IXM WEB Integration with AEOS by Nedap

Installation Instructions

V6.0

Table of Contents

List of Figures

List of Tables

1. Introduction

Purpose

This document outlines the process of configuring the software integration between Nedap's AEOS and Invixium's IXM WEB.

Description

IXM Link, a licensed module in IXM WEB, is required to synchronize the user database between IXM WEB (where biometric enrollment for users is performed) and Nedap AEOS Software (where access rules for the users and the organization are managed).

Note: To activate IXM Link within IXM WEB, the installer must contact Invixium Support at support@invixium.com to obtain the activation key.

The following sections will describe how to set up and configure IXM Link to keep IXM WEB users in sync with AEOS by using "Web Service" to import and export cardholders.

Acronyms

Acronym	Description
IXM	Invixium

Field Mappings

The following are the Nedap AEOS fields that are mapped to IXM WEB

Nedap AEOS Field	IXM WEB Field	Notes
First name	First Name	
Last name	Last Name	
Identifier (Identification)	Number (Card)	This is mandatory for adding users to Nedap AEOS from IXM WEB.
Identifier Type (Identification)	Card Type (Card)	
Status (Identification)	Status (Card)	Cards with the status “In Use” and “Replacement” in Nedap AEOS are only synchronized to IXM WEB as “Active Card”. In the case of other statuses, card status will sync as “Inactive” in IXM WEB.
Photo	Photo	
Date from	Start Date Time	Default time will be considered as 00:00:00
Date until	End Date Time	Default time will be considered as 23:59:00 The employee is marked as suspended if the date of import is greater than the “Date until” of the employee. At the end of the day at 00:00, the existing employee gets suspended.
Template	Employee Group/ Device Group/ Sync Group	Setting the flag “Map Template to User Group” to YES in configuration will create an Employee Group, Device Group, and Sync Group in IXM WEB. Further, employees imported with respective Template from AEOS will be added automatically to the Employee Group in IXM WEB. Only Template entity mapped with IXM WEB Entrance Group and Entrance will not be considered.

Note: Multiple Cards – Nedap AEOS can have multiple identifiers (cards) per person, and IXM WEB supports a maximum of 10 cards per employee.

2. Compatibility

Invixium Readers

TITAN	TFACE	TOUCH2	SENSE2	MERGE2	MYCRO
All models	All models	All models	All models	All models	All models

Software Requirements

Application	**Version**
Nedap AEOS	2023.1
Invixium IXM WEB	3.0.36.0
Operating Systems	Windows 10 Professional Version Windows 11 Pro Windows Server 2016 Standard Windows Server 2019
Microsoft .NET Framework	.NET Framework 4.8
Database Engine	SQL Server 2014 or higher
Internet Information Services (IIS)	Microsoft® Internet Information Services version 10.0
Web Browser	Google Chrome Mozilla Firefox Microsoft Edge (Internet Explorer not recommended)

Other Requirements

Server	2.4 GHz Intel Pentium or higher
RAM	8 GB or higher
Networking	10/100Mbps Ethernet connections

Note: Server requirements mentioned are ideal for small to medium business installations. For large enterprise installation server requirements, contact support@invixium.com.

Compatibility Matrix for IXM WEB & Nedap AEOS Integration:

IXM WEB version	Nedap AEOS version	Compatible
IXM WEB 2.2.224.0	2021.1	Yes
IXM WEB 2.2.230.0	2021.1	Yes
IXM WEB 2.2.252.0	2021.1	Yes
IXM WEB 2.2.330.0	2021.1	Yes
IXM WEB 2.3.2.0	2021.1	Yes
IXM WEB 2.3.12.0	2023.1	Yes
IXM WEB 3.0.36.0	2023.1	Yes

Table 1: Compatibility Matrix for IXM WEB & Nedap AEOS

3. Checklist

Item List	Interface
Prerequisites for IXM WEB Installation	Invixium
Installation of IXM WEB	Invixium
Email Configuration in IXM WEB	Invixium
IXM WEB and IXM Link Activation	Invixium
Configure IXM Link for Nedap AEOS	Invixium
Creation of System Users in IXM WEB for Enrollment	Invixium
Configure Invixium Readers	Invixium
Add an Invixium Device to a Device Group	Invixium
Face, Fingerprint or Finger Vein Enrollment	Nedap AEOS
Prerequisites for Getting Access in Nedap AEOS	Nedap AEOS
OSDP Configuration	Invixium & Nedap AEOS
DIP Configuration	Invixium & Nedap AEOS
Wiegand Configuration	Invixium & Nedap AEOS

4. Task List Summary

Task	IXM WEB Application Task List	Nedap AEOS Task List
1	Activate IXM WEB and IXM Link for Nedap AEOS	Enroll biometrics (face, fingerprint, finger vein) from Nedap AEOS
2	Configure IXM Link for Nedap AEOS	Mandatory configurations for getting access in Nedap AEOS
3	Add new System Users in IXM WEB for enrollment	OSDP / DIP / Wiegand Configurations in AEOS and AEmon
4	Register IXM Devices and configure settings as per the requirement	
5	Configure OSDP settings on the device for integration with the Access Panel	
6	Configure DIP settings on the device for integration with the Access Panel	
7	Configure Wiegand settings on the device for integration with the Access Panel	

Table 2: Task List Summary

5. Prerequisites for AEOS and IXM WEB Integration

Enable Soap WebService

Procedure

STEP 1

From the AEOS menu bar, go to **Administration** → **Maintenance** →**Settings.**

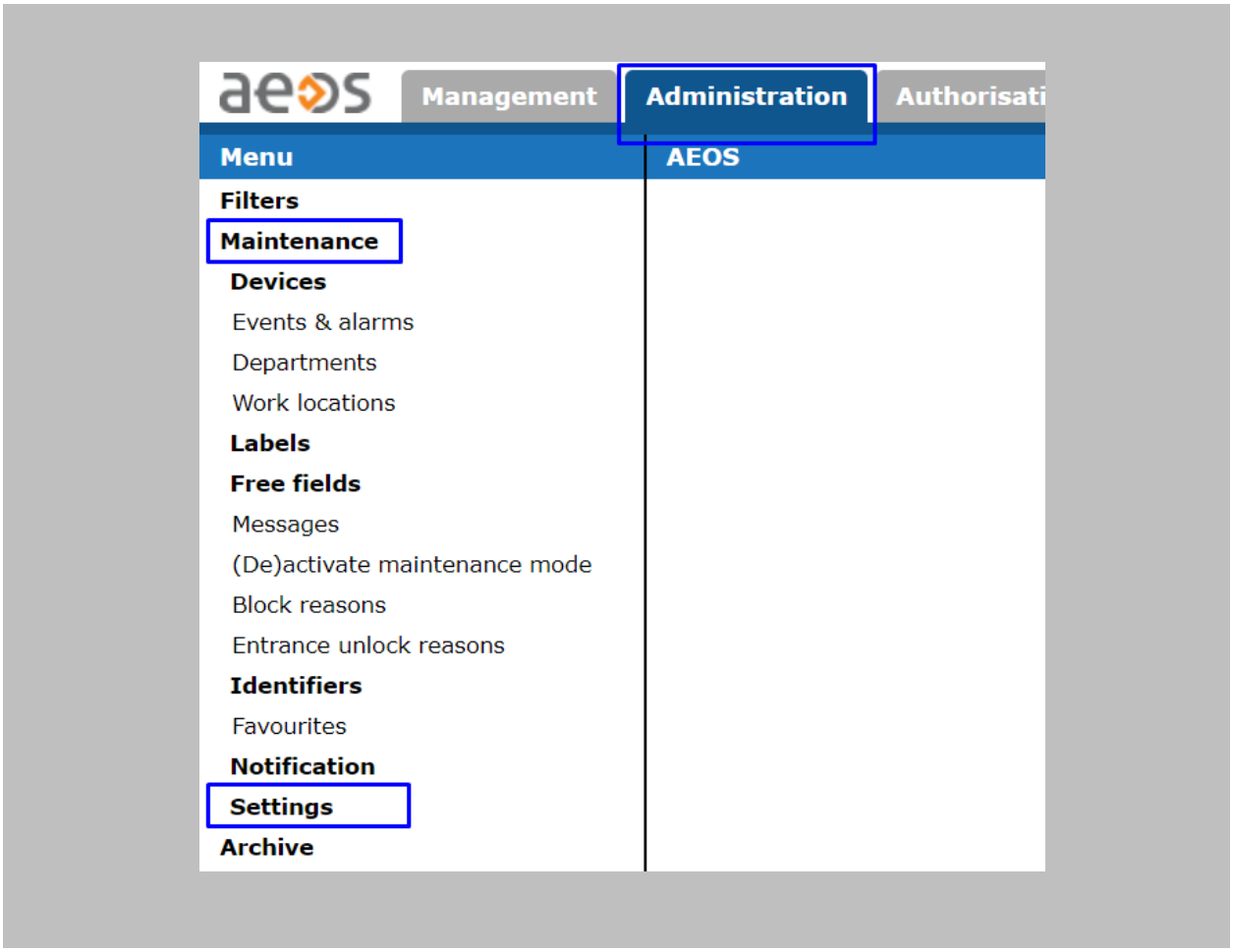


Figure 1: AEOS - Settings

STEP 2

Click on **System Properties.**

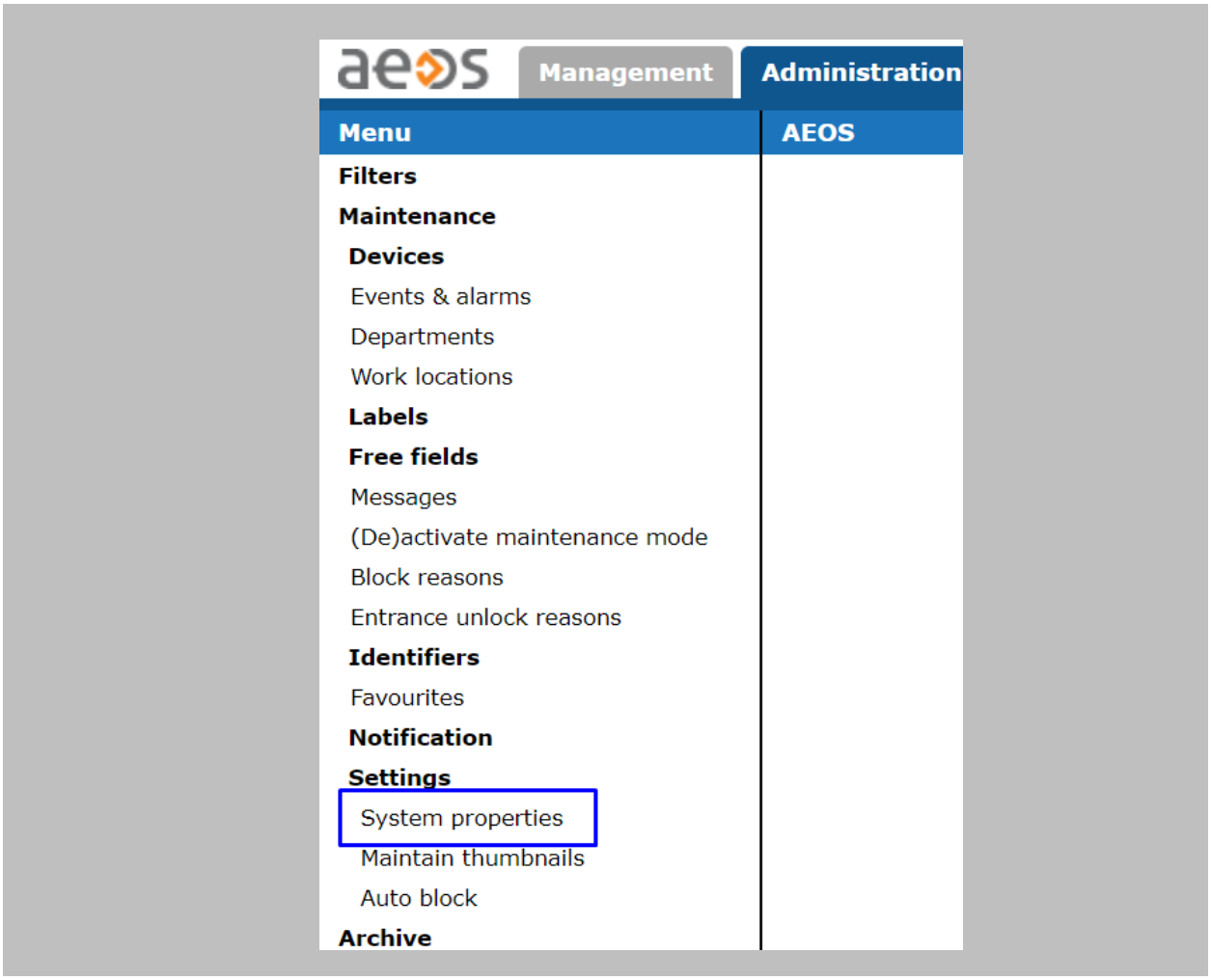
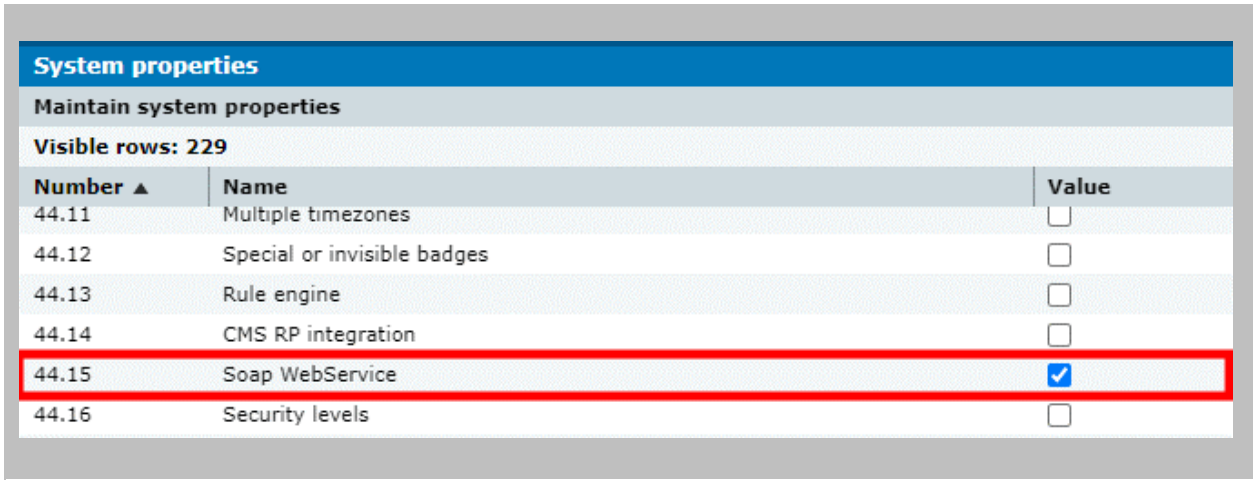


Figure 2: AEOS – System Properties

STEP 3

Select the checkbox “Soap WebService” to enable the service.



System properties

Maintain system properties

Visible rows: 229

Number ▲	Name	Value
44.11	Multiple timezones	☐
44.12	Special or invisible badges	☐
44.13	Rule engine	☐
44.14	CMS RP integration	☐
44.15	Soap WebService	☑
44.16	Security levels	☐

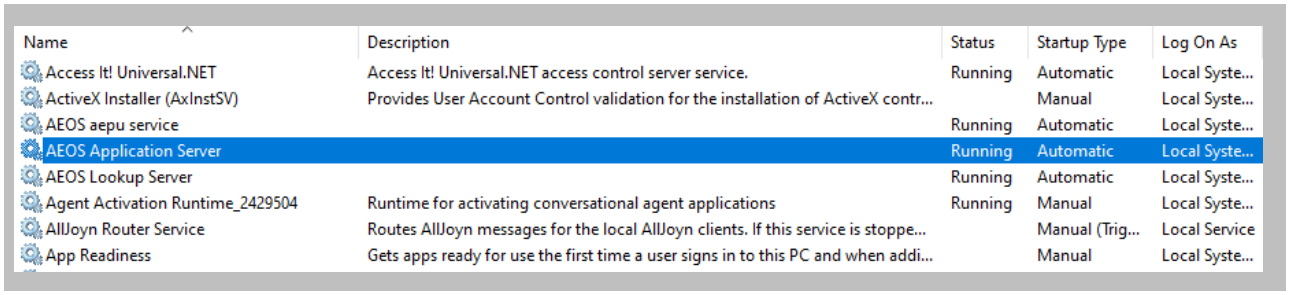
Figure 3: System Properties – Soap WebService

STEP 4

Click on **OK.**

STEP 5

Once saved, restart the service. Once the service starts, wait for 5 minutes to make the application up and running.



Name	Description	Status	Startup Type	Log On As
Access It! Universal.NET	Access It! Universal.NET access control server service.	Running	Automatic	Local Syste...
ActiveX Installer (AxInstSV)	Provides User Account Control validation for the installation of ActiveX contr...		Manual	Local Syste...
AEOS aepu service		Running	Automatic	Local Syste...
AEOS Application Server		Running	Automatic	Local Syste...
AEOS Lookup Server		Running	Automatic	Local Syste...
Agent Activation Runtime_2429504	Runtime for activating conversational agent applications	Running	Manual	Local Syste...
AllJoyn Router Service	Routes AllJoyn messages for the local AllJoyn clients. If this service is stoppe...		Manual (Trig...	Local Service
App Readiness	Gets apps ready for use the first time a user signs in to this PC and when addi...		Manual	Local Syste...

Figure 4: AEOS Application Server

6. Prerequisites for Installing Invixium IXM WEB Software

Getting IXM WEB activation key

Procedure

Complete the online form to receive instructions on how to download IXM WEB: https://www.invixium.com/download-ixm-web/

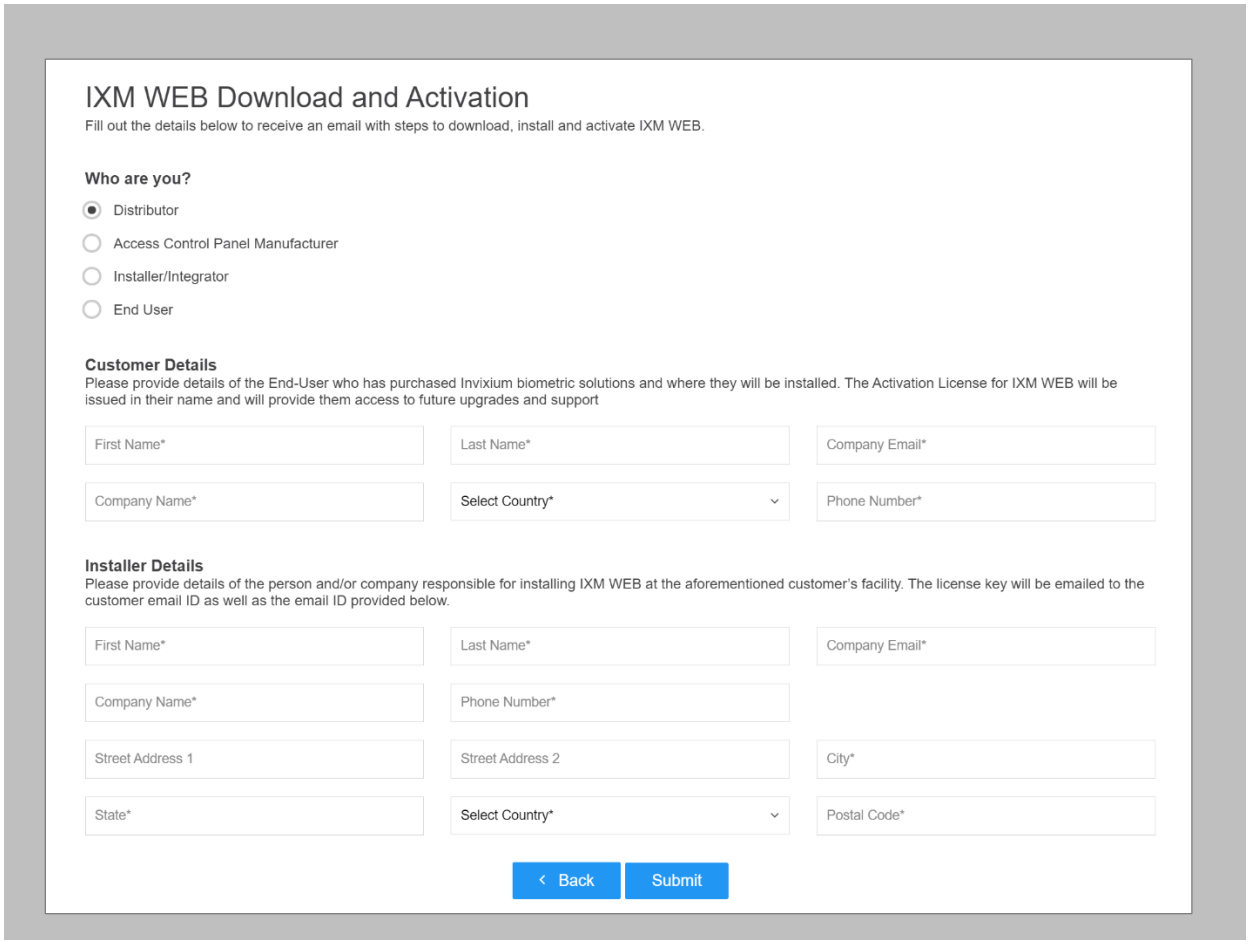


Figure 5: IXM WEB Online Request Form

After submitting the completed form, an email will be sent with instructions from support@invixium.com to the email ID specified in the form.

Please ensure to check the spam or junk folder.

See below for a sample email that includes instructions on how to download and install IXM WEB along with your Activation ID.

Dear [redacted]

Get the latest IXM WEB package from the link below. Depending on your internet speed, the download will take approximately 15 minutes.

Important:

1. Do not update if you are using IXM SDKs, a custom firmware or a custom IXM WEB version. Contact IXM Support for more details.

2. After updating IXM WEB, make sure all devices are first updated to the latest firmware before enrolment, configuration or changing settings.

3. For existing TITAN or TFACE users, this update of IXM WEB requires temporary internet connectivity to access Invixium servers for license validation. If connecting to the internet is not possible at your premises, contact IXM Support for help.

4. For new customers, Microsoft SQL version 2014 will be installed along with IXM WEB 2.2. For existing customers, please upgrade to Microsoft SQL 2014 or higher before upgrading IXM WEB.

IXM WEB 2.3.0.0 package

Activation ID: LW-D4-G6-[redacted]

Follow these steps to install or update IXM WEB:

1. Download the IXM WEB package.
2. Extract the compressed files and copy IXM WEB.exe to required server.
3. Install IXM WEB, open and create a login

New IXM WEB installations require Activation. To activate IXM WEB, first open and create a login and then follow these steps:

1. Online Activation (Recommended) – Requires an active internet connection.
   - Go to Left Navigation Menu → LICENSE → IXM WEB.
   - Select "Online" as activation Type. Enter your Activation ID and Click "activate".
   - Your Activation ID will be validated automatically and IXM WEB will be ready for use.
2. Offline Activation - For servers that are offline.
   - Go to Left Navigation Menu → LICENSE → IXM WEB.
   - Select "Offline" as Activation Type. Enter your Activation ID and Click "request".
   - Copy the details that pop up and email them to support@invixium.com.
   - Our support team will send you an email with an Activation Key to activate IXM WEB.
   - Once you receive the Activation Key, select the "Offline" as Activation Type and enter the Activation Key. Click Activate to start using IXM WEB.

Enjoy the Experience!

Figure 6: Sample Email After Submitting Online Request Form

Minor Checklist and Considerations

Use these tables to verify that you have conducted all required steps.

Other Minor Checklist	
Windows Updates	Windows Operating system needs to be up to date. System updates should not be pending. If any update is downloaded, you will have to restart the system to complete the Windows update.
User Privileges	The person who is setting up IXM WEB should have full administrator rights

Table 3: System Related Checklist

Port Assignment	**Port**
Inbound HTTP Port	9108
TCP	1433
Port to communicate between IXM WEB & Devices	9734
Inbound Port	1255
Nedap AEOS Port	8444

Table 4: Port Information

7. Installing IXM WEB

Software Installation

STEP 1

Run the IXM WEB installer (Run as administrator), then click **Install**. It will display a popup window to accept the **License Agreement**.

Figure 7: IXM WEB Installer

STEP 2

Click **'Yes'** in the popup window. The IXM WEB installer will start a basic installation process.

STEP 3

By default, IXM WEB performs basic installation and installs software to the default location with the default port number. If the user wants to, they can change the installation path and choose a port number that communicates with the IIS server. Click **Advance**.

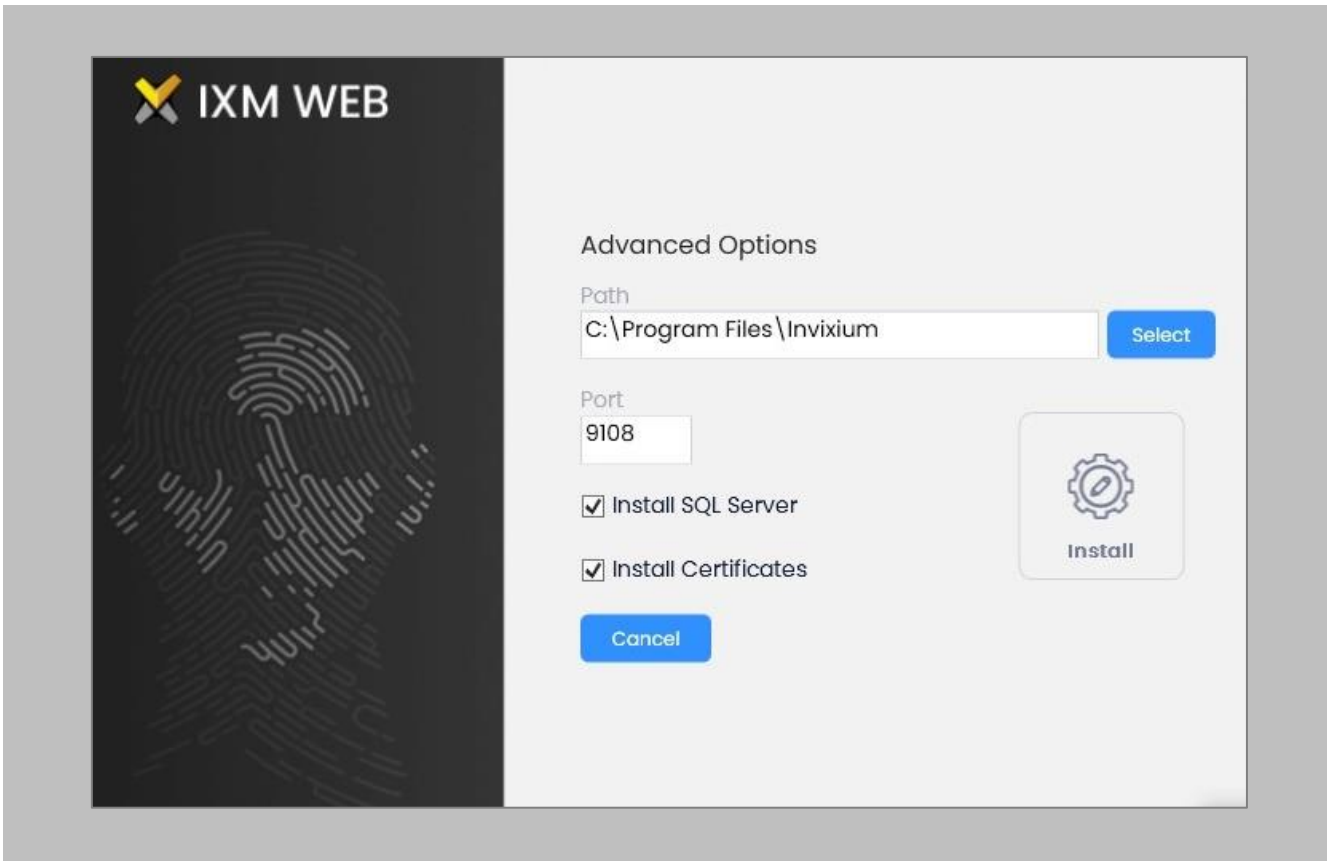


Figure 8: Advanced Option in IXM WEB Installer

STEP 4

In the **Advanced** installation section, the user can change the following options:

- **Installation Path:** In basic installations, the default path is – "***C:\Program Files (x86)\Invixium***". By changing the path, users can determine the new physical path on the machine where the IXM WEB package will be extracted.

- **Port Number:** By default, the port number is "**9108**". Users can change the port number that is generally used to communicate between the WEB Server (Internet Information Services) and IXM WEB.

- **Install SQL Server:** By default, this field is always selected. It means that IXM WEB will install **SQL Server 2014 Express Edition** along with the IXM WEB application. Users can uncheck this field if any other version of SQL Server will be used or if a different machine will be used as a Database Server.

- **Install Certificates:** By default, the IXM WEB installer installs all the necessary certificates that are used in SSL communication. It also installs specific certificates used for communication when configured through the cloud. Users can uncheck this field to prevent IXM WEB from installing all the necessary certificates. Invixium does not recommend deselecting this field.

STEP 5

Once the user completes the changes, click **Install**. IXM WEB packages will continue to install on the machine, and it will display the progress when any component is installed in the background.

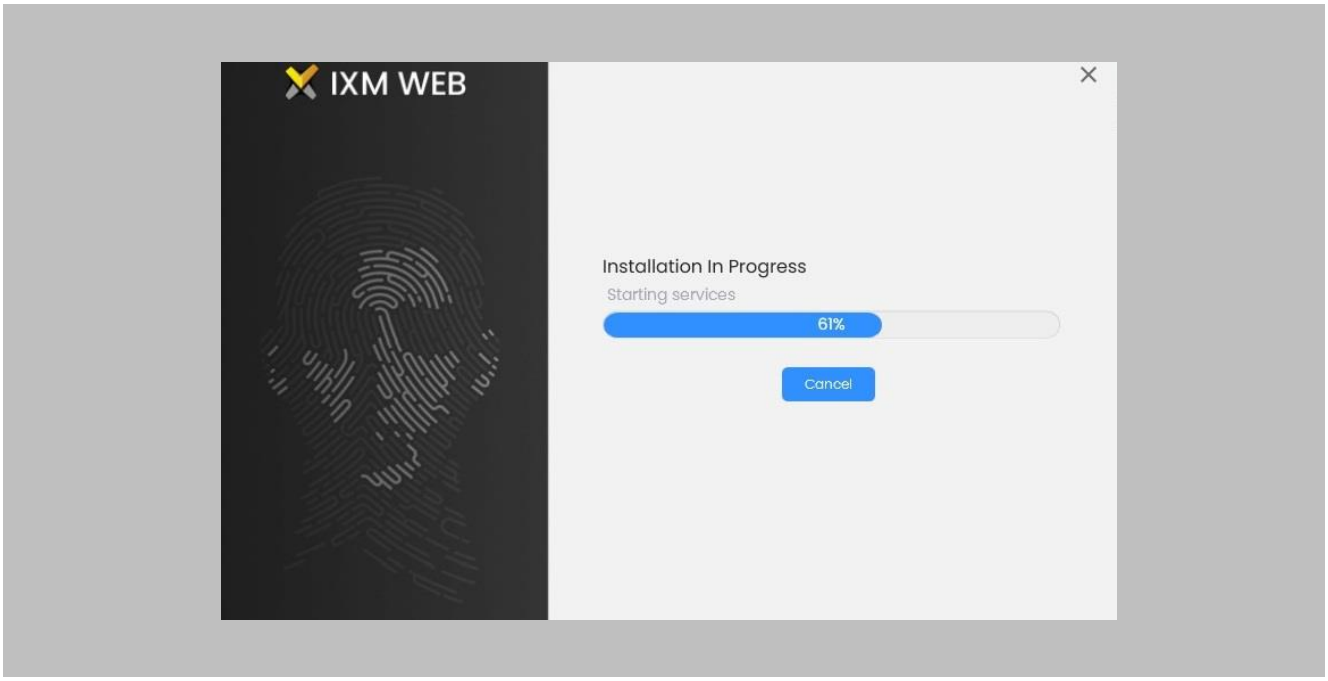


Figure 9: IXM WEB Installation

STEP 6

Once the installation process completes, the user can click **Complete** to finish.

Figure 10: IXM WEB Installation Completed

STEP 7

The IXM WEB package will create a **shortcut icon** on the desktop after the process.

Figure 11: IXM WEB Icon - Desktop Shortcut

STEP 8

Double click on the shortcut icon from the desktop to open **IXM WEB** in the default browser.
Users can also open a browser and run the IXM WEB application.

STEP 9

IXM WEB will populate the default SQL Server name and SQL Server instance.

STEP 10

If the user wants to configure a database that is installed on another machine, then select the **'SQL Server'** option from the Authentication field. By selecting the **'SQL Server'** option, the user will have to add credentials (SQL User Name and Password) to connect to the Database Server machine.

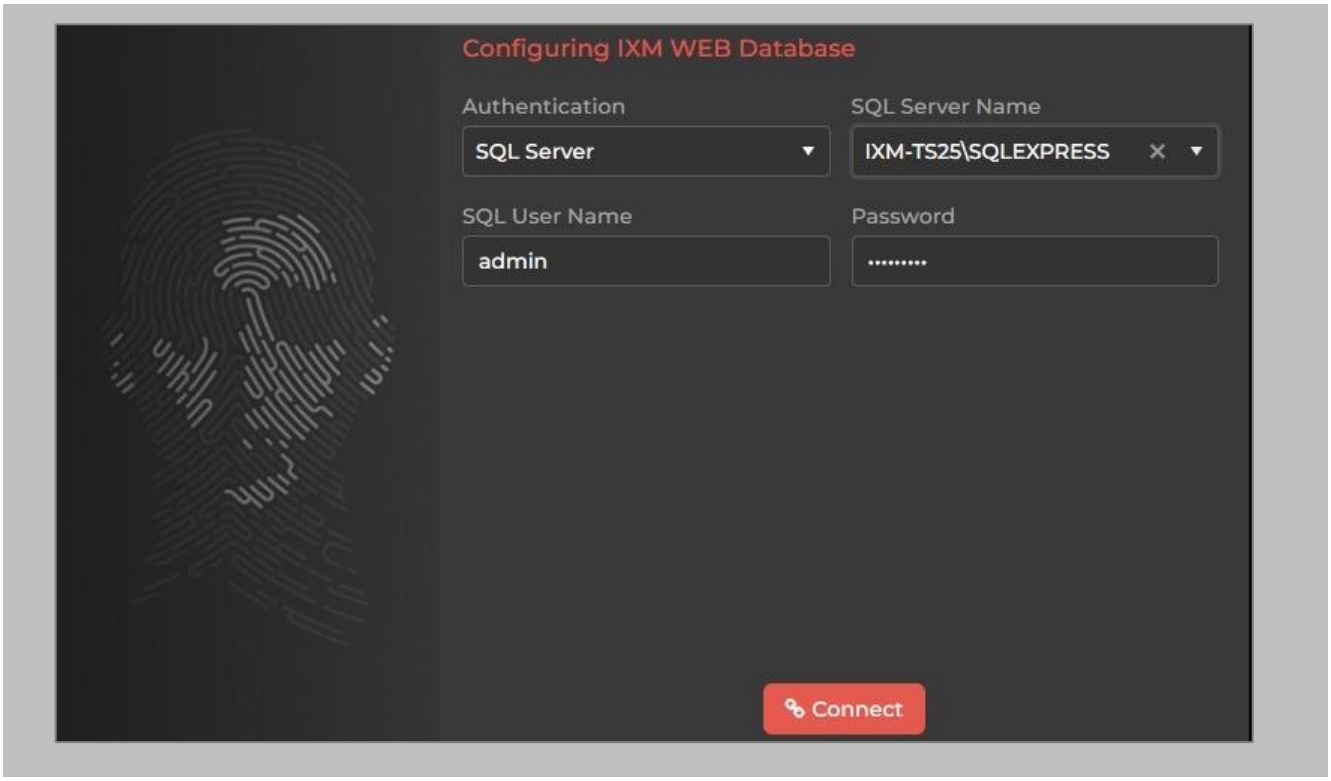


Figure 12: SQL Database Configuration

STEP 11

If a user wants to use the same database instance on the same machine, then click connect to verify if the connection is established with the SQL Instance.

STEP 12

Enter a new **Database** name if there is no previously set up database available.

STEP 13

Click **Next**.

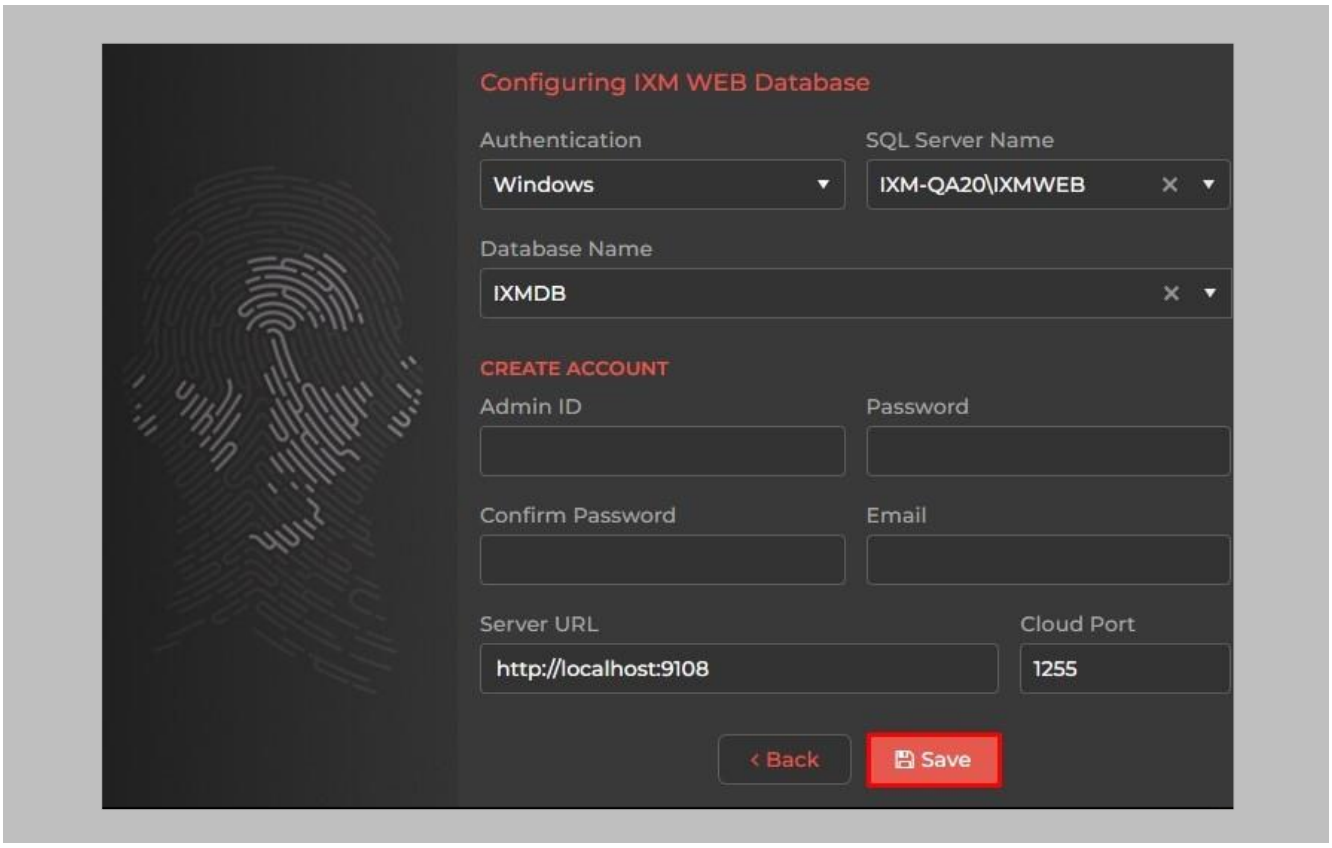


Figure 13: IXM WEB Administrator User Configuration

STEP 11

Users can provide the necessary values to all the fields displayed under the **'Create Account'** section.

STEP 12

The fields and their functions are mentioned below:

- **Invixium ID:** Users can add a username that will have all the rights to access any settings within IXM WEB. This Invixium ID should have a minimum of 5 characters. This Invixium ID configuration will have administrator rights.

- **Password:** The user can set a password. While typing the password, IXM WEB will also display the strength of the entered value to determine how secure the password field is.
- **Confirm Password:** Enter the password value once again. Users need to enter the same password that they entered in the password field.

- **Email:** Set an administrator email address, IXM WEB will use this email address in the future in case the password needs to be reset, or to send any type of email notification.

- **Server URL:** Users can set a Web URL or an IP Address on the machine where IXM WEB is installed along with the port number. By default, the port number is 9108. Format: **http://IP_IXMServer:9108**

- **Cloud Port:** If a user wants to configure the devices over WEB Cloud, then a specific port number needs to be mentioned in the Cloud Port field. By default, the Cloud Port value is 1255.

STEP 13

Once the user is done providing all the values, click **Save**.

STEP 14

Using the provided values, IXM WEB will create a database and, upon success, the user will be redirected to the **Login Page**.

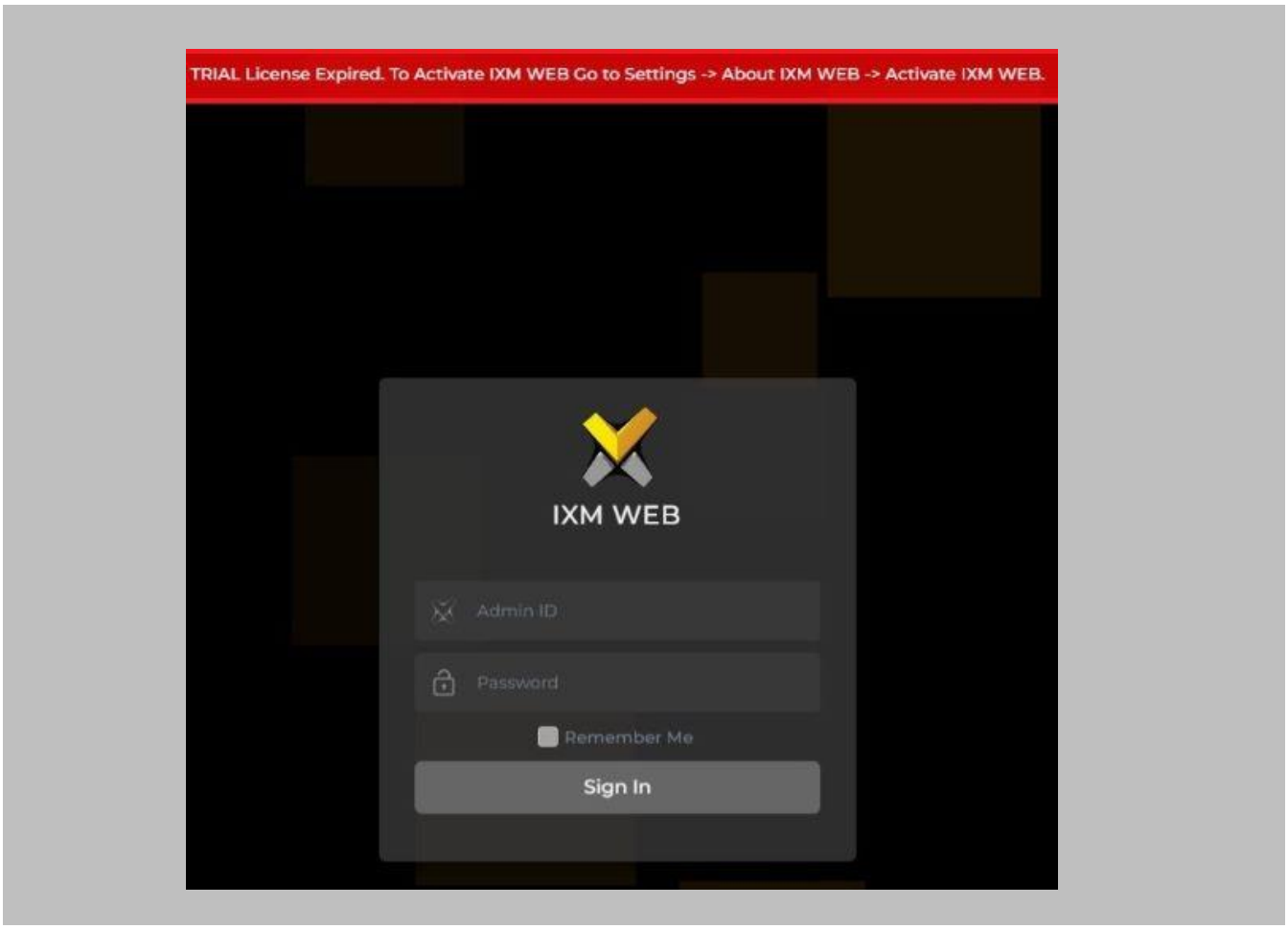


Figure 14: IXM WEB Login Page

Note: During an upgrade of IXM WEB from any previous release to 3.0.36.0, an internet connection is required for license validation. As this new version includes a face algorithm update, it will automatically convert templates without the need for re-enrollment of faces.

8. Configuring Email Settings Using IXM WEB

Configuring email settings is highly recommended as one of the first steps after installing IXM WEB. Email configuration settings will help the admin retrieve the password for IXM WEB in case it is forgotten. Valid email configuration makes activation and license key requests easier.

Email Setting Configuration

Procedure

STEP 1

Login and navigate to **Settings** icon on top right of the page → **System Notifications** → Click on **SMTP Settings.**

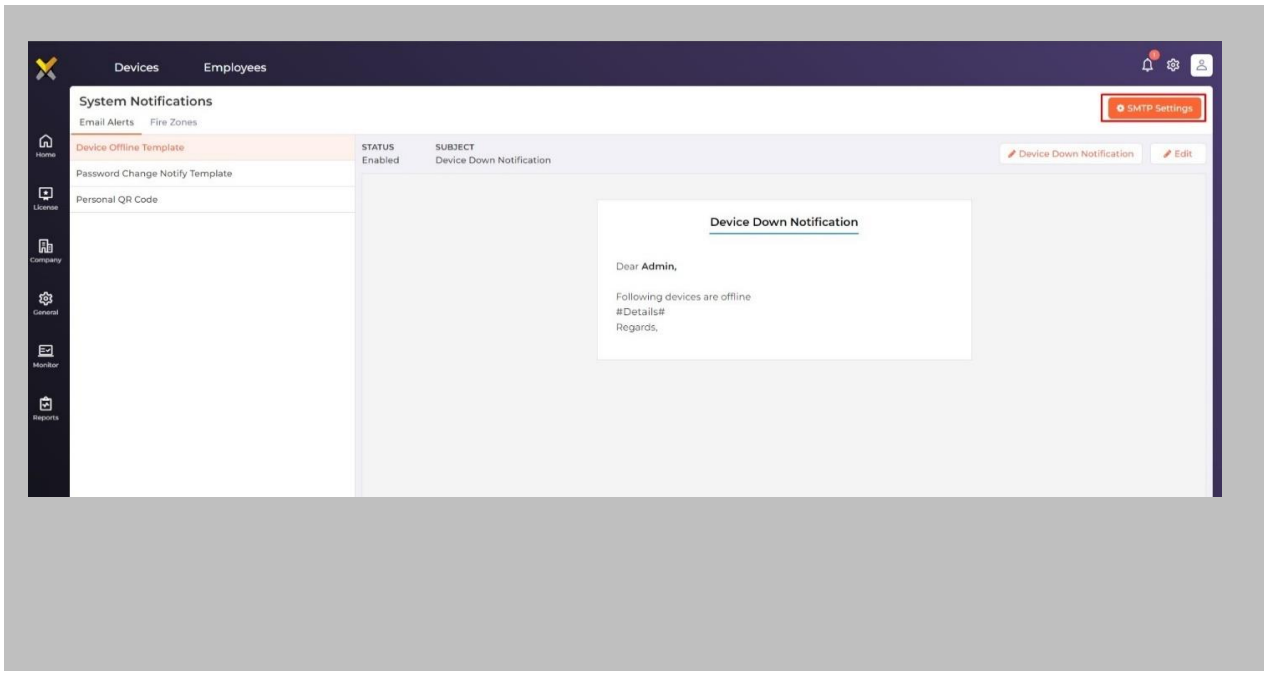


Figure 15: Configure Email

STEP 2

Enable “Status” and enter values for “SMTP Host”, “SMTP Port”, and “Send email message from” fields.

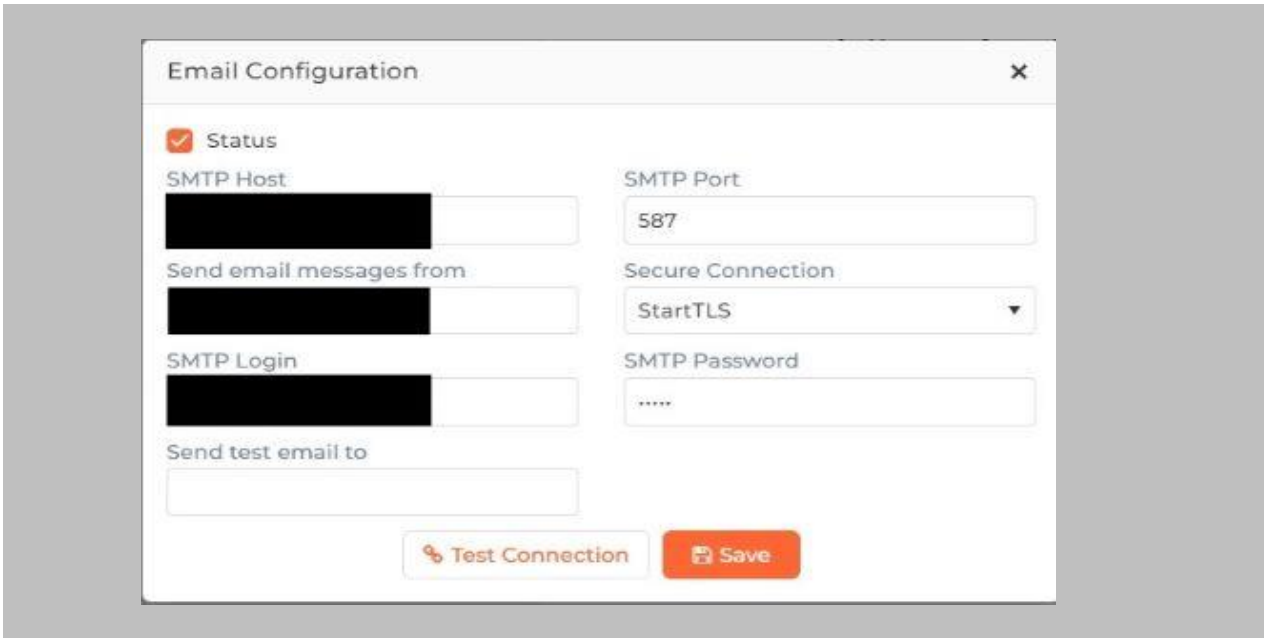


Figure 16: IXM WEB - SMTP Settings

Note: If Gmail/Yahoo/MSN etc. email servers are used for “SMTP Host” then “SMTP Login” and “SMTP Password” values need to be provided. Also in this case, “Secure Connection” needs to be set to either SSL or SSL/StartTLS.

STEP 3

After entering the values, click **Save** to save the SMTP Settings on the IXM WEB database.

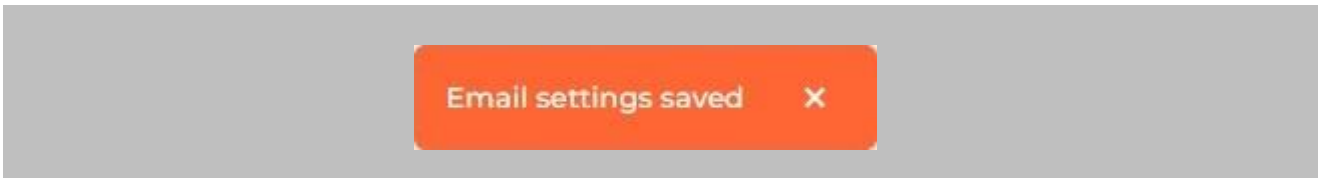


Figure 17: IXM WEB - Save Email Settings

To test the settings, navigate to **Settings** icon on top right of the page → **System Notifications** → Click on **SMTP Settings.** Provide a valid email address under **Send test email to** >> Click the **Test Connection** button.

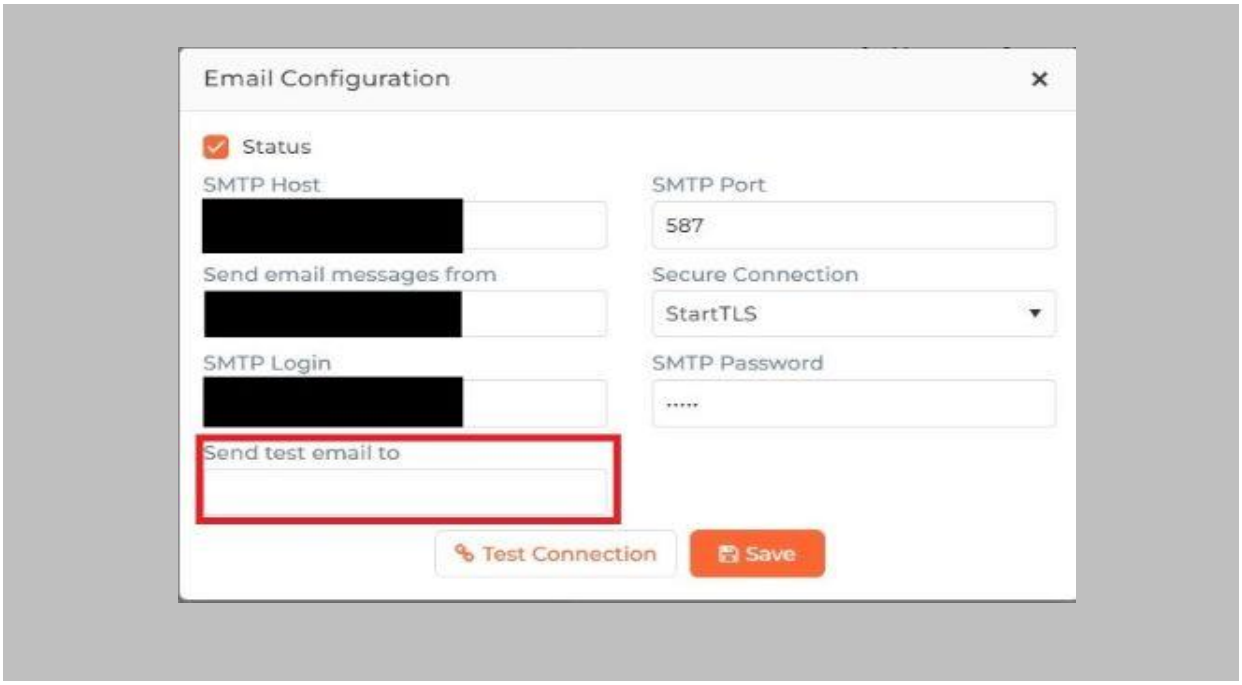


Figure 18: IXM WEB – Test Connection

STEP 4

Once email configuration is completed, a **Forgot password** link will appear on the Sign In page in its place.

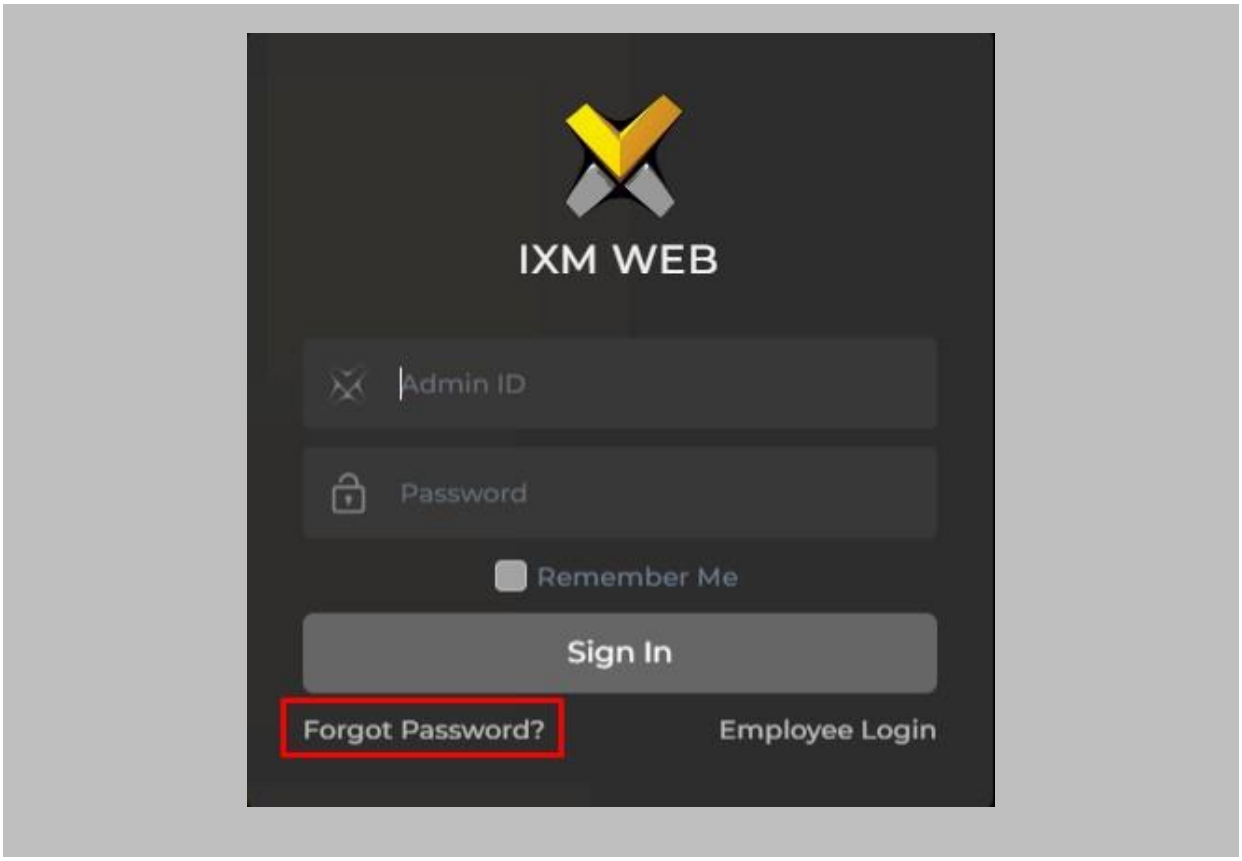


Figure 19: IXM WEB - Forgot Password

9. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

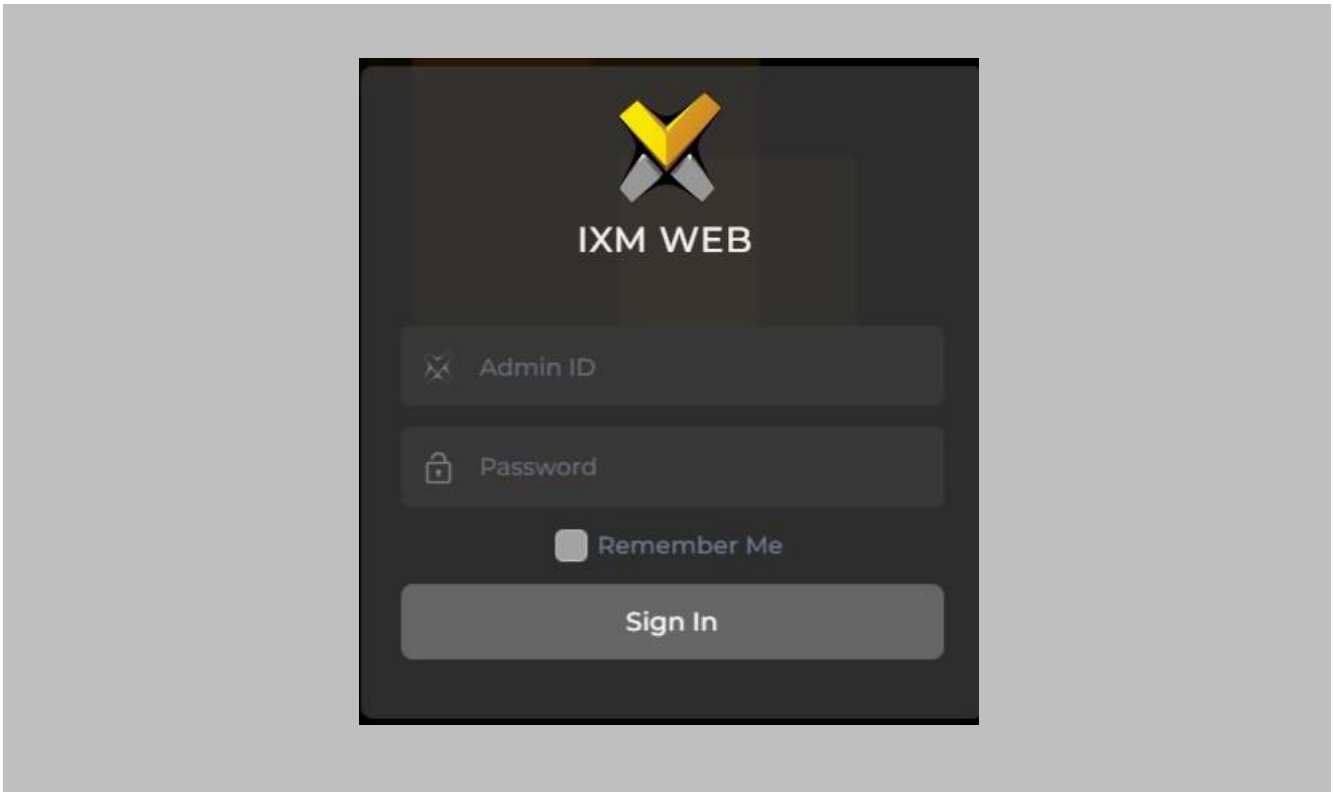


Figure 20: IXM WEB - Enter Login Credentials

STEP 2

Select the **Settings Icon** on top right of page then click **About IXM WEB.**

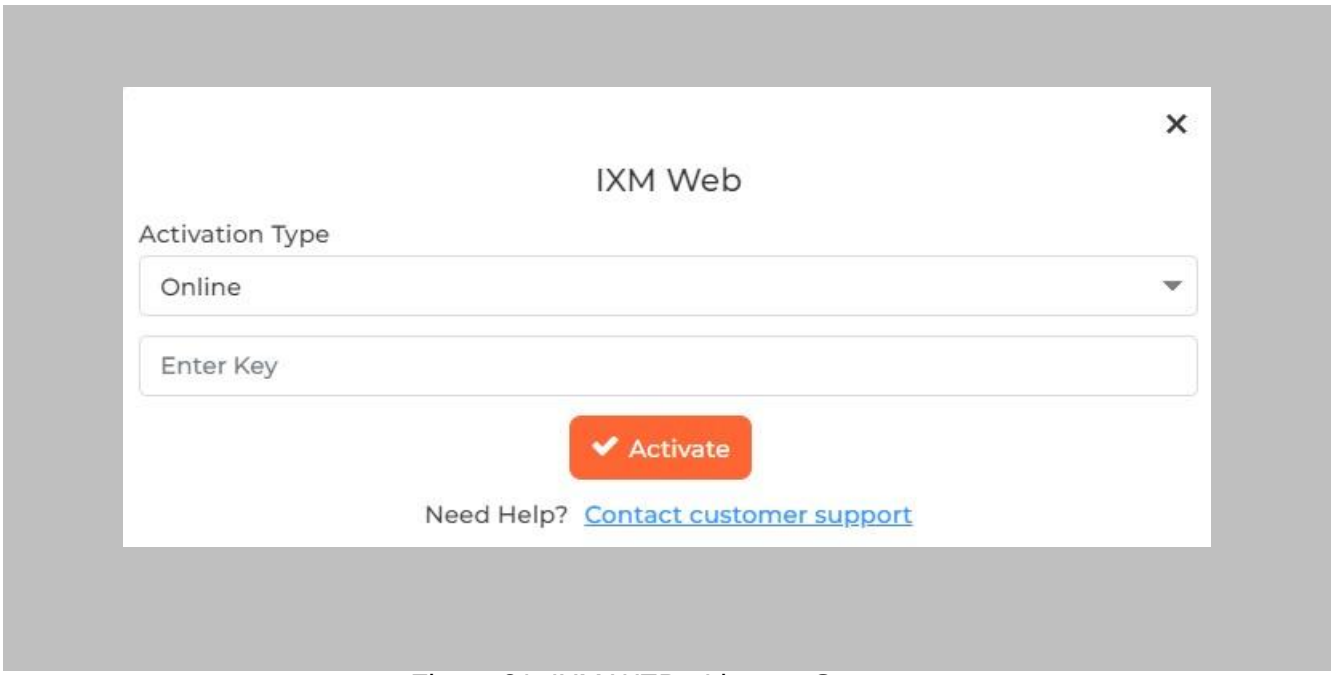


Figure 21: IXM WEB - License Setup

STEP 3

Request **Activation Key Online** or via **Offline Activation Options.**

Note: The Activation ID is in the email received when registering. If online activation fails, check with your local IT as the client may be blocked by your network.

STEP 4

Once the system is activated, the Status will be displayed as **Active**.

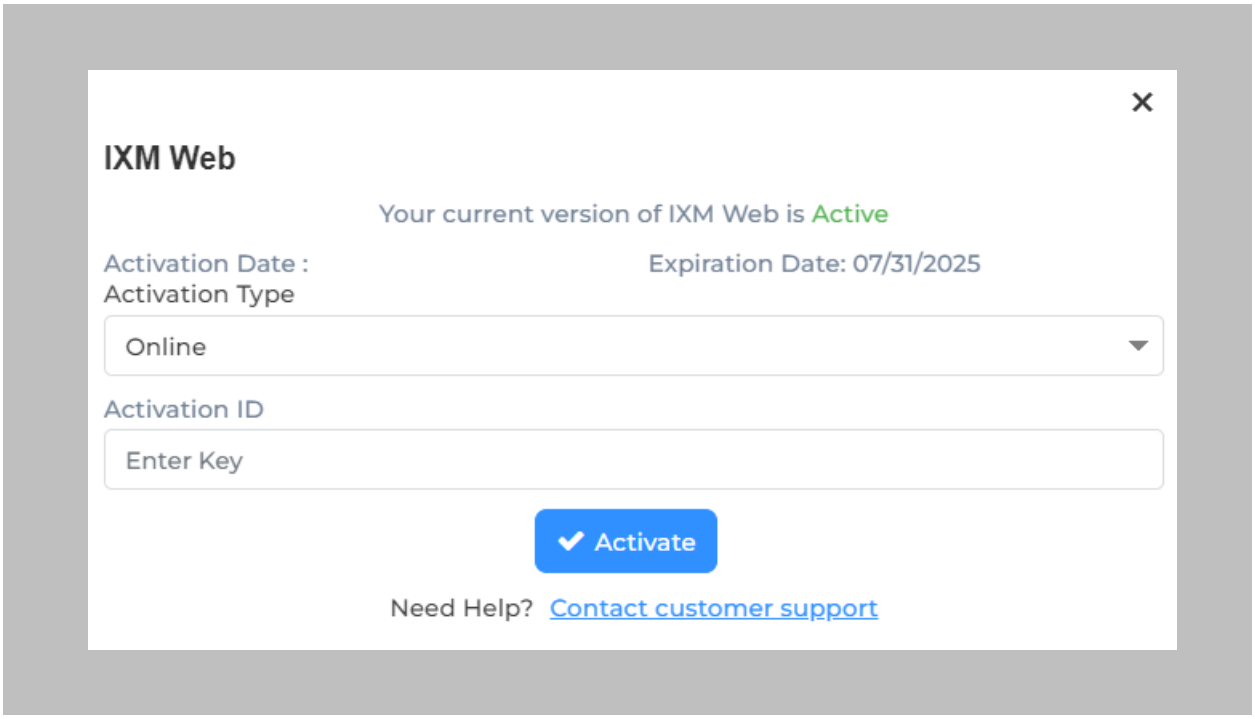


Figure 22: IXM WEB - Online Activation

Nedap AEOS Module Activation

The option to activate a Nedap AEOS License is available under the **License** tab.

STEP 1

Request a **License**.

STEP 2

From **Home**, expand the **Left Navigation Pane**, and go to the **License** tab. Click on **Nedap**

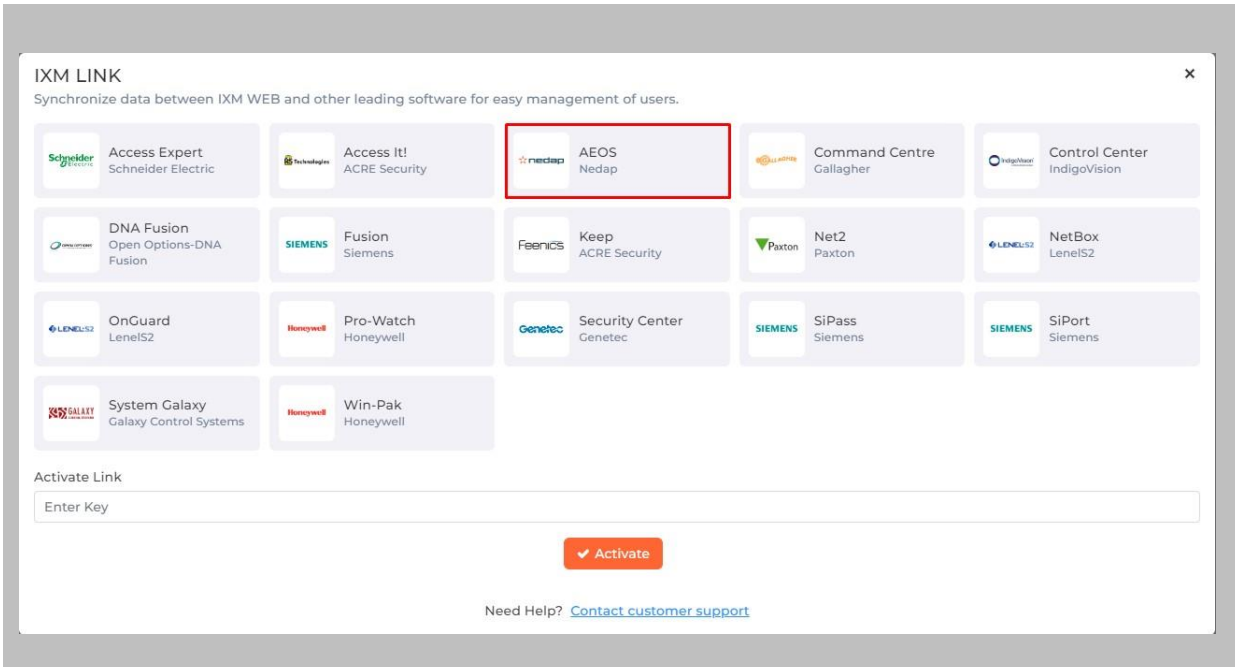


Figure 23: IXM WEB - Nedap Link Activation

STEP 3

You will receive an email from **Invixium Support** having a license key for the Nedap AEOS Activation.

From: Invixium Technical Services [support@invixium.com]
Sent: 14/1/2022 9:27 pm
To: [redacted]
Cc: [redacted]
Subject: IXM Link Activation For Nedap Integration

Dear [redacted]

Thank you for purchasing IXM Link. Your license details are given below:

Access Control Panel: **NEDAP**
Number of devices: **200**
License Key: [redacted]

To activate your IXM Link license, follow these steps:

- Open IXM WEB and login
- Expand **Left Navigation Panel**
- Click **License** tab
- Select the required Access Control Panel manufacturer
- Enter the License Key given above and click **Activate**

IXM Link should be activated and ready to use.

Enjoy the Experience!

For any queries, contact Invixium Technical Services Team.

Best Regards,

Invixium Technical Services Team

Contact US: +1 844 INVIXIUM (468 4948) Email: support@invixium.com
Work Hours: 12:00AM to 5:00PM (Eastern Time) Skype: invixium_support

This email and any attachments may contain confidential and privileged information. If you have received this message in error, please notify us immediately and destroy the material in its entirety, whether electronic or hard copy. Also, please consider the environment before printing this email.

Figure 24: Nedap AEOS License Key Email

STEP 4

Copy and **paste** the License Key in the box provided, and then select **Activate**.

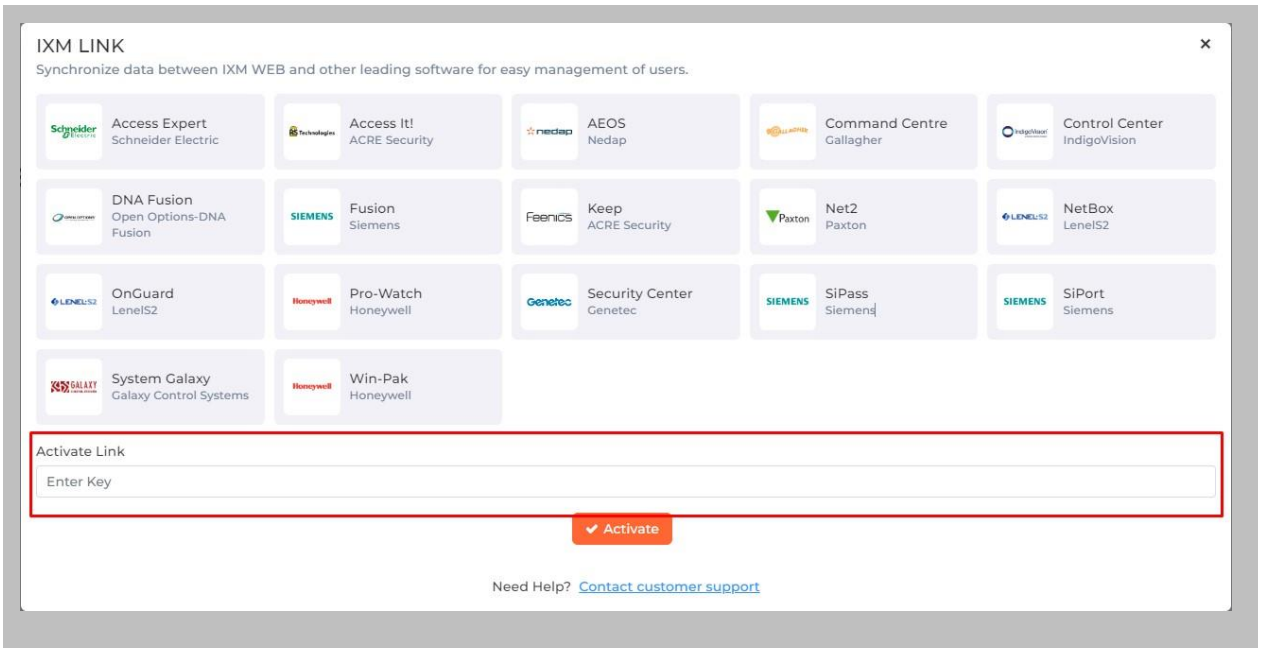


Figure 25: IXM WEB - Activate Nedap AEOS Link License

RESULT

IXM WEB is now licensed for use with Nedap AEOS and configuration can begin.

10. Configuring IXM Link for Nedap AEOS

Procedure

STEP 1

From the Left Navigation Pane → Link → click the AEOS (Nedap) icon.

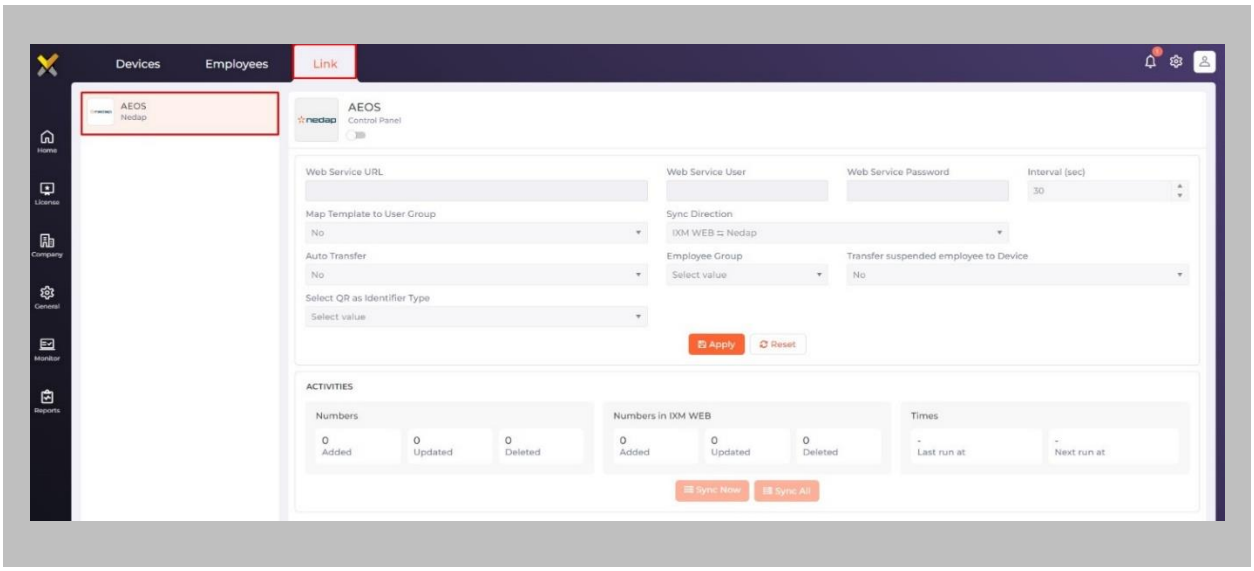


Figure 26: IXM WEB - Link Menu

STEP 2

Toggle the **Status** switch to enable.

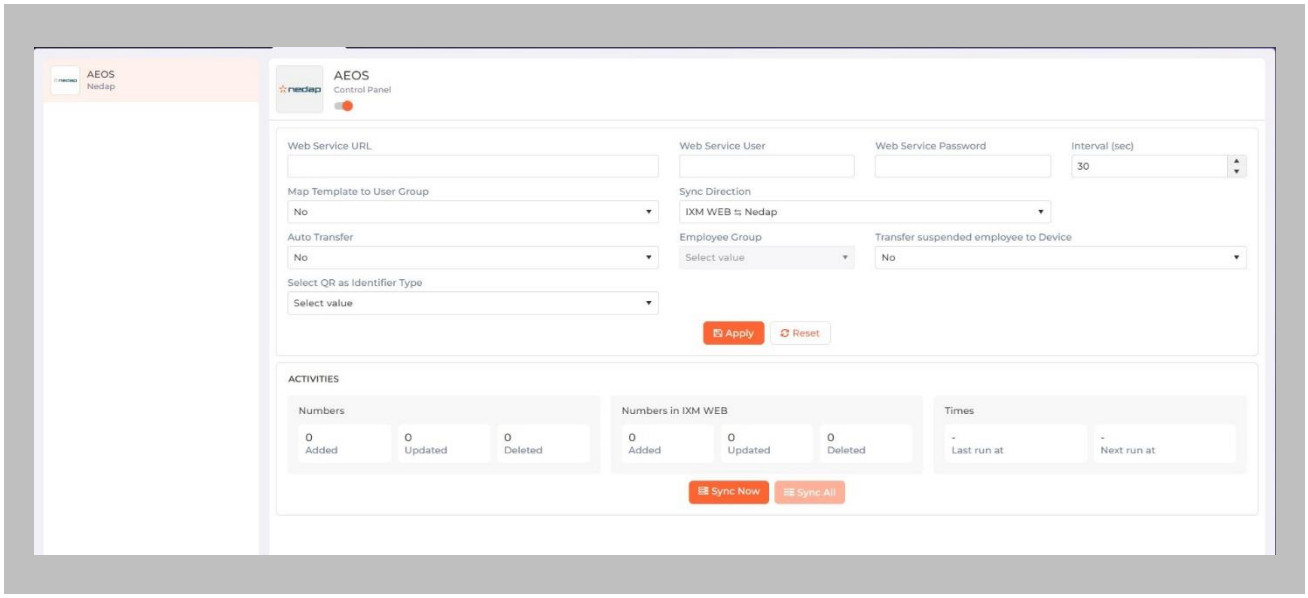


Figure 27: IXM WEB - Enable Nedap AEOS Link Module

Web Service URL:

Enter the **Nedap AEOS WEB Service URL**. For example: **https://172.16.254.40:8444/aeosws**

Web Service User:

Enter the Username to access the web service.

Web Service Password:

Enter the Password to access the web service.

Interval (Sec):

Enter the duration of interval for data transfer between Nedap AEOS and IXM WEB. The system will automatically try to establish connection after every specified interval of time and sync users.

Map Template to User Group:
This option allows to specify whether the Templates should be imported from Nedap AEOS to IXM WEB. The Templates will be imported as Employee Group, Device Group, and Sync Group in IXM WEB.

Click on either 'Yes' or 'No'. By default, 'No' is selected.

No: Templates will not be imported from Nedap AEOS to IXM WEB.

Yes: Templates will be imported from Nedap AEOS to IXM WEB.

Note : Template entity up to 100 characters mapped with IXM WEB Entrance Group and Entrance will not be considered.

Sync Direction:

Click on the field to select the direction of data transfer.

Select one-way sync direction IXM WEB ← Nedap to import a person from Nedap AEOS to IXM WEB.

Figure 28: IXM WEB - Sync Direction

Auto Transfer:

This option provides the facility to add employees into Employee Groups in IXM WEB. For example, if there is an Employee Group called 'Default Group' in IXM WEB, then all the employees from Nedap AEOS will be added directly to the 'Default Group'.

Click on either 'Yes' or 'No'.

No: Employees synchronized from Nedap AEOS will not be added automatically to any of the employee groups present in IXM WEB.

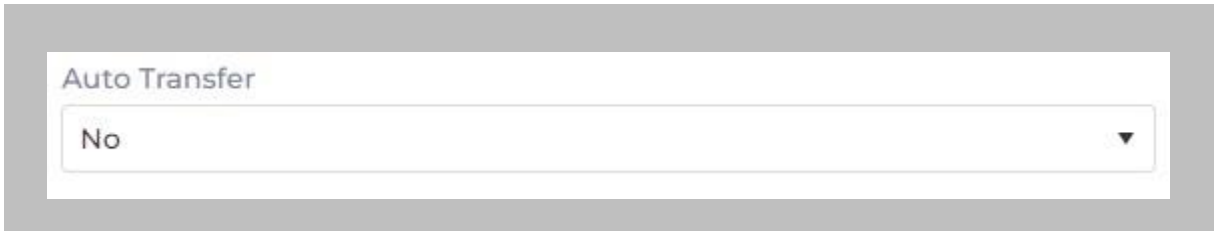


Figure 29: IXM WEB - Auto Transfer No

Yes: Employees synchronized from Nedap AEOS will be added automatically to the selected employee group.

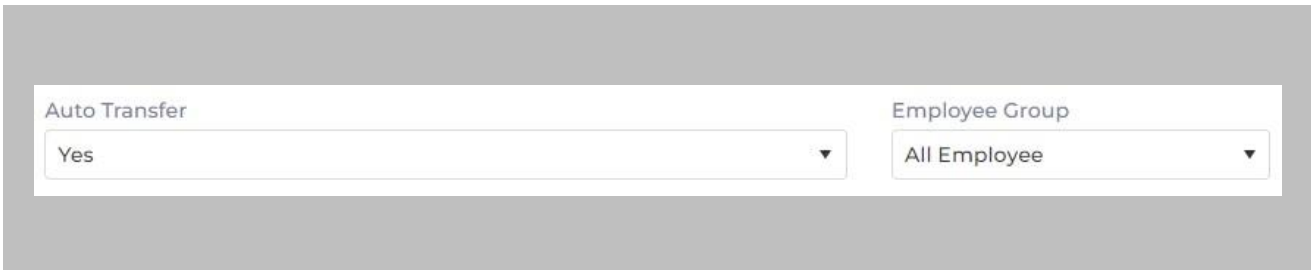


Figure 30: IXM WEB - Auto Transfer Yes

Employee Group:

- This option will be enabled only when 'Auto Transfer' is set as 'Yes'. Otherwise, it will remain disabled.

A list of existing Employee Groups created in IXM WEB is displayed. Click on the Employee Group to which employees should be transferred automatically.

Transfer suspended Employee to device:

This option allows to specify whether the suspended Employees should be transferred from Nedap AEOS to the device. An Employee is considered as "suspended" when their expiry date is no longer valid. While importing Employees, the system will check their joining start date and leaving expiry date. If the current date is greater than the expiry date, the Employee will be marked as suspended.

Click on either 'Yes' or 'No'. By default 'Yes' is selected.

No: Suspended Employees will not be transferred from Nedap AEOS to the device. Instead, all suspended employees currently stored in the device will be removed.

Yes: Suspended Employees will be transferred from Nedap AEOS to the device.

Select Identifier Type as QR:

A list of all Identifier Types available in Nedap AEOS is displayed. By default "Select value" will be displayed.

Select the Identifier Type from the dropdown list to consider cards as QR cards. Cards of Employees belonging to the selected Identifier Type will be converted to QR Cards in the IXM WEB.

Click **Apply.** The transfer of data between Nedap AEOS and IXM WEB is possible only after successful connection.

After applying your changes, you should see items being updated on the screen below:

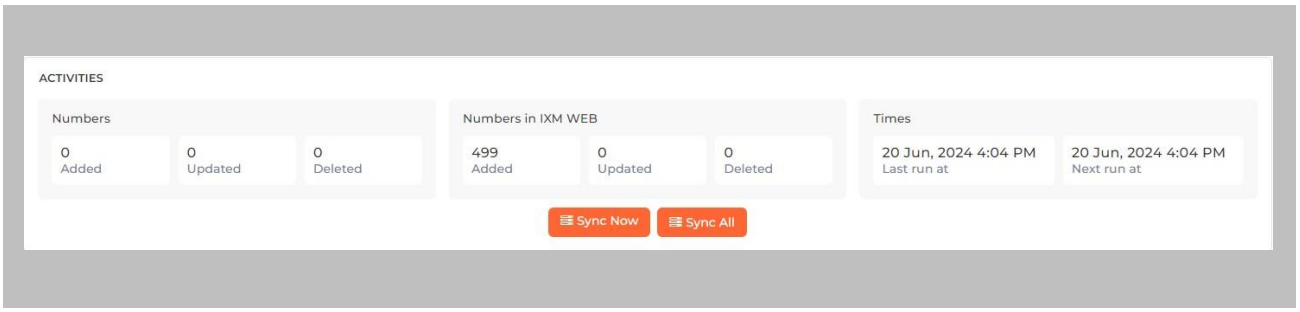


Figure 31: IXM WEB - Sync Activities

Numbers

The first two columns display the number of records added, updated and deleted in Nedap AEOS and IXM WEB respectively after each data transfer.

Times

The last column displays the time when the data was transferred last.

It also shows the time when the data will be transferred next. It is calculated as per the specified Interval.

STEP 3

Clicking **Sync Now** immediately starts synchronizing pending data. This is useful when you do not want to wait until the next scheduled run shown by “Next Run At”.

STEP 4

The **Sync All** feature allows a re-sync of the database from Nedap AEOS to IXM WEB. This will re-import missing cardholders or updated cardholders from Nedap AEOS to IXM WEB. Also, it will delete IXM WEB employee records according to cardholders available in Nedap AEOS.

- The **Sync All** button will be visible only when the sync direction is selected as Nedap AEOS to IXM WEB (One-way sync).

RESULT

When data is synchronizing at the given interval, the numbers in view will change accordingly.

11. Configuring Events in Nedap AEOS

Prerequisite

To send events from a device to Nedap AEOS, it is essential to install the Virtual AEPU (Access Event Processing Unit) beforehand.

Install Virtual AEPU (Access Event Processing Unit)

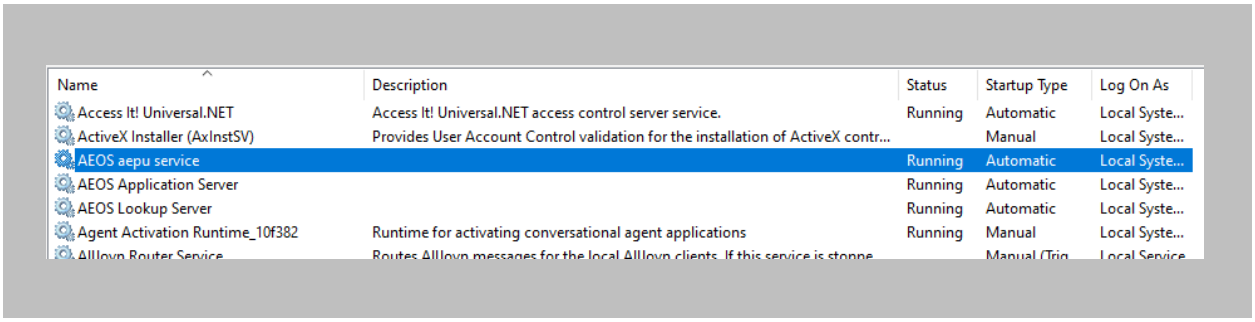
Procedure

STEP 1

Navigate to the **setup folder** → **Additional Programs** → **Virtual AEpu** and execute the file named “setup_aepu_” + <version number> to install the Virtual AEPU.

STEP 2

Confirm successful installation by checking the service from Windows Services (Services.msc).



Name	Description	Status	Startup Type	Log On As
Access It! Universal.NET	Access It! Universal.NET access control server service.	Running	Automatic	Local Syste...
ActiveX Installer (AxInstSV)	Provides User Account Control validation for the installation of ActiveX contr...		Manual	Local Syste...
AEOS aepu service		Running	Automatic	Local Syste...
AEOS Application Server		Running	Automatic	Local Syste...
AEOS Lookup Server		Running	Automatic	Local Syste...
Agent Activation Runtime_10f382	Runtime for activating conversational agent applications	Running	Manual	Local Syste...
AllJoyn Router Service	Routes AllJoyn messages for the local AllJoyn clients. If this service is stoppe		Manual (Trig	Local Service

Figure 32: AEOS aepu service

Configure Virtual AEPU (Access Event Processing Unit)

Procedure

STEP 1

Open **AEmon** and select the virtual **AEpu**.

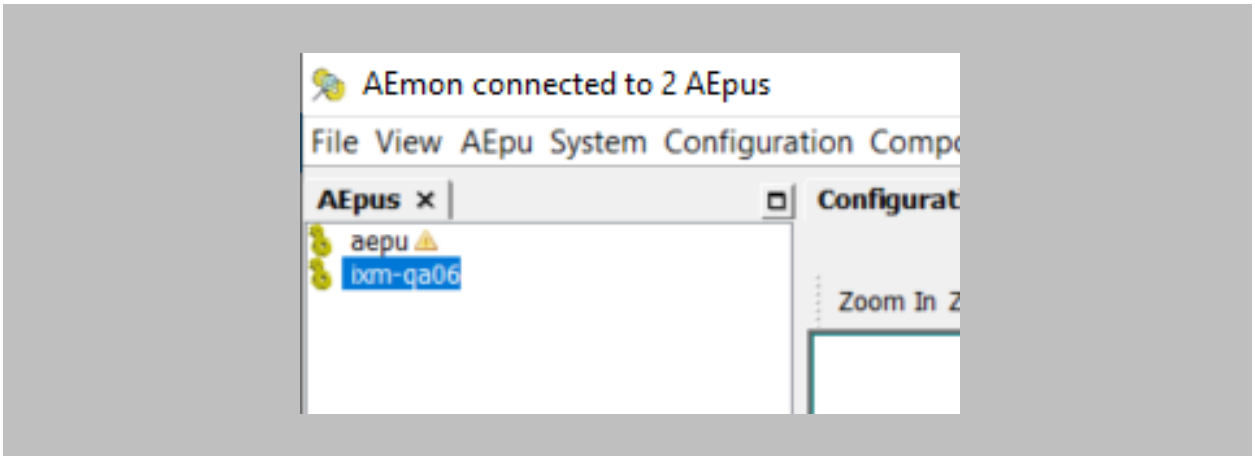


Figure 33: AEmon – Virtual AEpu

STEP 2

Navigate to **Component** tab and select **New**.

STEP 3

Create a separate Interface Server by giving it a name.

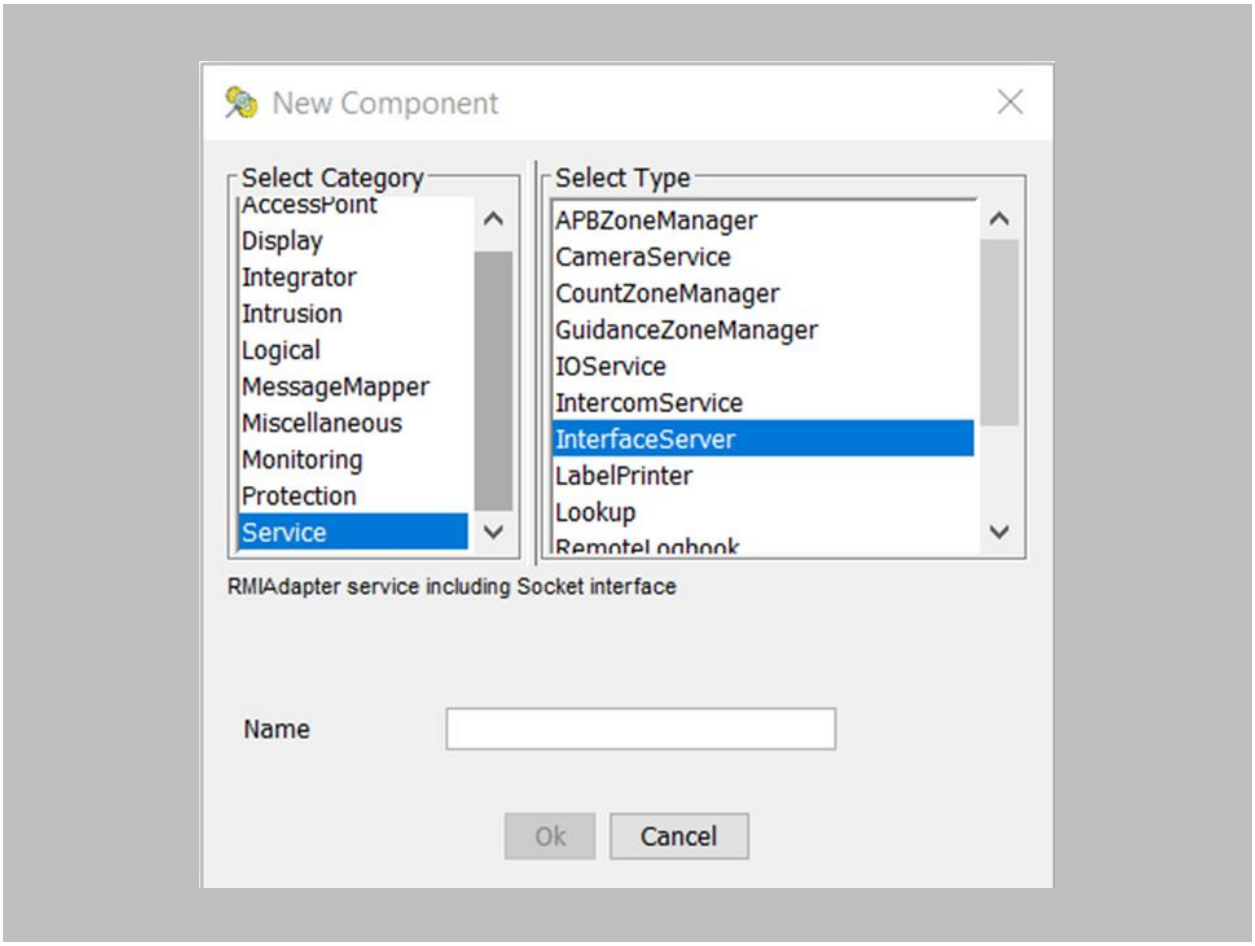


Figure 34: AEmon – Interface Server

STEP 4

Configure properties of the Interface Server.

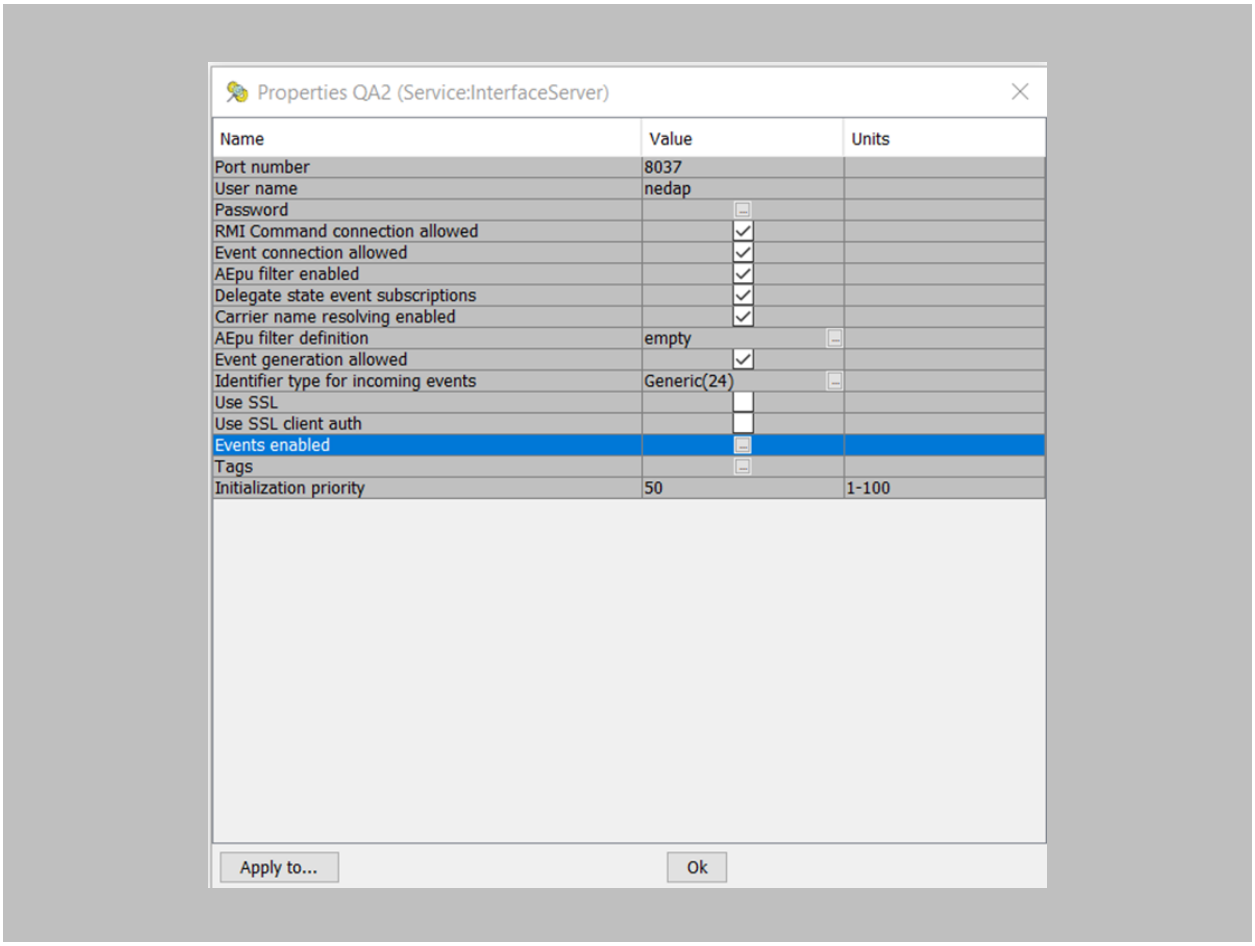


Figure 35: AEmon – Interface Server Properties

Port number:
The default Port number used by AEPU Controller for communication is 8035 but can be changed.

User name:
Enter the User name to connect to the server. The default user name is “nedap”.

Password:
Enter the Password to connect to the server. The default password is “nedap”.

Event connection allowed:
Enable this property by checking the box.

Event generation allowed:
Enable this property by checking the box.

Identifier type for incoming events:
Configure the required identifier from the dropdown list.

Invixium recommends Generic Identifier Type.

Upon selection, the following screen is displayed:

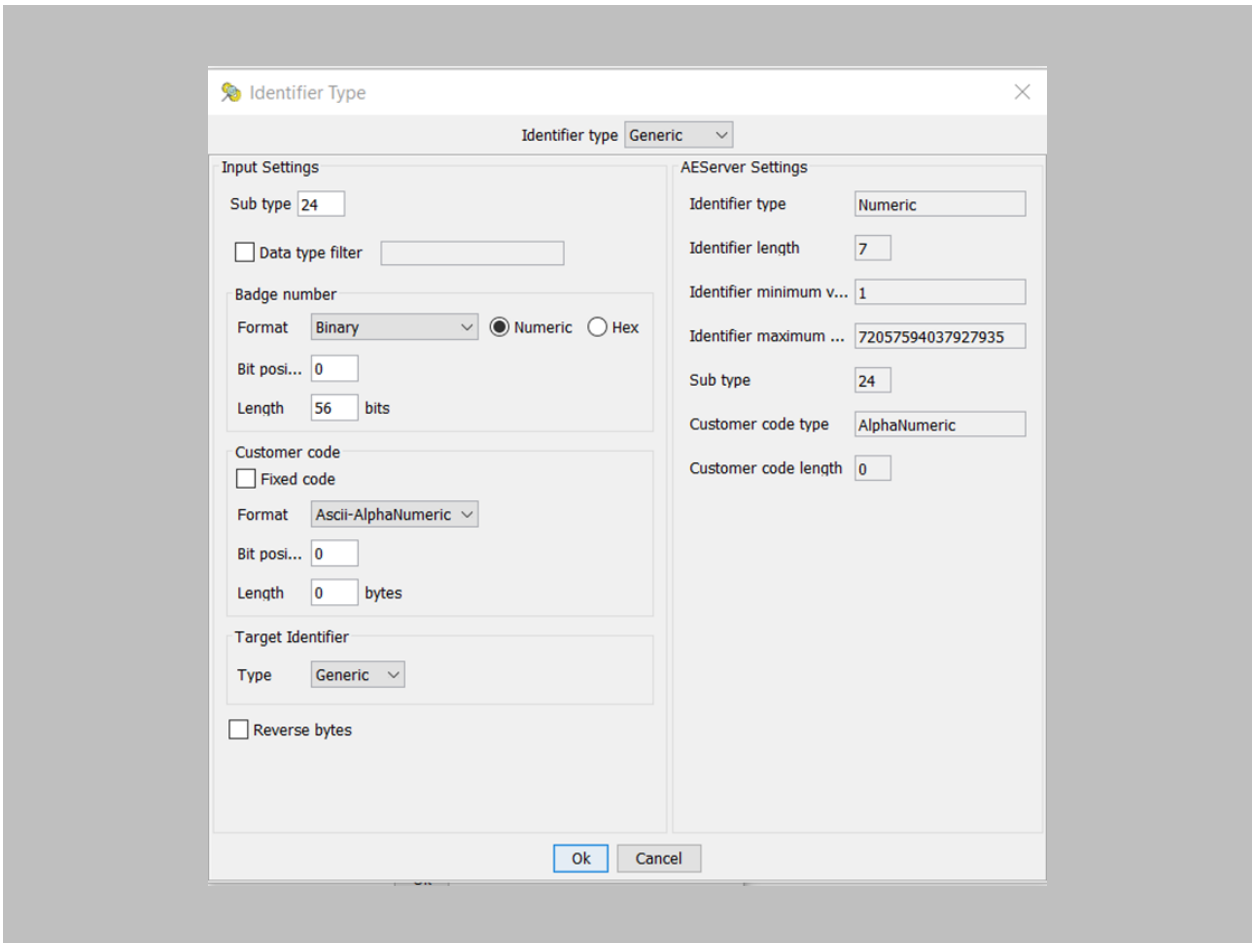


Figure 36: AEmon – Identifier Type for incoming events

STEP 6

<Right click> and select **Deploy configuration** to deploy the Interface Server.

Configure Events

Follow the steps below to configure events on Nedap AEOS for a device.

Procedure

STEP 1

From the Left Navigation Pane → **Link** → click the **AEOS (Nedap)** icon.

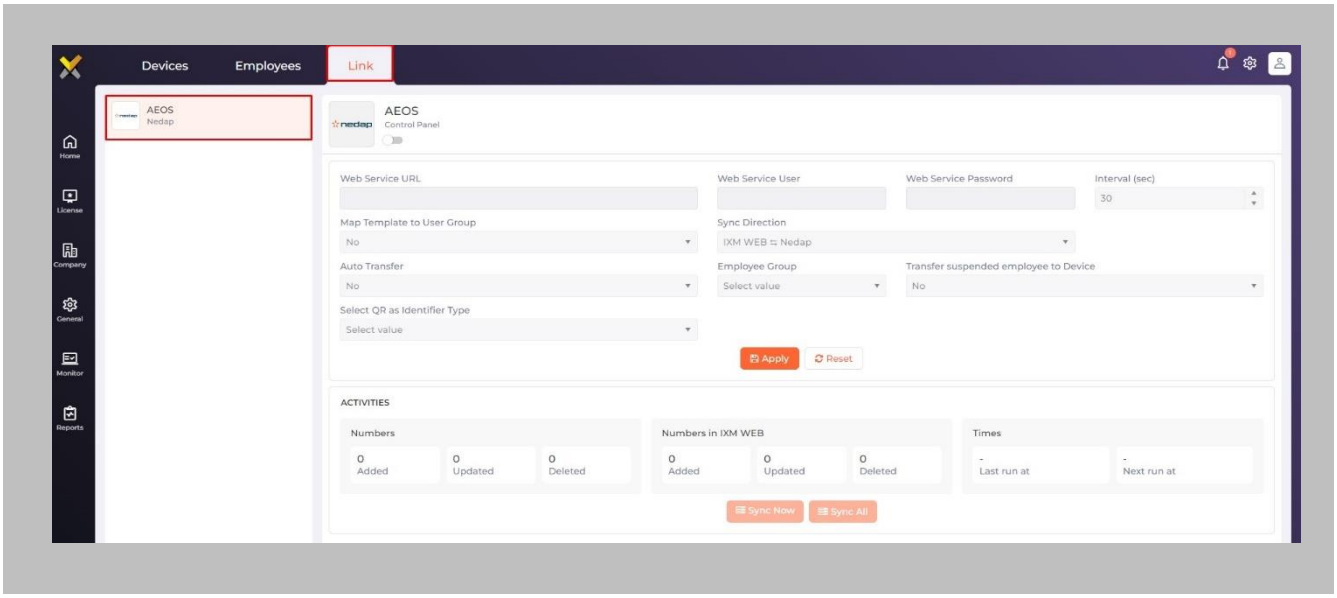


Figure 37: IXM WEB - Link Menu

STEP 2

Navigate to **Events Configuration** tab.

Note: This tab will be displayed only if there are registered device(s).

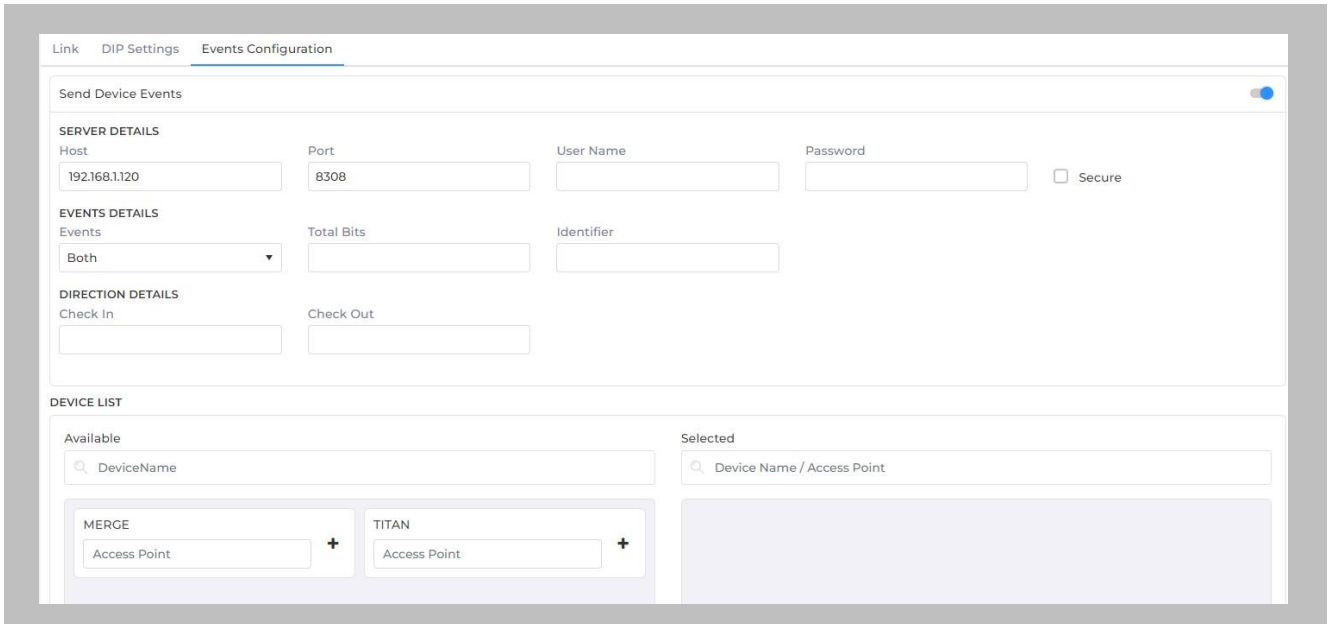


Figure 38: IXM WEB – Events Configuration

AEOS uses a Socket server to communicate with clients. The following information is required to connect with AEOS server:

SERVER DETAILS

Host:
Enter the Host name or IP Address where AEOS is running.

Port:
Enter the Port number of Interface Server.

User Name:
Enter the valid User name to connect to the Interface Server.

Password:
Enter the valid Password to connect to the Interface Server.

.

Secure:
Enable the checkbox to establish a secure stream and communicate with the server securely.

EVENTS DETAILS

Events:
Select the event(s) you want to send to AEOS server from the dropdown list.

- Both
- Access Granted
- Access Denied

Total Bits:
Enter the number of bits specified while configuring the Interface Server. Please refer the following screenshot for the same:

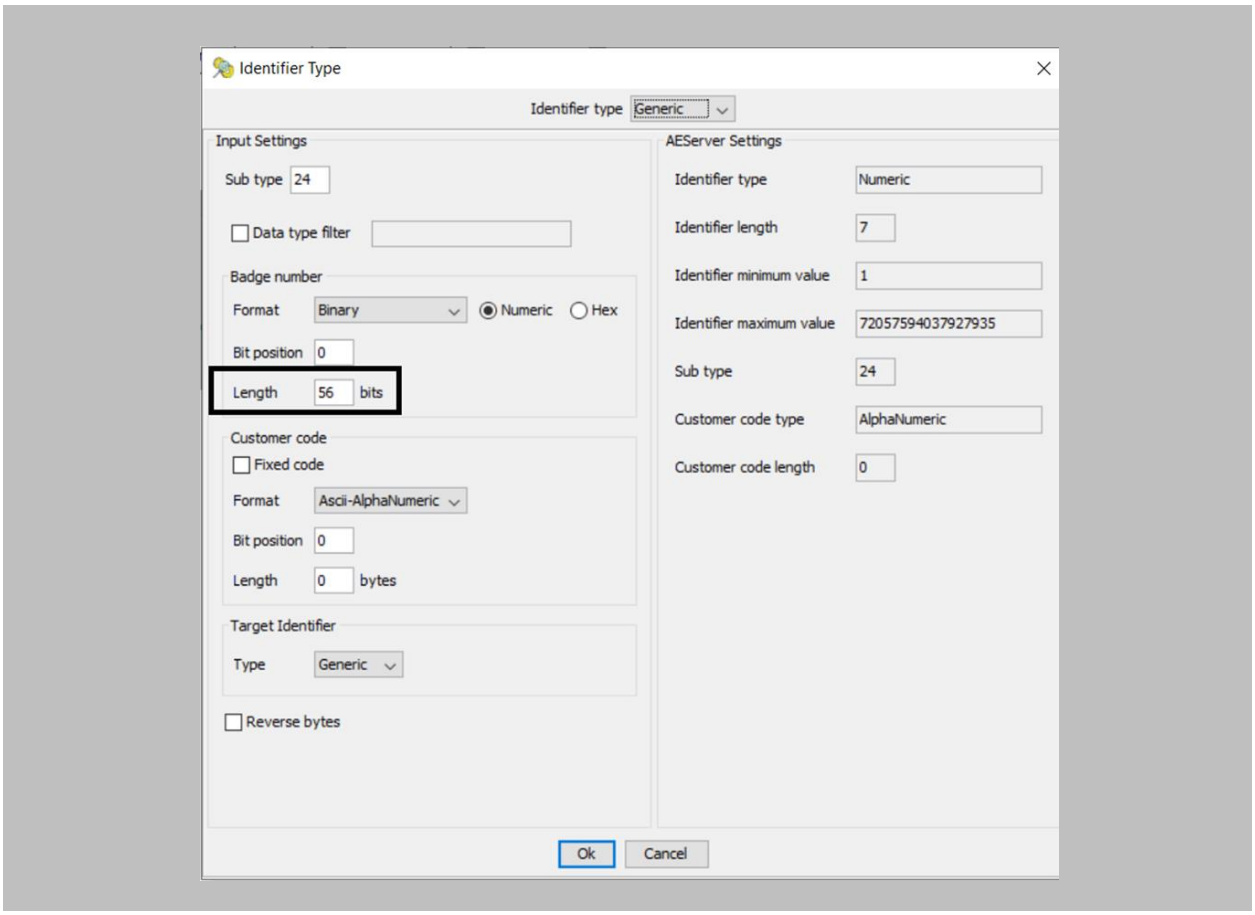


Figure 39: AEmon – Interface Server Identifier Type

Identifier:

In Aemon, during the configuration of the Access Point, it is necessary to specify the Identifier. This Identifier is then used to prepend additional bits to the Badge Number.

Specify the format based on the following screenshot:

If Wiegand 128 is selected in AEmon, then we need to set **0308** here.

For example:

Data type	Identifier
Nedap	
00 00	EF code
00 01	A code
00 02	EF (+ CB) code
00 03	B code
00 04	CF code
00 05	CF (+XF) code
00 06	DF code
00 07	DF (+XF) code
00 08	GF code
00 09	GF (+XF) code
00 0A	GF (+W) code
00 0B	GF (+W XF) code
00 0C	C code
00 0D	D code
00 0E	G code
Serial	
01 xx	Serial protocols
Omron	
02 01	Omron Track ISO 1
02 02	Omron Track ISO 2
02 03	Omron Track ISO 3
02 04	Omron max 200 ISO 2
Wiegand	
03 01	Wiegand 26
03 02	Wiegand 32
03 03	Wiegand 37
03 04	Wiegand 32Bin
03 05	Wiegand 44
03 06	Wiegand 35
03 07	Wiegand 64
03 08	Wiegand 128
03 09	Wiegand C1000

Data type	Identifier
Mifare	
05 01	Mifare CSN
05 02	Mifare Block data
05 03	Mifare DESfire CSN
05 04	Mifare DESfire Block data
05 05	Mifare Ultralight CSN
05 06	Mifare Ultralight Block data
05 07	
05 08	
05 09	Mifare Plus Block data
Legic	
07 01	Legic Prime CSN
07 02	Legic Prime Data
07 03	Legic Avant CSN
07 04	Legic Avant Data
HID	
08 01	IClass CSN
08 02	IClass Data
EM Marin	
09 01	EM4102
09 02	EM4050 Data
Converted from Input	
0A 00	Tamper state (0 false, 1 true)
0A 01	InputToBadge data
NFC	
0B 01	ISO 14443A
0B 02	ISO 14443B
0B 03	ISO 14443A and B

Table 5: AEmon – Data Type vs Identifier

Consider, **1051** is assigned badge to someone in IXM Web. And number of bits are 56 bits. So to send events related to this card number to AEOS, the following steps are required:

1. Convert card number to Hex. (As we are storing card as a decimal):
   1051 = 41B

2. Divide No. of bits by 4.
   56/4 = 14 bits will be sent to AEOS.

3. 0000000000**41B** number will be sent to AEOS.

4. But before sending this number, based on the selected Identifier Type we need to prepend the format. For example, if we have used **Wiegand 128** then we need to prepend **0308.** Hence our final number would be **0308**000000000**41B**.

5. In our case, for a Generic Identifier Type, our final number would be:

   0000000000000**41B**

DIRECTION DETAIL

Check In:
Enter Check-In value for FKey 1 that will be sent to Nedap server as a check-In event.

Check Out:
Enter Check-Out value for FKey 2 that will be sent to Nedap server as a check-Out event.

Note: Nedap AEOS will consider value “1” as in-direction, “2” as out-direction, and any other value as unknown direction.

DEVICE LIST

Available:
A list of available device(s) will be displayed. Click on the **+** icon of device to select. The selected device will be moved to the **Selected** list.

Selected:
A list of selected device(s) will be displayed. Click on **x** icon of device to deselect. The device will be moved back to the **Available** list.

Events of only selected devices will be sent to Nedap AEOS.

STEP 3

Click on **Apply**.

IXM Web will attempt to establish a connection with the AEOS server using the provided parameters. Only when the connection is successfully established, the details will be saved; otherwise, an error message will be displayed.

To send events to Nedap AEOS, a Badge Number is required. The default card of an Employee will be sent. If an employee does not have a card, no event will be sent to Nedap AEOS.

12. Create System User(s) for Biometric Enrollment

STEP 1

Log into IXM WEB.

On the top right of default page, click on the **User Menu** → Click **Users**. The application will redirect to the System Users window.

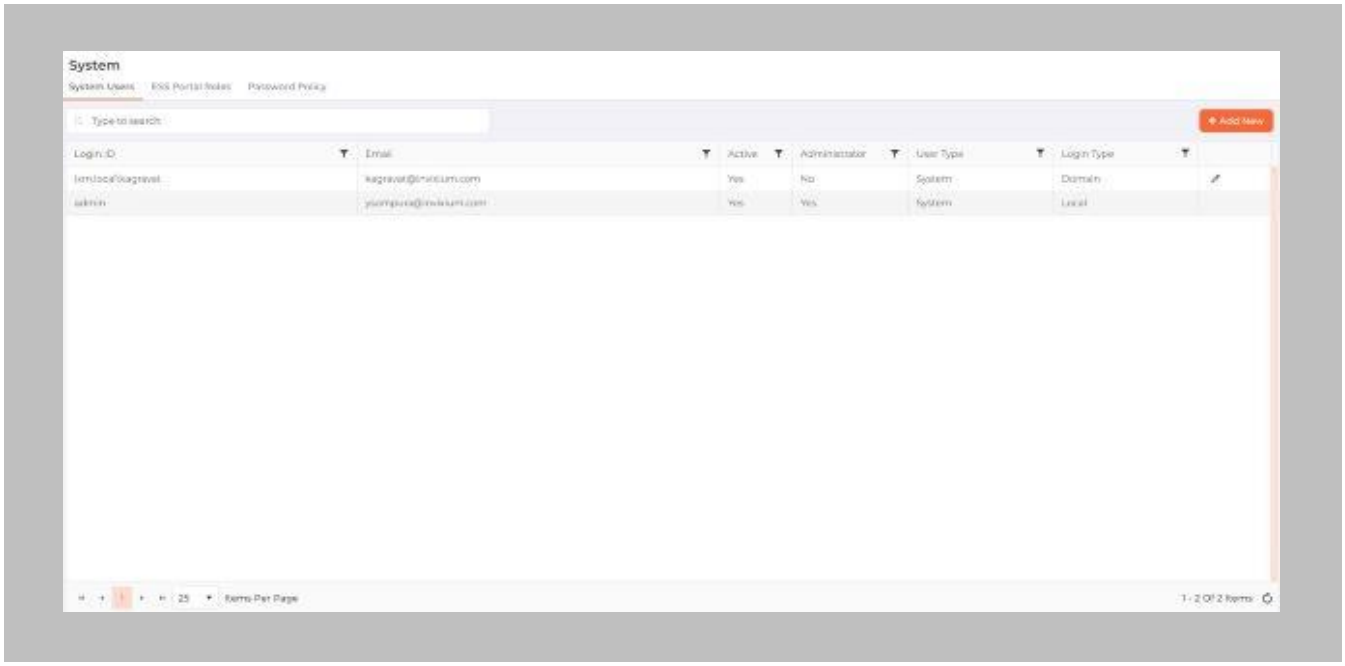


Figure 40: IXM WEB - Create System User

STEP 2

Click **Add New**.

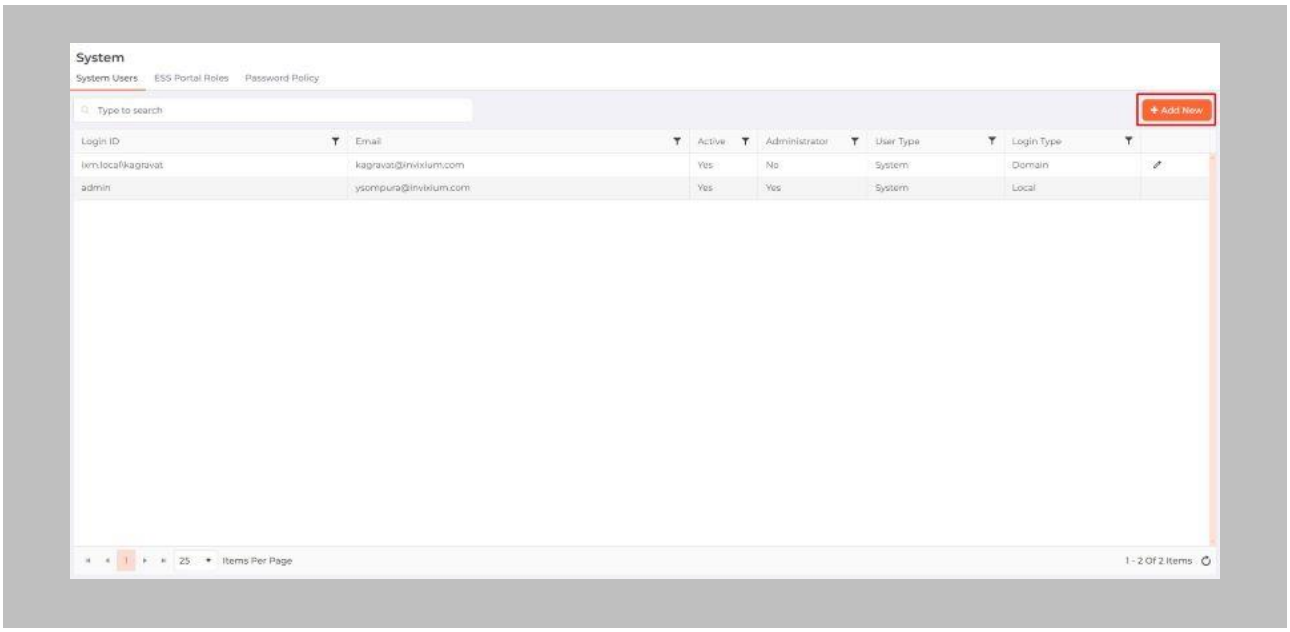


Figure 41: IXM WEB - Add New System User

Creating a system user requires the following details:

- Login type
    - i. Local employee
    - ii. Domain employee
- Invixium ID (User ID) (For domain employee login types, the User ID is automatically filled from AD)
- Password creation (For domain employee login types, password creation is not required)
- Email address
- Status
- Permission for modules

STEP 3

Select **Login Type (Local or Domain Employee)** from the dropdown list.

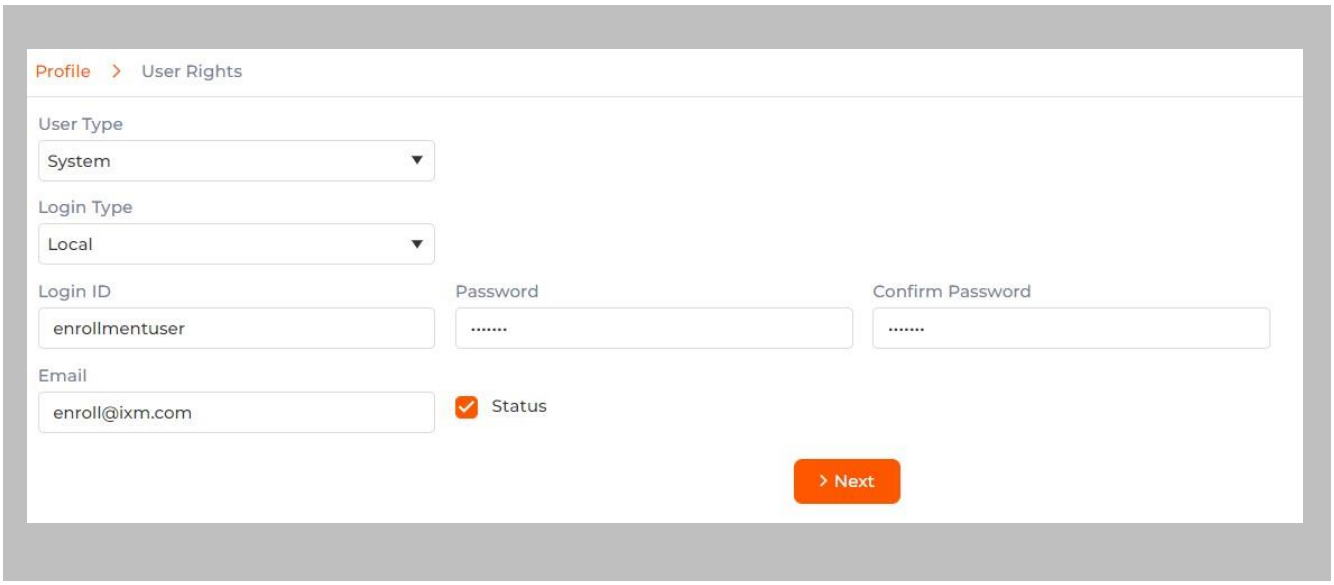


Figure 42: IXM WEB - New System User

STEP 4

Add an email address.

Apply for permission as “All” for **Employee & Employee Group** module.

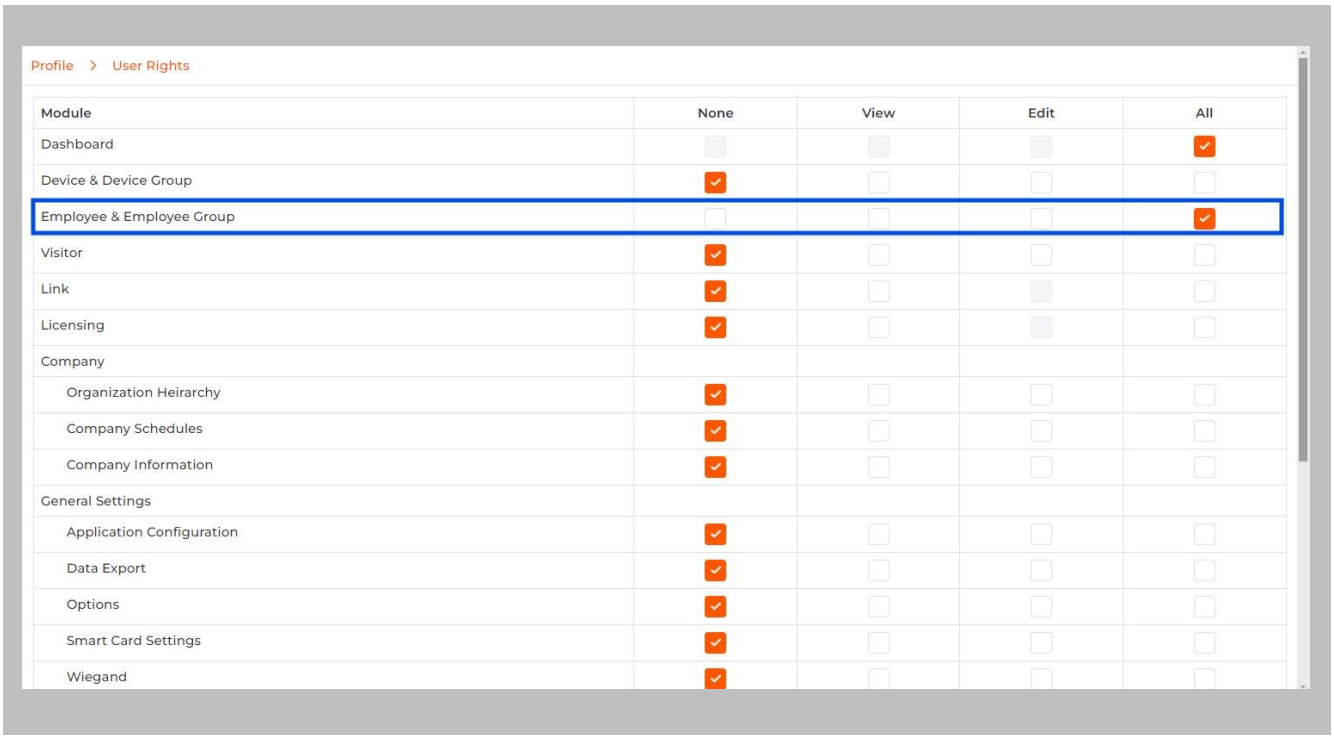


Figure 43: Employee and Employee Group Rights

STEP 5

Click **Save**.

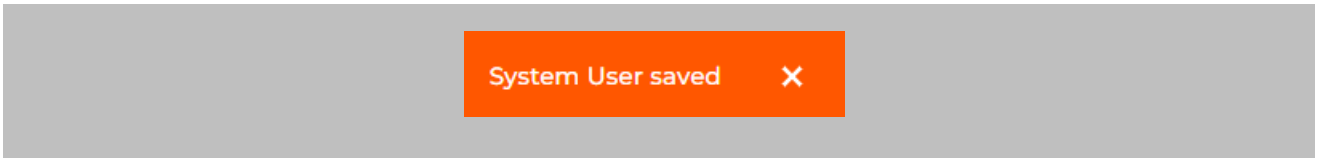


Figure 44: IXM WEB - Save System User

13. Add and Configure Invixium Readers

Adding an Invixium Reader in IXM WEB

Procedure

STEP 1

Click the **Devices** tab.

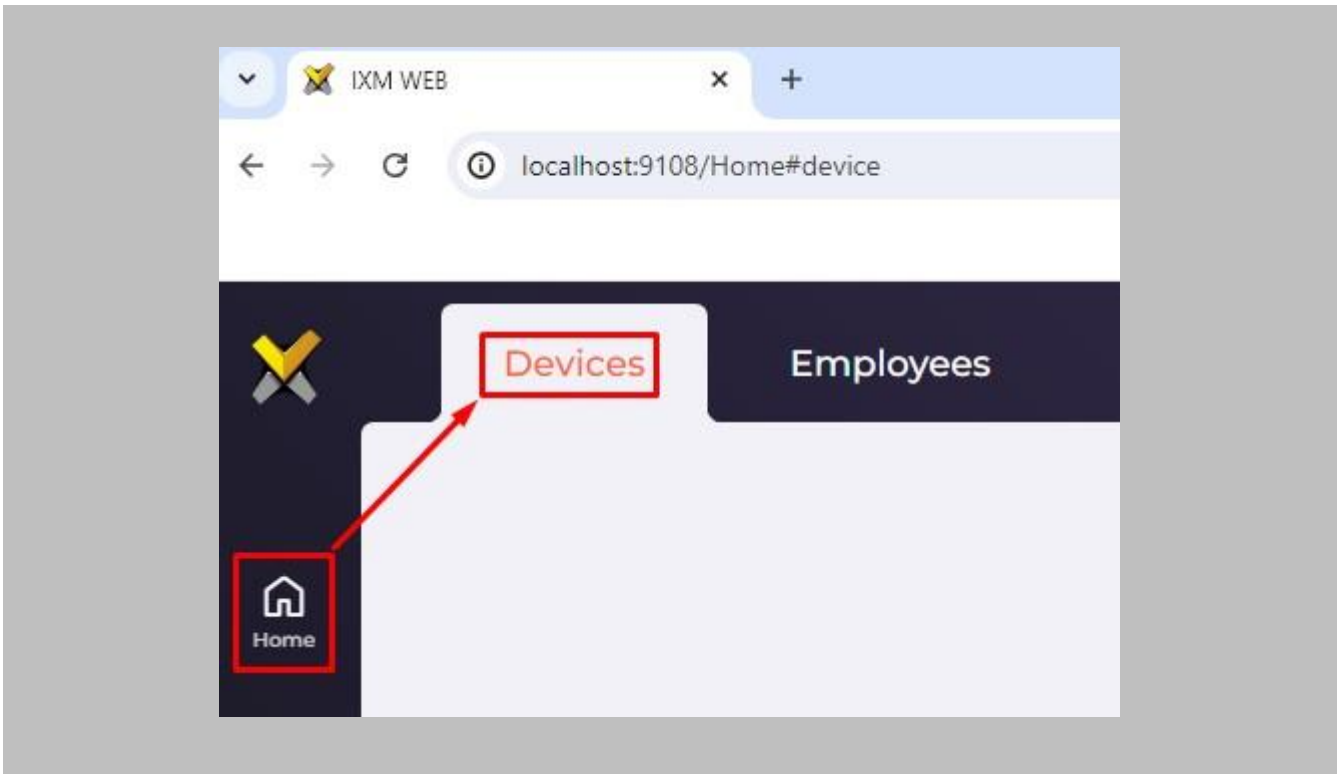


Figure 45: IXM WEB - Devices Tab

STEP 2

Select the **Add New Device** button on the right-hand side of the page. Then select the **Ethernet Discovery** option and add the reader's IP in the start IP section. Click on **Search** to find the device.

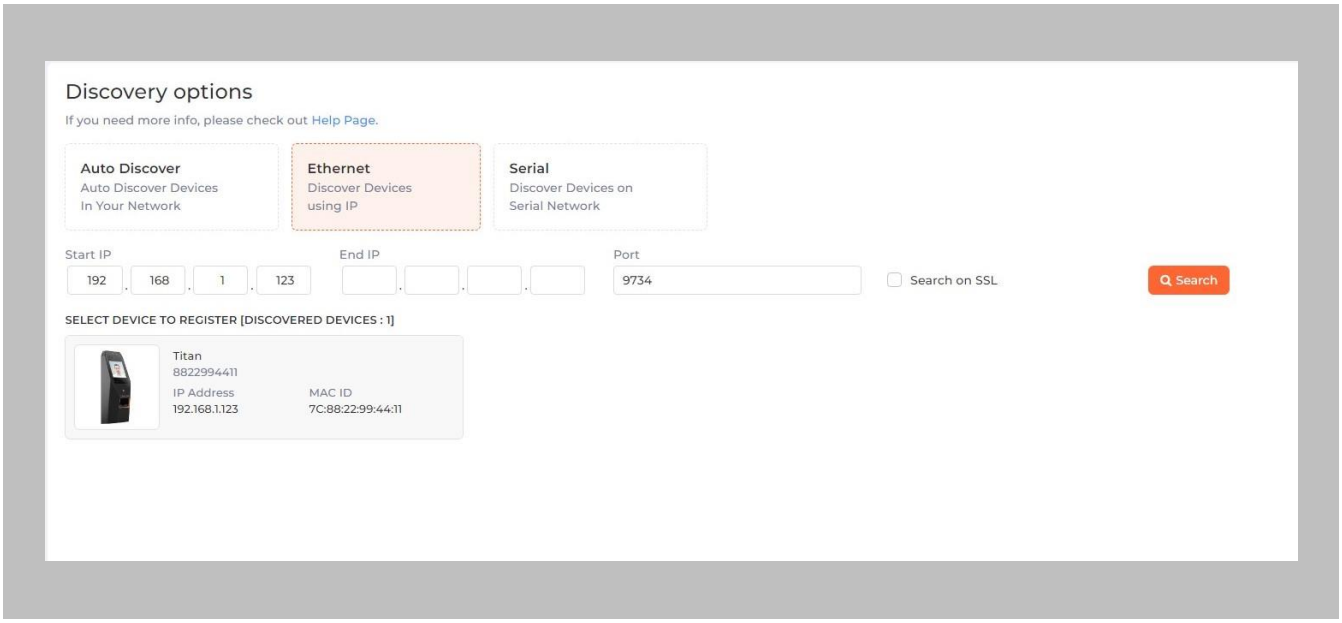


Figure 46: IXM WEB - Search Device Using IP Address

STEP 3

Once the device is found, click on it. Add the required fields and select **Register**.

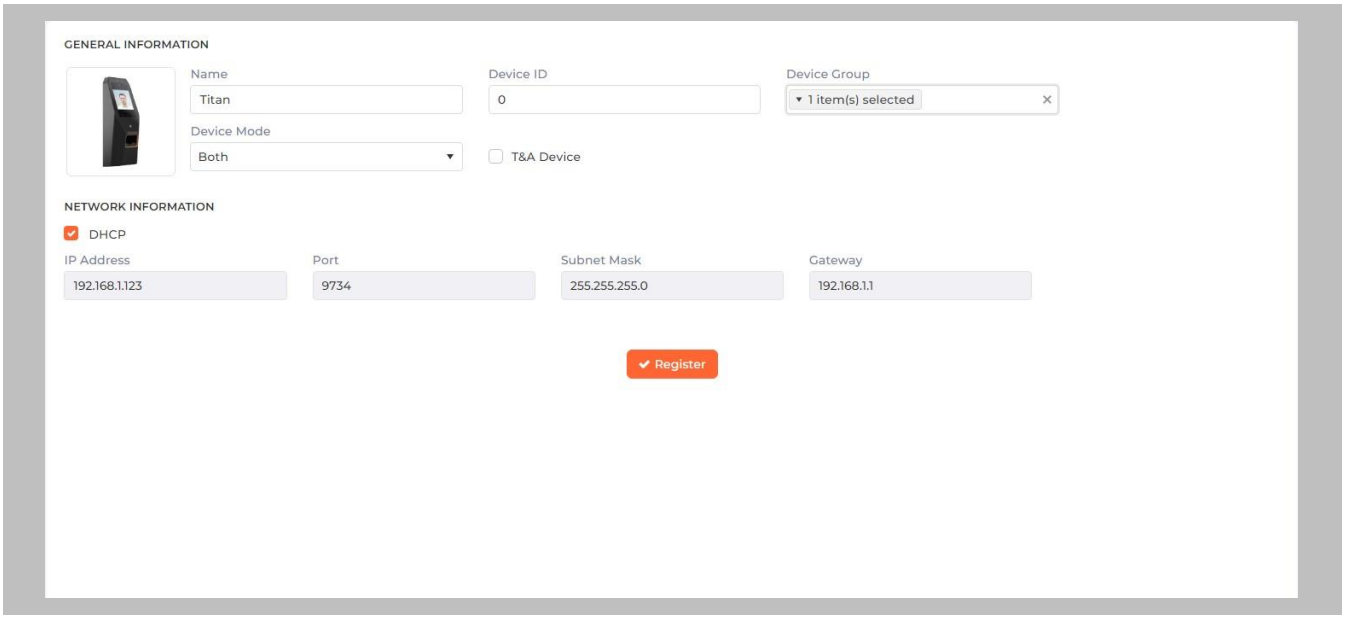


Figure 47: IXM WEB - Register Device

STEP 4

Name the **device** exactly as the name of the door it will be used for.

Device Mode: select accordingly.

Device Group: select the Access Group to which the reader will be assigned.

STEP 5

Once the device has successfully been **registered**, click **Done**.

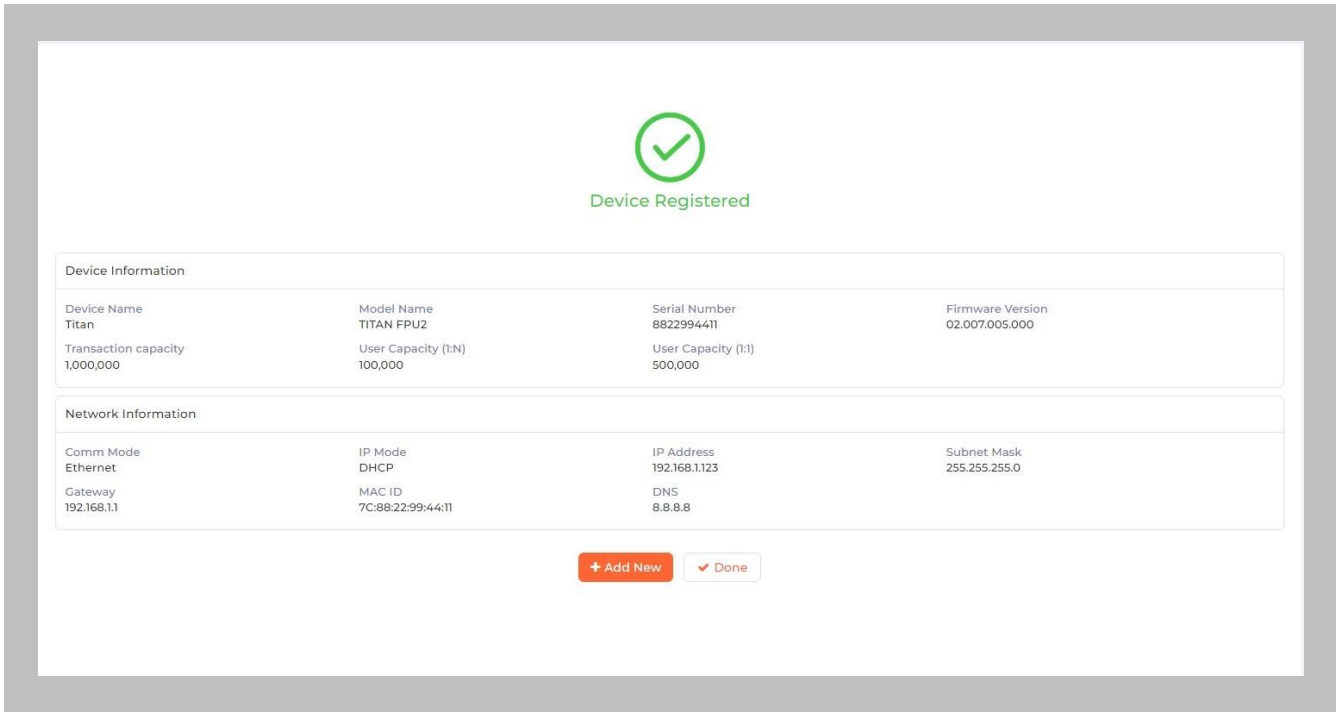


Figure 48: IXM WEB - Device Registration Complete

Go to **Dashboard** and confirm that the **Device Status** chart indicates that the reader is online (ie. hovering will tell you how many devices are online).

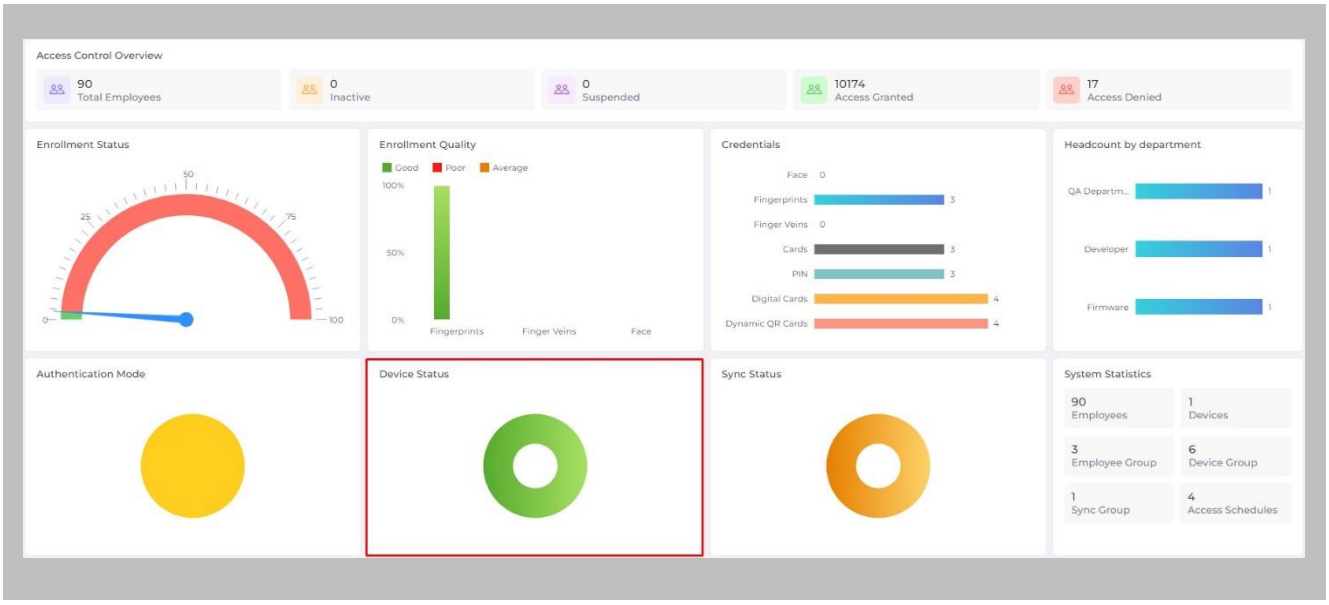


Figure 49: IXM WEB - Dashboard, Device Status

14. Adding an Invixium Device to a Device Group

Procedure

STEP 1

Any of below methods can be used to add device to device group.

METHOD 1: Go to **Devices** → click on **Manage Device Group**. Add the device by clicking vertical ellipses button of respective Device Group → click on **Add Device** → Search for device → click **Add** button.

METHOD 2: Go to **Devices** → click on **Manage Device Group**. Click on Device Group Name → click on **Add Device** button. Search for device → click **Add** button.

METHOD 3: On Device list page, click on vertical ellipses button of device → click on **Add to Group** → Search and select required group name → Click **Add.**

METHOD 4: On Device list page, select single or multiple device(s) → click on **Add to Group** icon visible next to search box → Search and select required group name → Click **Add**.

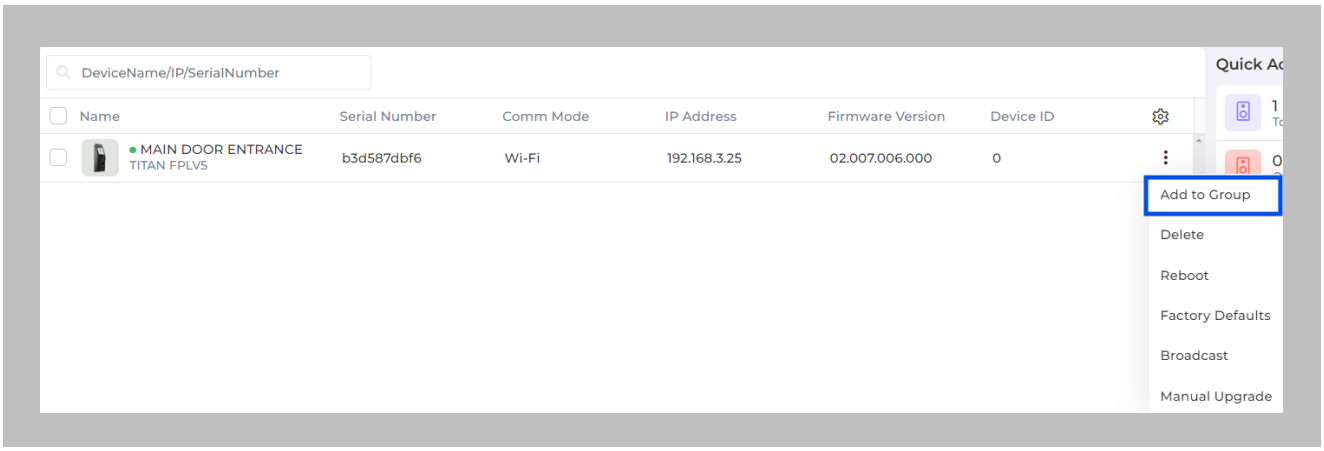


Figure 50: IXM WEB - Assign Device Group

Configuring Wiegand Format to Assign Invixium Readers

Note: Invixium devices support upto 512 bit long Wiegand format. Accordingly, you can create a Wiegand format as per your requirement.

STEP 1

Click **General** and Navigate to **Wiegand** → **Create.**

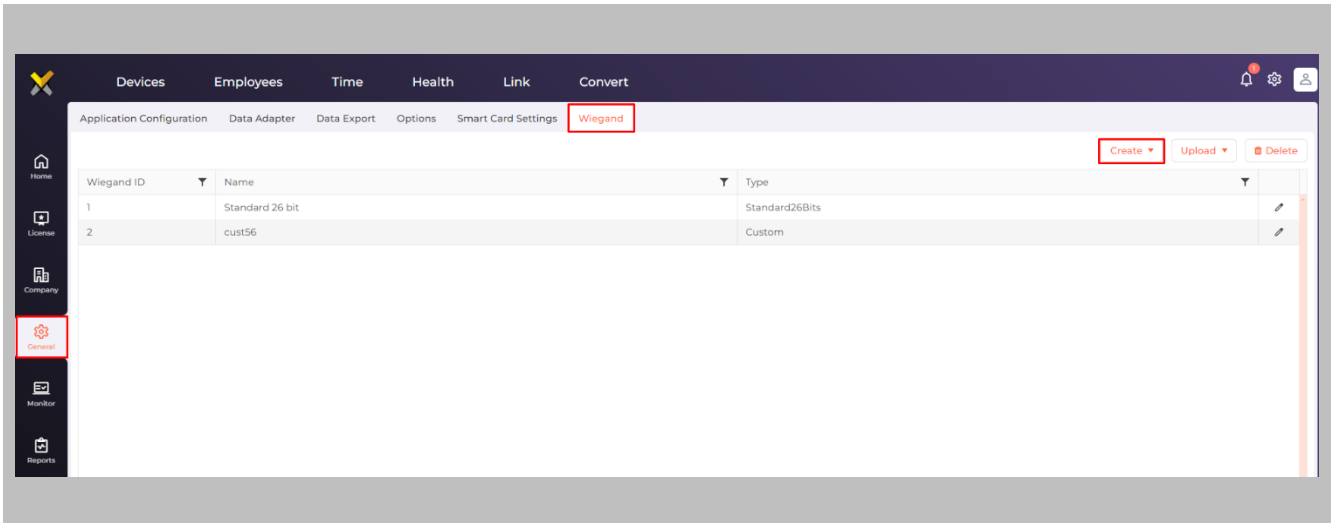


Figure 51: IXM WEB - Create Wiegand Format

STEP 2

Hover mouse over **Create** and select the **Custom** option from the dropdown menu**.**

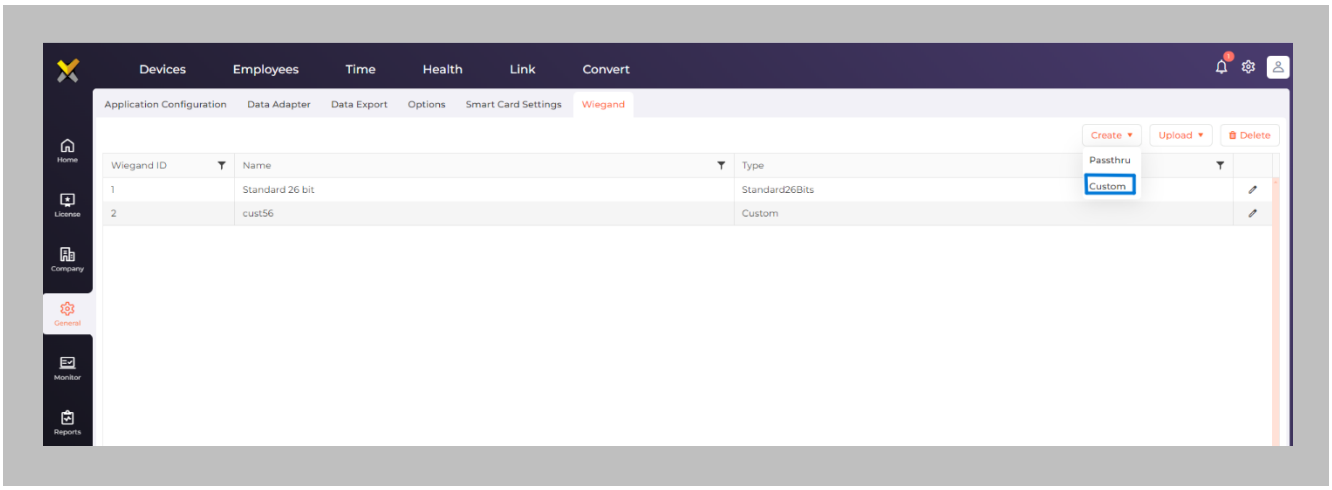


Figure 52: IXM WEB - Create Custom Wiegand Format

STEP 3

Enter **Name** of the custom Wiegand and assign **Bits**. Lets say we name the Wiegand as '32-BIT CSN' and define Total Bits as 32 bits where all the 32 bits are ID bits.

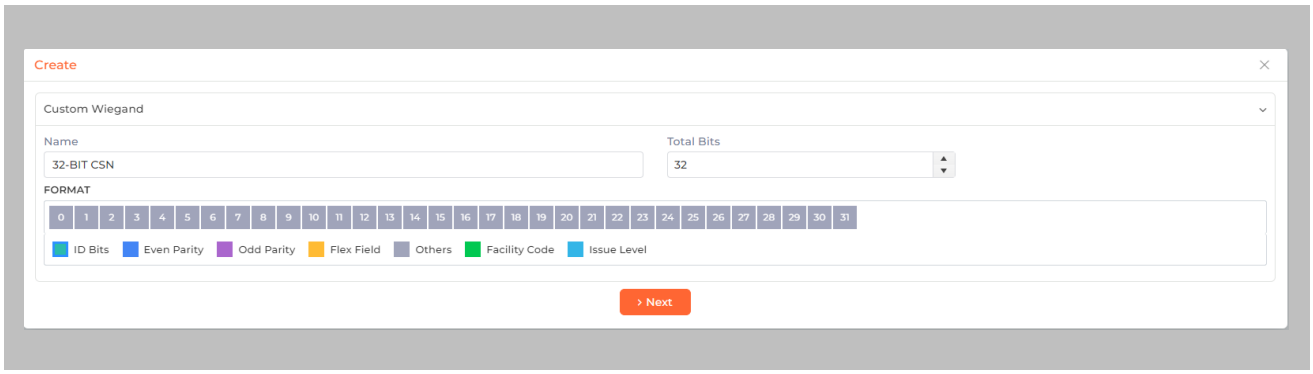


Figure 53: IXM WEB - Custom Wiegand Format

STEP 4

Click **Next** and **Save**. Wiegand Format created message will be displayed.

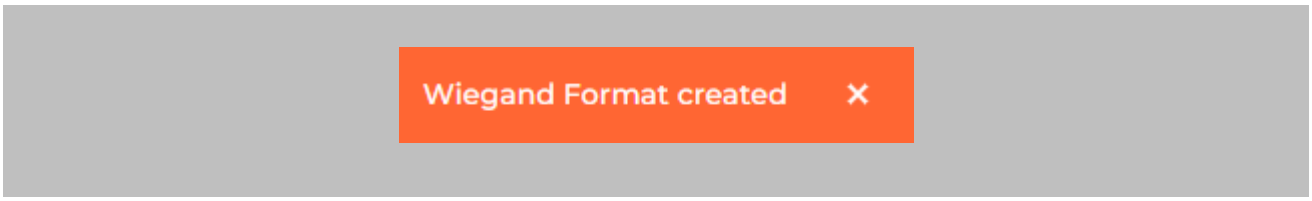


Figure 54: IXM WEB – Custom Wiegand Format Created

STEP 5

Click on **Upload** and select the device group (applies to all readers). Click **OK**.

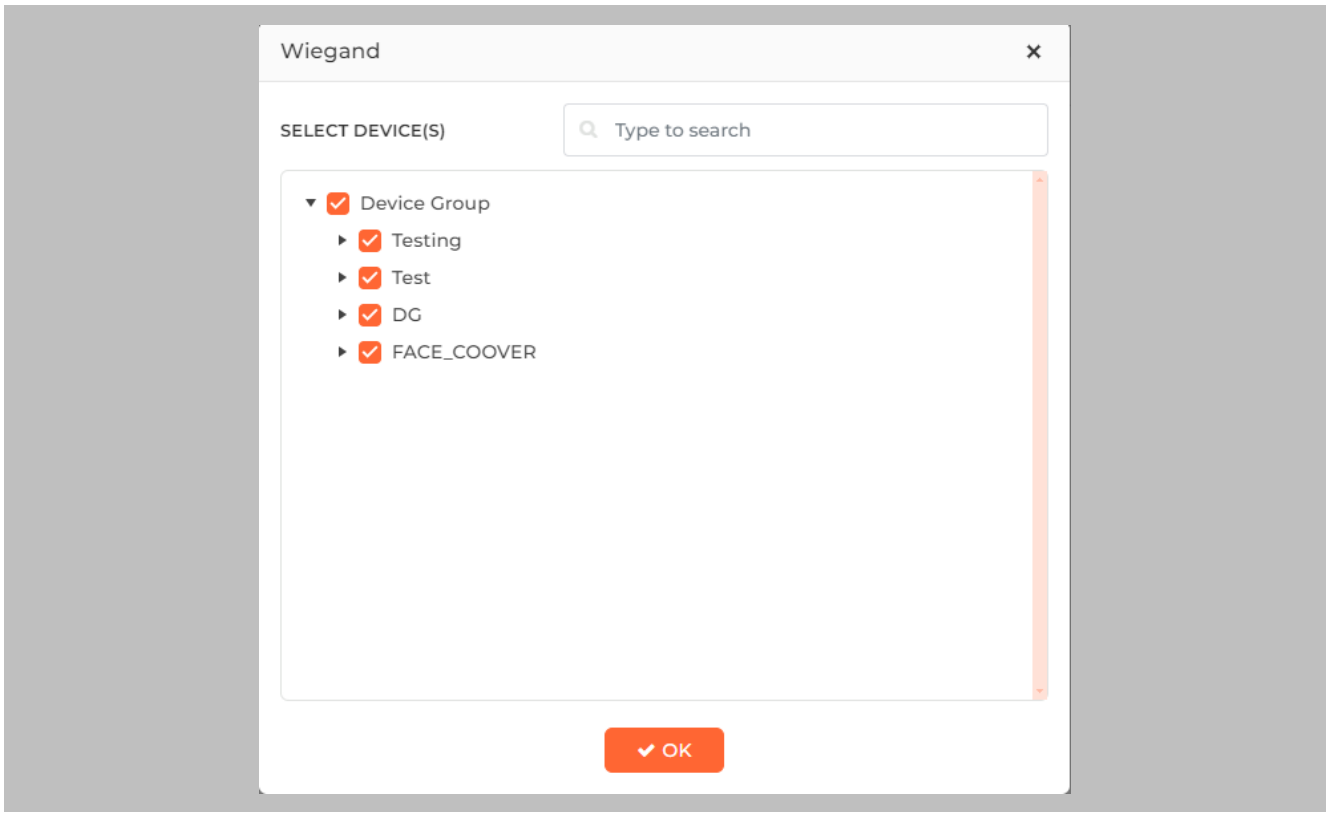


Figure 55: IXM WEB - Upload Wiegand Format

Assign Wiegand to Invixium Readers

Note: Face and finger will always give a Wiegand output based on the initial card that was synced from Honeywell to Invixium.

The created Wiegand will be used to define which output format will be sent to Pro-Watch.

STEP 1

From **Devices** tab. Select any device.

STEP 2

Navigate to the **Access Control** tab.

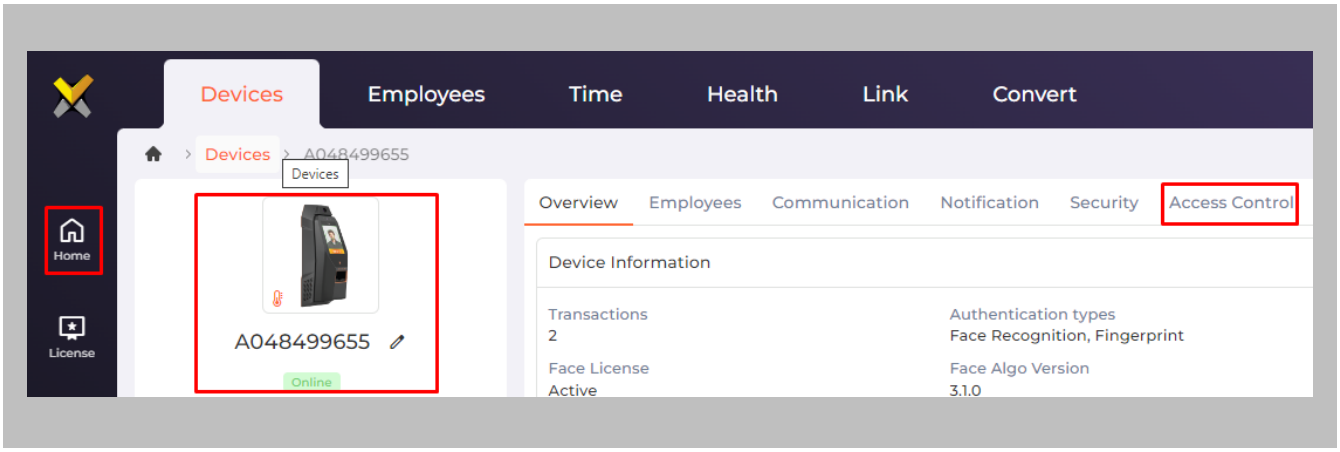


Figure 56: IXM WEB - Navigate to Access Control Tab

STEP 3

Scroll down and click on **Wiegand Output** and toggle the switch on the top right-hand side to enable Wiegand Output for the device.

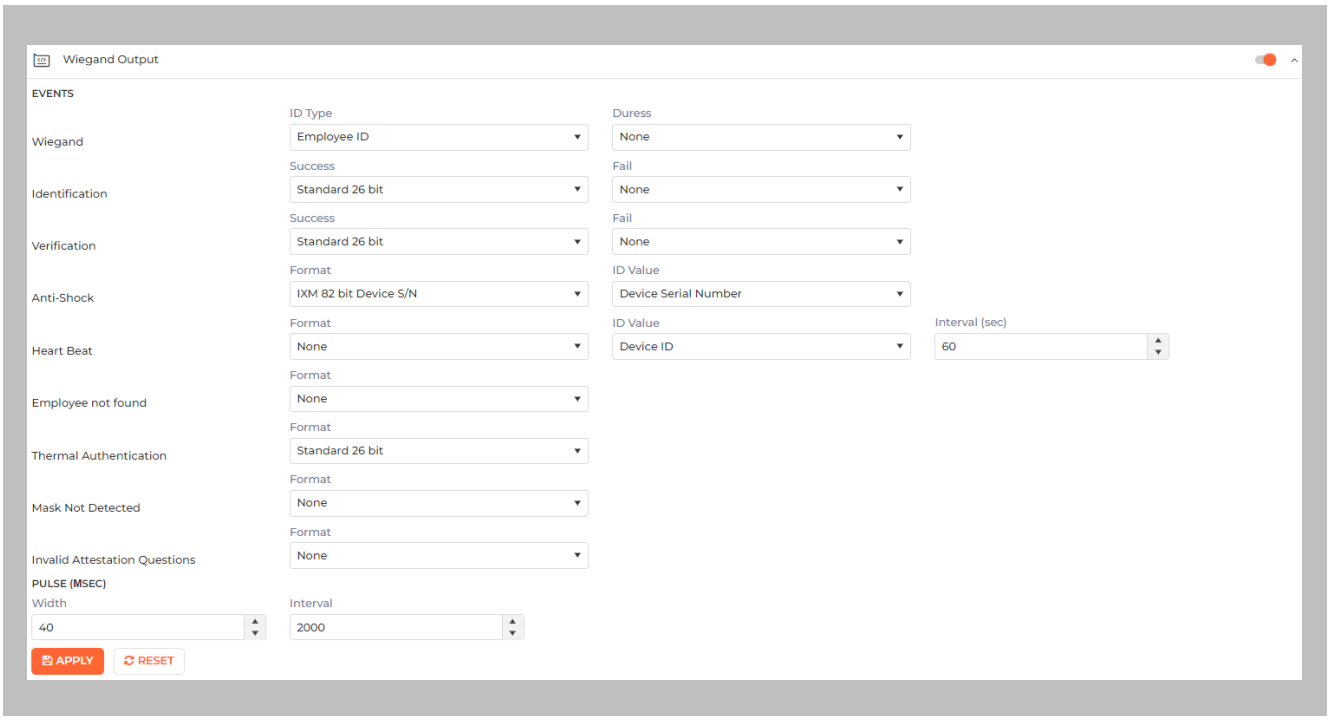


Figure 57: IXM WEB - Wiegand Output

ID types for Wiegand output are as follows:

1. Employee ID
2. Default Card
3. Actual Card

Set ID Type of output Wiegand to Employee ID/Default/Actual Card. By default, Employee ID is selected in Wiegand Event.

As the Employee ID field is not available in Pro-Watch, select either Default Card or Actual Card.

Empoyee ID: This is auto generated ID by IXM WEB for an imported cardholder in Honeywell.

Actual Card: When more than one card is assigned to the cardholder, and you want to generate Wiegand output data for the same card which is presented on the Invixium device.

Default Card: It will generate Wiegand output data for the card which is marked as the default.

Note: For fingerprint and face access, default card Wiegand output data will be generated.

STEP 4

Select desired format for Identification, Verification, Employees not found, Thermal Authentication and Mask not Detected for the selected Card.

STEP 5

Click **Apply.**

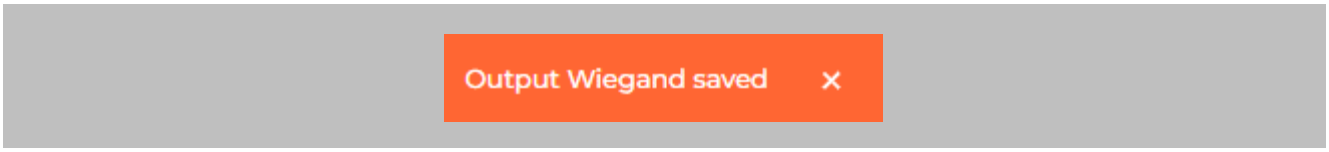


Figure 58: IXM WEB - Save Output Wiegand

RESULT

The Wiegand Output settings of the selected device are now updated.

Note:

- If you have more devices, follow the next steps to copy all Wiegand settings to all devices simultaneously. Note: This copies all Wiegand output settings. See Appendix C for more information.
- If the cardholder was assigned multiple cards, the first assigned card will be the 'default' selected card. The details of the card will be sent as the Wiegand bits input to Pro-Watch controller.
- To make this Wiegand output work on Honeywell, you will need to make sure the Wiegand format is available in Honeywell for use on the controllers talking to the Invixium reader (by Wiegand or OSDP).

Configuring Panel Feedback with Nedap

Procedure

STEP 1

Connect Wiegand Data D0 of the Honeywell Panel with **WDATA_OUT0** of the IXM device, Wiegand Data D1 of the Honeywell Panel with WDATA_OUT1, and Wiegand Ground of the Honeywell Panel with WGND of the IXM Device.

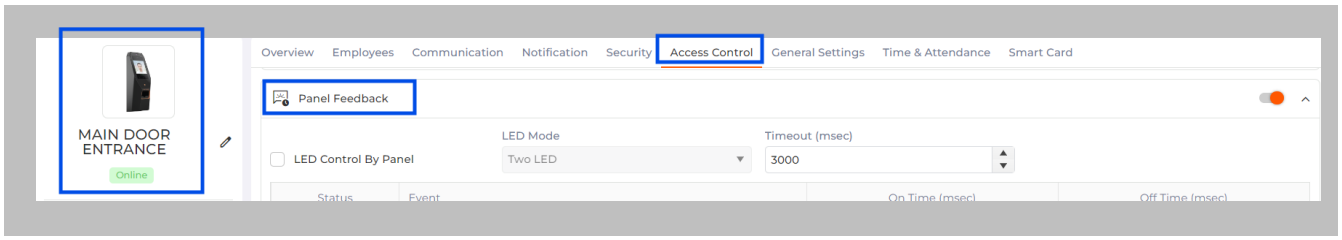
STEP 2

Connect the **LED** of the Honeywell Panel with **ACP_LED1** of the IXM device.

STEP 3

On the **Devices** tab, select the required device and navigate to the **Access Control** tab. Scroll down and click on **Panel Feedback**.

Figure 59: IXM WEB - Panel Feedback



STEP 4

By default, Panel Feedback is turned **OFF**. Toggle the Panel Feedback switch on the top right-hand side to the **ON** position, and then enable **LED Control** by the panel and set the LED Mode to **One LED**.

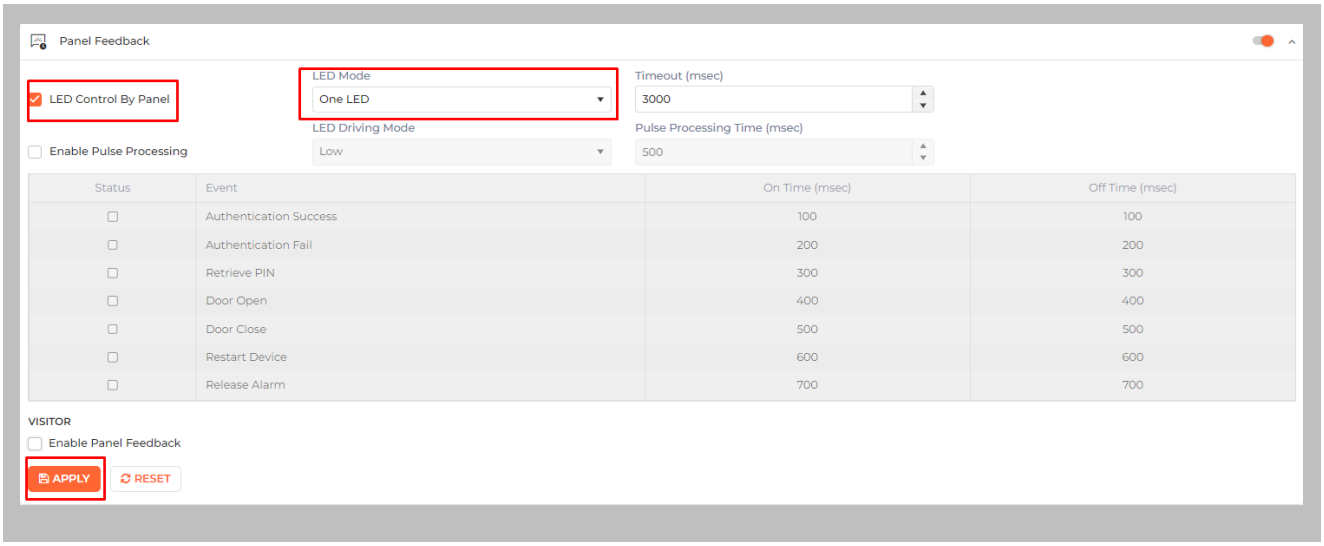


Figure 60: IXM WEB - Configuring Panel Feedback in IXM WEB

STEP 5

Click **Apply**.

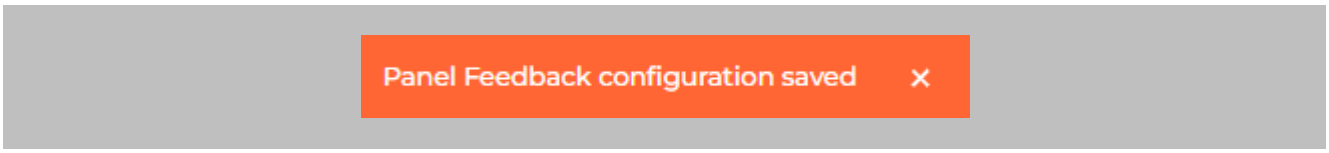


Figure 61: IXM WEB - Save Panel Feedback

15. Enrollment from Nedap AEOS

The Nedap AEOS application and IXM WEB should be browsed using https on the same browser session to overcome issues of a self-signed certificate.

Pre-configuration for enrollment

Procedure

STEP 1

Host **IXM WEB** on https. A certificate will be required to configure IXM WEB on https. For example: **https://172.16.254.40:9108**

STEP 2

Go to the location where **AEOS** is installed →Open **Key Store Explorer** for importing IXM WEB's CA certificate.

Default Location: C:\AEOS\AEserver\standalone\certs

STEP 3

Go to **Tools** →Click on **'Import Trusted Certificate'.**

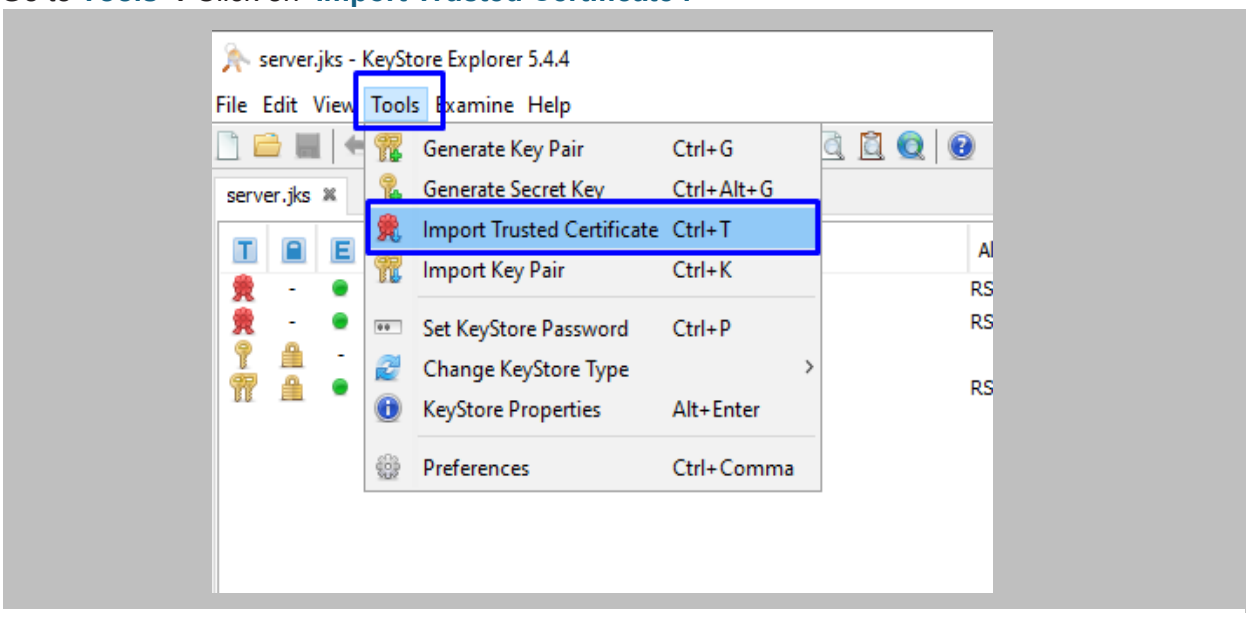


Figure 62: AEOS- Import Trusted Certificate

STEP 4

Select the **SSL** certificate and import it.

STEP 5

Go to the location where **AEOS** is installed → Open the **aeos.properties** file to make changes related to enrollment.

Default Location: C:\AEOS\AEserver\standalone\configuration\aeos.properties

STEP 6

Add the below details in **aeos.properties** file:

```
bioapi.settings.server.bms1.name=IXMEnroll
bioapi.settings.server.bms1.uri=https:// 172.16.254.40:9108/Link/
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'
172.16.254.40:9108/Enrollment/Enrollment/ https://
172.16.254.40:9108/Link/EnrollNedapAEOSUser/ 'unsafe-inline' 'unsafe-eval'; script-src
'self' https:// 172.16.254.40:9108/Enrollment/Enrollment/ https://
172.16.254.40:9108/Link/EnrollNedapAEOSUser/ 'unsafe-inline' 'unsafe-eval'; object-src
'self' https:// 172.16.254.40:9108/Enrollment/Enrollment/ https://
172.16.254.40:9108/Link/EnrollNedapAEOSUser/ 'unsafe-inline' 'unsafe-eval'; img-src
'self' https:// 172.16.254.40:9108/Enrollment/Enrollment/ data:
```

Note: Replace https://172.16.254.40:9108 with actual IXM WEB URL in above content security policy. Make sure there is no line break in above CSP

STEP 7

Open the **AEOS** application → From the AEOS menu bar, go to **Administration** → **Maintenance** →**Identifiers.**

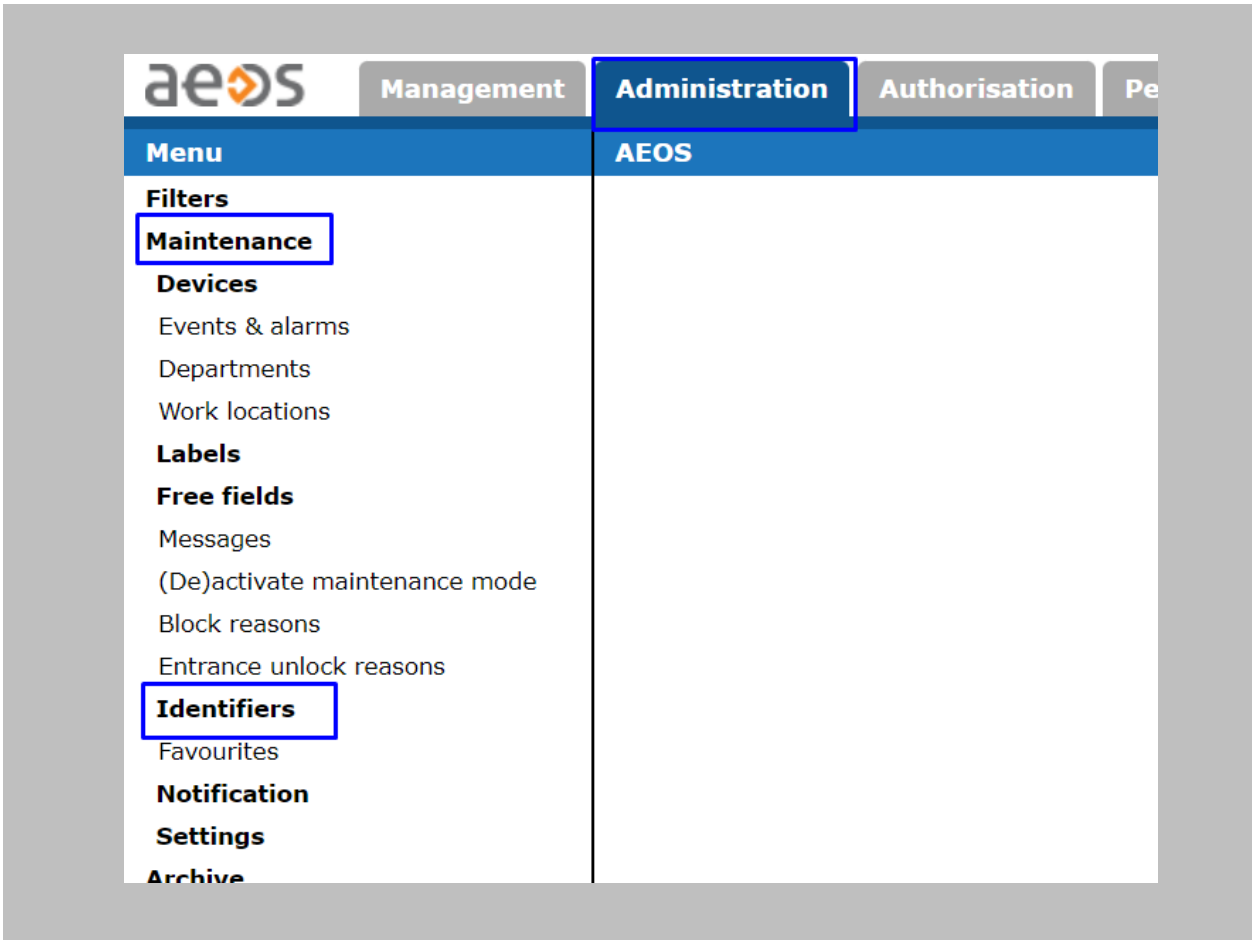


Figure 63: AEOS - Identifiers

STEP 8

Click on **Identifier Types** → from the **Identifier Types** dropdown, select the type of identifier you want to create.

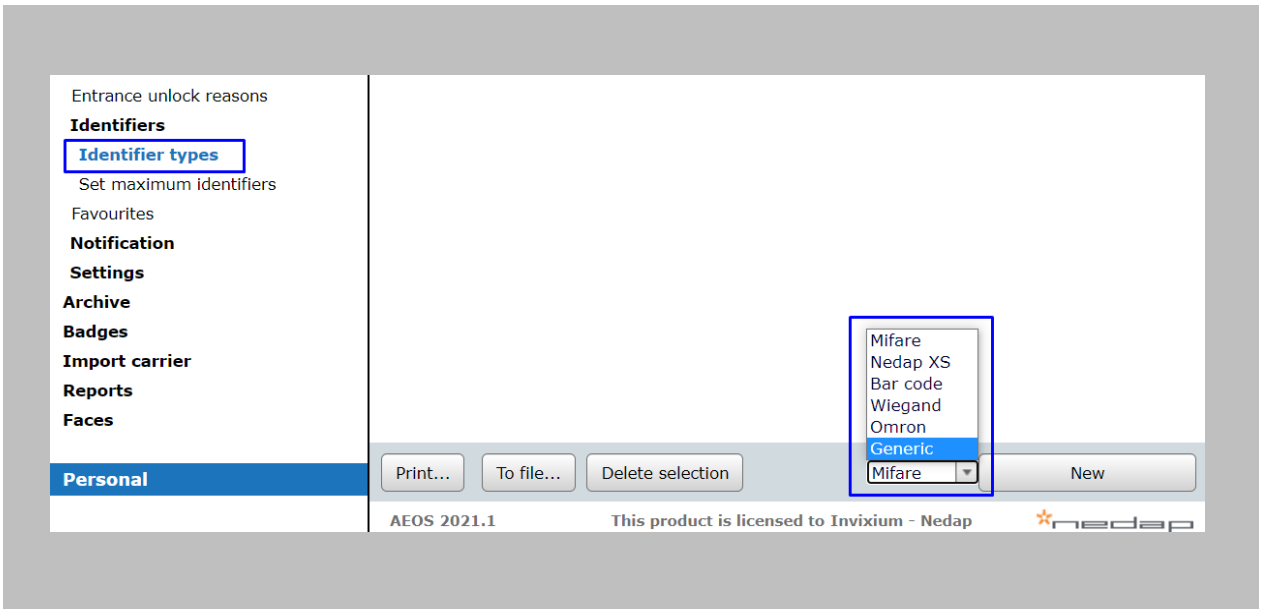


Figure 64: AEOS - Identifier Type Selection

Click on **New.**

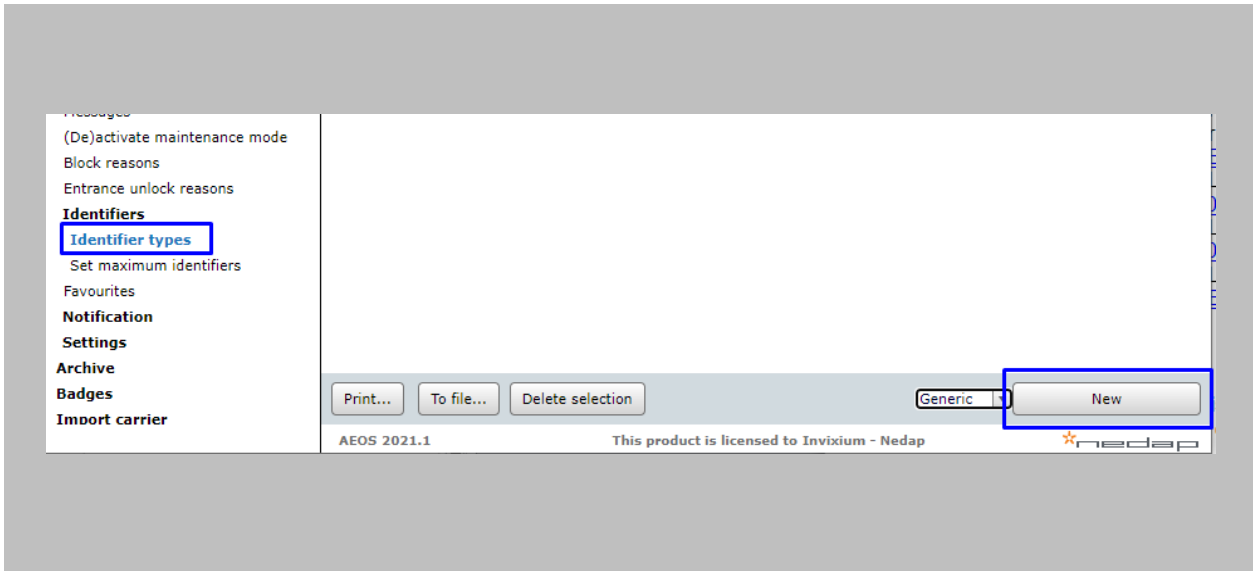


Figure 65: AEOS - Add New Identifier Type

STEP 9

Enter the following details for creating an **Identifier**:

Name: Define an Identifier with the same name as mentioned for **'bms1.name'** in the **'aeos.properties'** file.

For example: IXMEnroll.

Also, enter other mandatory details and Click on **OK.**

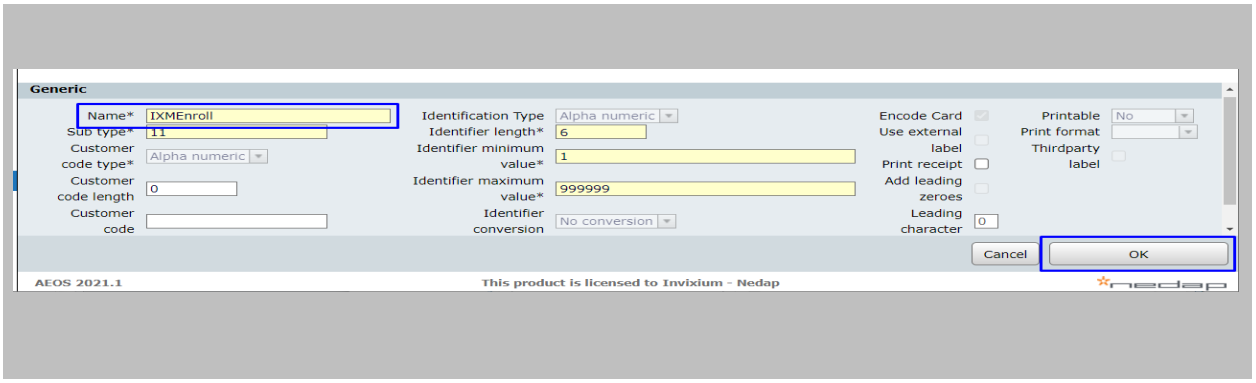


Figure 66: AEOS - New Identifier Type

STEP 10

From the AEOS menu bar, go to **Administration** → **Maintenance** →**Settings.**

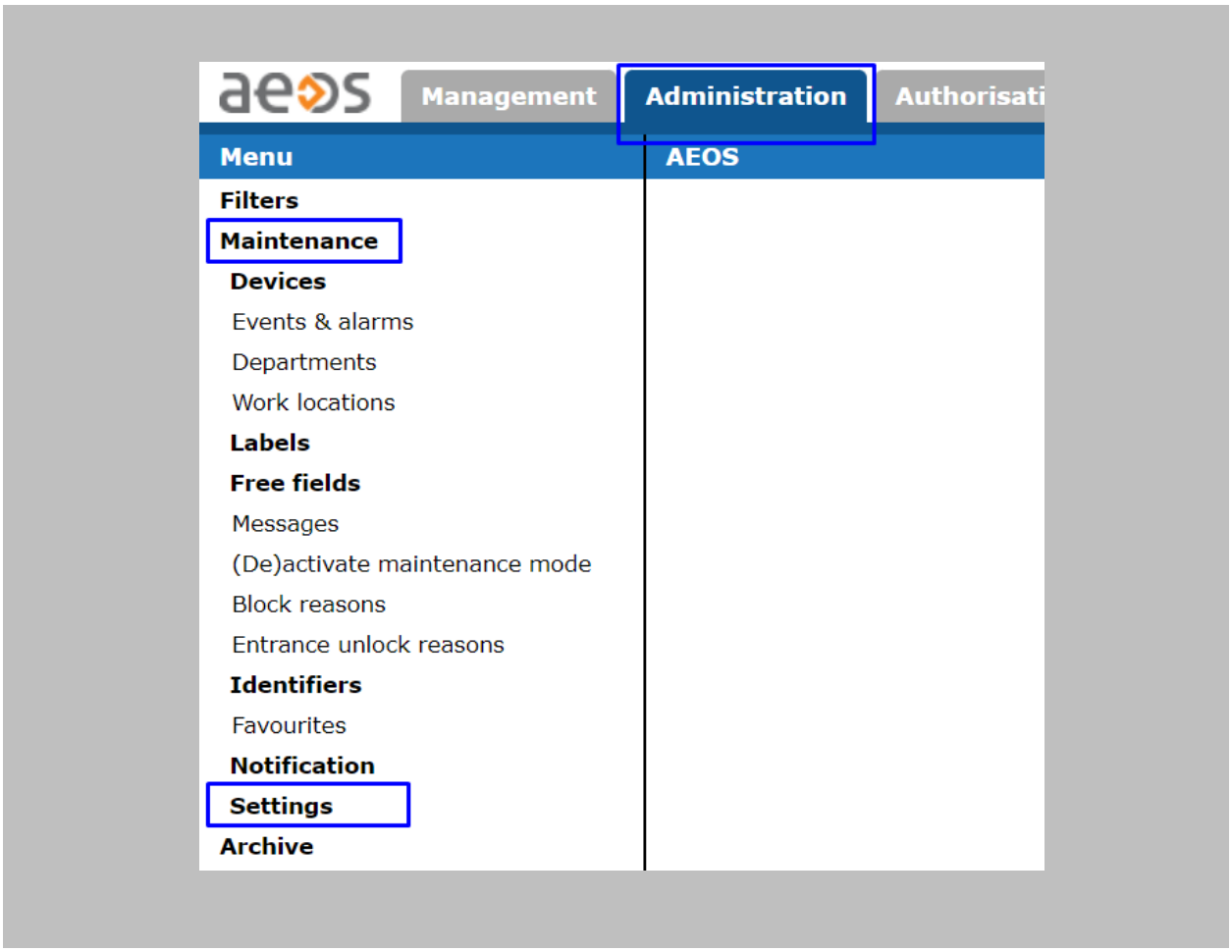


Figure 67: AEOS- Settings

STEP 11

Click on **System Properties.**

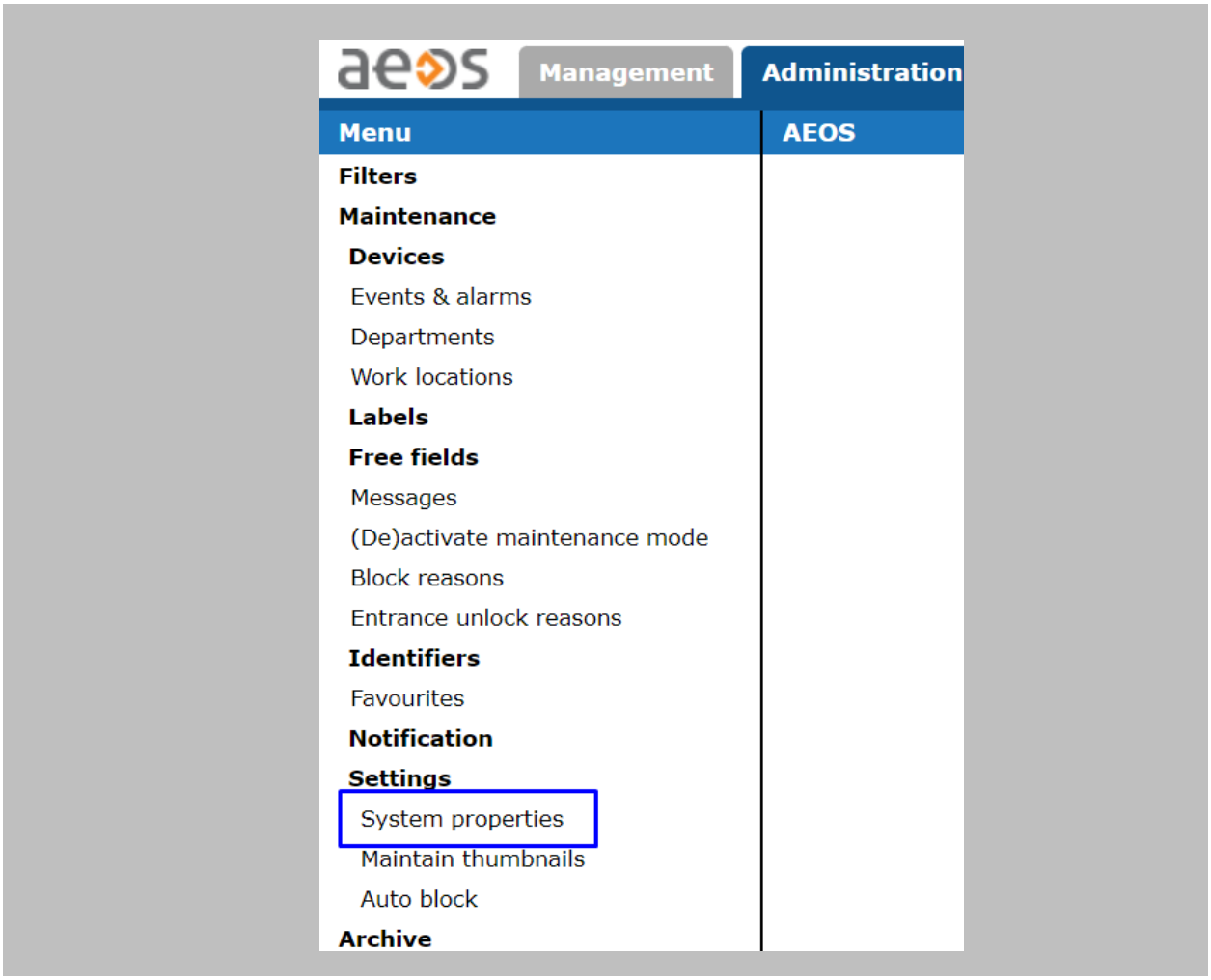


Figure 68: AEOS - System Properties

STEP 12

Update the below settings for performing enrollment from Nedap:

- **04.01 - General Default Identifier Type:** Select the **identifier type** created for enrollment. For example: **'IXMEnroll'**.

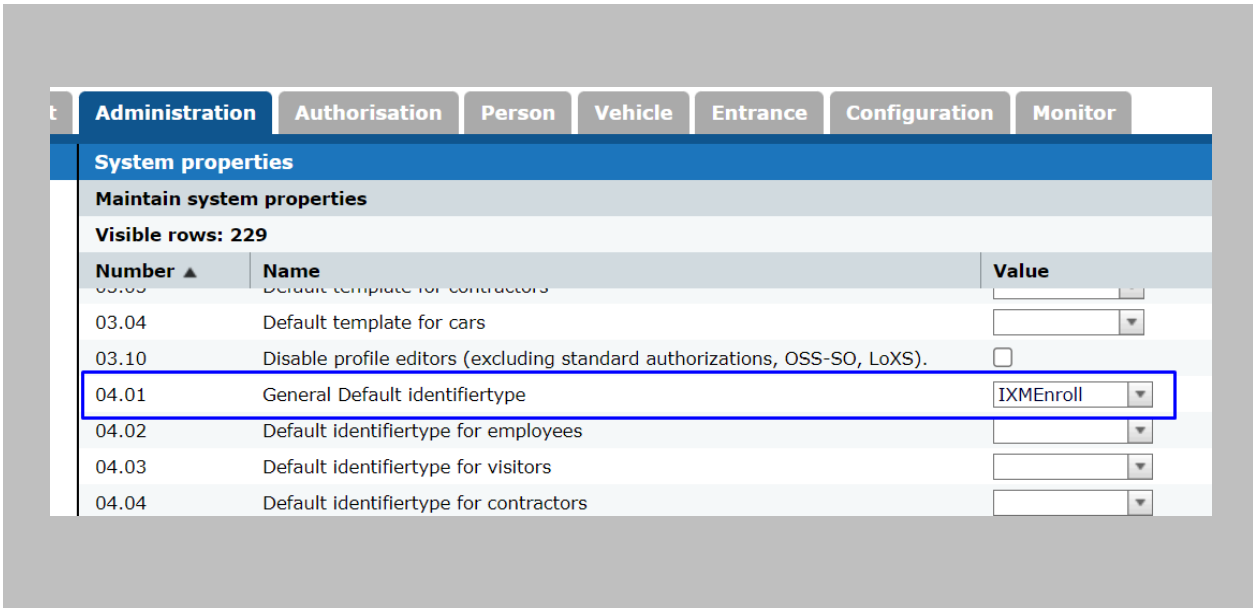


Figure 69: AEOS - System Properties Default Identifier

- **12.36 - Default BioAPI verification method (overrides default verification method):** Select the **identifier type** created for enrollment. For example: **'IXMEnroll'**.

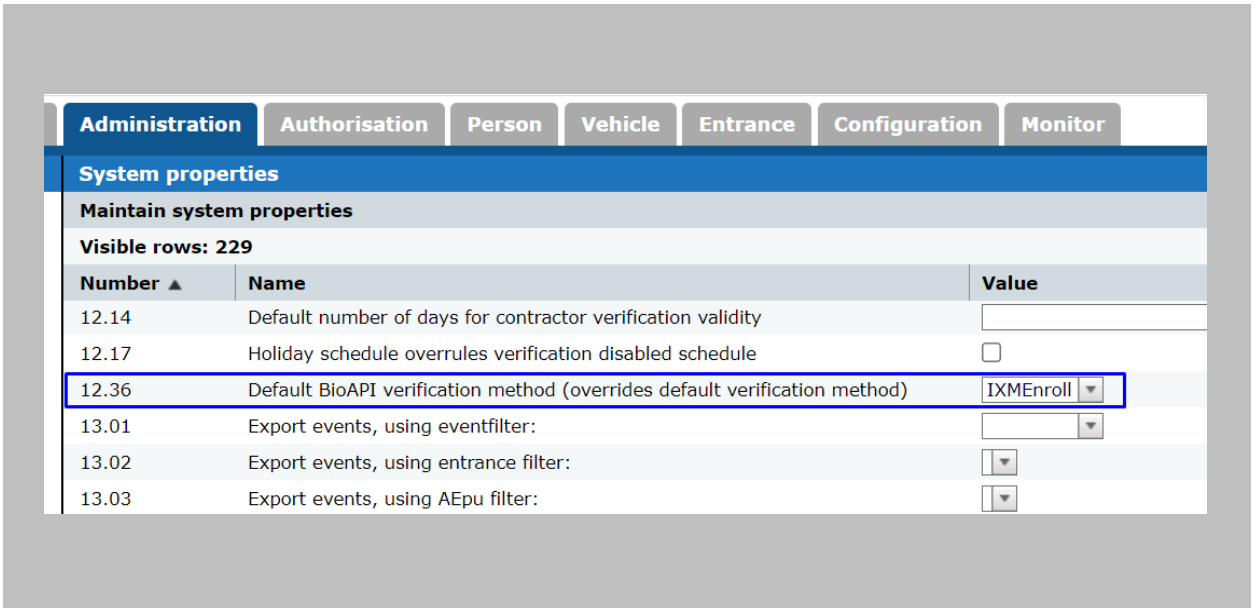


Figure 70: AEOS - System Properties Default BioAPI Verification

- **44.36 - Enable biometric API:** Select the checkbox to enable **biometric API**.

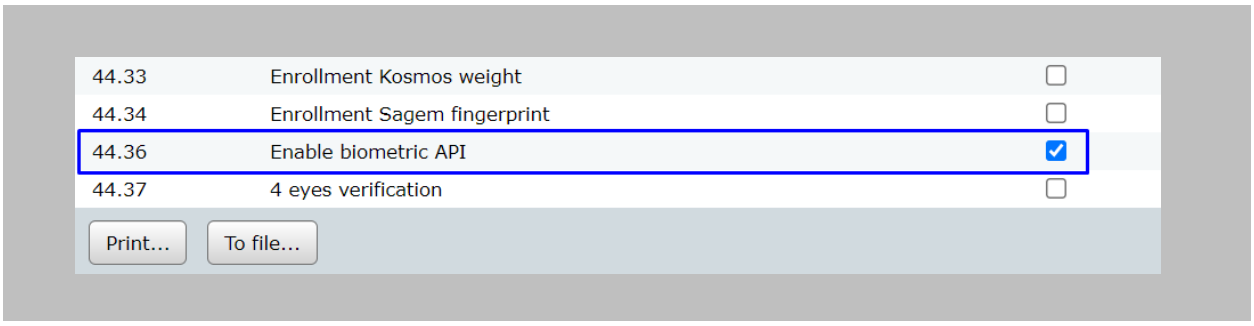


Figure 71: AEOS - System Properties Enable Biometric API

Click on **OK.**

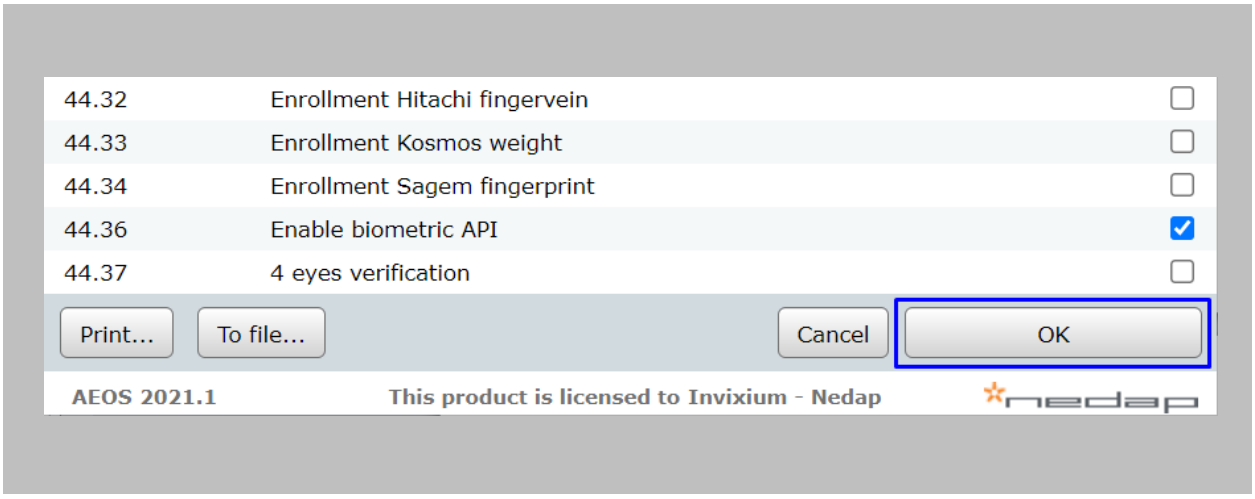


Figure 72: AEOS - Save System Properties

STEP 13

Once all the configurations are saved, restart **AEOS** services.

STEP 14

Go to the location where **IXM WEB** is installed. Open the web.config file to make changes related to the enrollment.

STEP 15

Note: In case of an upgrade of IXM WEB from any previous release to 3.0.36.0, pre-configuration for re-enrollment is required.

Update the below details in **web.config** file:

- Under httpProtocol>> customHeaders replace Content Security Policy with below:

  <add name="Content-Security-Policy"
  value="frame-ancestors 'self' **https://ixm-qa12:8443/aeos/**; script-src 'self' 'unsafe-inline' 'unsafe-eval' http://localhost:1400; style-src 'self' 'unsafe-inline'"/>

  Replace https://ixm-qa12:8443/aeos/ with valid AEOS URL

- For enrollment Set **Cookiesamesite , Samesite to "None**" and **requireSSL to "true"** like below :

```
<sessionState mode="InProc" timeout="60" cookieSameSite="None"
cookieName="Invixium_SID"
sessionIDManagerType="IXMWebMVC4.Helper.CustomSessionIDManager,IXMWebMVC4"/>
<httpCookies httpOnlyCookies="true" sameSite=" None" requireSSL="true"/>
<globalization culture="en-US" uiCulture="auto" enableClientBasedCulture="true"/>
<roleManager enabled="true"/>
<authentication mode="Forms">
<forms loginUrl="~/Home/Logout" timeout="60" slidingExpiration="true"
requireSSL="true" cookieSameSite=" None "/>
</authentication>
```

STEP 16

Reset IIS

Enrollment using Nedap Dashboard URL (recommended)

Note: It is recommended to use Nedap Dashboard URL for enrollment purposes instead of Nedap AEOS application.

Procedure

STEP 1

Open the **AEOS** application using Dashboard URL (e.g. https://ixm-qa12:8443/dashboard)

STEP 2

Click **Person** tab → Search person to enroll → Select Person from the list

STEP 3

Open Badge Editor → Select enrollment Badge type → Click **Re(enroll)** button

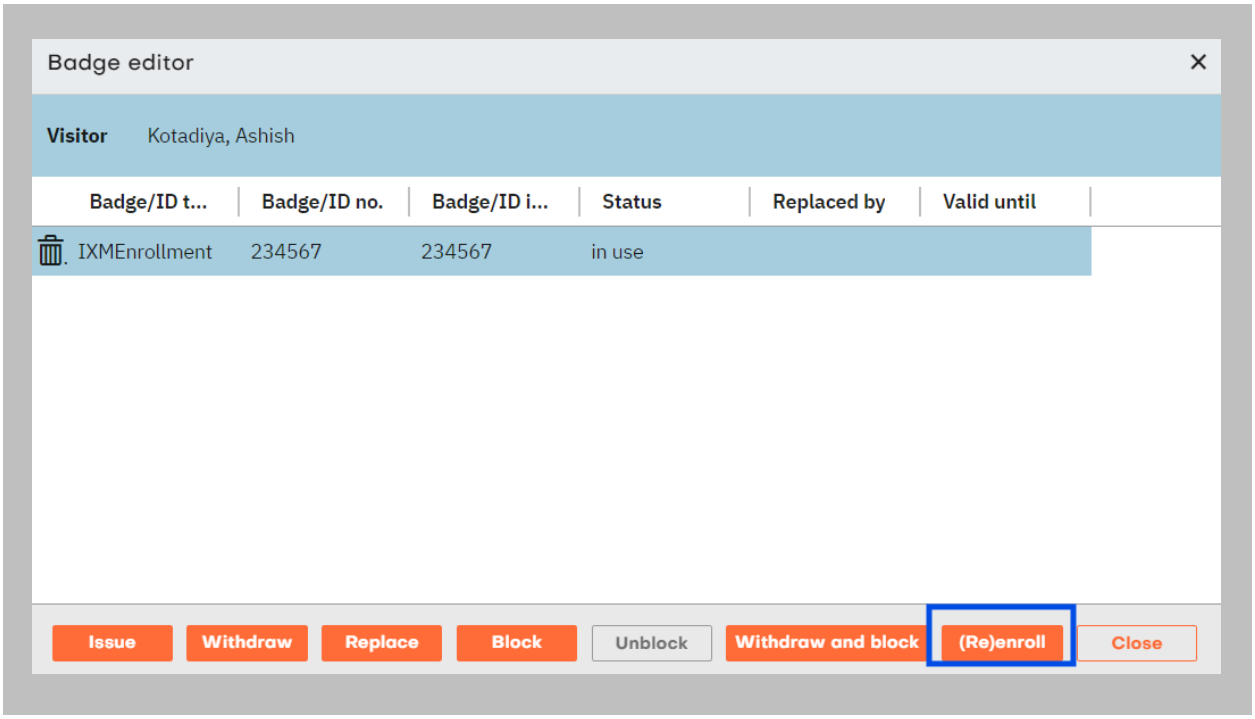


Figure 73: Nedap Dashboard Badge Editor

STEP 4

IXM WEB application will open → Enter login credentials. For first time login select **Remember Me** → click **Sign In**.

STEP 5

Complete enrollment of face, fingerprint or fingervien based on requirement → Click on **Save.** → close the browser.

Follow Invixium Enrollment guidelines for proper enrollment of faces, fingerprints, and finger veins

Enrollment using Nedap AEOS application

STEP 1

Open the **AEOS** application using Dashboard URL (e.g. https://ixm-qa12:8443/dashboard) →Select employee/visitor and click on the **'Enroll Biometric Identifiers'** button →Perform enrollment from this view.

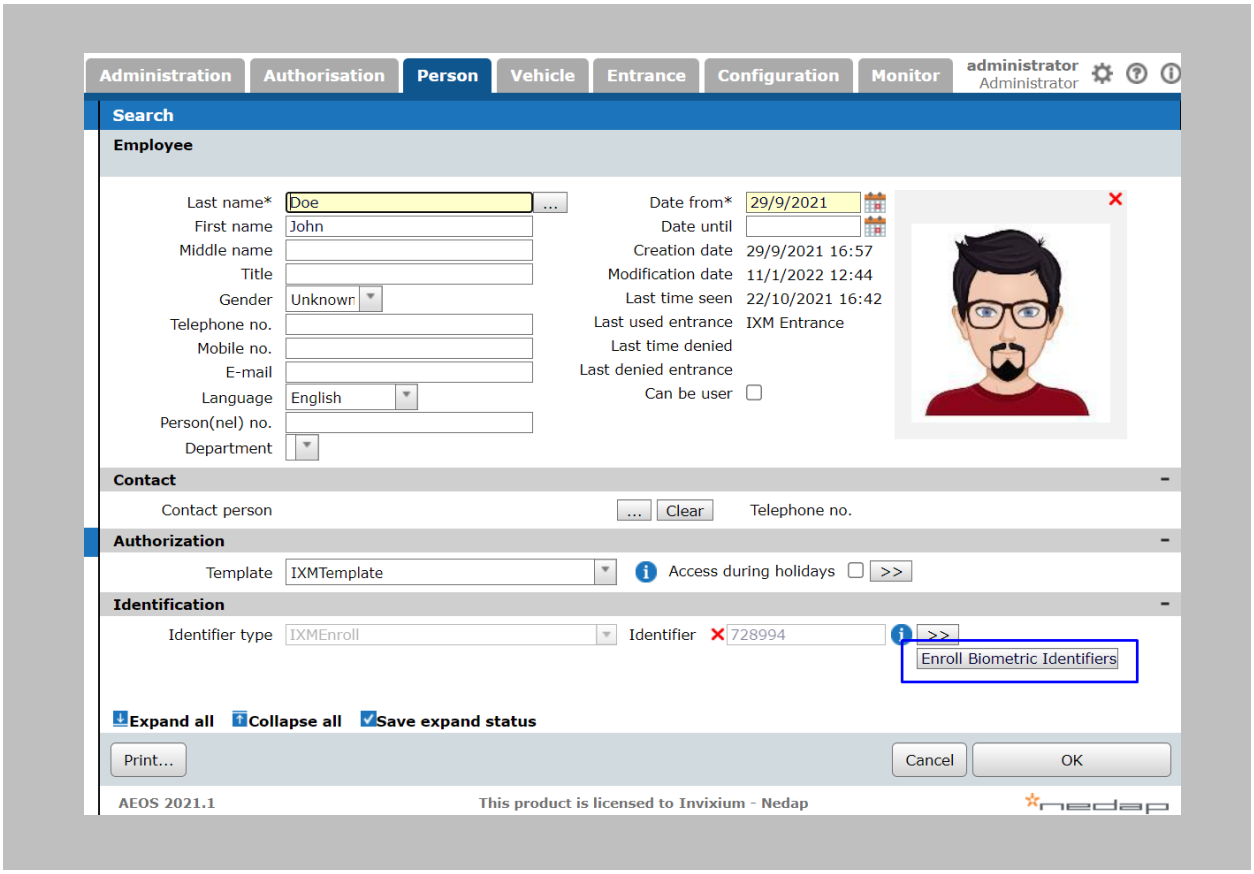


Figure 74: AEOS - Enroll Button

RESULT

The **'Enroll Biometric Identifiers'** button will be displayed on the Employee/Visitors window.

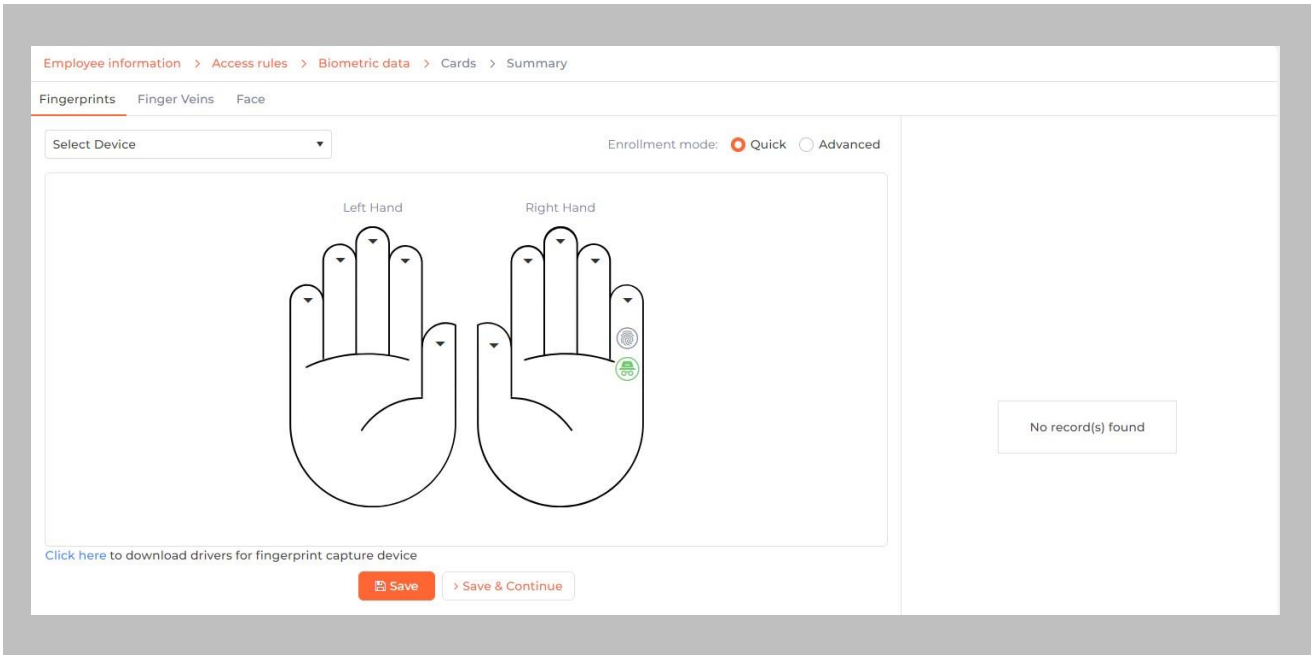


Figure 75: AEOS - Biometric Enrollment

Follow Invixium Enrollment guidelines for proper enrollment of faces, fingerprints, and finger veins.

16. Enrollment Best Practices

Fingerprint Enrollment Best Practices

- Invixium recommends using the index, middle, and ring fingers for enrollment.
- Make sure your finger is flat and centered on the sensor scanning area.
- The finger should not be at an angle and should be straight when placed on the sensor.
- Ensure that the finger is not too dry or too wet. Moisten your finger during enrollment if needed.

Avoid Poor Fingerprint Conditions

- Wet Finger: Wipe excessive moisture from the finger before placement.
- Dry Finger: Use moisturizer or blow warm breath over the finger before placement.
- Stained Finger: Wipe stains off from finger before placement.

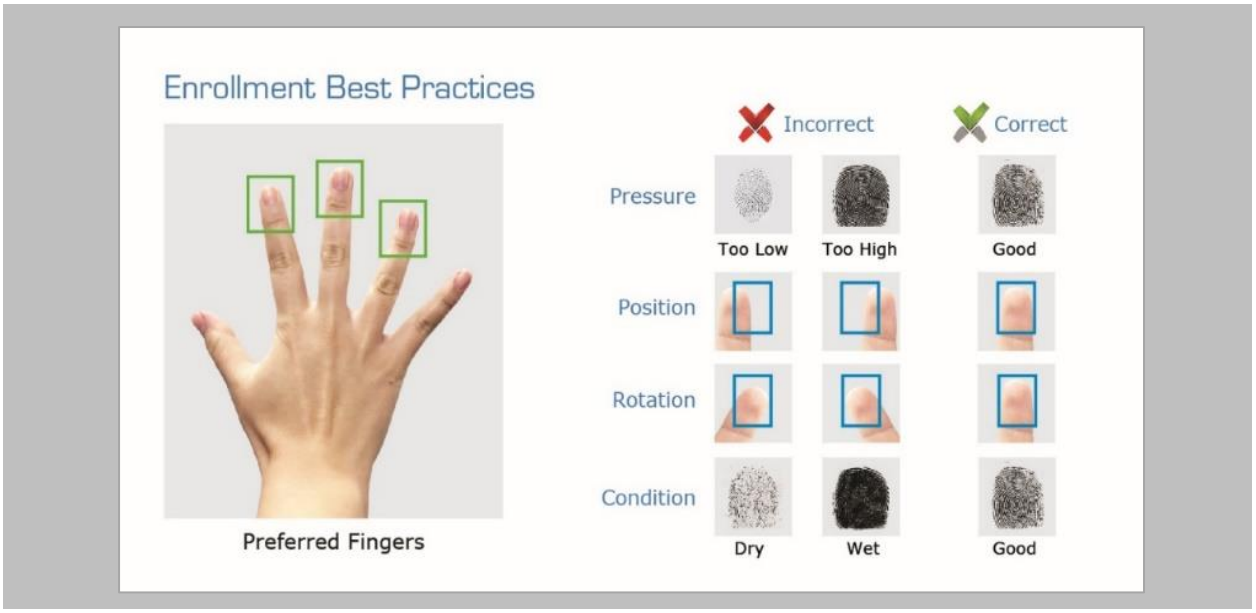


Figure 76: Fingerprint Enrollment Best Practices

Fingerprint Image Samples

Fingerprint Sample	Result	Recommendation
	Good Fingerprint	Always try and get a good fingerprint like this for a good enrollment score
	Fingerprint with cuts	Invixium recommends using Card + Biometrics or Card + PIN
	Dry finger	Moisten finger and re-enroll for better results
	Wet/Sweaty finger	Rub finger on clean cotton cloth and re-enroll for better results

Figure 77: Fingerprint Images Samples

Fingerprint Imaging Do's and Don'ts

Do's:

- Capture the index finger first for the best quality image. If it becomes necessary to capture alternate fingers, use the middle or ring fingers next. Avoid pinkies and thumbs because they generally do not provide a high-quality image.
- Ensure that the finger is flat and centered on the fingerprint scanner area.
- Re-enroll a light fingerprint. If the finger is too dry, moistening the finger will improve the image.
- Re-enroll a finger that has rolled left or right and provided a partial finger capture.

Remember to:

- Identify your fingerprint pattern.
- Locate the core.
- Position the core in the center of the fingerprint scanner.
- Capture an acceptable quality image.

Don'ts:

- Don't accept a bad image that can be improved. This is especially critical during the enrollment process.
- Don't assume your fingerprint is placed correctly.

Finger Vein Enrollment Best Practices

- Invixium recommends using the index and middle fingers for enrollment.
- Make sure your fingertip is resting on the finger guide at the back of the sensor cavity.
- The finger should be completely straight for the best finger vein scan.
- Ensure that the finger is not turned or rotated in any direction.

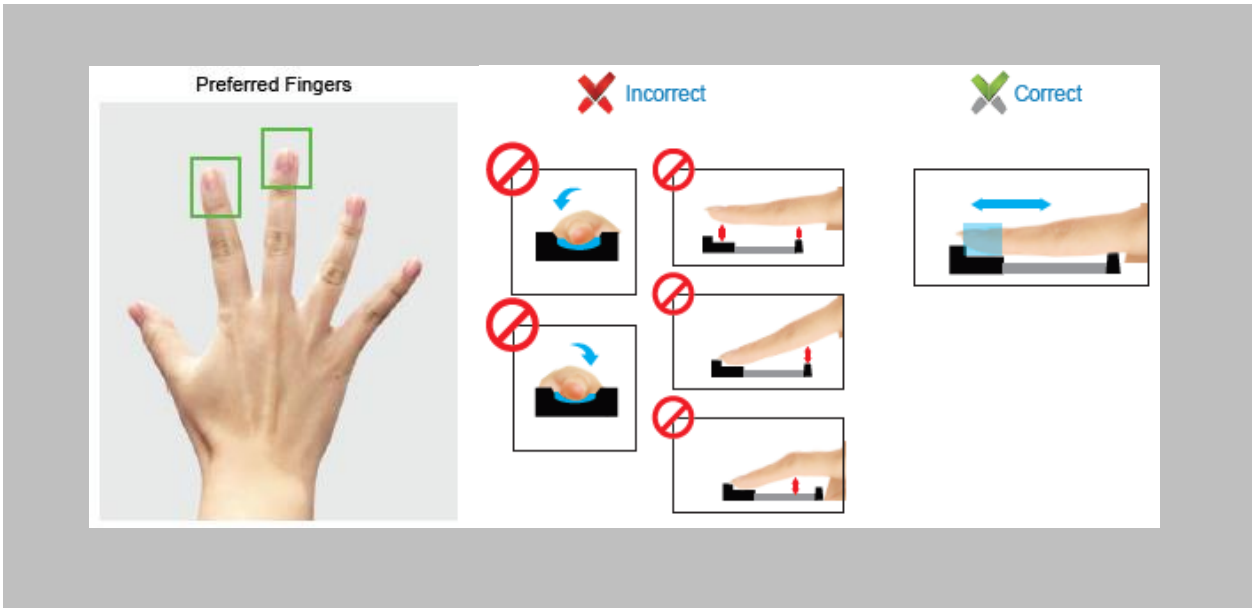


Figure 78: Finger Vein Enrollment Best Practices

Face Enrollment Best Practices

- Invixium recommends standing at 2 to 3 feet from the device when enrolling a face.
- Make sure your entire face is within the frame corners, which will turn green upon correct positioning.
- Look straight at the camera when enrolling your face. Avoid looking in other directions or turning your head during enrollment.

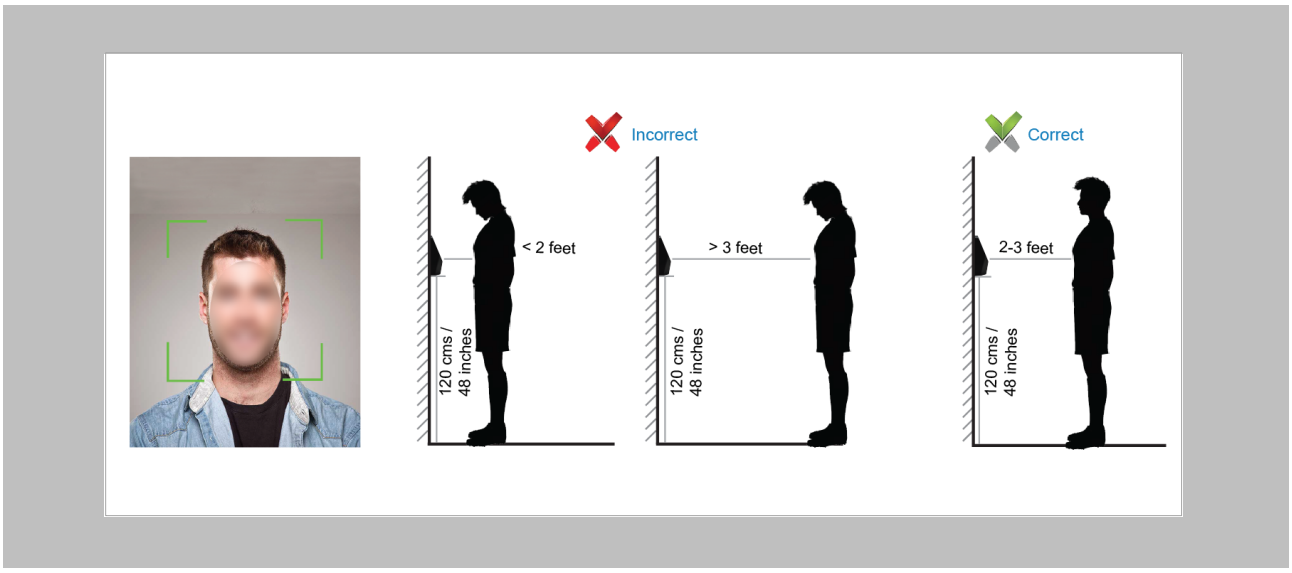


Figure 79: Face Enrollment Best Practices

17. Prerequisites for Getting Access in AEOS

The following configurations are required in Nedap AEOS for user access.

Procedure

STEP 1

Open **AEmon** and select the **AEpu** that is connected to the Invixium device.

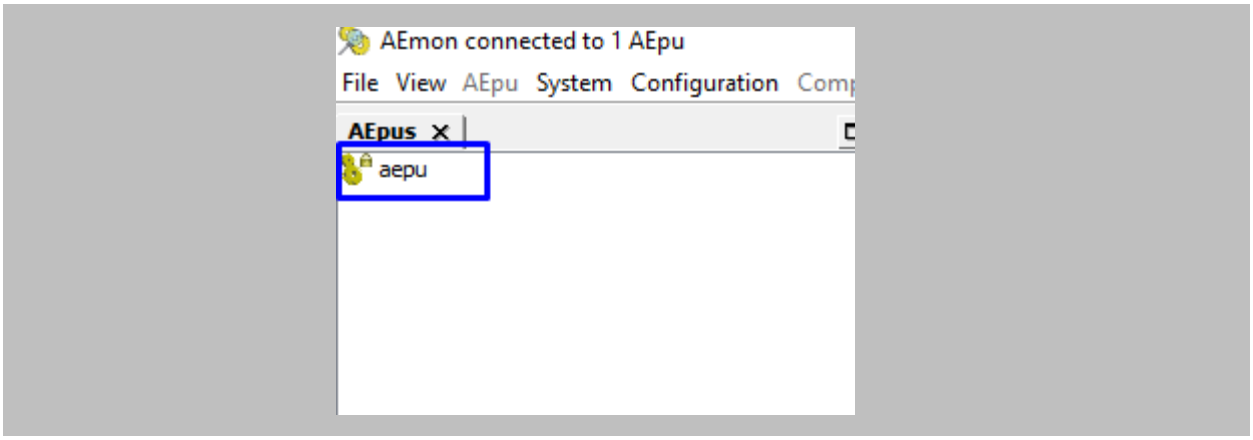


Figure 80: AEmon – Aepu

STEP 2

Go to View → Select Configuration.

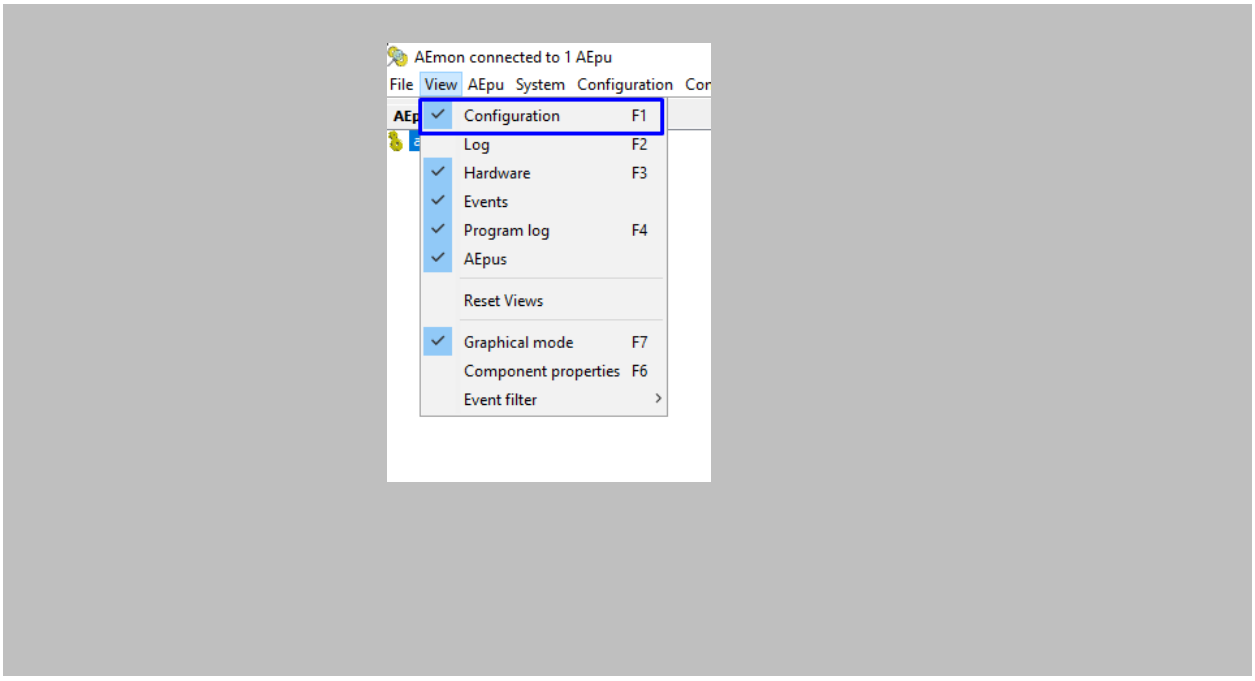


Figure 81: AEmon - AEpu Configuration

STEP 3

On the Configuration window search for StandardDoor → Add StandardDoor.

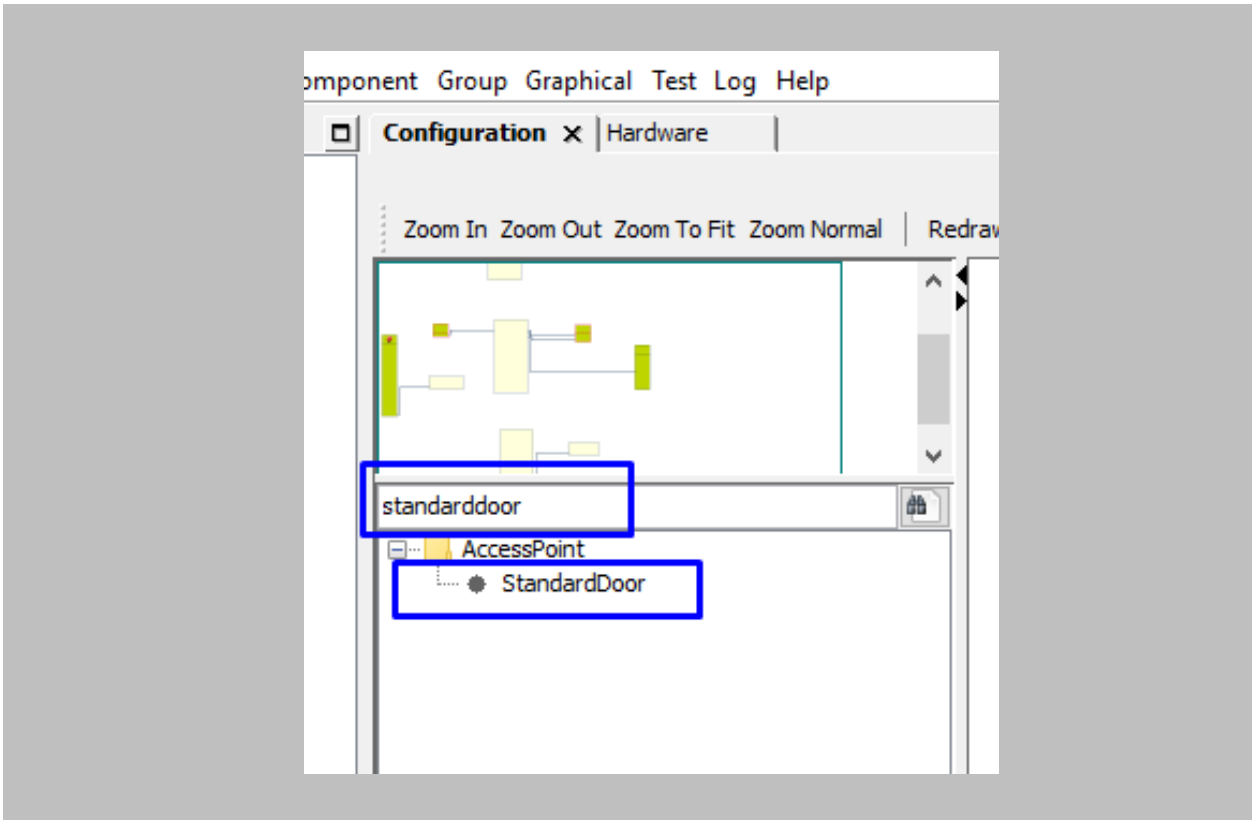


Figure 82: AEmon - Add Standard Door

STEP 4

Right Click on StandardDoor → Select Rename component.

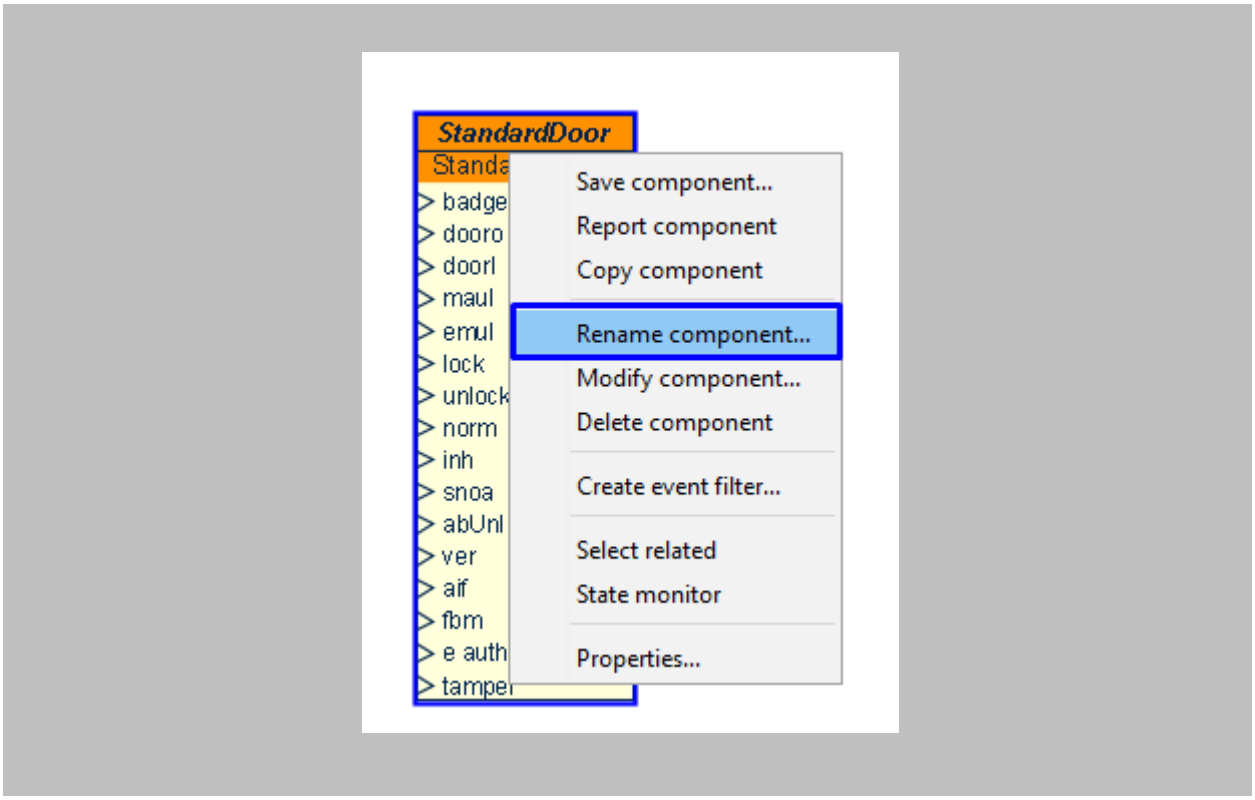


Figure 83: AEmon - Rename Component

Define the name of standard door → Click on **OK.**

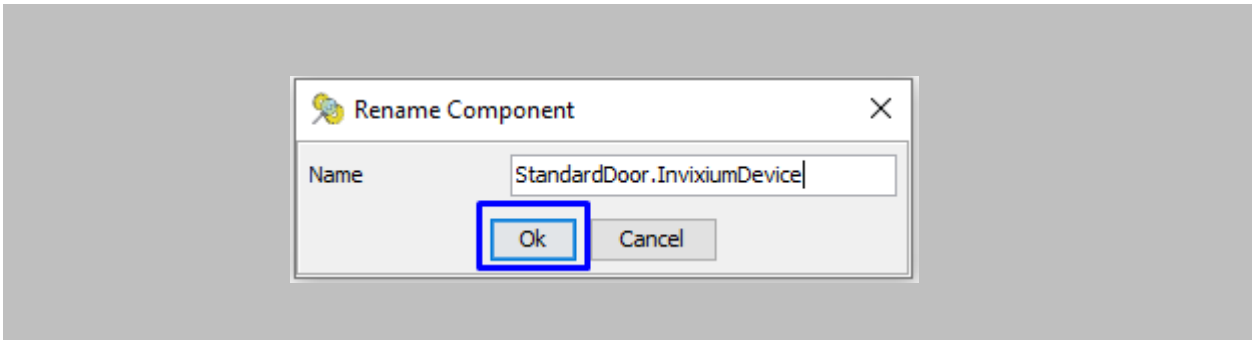


Figure 84: AEmon - Rename Standard Door

STEP 4

To deploy changes on the panel, right-click anywhere on the **'Configuration'** window → click on **Deploy Configuration.**

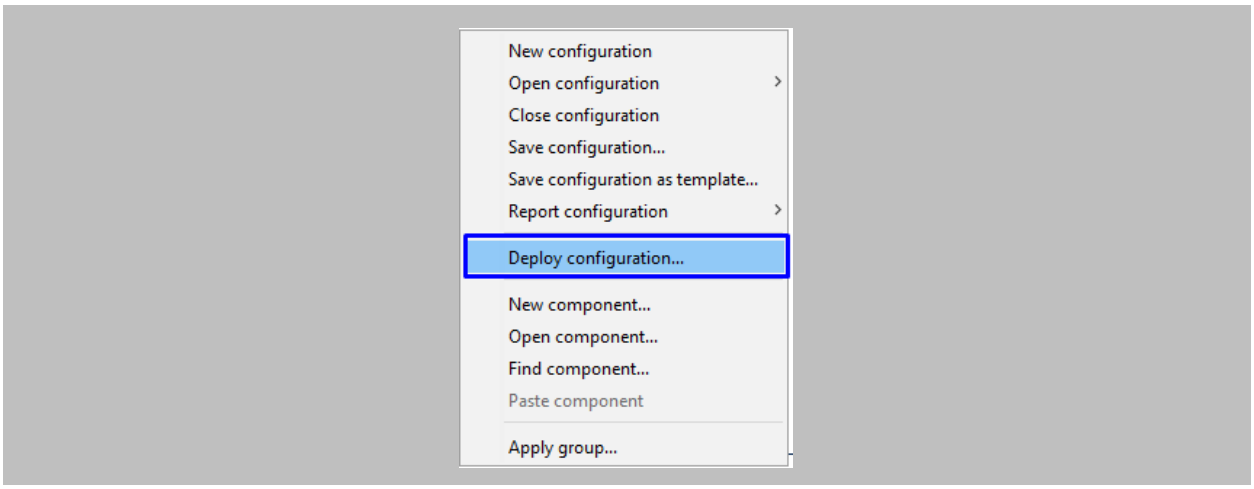


Figure 85: AEmon - Deploy Configuration

STEP 5

Open the **AEOS** application → From the AEOS menu bar, go to **Configuration** → **Maintenance** →**Confirm Access Points.**

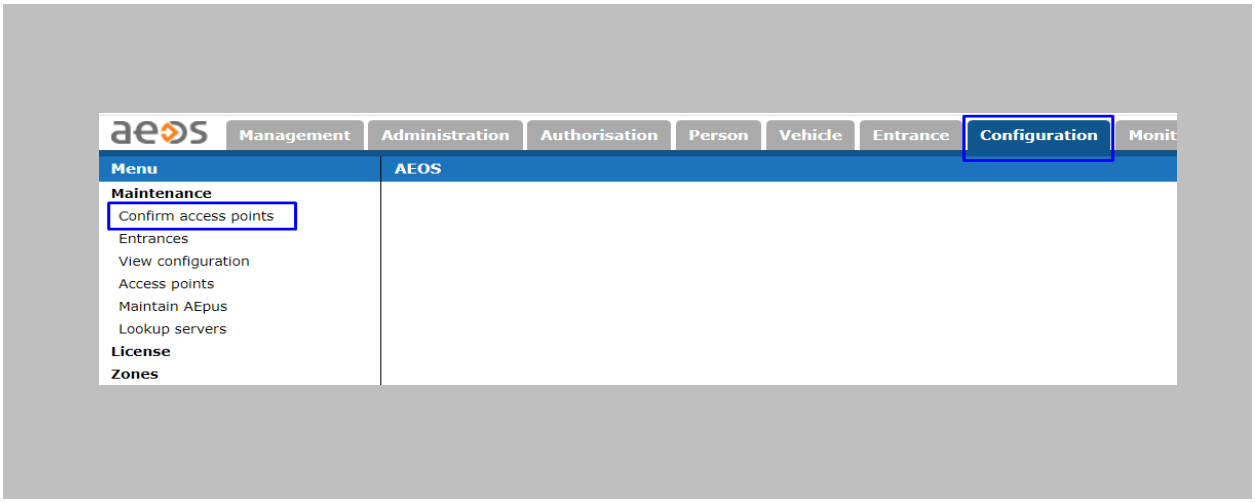


Figure 86: AEOS - Confirm Access Points

STEP 6

All the created **Access Points** will be displayed on this page → Select **Access Point** and click on the **Add** button.

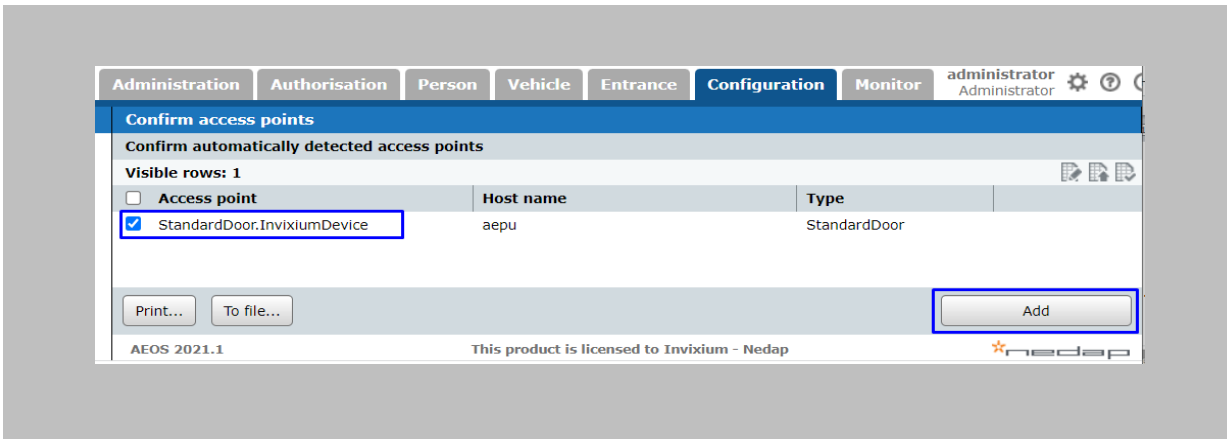


Figure 87: AEOS - Add Access Point

Once the **Access Point** is confirmed it will be displayed on the **Access Points** window→ To verify, go to **Configuration** → **Maintenance** →**Access Points.**

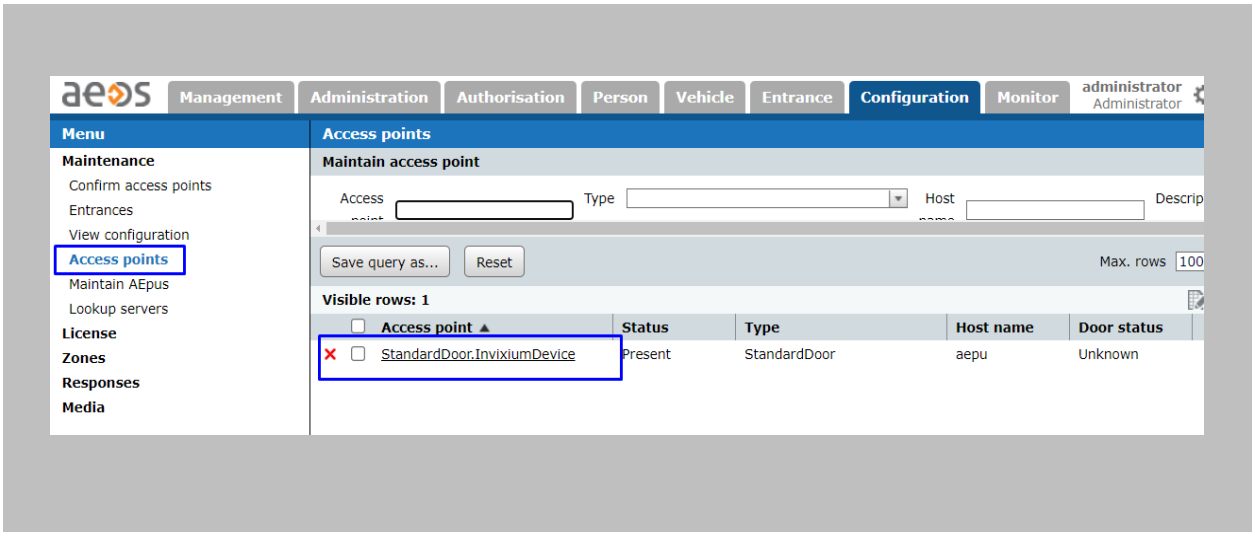


Figure 88: AEOS - Access Point

STEP 7

To add a new entrance, go to **Configuration** → **Maintenance** →**Entrances.**

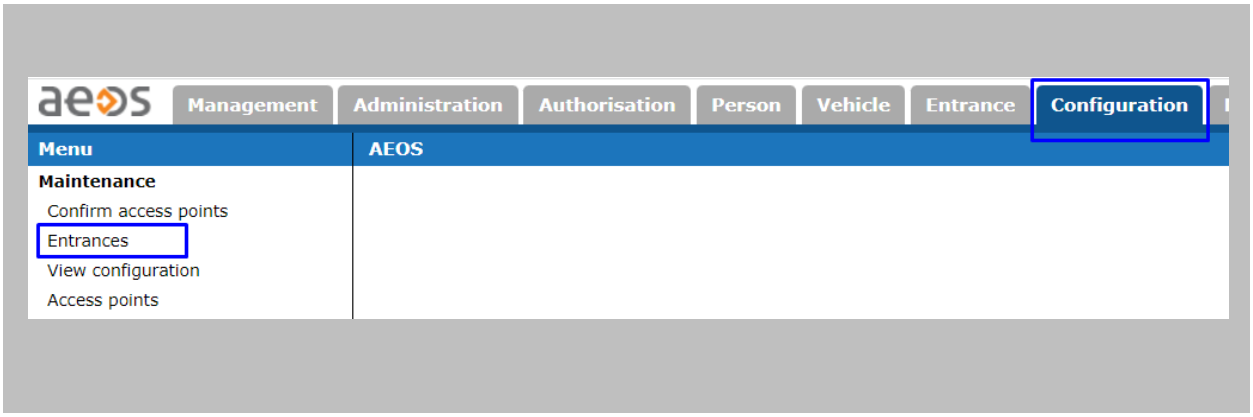


Figure 89: AEOS – Entrances

Click on the **New** button.

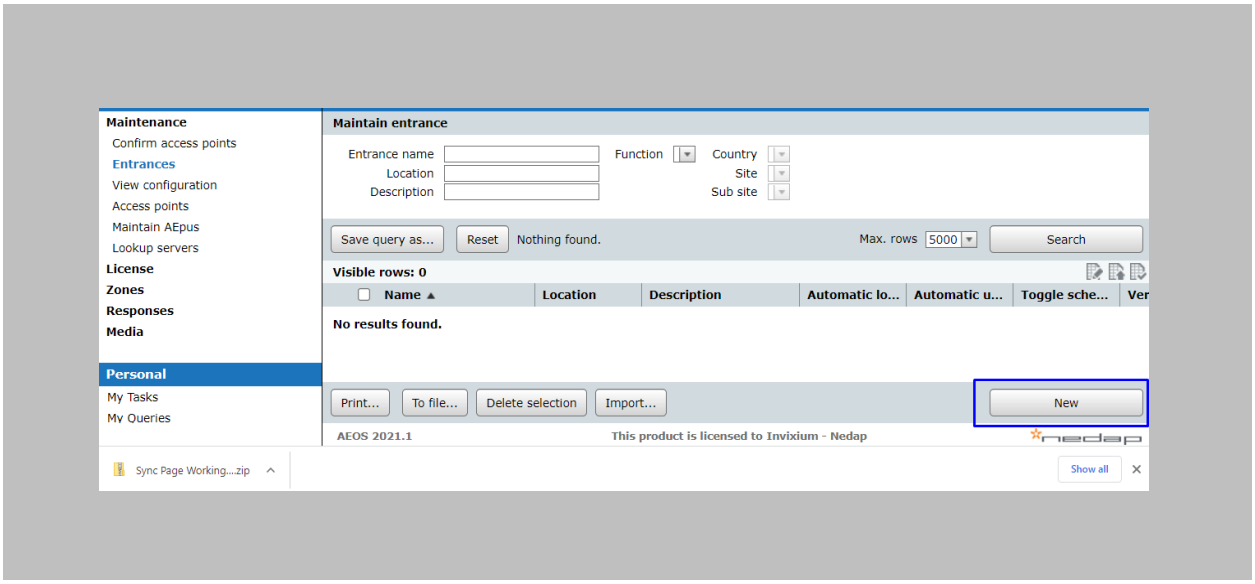


Figure 90: AEOS - New Entrance

STEP 8

Define **Entrance Name** → Click on **Add Access Points** button.

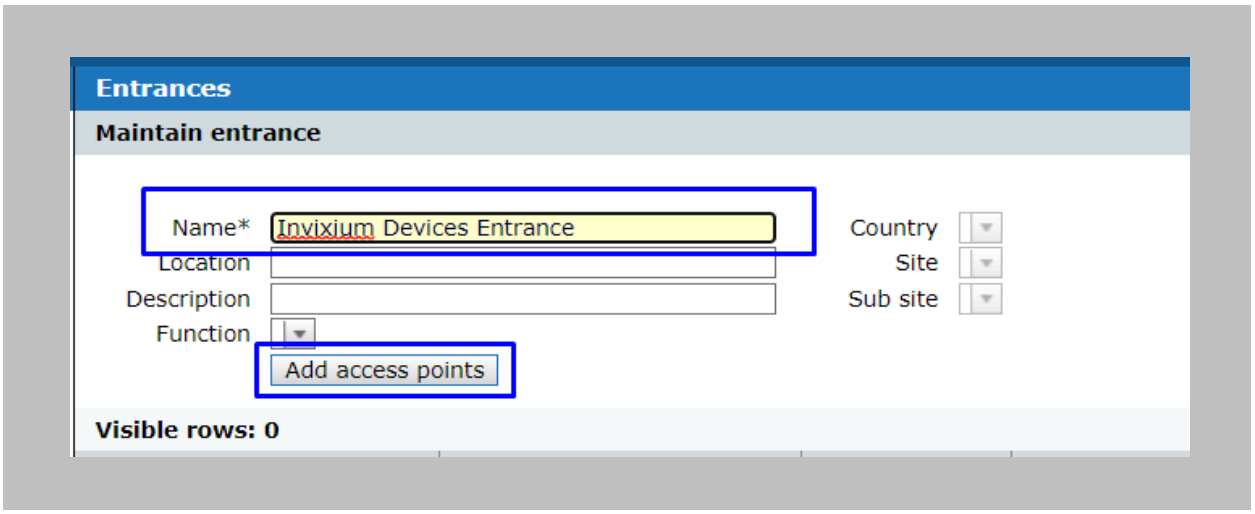


Figure 91: AEOS - Create New Entrance

Select the **Access Point** that you want to add for this **Entrance** and click on the **OK** button.

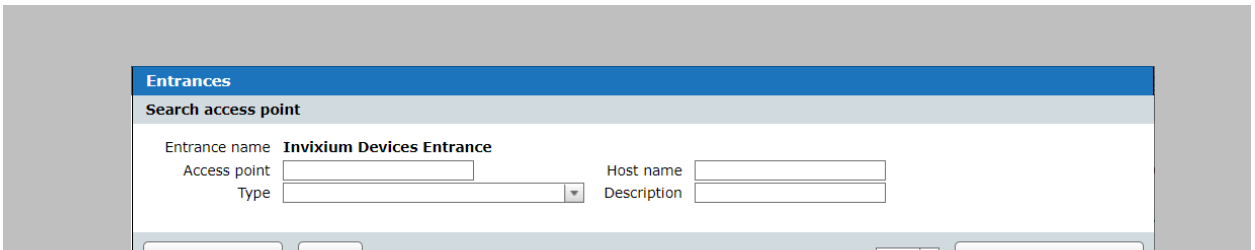


Figure 92: AEOS - Add Access Point in Entrance

Once the **Access Point** is added click on the OK button.

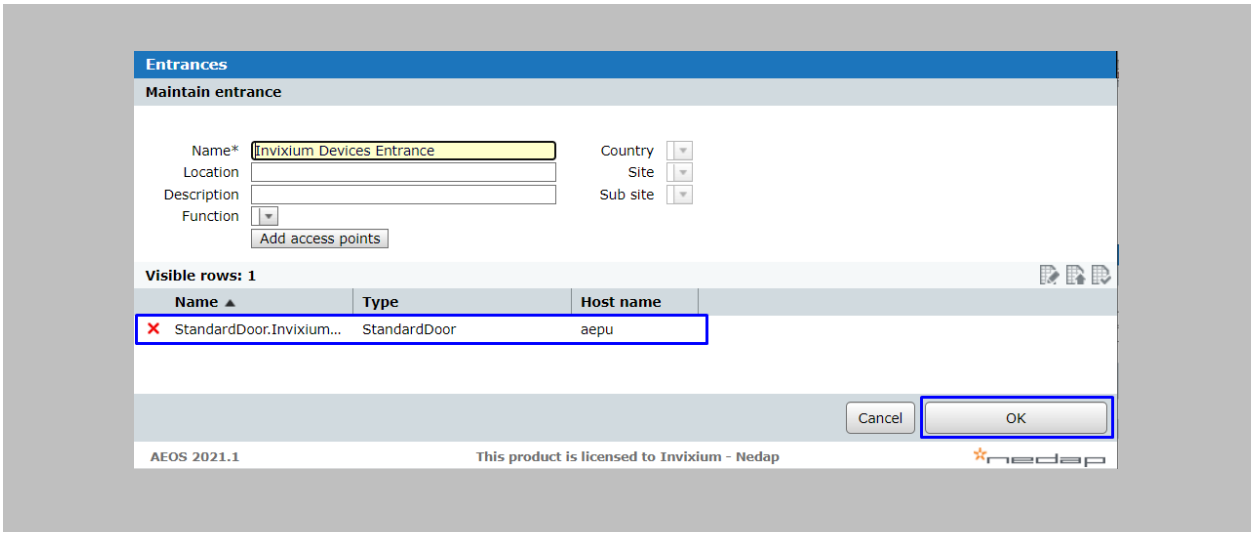


Figure 93: AEOS - Save Entrance

STEP 9

Go to **Authorization** → **Maintenance** →**Day/time Schedules** to create a new schedule.

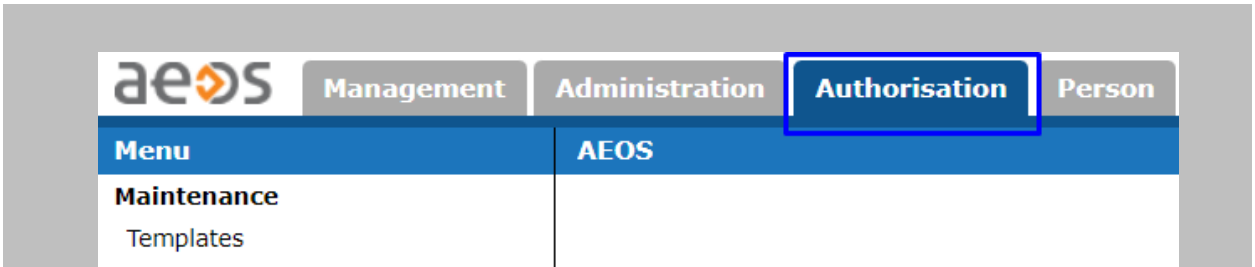


Figure 94: AEOS – DayTimeSchedules

Select **Weekly Schedule** from the dropdown and click on the **New** button.

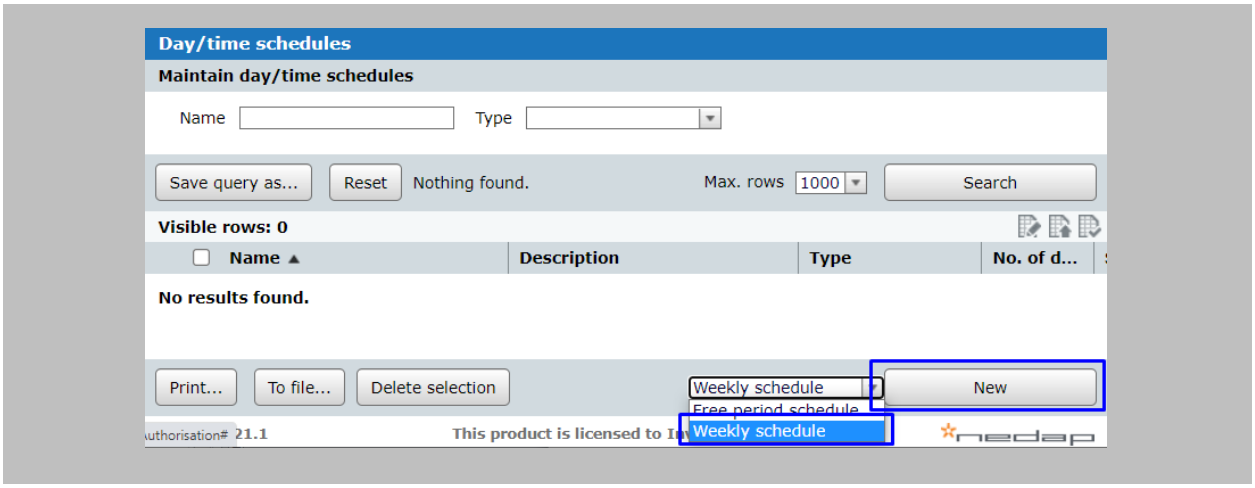


Figure 95: AEOS - New Weekly Schedule

STEP 10

Define **Schedule Name** → Define the start and end time for the new schedule as per your requirement →Click on the **OK** button.

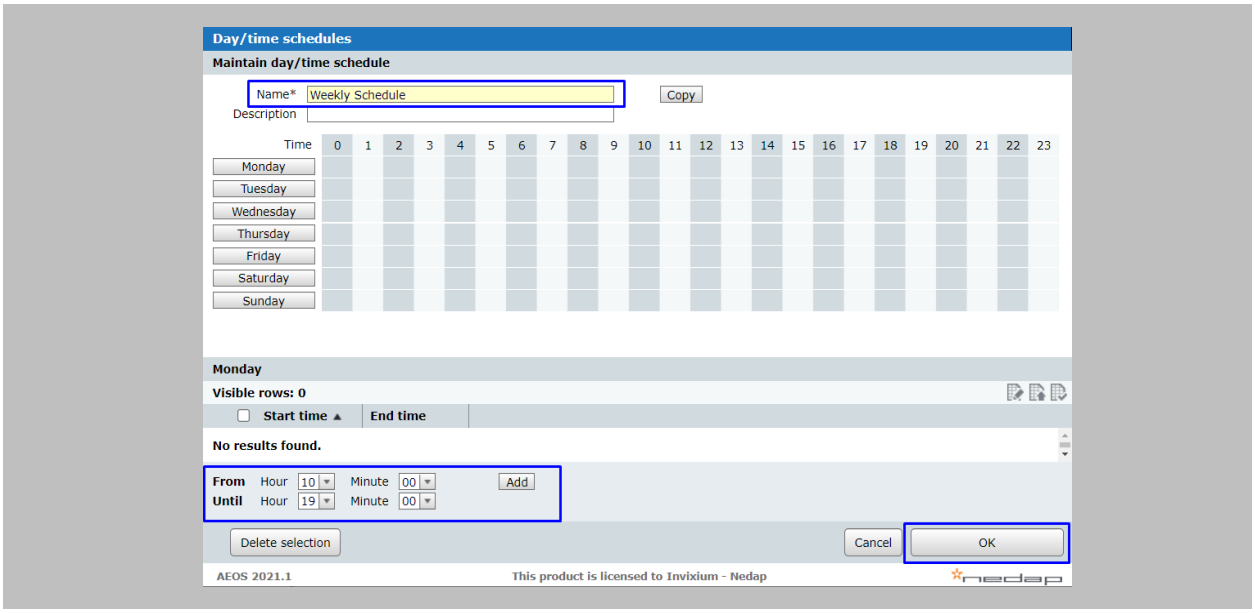


Figure 96: AEOS - Define Weekly Schedule

STEP 11

For **Employee Groups** creation, go to **Authorization** → **Maintenance** →**Employee Group.**

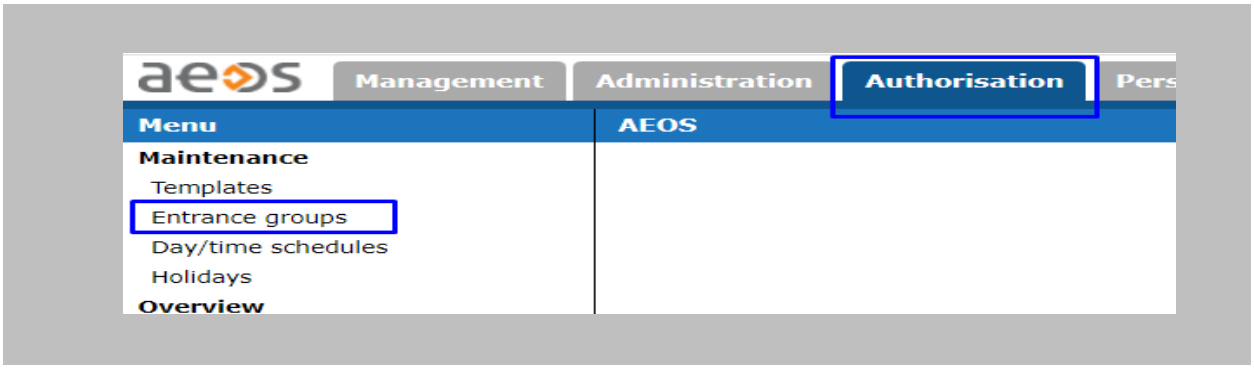


Figure 97: AEOS - Entrance Groups

Click on the **New** button.

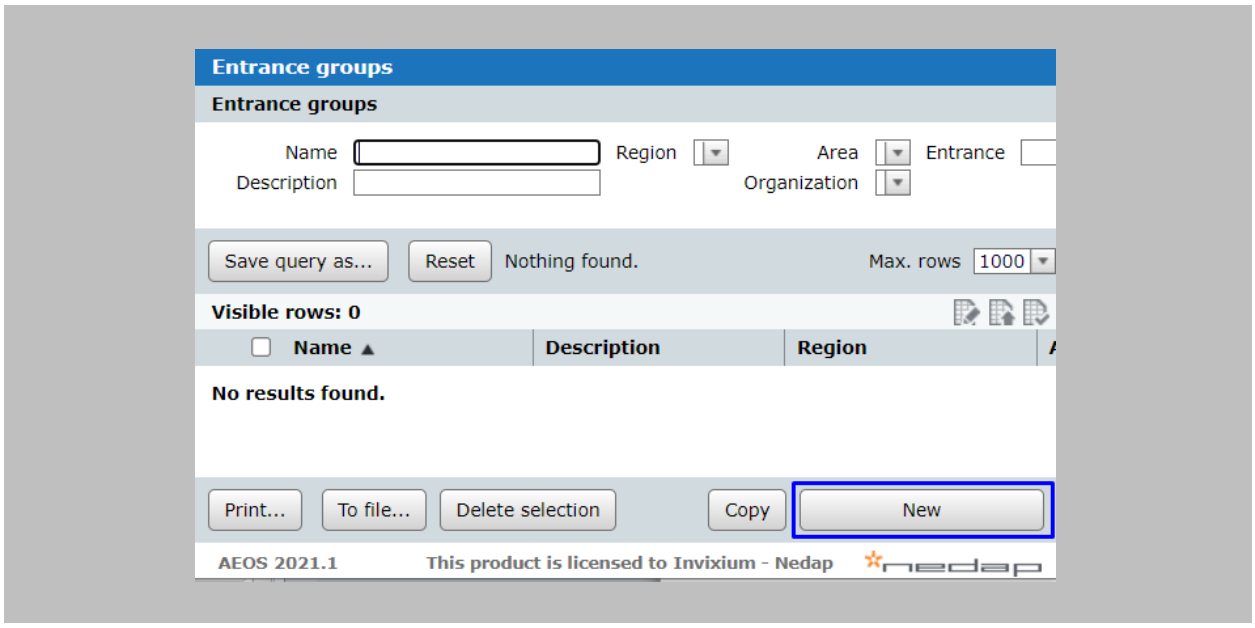


Figure 98: AEOS - New Entrance Group

STEP 12

Define **Entrance Group Name** → Click on **Add Entrances** button.

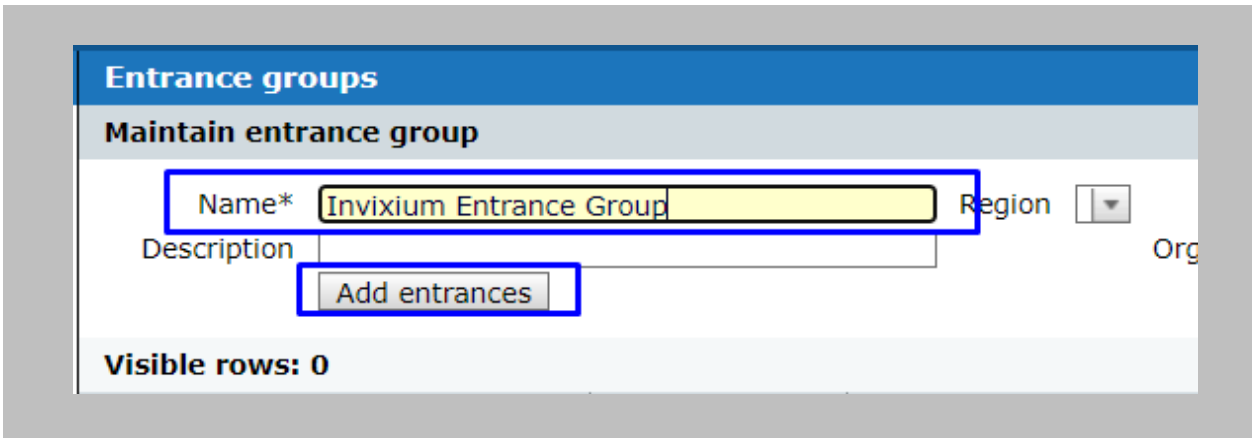


Figure 99: AEOS - Add Entrance in Entrance Group

Select the **Entrance** which you want to add to this **Entrance Group** and click on the **OK** button.

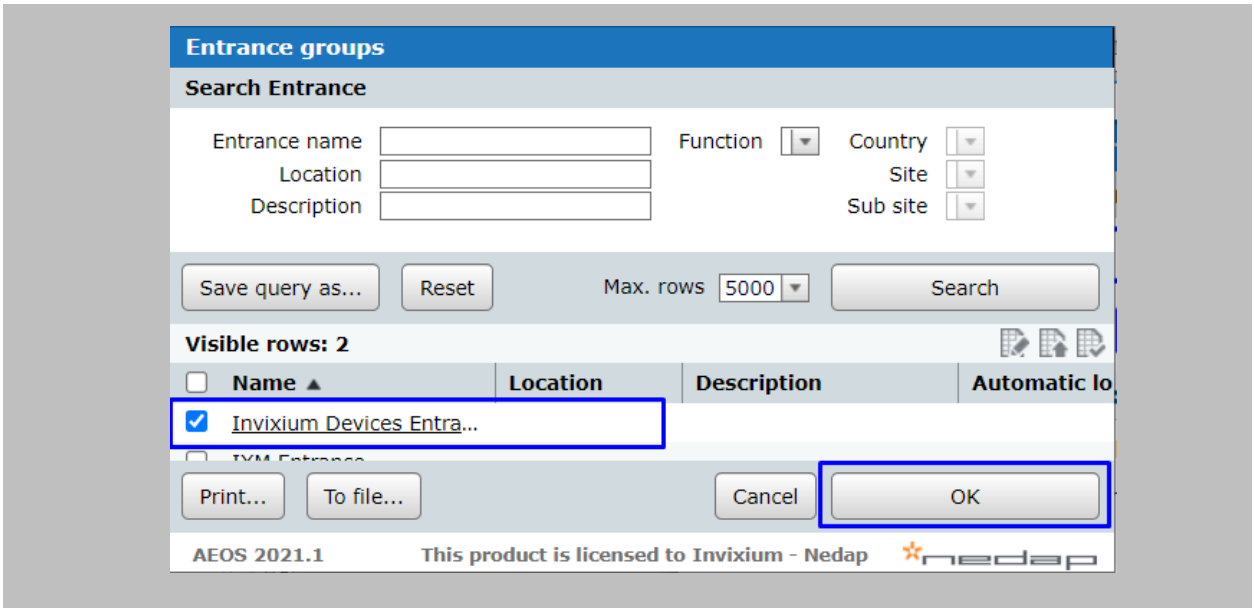


Figure 100: AEOS - Add Entrance Group

Once the **Entrance** is added click on the OK button.

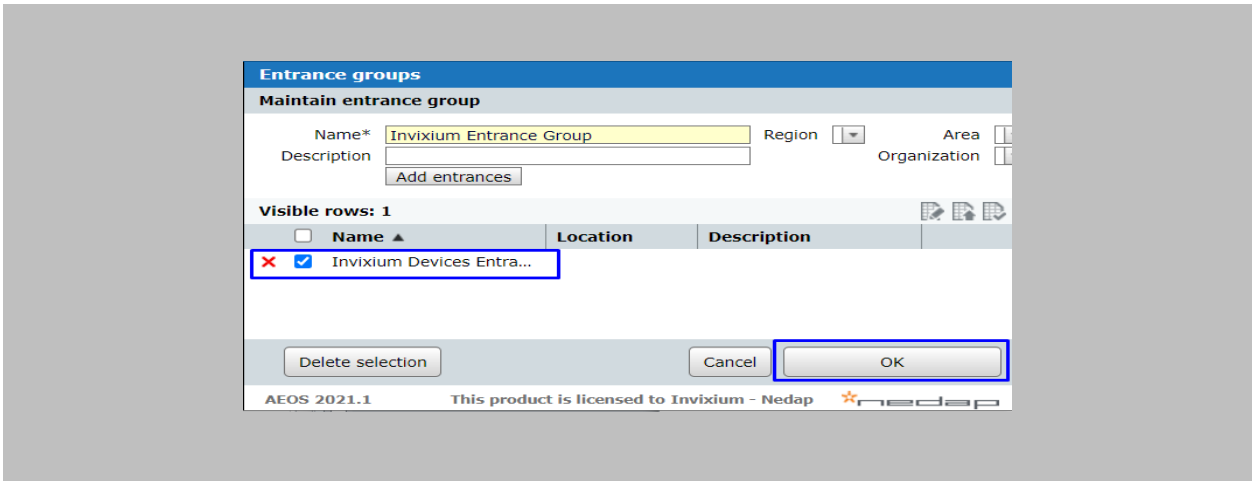


Figure 101: AEOS - Save Entrance Group

STEP 13

For **Template** creation, go to **Authorization** → **Maintenance** →**Templates.**

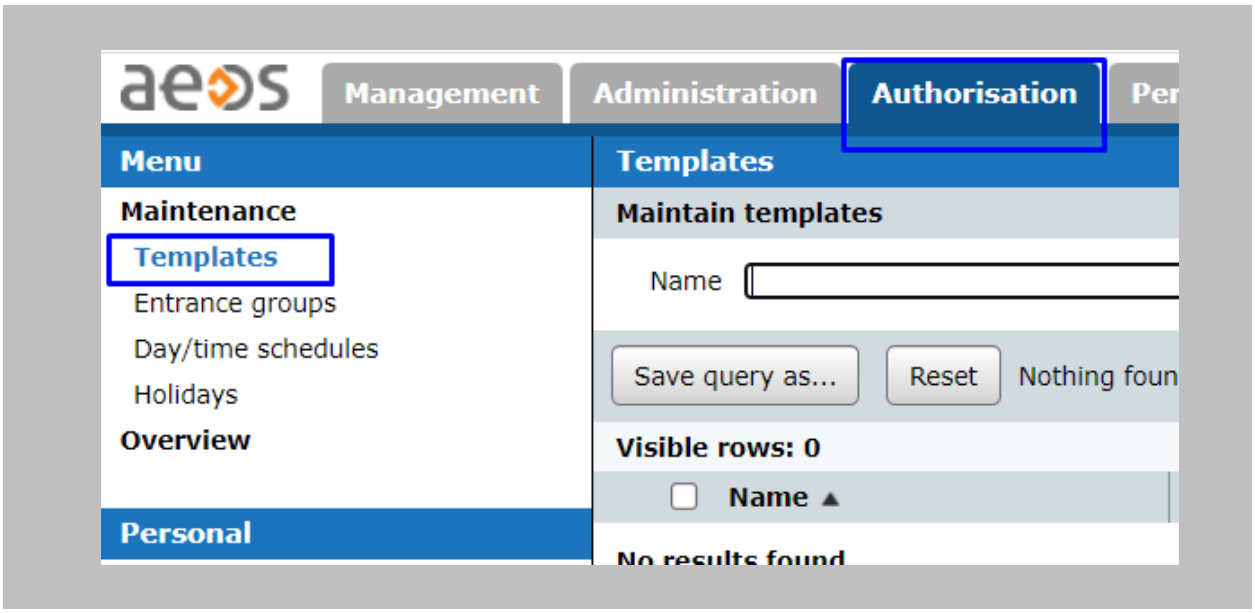


Figure 102: AEOS – Template

Click on the **New** button.

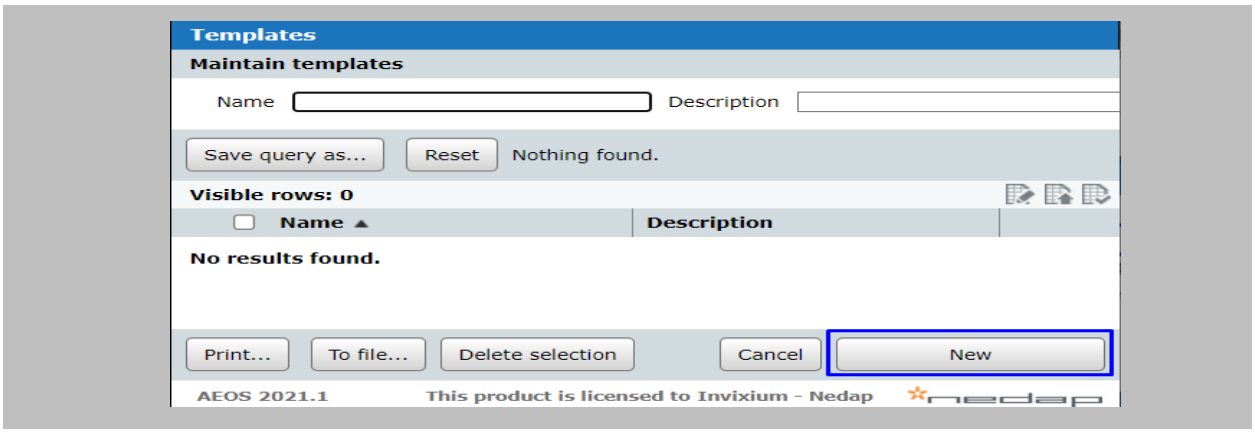


Figure 103: AEOS - New Template

STEP 14

Define **Template Name** → Click on the **Add** button for adding an **Entrance Group** to the **Template**.

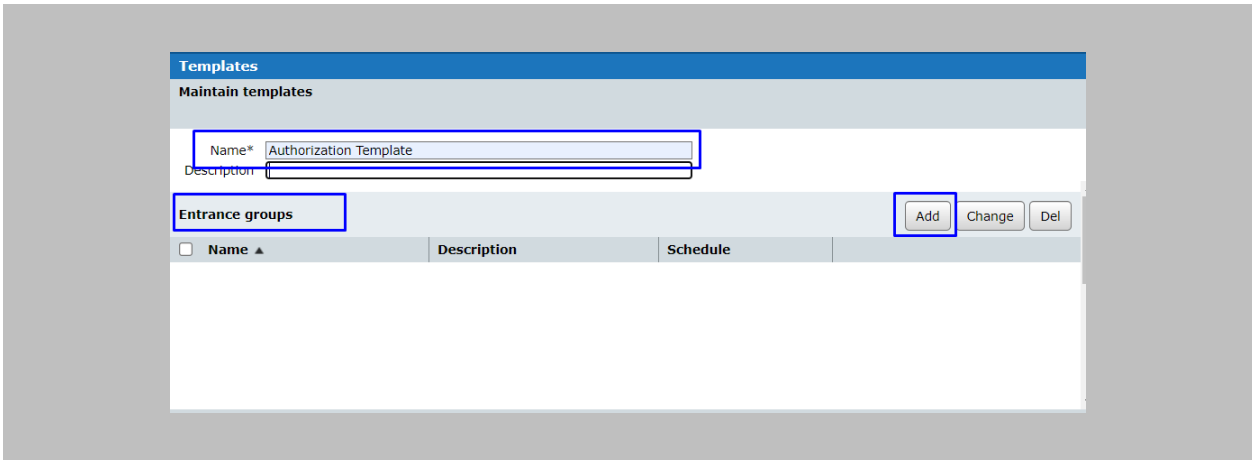


Figure 104: AEOS Template - Add Entrance Group

Select the **Entrance Group** from the list of Entrance Groups and click on the **OK** button.

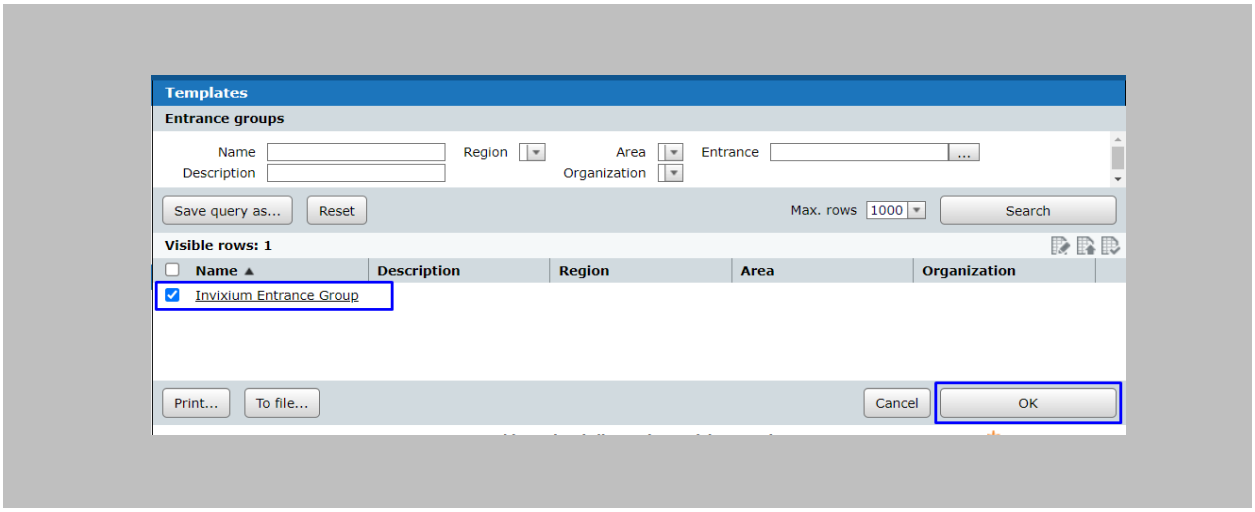


Figure 105: AEOS Template - Add Entrance Group

Select **Schedule** from the dropdown for the selected **Entrance Group** and click on the **OK** button.

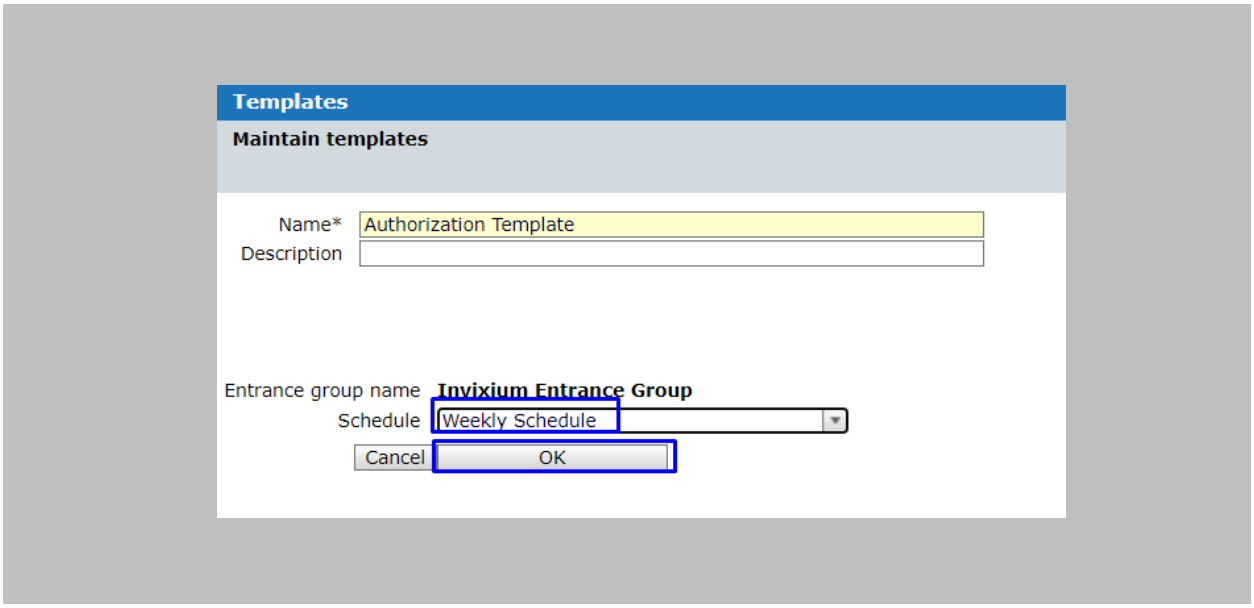


Figure 106: AEOS Template - Assign Schedule to Entrance Group

STEP 15

Click on the **Add** button to add an **Entrance** to the **Template**.

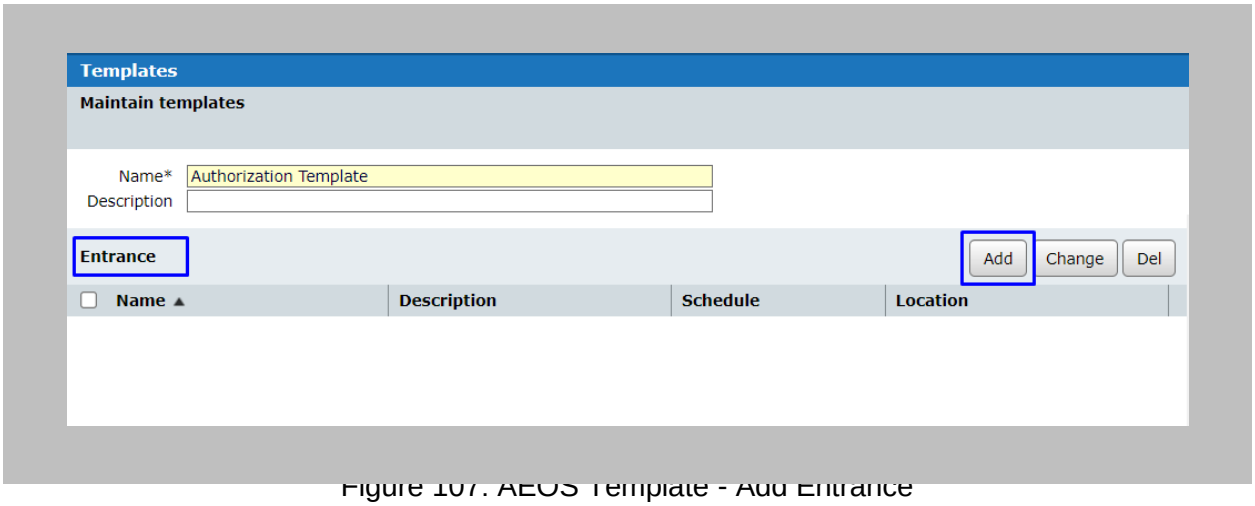


Figure 107: AEOS Template - Add Entrance

Select the **Entrance** from the list of **Entrances** and click on the **OK** button.

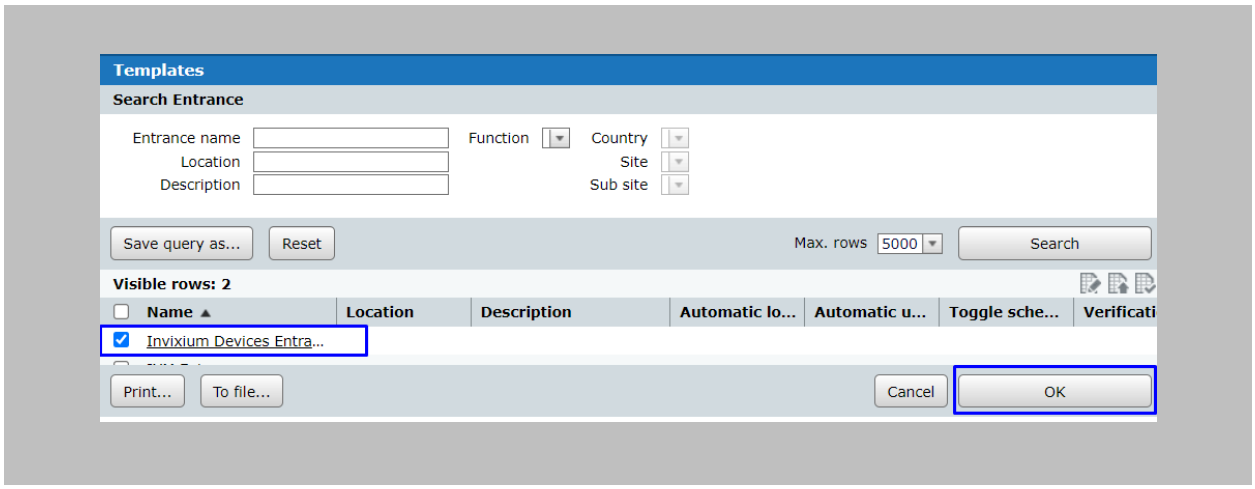


Figure 108: AEOS Template - Save Entrance

Select the **Schedule** from the dropdown for the selected **Entrance** and click on the **OK** button.

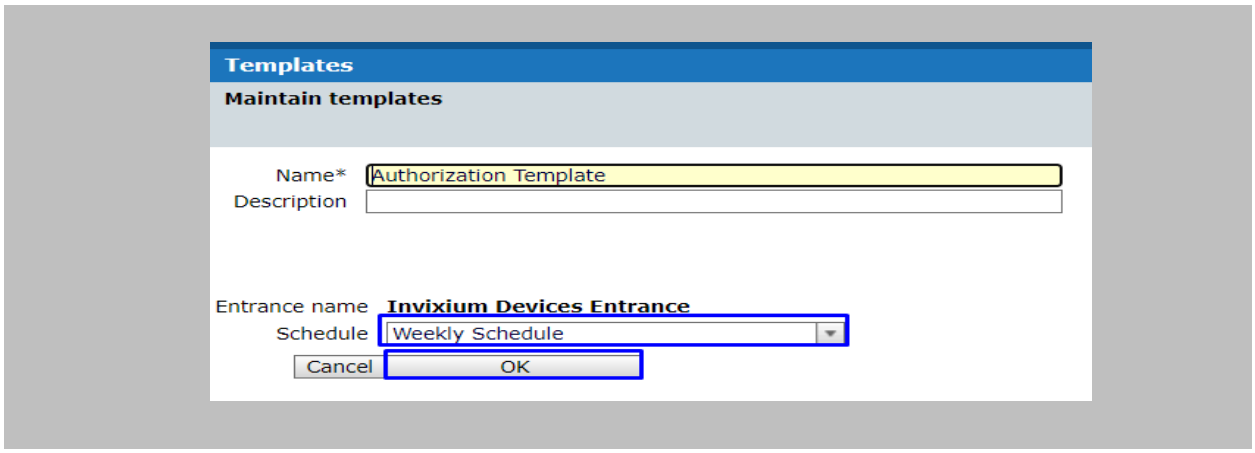


Figure 109: AEOS Template - Assign Schedule to Entrance

STEP 16

Once **Entrances** and **Entrance Groups** are added to the **Template**, click on the OK button.

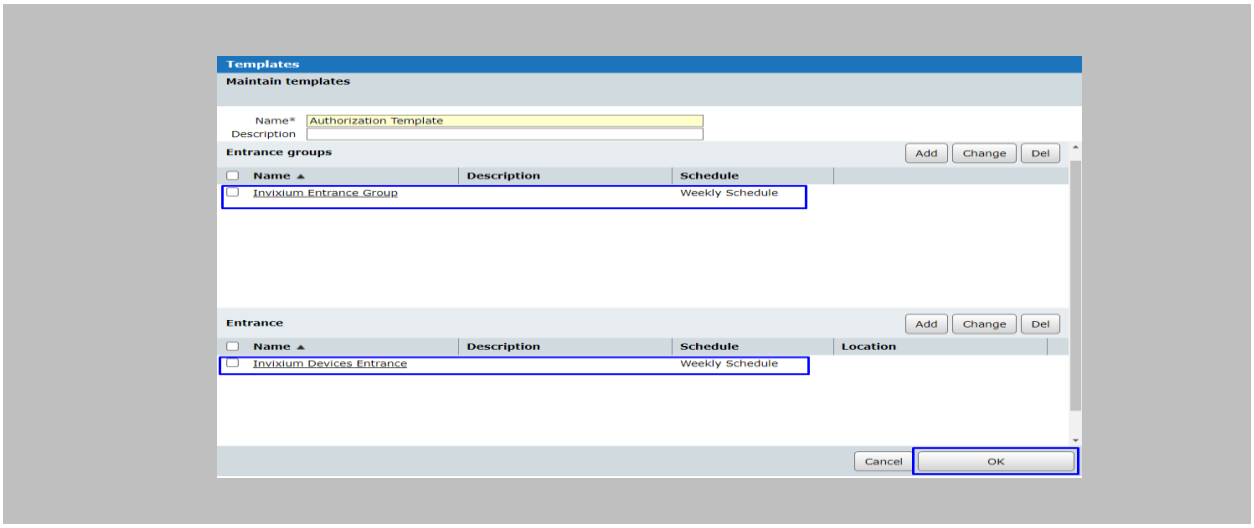


Figure 110: AEOS - Save Template

STEP 17

Assign the created **Template** to a new/existing person from the Authorization tab in order to grant access to the person.

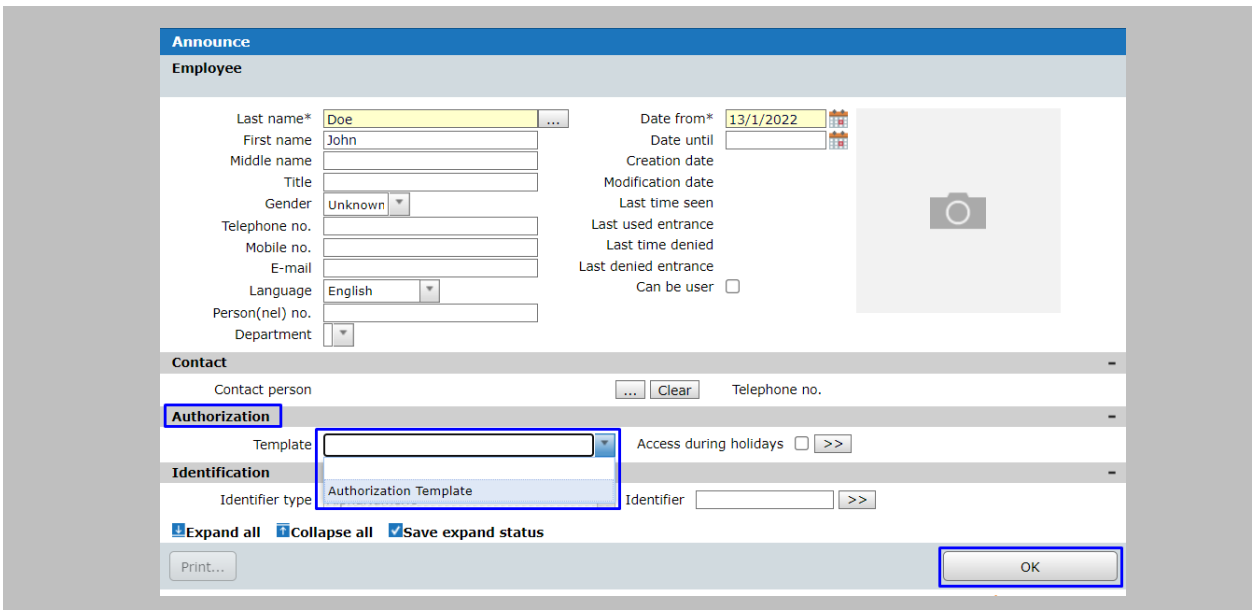


Figure 111: AEOS - Assign Template to Person

RESULT

All the **Employees/Visitors** with **Authorization Templates** will only get access in **Nedap AEOS**.

18. OSDP Configuration

The following configurations are required in IXM WEB and Nedap AEOS to use the OSDP feature.

Note:

1. The Nedap panel needs OSDP-supported firmware to use OSDP communication with the Invixium device. It can be found at the default location of AEOS i.e., C:\AEOS\AEmon\firmware
2. Wiegand Out should be in the Invixium device (Refer Assign Wiegand to Invixium Readers).
3. Standard Door should be created, and all the prerequisites should be configured to get access in the Nedap AEOS (Refer to Prerequisites for getting Access in AEOS).

Procedure

STEP 1

From **Home**, click the **Devices** tab. Select the required **Device** and navigate to **Access Control** → Click on **OSDP**.

By default, the OSDP configuration is turned **OFF**. Enable the OSDP by toggling the switch to **ON**.

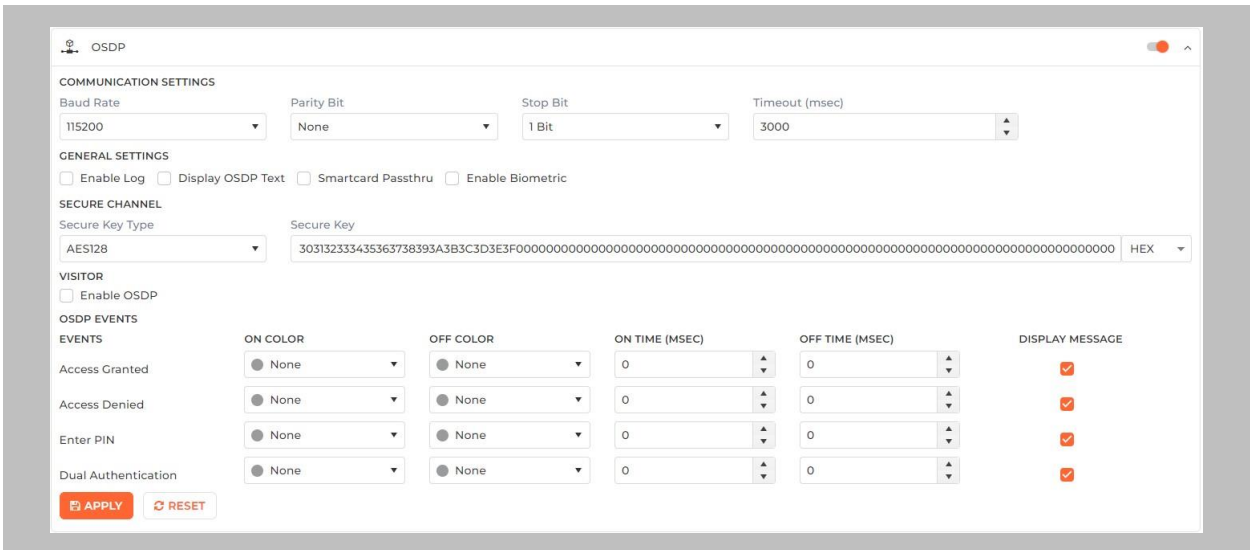


Figure 112: IXM WEB - OSDP Settings

STEP 2

Supply **values** for the configuration settings below:

Baud Rate	The baud rate of serial communication. The value must be the same as the Access Control Panel's value.
Parity Bit	The parity bit of the serial communication. The value must be the same as the Access ControlPanel's value.
Stop Bit	The stop bit of the serial communication. The value must be the same as the Access Control Panel's value.
Enable Log	This logs OSDP events for support and debugging purposes. Invixium recommends disabling this feature unless needed.
Smartcard Passthru	When presenting a smart card, the device passes the smart card CSN (Card Serial Number) to the Access Control Panel without taking any other action.
Enable Biometric	Enables biometric template verification.
Secure Channel	The secure key is provided by your Access Control Panel most of the time. However, provisions for manual entry can be added as TEXT or HEX.
Event	The OSDP static events for panel feedback and capture pin are: Access Granted Access Denied Enter Pin Dual Authentication – It is an access mode that requires valid access by two authorized cardholders to enter an access zone within a specified time period. This feature is available only if the **Multi-User Authentication** feature is enabled and configured. To configure the Multi-User Authentication feature, from **Home**, click the **Devices** tab. Select the required Device and navigate to **General Settings**. Click on the **Multi-User Authentication** section. Upon enabling this feature, the following actions

	will be performed: • The Device will request the credentials of the second user after the first user is authenticated successfully. • Card numbers for both the first and the second user will be transferred to the Access Control Panel. Two events, one for the first user and the other for the second user will be logged into the Access Control Panel.
On Color/Off Color	The LED color configuration based on panel events. The value must be the same as the Access Control Panel's value. Options are: • Red • Green • Yellow • Blue
Enable VISITOR OSDP	The option sends card details to ACP even if then card is not assigned to any employee on device. Based on response from ACP; device will display "Access Granted" or "Access Denied"

Table 6: IXM WEB - OSDP Configuration Options

Note: Mismatches between the unit and Access Control Panel LED configuration will cause unrecognized events.

Display OSDP Text	Enables to display OSDP Text.
Display Message	Notification on the device's screen. If enabled: Displays both the unit hard-coded notification and the Access Control Panel notification. IXM notification - Access Granted or Access Denied. Access Control Panel notification – Valid or Invalid. If disable: Displays only the Access Control Panel notification.

Table 7: IXM WEB - OSDP Text Options

STEP 3

Click **Apply** to save the settings.

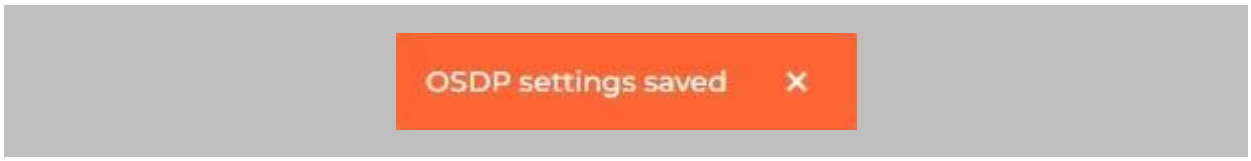


Figure 113: IXM WEB - Save OSDP Setting

STEP 4

Open the edit option on the reader and note the **Device ID**. This will be the address used in the configuration of the reader in Nedap AEOS.

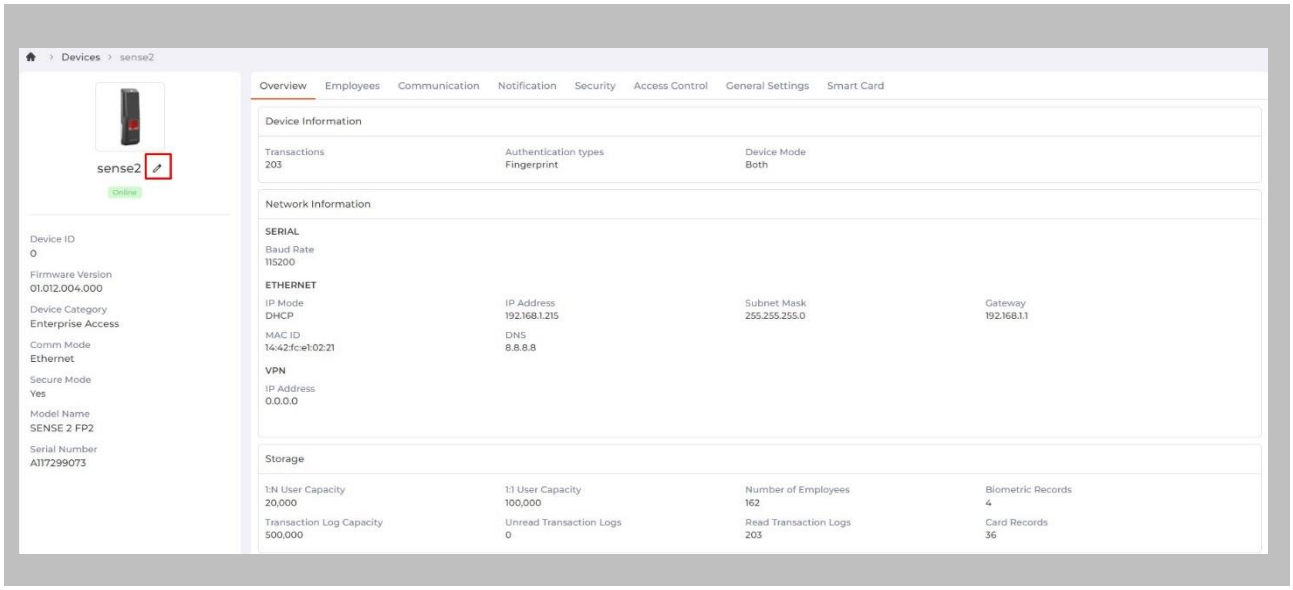


Figure 114: IXM WEB - Edit Device

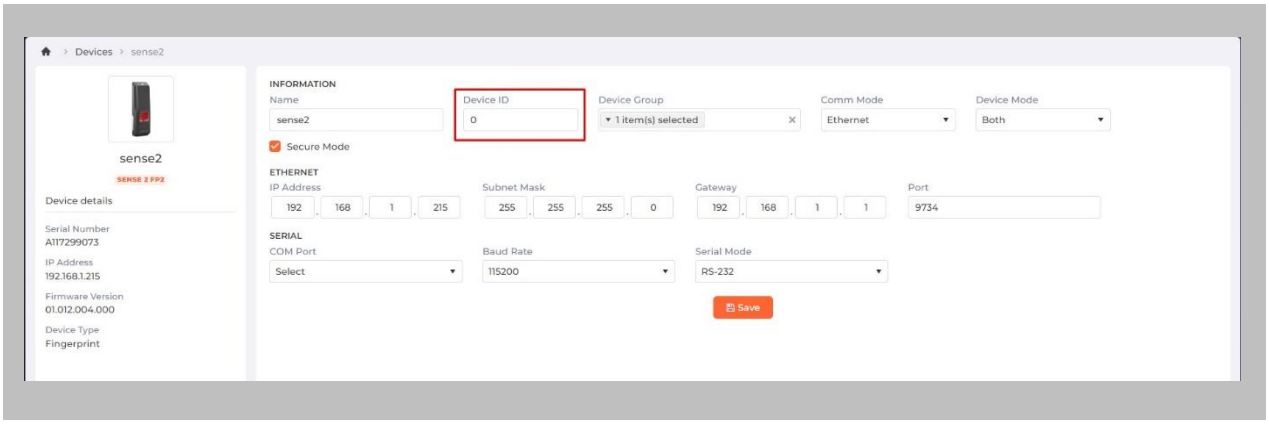


Figure 115: IXM WEB - Edit Device Options

Note: Invixium's reader address should be the same as the OSDP reader address.

STEP 5

Wiegand input and output also need to be **configured** to allow OSDP communication to work. Create the same settings for Wiegand connections as you did previously.

STEP 6

Disable Panel feedback for any OSDP-connected reader to stop multiple access granted messages from being sent to Nedap AEOS.

STEP 7

Once OSDP settings are applied to the Invixium device, the device will be added to 'AEmon' as new hardware.

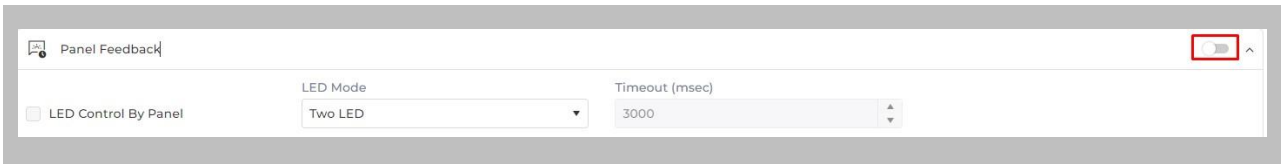


Figure 116: IXM WEB - Disable Panel Feedback

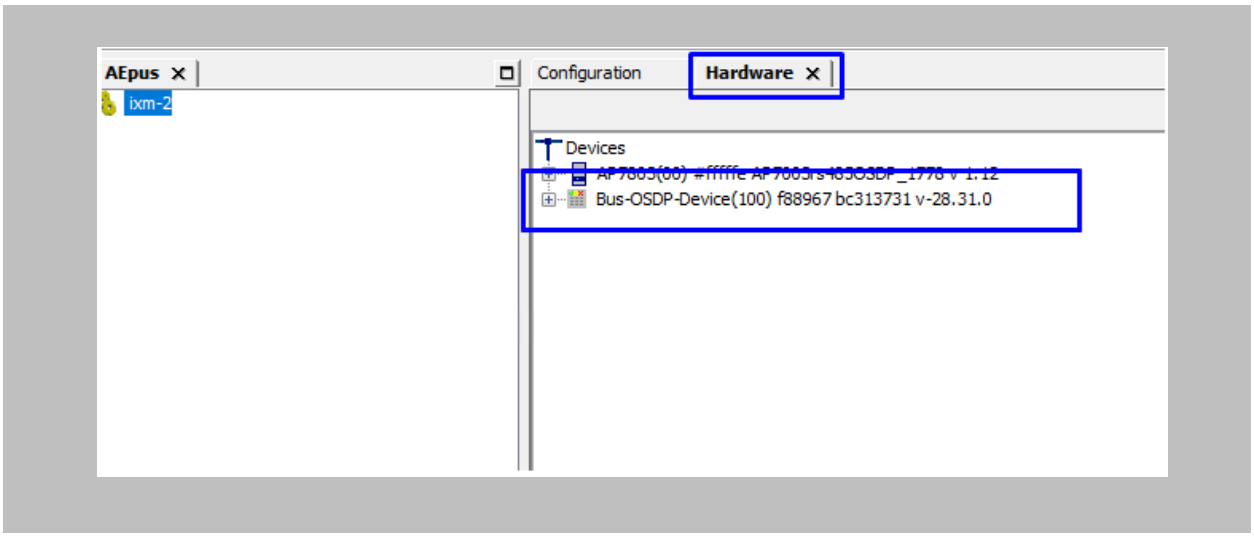


Figure 117: AEmon - OSDP Device

STEP 8

Click on **Configuration** → Define behavior of the OSDP device as shown in the image below.

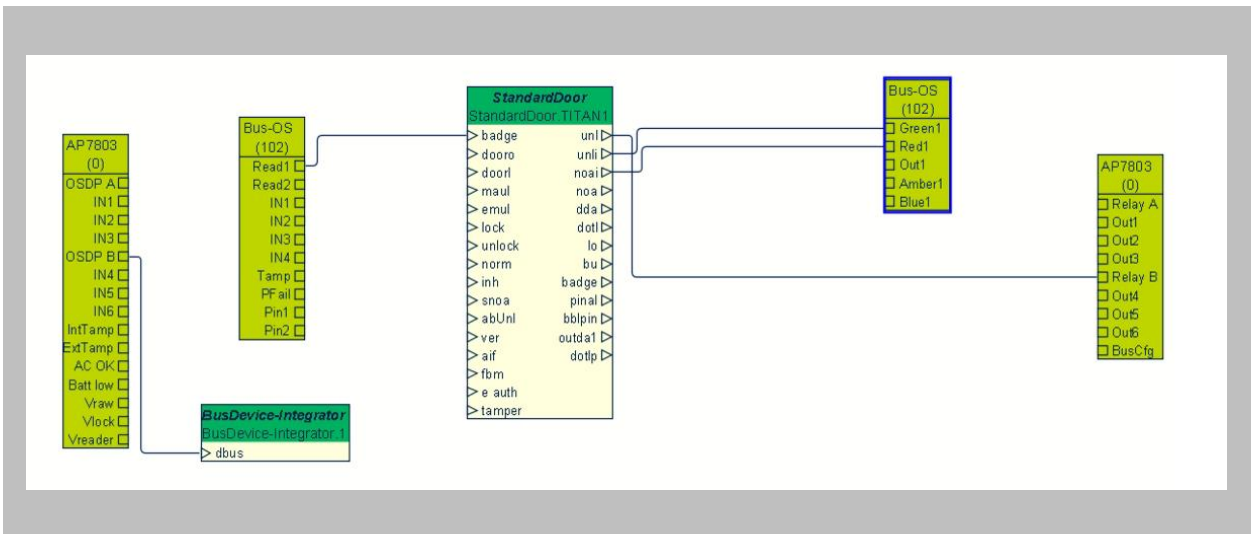


Figure 118:AEmon - OSDP Device Behavior

STEP 9

Right click on Standard Door → Properties.

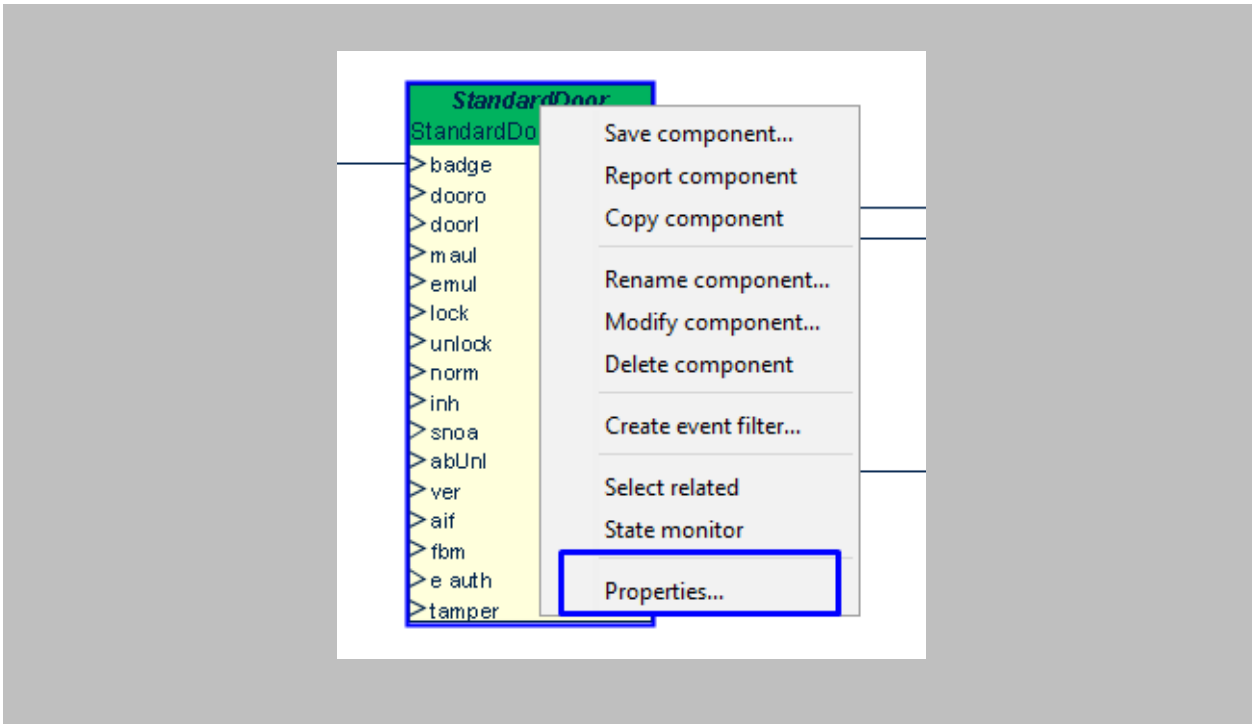


Figure 119: AEmon - Standard Door Property

STEP 10

Click on the ellipsis button of **Primary Identifier Type.**

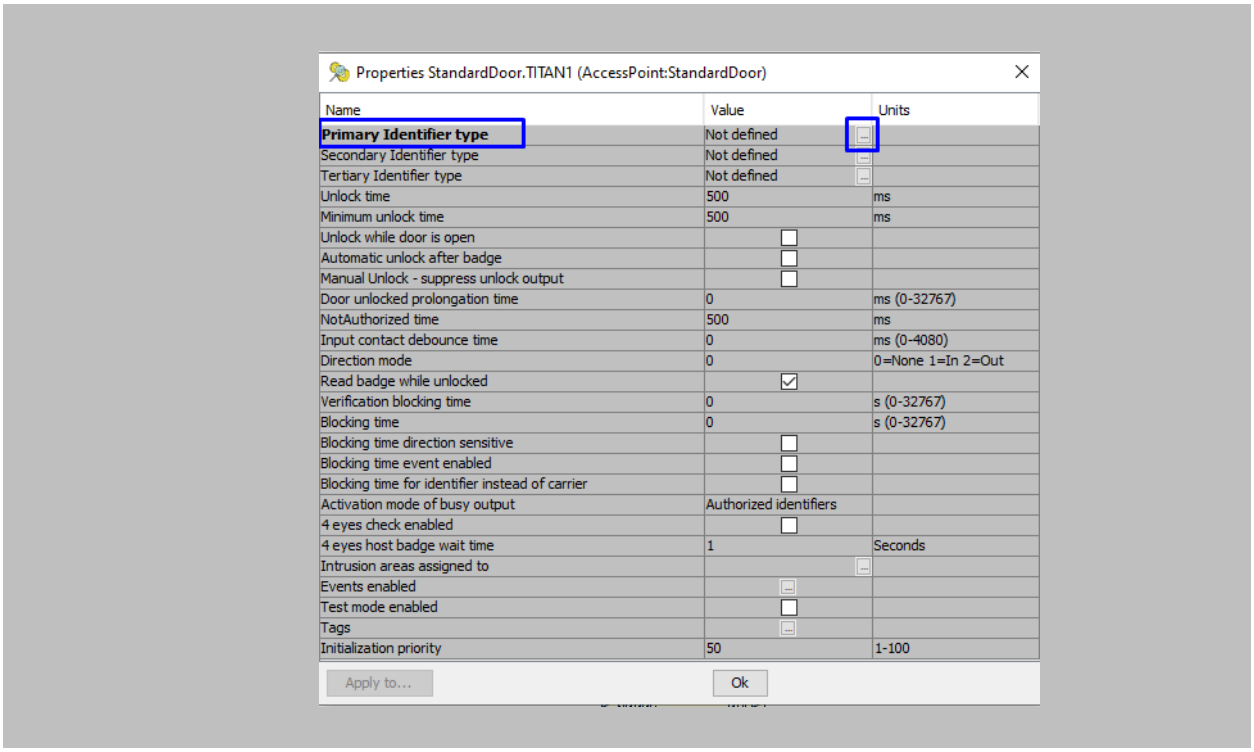


Figure 120: AEmon - Primary Identifier Type

Configure **identifier type** as shown in the image below and click on **OK.**

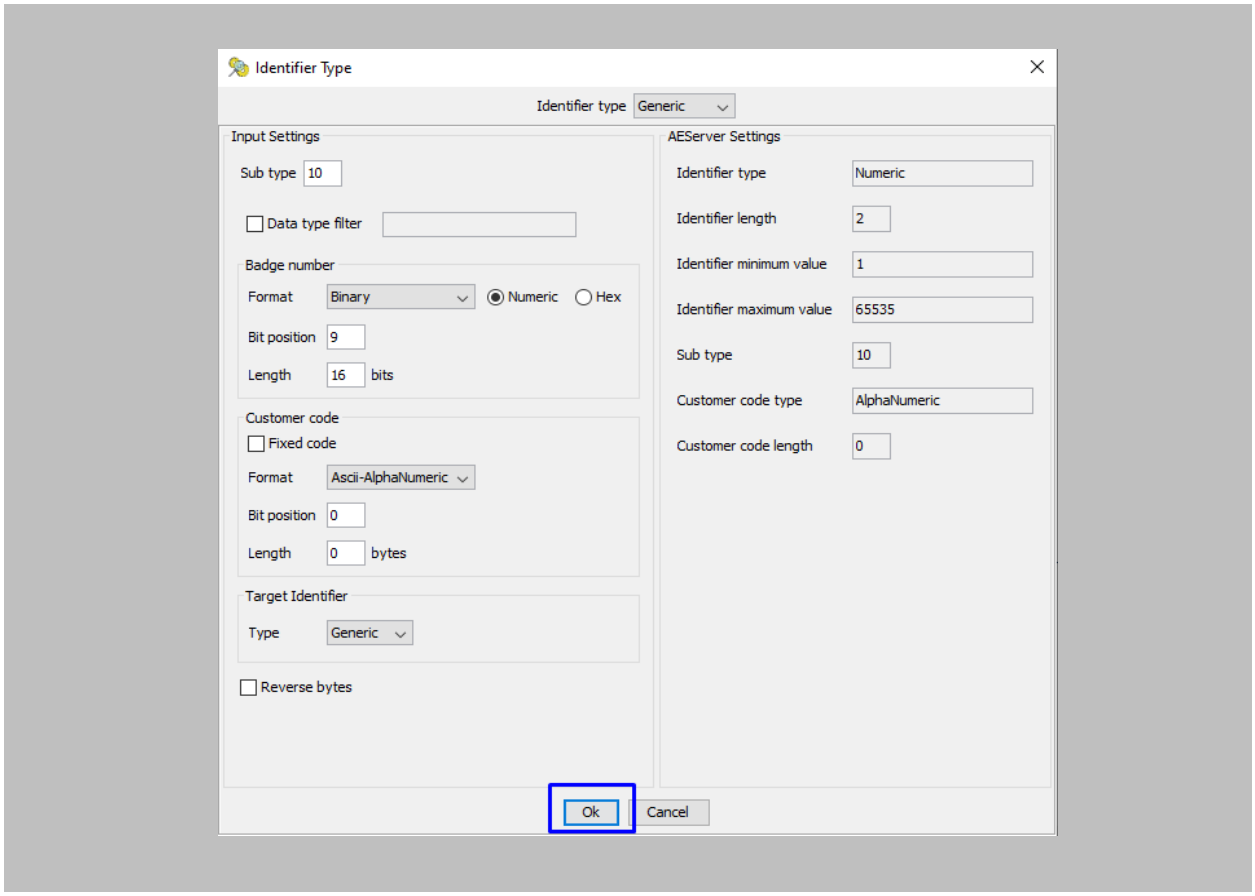


Figure 121: AEmon - Configure Primary Identifier Type

STEP 11

Configured Identifier Type will be displayed as **Primary Identifier Type** → click on **OK.**

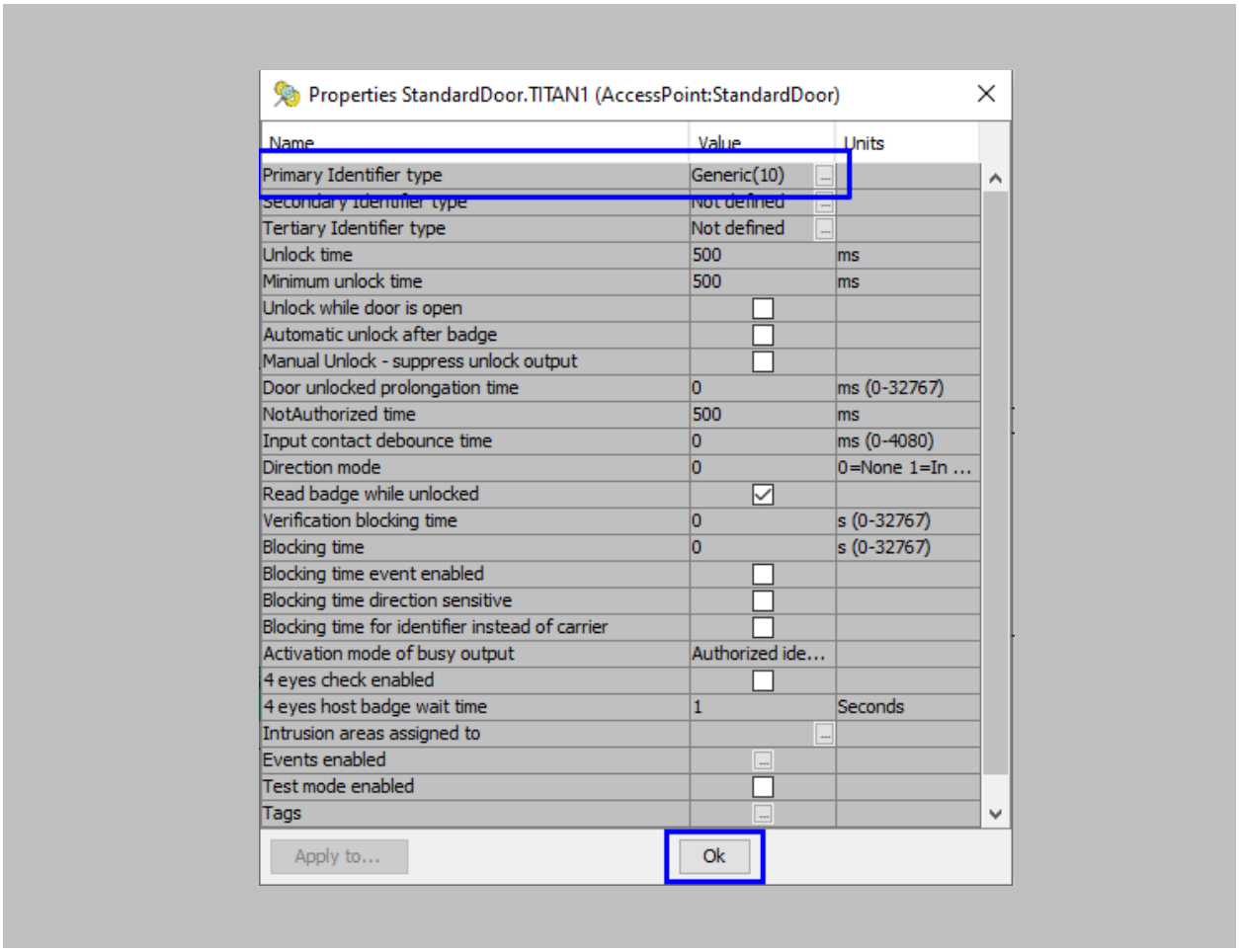


Figure 122: AEmon - Generic Primary Identifier Type

STEP 12

To deploy changes on the panel, right click anywhere on the **'Configuration'** window → click on **Deploy Configuration.**

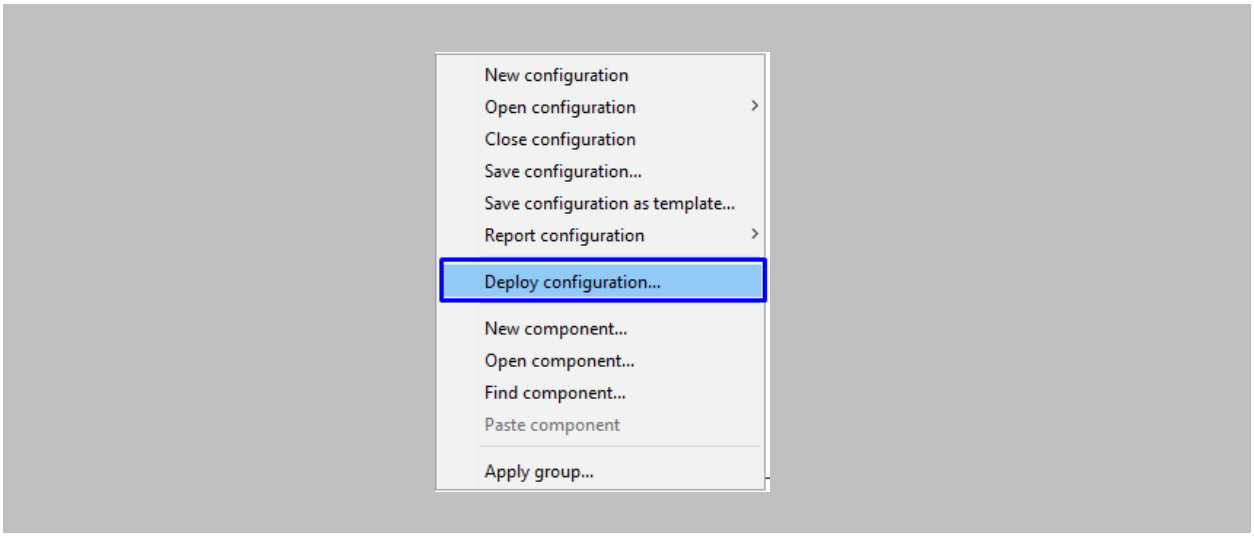


Figure 123: AEmon - Deploy Configuration

19. DIP Configuration

The following configurations are required in IXM WEB and Nedap AEOS to use the DIP feature.

Note:

1. Wiegand Out should be in the Invixium device (Refer Assign Wiegand to Invixium Readers).
2. Standard Door should be created, and all the prerequisites should be configured to get access in Nedap AEOS (Refer to Prerequisites for getting Access in AEOS).

Procedure

STEP 1

Open **AEmon**, select the **AEpu** that is connected to the Invixium device → go to the **Configuration tab**.

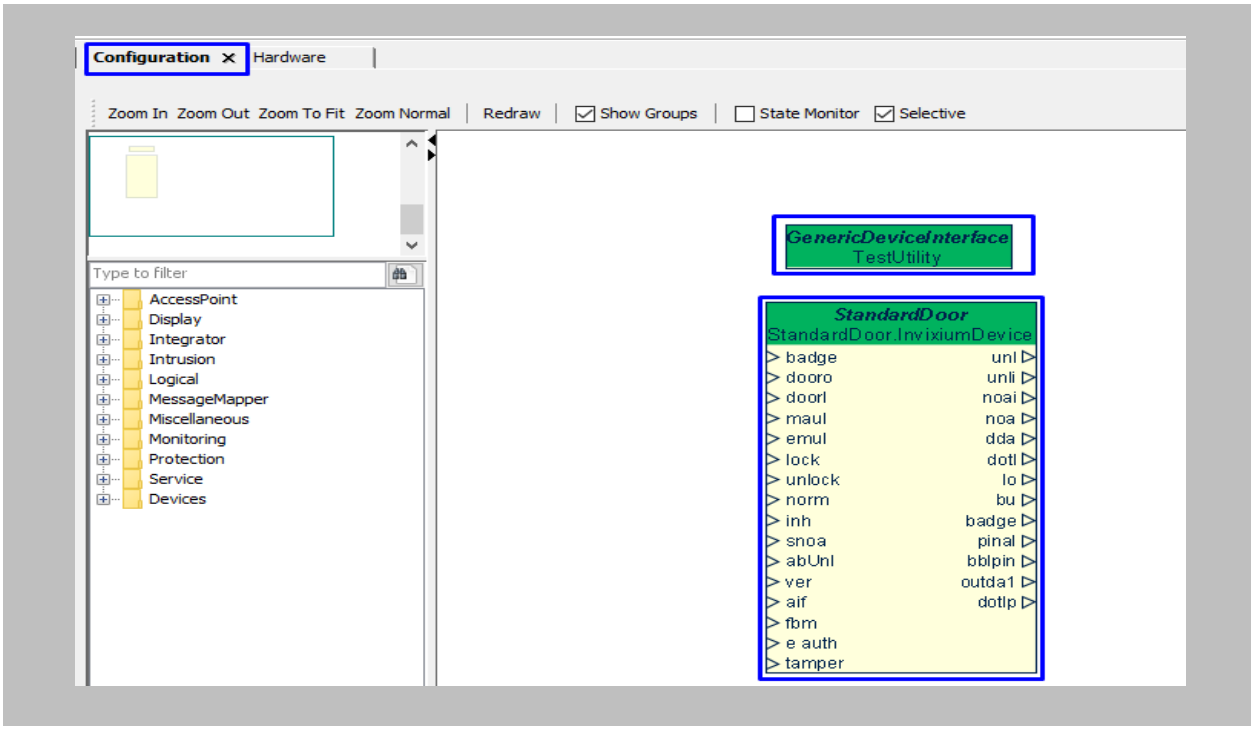


Figure 124: AEmon - Configuration tab

STEP 2

Search for ACLabelConverter → Add ACLabelConverter.

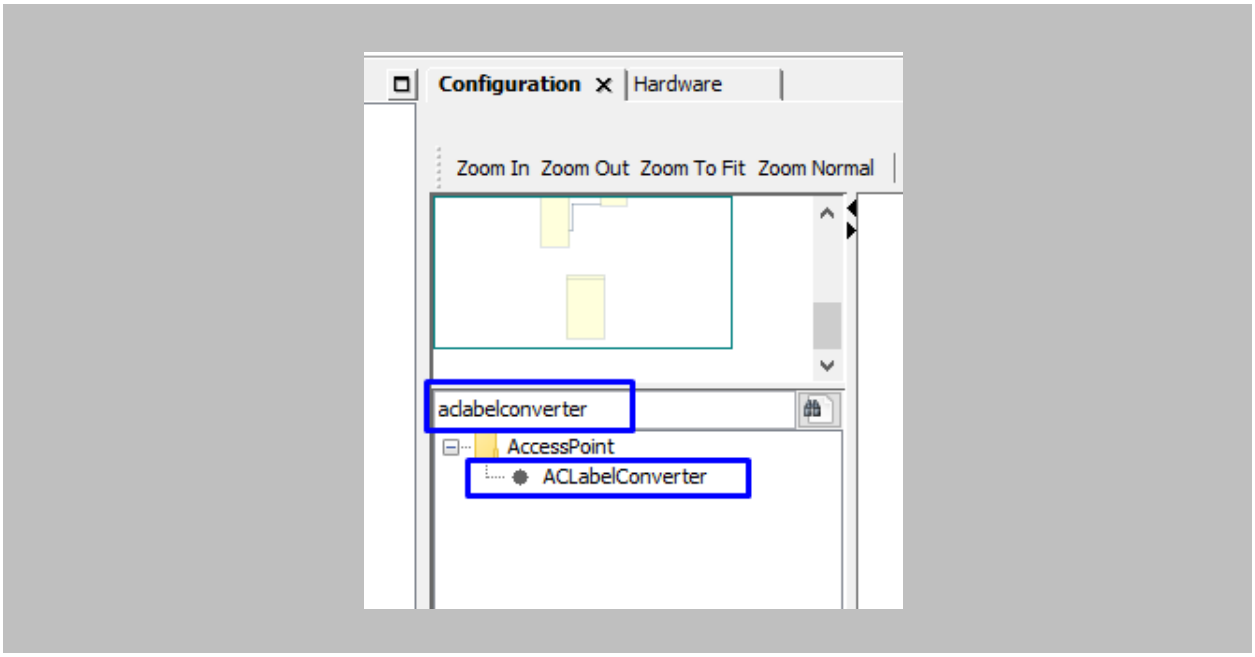


Figure 125: AEmon - Add ACLabelConverter

STEP 3

Connect ‘Output Data1’ of StandardDoor with ‘Access Point Status’ of ACLabelConverter.

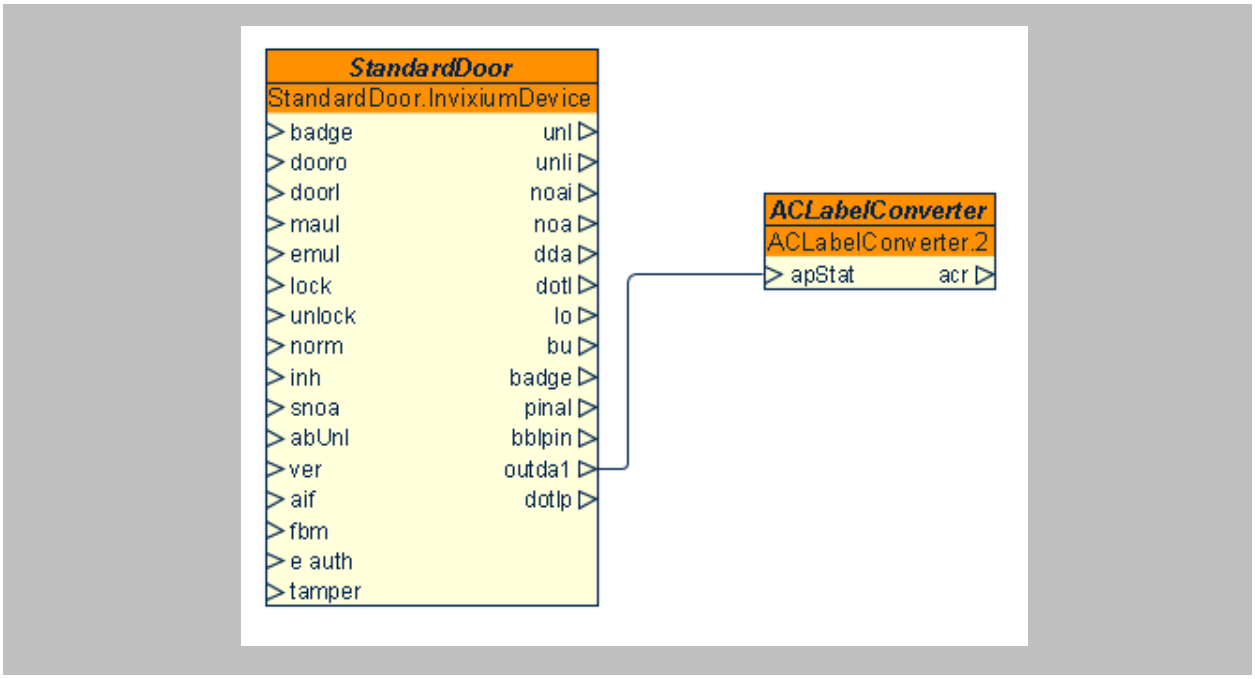


Figure 126: AEmon - StandardDoor and ACLabelConverter Connection

STEP 4

Right click on GenericDeviceInterface → click on Properties.

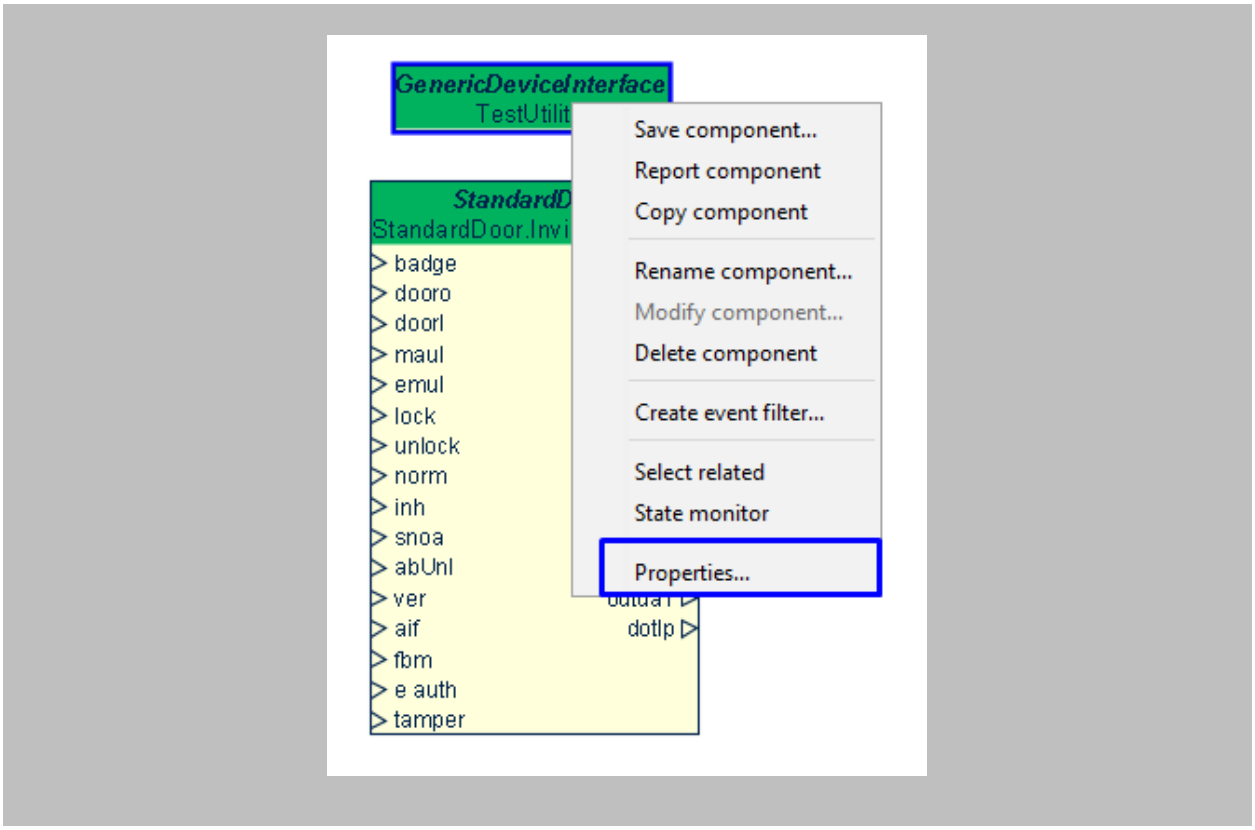


Figure 127: AEmon - GenericDeviceInterface Properties

STEP 5

Click on the ellipsis button of **Device Channel Address.**

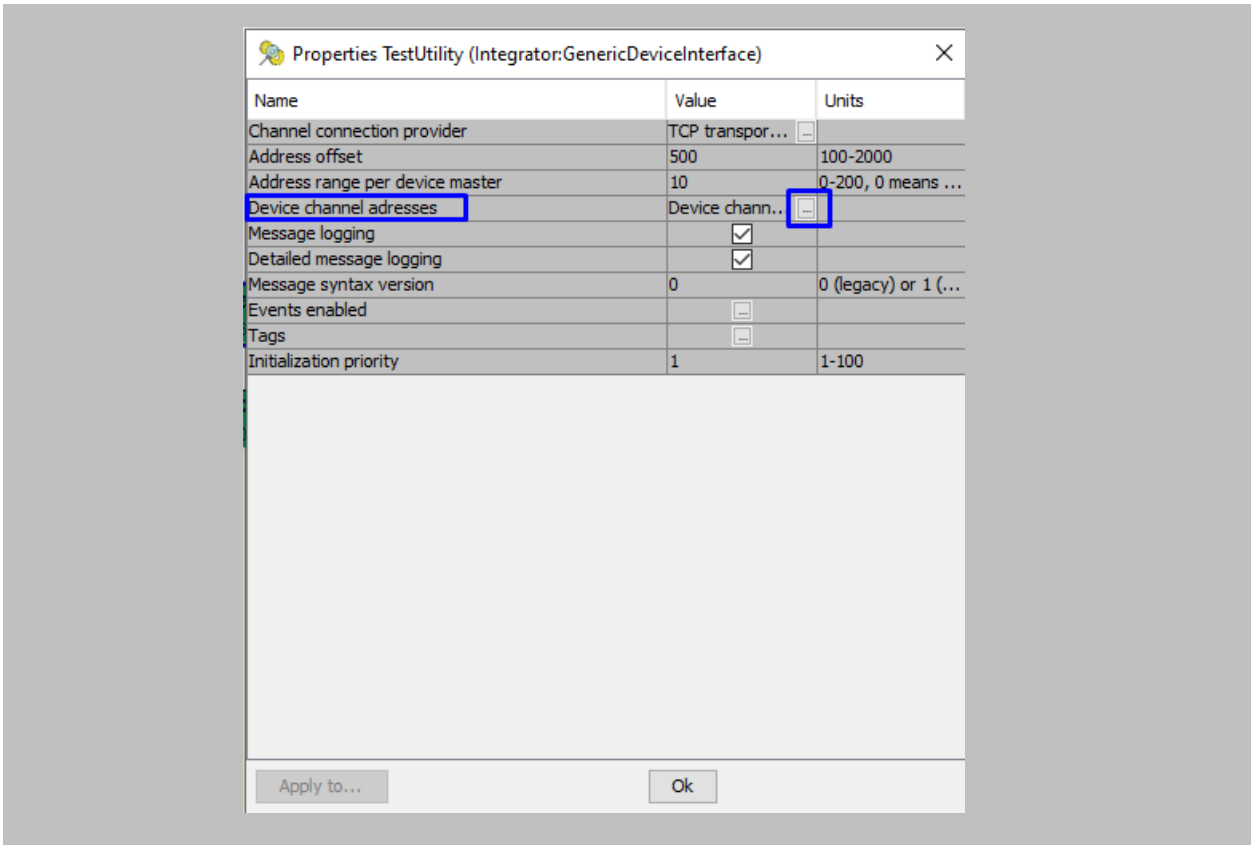


Figure 128: AEmon - Device Channel Address

STEP 6

Click on the **Add** button → Define 8 digits of the **Channel address** → click on the **OK** button.

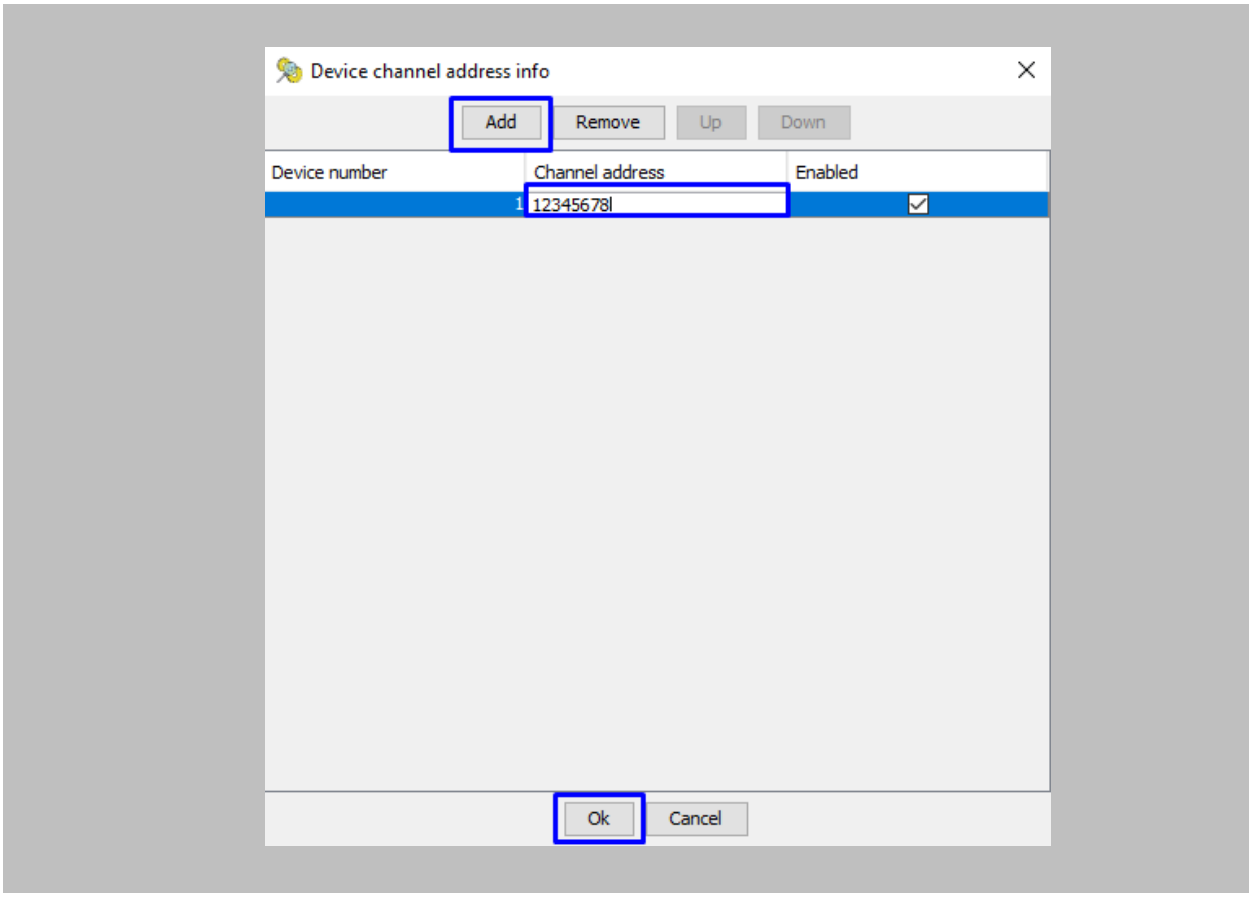


Figure 129: AEmon - Add Channel Address

STEP 7

Deploy changes on the panel. To deploy, right click anywhere on the **'Configuration'** window → click on **Deploy Configuration.**

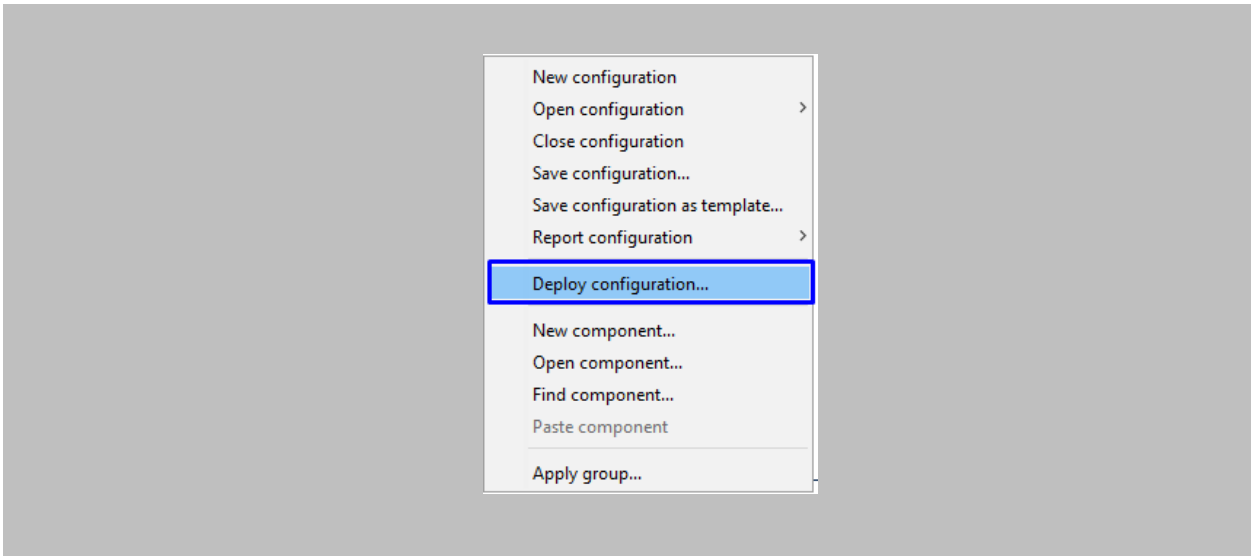


Figure 130: AEmon - Deploy Configuration

STEP 8

Open **IXM WEB**, from the **Left Navigation Pane** go to **Link** → click on the **AEOS (Nedap)** icon → click on the **Add DIP Settings** button.

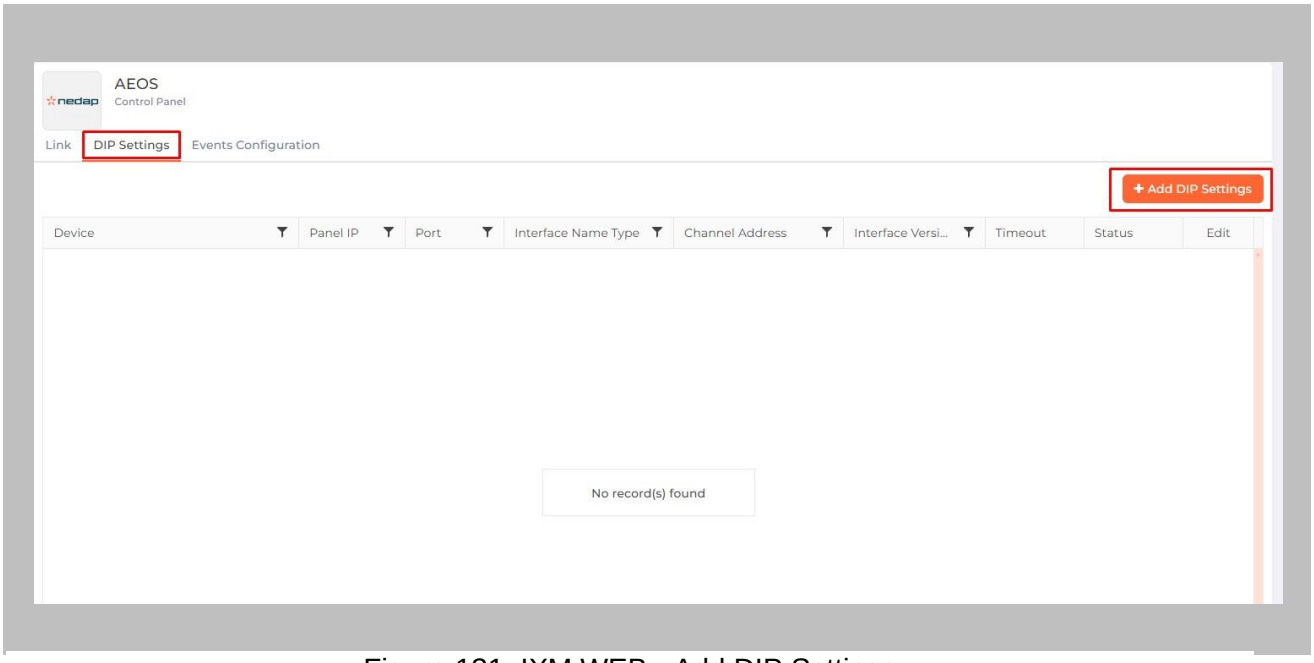


Figure 131: IXM WEB - Add DIP Settings

STEP 9

Enter the below details:

- **Status**: Select **'Status'** to enable DIP settings on the device.
- **Debug:** This logs DIP events for **support** and **debugging** purposes. Invixium recommends disabling this feature unless needed.
- **Device:** Select the Invixium device on which you want to enable **DIP settings**.
- **Port:** Enter the communication **port** number which is used for communication between the Invixium device and the Nedap panel. Default value: 8001
- **IP:** Enter the **IP address** of the panel.
- **Channel Address:** Enter the **Channel address** specified in AEmon (Refer Add Channel Address in AEMon).
- **Timeout:** Provide a **timeout** value (in seconds) for getting a response from the Nedap panel. Default value: 10 seconds.

Click on the **Save** button.

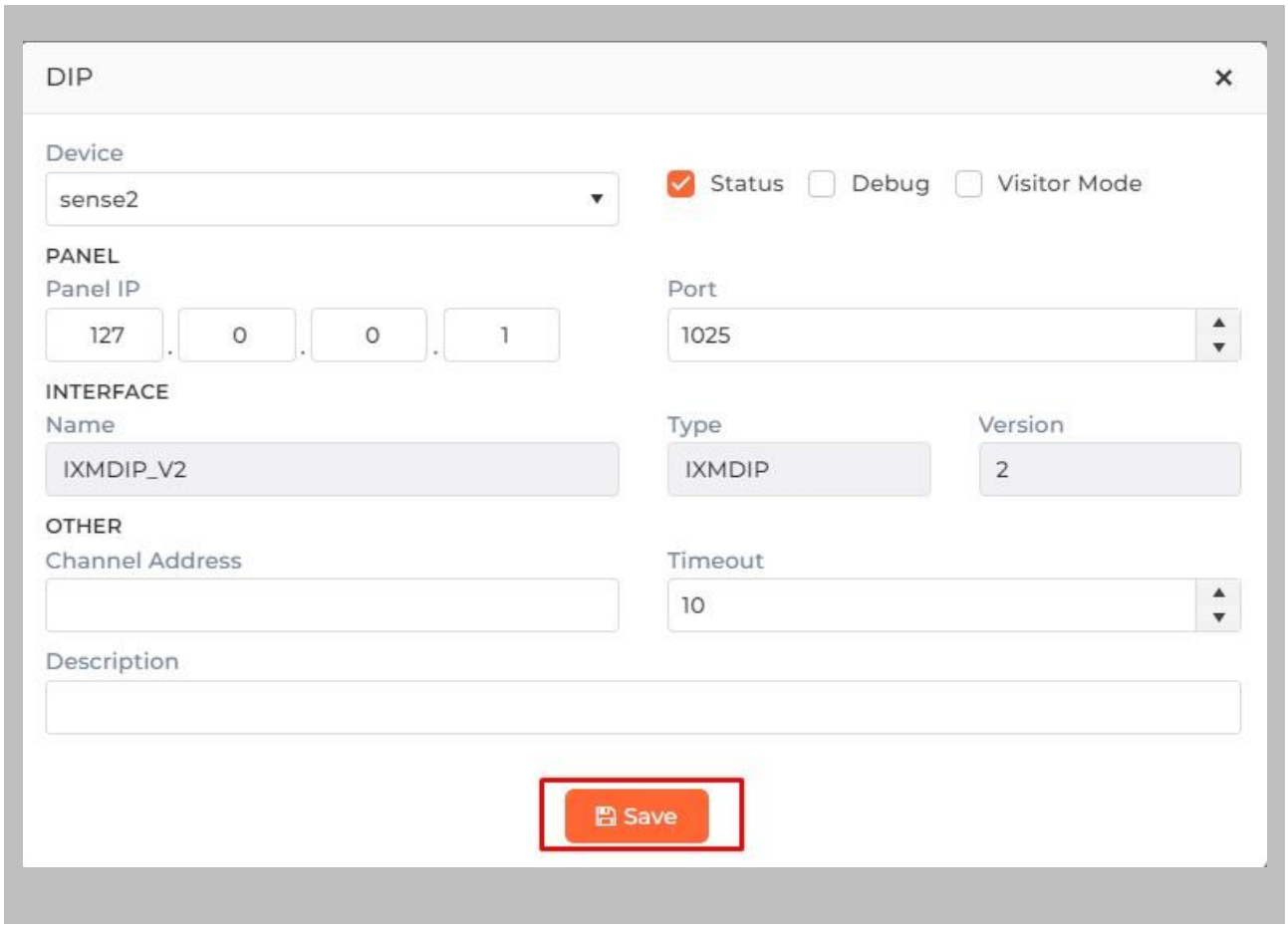


Figure 132: IXM WEB - Save DIP Settings

STEP 10

Once DIP settings are applied on the Invixium device, the device will be added in ‘AEmon’ as new hardware.

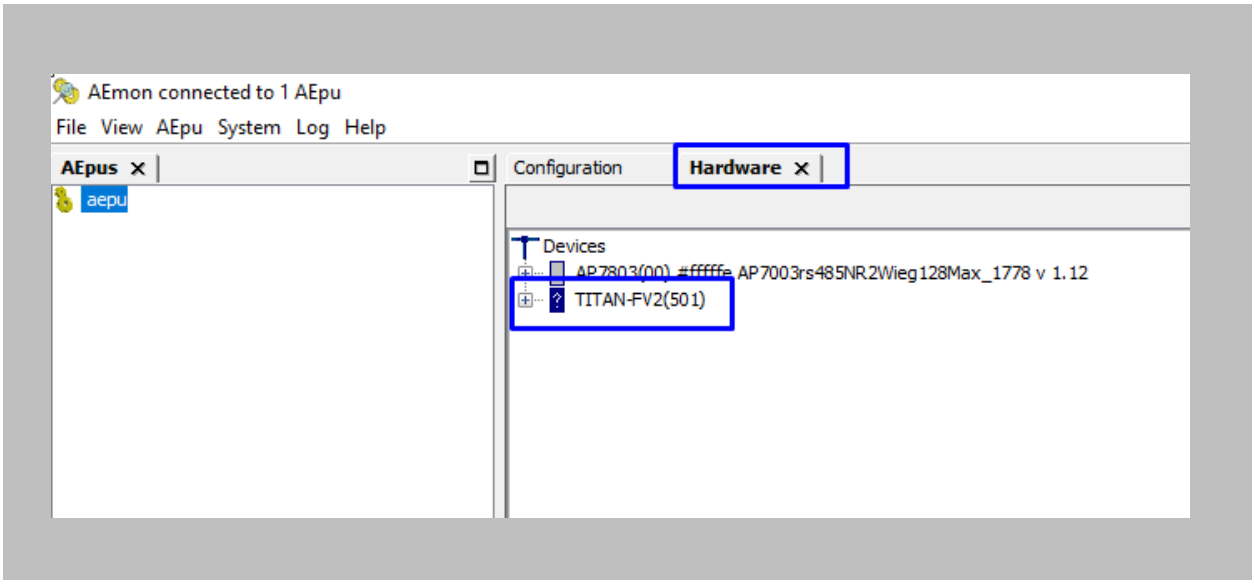


Figure 133: AEmon - DIP Device

STEP 11

Go to the **Configuration** taband define the behavior device and panel as shown in the below image.

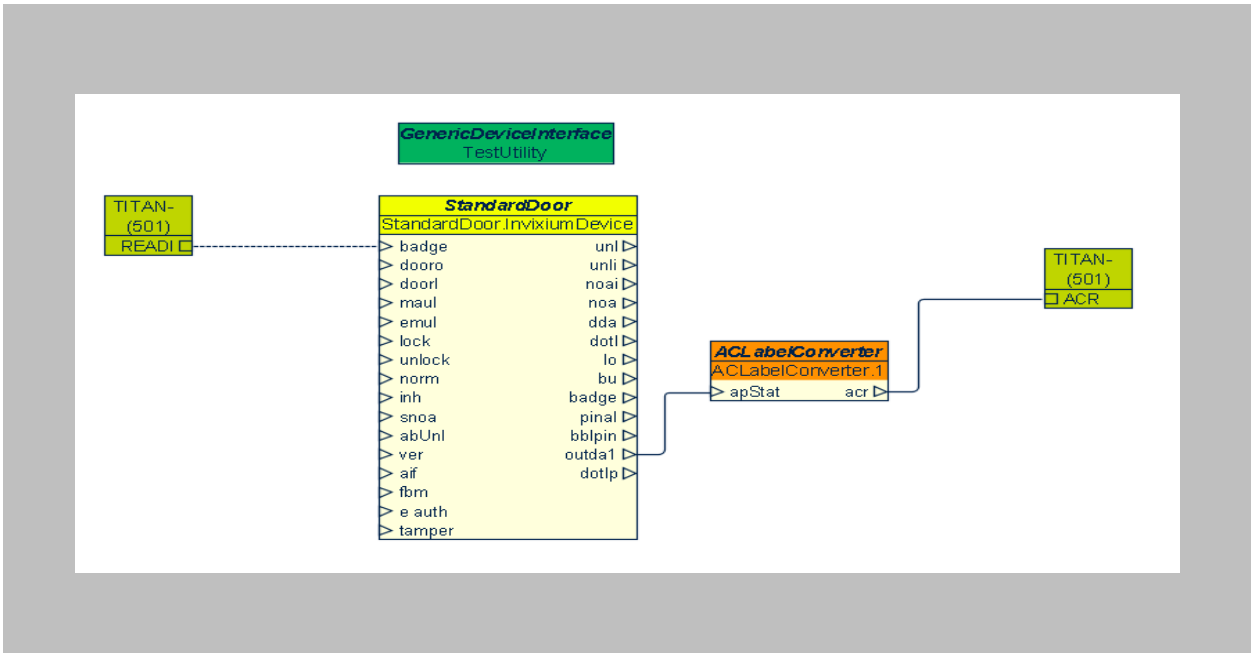


Figure 134: AEmon - DIP Device Behavior

STEP 12

Right click on Standard Door → Properties.

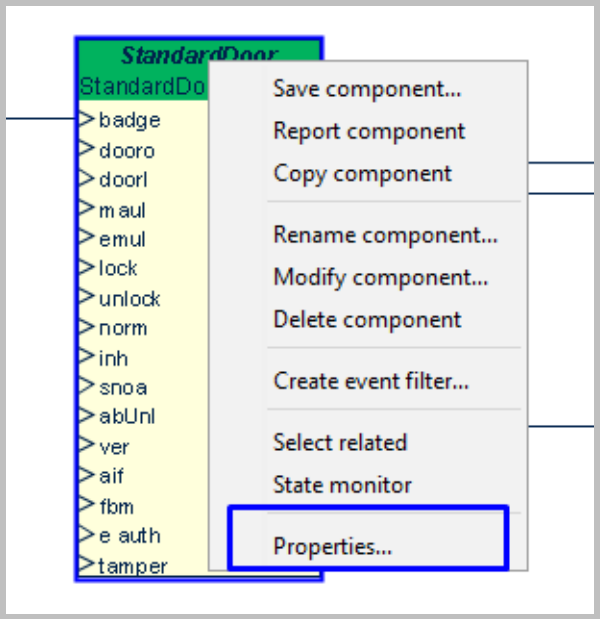


Figure 135: AEmon - Standard Door Property

STEP 13

Click on the ellipsis button of **Primary Identifier Type.**

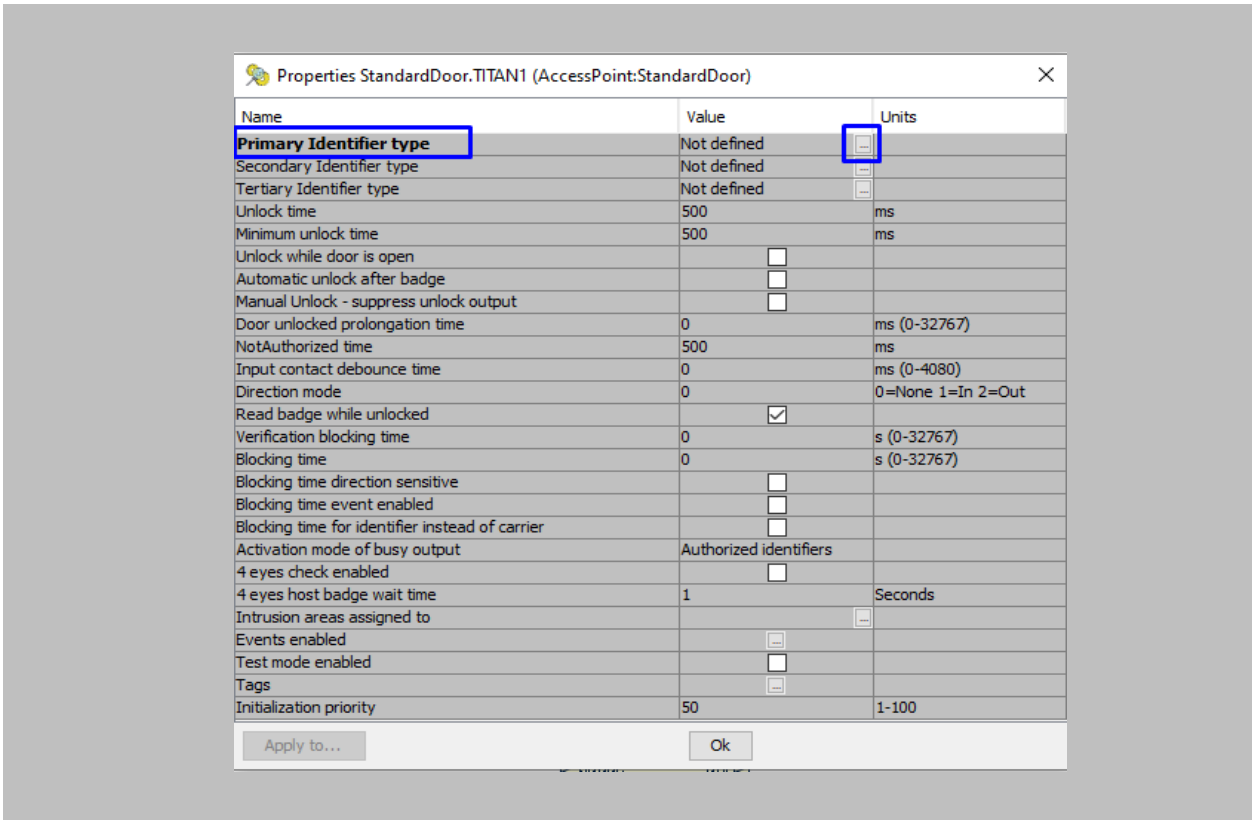


Figure 136: AEmon DIP - Primary Identifier Type

Configure **identifier type** as shown in the below image and click on **OK.**

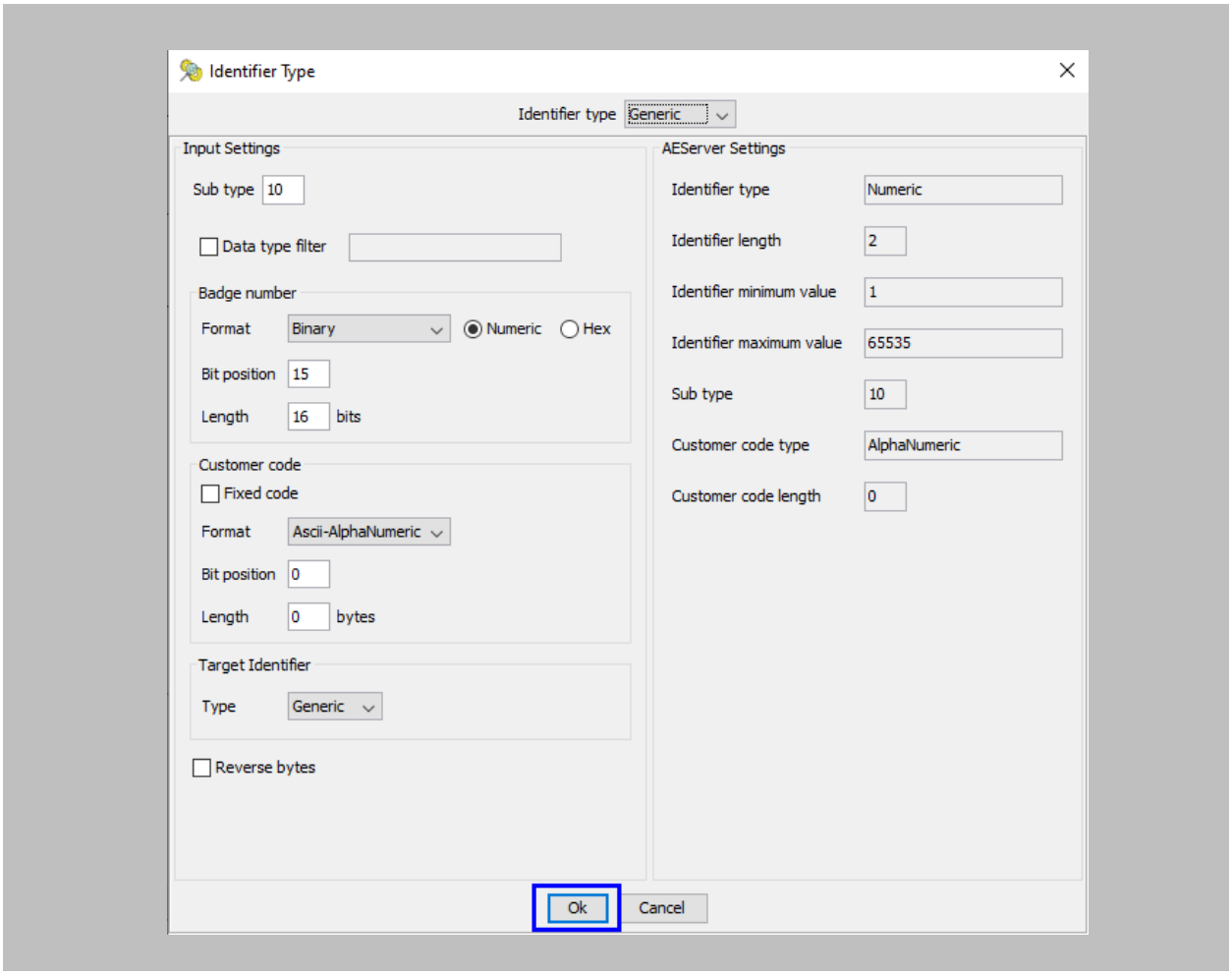


Figure 137: AEmon DIP - Primary Identifier Configuration

STEP 14

Configured Identifier Type will be displayed as **Primary Identifier Type** → click on **OK.**

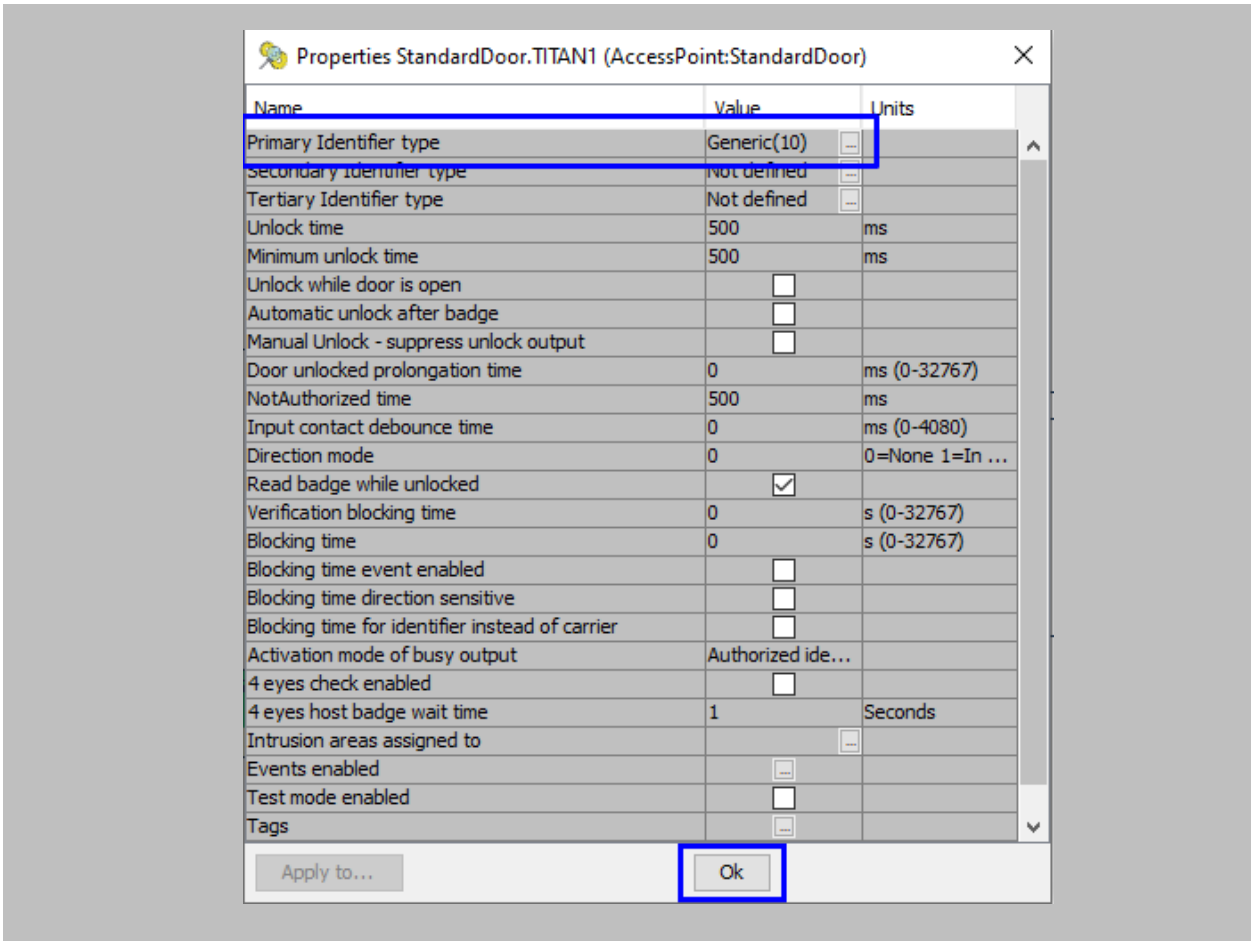


Figure 138: AEmon DIP - Generic Primary Identifier Type

STEP 15

In order to deploy changes on the panel, right click anywhere on the **'Configuration'** window → click on **Deploy Configuration.**

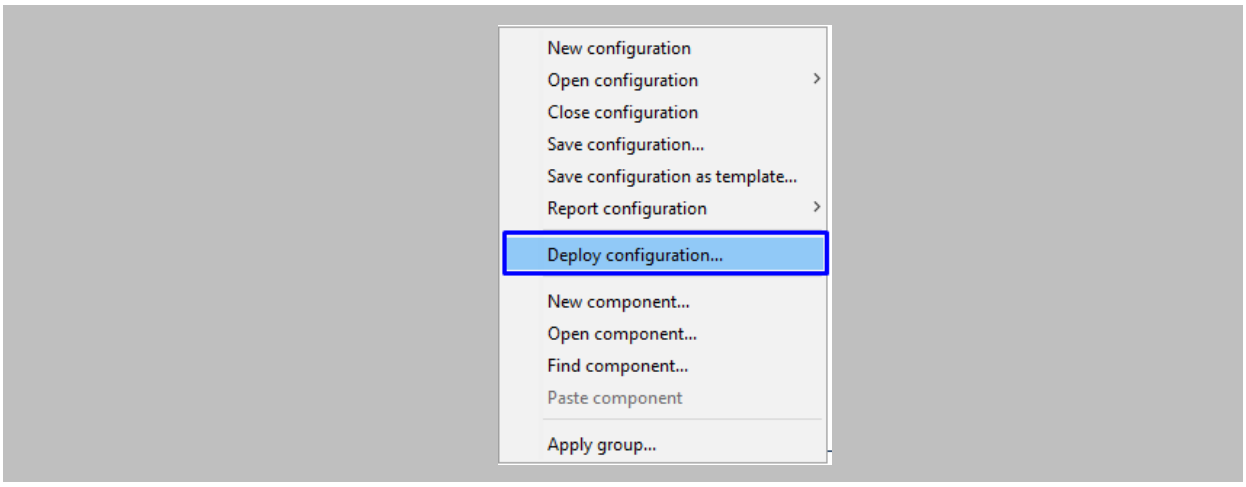


Figure 139: AEmon - Deploy Configuration

20. Wiegand Configuration

The following configurations are required in IXM WEB and Nedap AEOS to use the Wiegand feature.

Note:

1. Nedap panel's firmware must be compatible with Wiegand to use the Wiegand feature with the Invixium device. It can be found at the default location of AEOS i.e., C:\AEOS\AEmon\firmware
2. Wiegand Out should be in the Invixium device (Refer Assign Wiegand to Invixium Readers).
3. Standard Door should be created, and all the prerequisites should be configured to get access in Nedap AEOS (Refer to Prerequisites for getting Access in AEOS).

Procedure

STEP 1

Connect Wiegand Data D0 of the Nedap Panel with **WDATA_OUT0** of the IXM device, Wiegand Data D1 of the Nedap Panel with **WDATA_OUT1** and Wiegand Ground of the Nedap Panel with WGND of the IXM Device.

STEP 2

Open **AEmon**, select the **AEpu** that is connected to the Invixium device → go to the **Configuration tab** →Define the behavior of the device as shown in the image below.

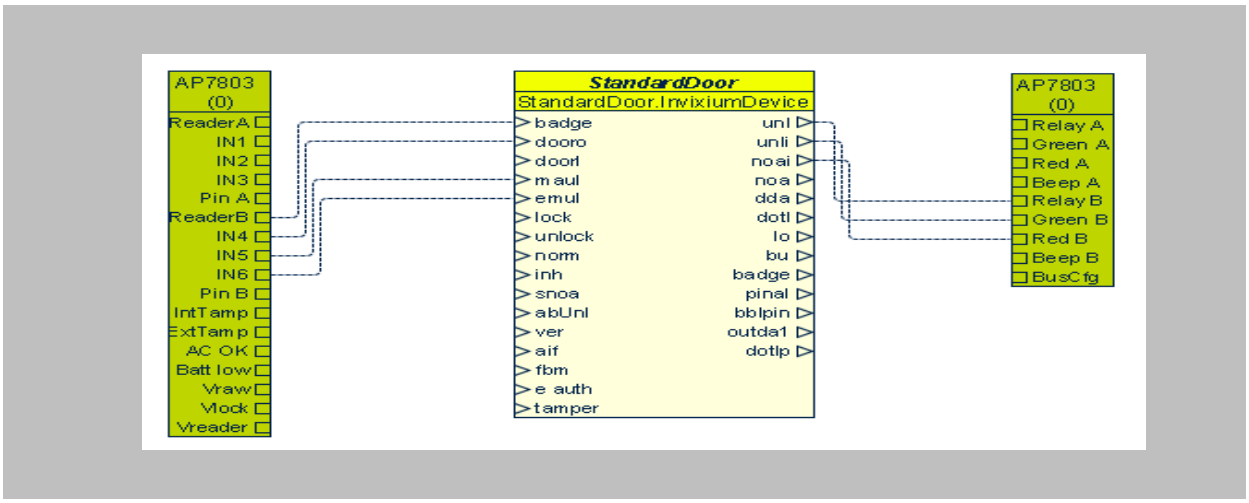


Figure 140: AEmon - Wiegand Device Behavior

STEP 3

Right Click on Standard Door → Properties.

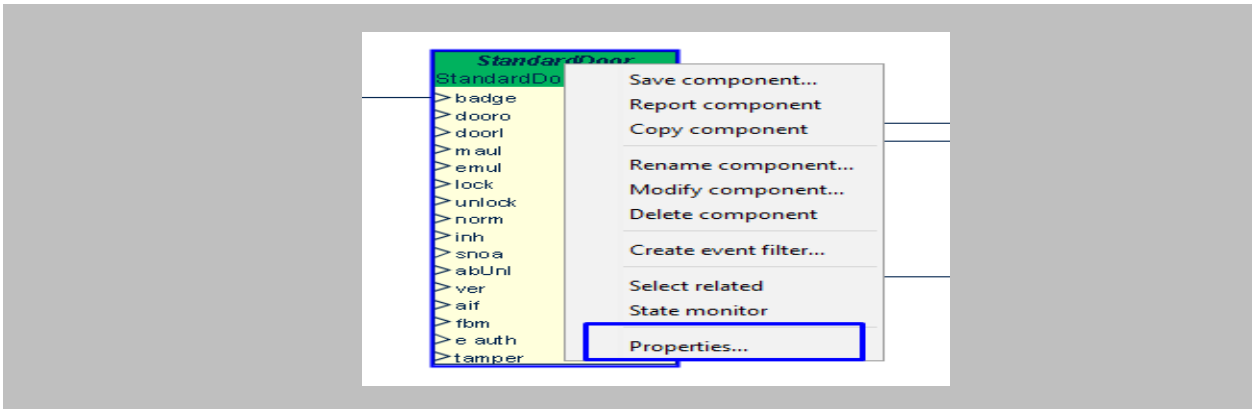


Figure 141: AEmon - Standard Door Property

STEP 4

Click on the ellipsis button of **Primary Identifier Type.**

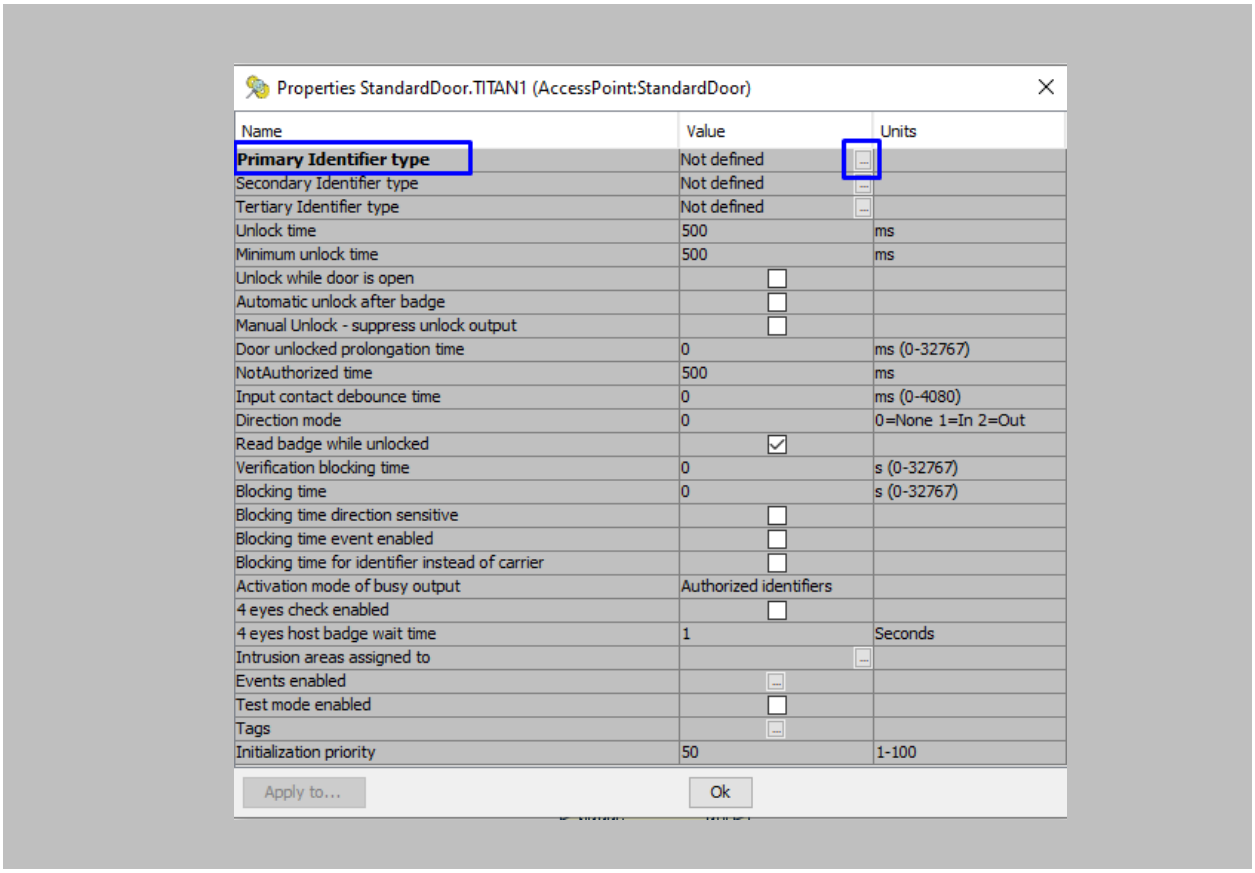


Figure 142: AEmon Wiegand – Primary Identifier Type

Configure **identifier type** as shown in the image below and click on **OK.**

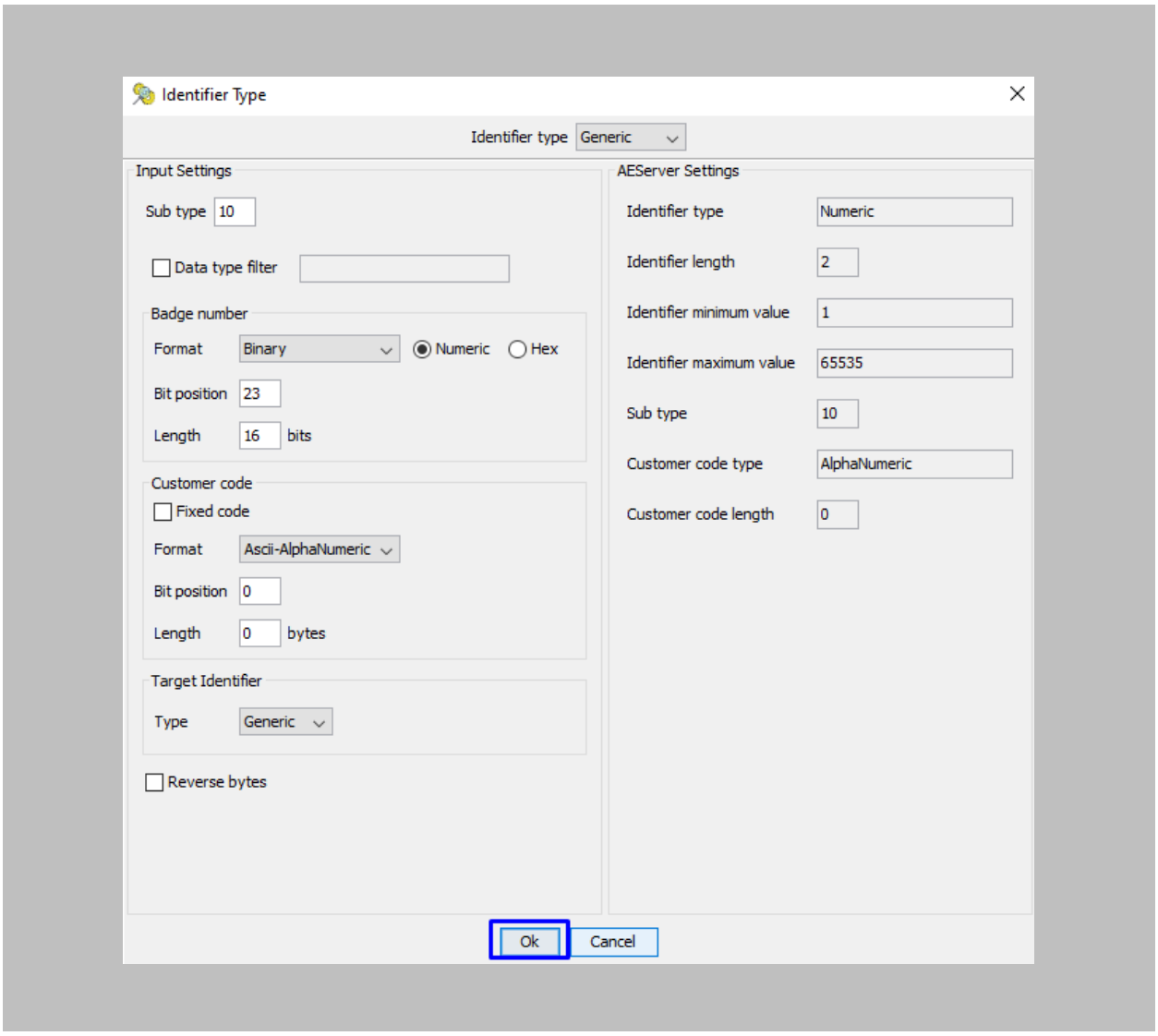


Figure 143: AEmon Wiegand - Configure Primary Identifier Type

STEP 5

Configured Identifier Type will be displayed as **Primary Identifier Type** → click on **OK.**

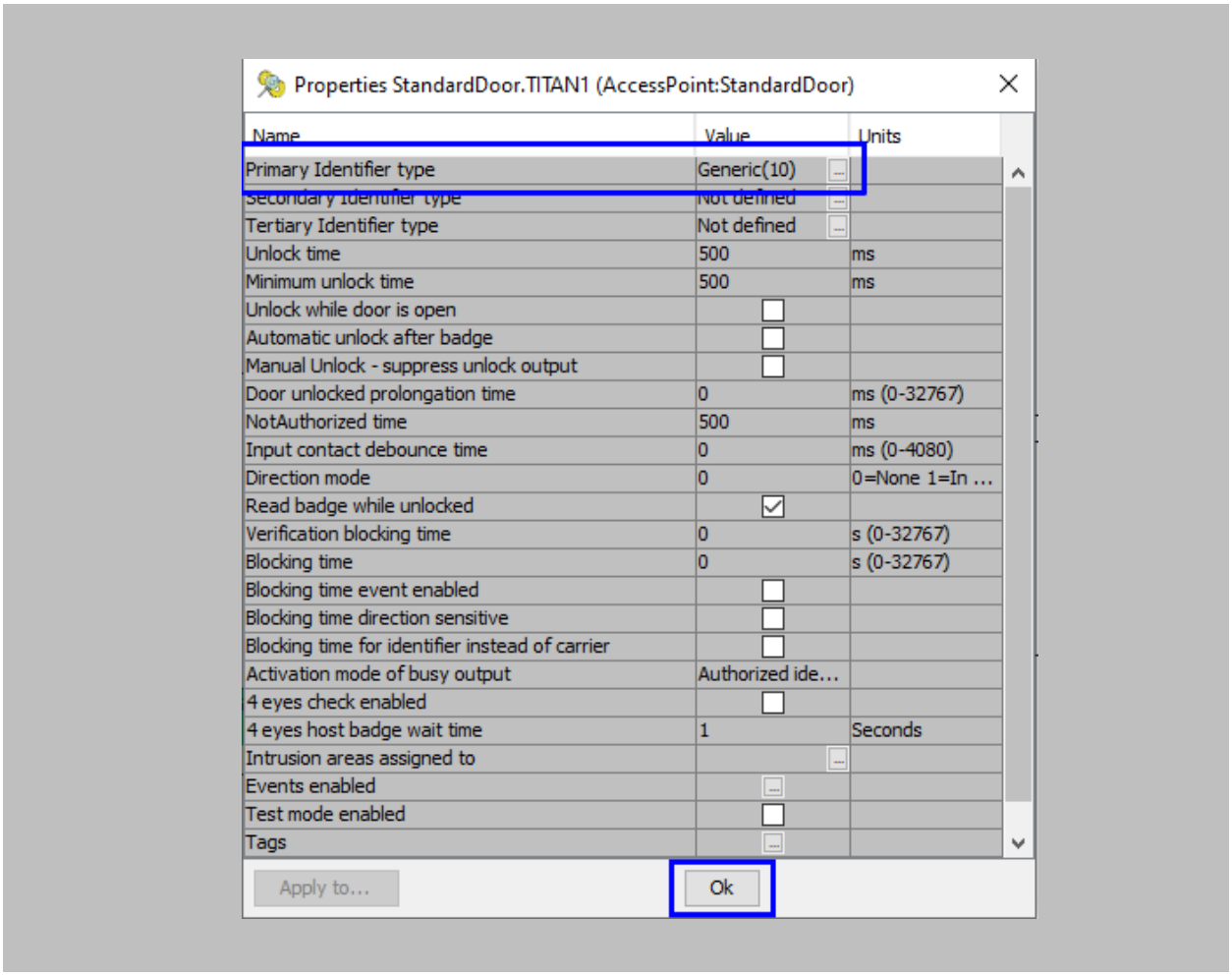


Figure 144: AEmon Wiegand- Generic Primary Identifier Type

STEP 6

In order to deploy changes on the panel, right click anywhere on the **'Configuration'** window → click on **Deploy Configuration.**

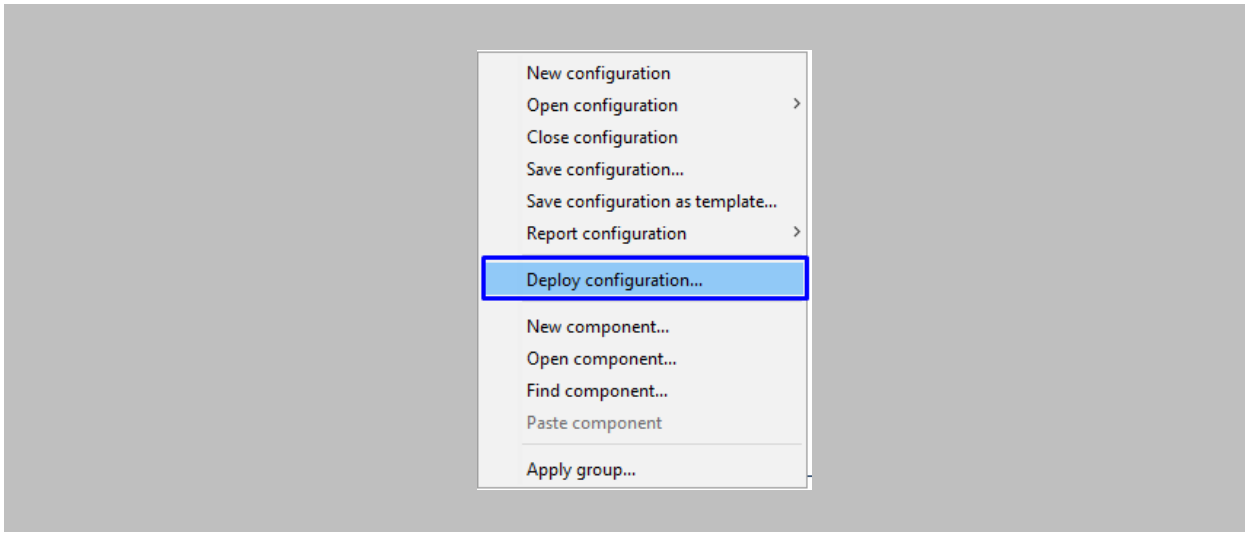


Figure 145: AEmon Wiegand- Deploy Configuration

21. Appendix

Pushing Configuration to Multiple Invixium Readers

Procedure

STEP 1

To push these configurations to other Invixium readers, while the configured Invixium device is selected, click the **Broadcast** option from vertical ellipses button.

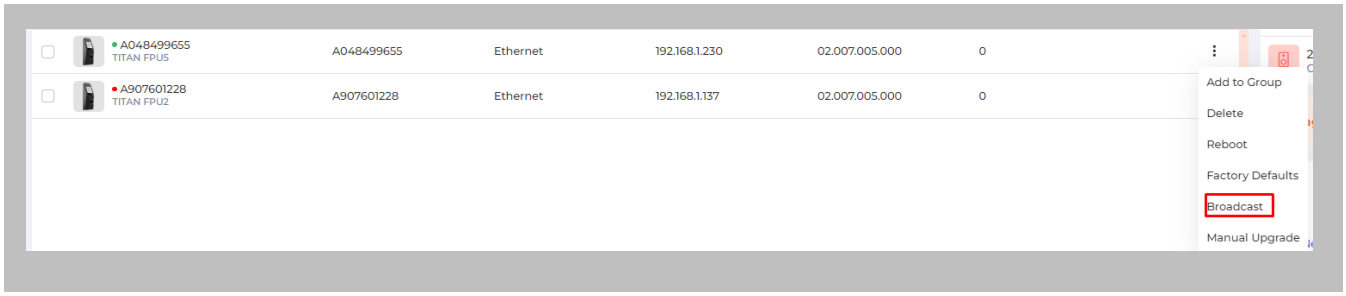


Figure 146: IXM WEB - Broadcast Option

STEP 2

Scroll down to the **Access Control** section → check **Wiegand Output** option → Click on **Broadcast**.

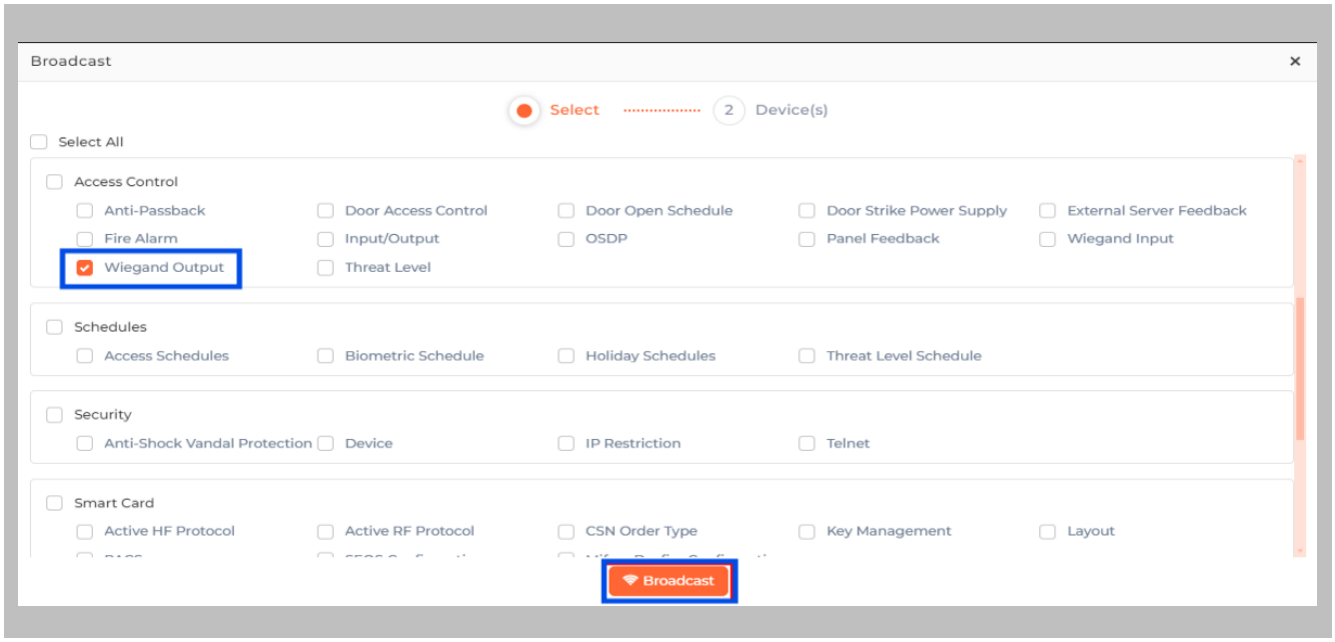


Figure 147: IXM WEB - Broadcast Wiegand Output Settings

STEP 3

Select the rest of the devices in the popup. Click **OK** to copy all Wiegand output settings of the source device to all destination devices.

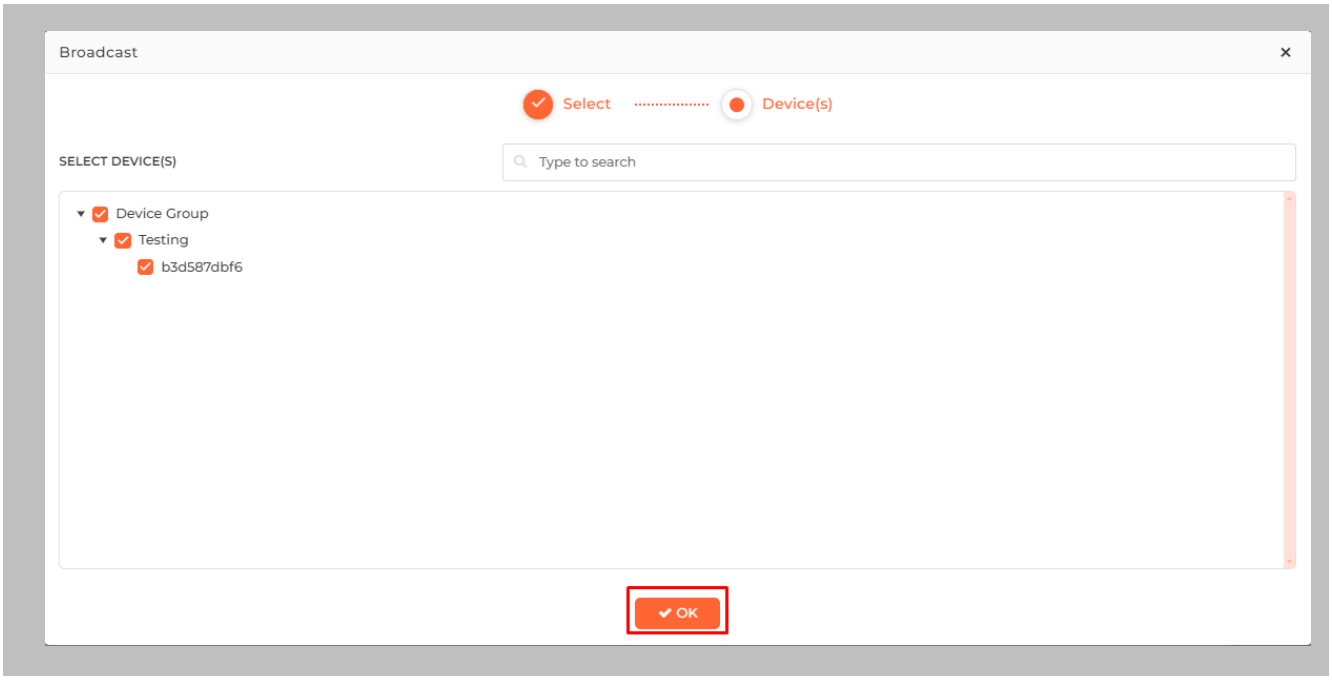


Figure 148: IXM WEB - Broadcast to Devices

Wiring and Termination

Procedure

Earth Ground

For protection against ESD, Invixium recommends the use of a ground connection between each Invixium device to a high-quality Earth Ground on site.

STEP 1

Connect the **green** and **yellow** earth wire from the wired back cover.

STEP 2

Connect the **open end** of earth ground wire provided in the install kit box to the **building earth ground**.

STEP 3

Screw the **lug end** of the earth ground.

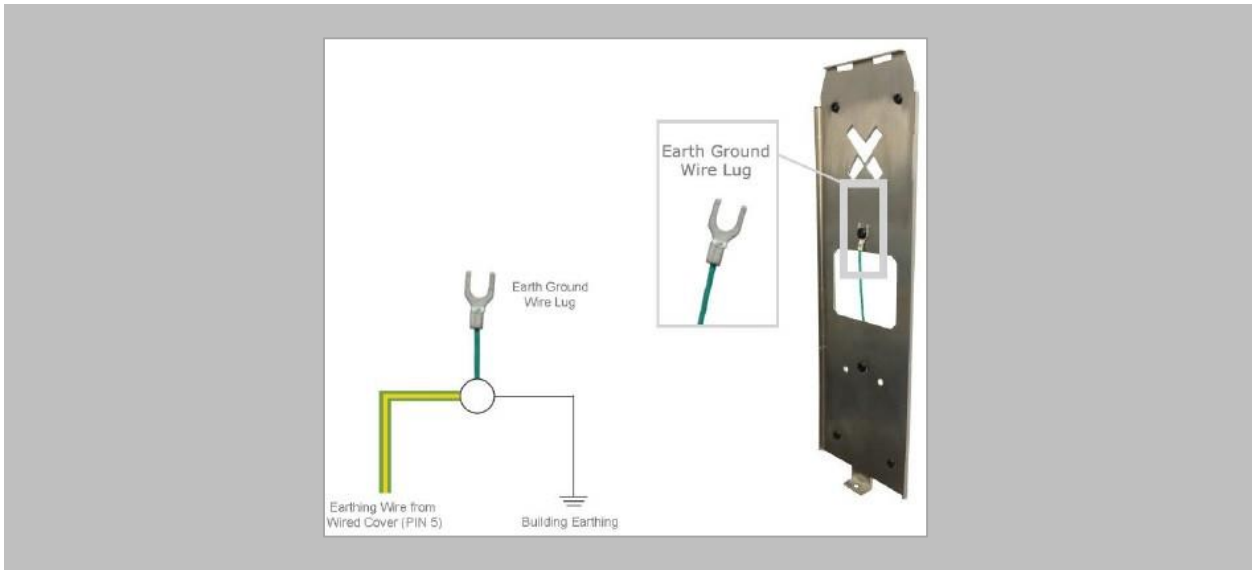


Figure 149: Earth Ground Wiring

WIRING

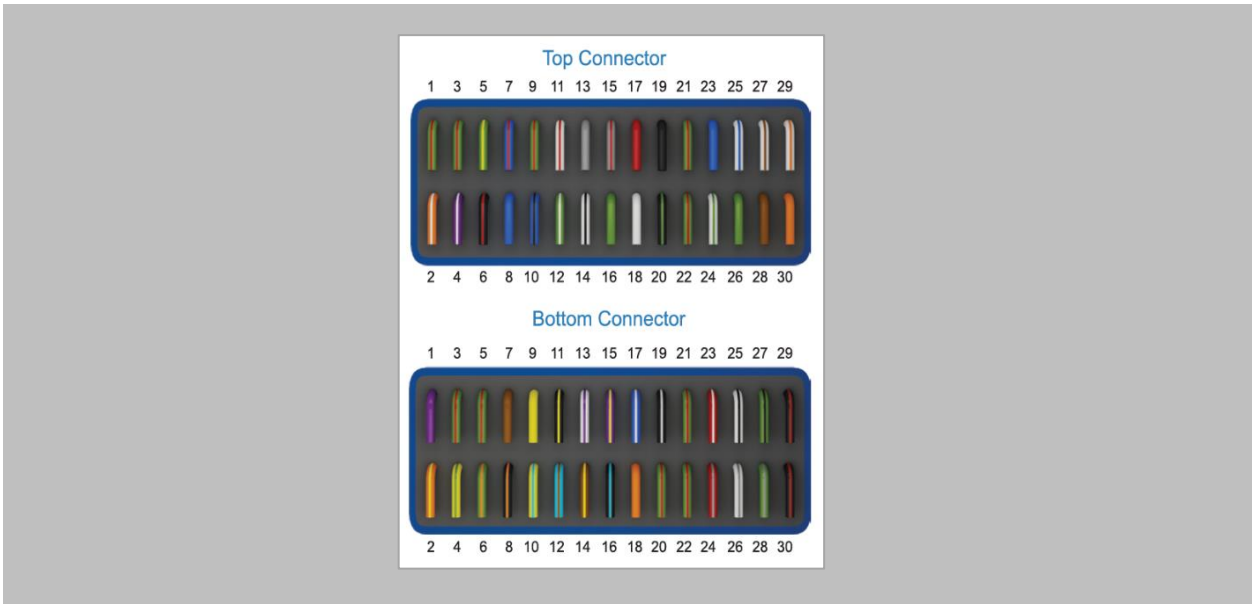
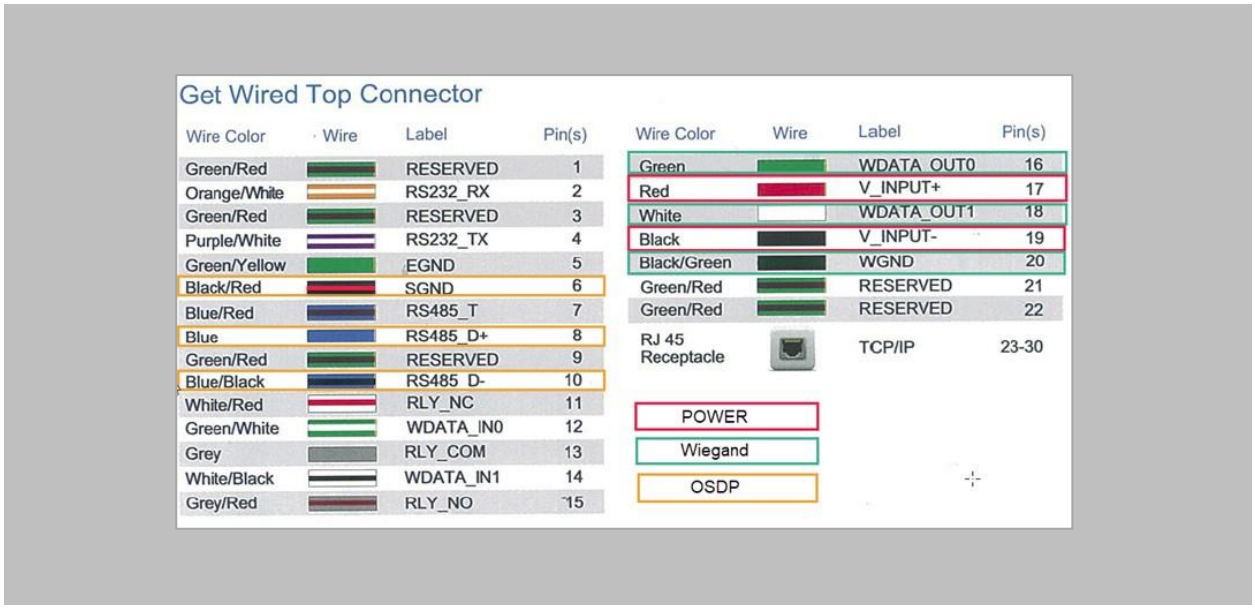


Figure 150: IXM TITAN – Top & Bottom Connector Wiring



Get Wired Top Connector

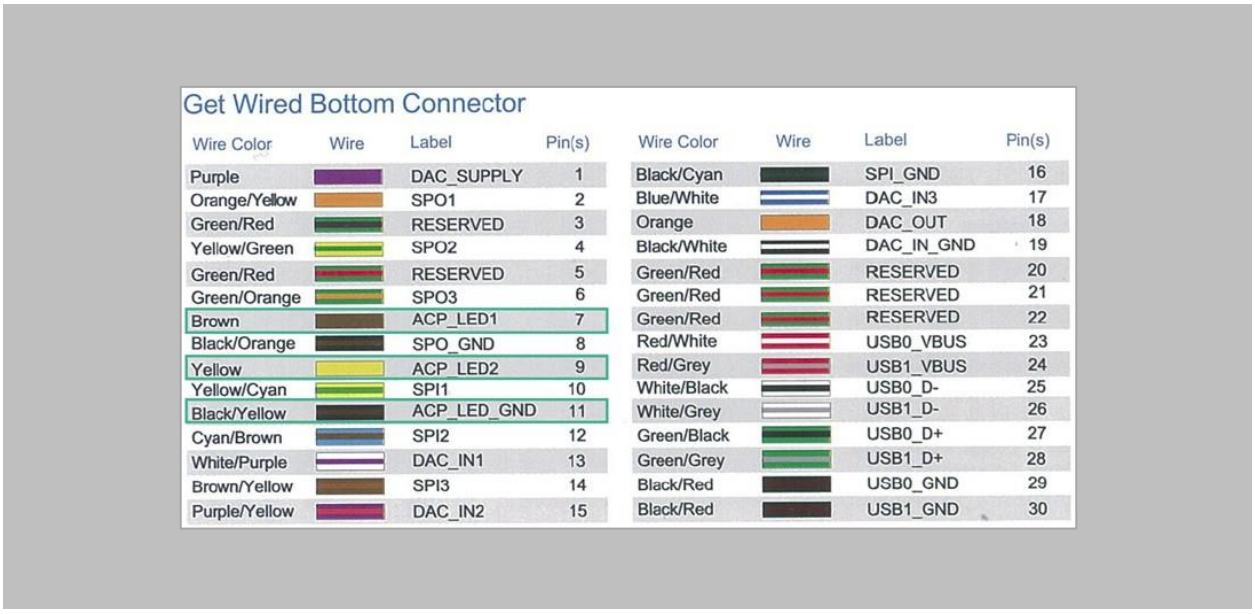
Wire Color	Wire	Label	Pin(s)
Green/Red		RESERVED	1
Orange/White		RS232_RX	2
Green/Red		RESERVED	3
Purple/White		RS232_TX	4
Green/Yellow		EGND	5
Black/Red		SGND	6
Blue/Red		RS485_T	7
Blue		RS485_D+	8
Green/Red		RESERVED	9
Blue/Black		RS485_D-	10
White/Red		RLY_NC	11
Green/White		WDATA_IN0	12
Grey		RLY_COM	13
White/Black		WDATA_IN1	14
Grey/Red		RLY_NO	15

Wire Color	Wire	Label	Pin(s)
Green		WDATA_OUT0	16
Red		V_INPUT+	17
White		WDATA_OUT1	18
Black		V_INPUT-	19
Black/Green		WGND	20
Green/Red		RESERVED	21
Green/Red		RESERVED	22
RJ 45 Receptacle		TCP/IP	23-30

POWER

Wiegand

OSDP



Get Wired Bottom Connector

Wire Color	Wire	Label	Pin(s)
Purple		DAC_SUPPLY	1
Orange/Yellow		SPO1	2
Green/Red		RESERVED	3
Yellow/Green		SPO2	4
Green/Red		RESERVED	5
Green/Orange		SPO3	6
Brown		ACP_LED1	7
Black/Orange		SPO_GND	8
Yellow		ACP_LED2	9
Yellow/Cyan		SPI1	10
Black/Yellow		ACP_LED_GND	11
Cyan/Brown		SPI2	12
White/Purple		DAC_IN1	13
Brown/Yellow		SPI3	14
Purple/Yellow		DAC_IN2	15

Wire Color	Wire	Label	Pin(s)
Black/Cyan		SPI_GND	16
Blue/White		DAC_IN3	17
Orange		DAC_OUT	18
Black/White		DAC_IN_GND	19
Green/Red		RESERVED	20
Green/Red		RESERVED	21
Green/Red		RESERVED	22
Red/White		USB0_VBUS	23
Red/Grey		USB1_VBUS	24
White/Black		USB0_D-	25
White/Grey		USB1_D-	26
Green/Black		USB0_D+	27
Green/Grey		USB1_D+	28
Black/Red		USB0_GND	29
Black/Red		USB1_GND	30

Figure 151: Power, Wiegand & OSDP Wires

All Invixium devices support Wiegand and OSDP.

Invixium devices can be integrated with a Nedap Controller on:

1. Wiegand (one-way communication)
2. Wiegand with panel feedback (two-way communication)
3. OSDP (two-way communication)

Wiegand Connection

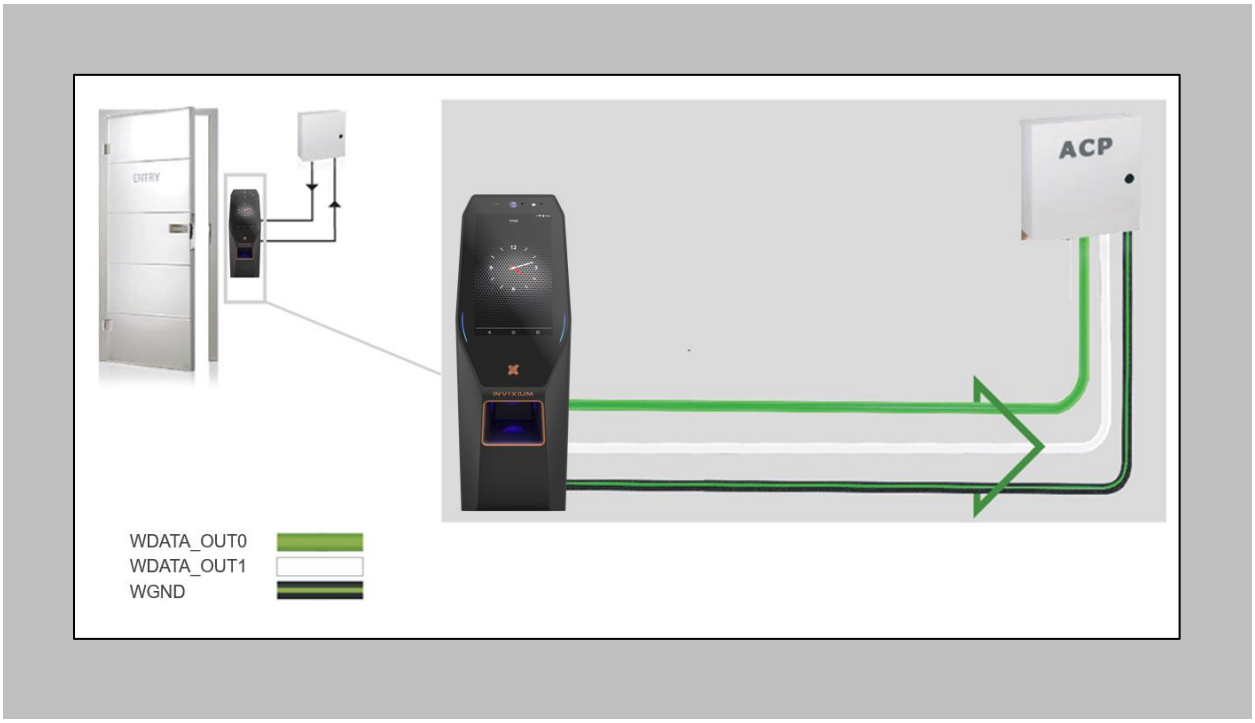


Figure 152: IXM TITAN - Wiegand

Please refer to the INGUIDE document provided for each product on Invixium.com under the **Download** section of the **Products** menu.

Wiegand Connection with Panel Feedback

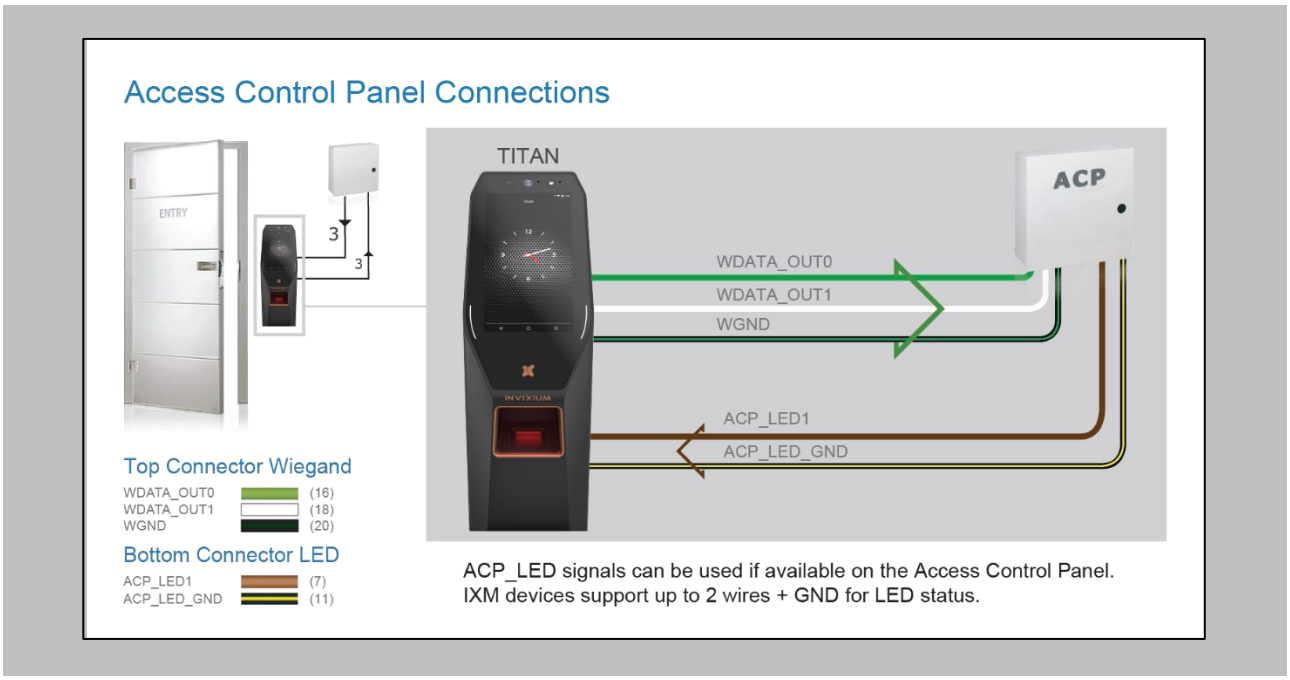


Figure 153: IXM TITAN - Panel Feedback

Please refer to the INGUIDE document provided for each product on Invixium.com under the **Download** section of the **Products** menu.

OSDP Connections

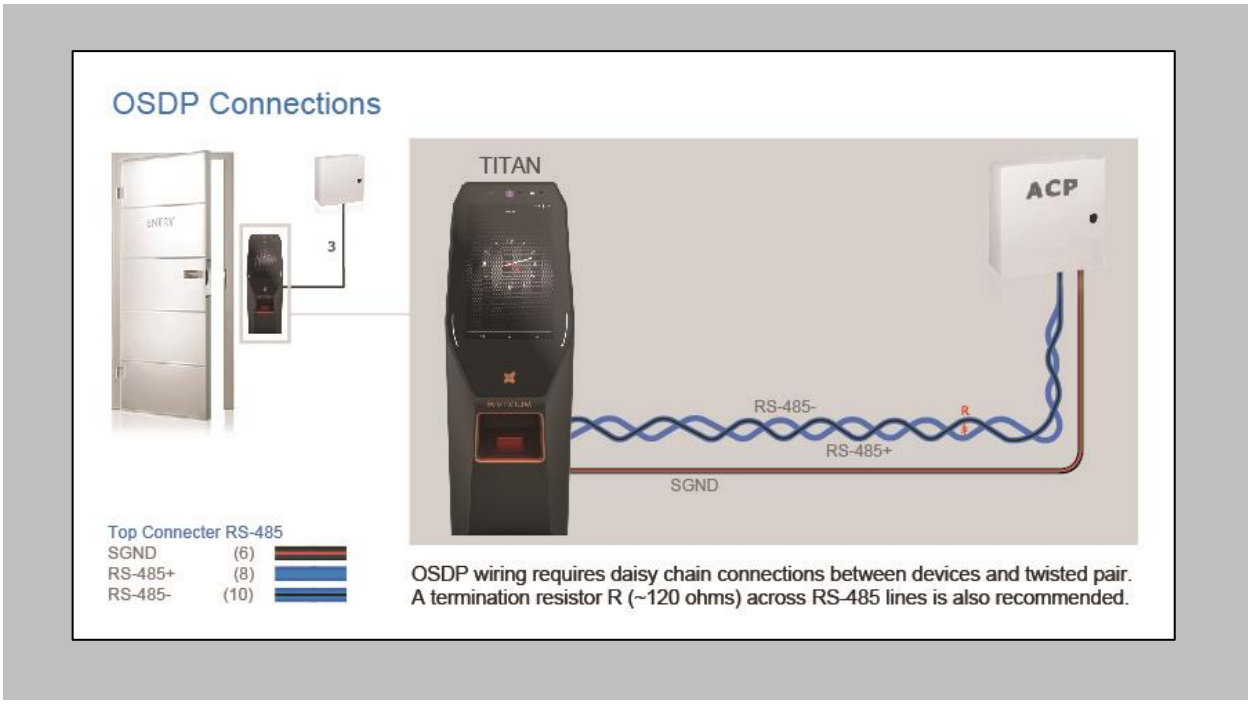


Figure 154: IXM TITAN - OSDP Connections

Please refer to the INGUIDE document provided for each product on Invixium.com under the **Download** section of the **Products** menu.

22. Troubleshooting

Reader Offline from IXM WEB Dashboard

Note: Confirm communication of the IXM WEB server to the Invixium reader.

Procedure

STEP 1

From **Home**, click the **Devices** tab.

STEP 2

Select any device.

STEP 3

Navigate to the **Communication** tab.

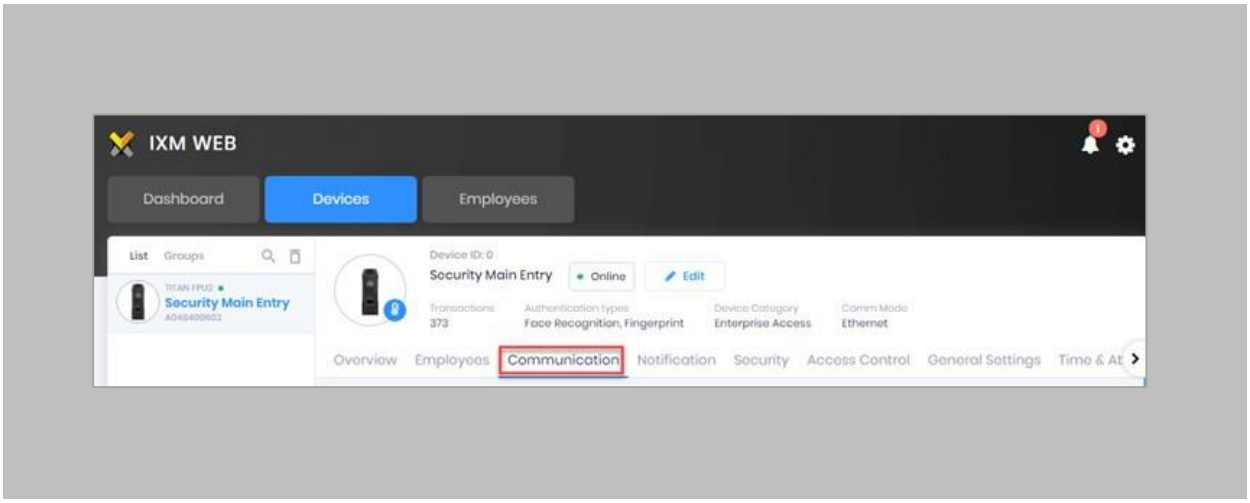


Figure 155: IXM WEB - Device Communication Settings

STEP 4

Scroll down and click on **IXM WEB Server**.

Figure 156: IXM WEB - Server URL Setting

Ensure the correct **IP address** of the server is listed here. If not, **correct** and **apply.**

STEP 5

Enter the **IP address** of the Invixium server followed by **port 9108.**

Format: **http://IP_IXMServer:9108**

STEP 6

Navigate to **General Settings** and make sure that the **URL** reflects the same setting.

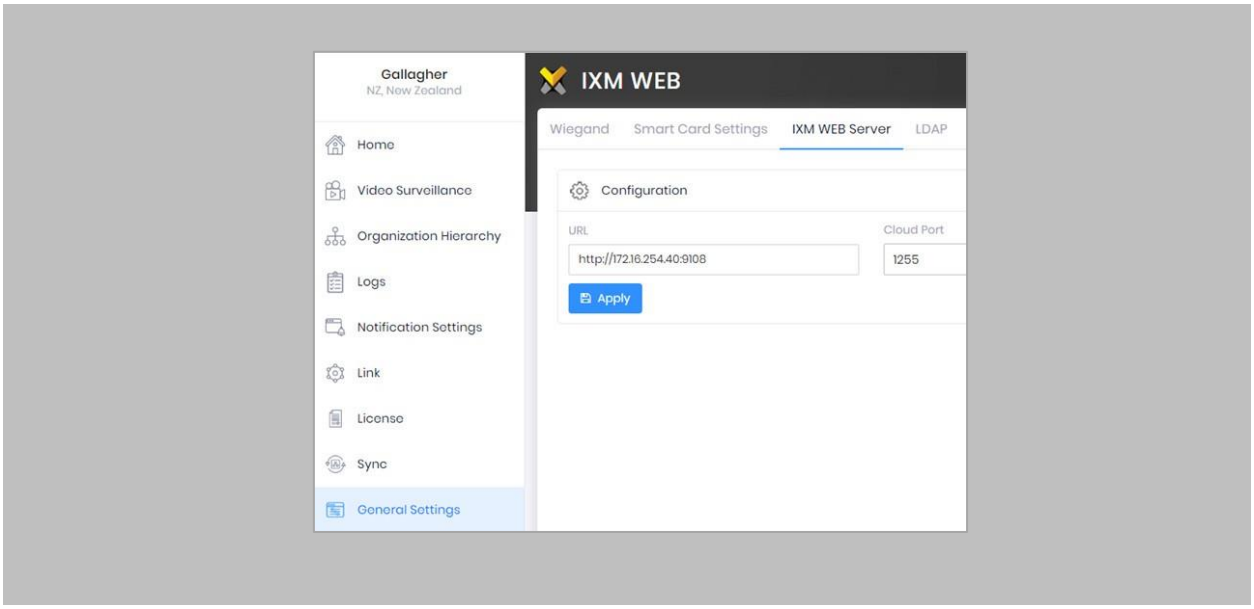


Figure 157: IXM WEB - Server URL Setting from General Setting

Logs in IXM WEB Application

Device Logs: Device Logs are used for debugging device-related issues.

From **Home** → Click the **Devices** tab on the top → Select the required **Device** → Navigate to the General Settings tab for the device → Click on Device Log → Enable Capture Device Logs.

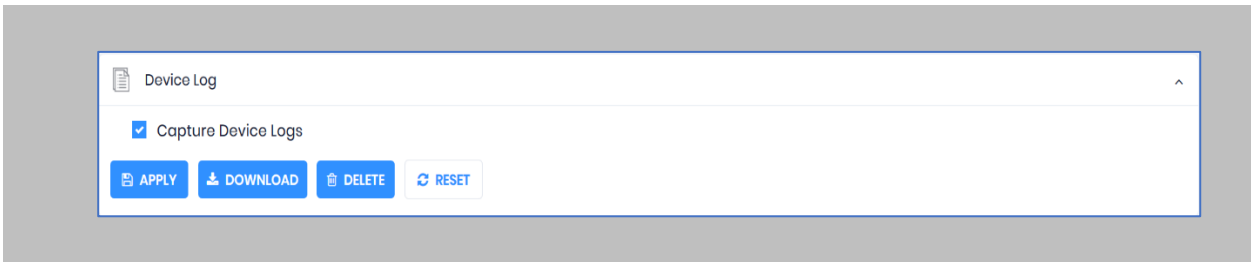


Figure 158: IXM WEB - Enable Device Logs

Click **Download** to initialize the process to download the device log file.

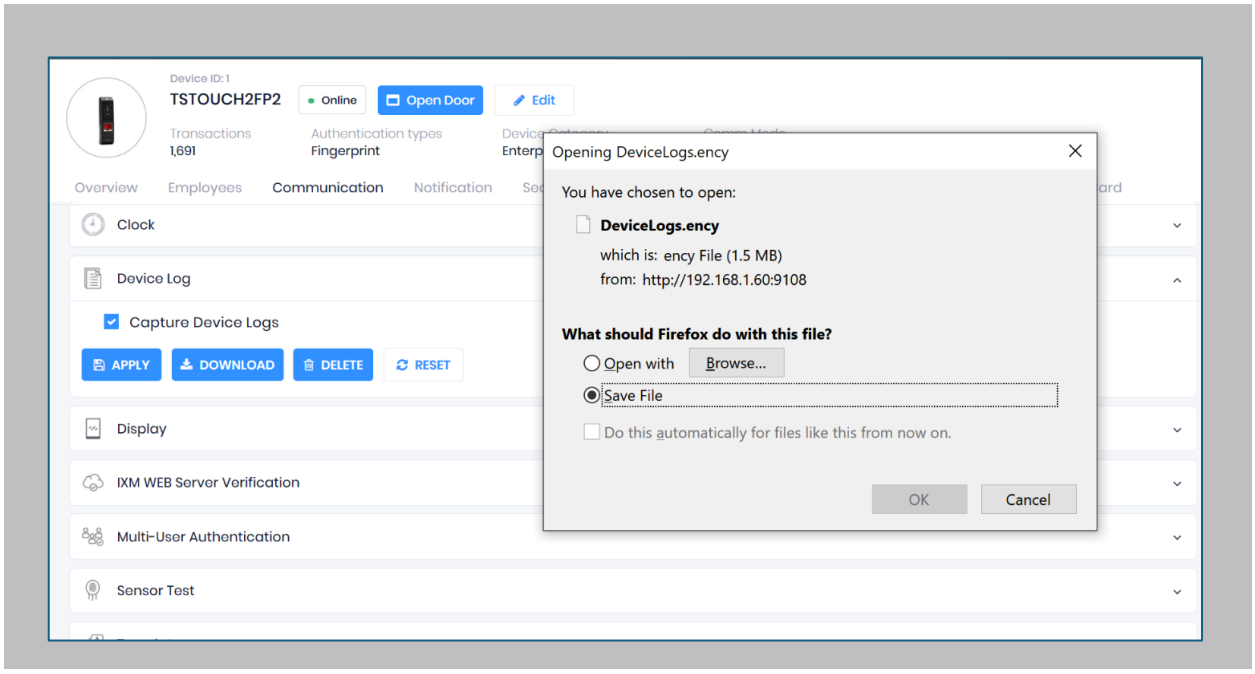


Figure 159: Save Device Log File

Select Save File and Click **OK** to store the device log file on your machine.

Transaction Logs (TLogs): Events or activities taking place on the IXM device.

- Transactions Logs can be viewed and exported from IXM WEB.
- Go to Logs in Left Navigation pane in IXM WEB and click on Transaction Logs. A filter option is available in the Transaction Logs column.

Application Logs: Application logs are available for any event, error, or information generated in IXM WEB.

- Application Logs can be viewed and exported from IXM WEB.
- Go to Logs in the Left Navigation pane in IXM WEB and click on Application Logs. A filter option is available in the Application Log column.

Logs folder location on IXM WEB Server:

IXM WEB Logs	C:\Program Files (x86)\Invixium\IXM WEB\Log
IXM WEB Service Logs	C:\Program Files (x86)\Invixium\IXMWebService
IXM API Logs	C:\Program Files (x86)\Invixium\IXMAPI\Log

Table 8: Logs Folder Location

23. Support

For more information relating to this document, please contact support@invixium.com.

24. Disclaimer and Restrictions

This document and the information described throughout are provided in their present condition and are delivered without written, expressed, or implied commitments by Invixium. and are subject to change without notice. The information and technical data herein are strictly prohibited for the intention of reverse engineering and shall not be disclosed to parties for procurement or manufacturing.

This document may contain unintentional typos or inaccuracies.

TRADEMARKS

The trademarks specified throughout the document are registered trademarks of Invixium. All third-party trademarks referenced herein are recognized to be trademarks of their respective holders or manufacturers.