Middle, Left Ring, and Left Little. Under 'Enrolled', there is a large empty box. Under 'NONE', there are two boxes labeled 'Raw Image'. At the bottom, there is an 'Enroll' button.

Enroll Fingerprint

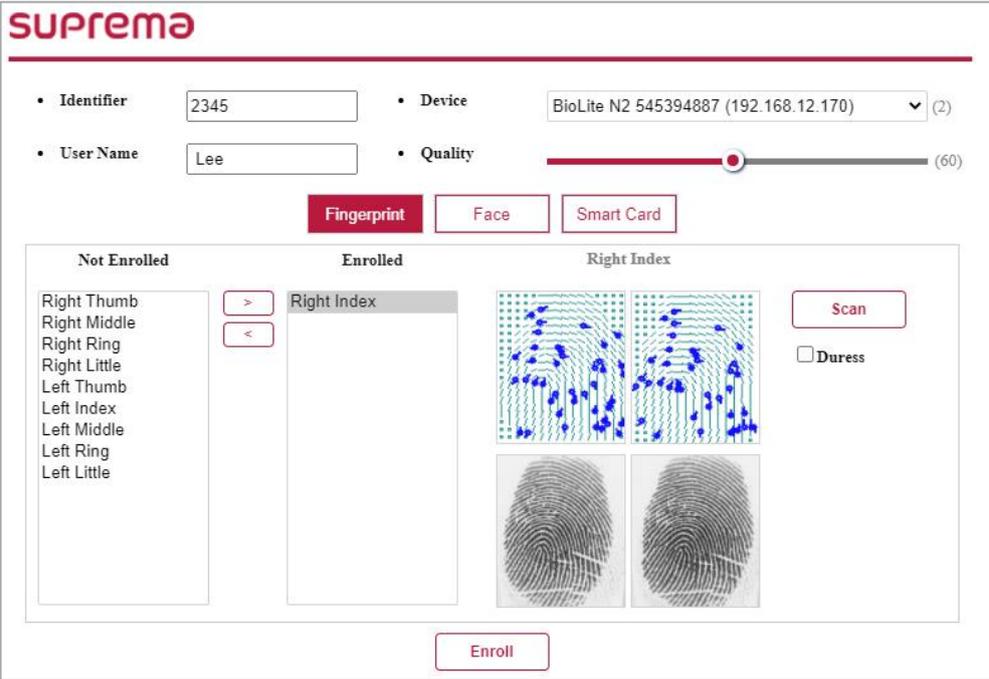
1 Click **Fingerprint** and select the device to capture fingerprint.



2 Select a finger to enroll from the left panel and click the right arrow button. Then, click **Scan** to scan the fingerprint.

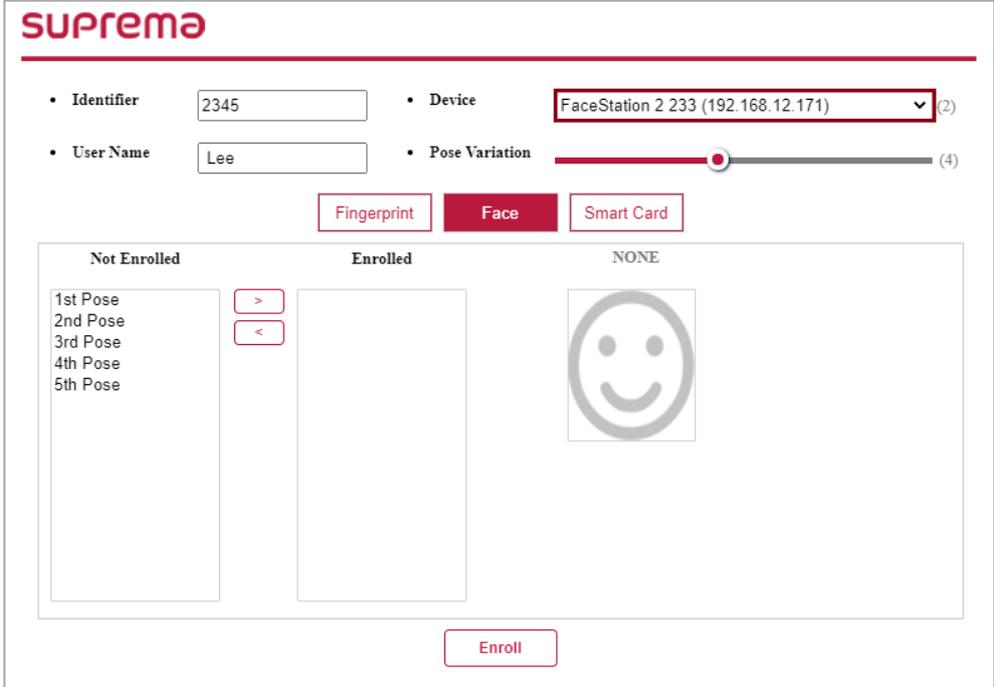


3 Click **Enroll** to confirm the enrollment.



Enroll Face

1 Select **Face** and select the device to capture face.



2 Select the index of the pose. Then, click **Scan** to scan the face. One face template is recommended per user.

SUPrema

- Identifier: 2345
- Device: FaceStation 2 233 (192.168.12.171) (2)
- User Name: Lee
- Pose Variation: (4)

Fingerprint | **Face** | Smart Card

Not Enrolled	Enrolled	1st Pose
2nd Pose 3rd Pose 4th Pose 5th Pose	1st Pose	

Enroll

3 Click **Enroll** to confirm the enrollment.

SUPrema

- Identifier: 2345
- Device: FaceStation 2 233 (192.168.12.171) (2)
- User Name: Lee
- Pose Variation: (4)

Fingerprint | **Face** | Smart Card

Not Enrolled	Enrolled	1st Pose
2nd Pose 3rd Pose 4th Pose 5th Pose	1st Pose	

Enroll

Troubleshooting

When Suprema Integration with Nedap AEOS web service does not work normally

- Check if the certificate is correctly applied to the AEOS keystore.
- Check the version of OpenSSL installed. OpenSSL version 1.0.2I or later that supports the TLS 1.2 protocol must be installed.

When the device can not connected to Suprema Integration with Nedap AEOS web service

- If you have BioStar 2 installed on your PC, make sure the BioStar 2 server is stopped. The device can be connected to the BioStar 2 server first when the window is restarted. If possible, use BioStar 2 and Suprema Integration with Nedap AEOS on different PCs.

Appendices

- The path of the system components is shown below.
 - Configuration file: (C:\Program Files (x86)\Suprema\Suprema Integration with Nedap AEOS\conf\server.json)
 - Database: (C:\Program Files (x86)\Suprema\Suprema Integration with Nedap AEOS\db)

The logo for Suprema, featuring the word "suprema" in a bold, lowercase, sans-serif font. Below it, the words "SECURITY & BIOMETRICS" are written in a smaller, uppercase, sans-serif font. The entire logo is contained within a dark red rectangular box.

suprema
SECURITY & BIOMETRICS

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang- gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA
Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

©2020 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc. All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies. Product appearance, build status and/or specifications are subject to change without notice.