

BioStar Integration for Nedap

SETUP GUIDE

Version 1.10
English

Contents

Target Audience	3
Introduction	4
Features.....	4
System diagram.....	4
Installation	5
Prerequisites	5
Configuration procedure.....	5
Installing BioStar Integration for Nedap	6
Installing BioStar Integration for Nedap Setup file	6
Installing the license key.....	7
Configuration	8
Biometric Device	8
Setting the biometric device network	8
Setting the biometric device Wiegand Out	10
AEOS	12
Generating a new certificate.....	12
Importing the trustCAcert to AEOS keystore.....	14
Enrolling Identifier Type to AEOS.....	15
Setting AEOS for BioStar Integration.....	15
Configuring AEOS for BioStar Integration.....	16
AEpus Controller	17
Detecting AEpus on AEOS	17
Setting Identifier Type on AEpu Controller.....	19
Fingerprint Enrollment	21
Adding a day and time schedule	21
Adding a new entrance.....	22
Adding an entrance template	23
Enrolling a fingerprint.....	24
Troubleshooting	27
When BioStar Integration for Nedap web service does not work normally	27
When the device can not connected to BioStar Integration for Nedap web service	27
Appendices	28

Target Audience

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

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

BioStar Integration for Nedap 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 BioStar Integration for Nedap, you can easily setup and build the Biometric Management System for the AEOS using Suprema biometric devices.

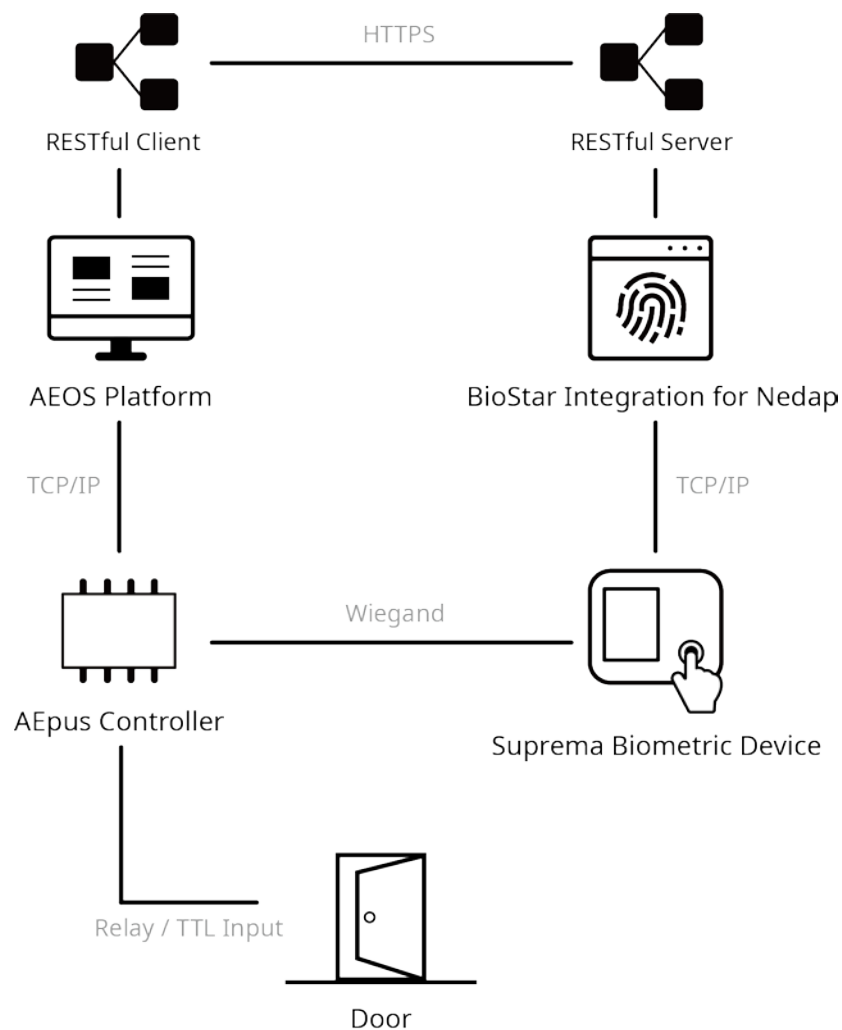
BioStar Integration for Nedap provides the following features:

- 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 is able to 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 BioStar Integration for Nedap.
- 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

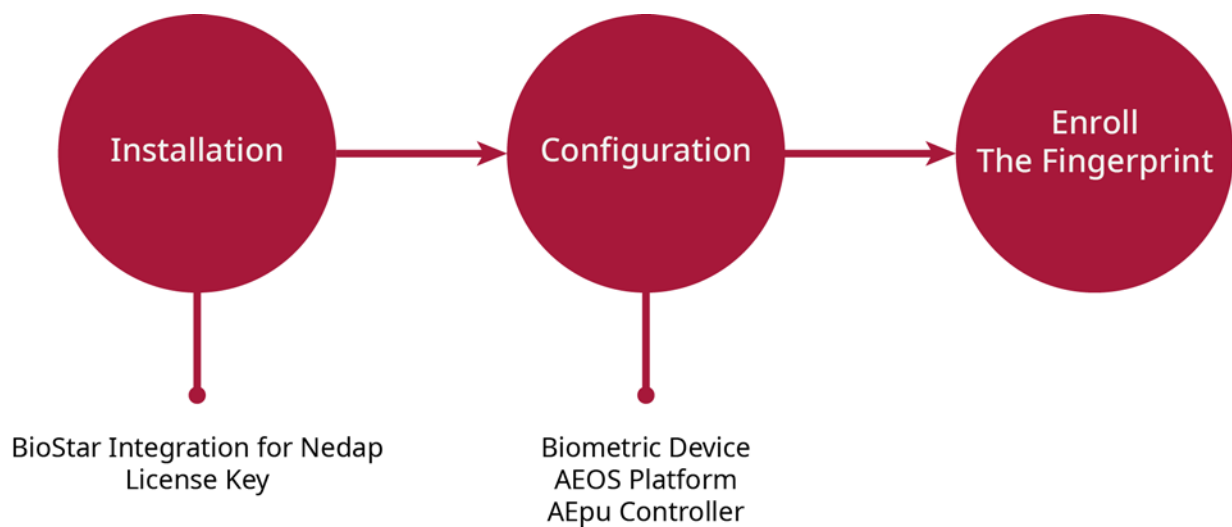
The following prerequisites are required to use BioStar integration for Nedap. Check the support conditions before installing the BioStar integration for Nedap.

- Operating system
 - Microsoft Windows 7(x86 / x64), Microsoft Windows 10(x64), Microsoft Windows Server 2012
- Web browsers
 - Chrome 6x, IE10 / IE11
- AEOS
 - AEOS 3.2.x, AEOS 3.3.1, AEOS 3.3.2
- Biometric Device
 - BioStation 2, BioStation A2, BioStation L2, BioEntry W2
- BS_SDK_V2
 - 2.5.0

NOTE

- BS_SDK_V2 is included in BioStar Integration for Nedap installation file.

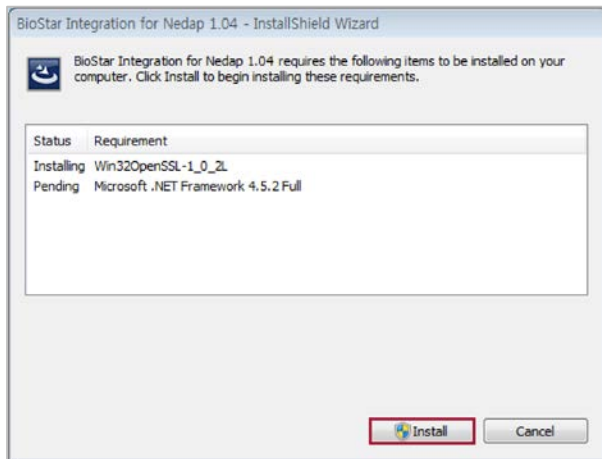
Configuration procedure



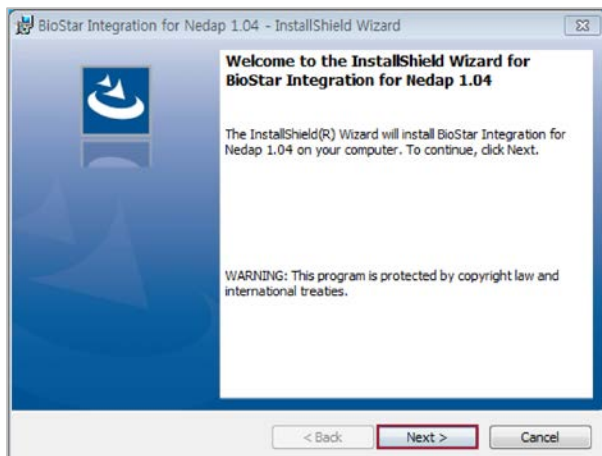
Installing BioStar Integration for Nedap

Installing BioStar Integration for Nedap Setup file

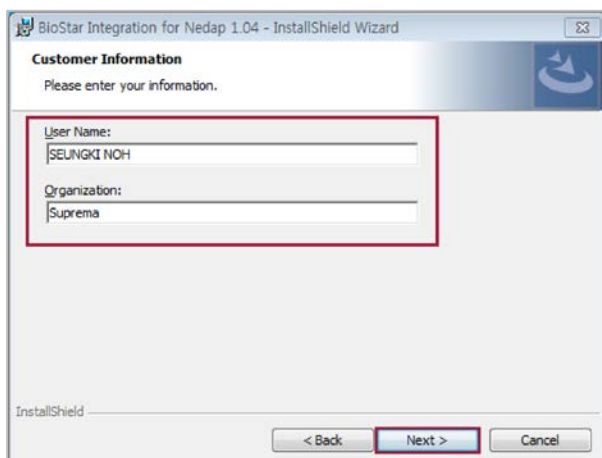
- 1 Run the **BioStar Integration for Nedap 1.04** setup file.
- 2 Click **Install** to continue. BioStar Integration for Nedap requires some items to be installed.



- 3 To continue the installation, click **Next**.



- 4 Enter the customer information and then click **Next**.



- 5 If ready to install, click **Install**.
- 6 Click **Finish** to complete installing BioStar Integration for Nedap.

Installing the license key

- 1 Run the command prompt (cmd) on the PC where BioStar Integration for Nedap is installed.

NOTE

- You can run the command prompt in the following ways: Click the Windows Start button and enter **cmd** in **Search programs and files** text box.

- 2 Enter **ipconfig/all** in the Command Prompt window and press **Enter** key. When you see the results, check the Mac address.

```
C:\Windows\system32\cmd.exe
C:\Users\UM-SEUNGKI>ipconfig /all

Windows IP Configuration

Host Name . . . . . : UM-SEUNGKI-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  :
   Description . . . . . : Local (P) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . : 08-00-27-AC-54-35
   DHCP Enabled. . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8921:2867:388f:fd84:10<Preferred>
   IPv4 Address. . . . . : 192.168.12.20<Preferred>
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.12.1
   DNS Servers . . . . . : 192.168.1.253
                           192.168.1.6
   NetBIOS over Tcpip. . . . . : Enabled

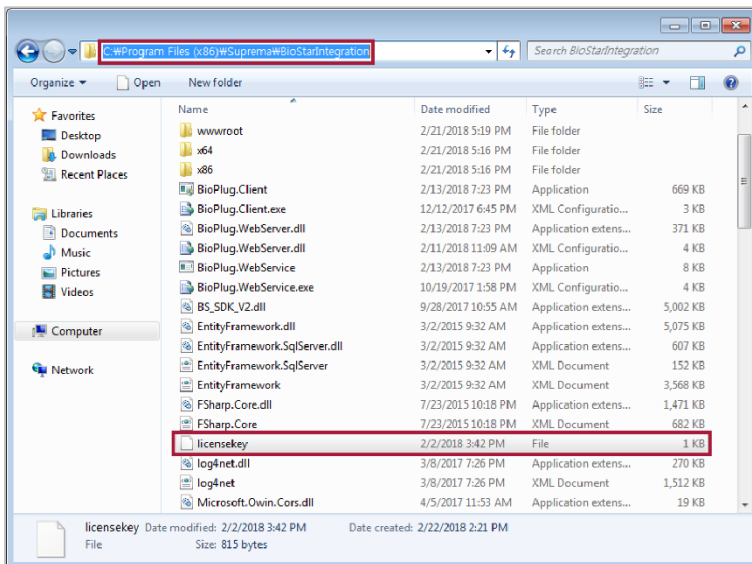
Tunnel adapter isatap.{B1D01210-C1B9-40B1-A305-420E9DAE15BF}:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix  :
   Description . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . : 00-00-00-00-00-00-E0
   DHCP Enabled. . . . . : No
   Autoconfiguration Enabled . . . . : Yes

C:\Users\UM-SEUNGKI>
```

- 3 Send the Mac address and period of use to your place of purchase via email and request a license key.

- 4 Save the license key in the BioStar Integration for Nedap installation folder.



NOTE

- The path of the BioStar Integration for Nedap installation folder is as follows: **C:\Program Files (x86)\Suprema\BioStarIntegration**

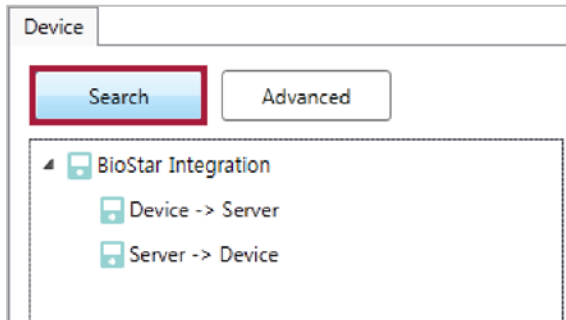
Configuration

Biometric Device

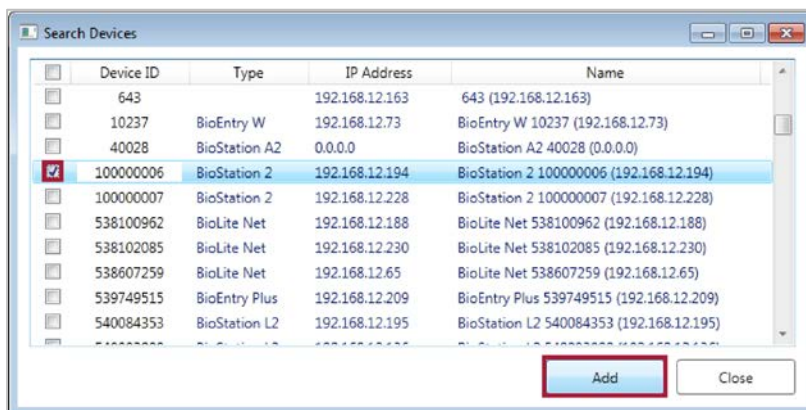
Setting the biometric device network

Biometric devices must be connected on the server of BioStar Integration for Nedap.

- 1 Run **BioStar Integration Manager** and click **Search**.



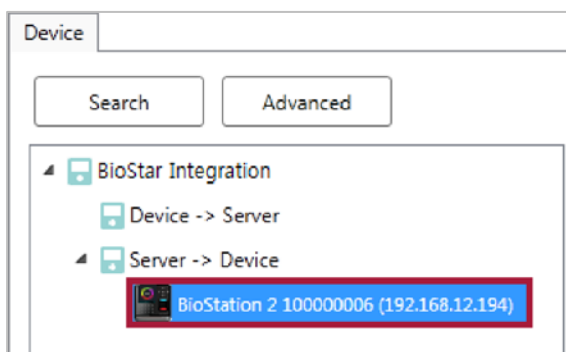
- 2 Select the device for connecting to BioStar Integration Manager and then click **Add**.



NOTE

- This document explains BioStation 2 as an example, and it is possible to connect with BioStation A2, BioStation L2, and BioEntry W2.

- 3 Select a device on BioStar Integration panel.



4 In Network tab, click **Device -> Server Connection** and then fill in **Server IP** and **Server Port**.

The screenshot shows the 'Network' configuration tab with the following fields:

- DHCP
- IP Address: 192.168.12.194
- Subnet Mask: 255.255.255.0
- Gateway: (empty)
- Device Port: 51211

Under the 'Server' section:

- Device -> Server Connection
- DNS
- Server IP: 192.168.12.20
- DNS Address: (empty)
- Server Port: 51212
- Server URL: (empty)

An 'Apply' button is located at the bottom right of the configuration area.

5 The connected device will be displayed on **Device -> Server**.

The screenshot shows the 'Device' list with the following structure:

- BioStar Integration
 - Device -> Server
 - BioStation 2 100000006 (192.168.12.194)** (highlighted with a red box)
 - Server -> Device

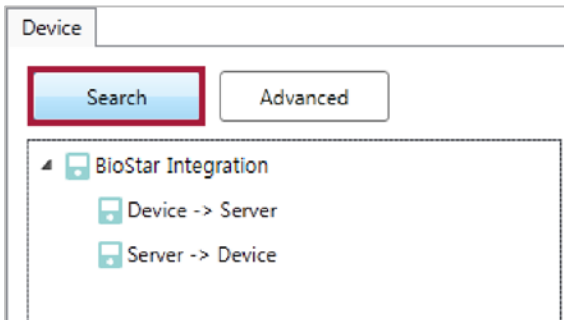
NOTE

- If the connected device is not displayed on the panel, reboot **BioStar Integration Manager**.

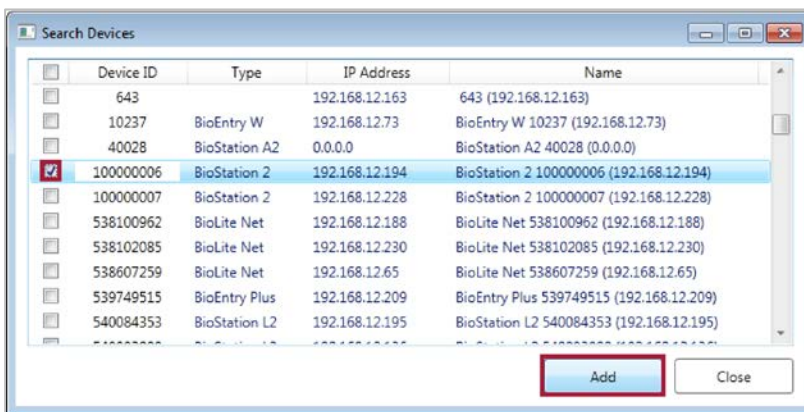
Setting the biometric device Wiegand Out

Biometric devices and AEpus Controller are connected by a Wiegand protocol.

- 1 Run **BioStar Integration Manager** and click **Search**.



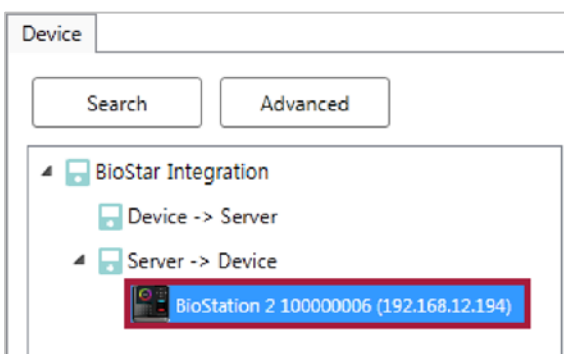
- 2 Select the device for connecting to BioStar Integration Manager and then click **Add**.



NOTE

- This document explains BioStation 2 as an example, and it is possible to connect with BioStation A2, BioStation L2, and BioEntry W2.

- 3 Select a device on BioStar Integration panel.



4 In Wiegand tab, select a Wiegand format of the default list or create a new custom Wiegand format.

The screenshot shows the 'Wiegand' configuration tab. The 'Type' dropdown menu is open, displaying a list of options: '36 Bit Wiegand HID H10301', '37 Bit Wiegand HID H10302', '37 Bit Wiegand HID H10304', '35 Bit Wiegand HID Corporate 1000', '48 Bit Wiegand HID Corporate 1000', and 'Custom Format'. The '37 Bit Wiegand HID H10302' option is highlighted in red. Other settings include 'Mode: OUT', 'Length: 35', 'ByPass' checkbox, 'CSN Card' section with 'Byte Order: MSB' and 'Wiegand Format' checkbox, and an empty 'ID' table.

NOTE

- Set the Wiegand format according to the Wiegand type you want to use. This document provides an example with 37 Bit Wiegand.
- If you want to use CSN Card to Wiegand Type, click the **Wiegand Format** checkbox at CSN Card frame.

5 Click **Apply**.

The screenshot shows the 'Wiegand' configuration tab with the '37 Bit Wiegand HID H10302' format selected. The 'Wiegand Format' checkbox is checked. The 'Out Pulse' section shows 'Pulse width (µs): 40' and 'Pulse interval (µs): 10000'. The 'ID' table contains one entry: ID0, start bit position 1, end bit position 35, size 35, and binary value 01111 11111111 11111111 11111111 11111110. The 'Parity' table contains two entries: EVEN (parity pos 0, parity code 68719214592, hexadecimal 0xFFFFC000, binary 01111 11111111 11111100 00000000 00000000) and ODD (parity pos 36, parity code 524286, hexadecimal 0x7FFE, binary 00000 0000000 00000111 11111111 11111110). The 'Apply' button is highlighted with a red box.

AEOS

Generating a new certificate

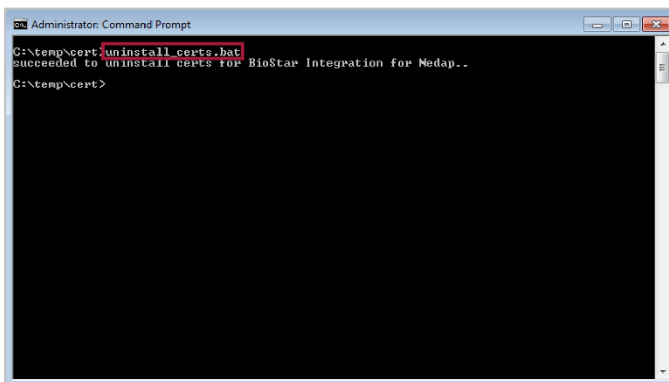
AEOS and BioStar Integration for Nedap require a certificate because they are linked in HTTPS protocol. You can use the certificate provided by BioStar Integration for Nedap, or you can generate a new certificate using the desired domain name and IP address. This section describes how to generate a new certificate.

- 1 Move the entire certificate script files to the desired working directory.

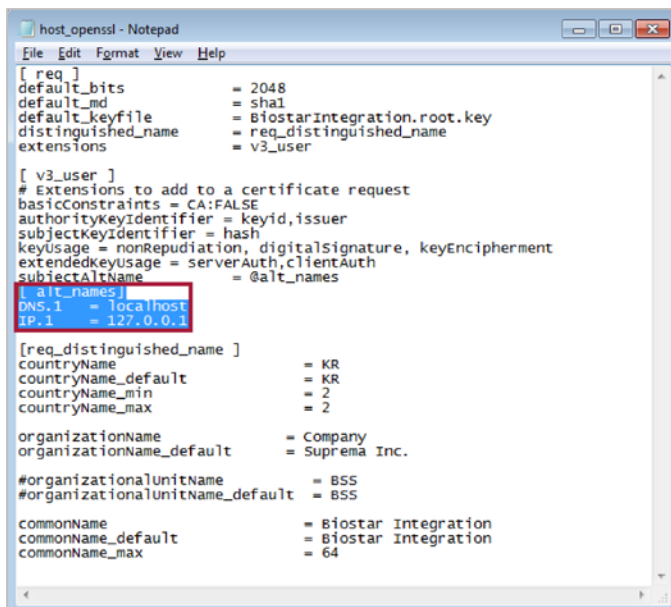
NOTE

- The path of the BioStar Integration certificate script files is as follows: `C:\Program Files (x86)\Suprema\BioStarIntegration\cert`

- 2 Run the command prompt (cmd) and then enter `uninstall_certs.bat`.



- 3 Delete the default certificate files (BioStarIntegration.root, BioStarIntegration.user) from the working directory.
- 4 Open the `host_openssl` file.
- 5 Modify the domain name and IP address, and then save the file.



6 Run the command prompt and then enter `default_cert.sh`.

```
Administrator: Command Prompt - sh default_cert.sh
C:\temp\cert>sh default_cert.sh
Generating RSA private key, 2048 bit long modulus
.....***
e is 65537 (0x10001)
writing RSA key
Subject Attribute /C has no known NID, skipped
Signature ok
subject=/O=Suprema/CN=Suprema Root CA
Getting Private key
Generating RSA private key, 2048 bit long modulus
.....***
e is 65537 (0x10001)
writing RSA key
Subject Attribute /C has no known NID, skipped
Signature ok
subject=/O=Suprema/CN=localhost
Getting CA Private Key
Enter Export Password:
```

NOTE

- `default_cert.sh` is a script that can be run without any extra parameters.
- `default_cert.sh` is a bash shell script. To run this script, `win-bash` must be installed on your PC. Install `win-bash` and then add the install path to the System PATH variable in Windows.

7 Set the export password for the new certificate to **suprema123**. The new certificate file will be generated at the working directory.

```
Administrator: Command Prompt - sh default_cert.sh
C:\temp\cert>sh default_cert.sh
Generating RSA private key, 2048 bit long modulus
.....***
e is 65537 (0x10001)
writing RSA key
Subject Attribute /C has no known NID, skipped
Signature ok
subject=/O=Suprema/CN=Suprema Root CA
Getting Private key
Generating RSA private key, 2048 bit long modulus
.....***
e is 65537 (0x10001)
writing RSA key
Subject Attribute /C has no known NID, skipped
Signature ok
subject=/O=Suprema/CN=localhost
Getting CA Private Key
Enter Export Password:
suprema123
```

8 Enter `Install_cert.bat` at the command prompt to install the new certificate.

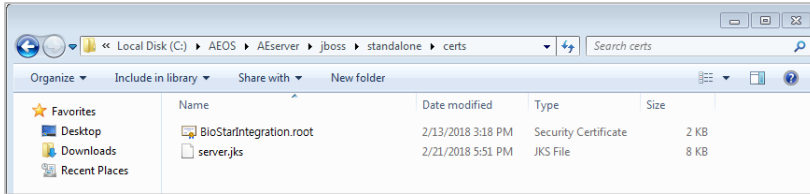
```
Administrator: Command Prompt
C:\temp\cert>sh default_cert.sh
Generating RSA private key, 2048 bit long modulus
.....***
e is 65537 (0x10001)
writing RSA key
Subject Attribute /C has no known NID, skipped
Signature ok
subject=/O=Suprema/CN=Suprema Root CA
Getting Private key
Generating RSA private key, 2048 bit long modulus
.....***
e is 65537 (0x10001)
writing RSA key
Subject Attribute /C has no known NID, skipped
Signature ok
subject=/O=Suprema/CN=localhost
Getting CA Private Key
Enter Export Password:
suprema123
Verifying - Enter Export Password:
suprema123
C:\temp\cert>default_cert.sh
C:\temp\cert>install_certs.bat
succeeded to install certs for BioStar Integration for Medap..
C:\temp\cert>_
```

9 Move the new certificate file (BioStarIntegration.root) to the AEOS certificate directory.

Importing the trustCAcert to AEOS keystore

AEOS and BioStar Integration for Nedap require a certificate because they are linked in HTTPS protocol. You can use the certificate provided by BioStar Integration for Nedap, or you can generate a new certificate using the desired domain name and IP address. This section describes how to import the certificate provided by BioStar Integration for Nedap.

- 1 Move the BioStar Integration root certificate file (BioStarIntegration.root) to the AEOS certificate directory.



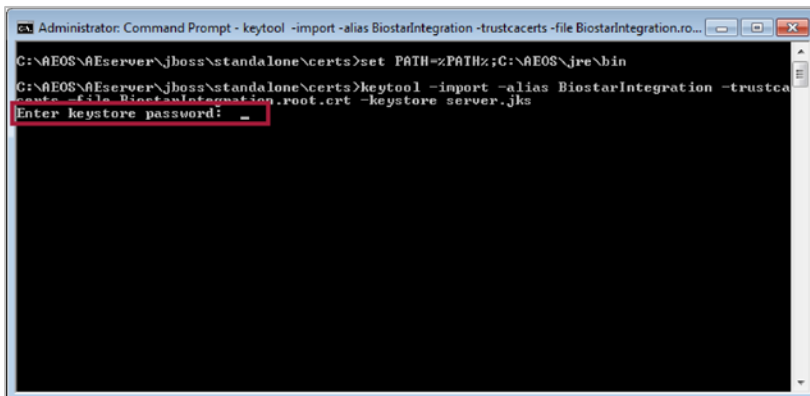
NOTE

- The path of the BioStar Integration root certificate file is as follows: C:\Program Files (x86)\Suprema\BioStarIntegration\cert

- 2 Open **server.jks** file in the AEOS certificate directory.

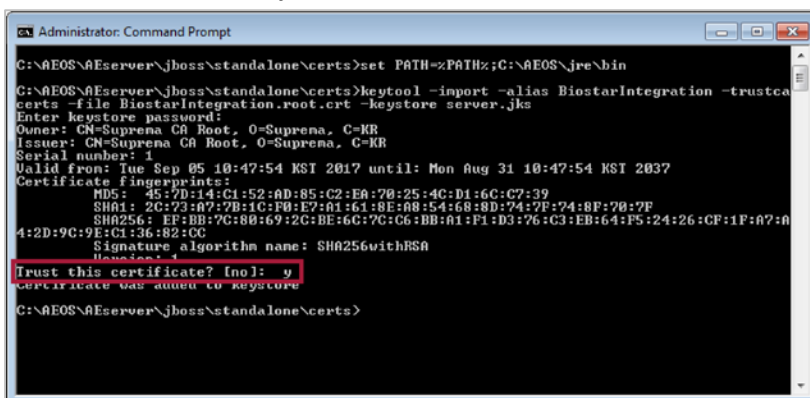
- 3 Enter the password as shown below.

- Keystore password: **nedap123**



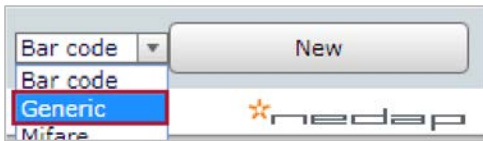
- 4 Answer the following a question.

- Trust this certificate? [no]: **y**

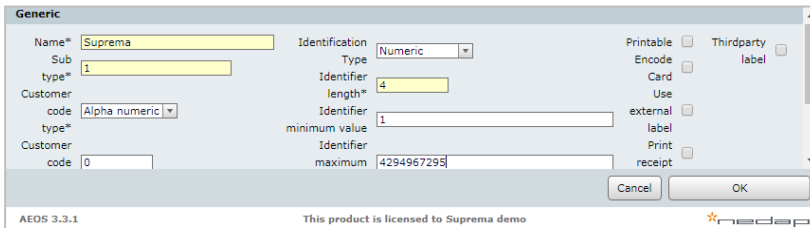


Enrolling Identifier Type to AEOS

- 1 Run AEOS and click **Administration > Maintenance > Identifiers > Identifier types**.
- 2 Select the identifier type **Generic** and then click **New**.



- 3 Enter the identifier type information and then **OK**.



Setting AEOS for BioStar Integration

To launch the fingerprint enrollment page in AEOS platform, you must configure BioStar Integration for Nedap in AEOS.

- 1 Open the **AEOS** folder and click **AEserver > jboss > standalone > configuration**.
- 2 Open **aeos.properties** file.
- 3 Set the Suprema Identifier type and the BioStar Integration web server URL as shown below.
 - bioapi.settings.server.bms1.id = 1
 - bioapi.settings.server.bms1.name=Suprema
 - bioapi.settings.server.bms1.uri=https://192.168.12.20:44301/bioapi
 - bioapi.settings.server.bms1.optional.carrierName = true
 - bioapi.settings.server.bms1.optional.cards=true
 - bioapi.settings.server.bms1.optional.PIN=true

```

aeos.properties - Notepad
File Edit Format View Help
#bioapi.settings.server.test1.optional.PIN=true
# whether the carrier's PIN-code should be sent to the biometric management system, when AEOS registers
# False by default.
#
#bioapi.settings.server.test1.api.service.username=myname
#bioapi.settings.server.test1.api.service.password=mypassword
# These are used for authentication between AEOS and the biometric management system adapter Layer.
# For this to work, it also needs to be configured on the container runner (E.g.; JBoss or Tomcat).
# can be omitted.
# Note that each set of settings needs to have it's own namespace.
# E.g.; bioapi.settings.server.bms1.id, bioapi.settings.server.bms2.id, bioapi.settings.server.bms3.id.
#
# Example settings:
#bioapi.settings.server.bms0.id=0
#bioapi.settings.server.bms0.name=Test0
#bioapi.settings.server.bms0.uri=https://testserver0:8444/bms/
#bioapi.settings.server.bms1.id=1
#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
#####
# SUPREMA - BIOSTAR INTEGRATION SERVICE
#####
bioapi.settings.server.bms1.id=1
bioapi.settings.server.bms1.name=Suprema
bioapi.settings.server.bms1.uri=https://192.168.12.20:44301/bioapi
bioapi.settings.server.bms1.optional.carrierName=true
bioapi.settings.server.bms1.optional.cards=true
bioapi.settings.server.bms1.optional.PIN=true
#####
# aeos.service.verification for distributing the SuspendStartTime
#####
#aeos.service.verification.httpHosturl=https://<master-aeos>:8443
#aeos.service.verification.httpHosturl=
#aeos.service.verification.UserName=
#aeos.service.verification.Password=
    
```

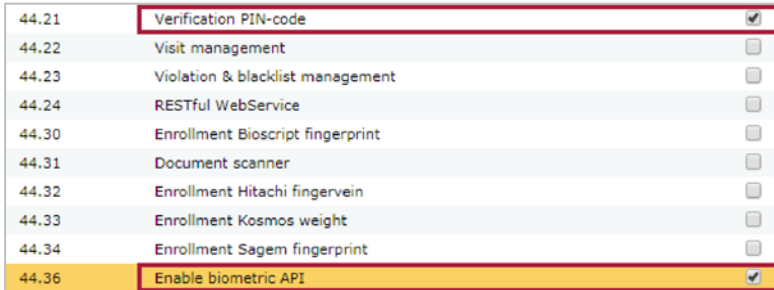
NOTE

- If you are using AEOS 3.3.2 or later, please make the following additional settings for added security:
 - bioapi.settings.server.bms1.Content-Security-Policy=default-src 'self' https://127.0.0.1:44301 https://127.0.0.1:44301/WECCClient 'unsafe-inline' 'unsafe-eval'; script-src 'self' https://127.0.0.1:44301 https://127.0.0.1:44301/WECCClient https://127.0.0.1:44301/bioapi/cmdfingers/scan 'unsafe-inline' 'unsafe-eval'; object-src 'self' https://127.0.0.1:44301 https://127.0.0.1:44301/WECCClient 'unsafe-inline' 'unsafe-eval'; img-src 'self' data

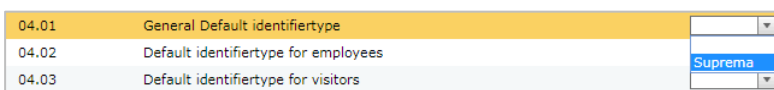
Configuring AEOS for BioStar Integration

You can configure BioStar Integration on the Administration menu.

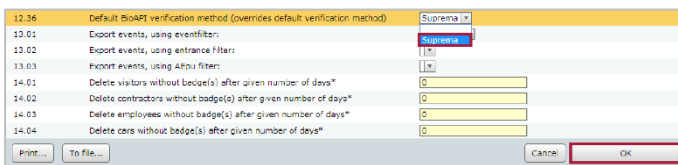
- 1 Run **AEOS** and click **Administration > Maintenance > Settings > System Properties**.
- 2 Click **Verification PIN-code** and **Enable biometric API**.



- 3 Select the biometric server name for the default identifier type.

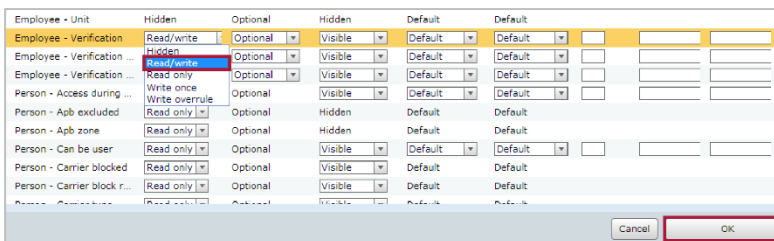


- 4 Select the biometric server name for the default verification type, then click **OK**.

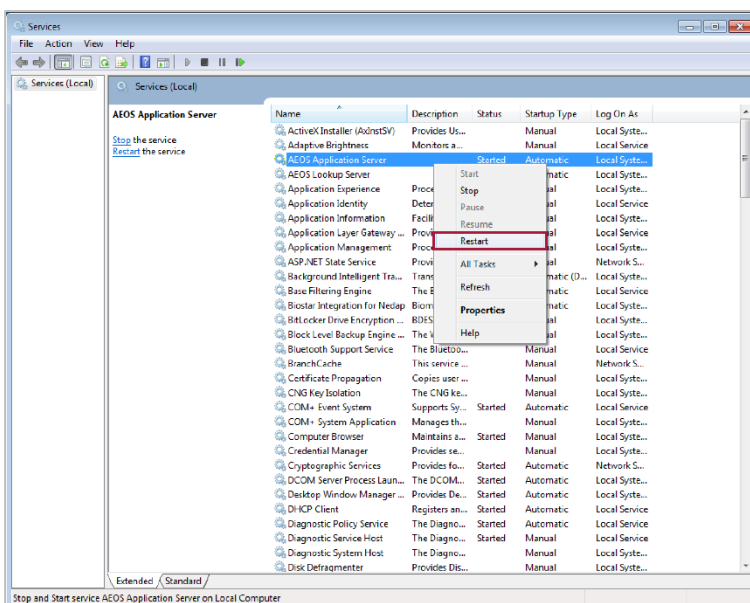


- 5 Click **Management > Maintain user role** and select **Administrator**.

- 6 Set **Employee - Verification** to **Read / Write** and click **OK**.



- 7 Restart AEOS Application Server.

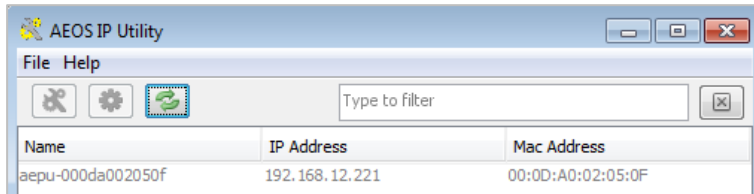


AEpus Controller

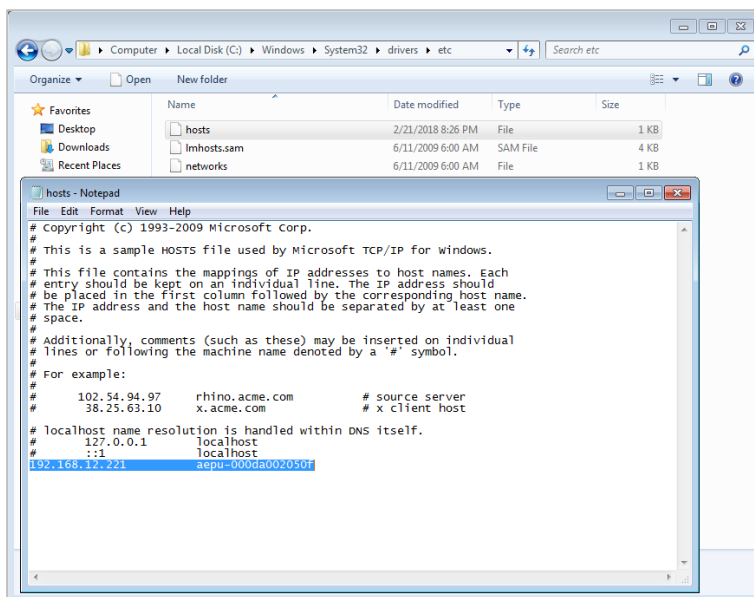
The AEpus Controller matches information that read from the device with user information and controls the door. This section describes how to connect the AEpus Controller to the AEOS and set the Identifier type.

Detecting AEpus on AEOS

- 1 Open **AEOS IP Utility** on AEOS folder and check the AEpu host name.



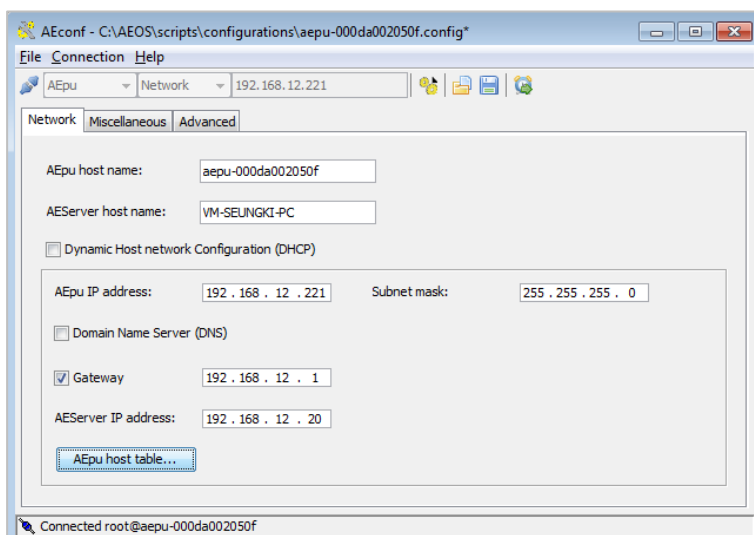
- 2 Enroll AEpu host name on hosts for IP mapping.



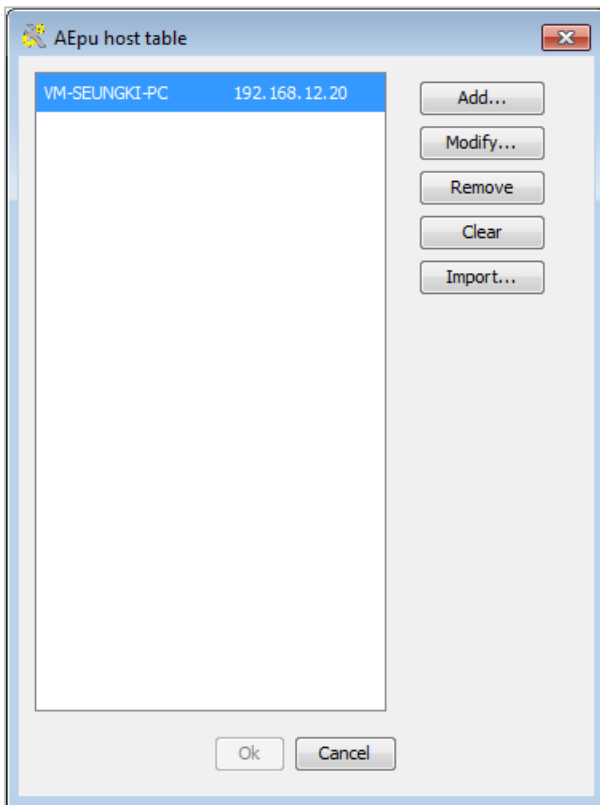
NOTE

- The path of the hosts file is as follows: C:\Windows\System32\drivers\etc.

- 3 Run **AEconf** and click **AEpu host table...**



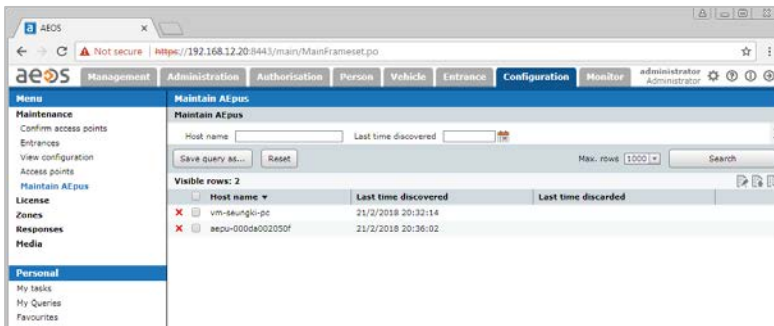
4 Select the host and click OK.



5 Click and to save and set AEpu IP settings.

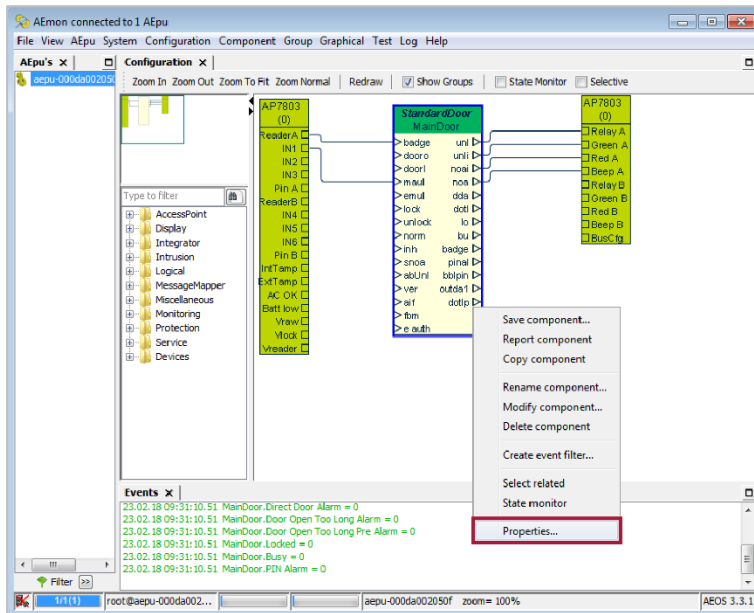
6 Click to synchronize the time of the AEpu from NTP server.

7 Connect to AEOS and check if AEpus is connected.

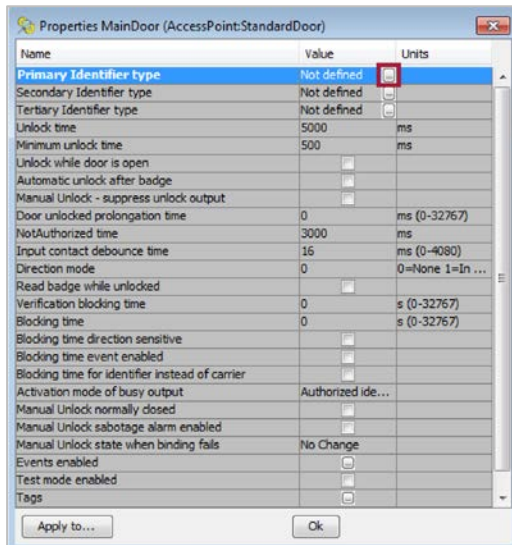


Setting Identifier Type on AEpu Controller

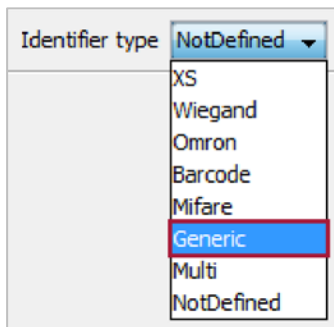
- 1 Run AEmon connected to 1 AEpu and select aepe controller.
- 2 Right-click on **MainDoor** and then select **Properties...**



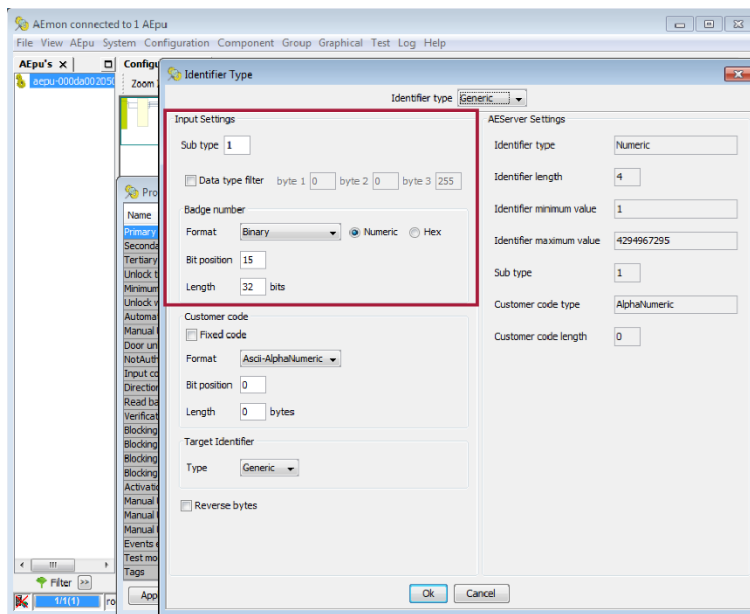
- 3 Click  Icon to open the property editor for Primary Identifier type.



- 4 Select the identifier type **Generic** and then click **OK**.



5 Enter the **Sub type**, **Format**, **Bit position** and **Length** information and click **OK**.



NOTE

- The Identifier Type of the AEpu controller must be set the same as the Suprema Identifier Type set in AEOS.
 - Set **Sub type** to 1.
 - Set **Length** to 32 bits (4 bytes).
 - Set **Bit position** to 15.
- Contact Nedap for details on setting up AEpus Controller.

Fingerprint Enrollment

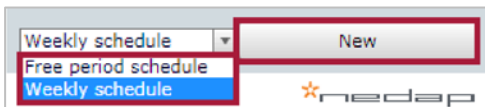
NOTE

- 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.

Adding a day and time schedule

You can set the day and time schedule in AEOS. Schedules can be set by specifying **Weekly schedule** or **Free period schedule**. This section describes based on Weekly schedule.

- Run AEOS and click **Authorization > Day/time schedules**.
- Select **Weekly schedule** or **Free period schedule** and click **New**.



- Enter information of the schedule then select days of the week to be set, specify the start time and end time, and click **Add**.

 A screenshot of the 'Day/time schedules' configuration window. The window title is 'Day/time schedules'. It has a section 'Maintain day/time schedule' with fields for 'Name*' (WorkingTimes) and 'Description'. Below is a calendar grid with days of the week and hours 0-23. The grid shows a blue shaded area from 8:00 to 17:00 on Monday through Friday. Below the grid is a section for 'Friday' with 'Visible rows: 1'. It shows a table with 'Start time' and 'End time' columns, with a row containing '08:00' and '17:00'. At the bottom, there are 'From' and 'Until' time selection fields with 'Hour' and 'Minute' dropdowns, and an 'Add' button. The 'Add' button is highlighted with a red box. Other buttons include 'Delete selection', 'Cancel', and 'OK'.

- Click **OK** to complete the schedule creation.

Adding a new entrance

You can add new entrances on the configuration menu.

- 1 Run **AEOS** and click **Configuration > Entrance**.
- 2 Click **New** to add a new Entrance.
- 3 Enter information of the entrance then click **Add access points**.

The screenshot shows the 'Entrances' configuration window with the 'Maintain entrance' tab selected. The form contains the following fields and controls:

- Name***: Text input field containing 'EntranceDoor'.
- Location**: Text input field.
- Description**: Text input field.
- Function**: Dropdown menu.
- Country**: Dropdown menu.
- Site**: Dropdown menu.
- Sub site**: Dropdown menu.
- Add access points**: Button.

- 4 Select the access point and click **OK**.

The screenshot shows the 'Entrances' configuration window with the 'Search access point' dialog open. The dialog contains the following fields and controls:

- Entrance name**: Text input field containing 'EntranceDoor'.
- Access point**: Text input field.
- Type**: Dropdown menu.
- Host name**: Text input field.
- Description**: Text input field.
- Save query as...**: Button.
- Reset**: Button.
- Max. rows**: Dropdown menu set to '1000'.
- Search**: Button.
- Visible rows: 1**: Text label.
- Access point**: Column header.
- Type**: Column header.
- Host name**: Column header.
- Description**: Column header.
- MainDoor**: Row in the table with a checkmark in the first column.
- StandardDoor**: Row in the table.
- eeu-000a002050f**: Row in the table.
- Print...**: Button.
- To file...**: Button.
- Delete selection**: Button.
- Cancel**: Button.
- OK**: Button.

- 5 Click **OK** to complete adding entrance.

Adding an entrance template

You can manage the entrance template on the Authorization menu. This section describes how to add an entrance.

- 1 Run **AEOS** and click **Authorization > Templates**.
- 2 Click **New** to create an entrance template.
- 3 Enter information of the entrance template then click **Add** in **Entrance** part.

The screenshot shows the 'Templates' window with the 'Entrance groups' section. The 'Name' field is highlighted with a red box and contains the text 'EntranceTemplate'. The 'Description' field is empty. Below the fields are buttons for 'Add', 'Change', and 'Del'. At the bottom of the window, there is an 'Entrance' section with an 'Add' button highlighted in red.

- 4 Select the entrance and click **OK**.

The screenshot shows a table with one row selected. The row is highlighted with a red border and contains the text 'EntranceDoor'. The table has columns for 'Name', 'Location', 'Description', 'Automatic lo...', 'Automatic u...', 'Toggle sche...', and 'Verification ...'. At the bottom of the window, there are buttons for 'Print...', 'To file...', 'Cancel', and 'OK', with 'OK' highlighted in red.

- 5 Select the schedule for entrance template and click **OK**.

The screenshot shows a dialog box with the 'Entrance name' field set to 'EntranceDoor' and the 'Schedule' dropdown menu set to 'WorkingTimes'. There is a 'Cancel' button and a 'WorkingTimes' button highlighted in blue.

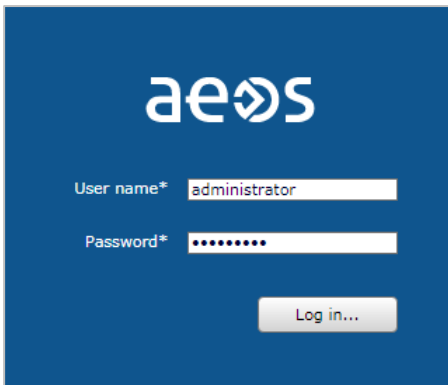
- 6 Click **OK** to complete creating an entrance template.

The screenshot shows the 'Entrance' window with a table containing one row. The row is highlighted with a red border and contains the text 'EntranceDoor' and 'WorkingTimes'. The table has columns for 'Name', 'Description', 'Schedule', and 'Location'. At the bottom of the window, there are buttons for 'Add', 'Change', 'Del', 'Cancel', and 'OK', with 'OK' highlighted in red.

Enrolling a fingerprint

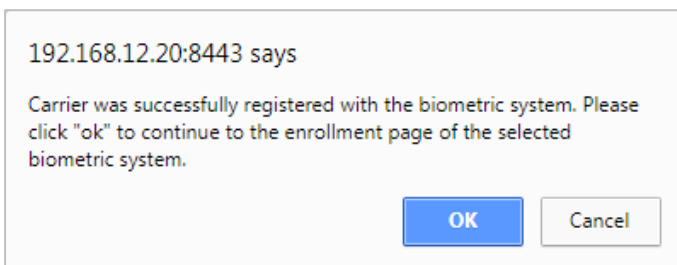
Once you have configured BioStar Integration for Nedap, you can enroll and manage fingerprints of user on the AEOS platform.

- 1 Run **AEOS** and then log in as an administrator account.

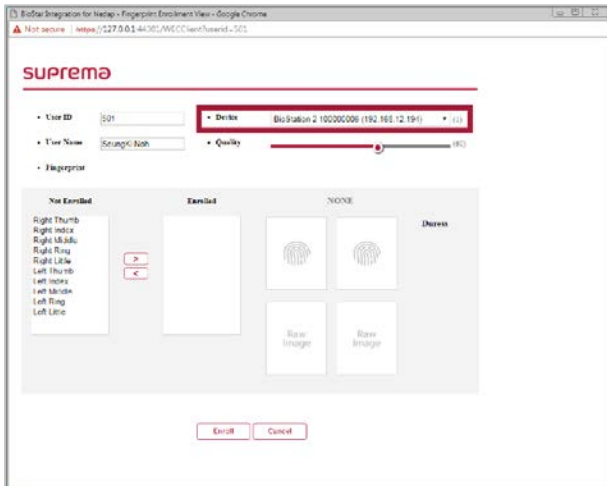


- 2 Click **Person > Announce**.
- 3 Enter the information of the employee to enroll the fingerprint and set **Contact, Authorization, Identification** and **Verification**, then click **>>**.

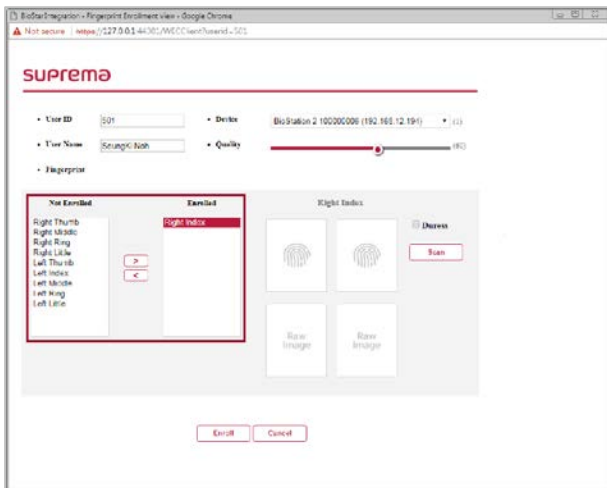
- 4 When the pop up window appears, read the notice and click **OK**.



5 Select the device to enroll the fingerprint.



6 Select the finger to enroll the fingerprint in the **Not Enrolled** list and click . When the selected item appears in the **Enrolled** list, press **Scan**.



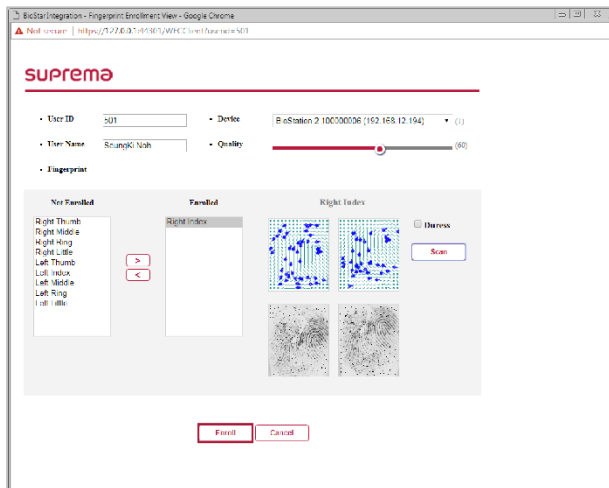
7 When a message saying "Please place the finger on the sensor." is displayed on the page, place the finger with the fingerprint you wish to enroll on the fingerprint authentication unit of the device and press the finger gently for better authentication.

8 When the re-input screen is displayed on the device after a beep sound, scan the fingerprint of the enrolled finger again (scan the fingerprint of a finger to be enrolled twice).

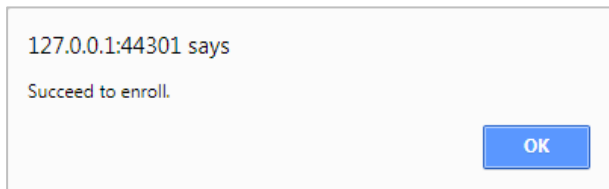
NOTE

- For more information on fingerprint enrollment, refer to the manual for the Suprema biometric device.


9 When the scan is complete, click **Enroll**.



10 When the pop up window appears, read the notice and click **OK**.



NOTE

- To delete an enrolled fingerprint: In the **Enrolled** frame, select the fingerprint you want to delete and click . When you click the **Enroll**, the fingerprint will be deleted.

Troubleshooting

When BioStar Integration for Nedap web service does not work normally

- Make sure the database (BioStarIntegration.sqlite) is in the correct path. If the database has been deleted, delete **BioStarIntegration.DbServerConfig.ini** file and rerun the server to create a new database.
- Check the version of OpenSSL installed. OpenSSL version 1.0.2l or later that supports the TLS 1.2 protocol must be installed.

When the device can not connected to BioStar Integration for Nedap web service

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

Appendices

- Identifier type of Identification is supported only for NedapTest, test type, Suprema, CSN, Secure, Access, and Wiegand. Supported Identifier types can be updated at a later date.
- If you delete the **BioStar Integration.DbServerConfig.ini** configuration file, a new database will be created.
- The path of the configuration file is shown below.
 - Configuration file: (C:\Windows\ BioStar Integration.DbServerConfig.ini, BioStar Integration.WebServerConfig.ini)
 - Database: (C:\ProgramData\Suprema\BioStarIntegration\db\BioStarIntegration.sqlite)
- Configuration files and databases are not deleted through the Uninstaller of BioStar Integration for Nedap.



suprema
BIOMETRICS & SECURITY

Suprema Inc.

16F 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@supremainc.com

©2018 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.