IXM WEB Integration with AEOS by Nedap

Installation Instructions

V2.0

P/N XAD-TPI-004-02G

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	

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	2021.1
Invixium IXM WEB	2.2.252.0
Operating Systems	Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2 Windows 10 Professional Version Windows Server 2016 Standard Windows Server 2019
Microsoft .NET Framework	.NET Framework 4.7.2
Database Engine	SQL Server 2014 or higher
Internet Information Services (IIS)	Microsoft® Internet Information Services version 7.5 or higher
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

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 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/

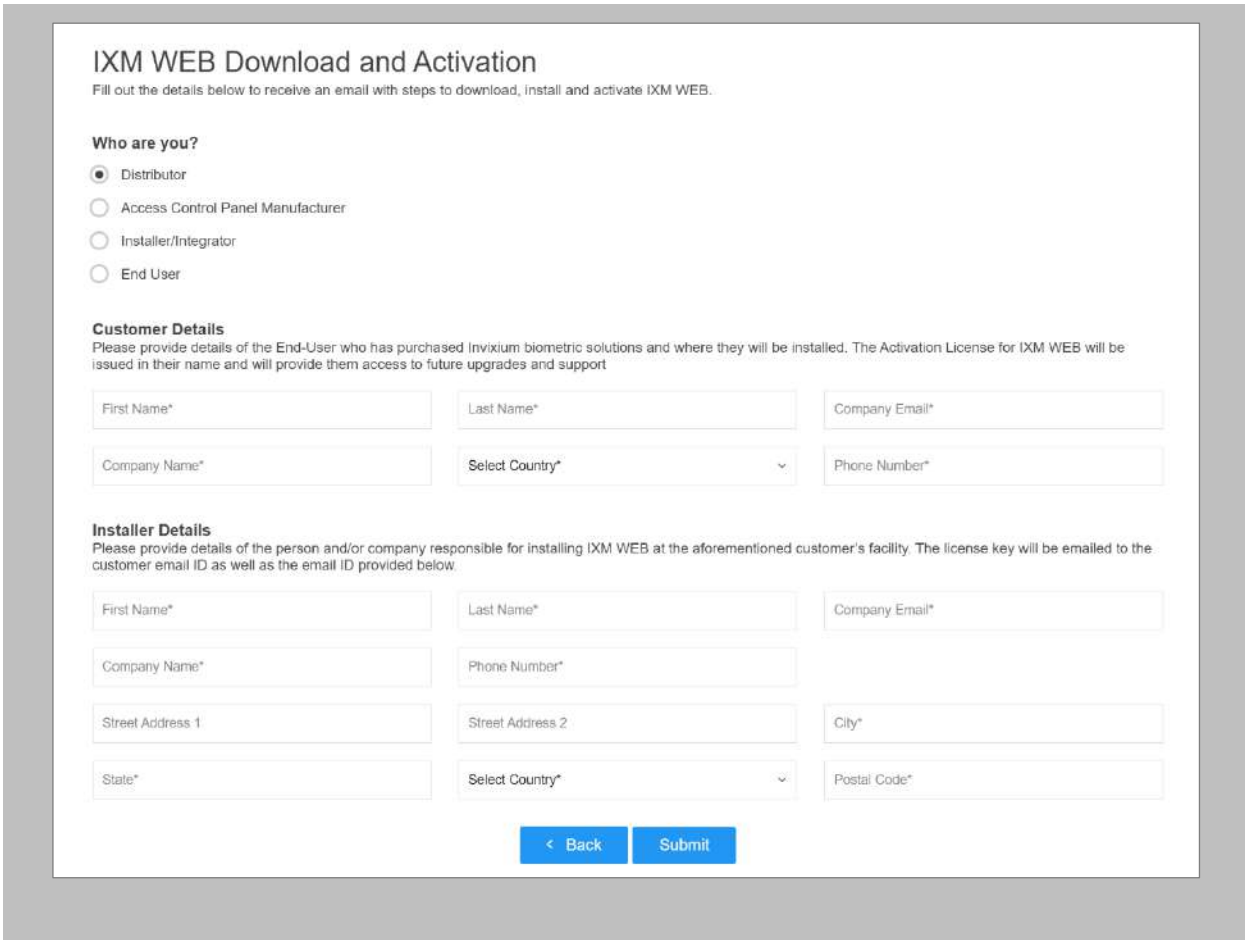
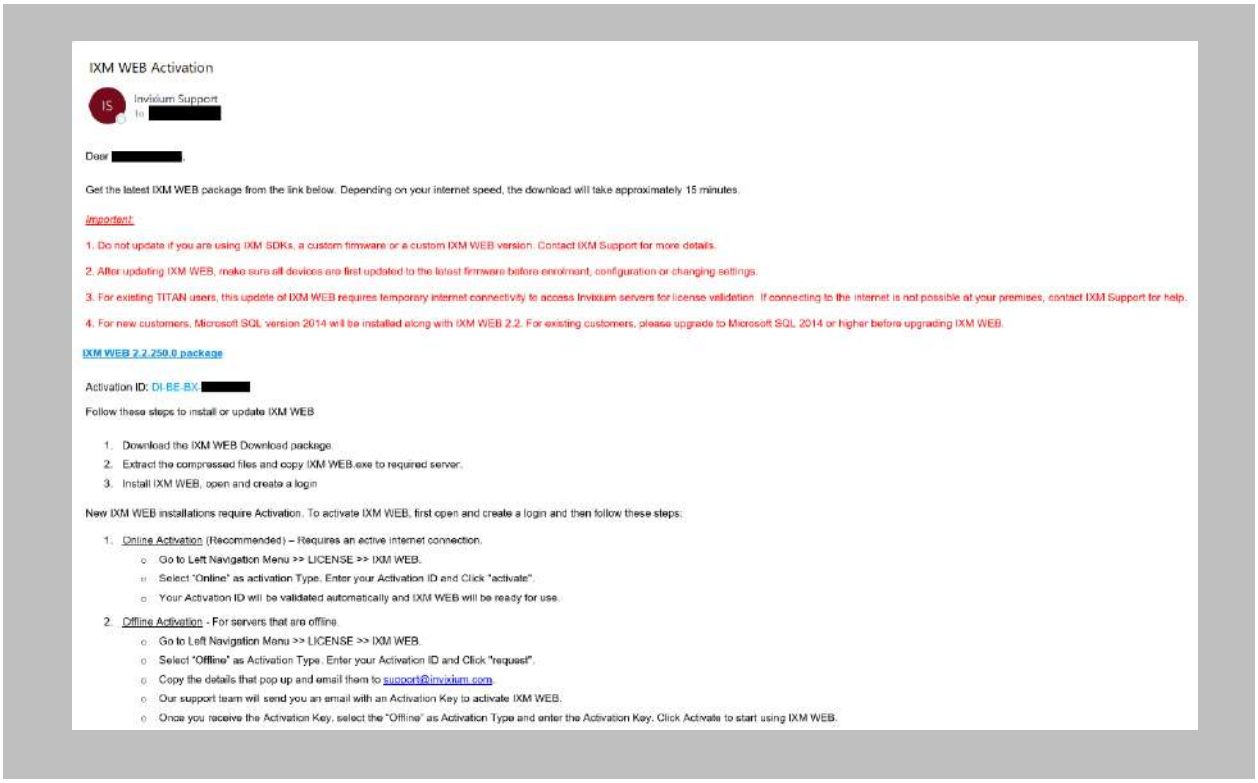


Figure 1: IXM WEB Online Request Form

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 sampleemail that includes instructions on how to download and install IXM WEB along with your Activation ID.



IXM WEB Activation

IS Invixium Support
to [redacted]

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 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 2.2.250.0 package

Activation ID: DI-BE-BX-[redacted]

Follow these steps to install or update IXM WEB

1. Download the IXM WEB Download 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.

Figure 2: 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 WEBshould 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

6. Installing IXM WEB

Software Install

Procedure

STEP 1

Run the IXM WEB installer (Run as administrator). Click **Install** to continue. It will display apopup window to accept the **License Agreement**.

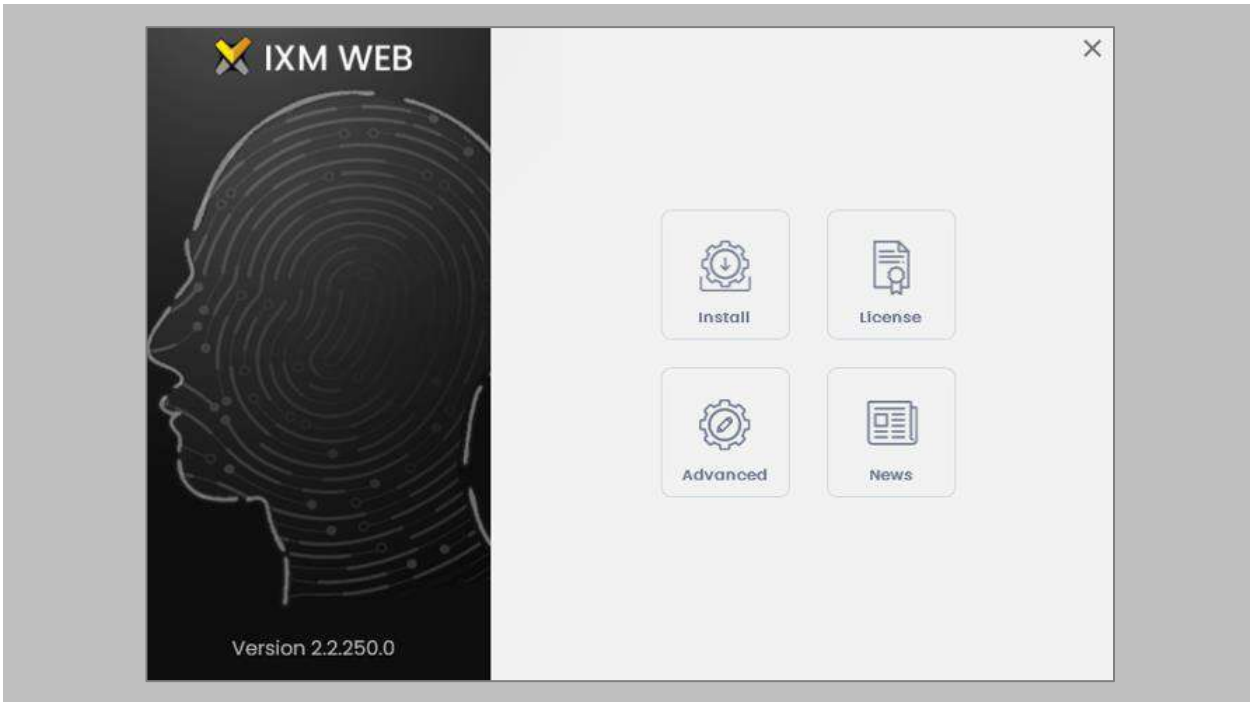


Figure 3: IXM WEB Installer

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 specify a port number that communicateswith the IIS server. Click **Advance**.

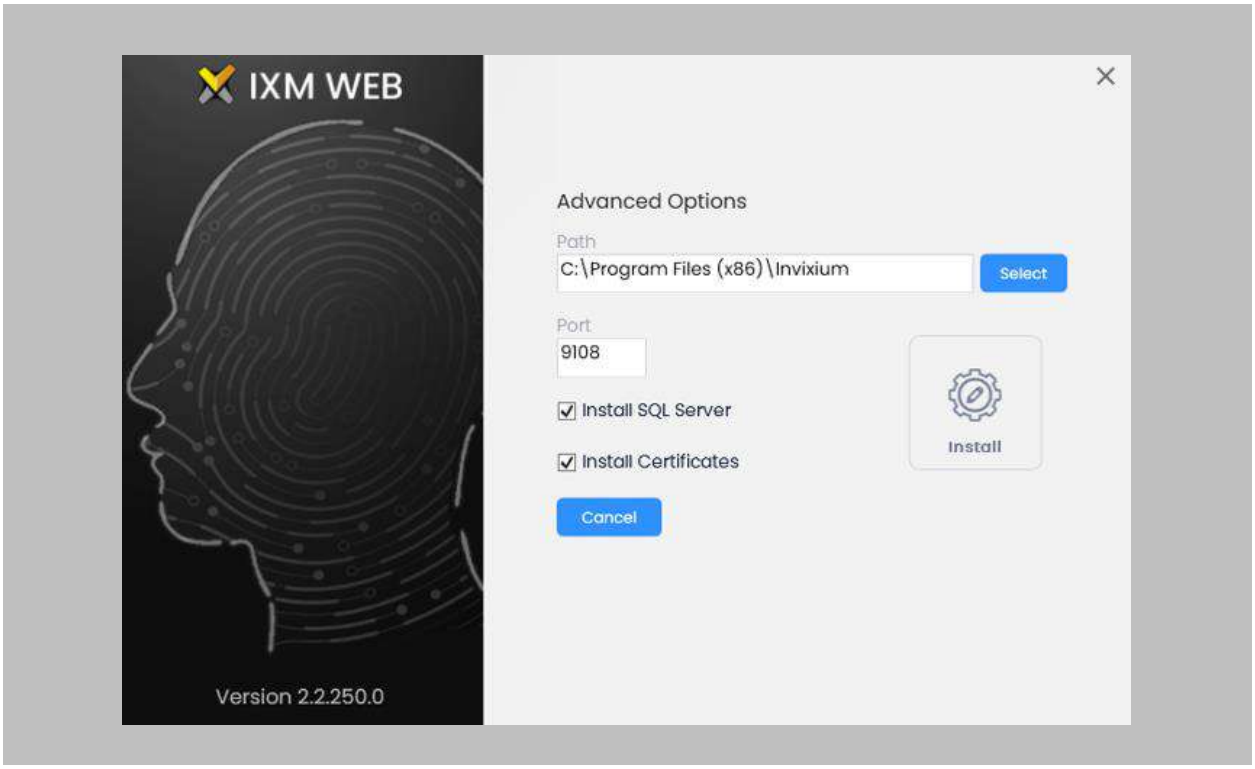


Figure 4: Advanced Option in IXM WEB Installer

STEP 4

In **Advanced** installations, the user can change the following options:

- **Installation Path:** In basic installation, 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.If IXM WEB is configured over the cloud, it will install a specific certificate for that purpose. 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.

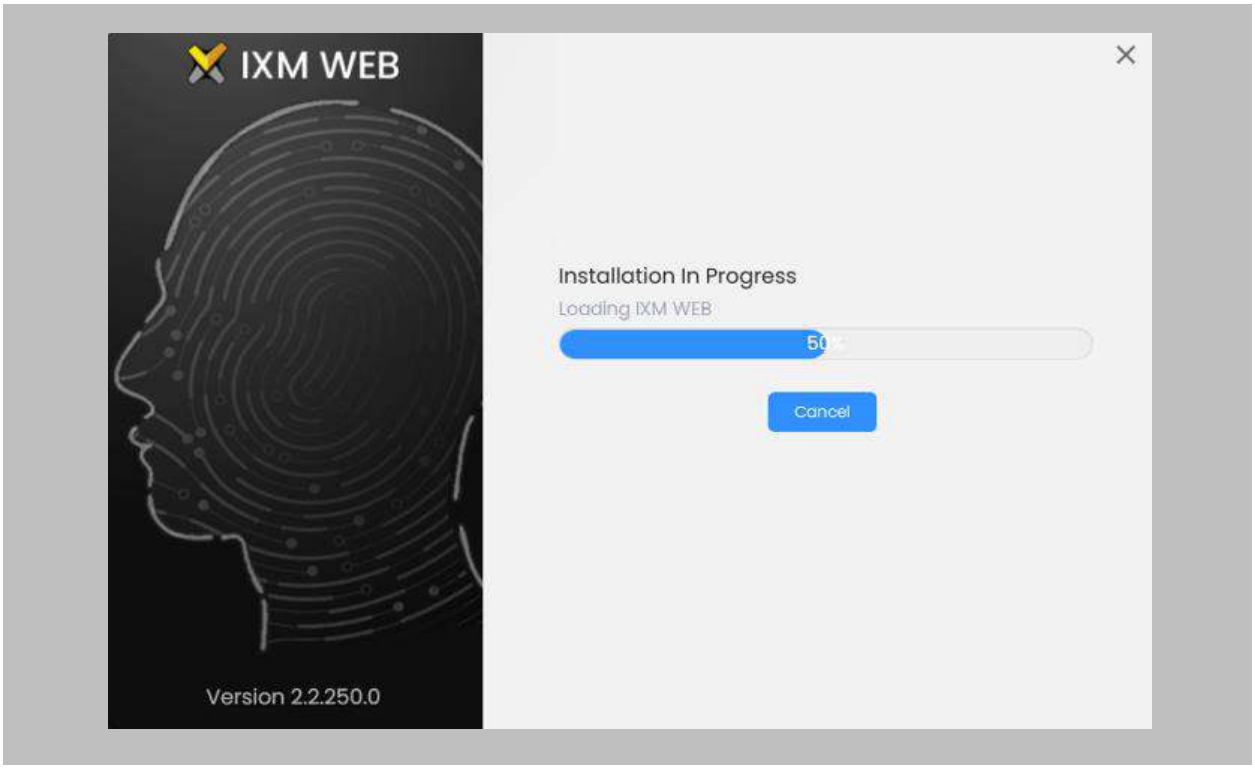


Figure 5: IXM WEB Installation

STEP 6

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

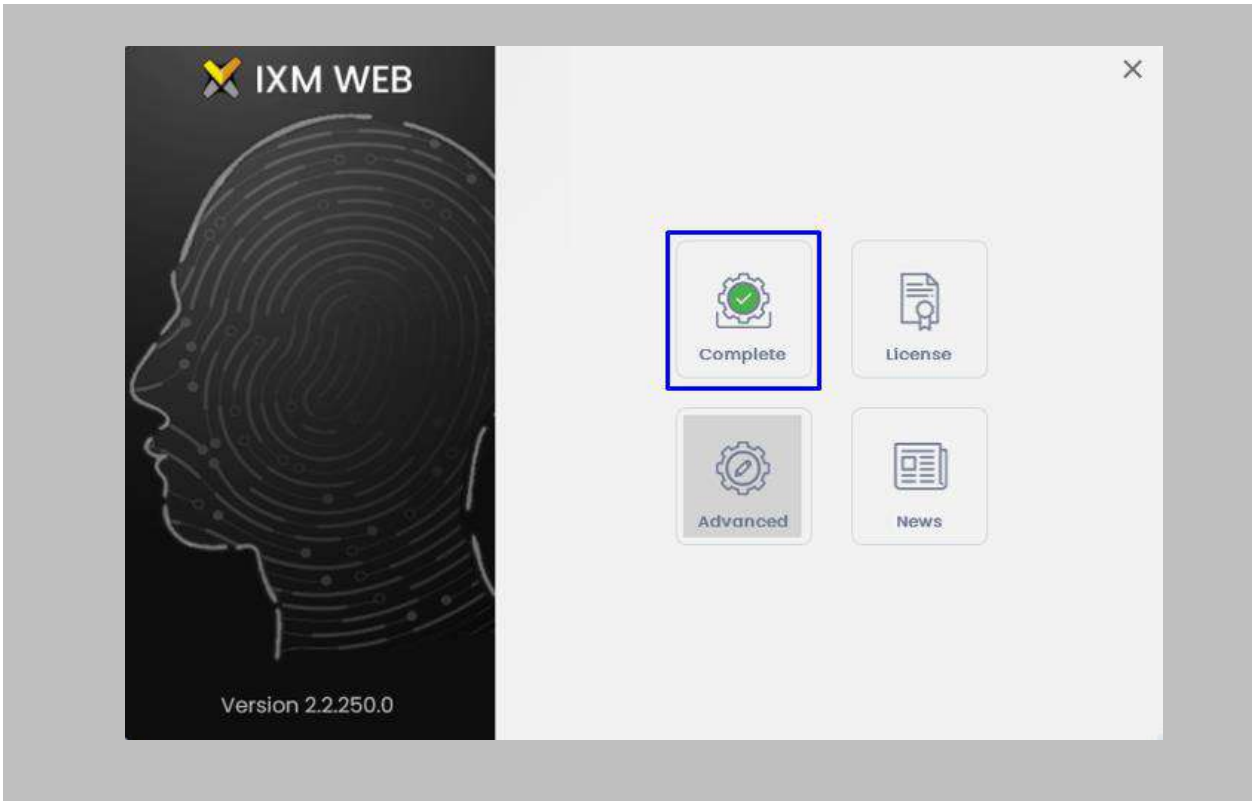


Figure 6: IXM WEB Installation Completed

STEP 7

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

Figure 7: 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.

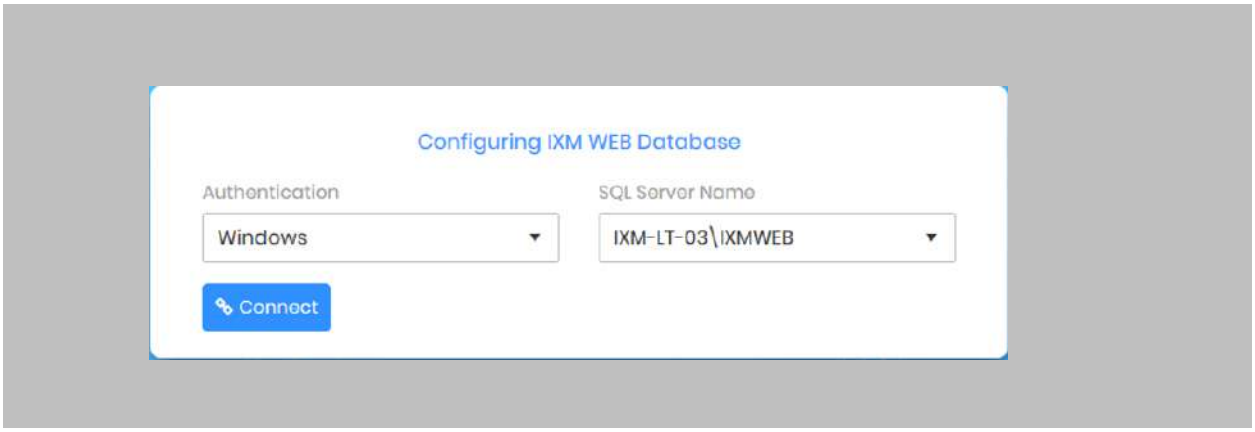


Figure 8: IXM WEB Database Configuration

STEP 9

IXM WEB will populate the default SQL Server Name and SQL Server Instance.

STEP 10

If the user wants to configure the 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 be required to add credentials (SQL Username and Password) to connect to the database server machine.

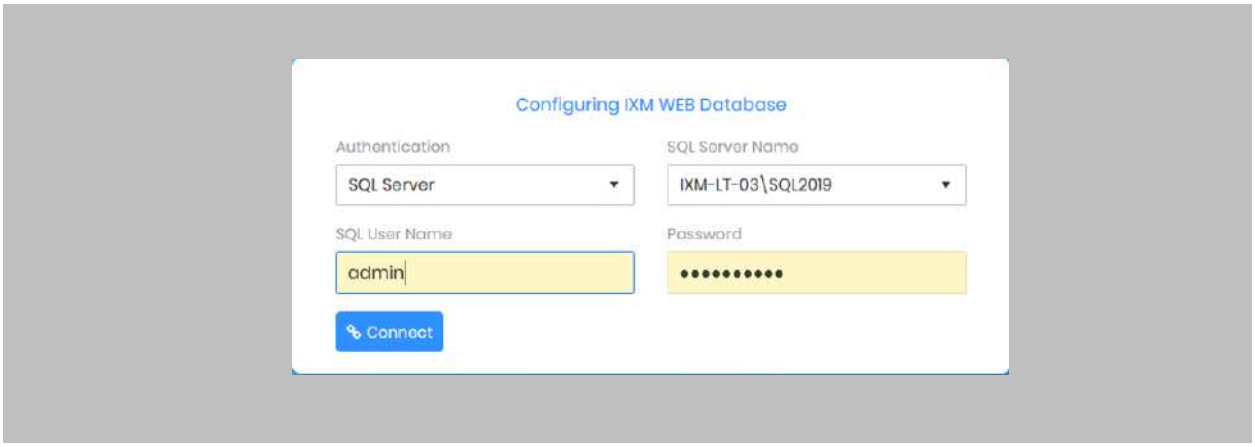


Figure 9: SQL Database Configuration

STEP 11

If a user wants to use the same database instance of 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.

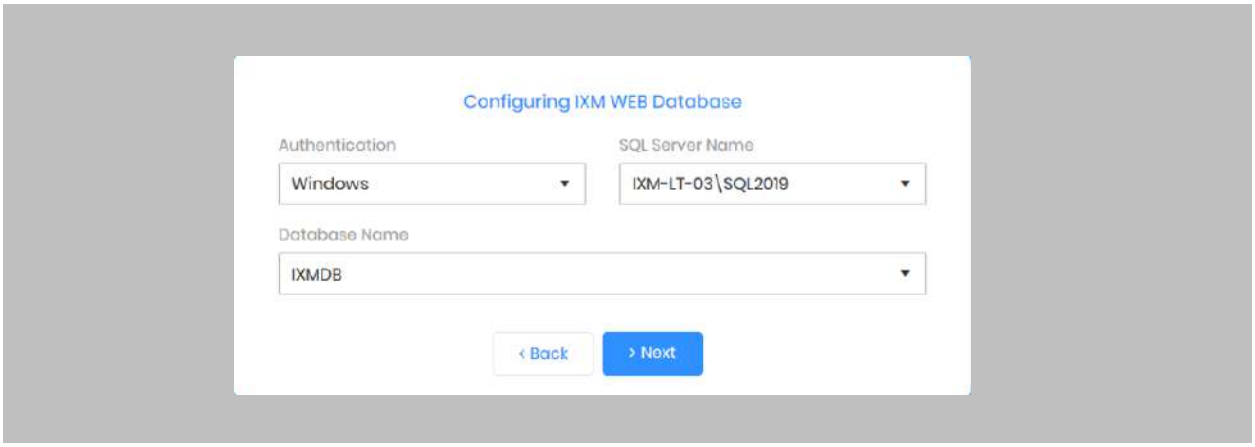


Figure 10: IXM WEB Database Name

STEP 13

Click **Next**.

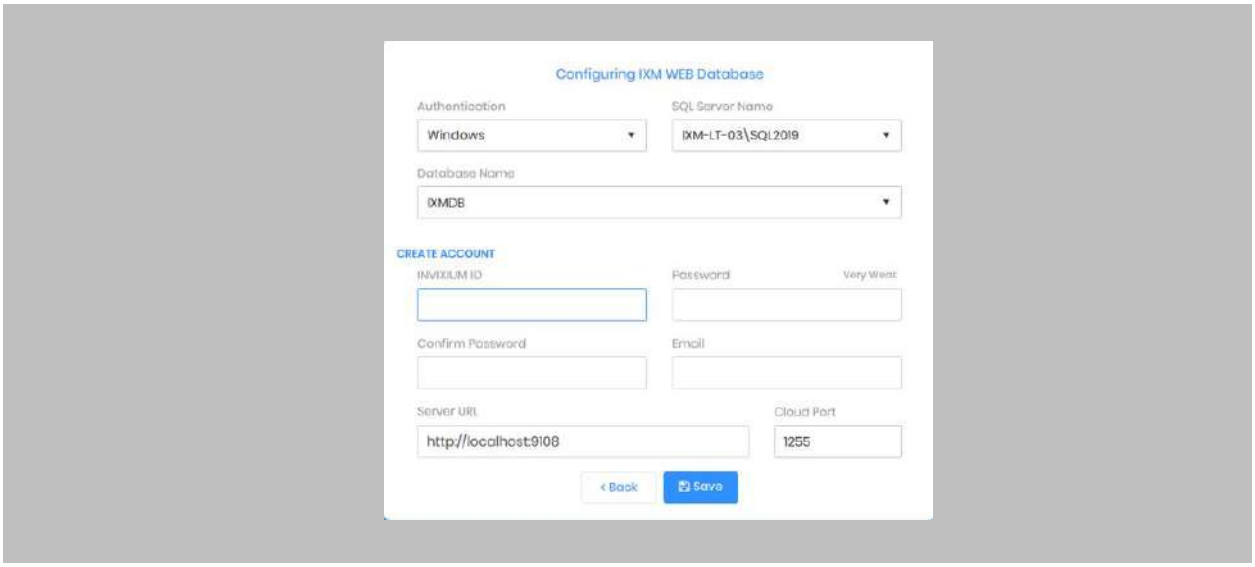


Figure 11: IXM WEB Administrator User Configuration

STEP 14

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

STEP 15

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 is 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 any email notification must be sent.

- **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 16

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

Figure 12: Save Database Configuration

STEP 17

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

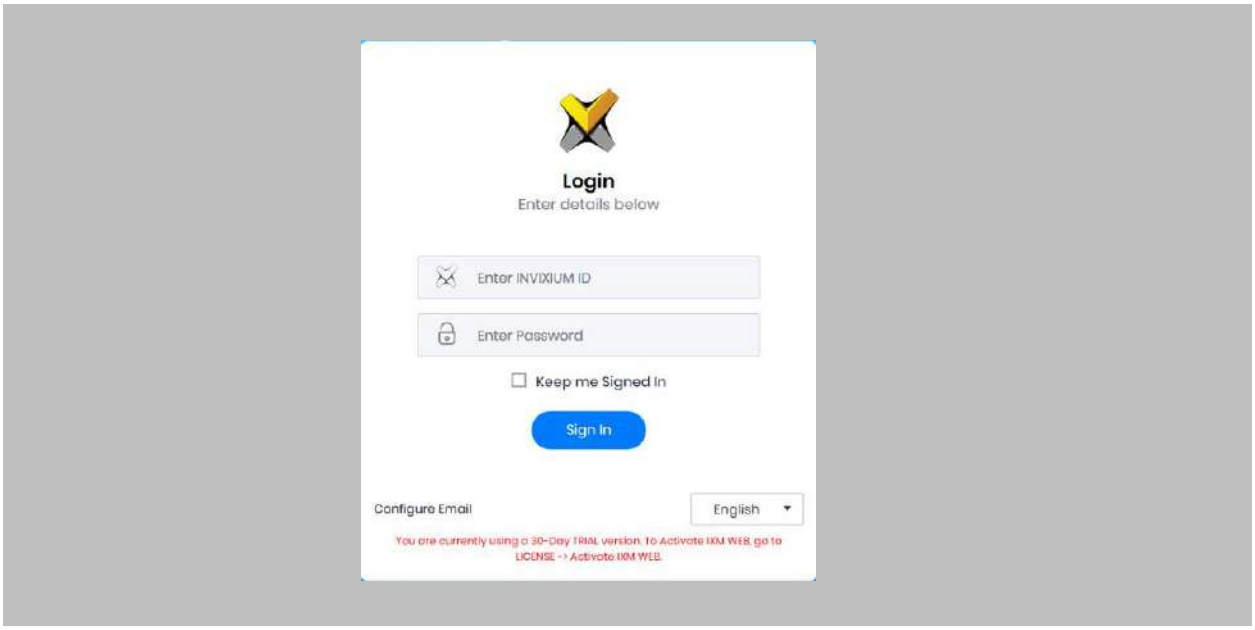


Figure 13: IXM WEB Login Page

7. 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

Click **Configure Email** on the Login page**.**

OR

Expand the **Left Navigation Pane** → Navigate to **Notification Settings** → **Email Configuration** → Click **Manage Preferences**.

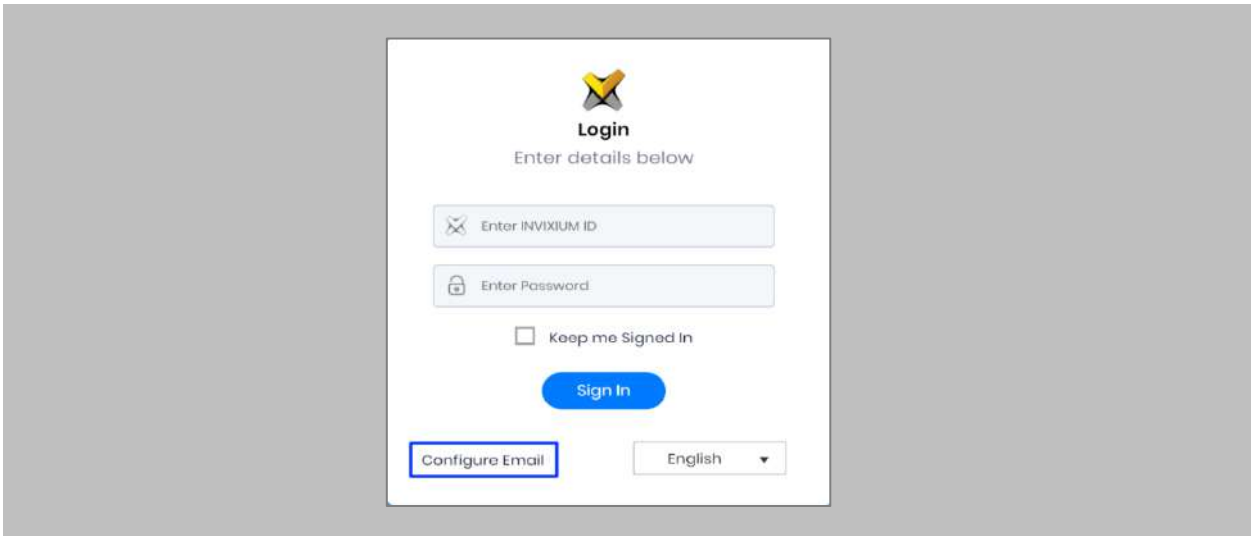


Figure 14: Configure Email

STEP 2

Select **'Enable Email Configuration'** and enter values for **'SMTP Host,' 'SMTP Port'** and **'Send email message from'** fields.

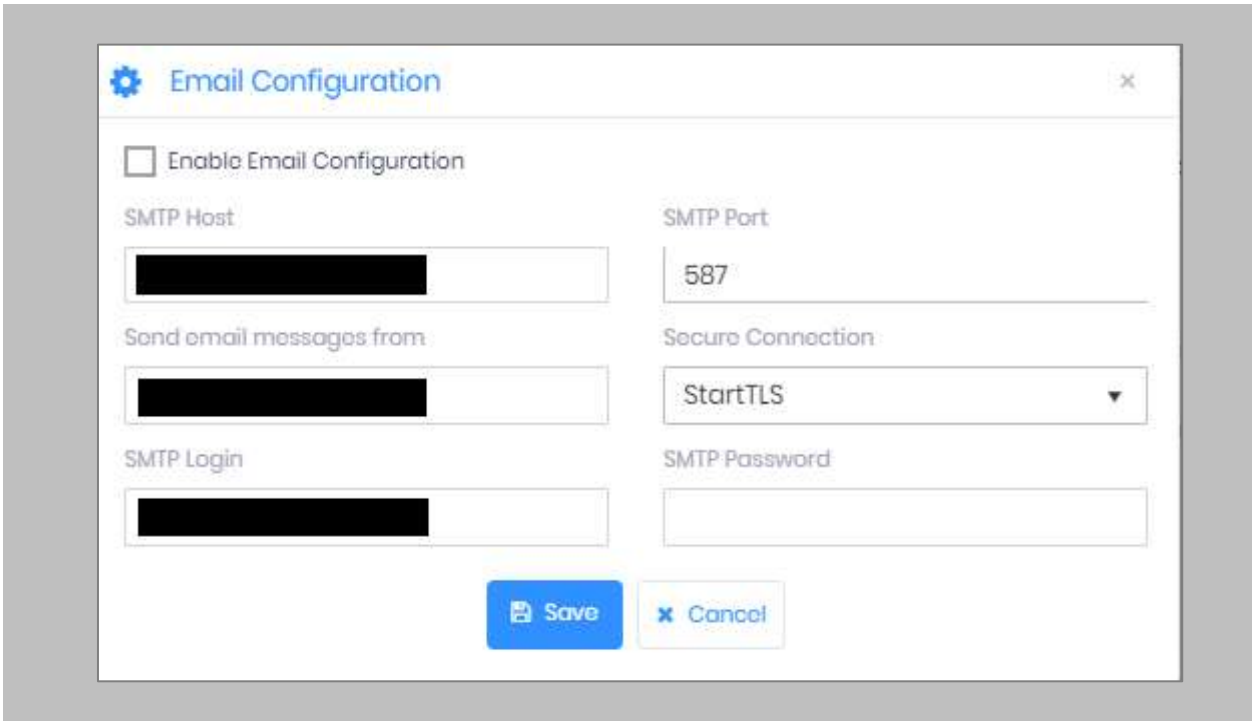


Figure 15: IXM WEB - SMTP Settings

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.

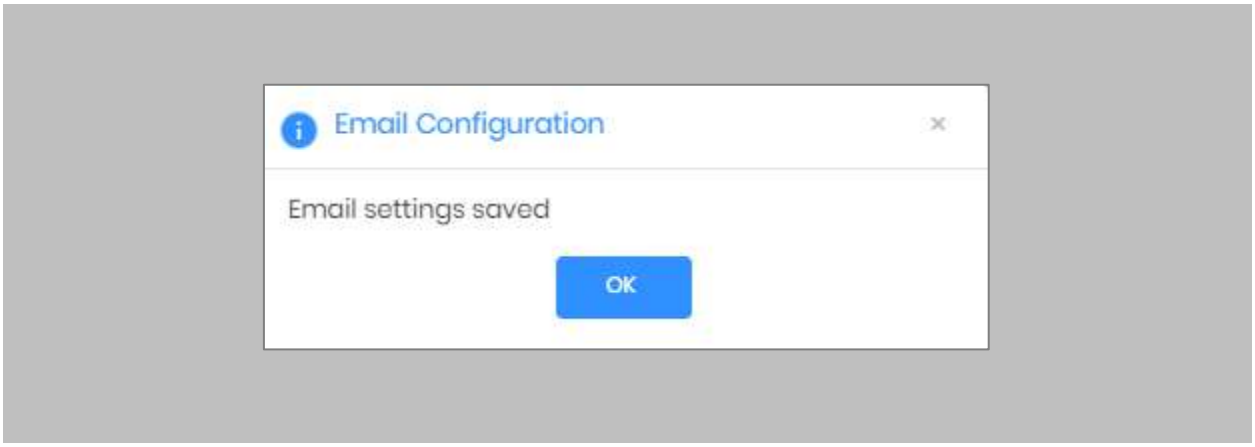


Figure 16: IXM WEB - Save Email Settings

To test the settings, Navigate to **Notification Settings** from **the Left navigation Pane** → Go to **Email Configuration** → Click **the Test Connection** button on the right.

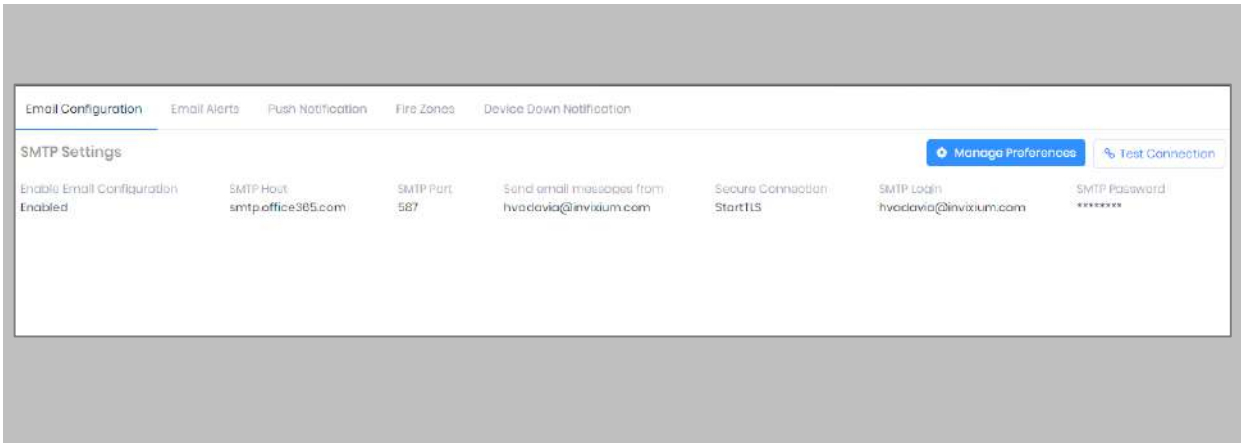


Figure 17: IXM WEB - Test Connection

Provide a valid email address. Click **Send** to send a test email.

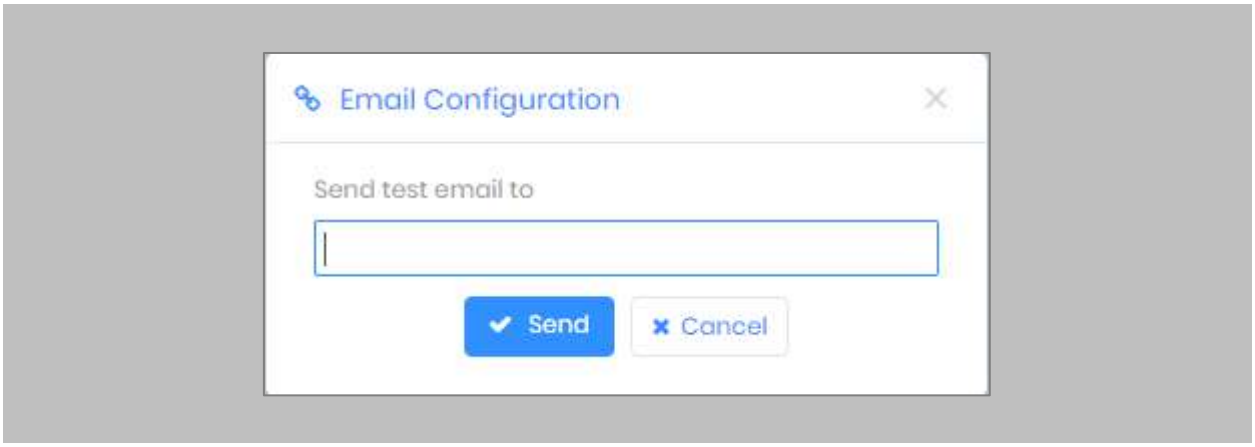


Figure 18: IXM WEB - Enter Email ID

STEP 4

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

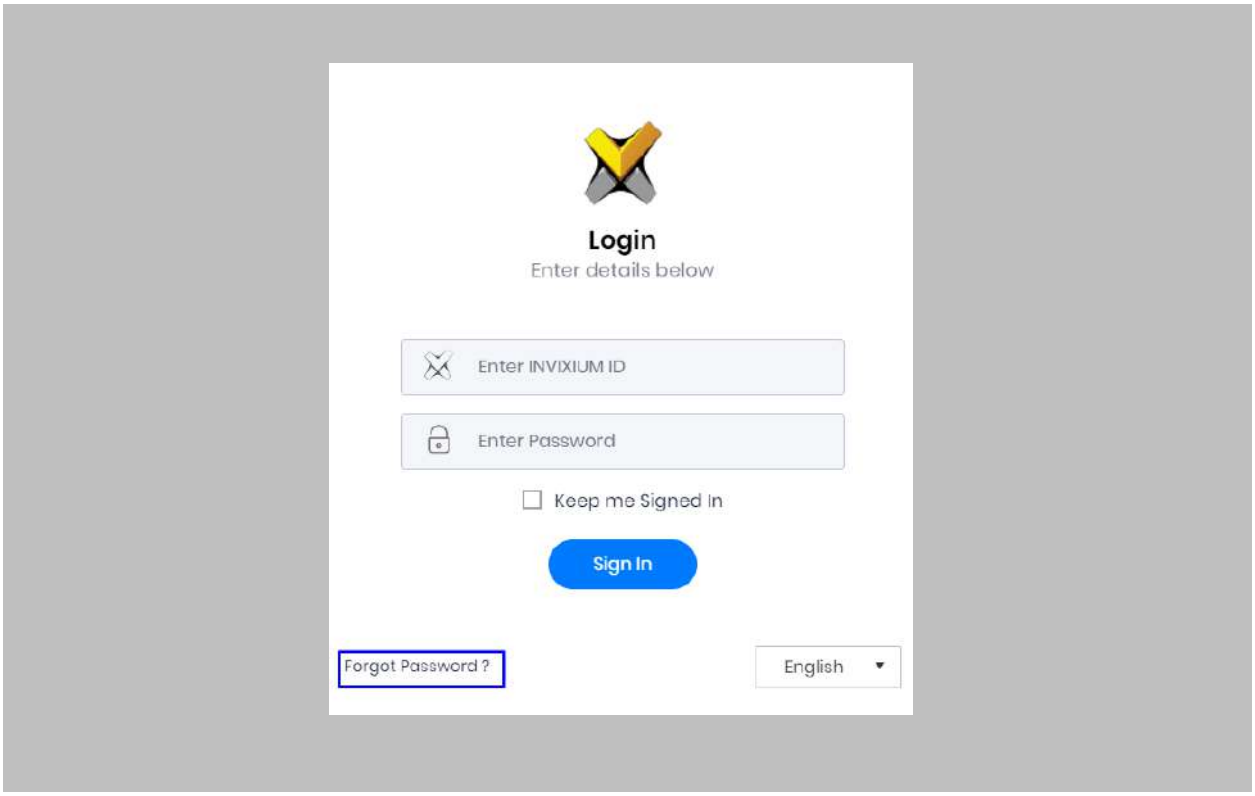


Figure 19: IXM WEB - Forgot Password

8. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

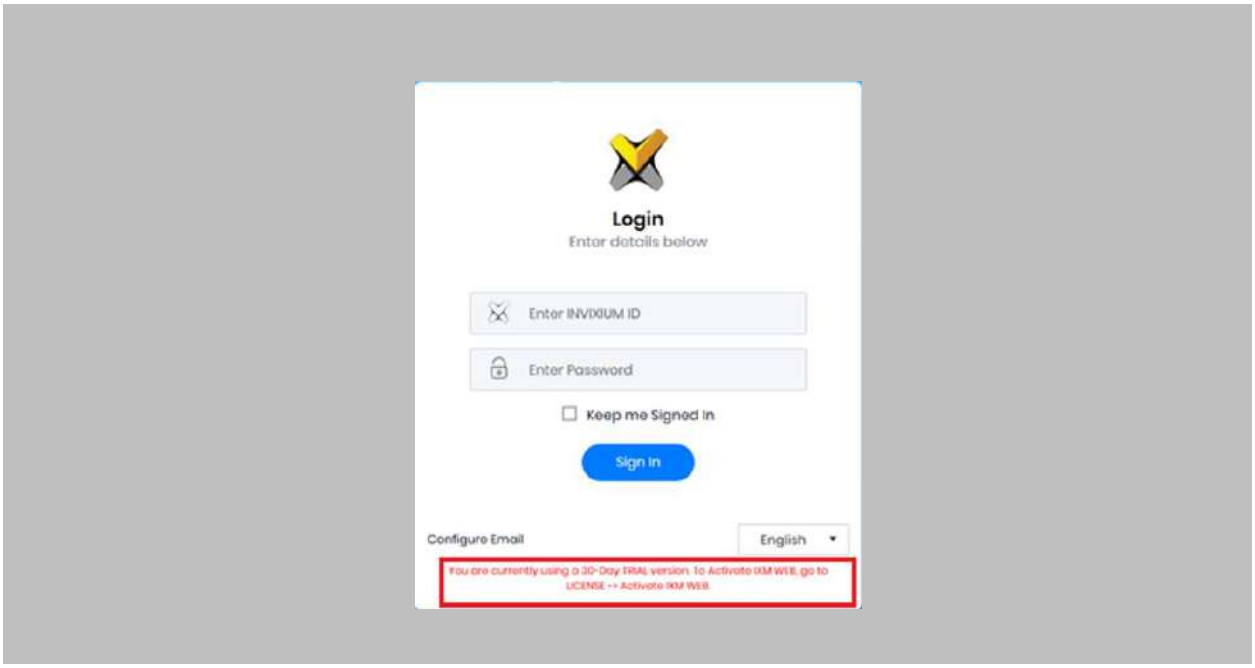


Figure 20: IXM WEB - Enter Login Credentials

STEP 2

Select the **License Tab** and then select the **IXM WEB** module to request an activation key for **IXM WEB.**

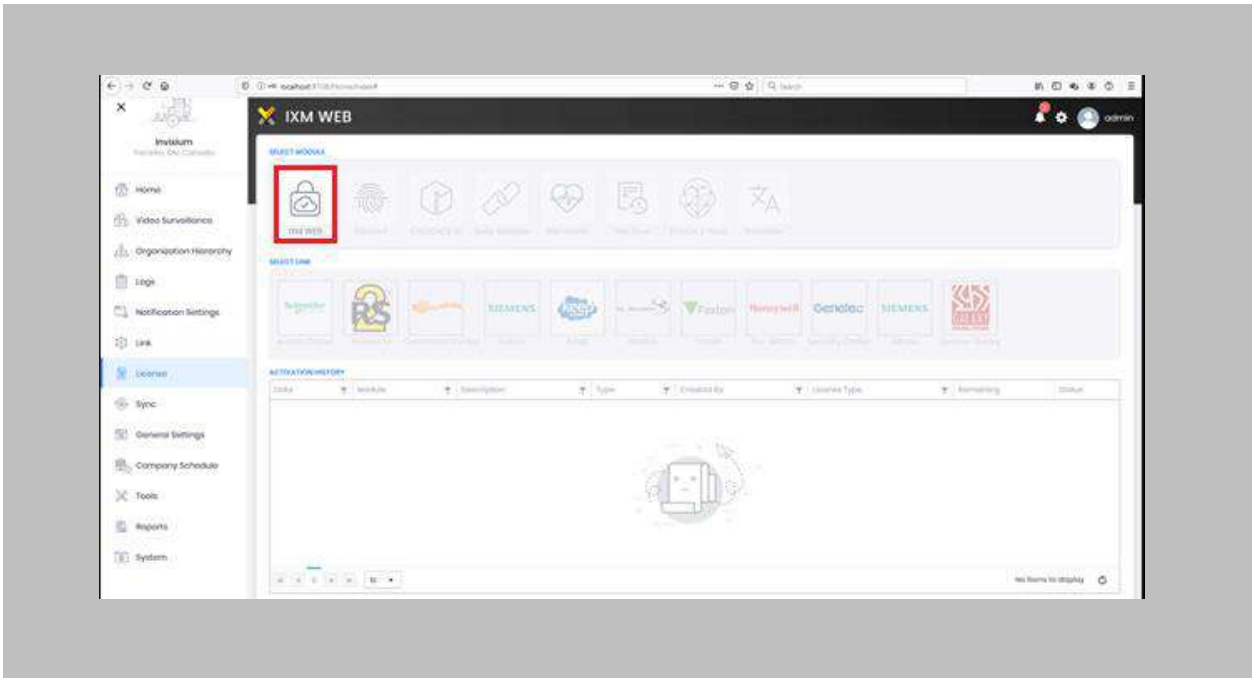


Figure 21: IXM WEB - License Setup

STEP 3

Request Activation Key Online or via Offline Activation Options.

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

STEP 4

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

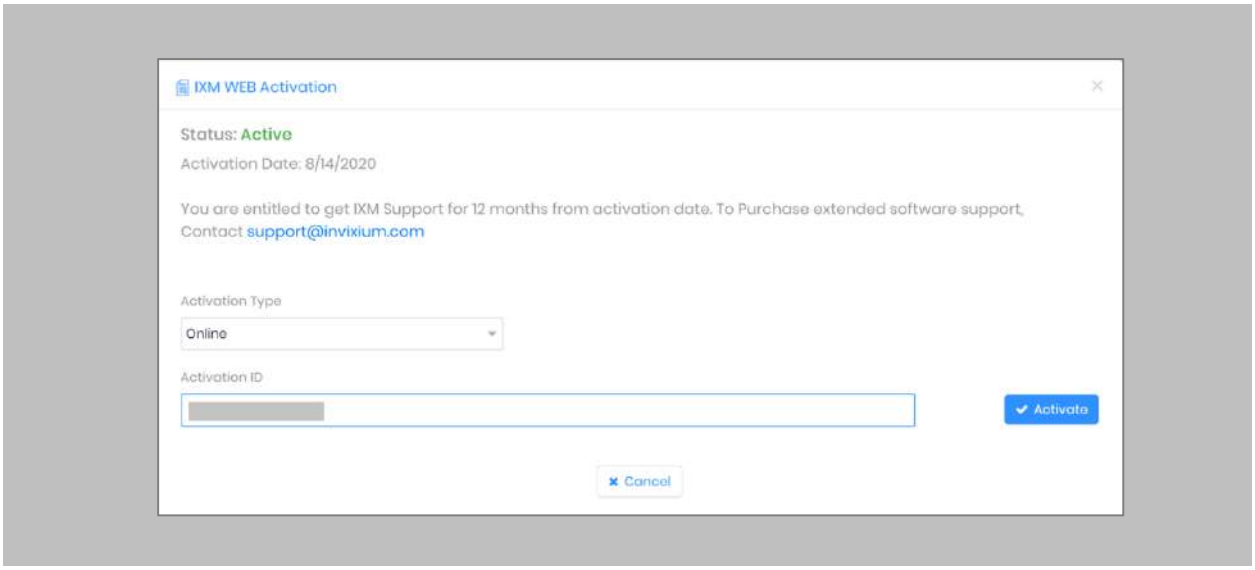


Figure 22: IXM WEB - Online Activation

Nedap AEOS Module Activation

The option to request 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**

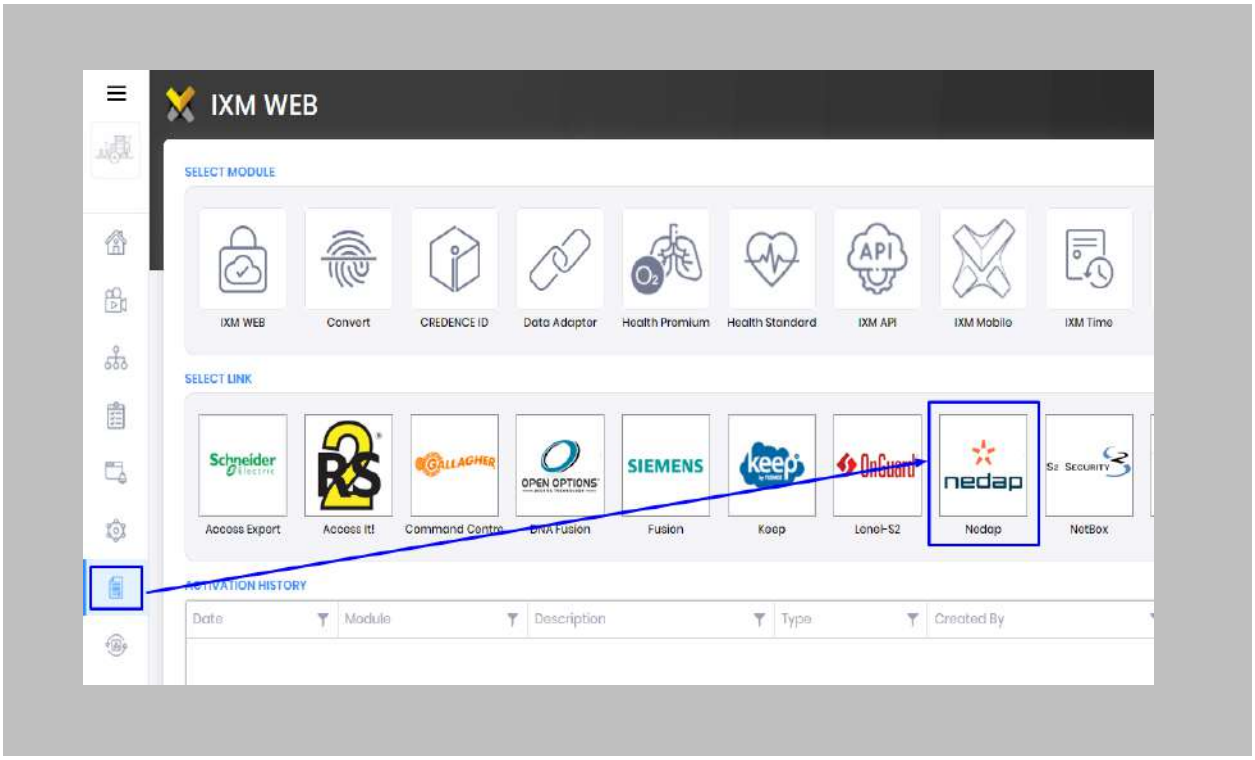


Figure 23: IXM WEB - Nedap Link Activation

STEP 3

Select the required license based on the number of devices that the install site has and click **Request** to see the details.

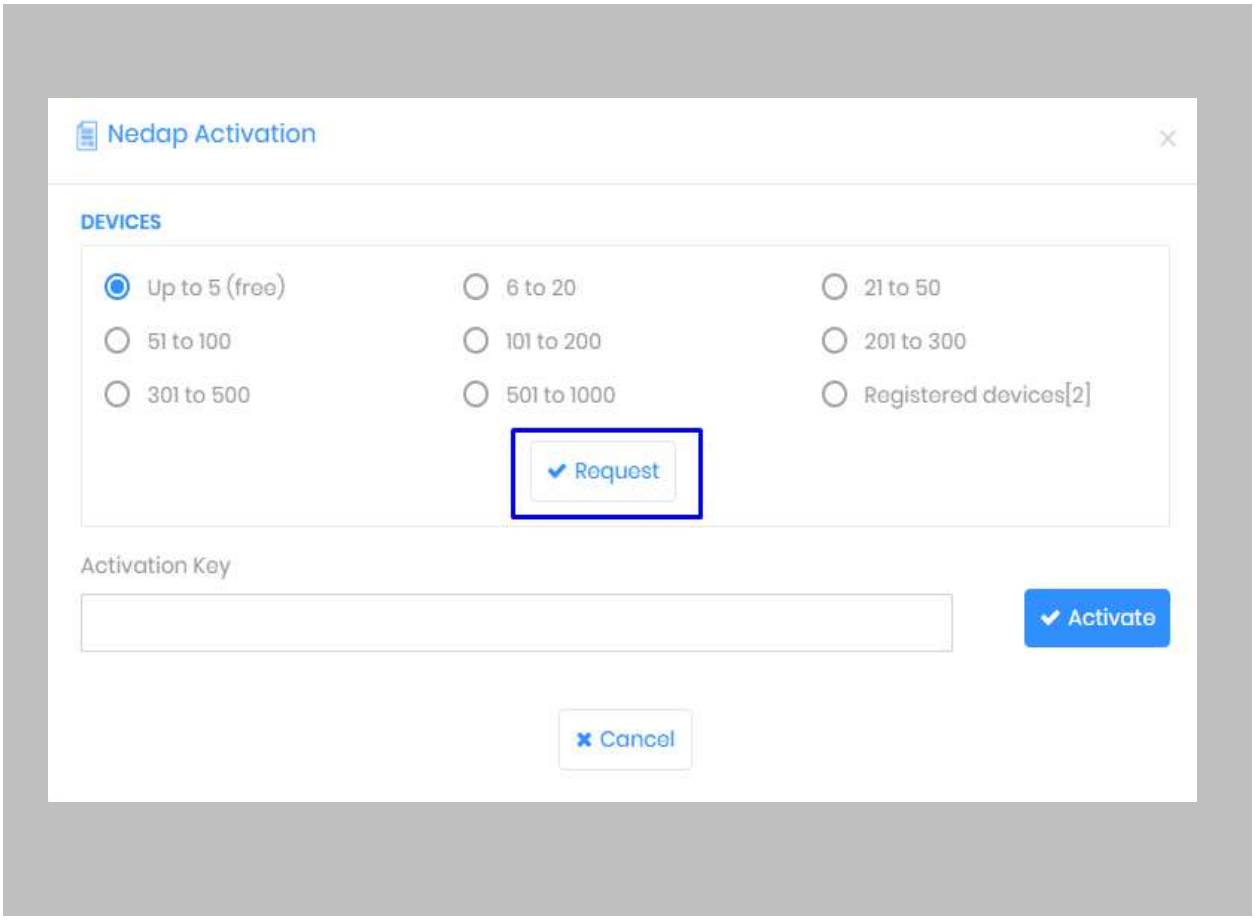


Figure 24: Nedap License Request

Note: The details screen will vary based on whether SMTP settings are configured in IXM WEB. If SMTP settings are not configured, a “Copy to Clipboard” icon will appear. When SMTP settings are configured, a “Send” button and a “Copy to Clipboard” button will appear.

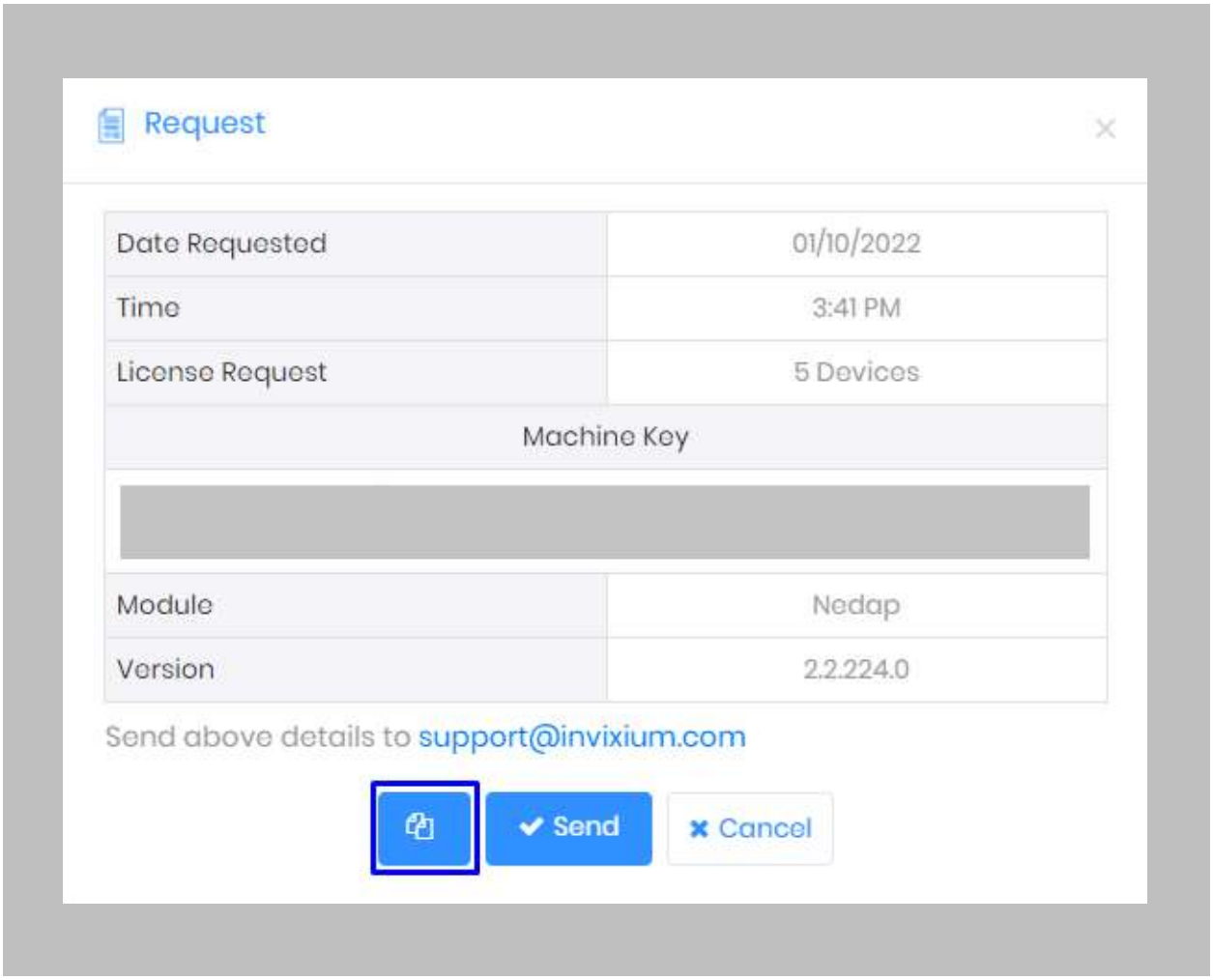
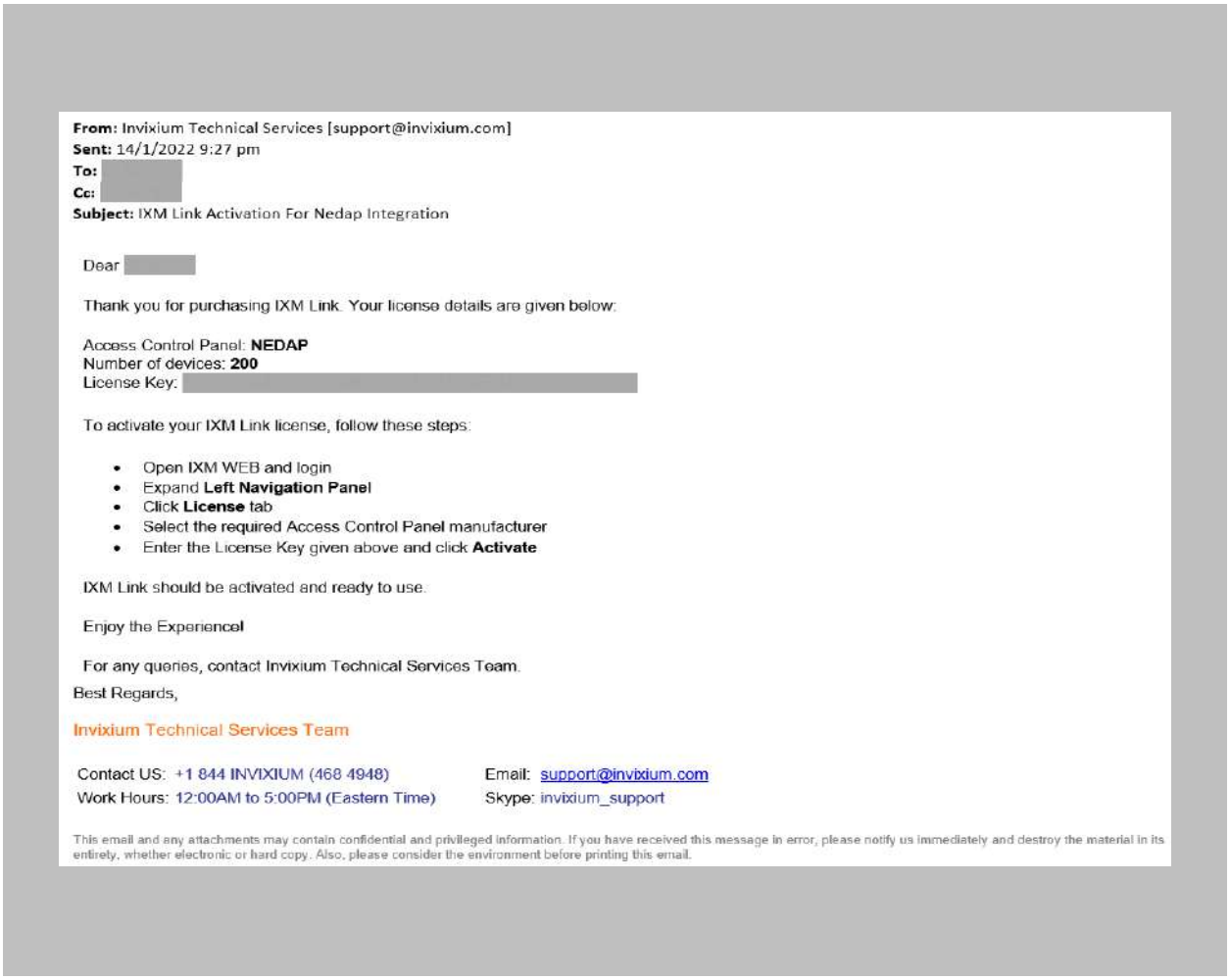


Figure 25: Nedap License

STEP 4

Click Copy to Clipboard and then paste the details in an email to **Invixium Support** to begin the licensing process

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:
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

Figure 26: Nedap AEOS License Key Email

STEP 5

Copy and **paste** the License Key into the Activation Key area in the IXM WEB Nedap AEOS Activation sectio, and then select **Activate**.

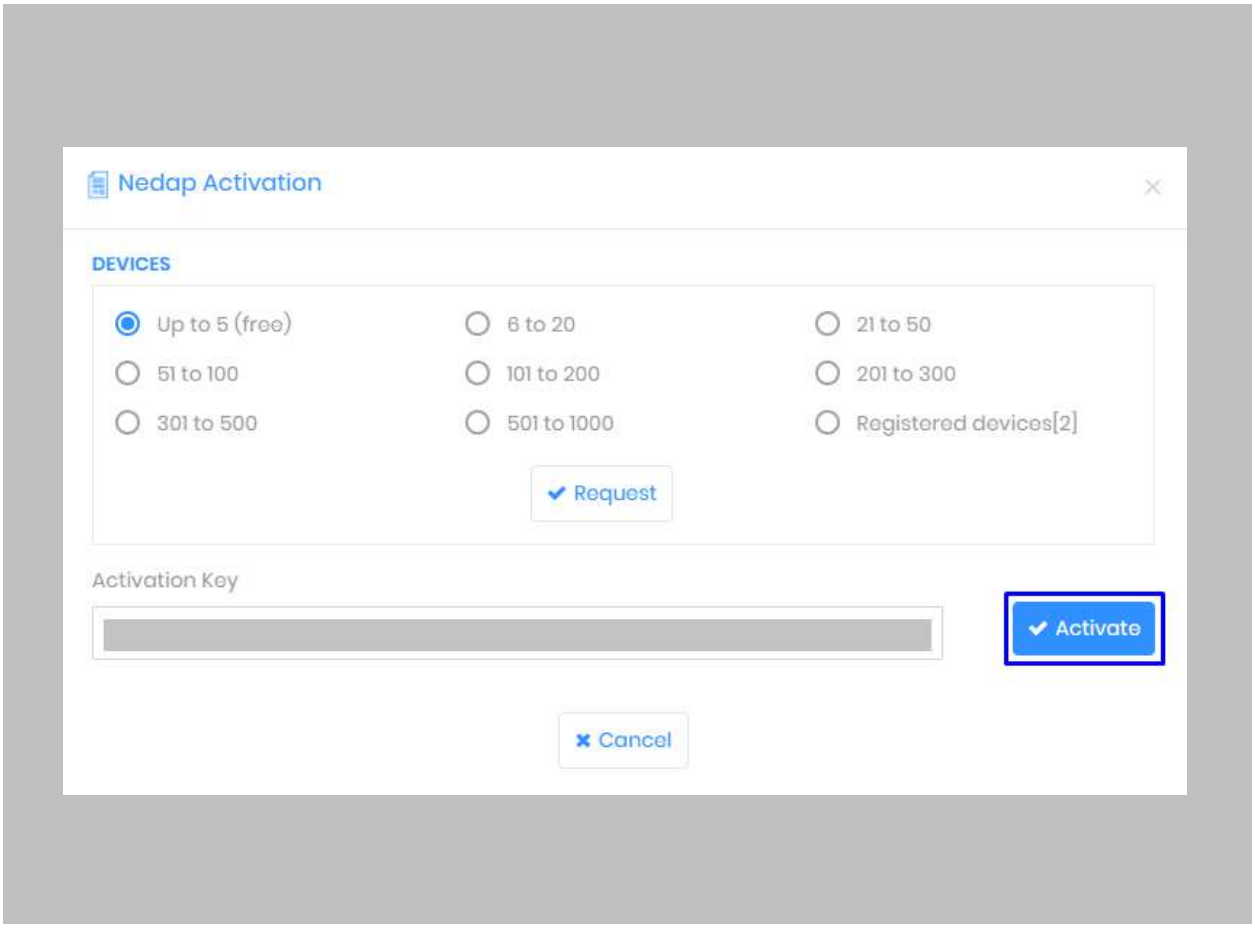


Figure 27: IXM WEB - Activate Nedap AEOS Link License

RESULT

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

9. Configuring IXM Link for Nedap AEOS

Procedure

STEP 1

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

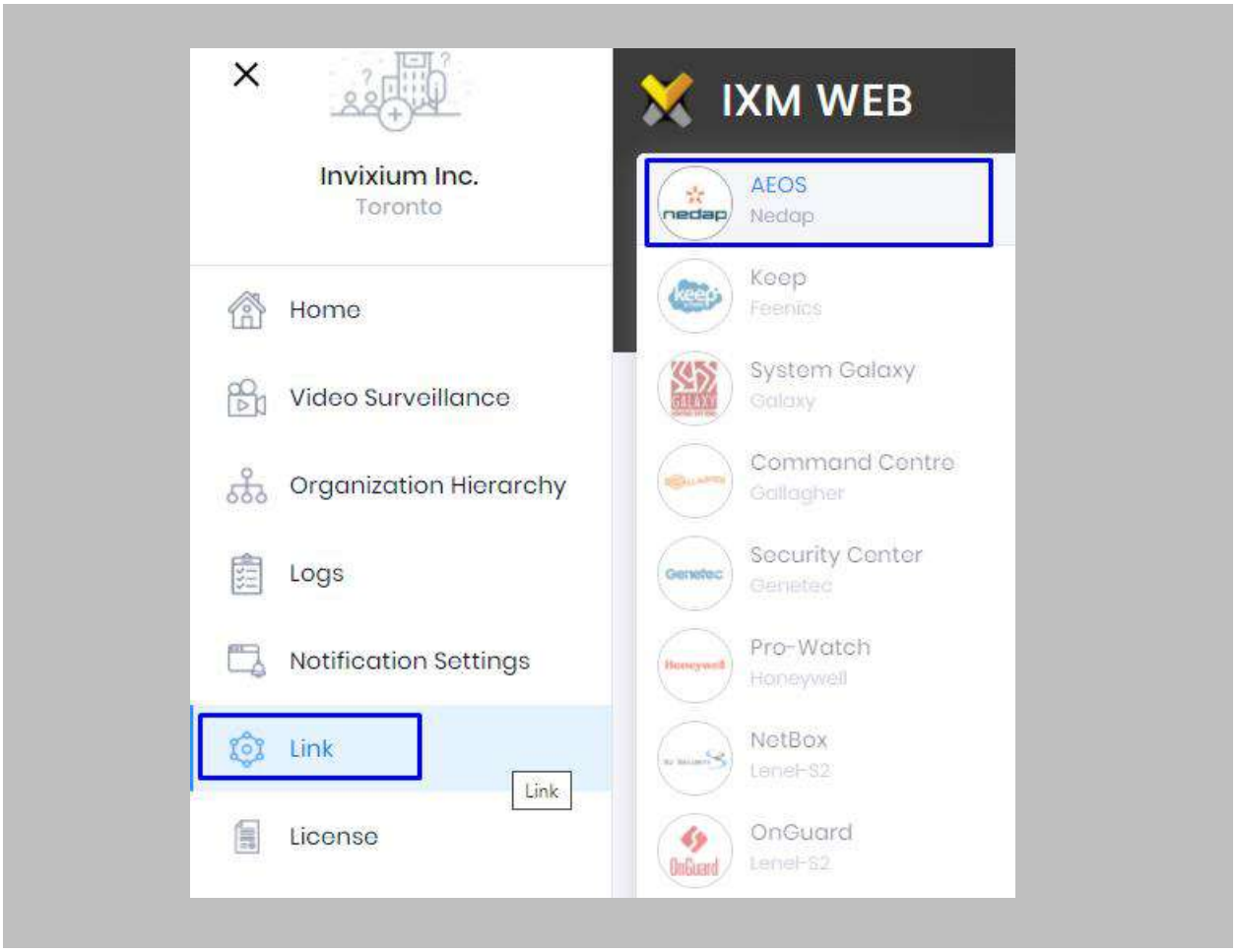


Figure 28: IXM WEB - Link Menu

STEP 2

Toggle the **Status** switch to enable.

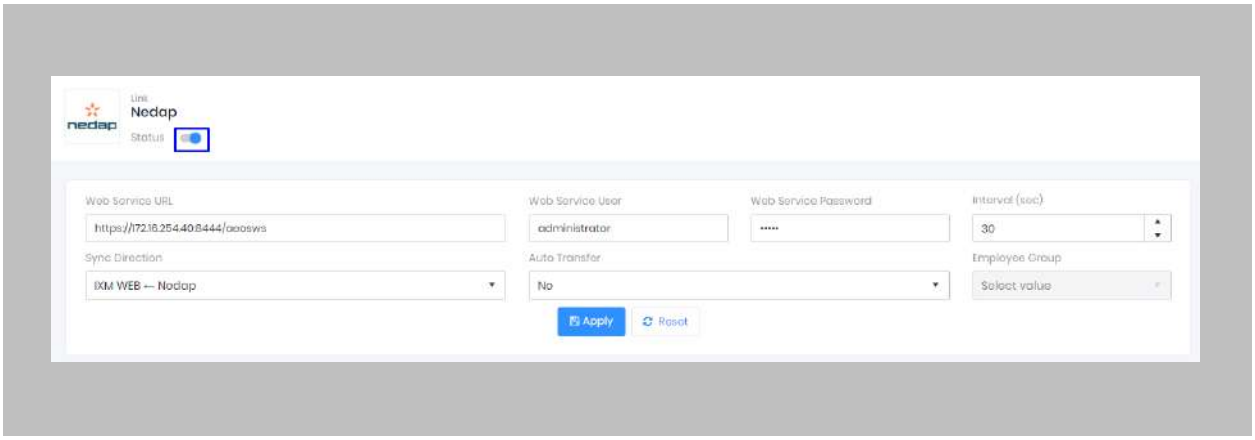


Figure 29: IXM WEB - Enable Nedap AEOS Link Module

STEP 3

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

STEP 4

Enter **Web Service Username** and **Web Service Password** for accessing the web service.

STEP 5

Specify in seconds how often **sync** should take place.

STEP 6

Select **Sync Direction.**

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

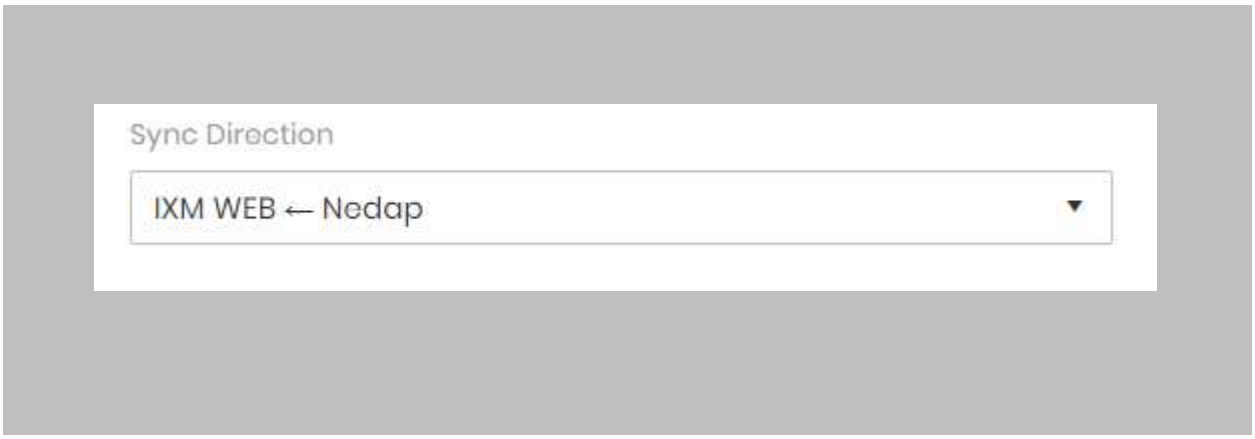


Figure 30: IXM WEB - Sync Direction

STEP 7

Auto Transfer

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

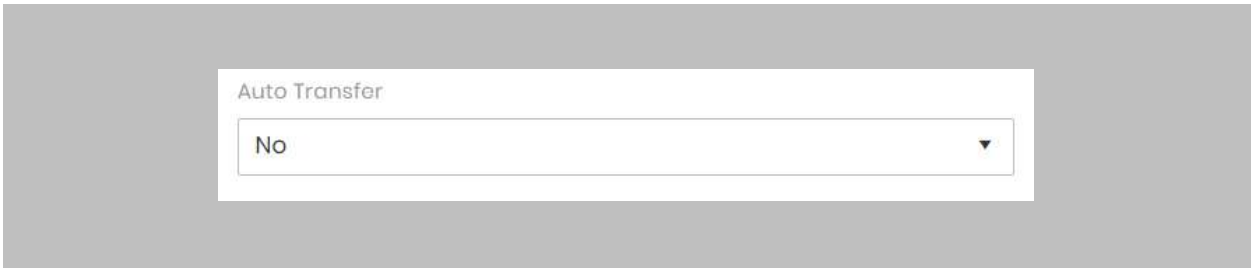


Figure 31: IXM WEB - Auto Transfer No

Yes: On selecting 'Yes' for Auto Transfer, an employee group selection dropdown enables which displays all the employee groups present in IXM WEB. All the employees synchronized from Nedap AEOS will be automatically added to the employee group selected on Link Configuration Page.

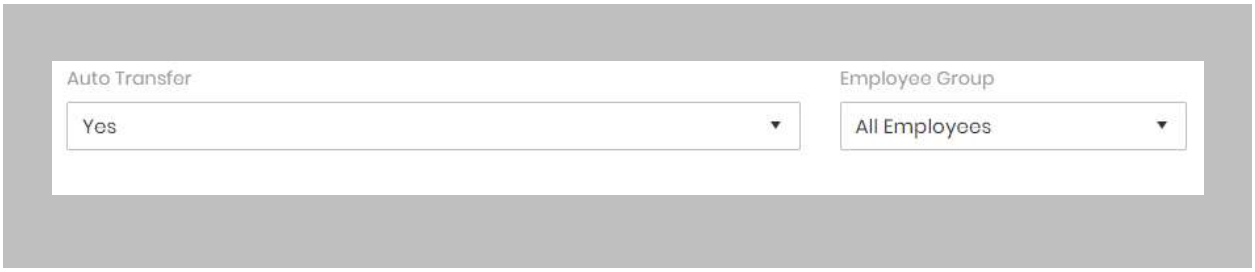


Figure 32: IXM WEB - Auto Transfer Yes

STEP 8

Click **Apply**

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

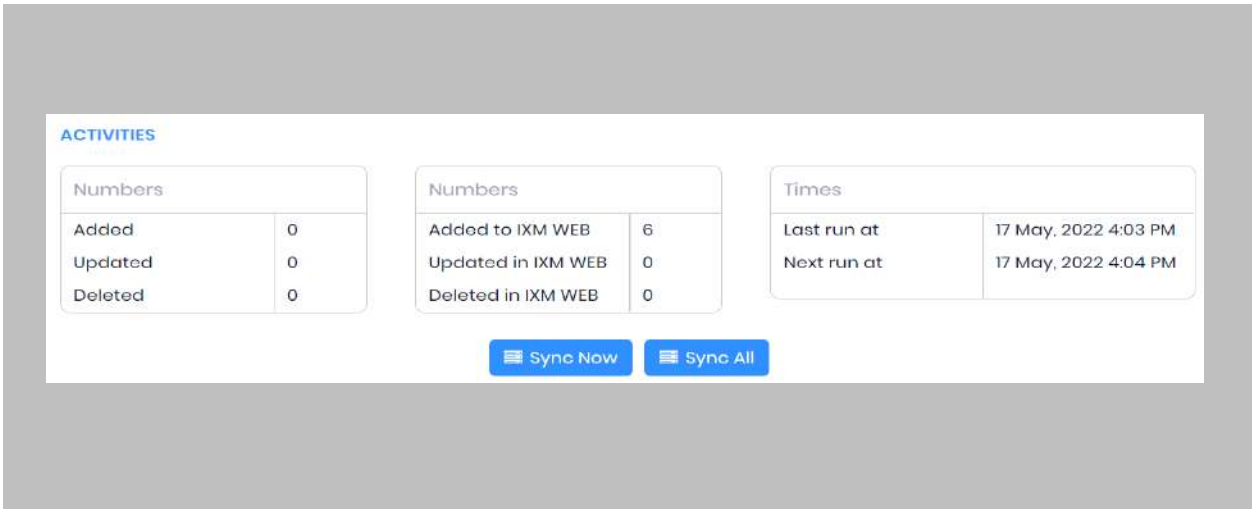


Figure 33: IXM WEB - Sync Activities

STEP 11

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 12

If sync direction is selected as Nedap AEOS to IXM WEB (One-way sync) then the **Sync All** button will get displayed.

STEP 13

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 GCC.

RESULT

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

10. Create System User(s) for Biometric Enrollment

Procedure

STEP 1

Log into IXM WEB.

On the home page, expand the **Left Navigation Pane** → **System**. The application will redirect to the System Users window.

Figure 34: IXM WEB - Create API User

STEP 2

Click **Add New**.

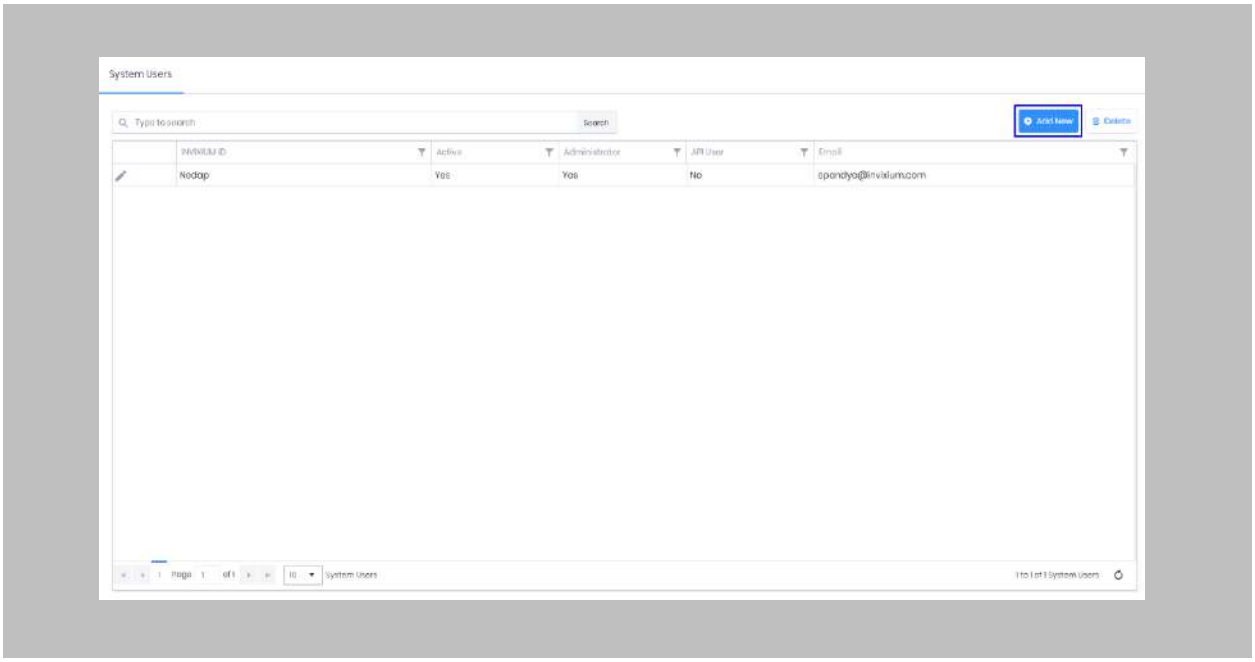


Figure 35: IXM WEB - Add New System User

Creating a system user requires the following details:

- Login Type
    i. Local employee
    ii. Domain employee
- Invixium ID (User ID) (For domain employee logins, User ID is automatically filled from AD)
- Password (For domain employee logins, password creation is not required)
- Confirm Password
- Email Address
- Status
- Permission for Modules

STEP 3

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

STEP 4

Enter **Invixium ID and Password** for API user.

STEP 5

Add an email address.

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

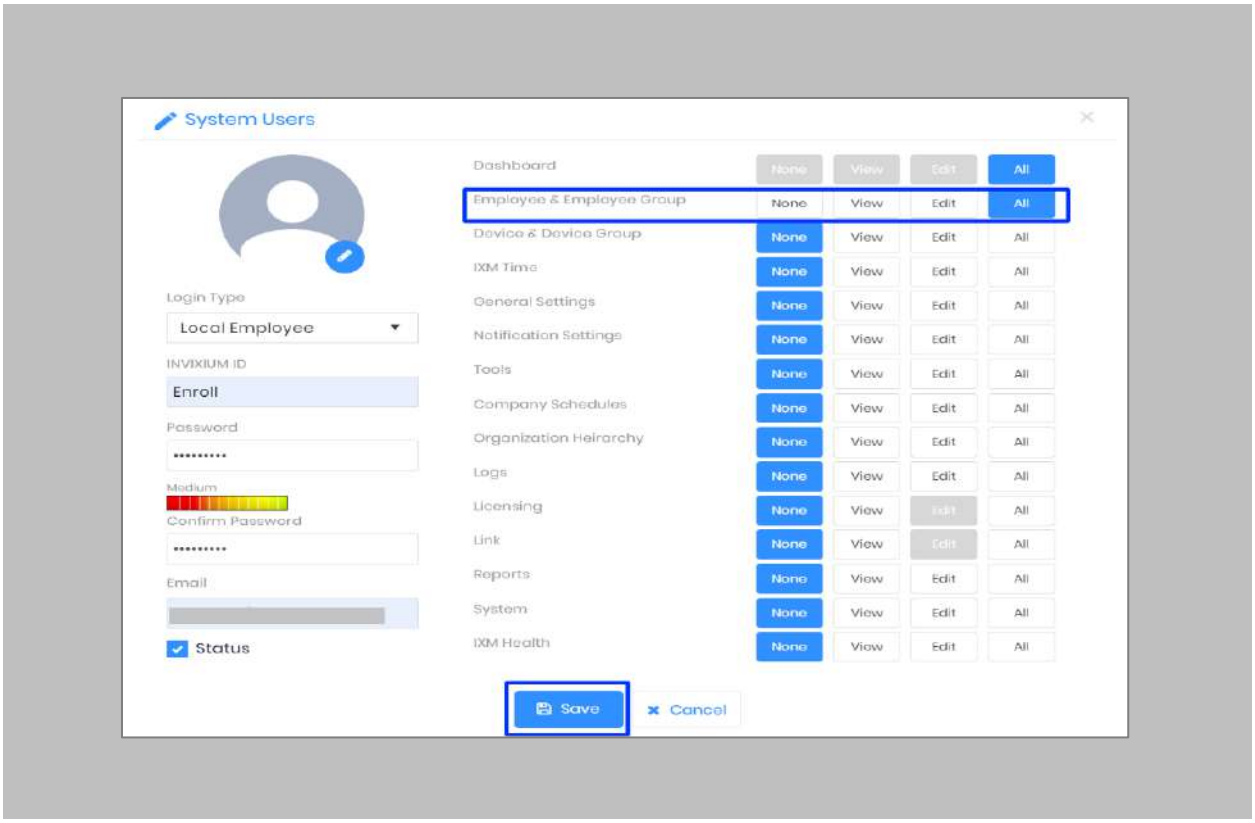


Figure 36: IXM WEB - New System User

STEP 6

Click **Save**.

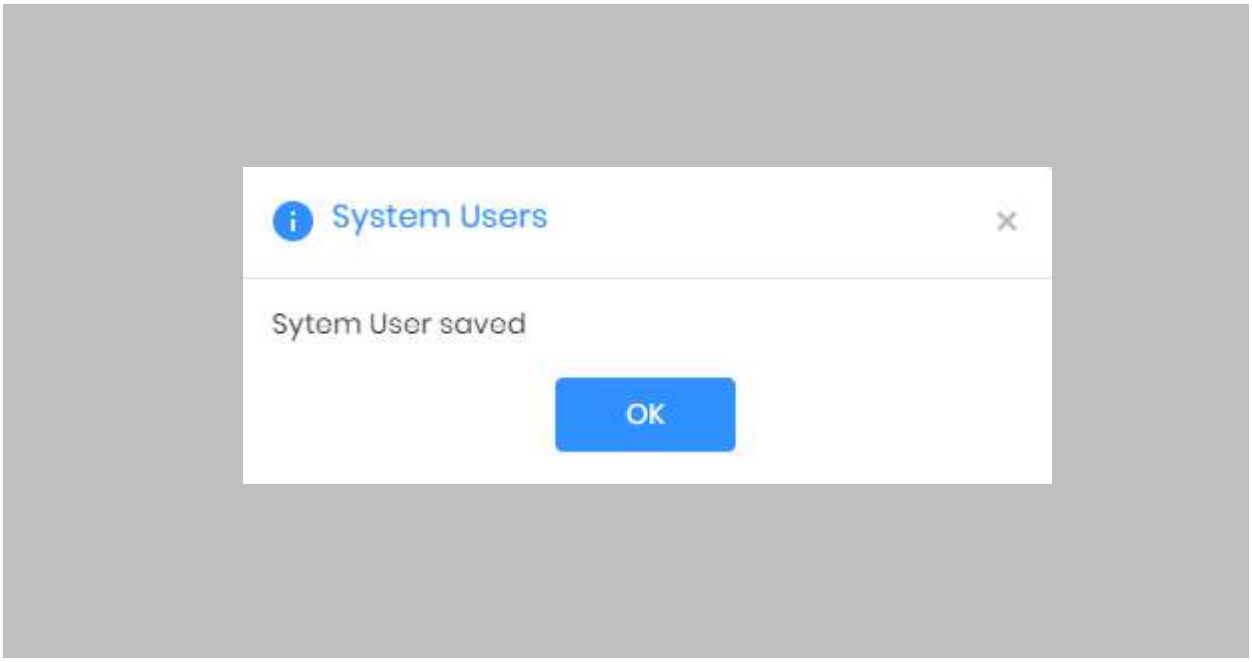


Figure 37: IXM WEB - Save System User

11. Add and Configure Invixium Readers

Adding an Invixium Reader in the IXM WEB application

Procedure

STEP 1

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

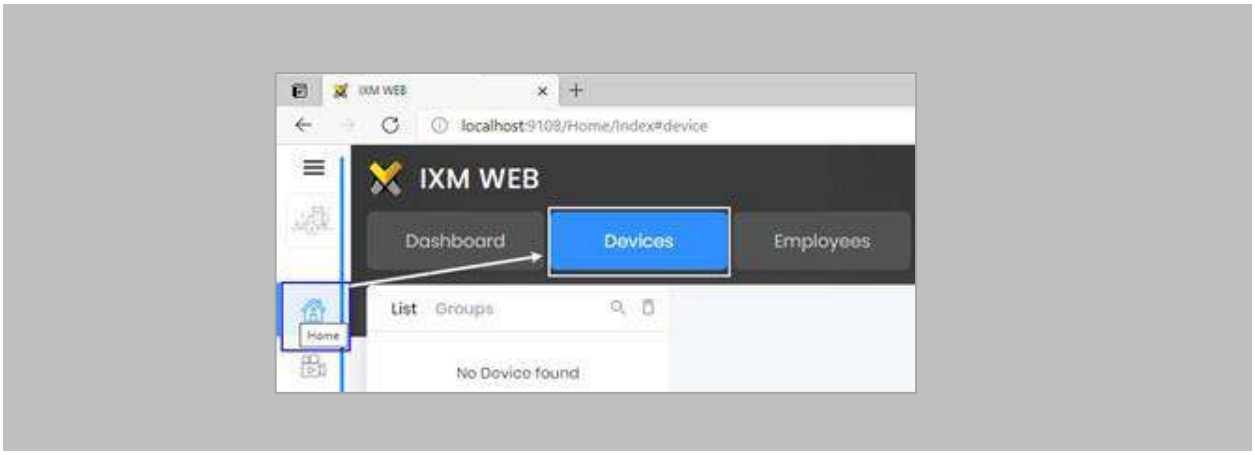


Figure 38: IXM WEB - Devices Tab

STEP 2

Select the **Add 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.

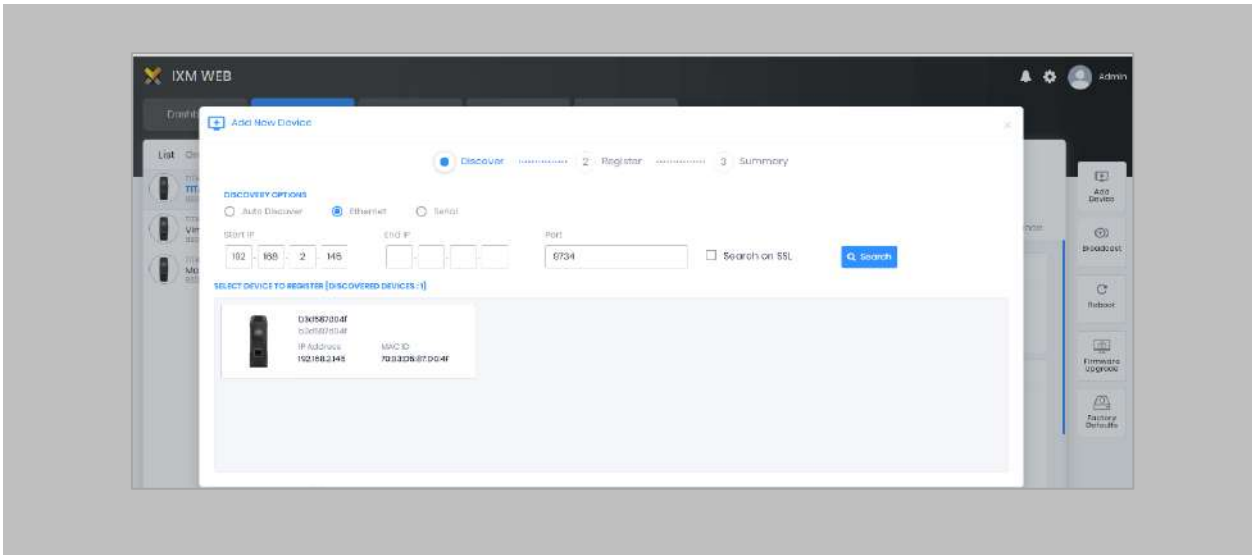


Figure 39: IXM WEB - Search Device using IP Address

STEP 3

Once the device is found, click on it. Enter following details:

- **Device Name:** Define the name of the **device** in IXM WEB.
- **Device Group:** Create a **'Default'** device group and select it.
- **Device Mode:** Select device mode as 'Entry', 'Exit', or 'Both' (Based on requirement).

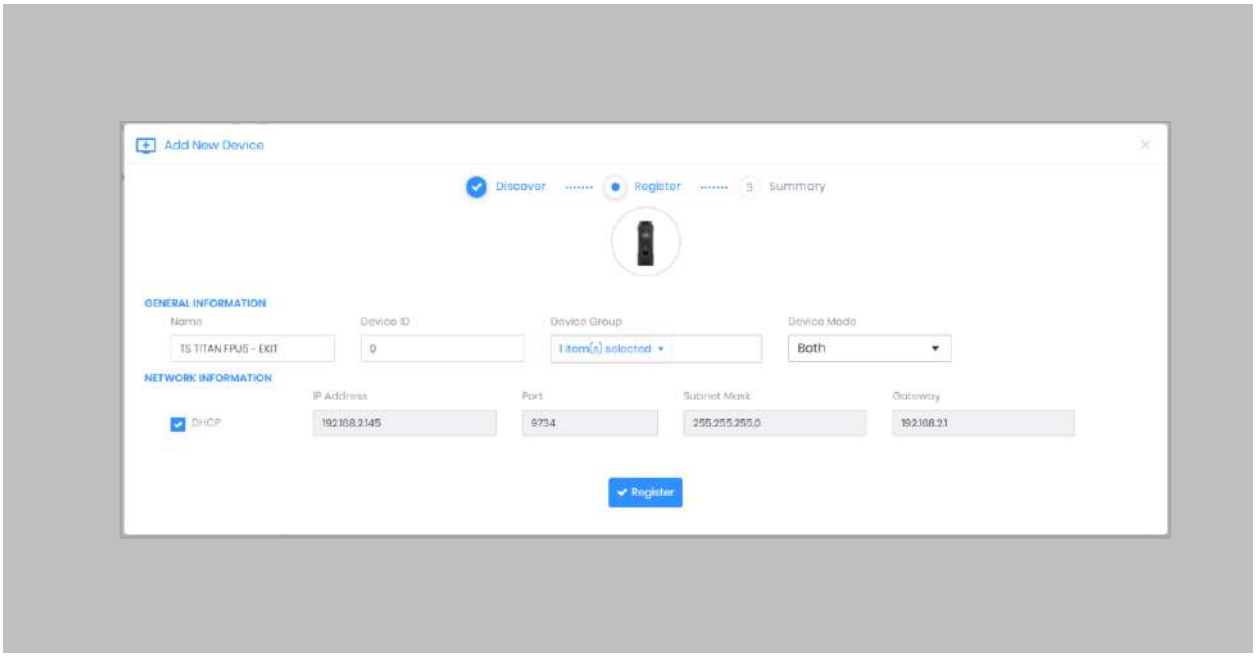


Figure 40: IXM WEB - Register Device

STEP 4

Click **Register**.

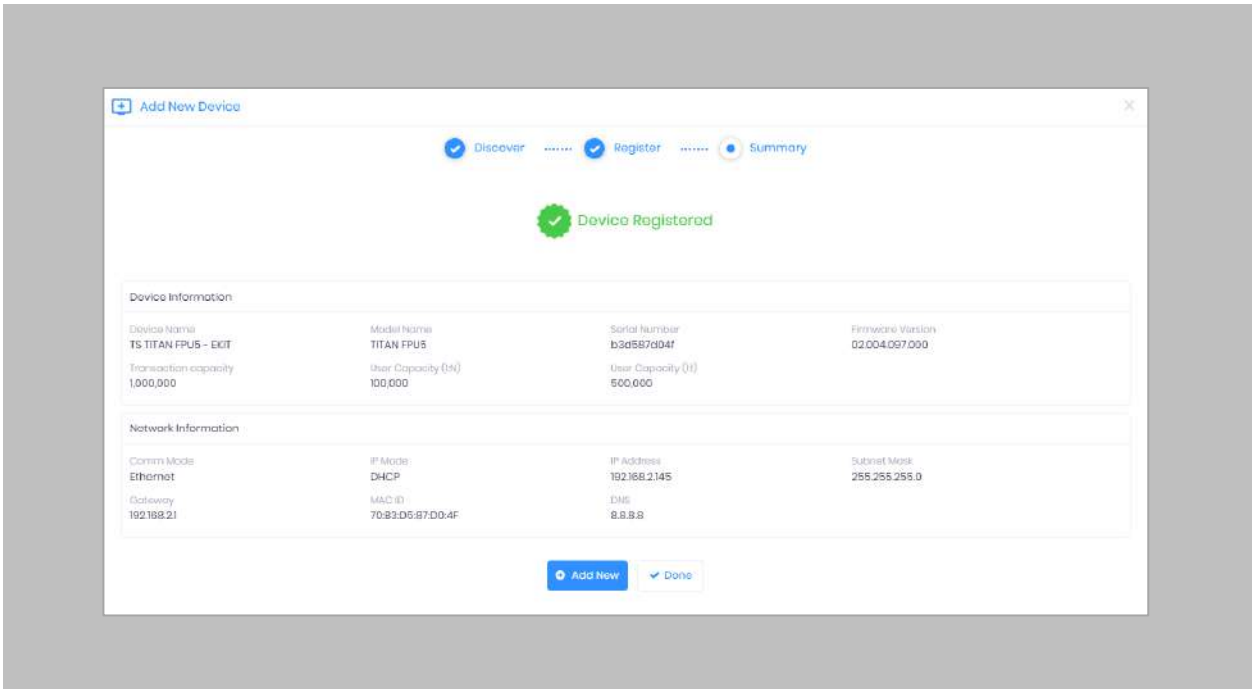


Figure 41: IXM WEB - Device Registration Complete

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

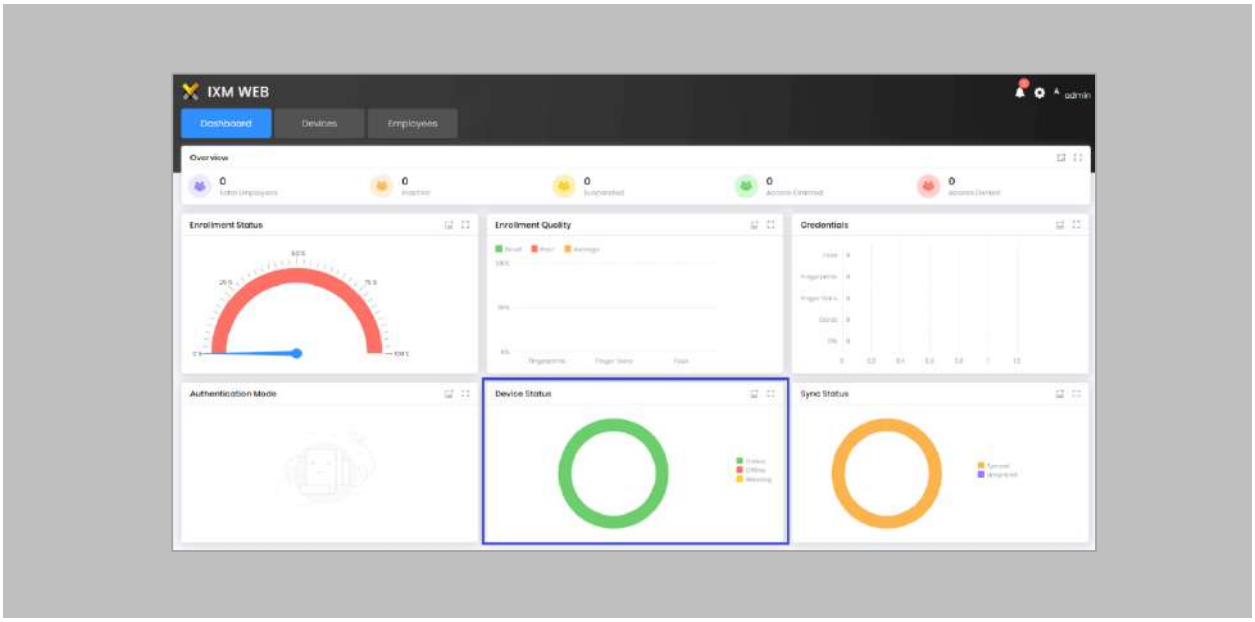


Figure 42: IXM WEB - Dashboard, Device Status

12. Adding an Invixium Device to a Device Group

Procedure

STEP 1

Go to **Devices** → **Groups**.

Add the device from the Right Side pane to the respective **Device Group.**

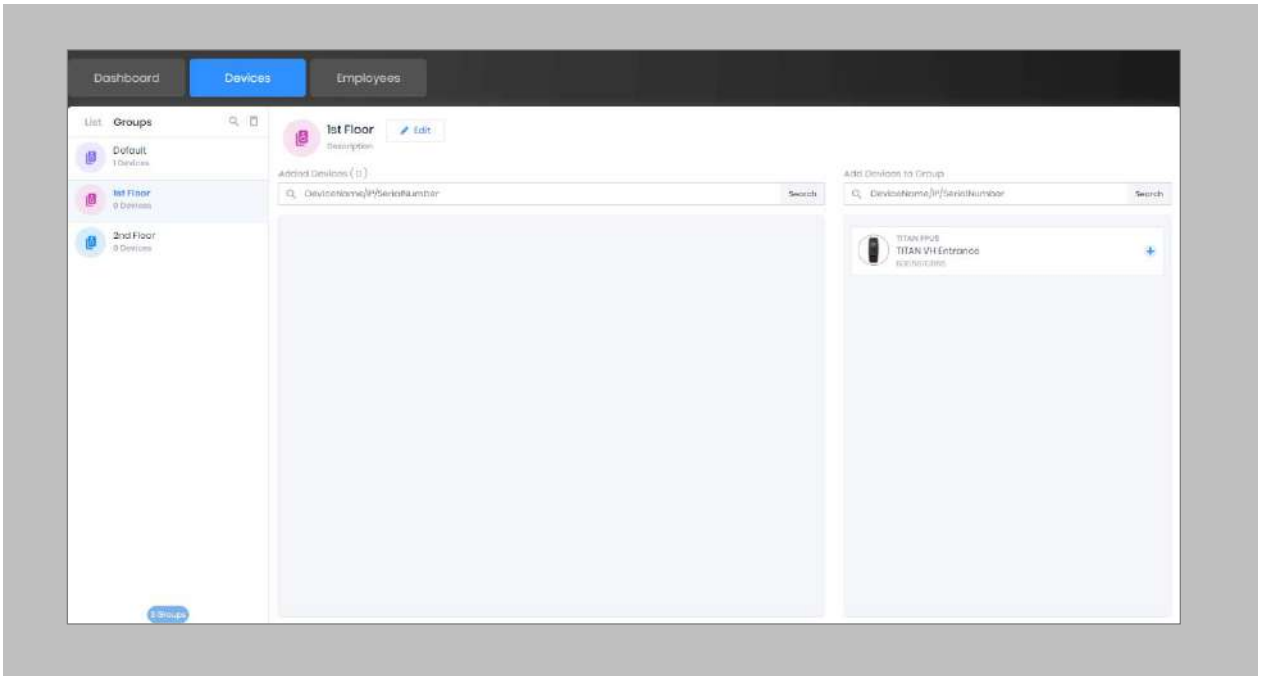


Figure 43: IXM WEB - Assign Device Group

Assign Wiegand to Invixium Readers

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

The Standard 26 Bit Wiegand will be used to define which output format will be sent to Nedap AEOS.

STEP 1

From **Home** > click the **Devices** tab. Select any device.

STEP 2

Navigate to the **Access Control** tab.

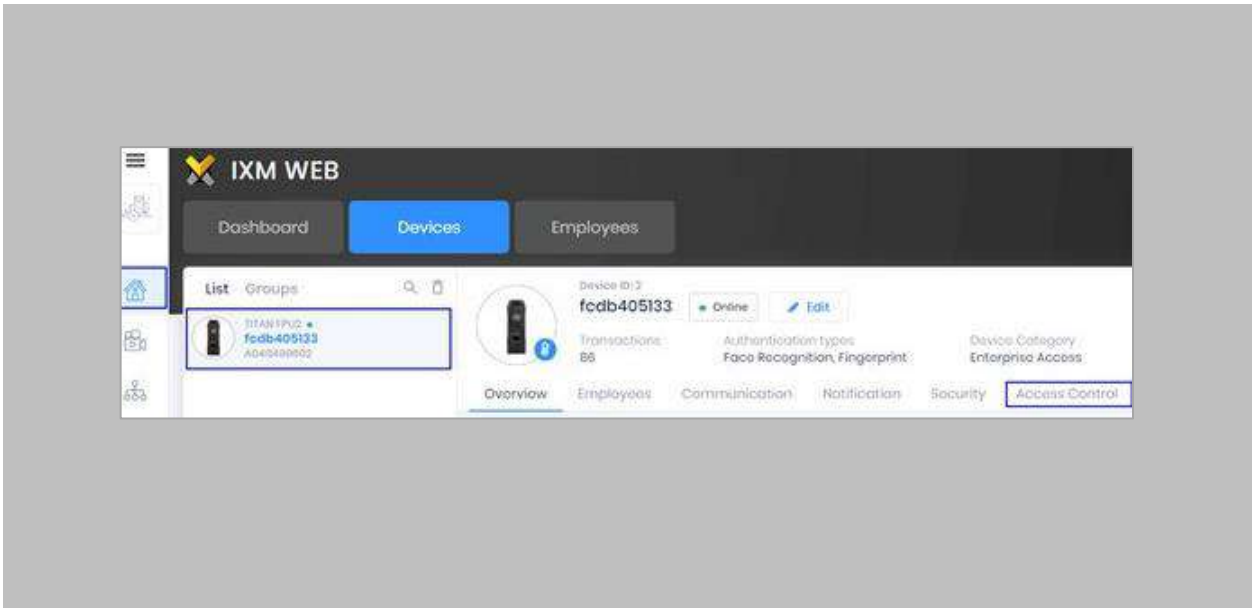


Figure 44: IXM WEB - Navigate to Access Control Tab

STEP 3

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

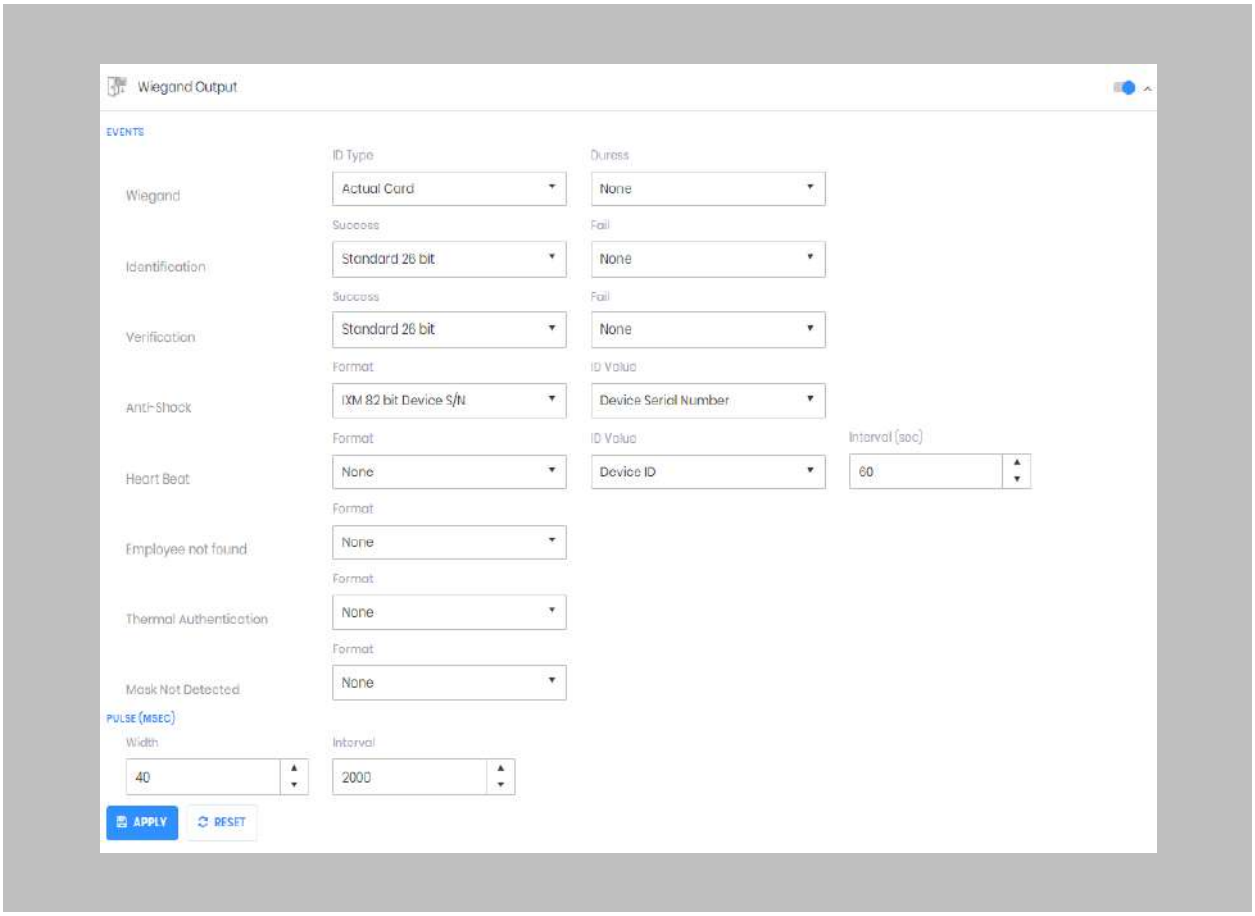


Figure 45: IXM WEB - Wiegand Output

The ID types for Wiegand output are as follows:

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

By default, Employee ID is selected in Wiegand Event.

As the Employee ID field is not available in Nedap AEOS, select either Default Card or Actual Card.

Actual Card: when more than one card is assigned to a 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 default in IXM WEB.

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

STEP 4

Set the **items**:

Wiegand	Actual Card
Identification	26 - bit
Verification	26 - bit

STEP 5

Click **Apply.**

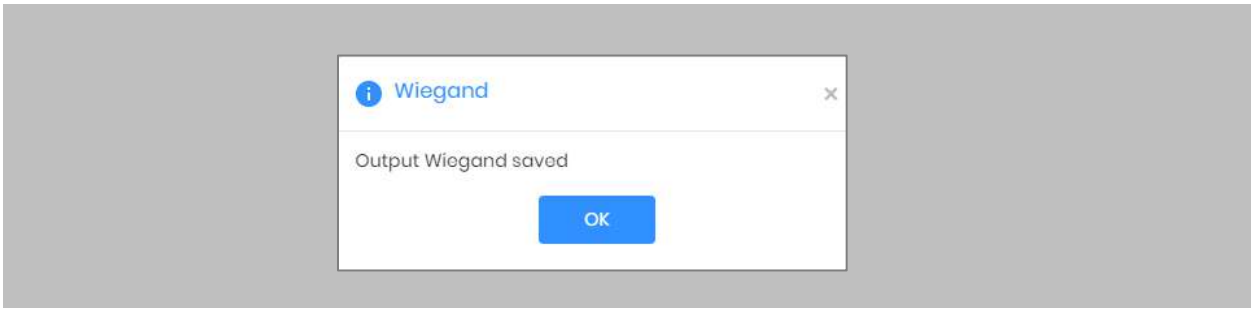


Figure 46: IXM WEB - Save Output Wiegand

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 for more information.
- If a 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 Nedap Panel.

Configuring Panel Feedback with Nedap

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

Connect the **Green** of the Nedap 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**.

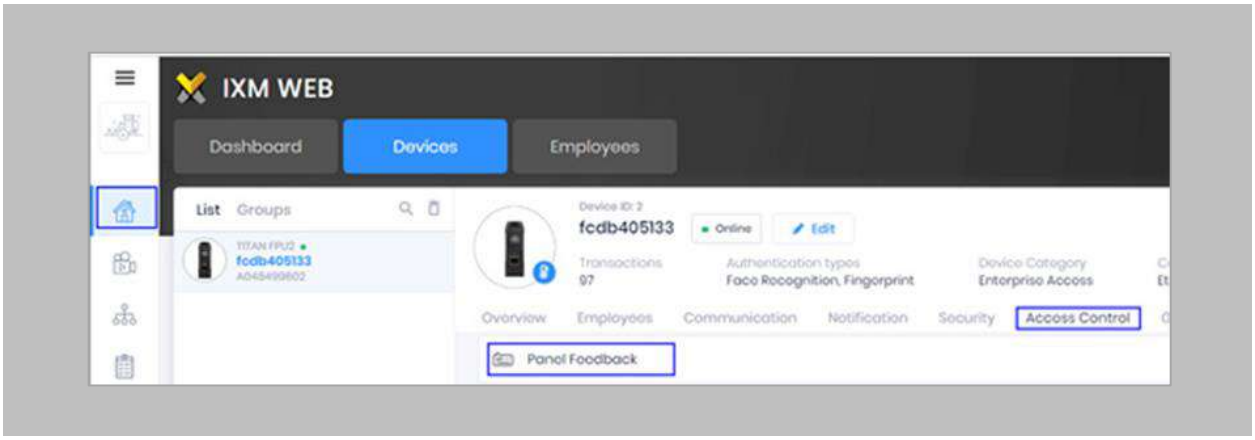


Figure 47: IXM WEB - Panel Feedback

STEP 4

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

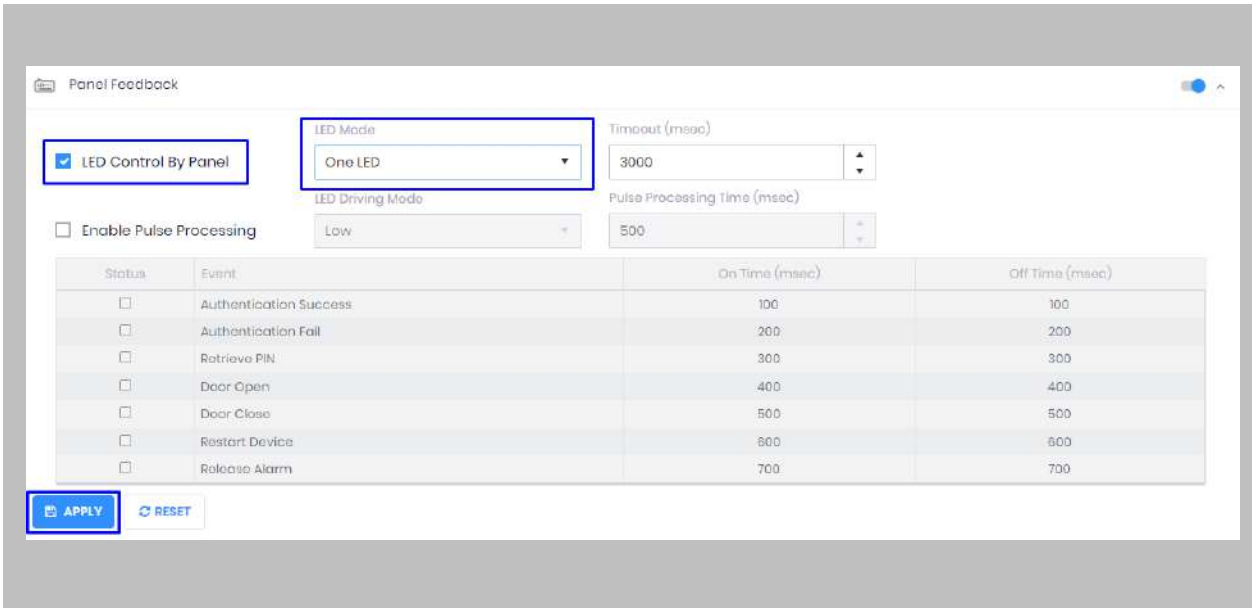


Figure 48: IXM WEB - Configuring Panel Feedback in IXM WEB

STEP 5

Click **Apply**.

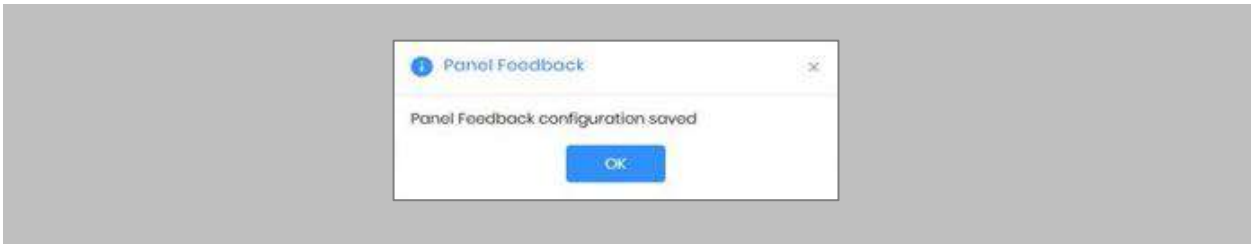


Figure 49: IXM WEB - Save Panel Feedback

Pre-configuration for enrollment Procedure

STEP 1

Host **IXM WEB** on https. A certification 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 SSL certificate.

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

STEP 3

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

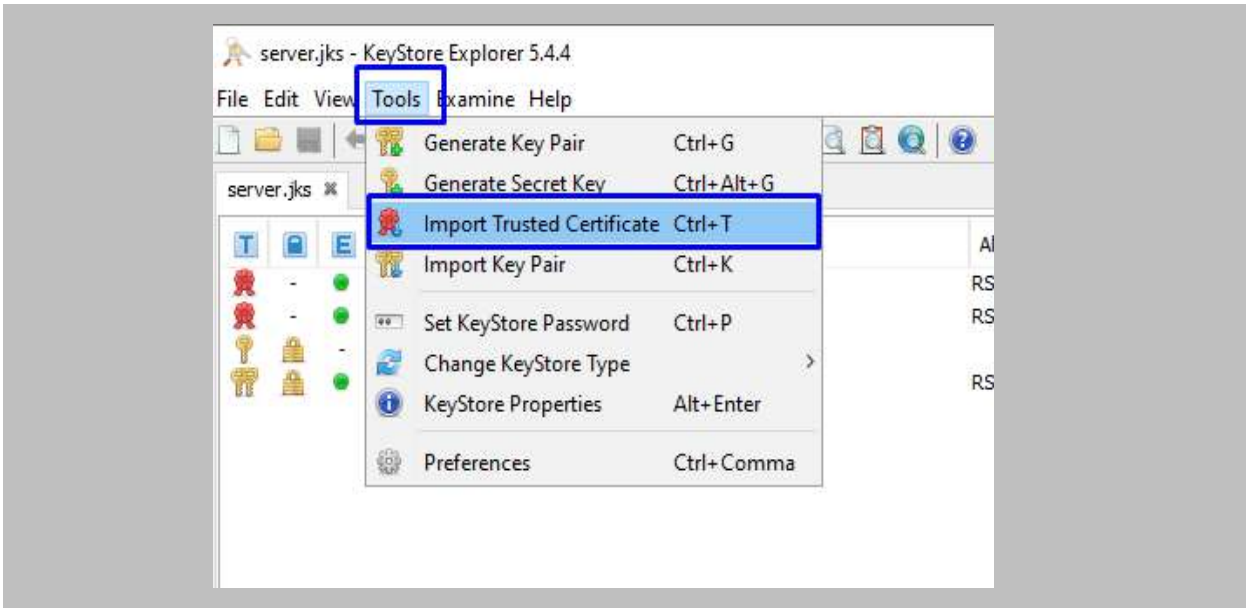


Figure 50: AEOS- Import Trusted Certificate

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:

STEP 7

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

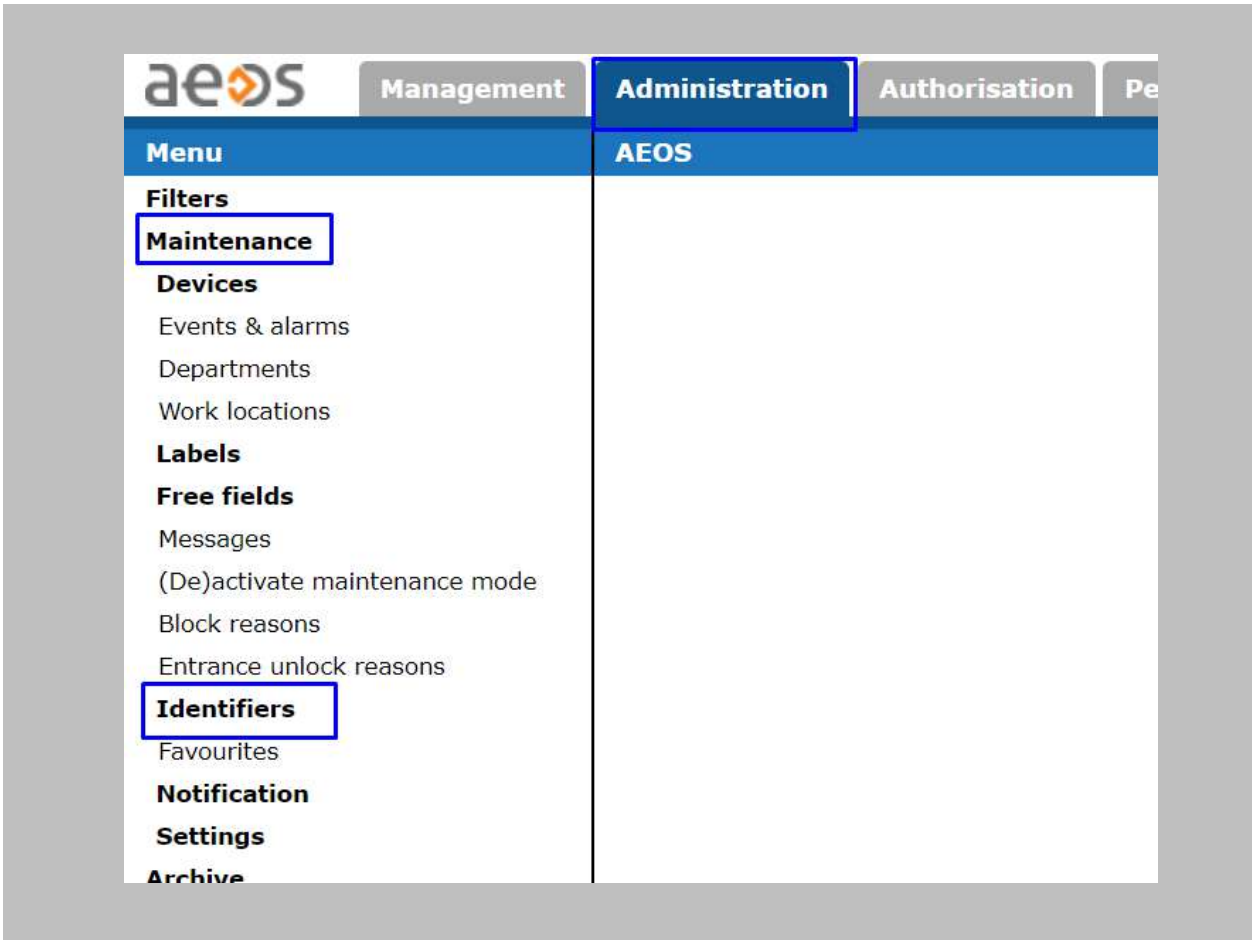


Figure 51: AEOS - Identifiers

STEP 8

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

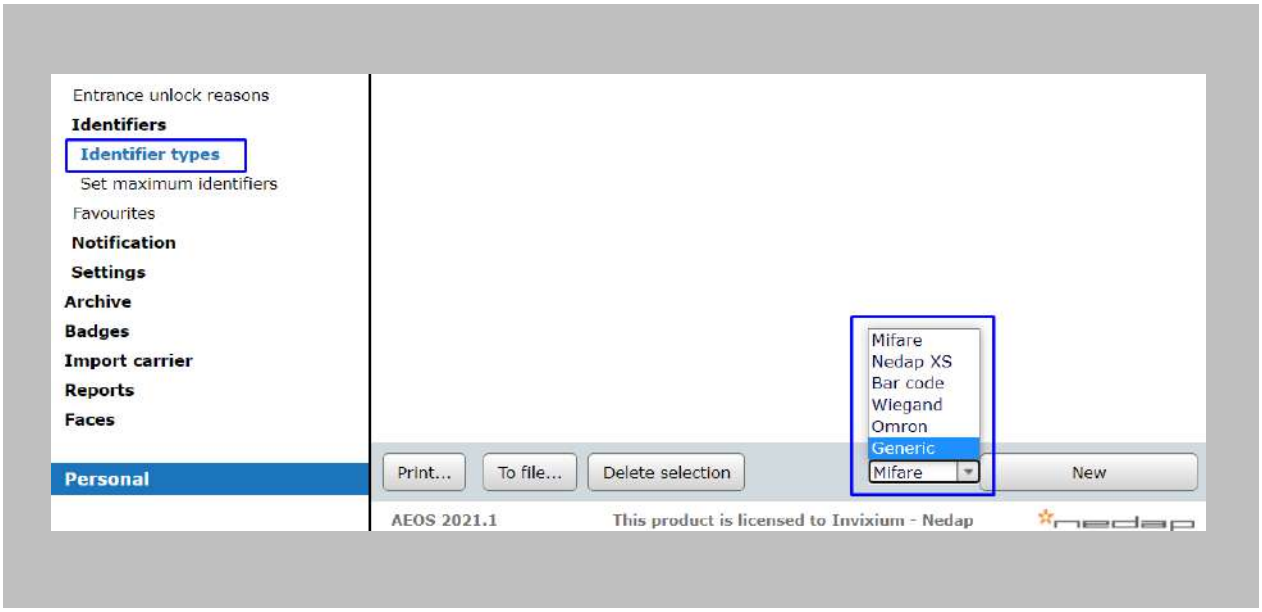


Figure 52: AEOS - Identifier Type Selection

Click on **New.**

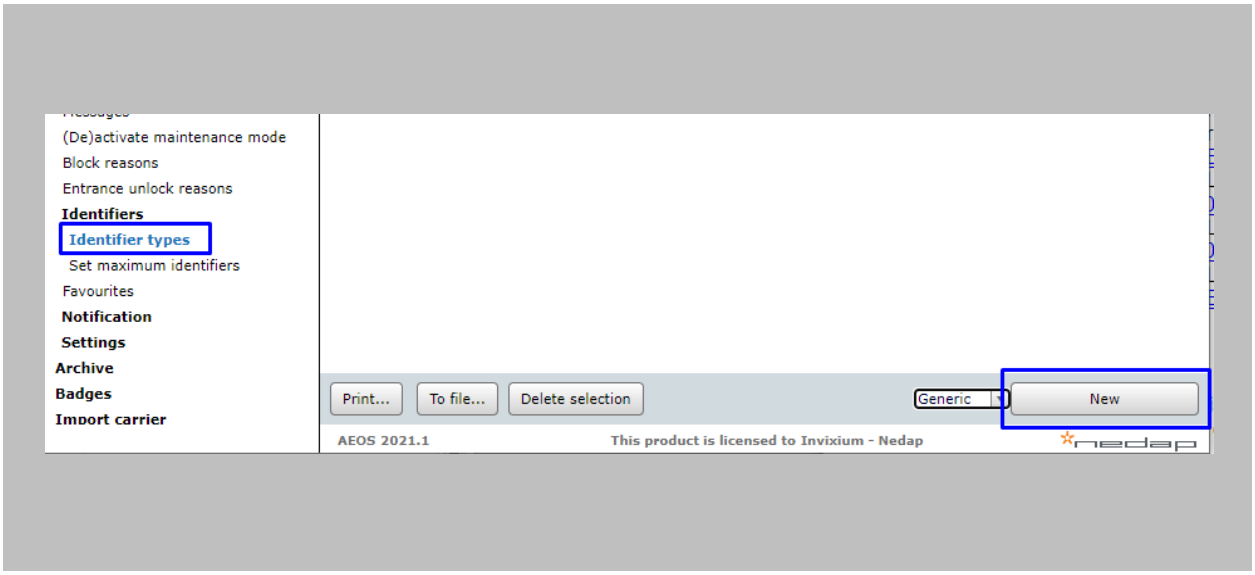


Figure 53: AEOS - Add New Identifier Type

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 54: AEOS - New Identifier Type

STEP 10

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

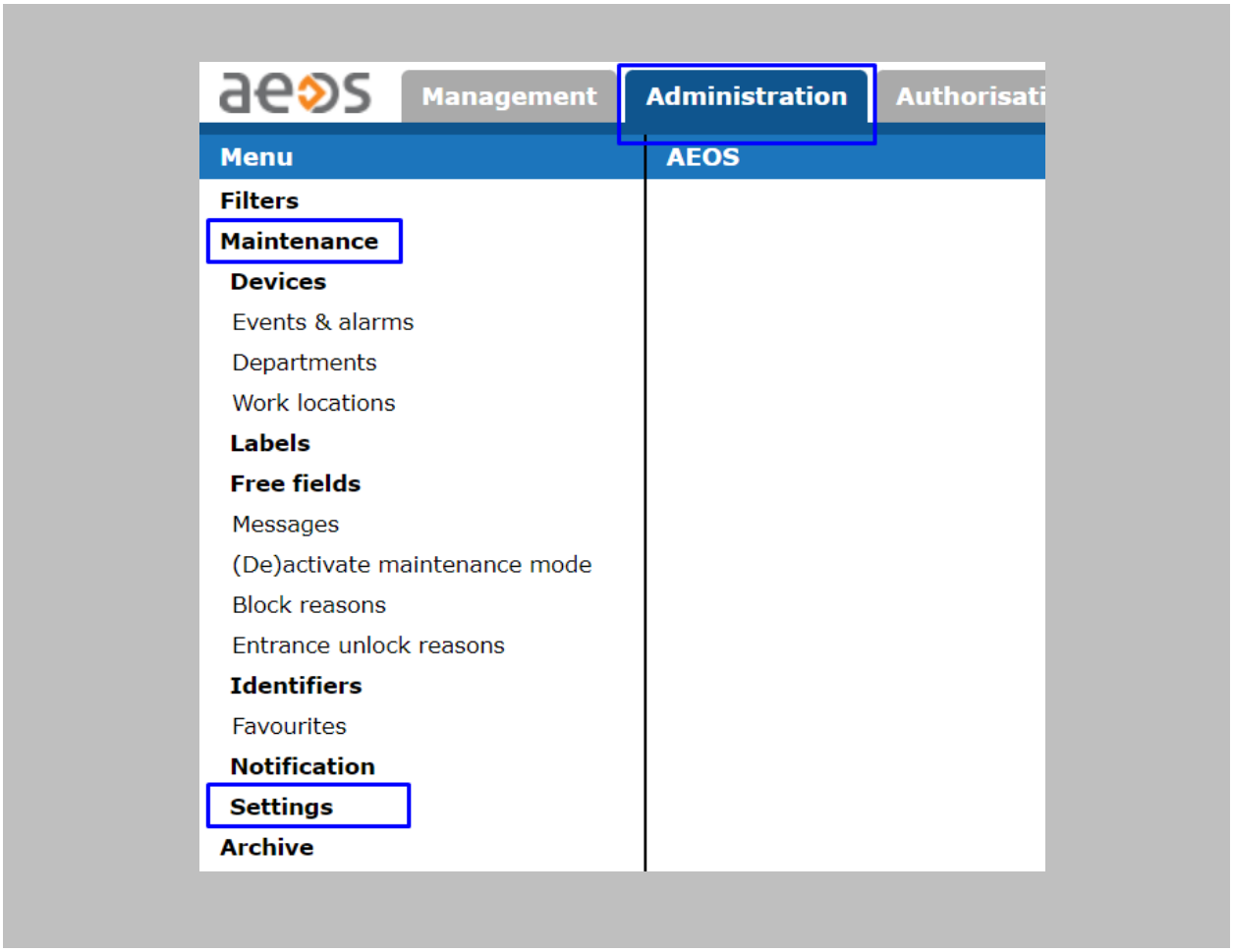


Figure 55: AEOS- Settings

STEP 11

Click on **System Properties.**

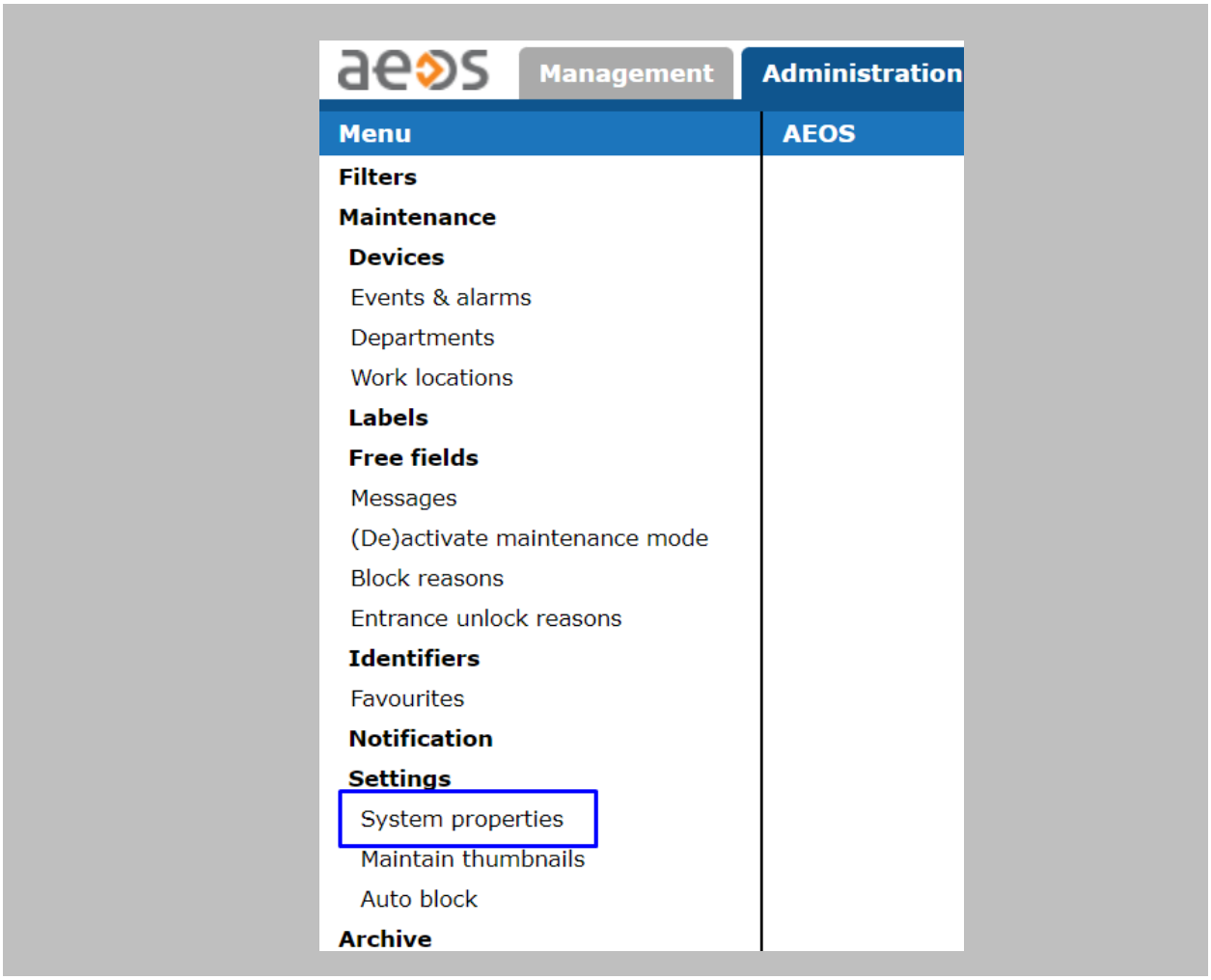


Figure 56: AEOS - System Properties

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'**.

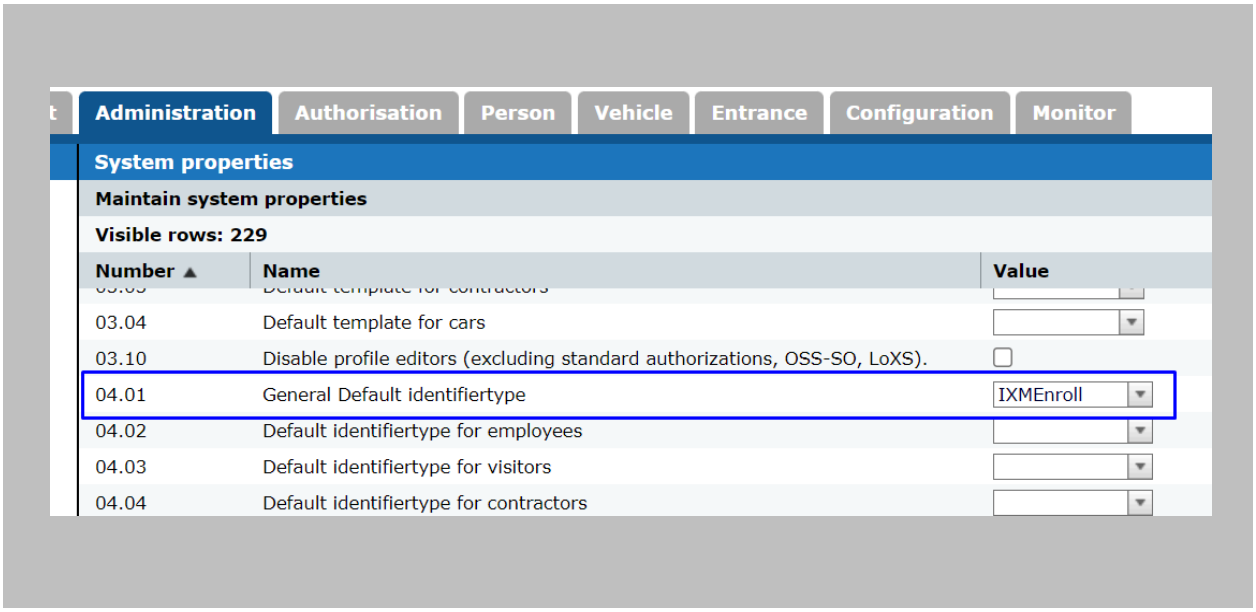


Figure 57: AEOS - System Properties Default Identifier

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

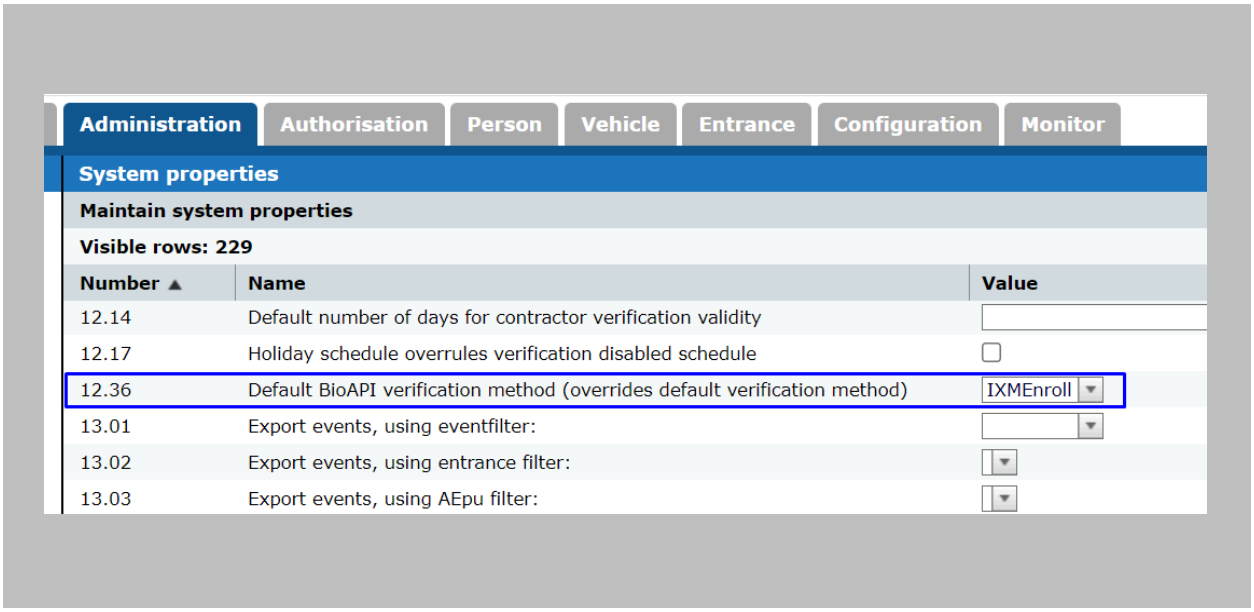


Figure 58: AEOS - System Properties Default BioAPI Verification

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

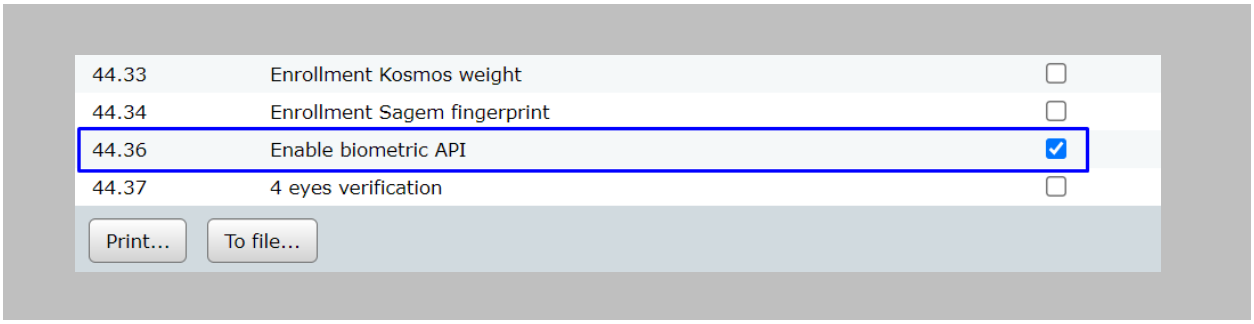


Figure 59: AEOS - System Properties Enable Biometric API

Click on **OK.**

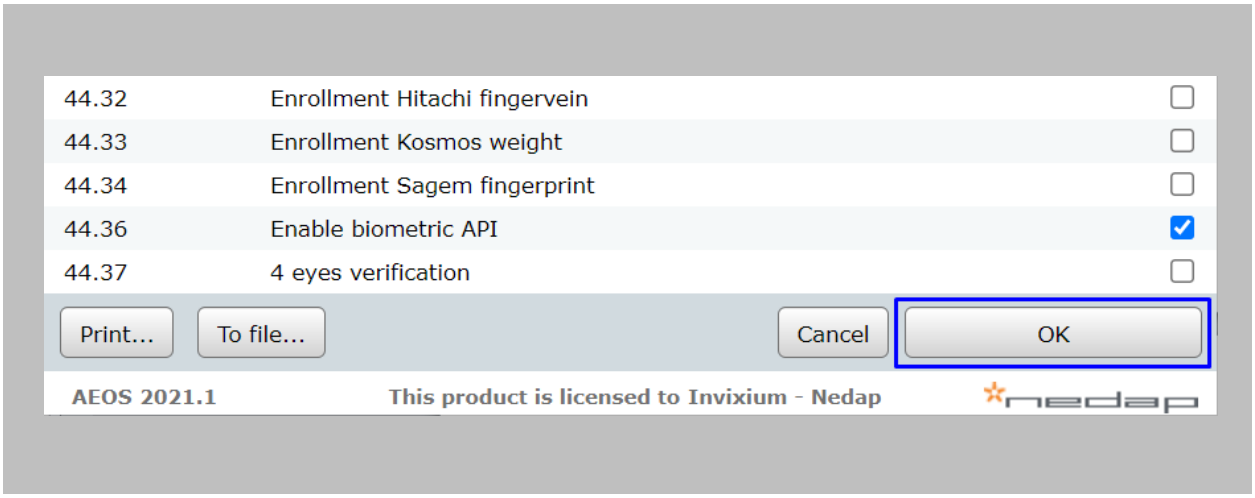


Figure 60: AEOS - Save System Properties

STEP 13

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

RESULT

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

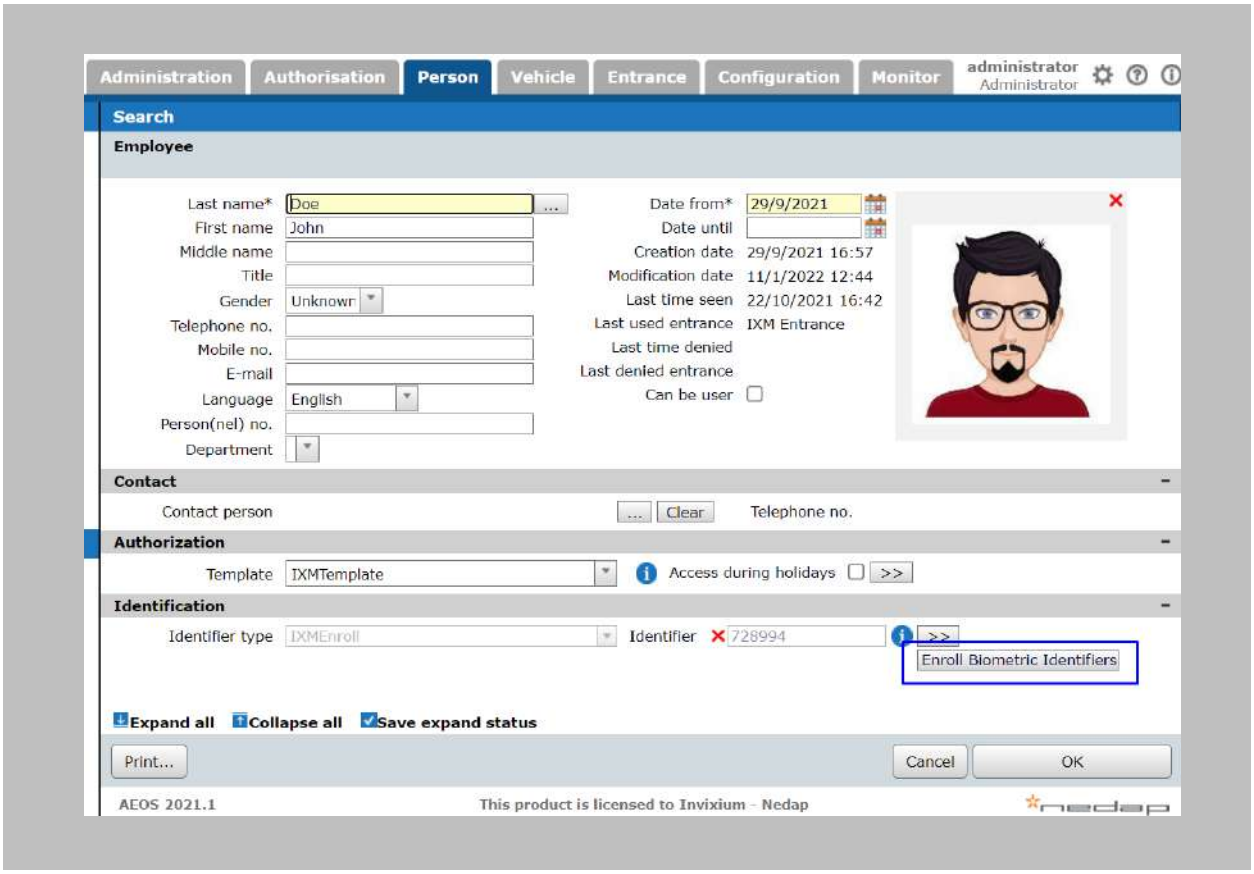


Figure 61: AEOS - Enroll Button

13. 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.

Procedure

STEP 1

Open the **AEOS** application →Select employee/visitor and click on the **'Enroll Biometric Identifiers'** button →Perform enrollment from this view.

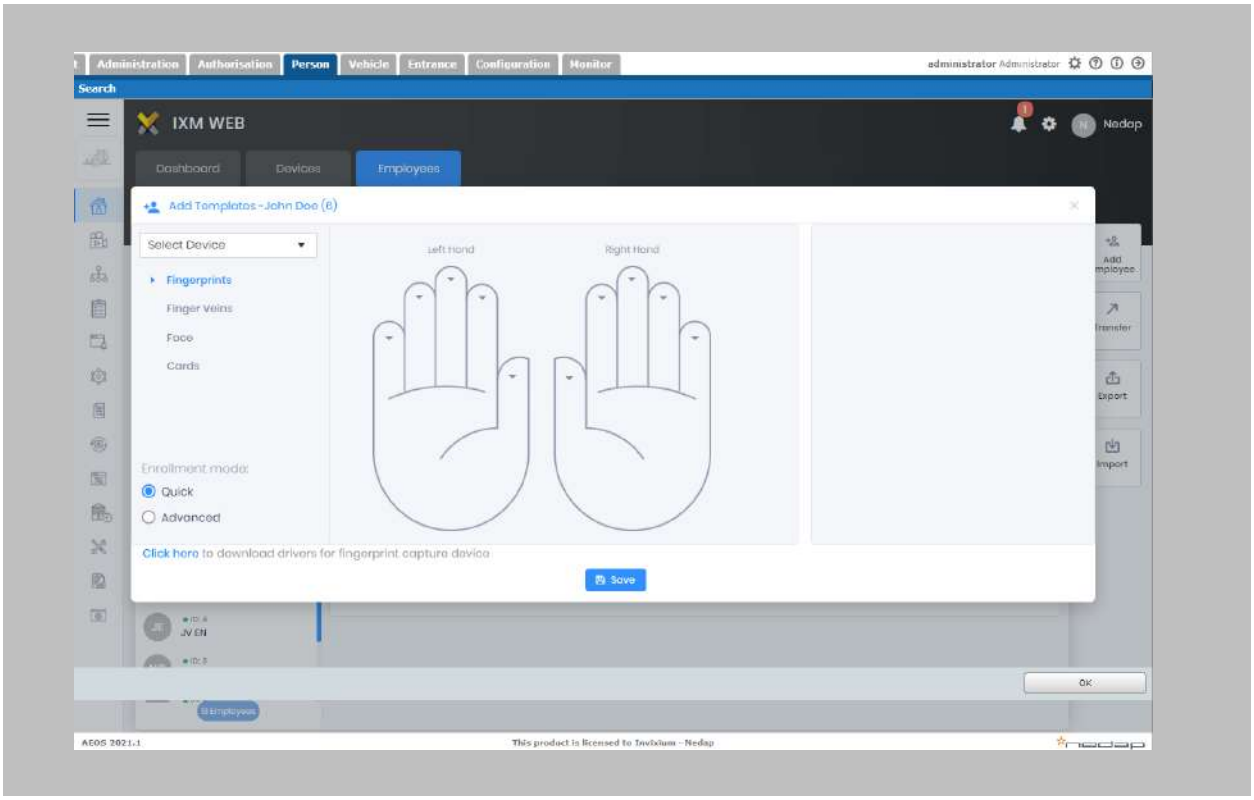


Figure 62: AEOS - Biometric Enrollment

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

14. 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.

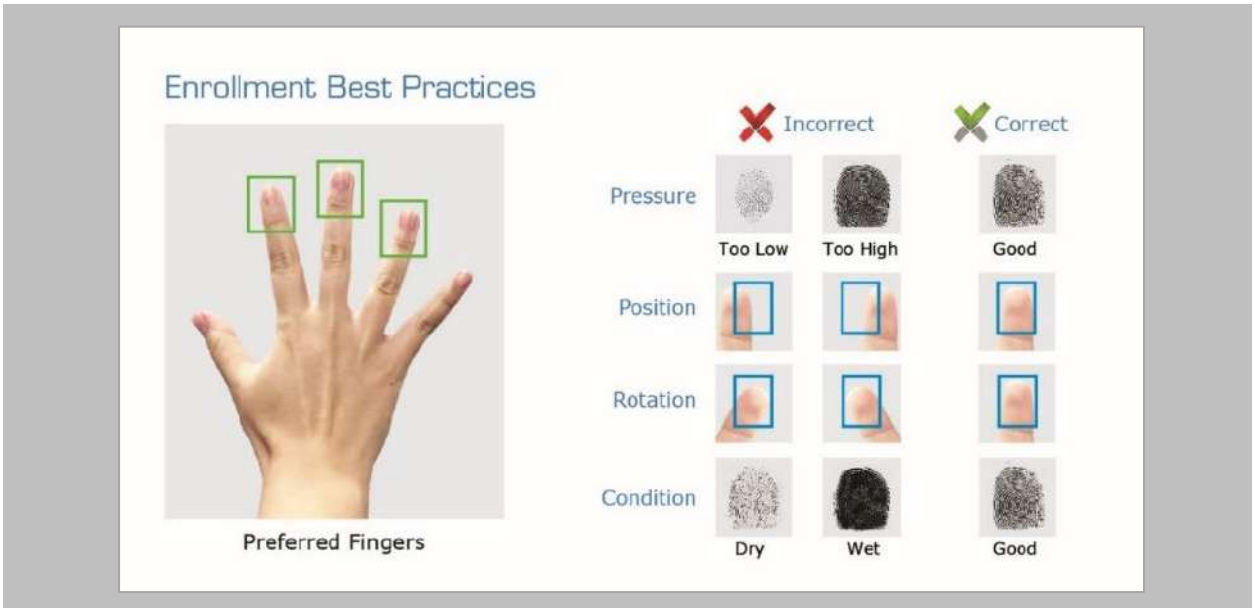


Figure 63: Fingerprint Enrollment Best Practices

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 64: 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.

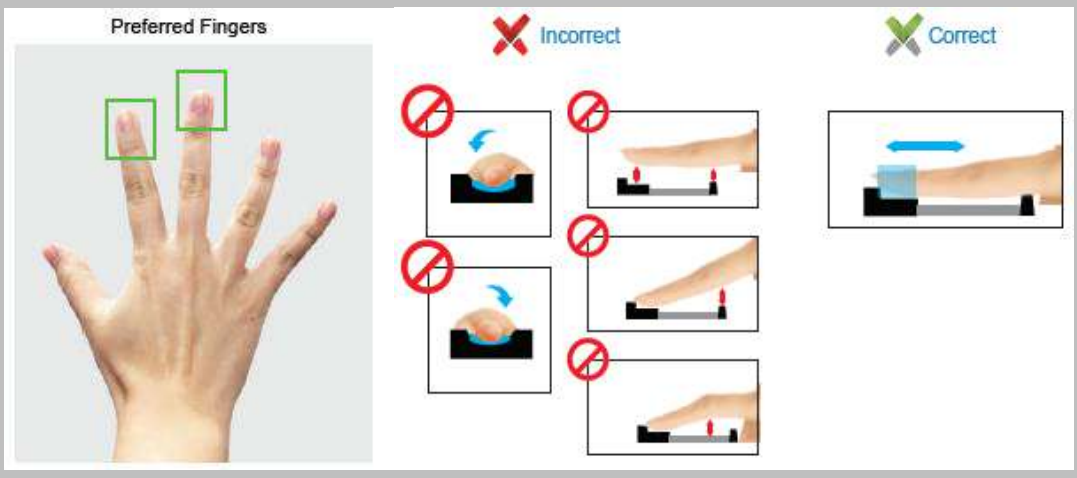


Figure 65: Finger Vein Enrollment Best Practices

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.

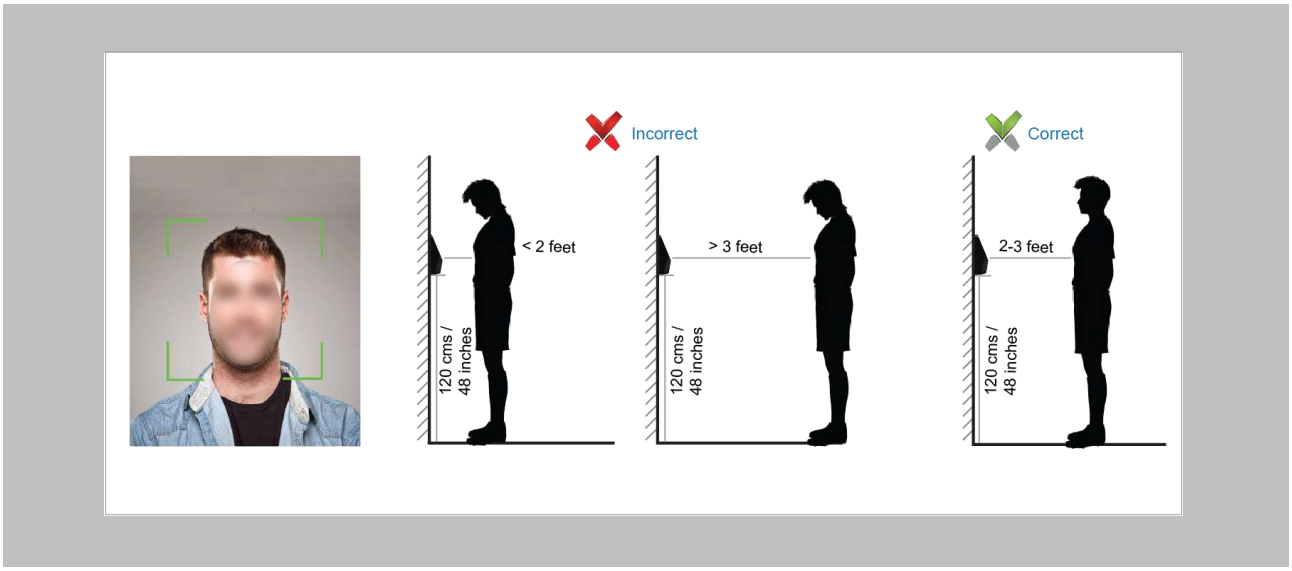


Figure 66: Face Enrollment Best Practices

15. 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.

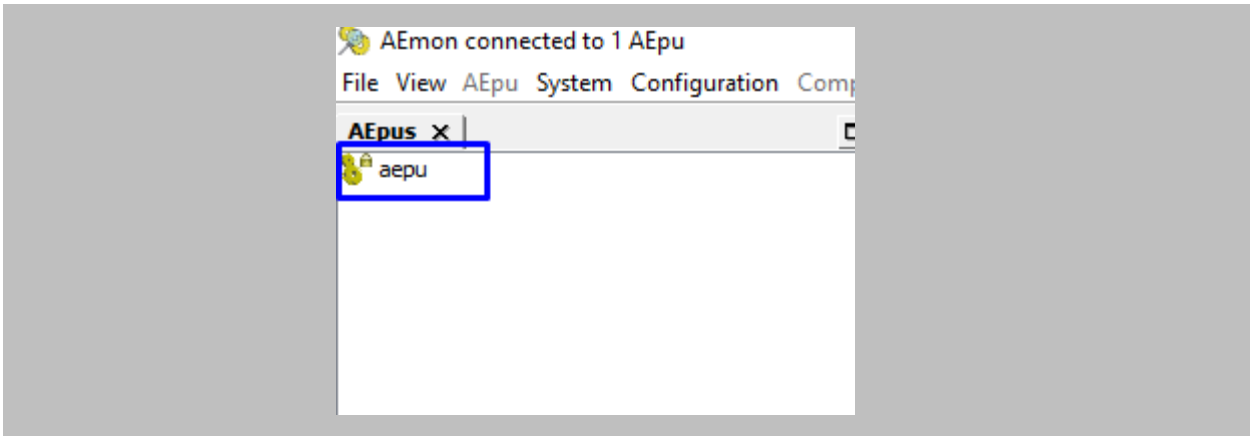


Figure 67: AEmon – Aepu

STEP 2

Go to View → Select Configuration.

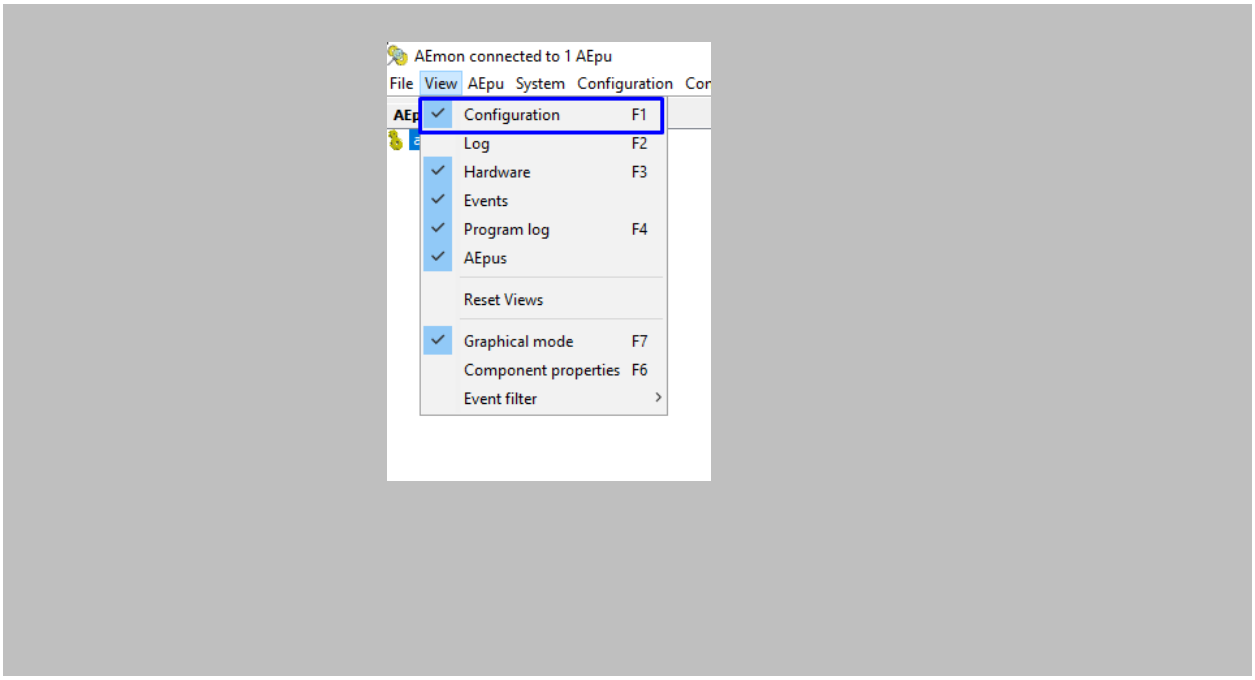


Figure 68: AEmon - AEpu Configuration

STEP 3

On the Configuration window search for StandardDoor → Add StandardDoor.

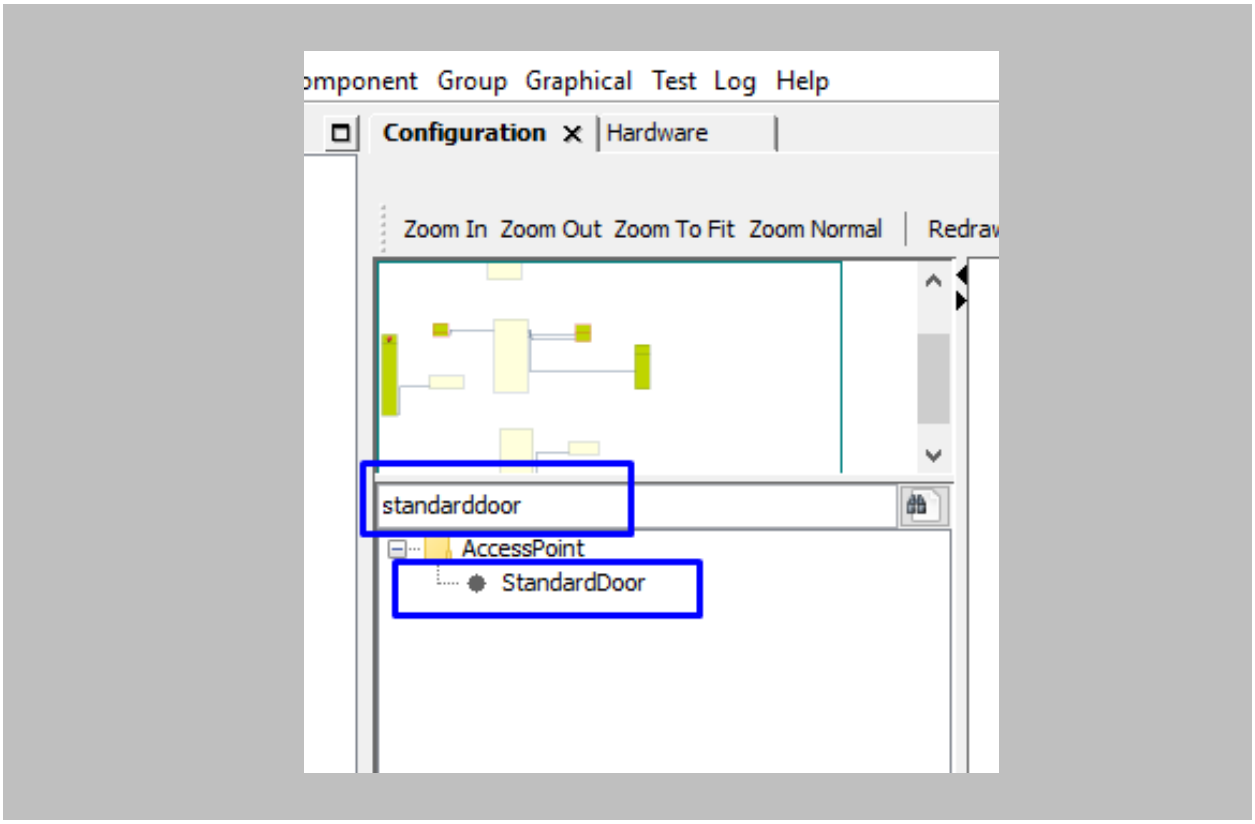


Figure 69: AEmon - Add Standard Door

STEP 4

Right Click on StandardDoor → Select Rename component.

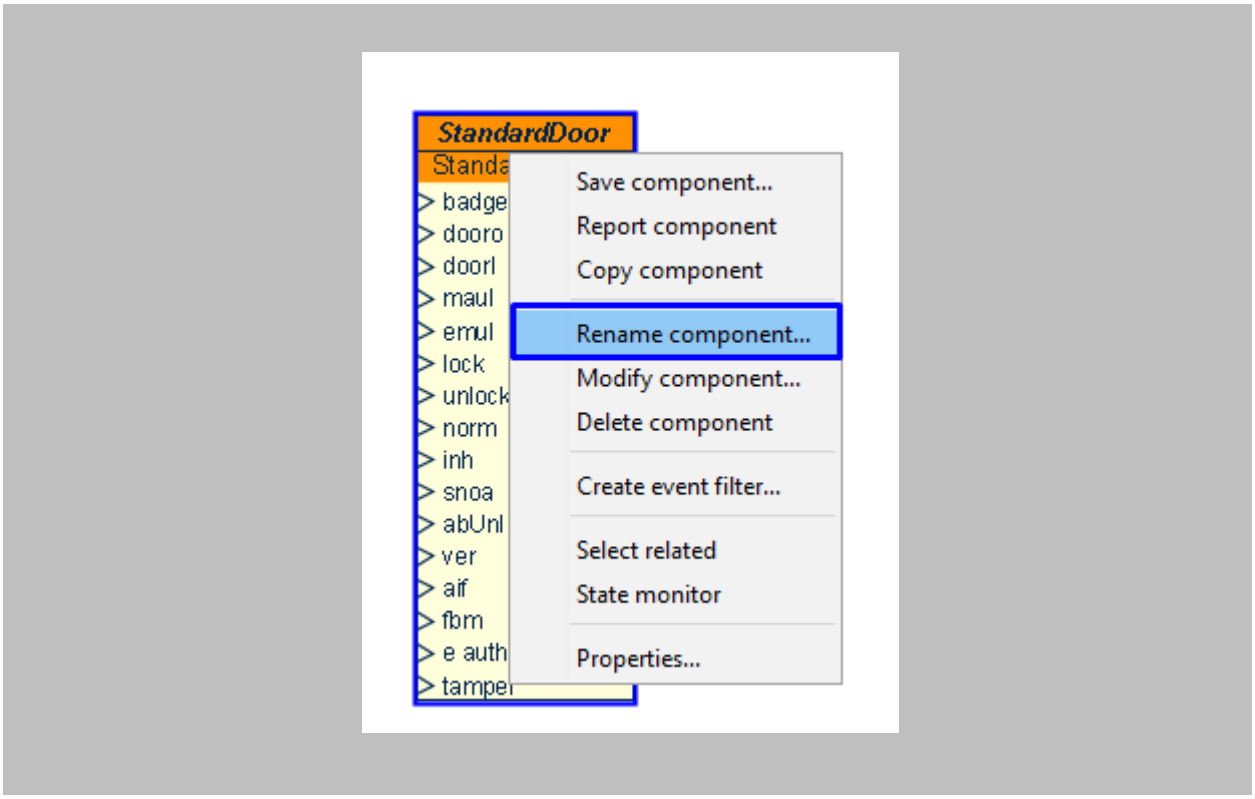


Figure 70: AEmon - Rename Component

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

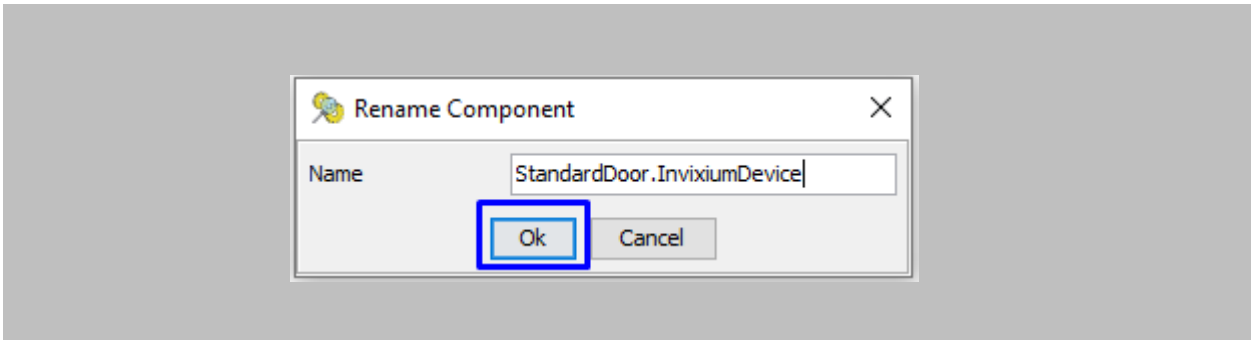


Figure 71: AEmon - Rename Standard Door

STEP 4

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

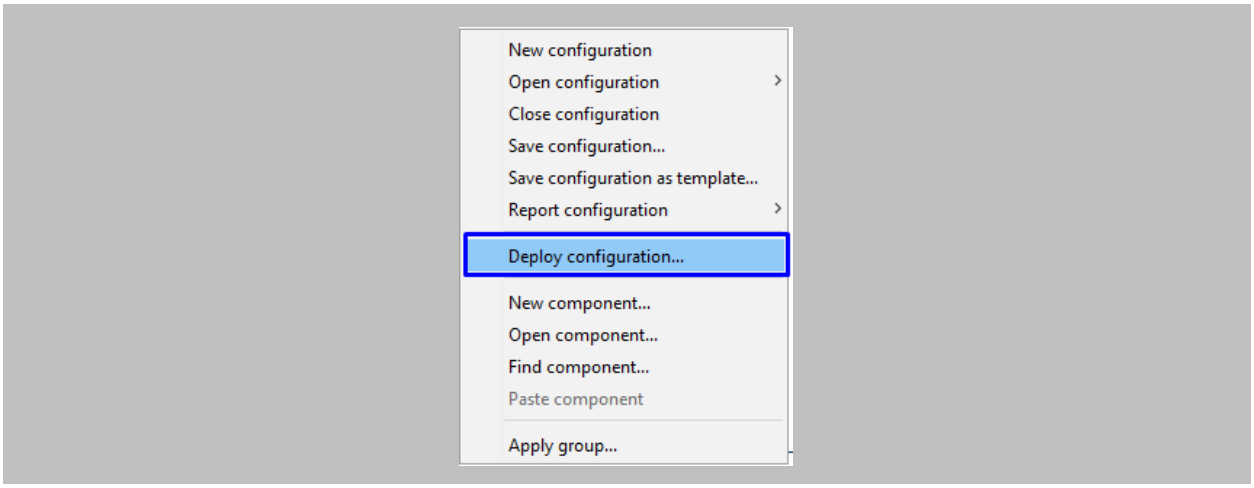


Figure 72: AEmon - Deploy Configuration

STEP 5

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

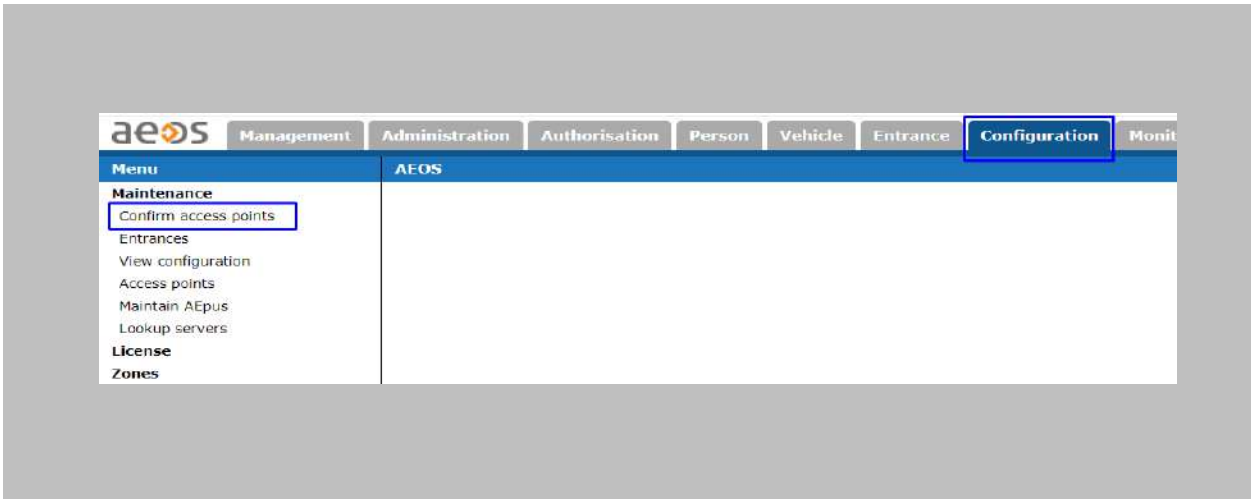


Figure 73: AEOS - Confirm Access Points

STEP 6

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

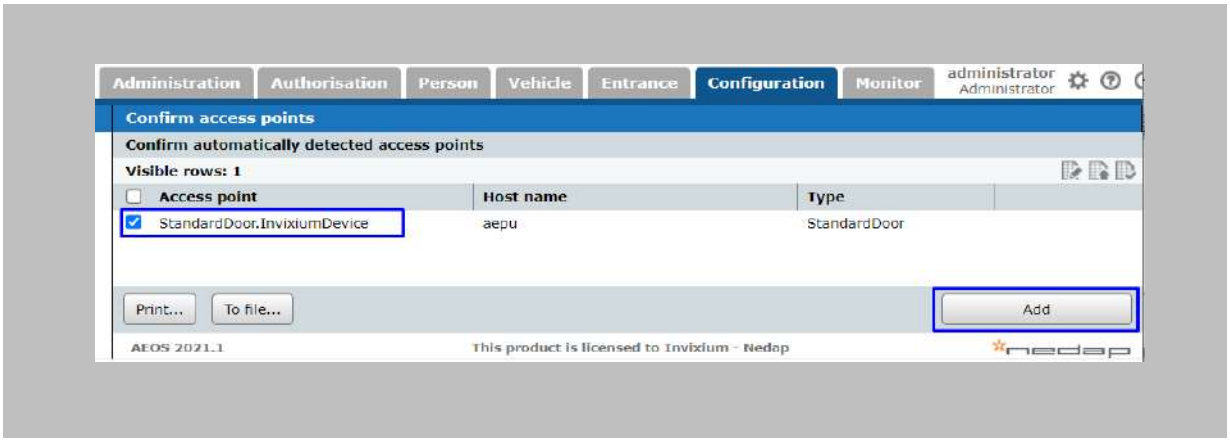


Figure 74: AEOS - Add Access Point

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

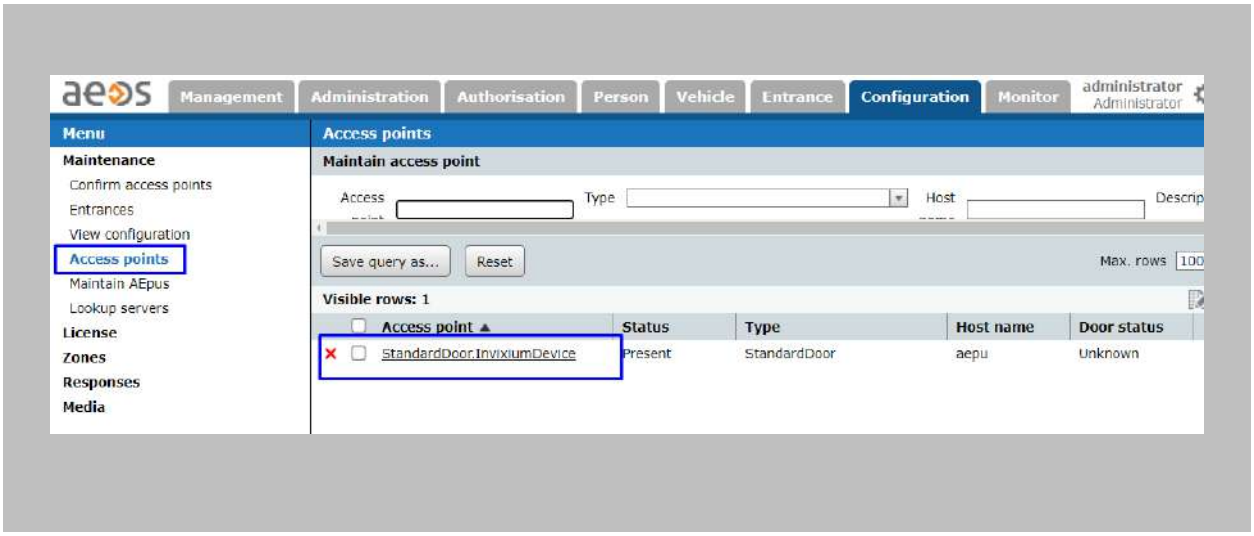


Figure 75: AEOS - Access Point

STEP 7

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

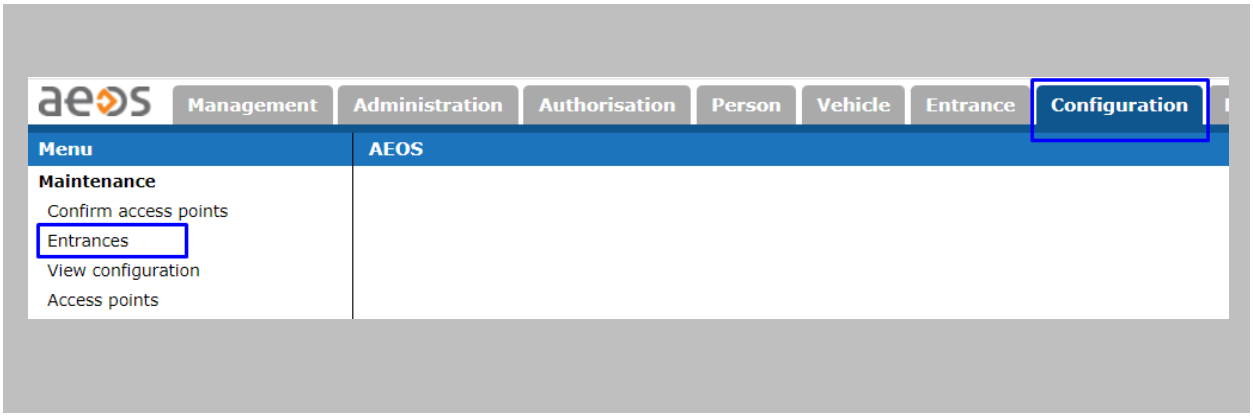


Figure 76: AEOS – Entrances

Click on the **New** button.

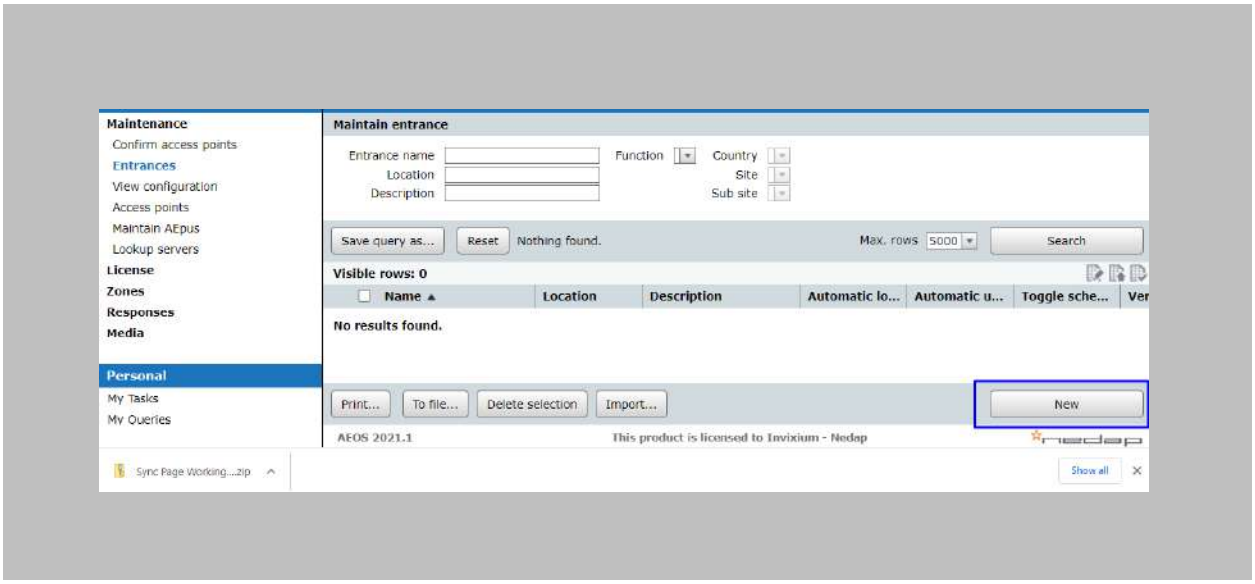


Figure 77: AEOS - New Entrance

STEP 8

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

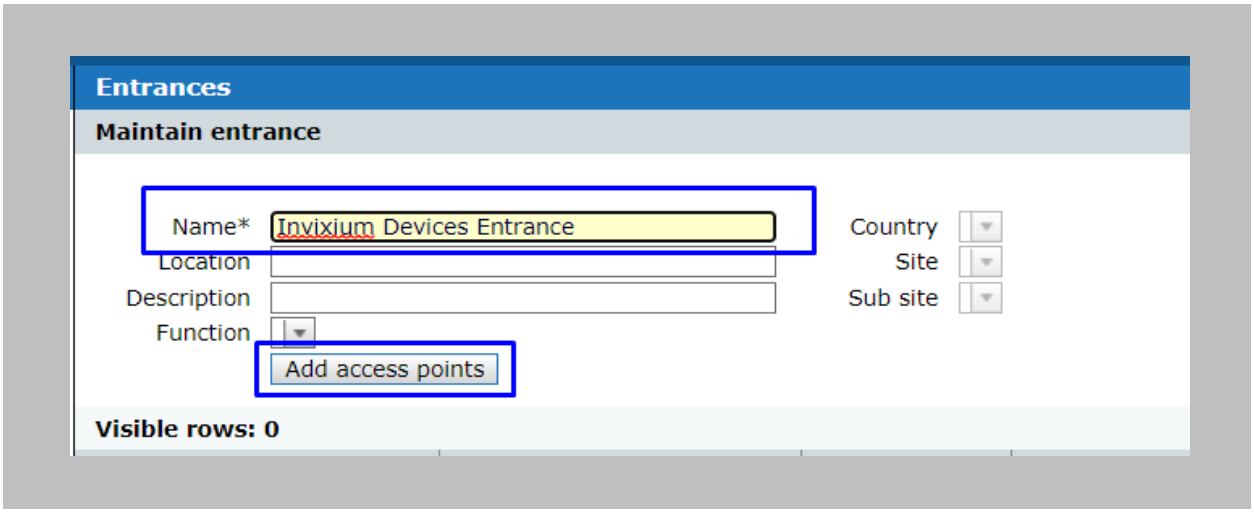


Figure 78: AEOS - Create New Entrance

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

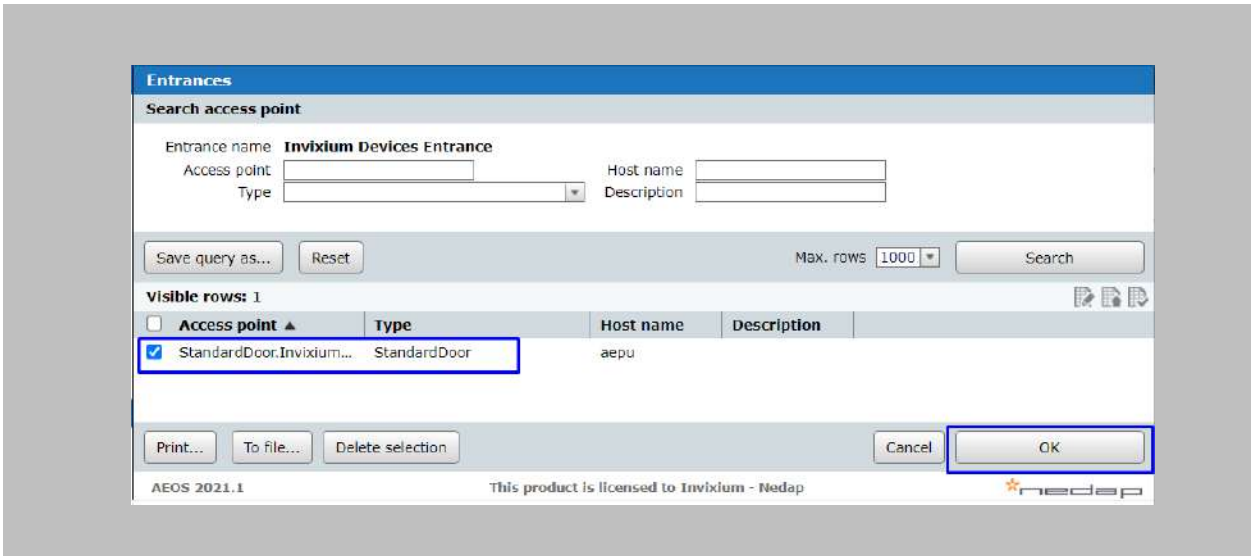


Figure 79: AEOS - Add Access Point in Entrance

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

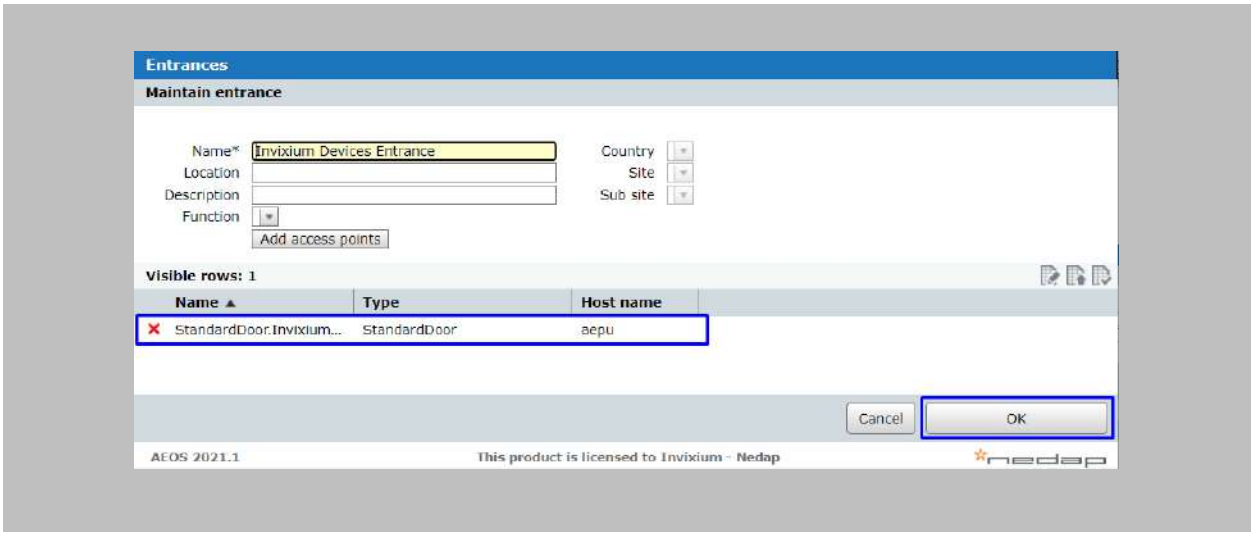


Figure 80: AEOS - Save Entrance

STEP 9

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

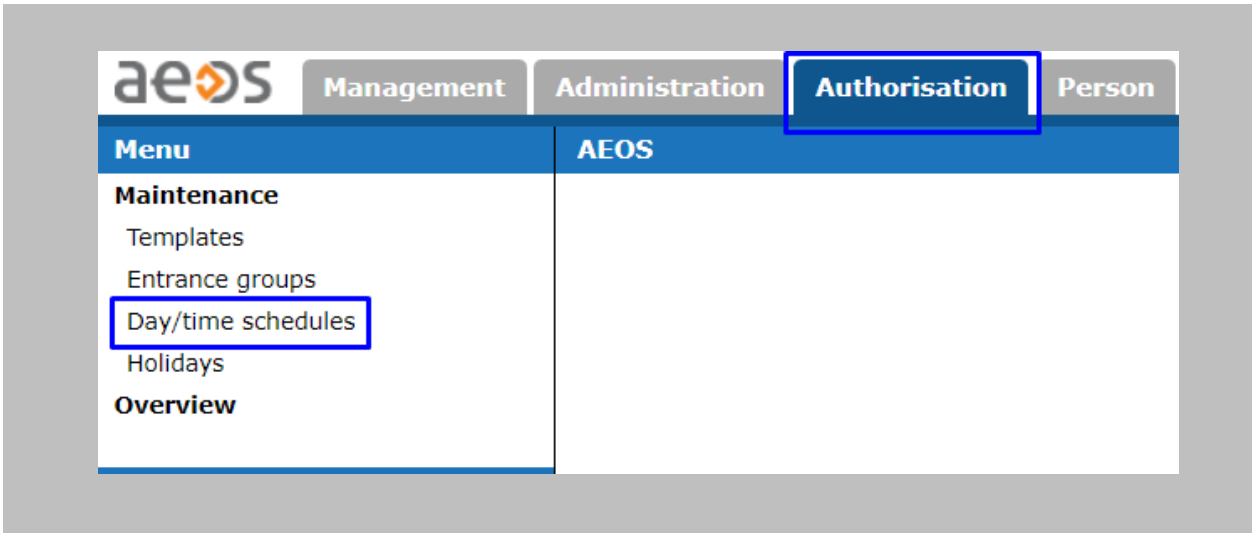


Figure 81: AEOS – DayTimeSchedules

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

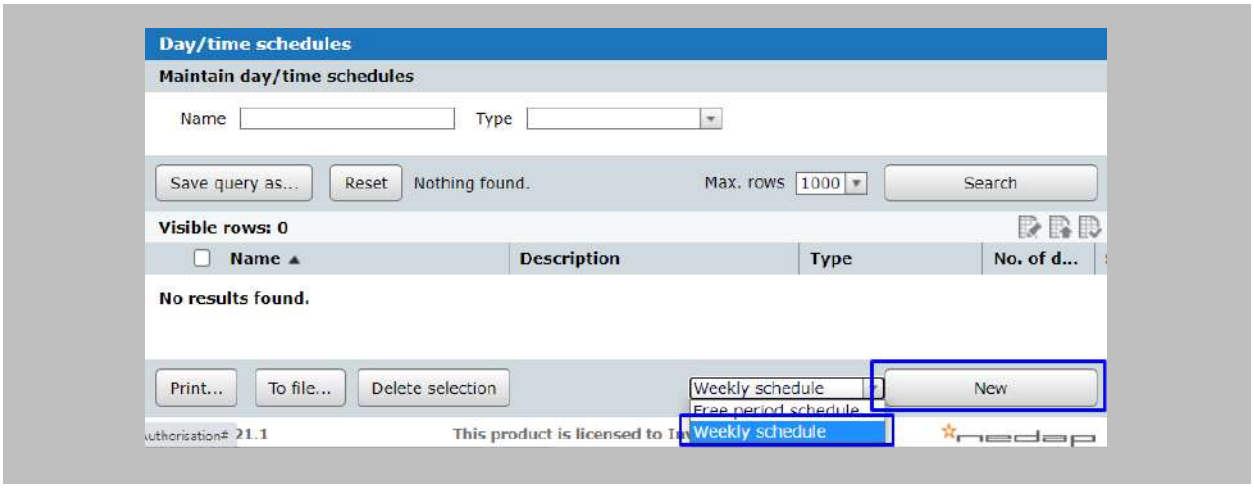


Figure 82: AEOS - New Weekly Schedule

STEP 10

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

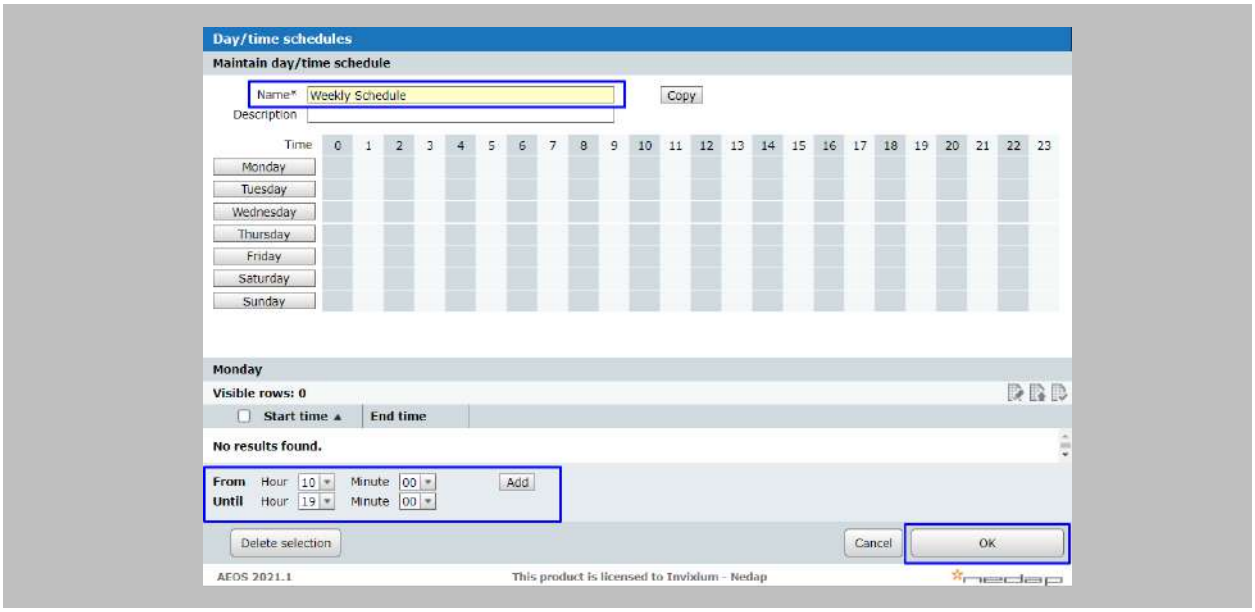


Figure 83: AEOS - Define Weekly Schedule

STEP 11

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

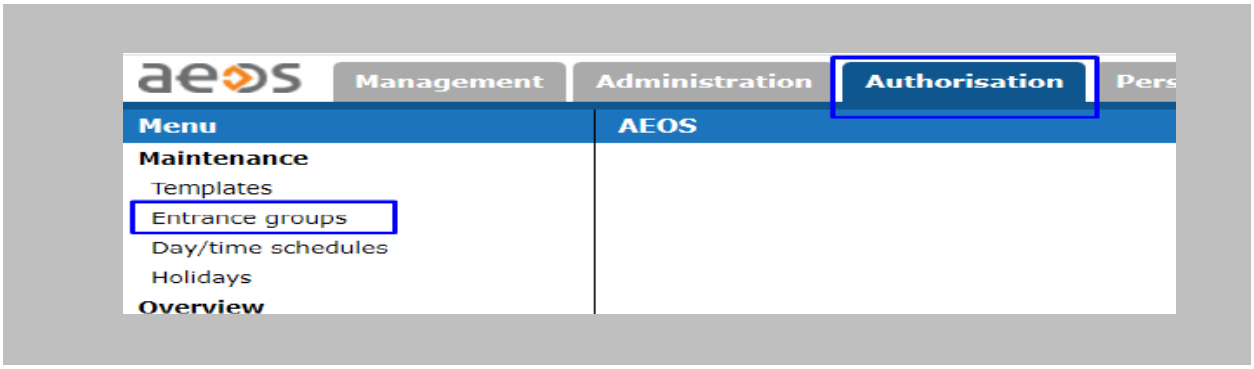


Figure 84: AEOS - Entrance Groups

Click on the **New** button.

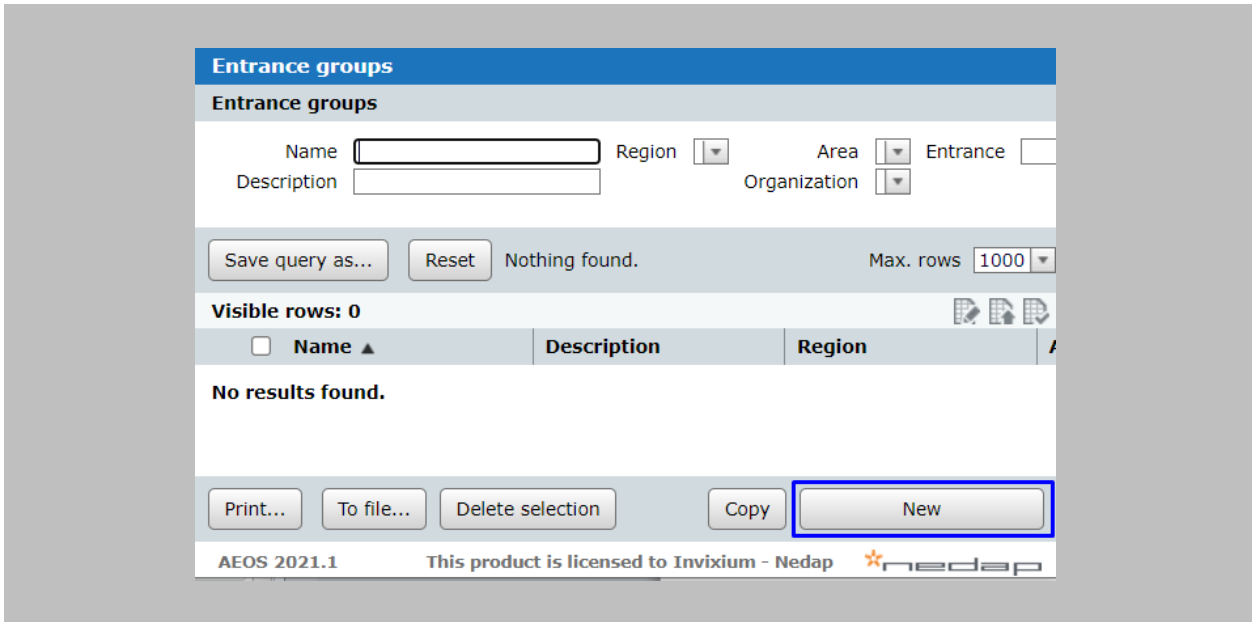


Figure 85: AEOS - New Entrance Group

STEP 12

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

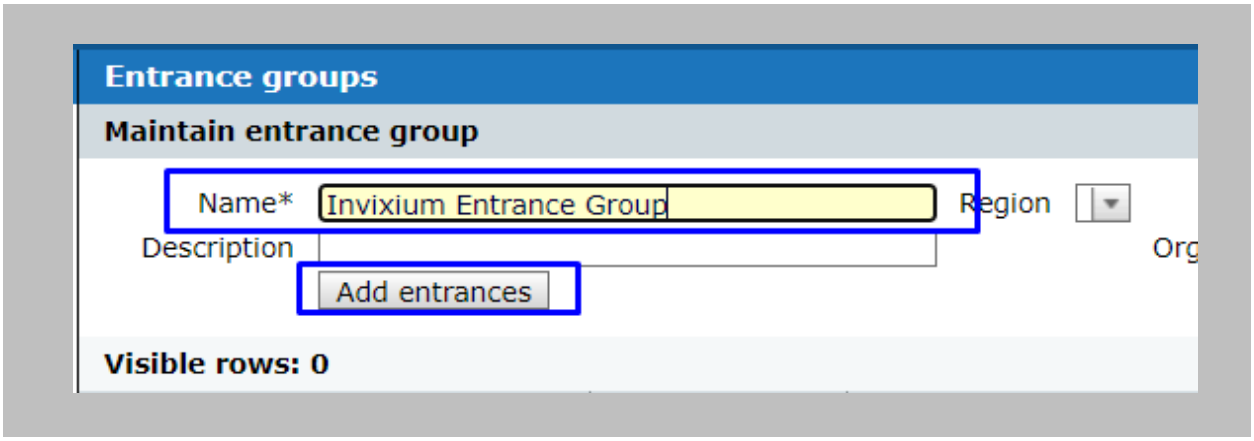


Figure 86: AEOS - Add Entrance in Entrance Group

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

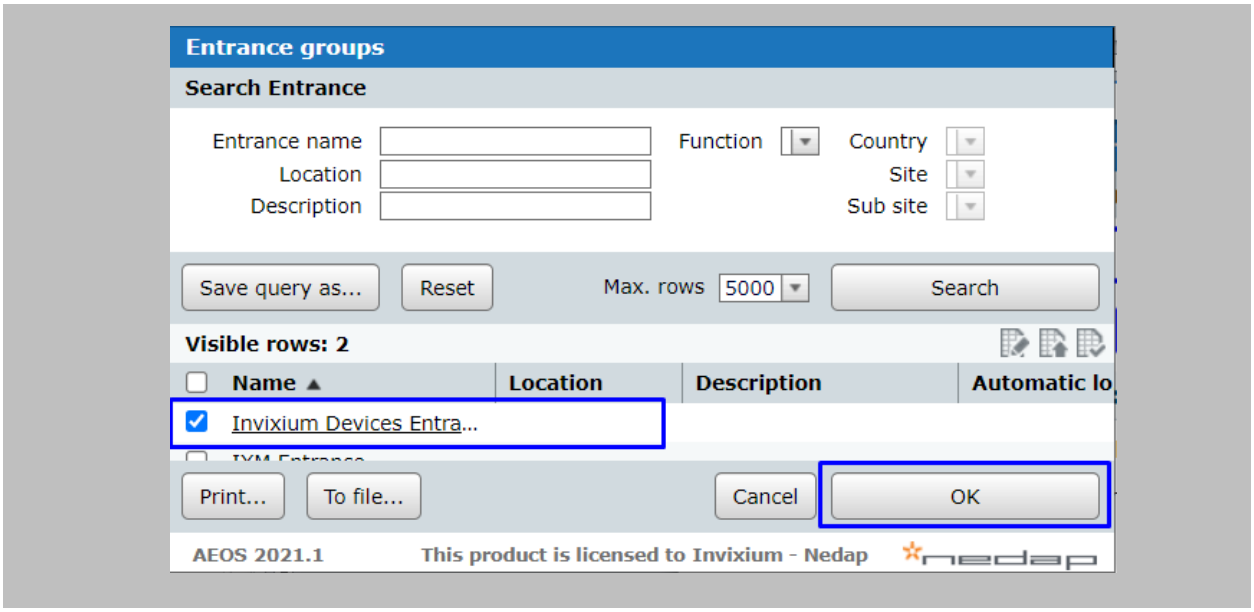


Figure 87: AEOS - Add Entrance Group

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

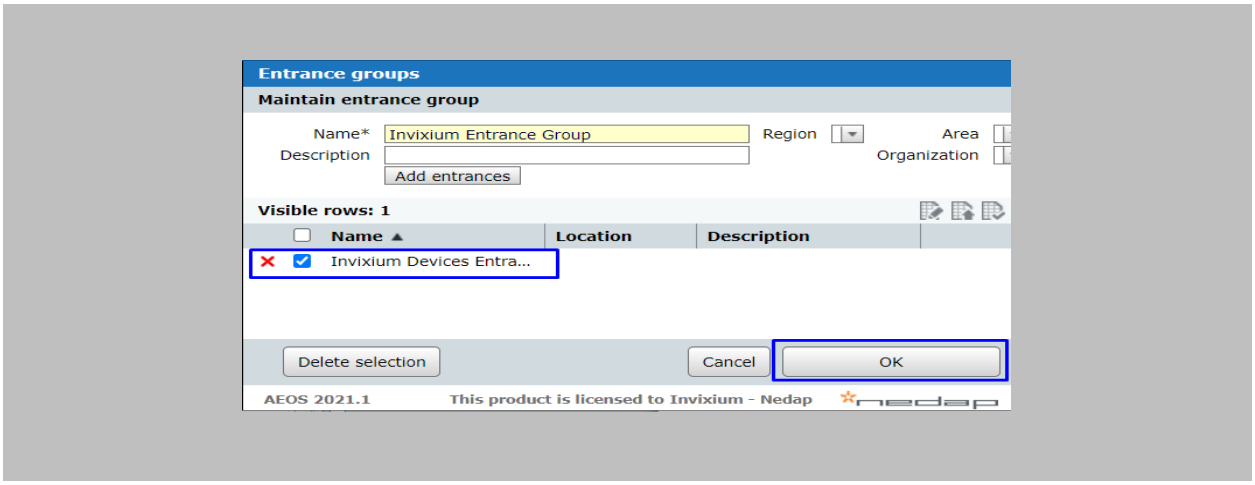


Figure 88: AEOS - Save Entrance Group

STEP 13

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

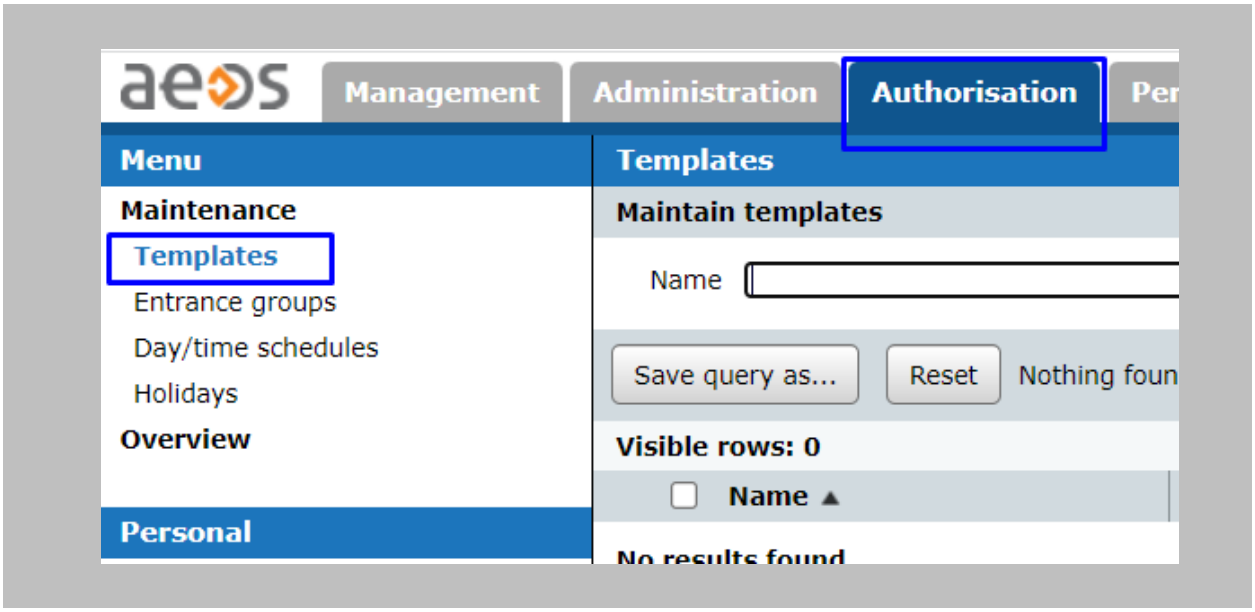


Figure 89: AEOS – Template

Click on the **New** button.

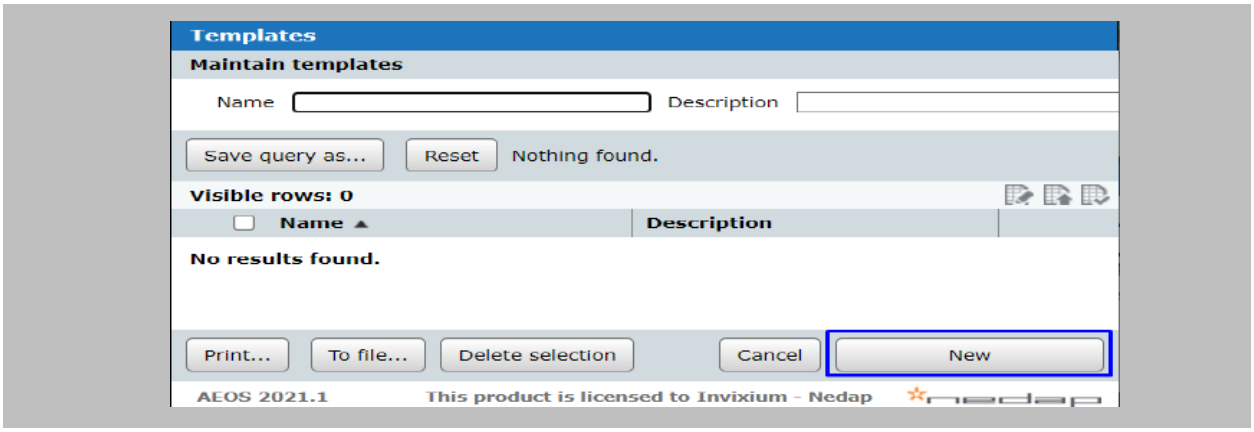


Figure 90: AEOS - New Template

STEP 14

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

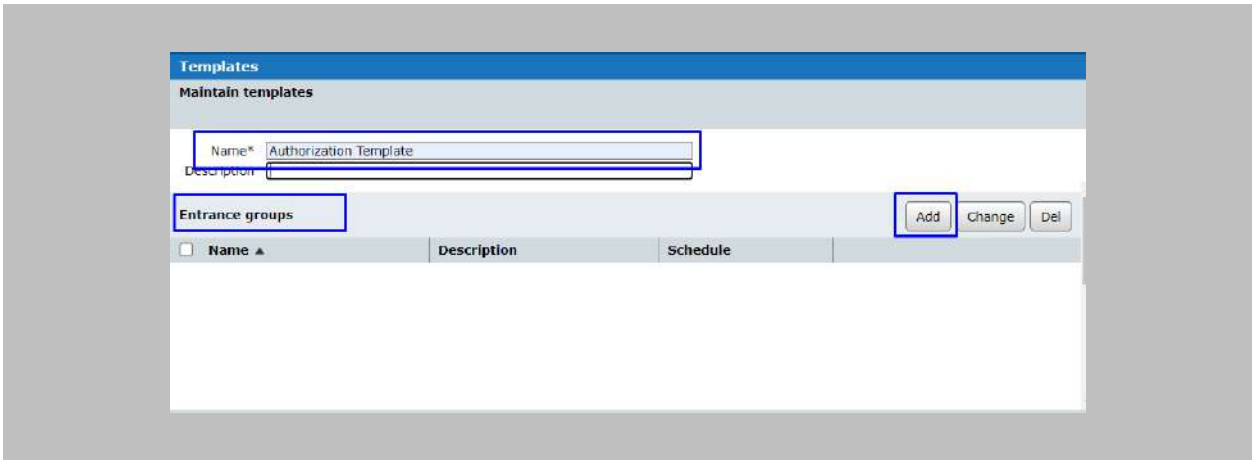


Figure 91: AEOS Template - Add Entrance Group

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

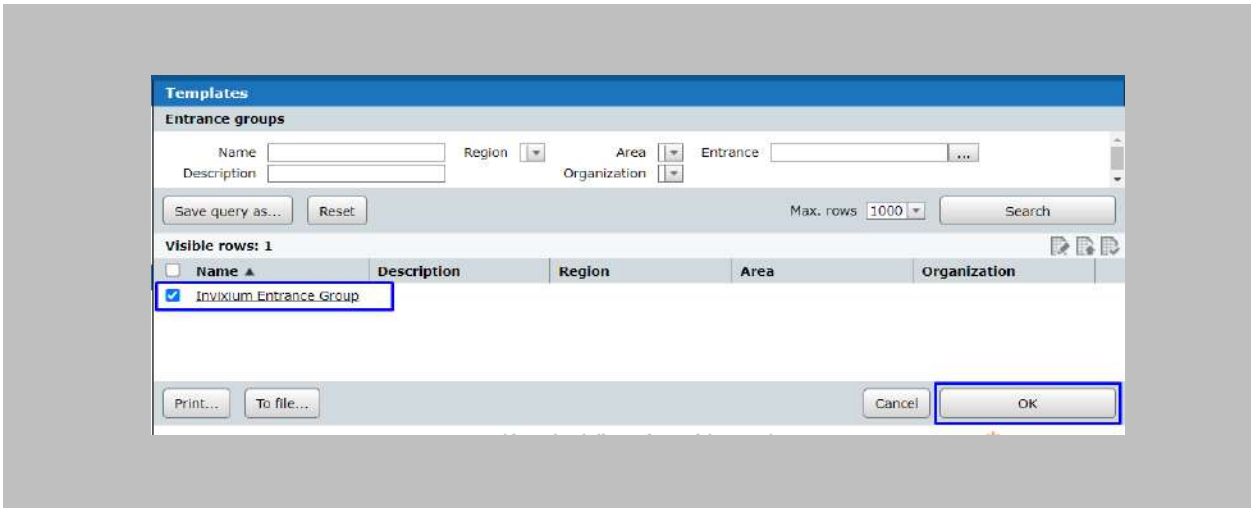


Figure 92: AEOS Template - Add Entrance Group

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

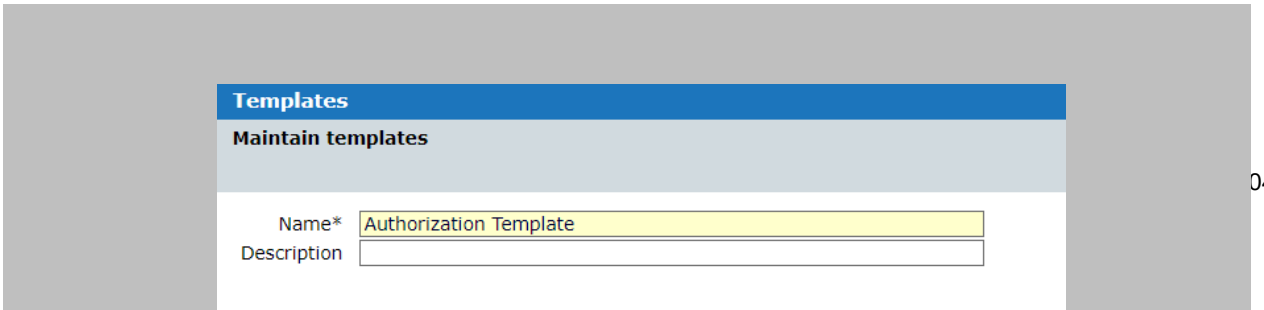


Figure 93: AEOS Template - Assign Schedule to Entrance Group

STEP 15

Click on the **Add** button for adding an **Entrance** to the **Template**.

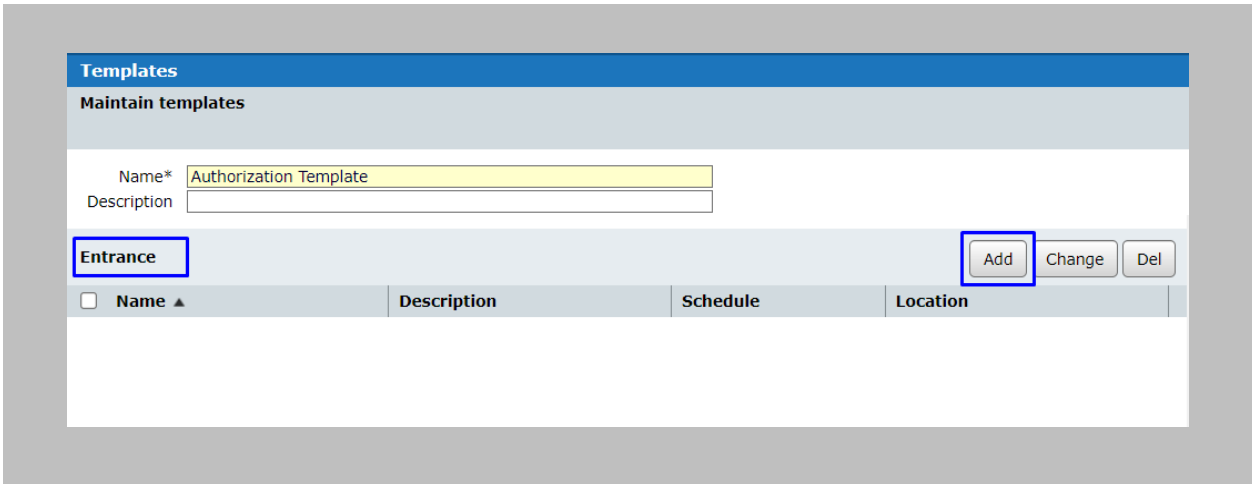


Figure 94: AEOS Template - Add Entrance

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

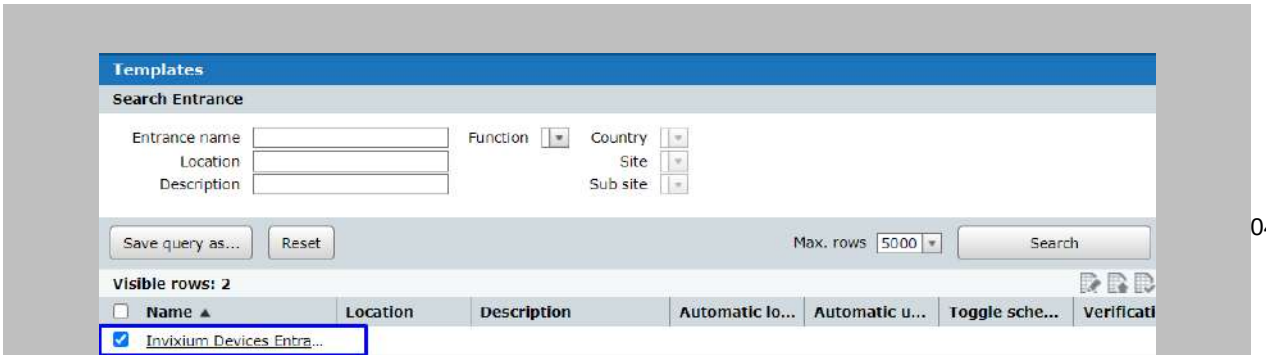


Figure 95: AEOS Template - Save Entrance

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

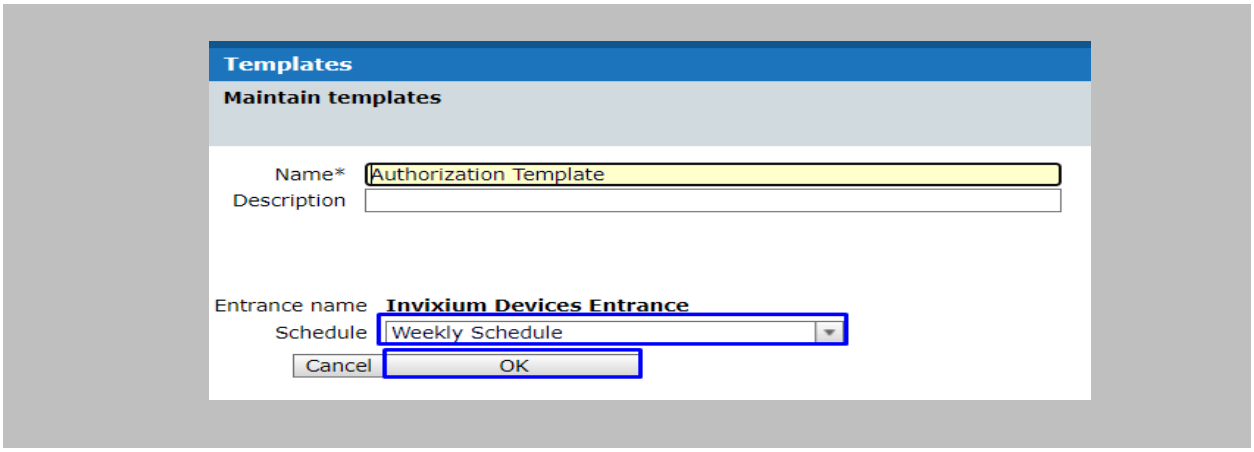


Figure 96: AEOS Template - Assign Schedule to Entrance

STEP 16

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

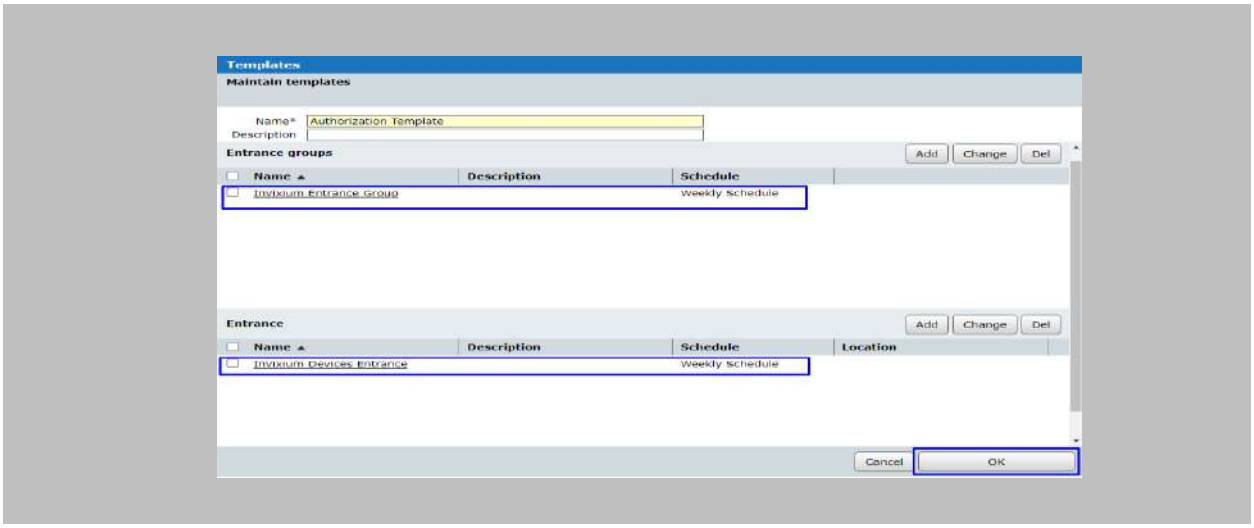


Figure 97: AEOS - Save Template

STEP 17

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

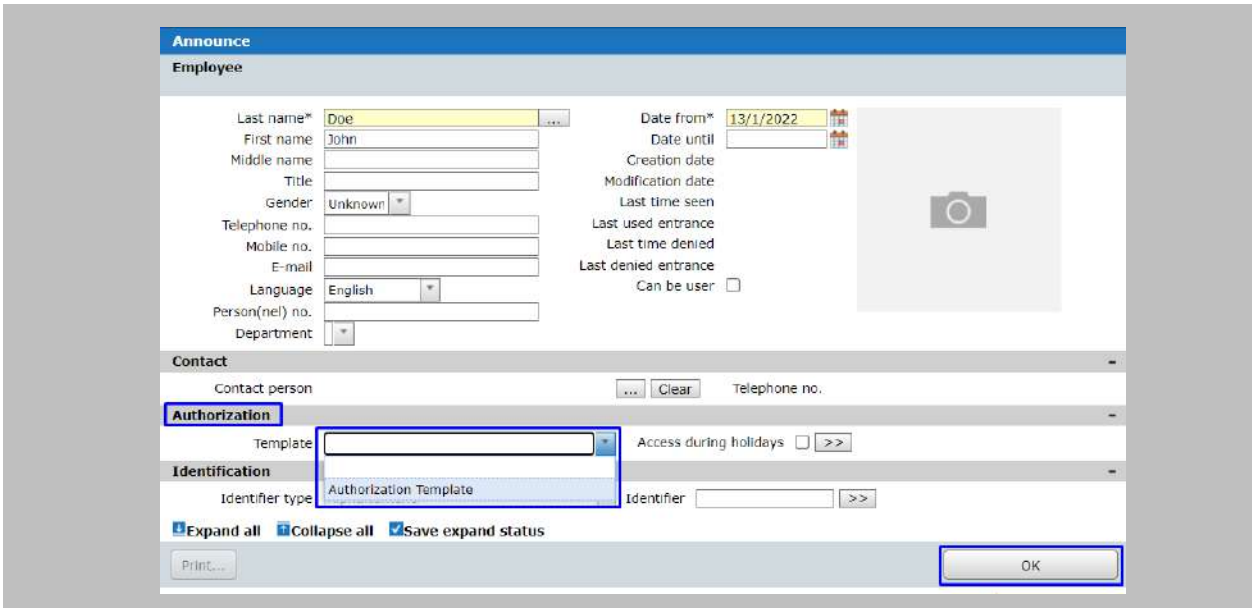


Figure 98: AEOS - Assign Template to Person

RESULT

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

16. 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**.

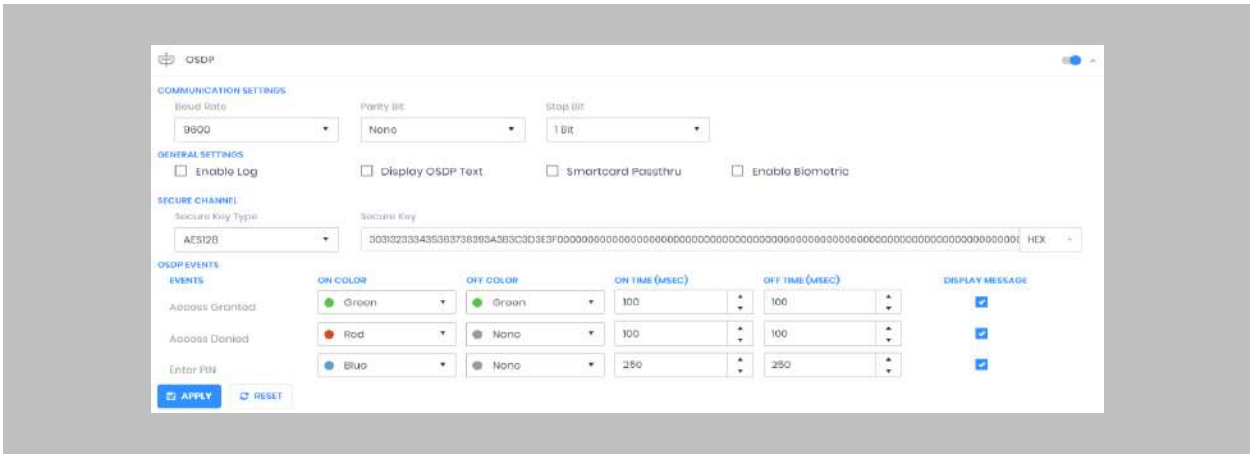


Figure 99: IXM WEB - OSDP Settings

STEP 2

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

Baud Rate	The baud rate of the 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
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

Table 5: 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 6: IXM WEB - OSDP Text Options

STEP 3

Click **Apply** to save the settings.

Figure 100: 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.

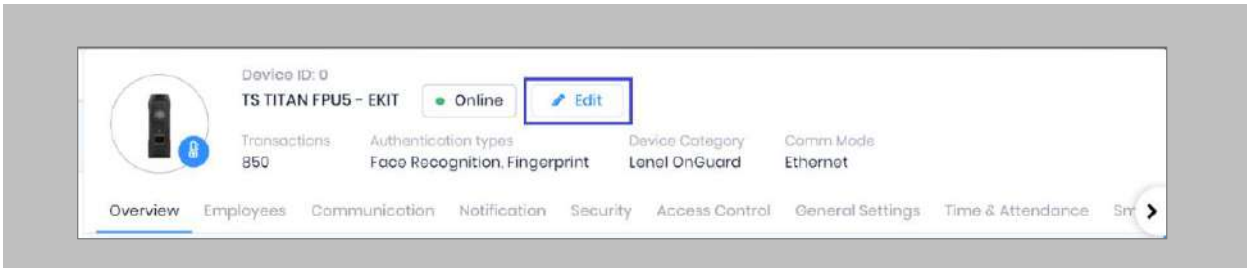


Figure 101: IXM WEB - Edit Device

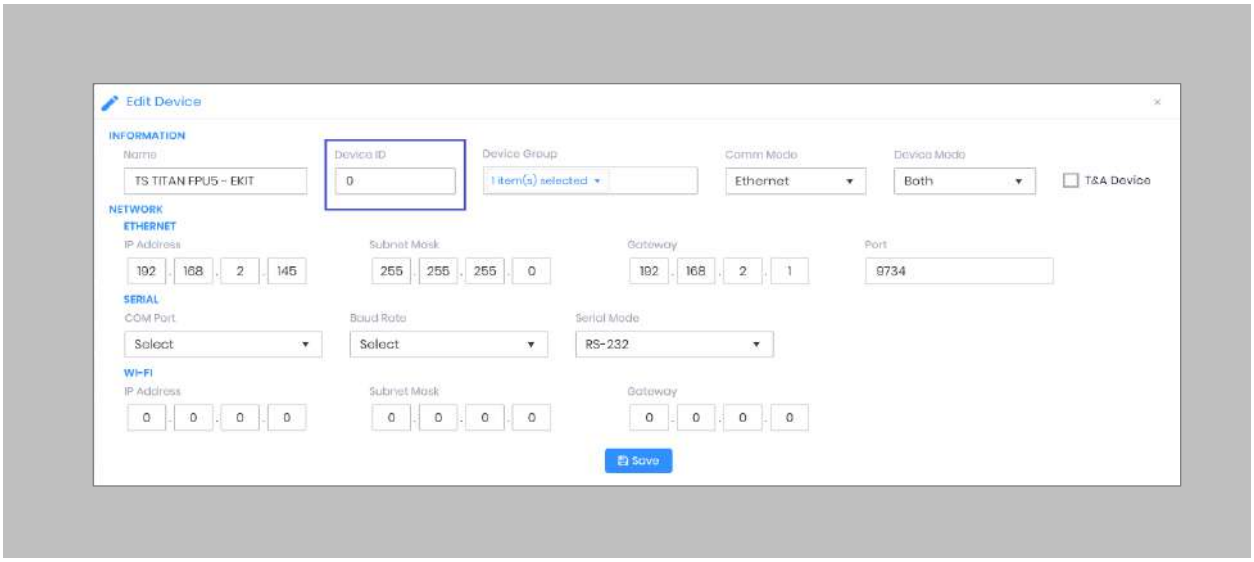


Figure 102: IXM WEB - Edit Device Options

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.

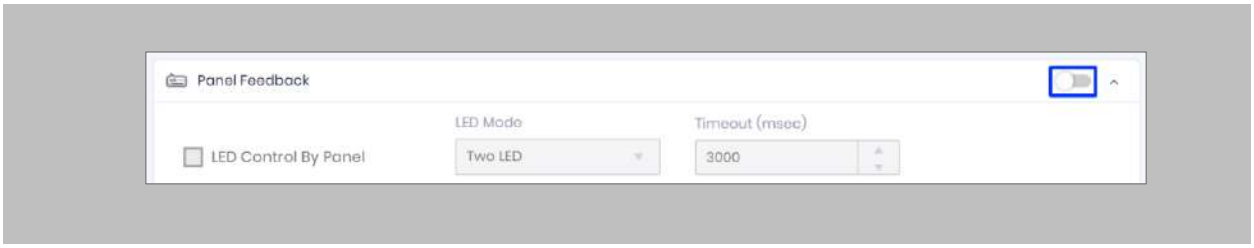


Figure 103: IXM WEB - Disable Panel Feedback

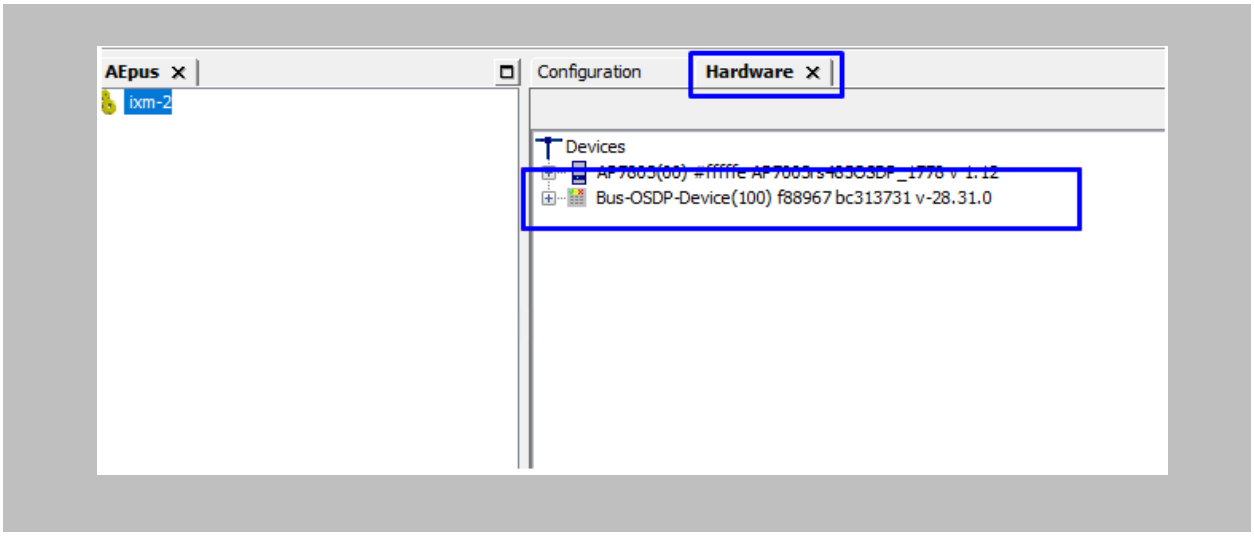


Figure 103: AEmon - OSDP Device

STEP 8

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

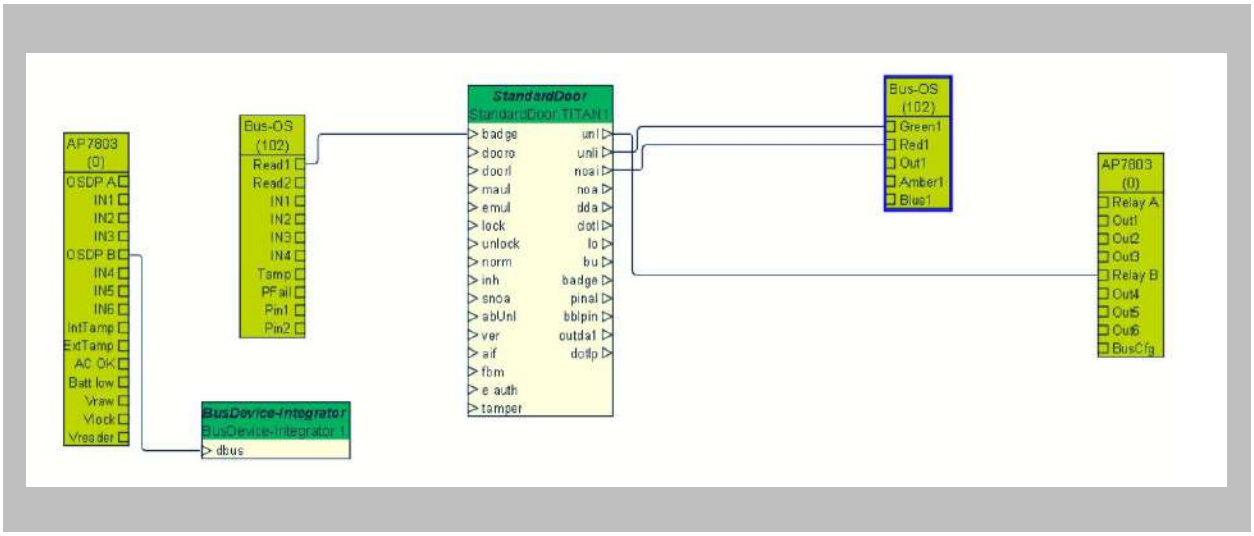


Figure 104:AEmon - OSDP Device Behavior

STEP 9

Right click on Standard Door → Properties.

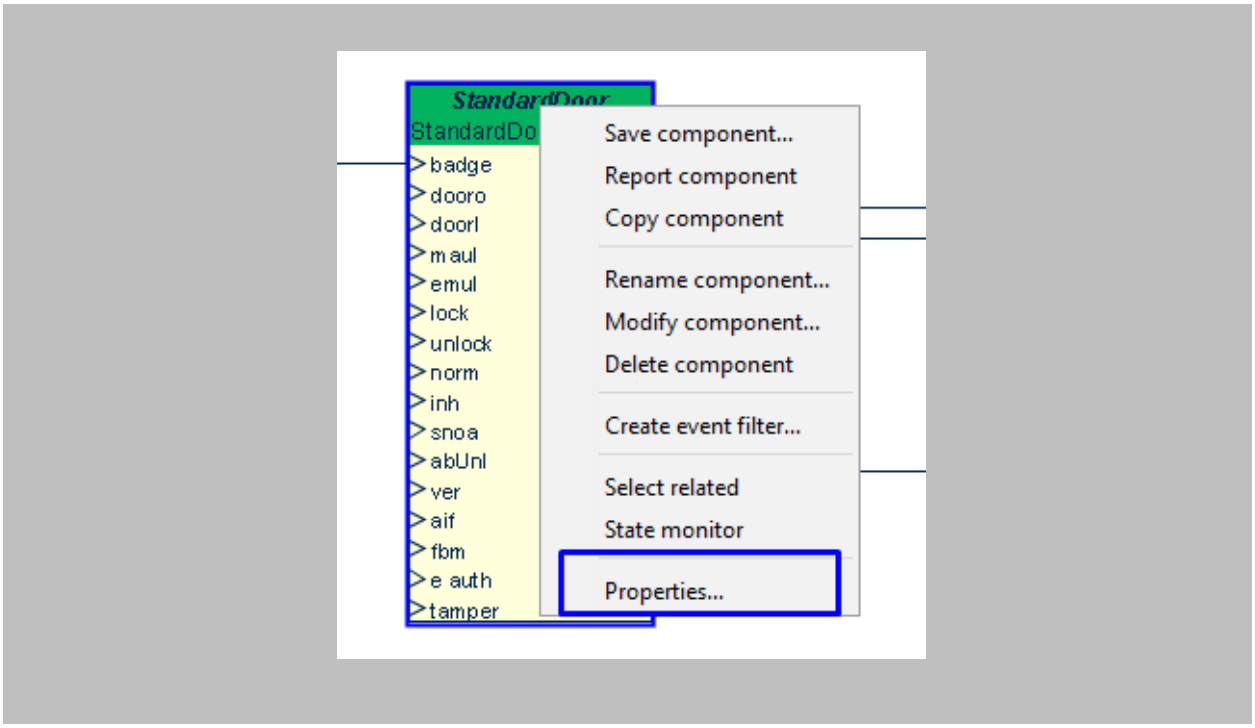


Figure 105: AEmon - Standard Door Property

STEP 10

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

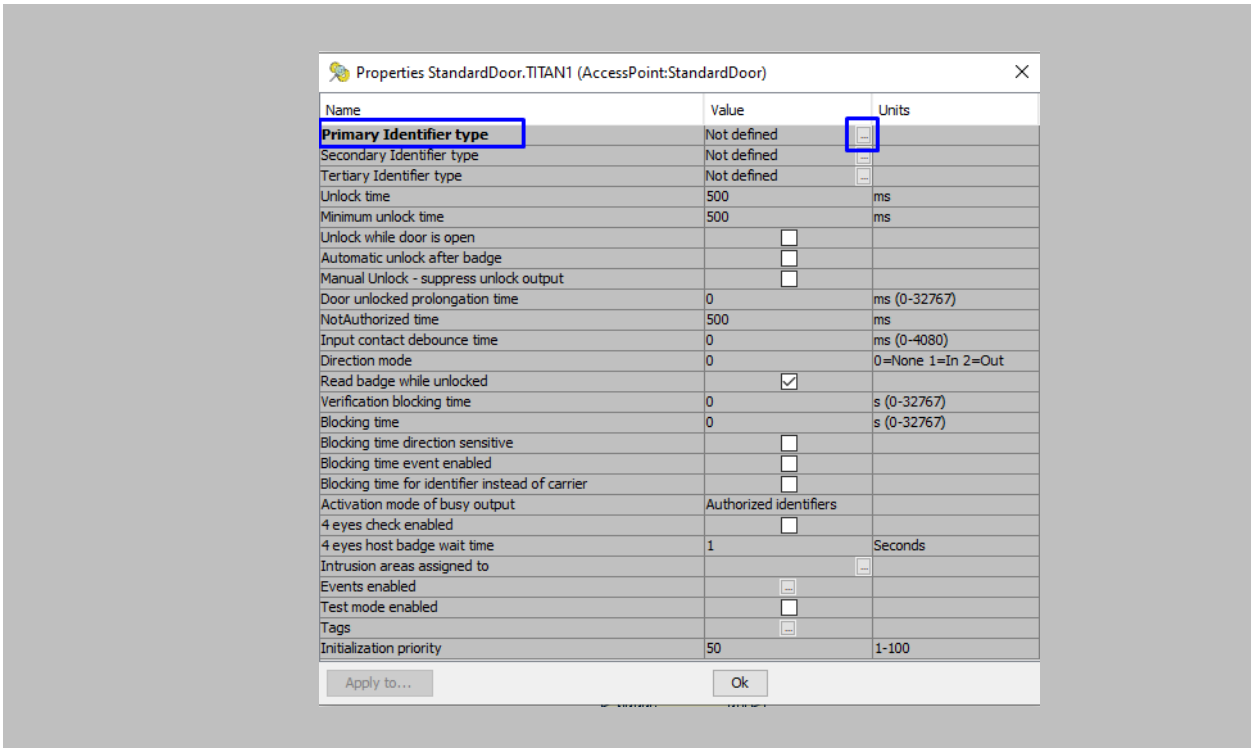


Figure 106: AEmon - Primary Identifier Type

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

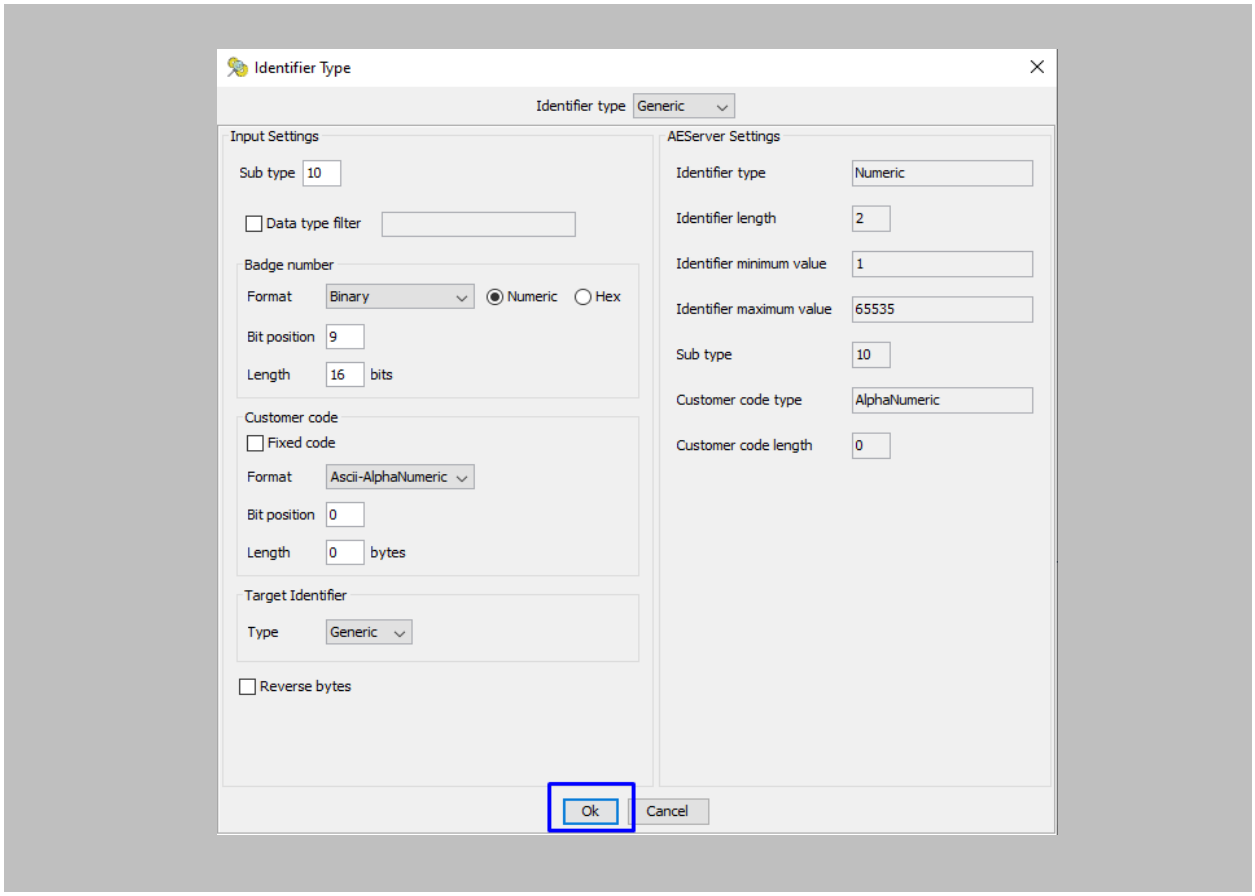


Figure 107: AEmon - Configure Primary Identifier Type

STEP 11

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

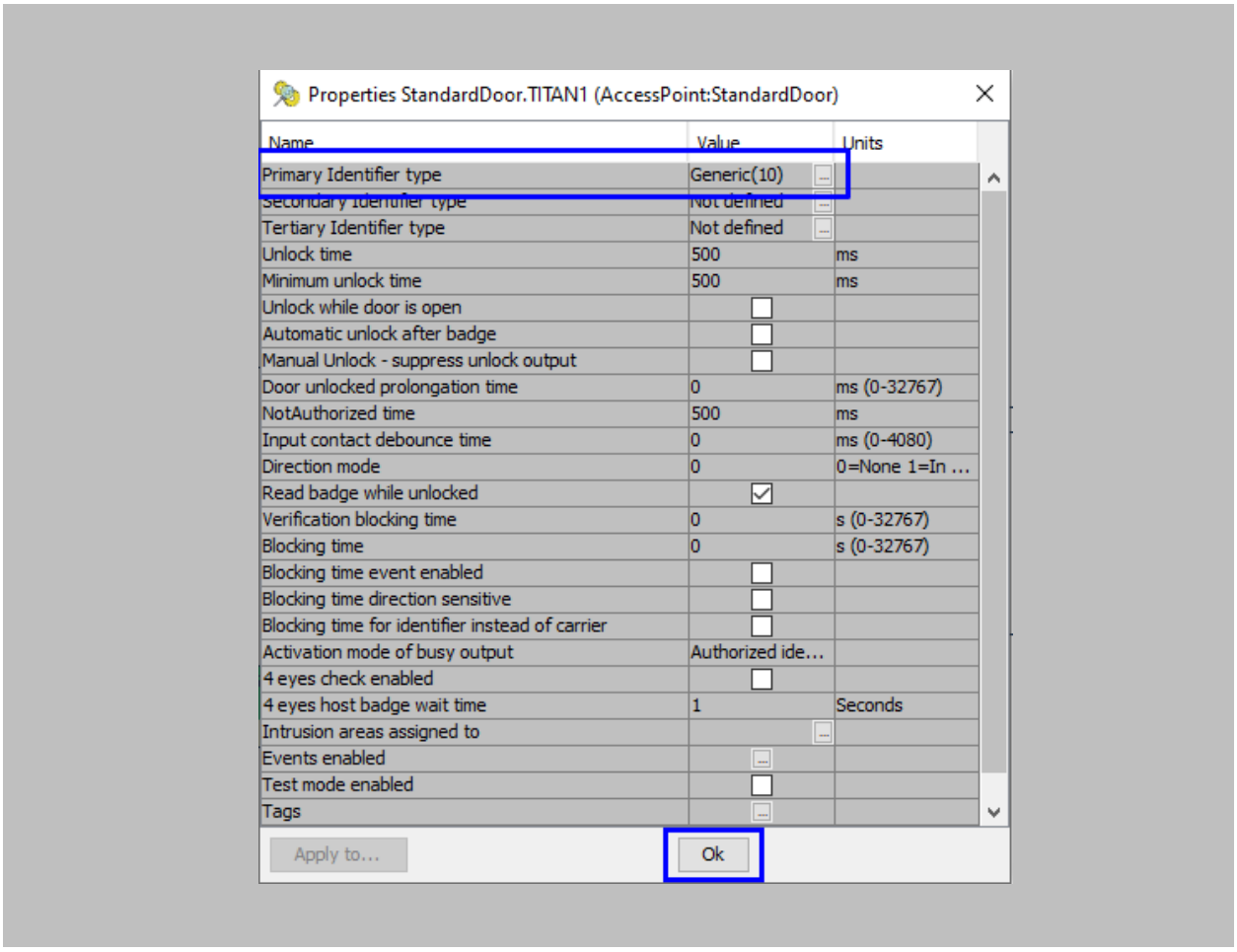


Figure 108: AEmon - Generic Primary Identifier Type

STEP 12

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

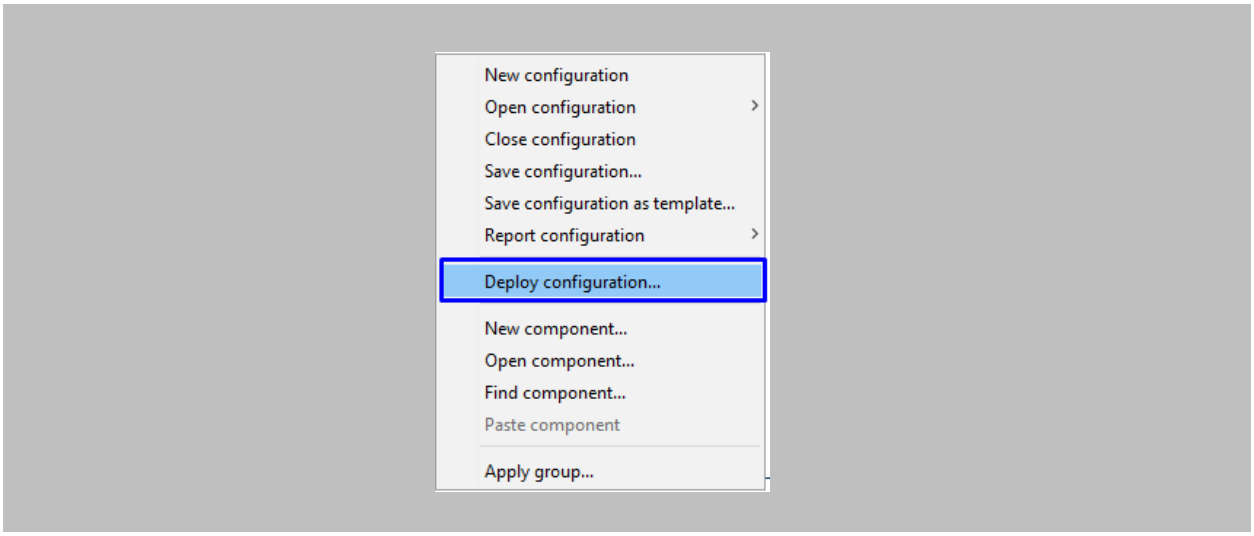


Figure 109: AEmon - Deploy Configuration

17. 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**.

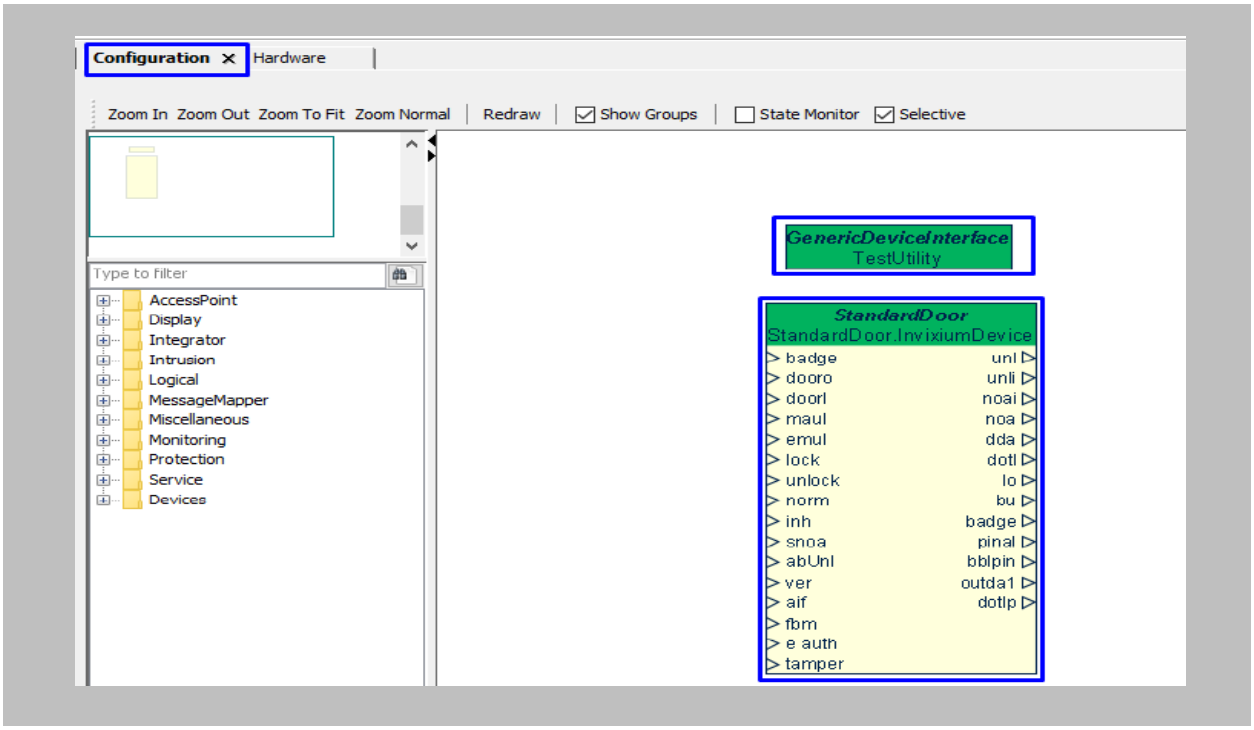


Figure 110: AEmon - Configuration tab

STEP 2

Search for ACLabelConverter → Add ACLabelConverter.

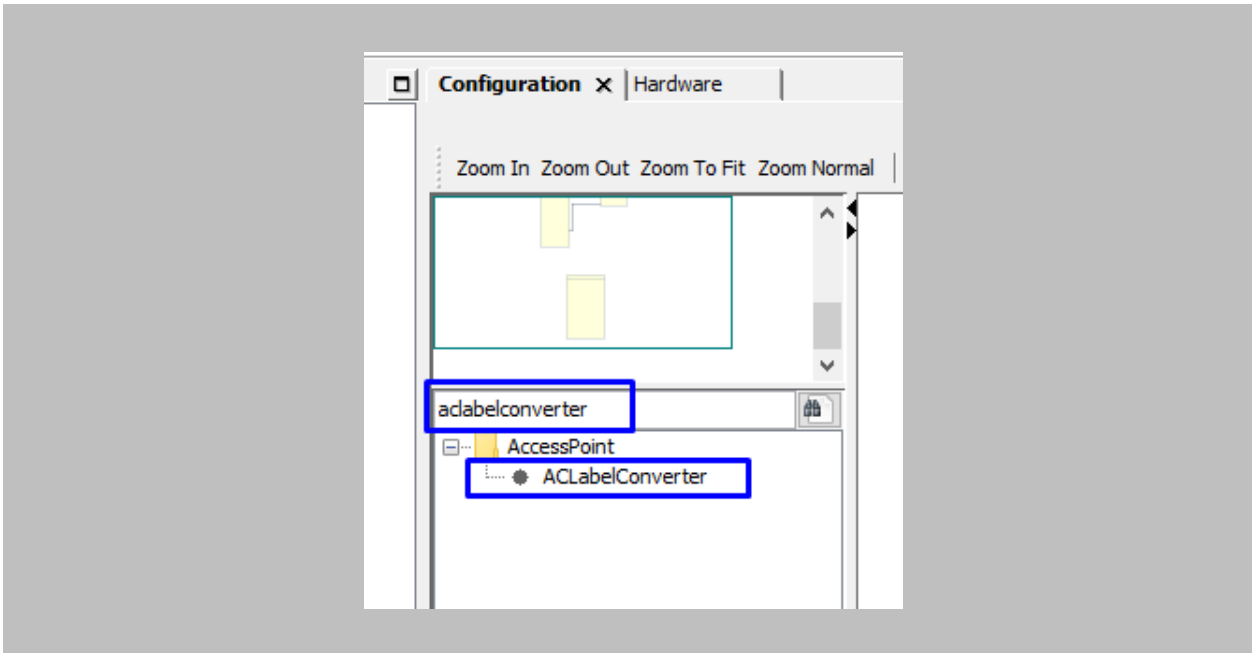


Figure 111: AEmon - Add ACLabelConverter

STEP 3

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

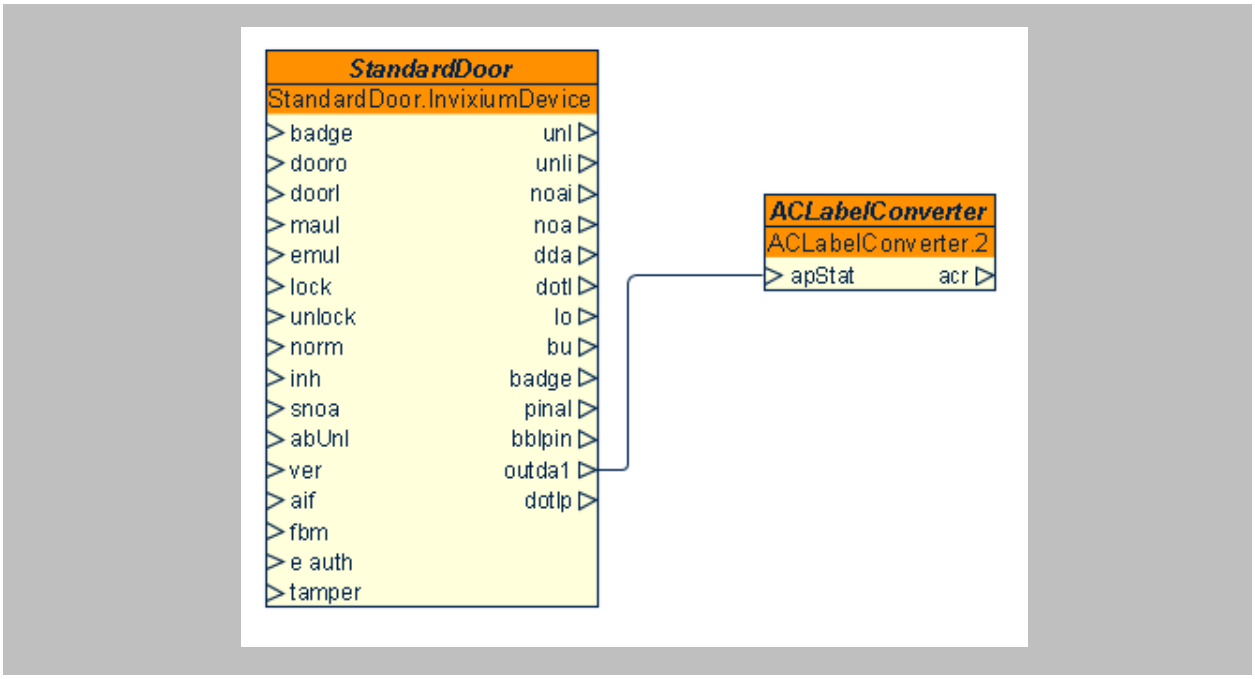


Figure 112: AEmon - StandardDoor and ACLabelConverter Connection

STEP 4

Right click on GenericDeviceInterface → click on Properties.

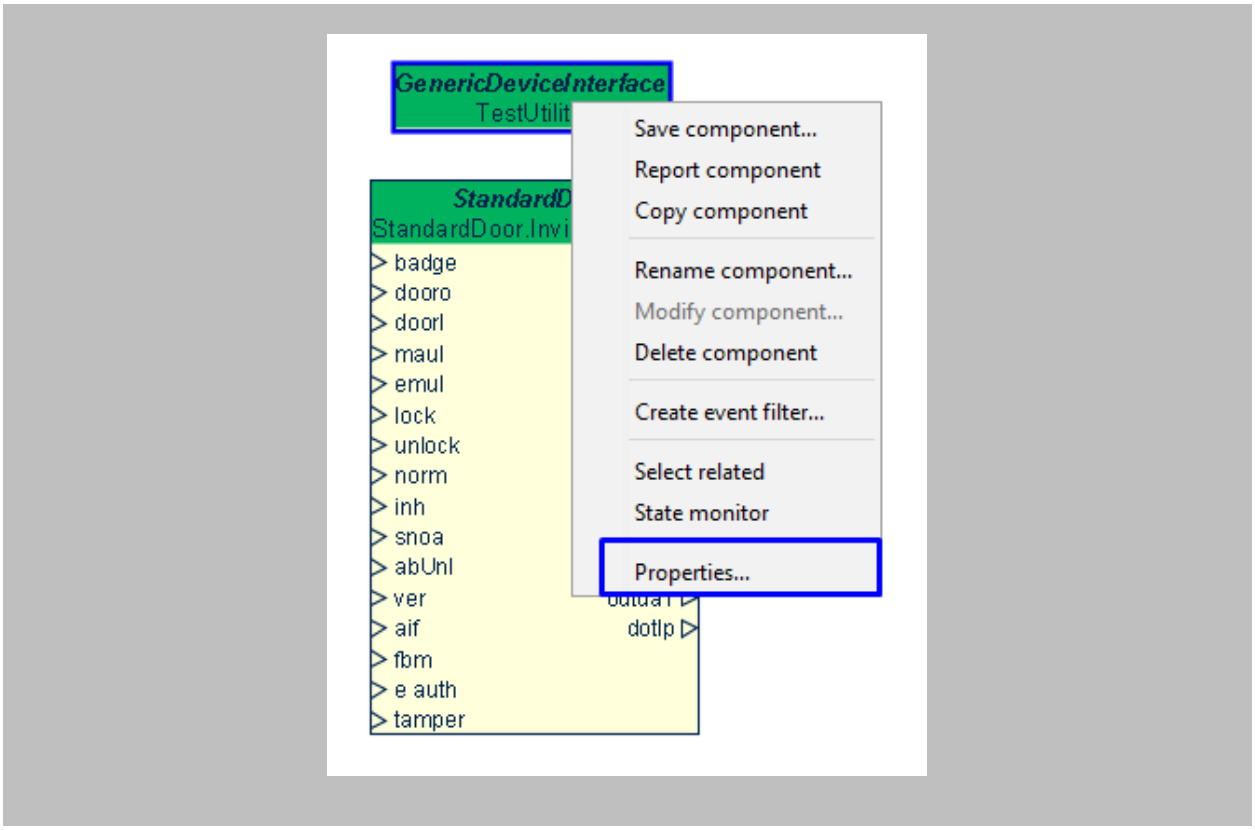


Figure 113: AEmon - GenericDeviceInterface Properties

STEP 5

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

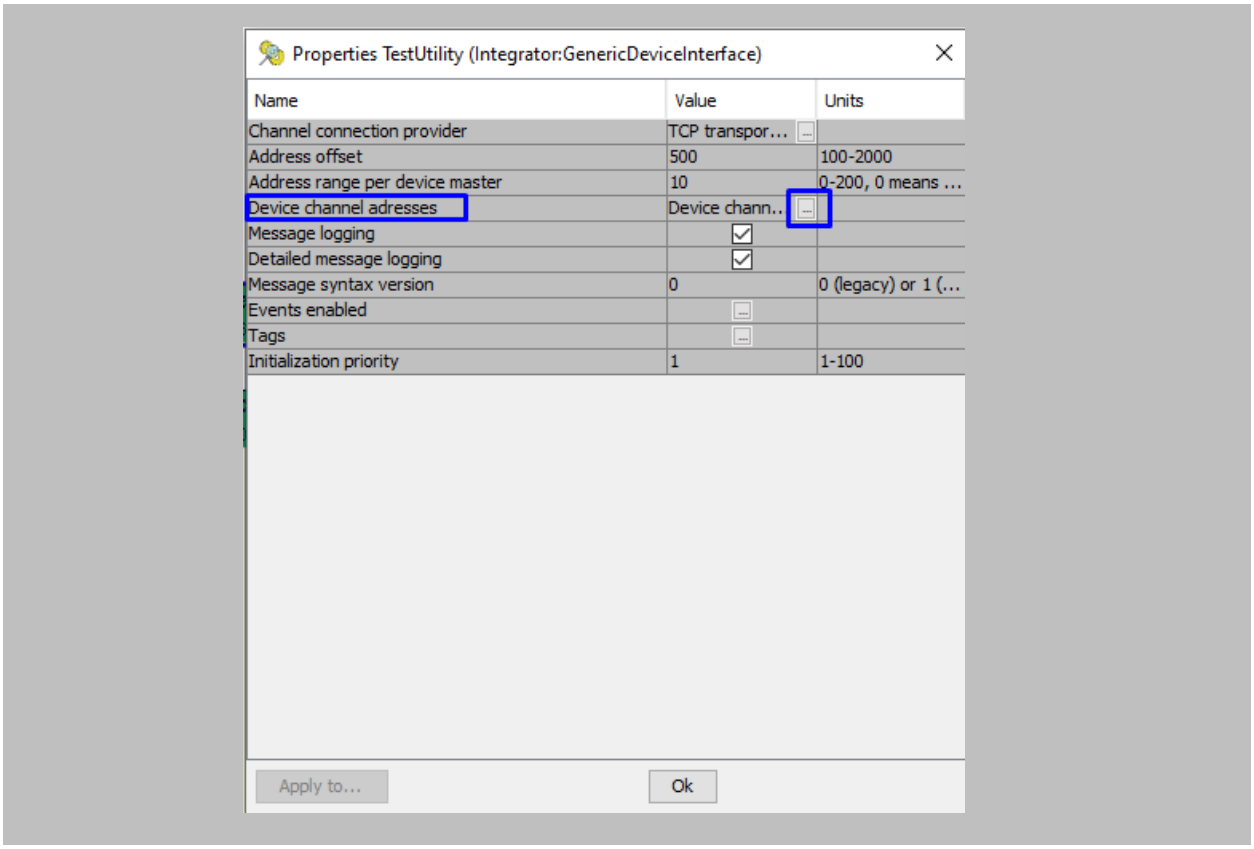


Figure 114: AEmon - Device Channel Address

STEP 6

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

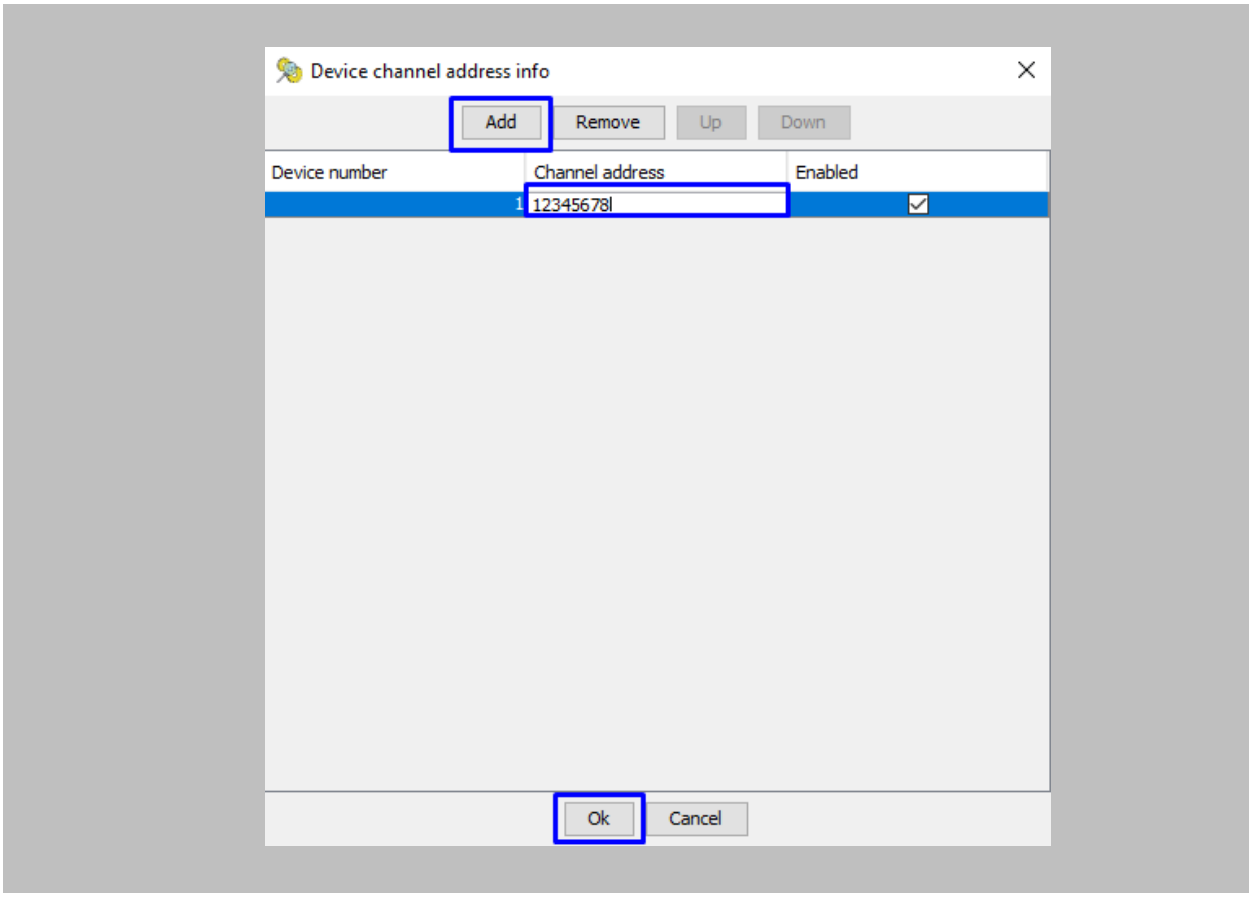


Figure 116: AEmon - Add Channel Address

STEP 7

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

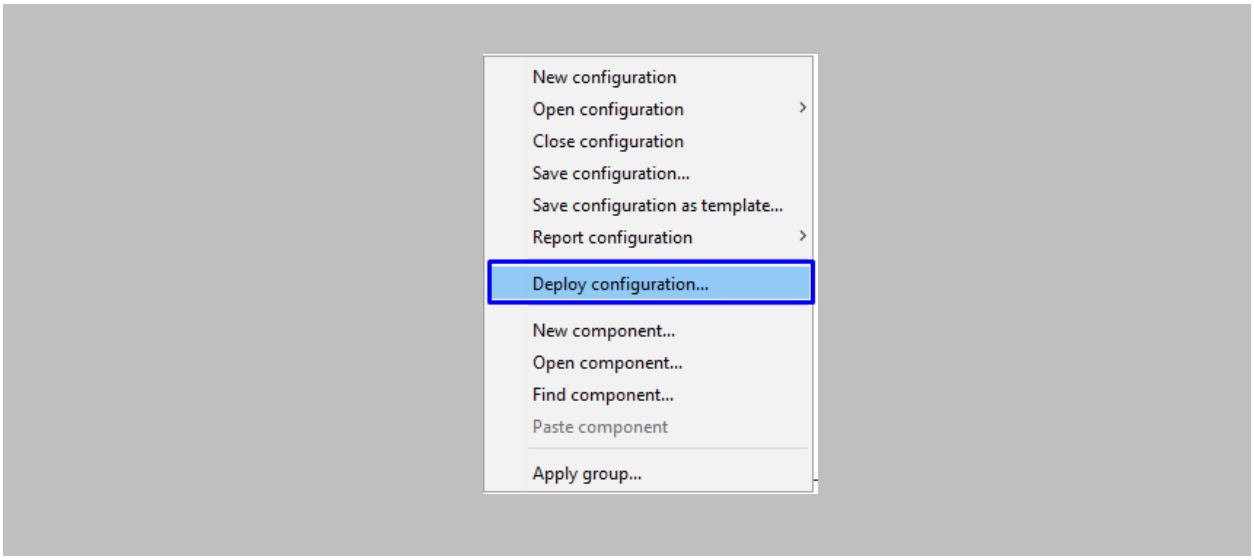


Figure 115: AEmon - Deploy Configuration

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.

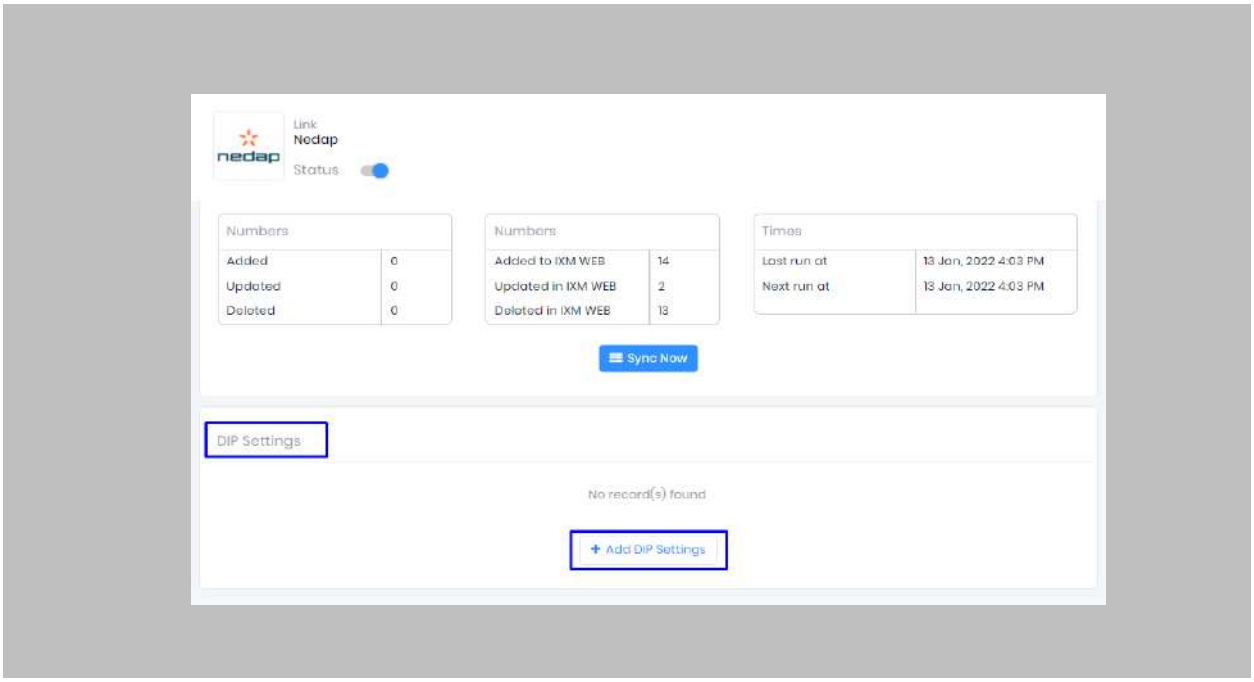


Figure 116: IXM WEB - Add DIP Settings

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.

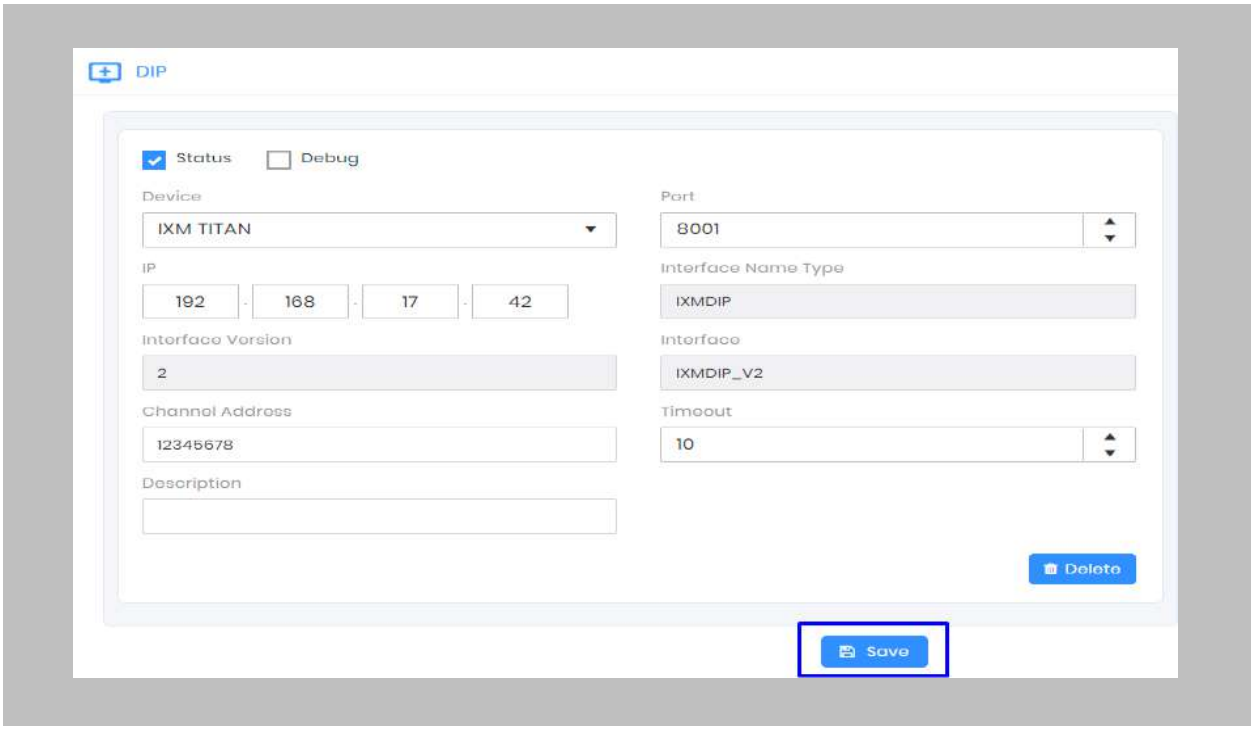


Figure 117: IXM WEB - Save DIP Settings

STEP 10

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

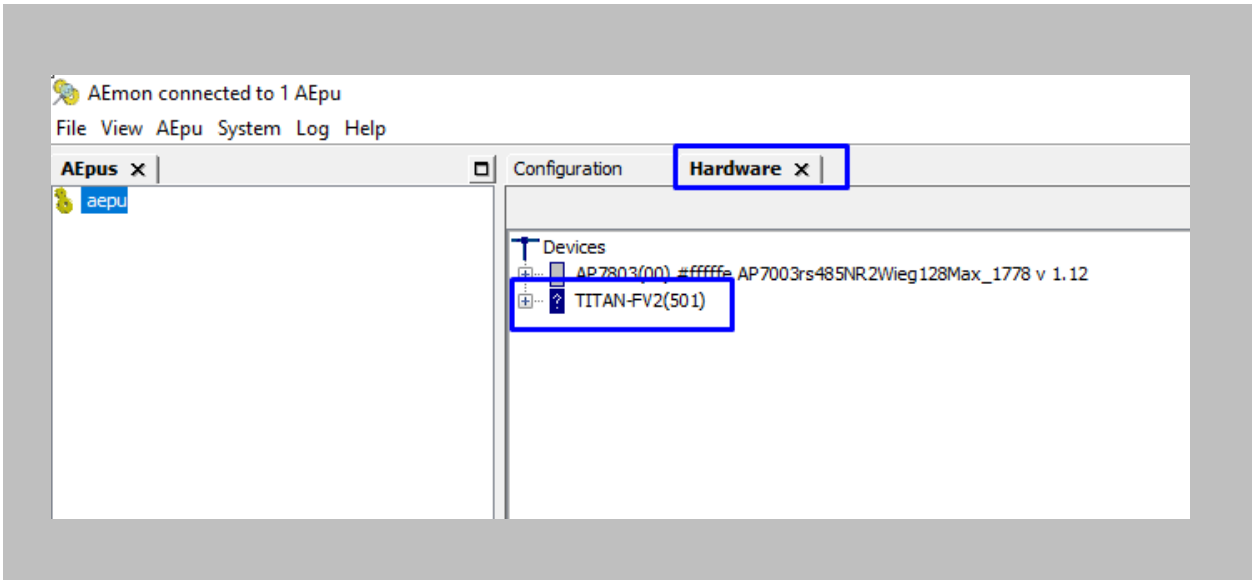


Figure 118: AEmon - DIP Device

STEP 11

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

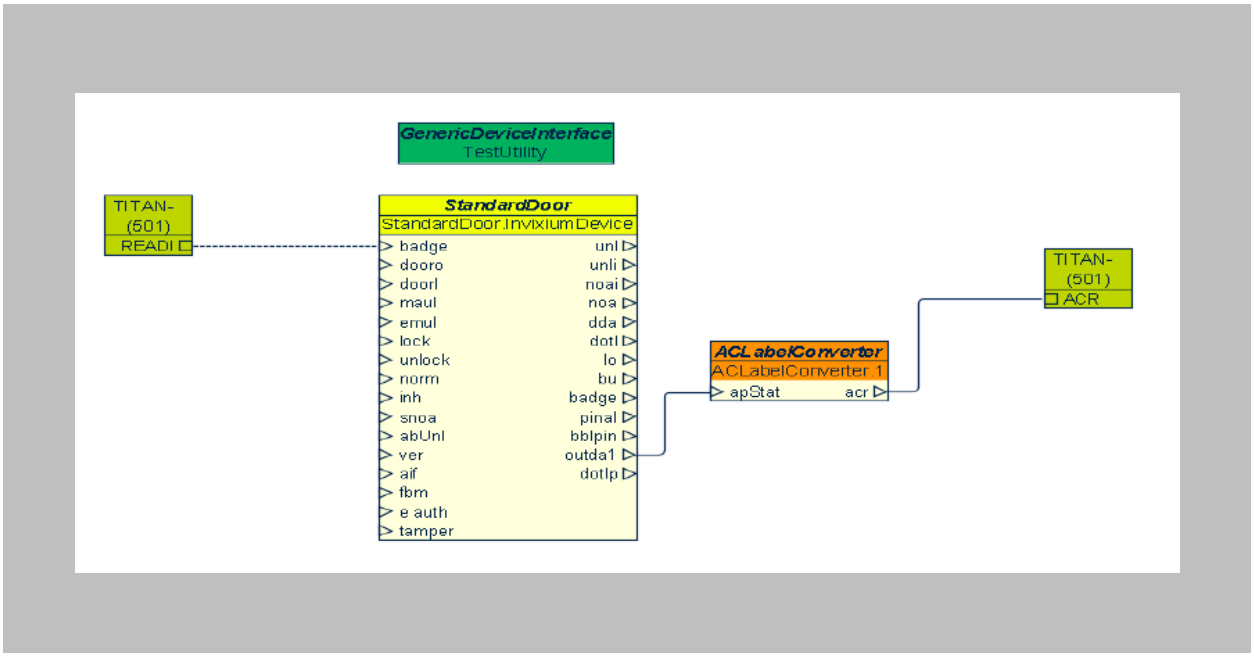


Figure 119: AEmon - DIP Device Behavior

STEP 12

Right click on Standard Door → Properties.

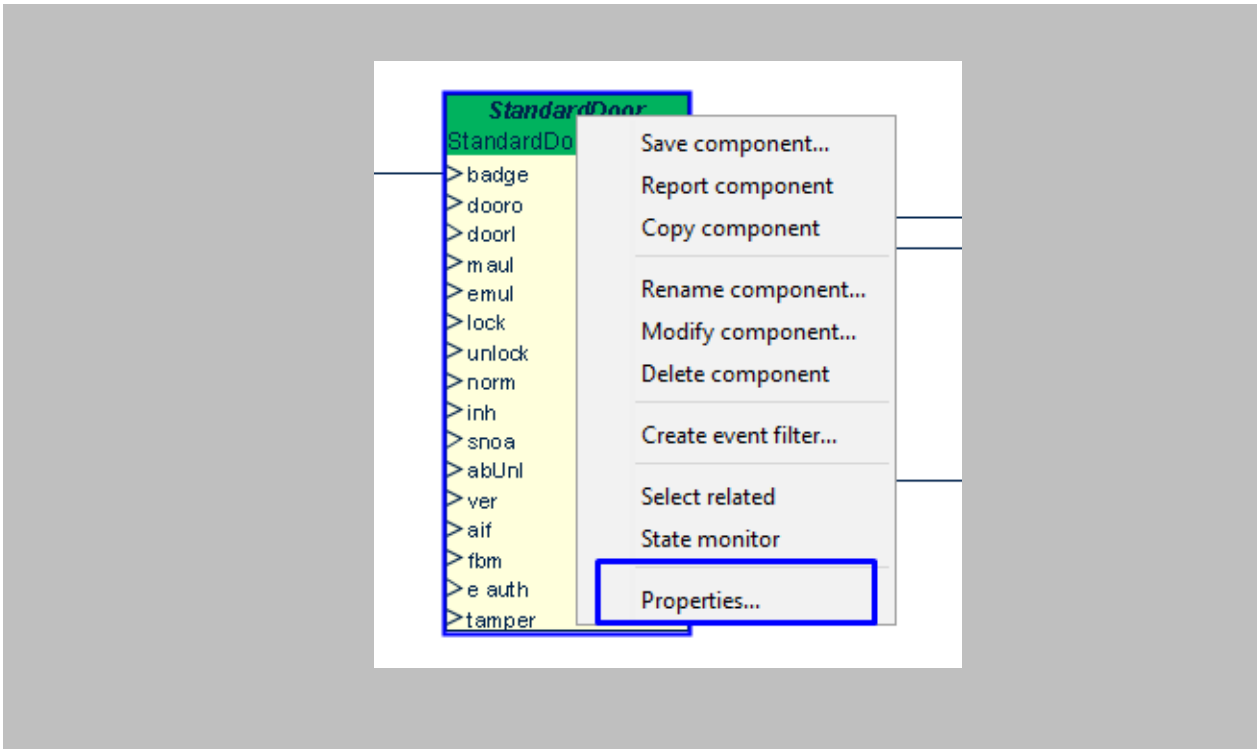


Figure 120: AEmon - Standard Door Property

STEP 13

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

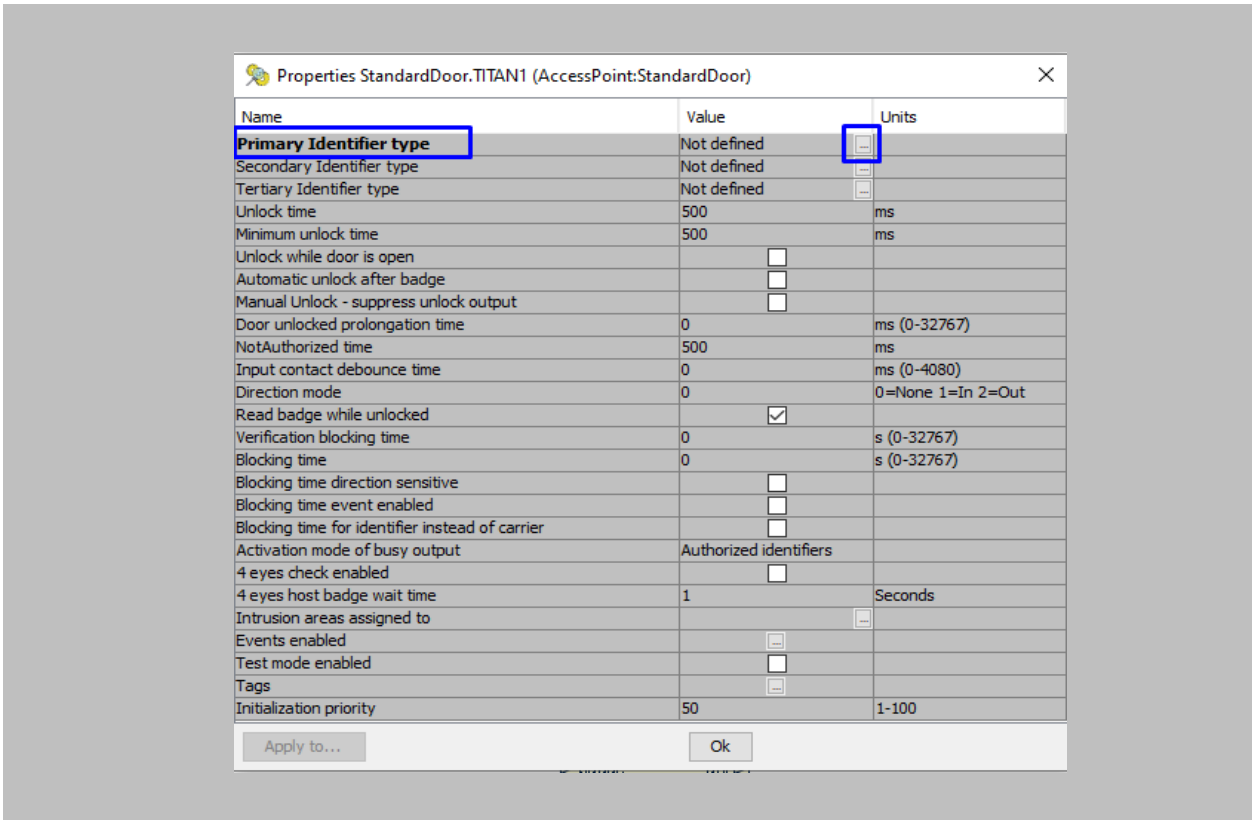


Figure 121: AEmon DIP - Primary Identifier Type

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

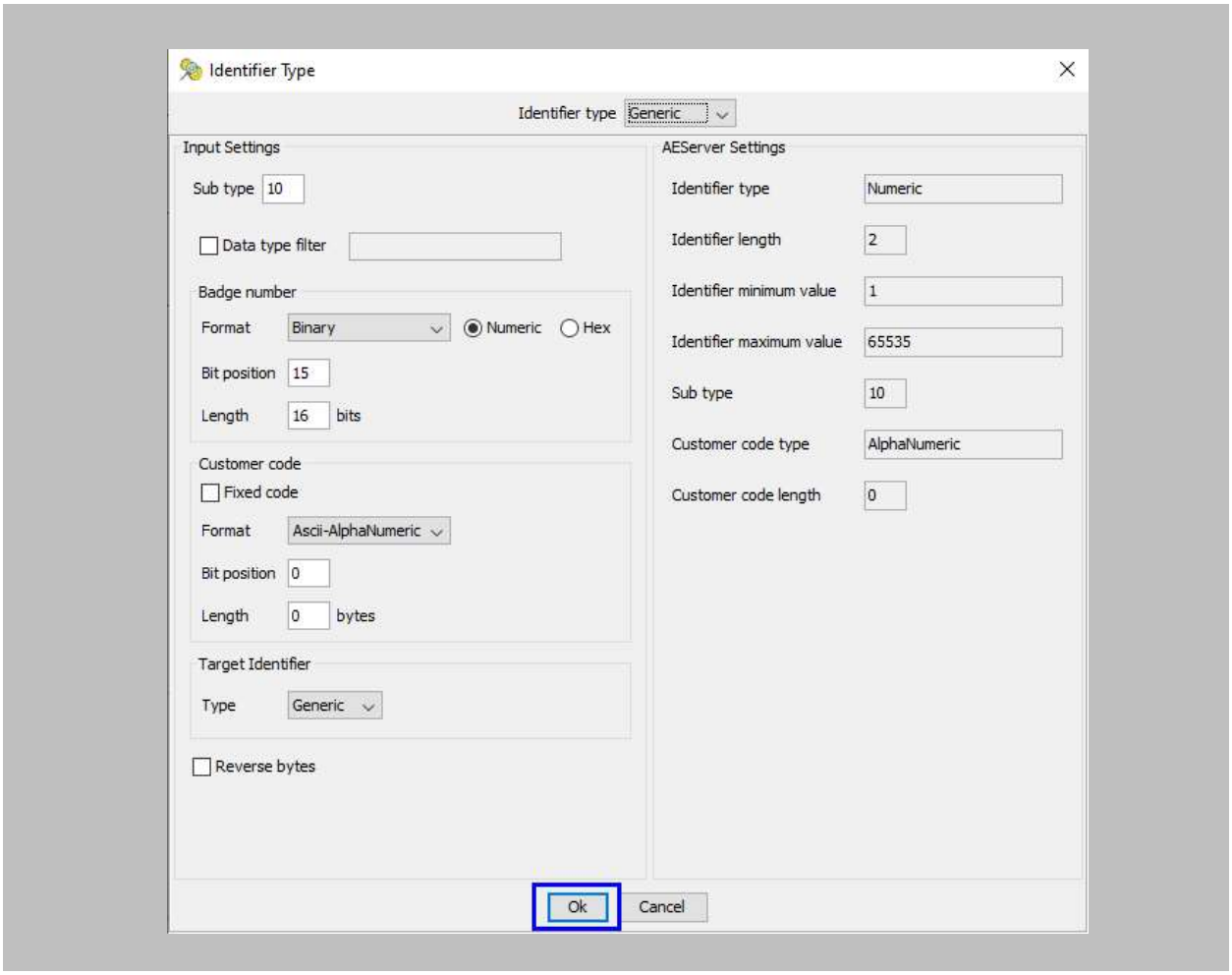


Figure 122: AEmon DIP - Primary Identifier Configuration

STEP 14

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

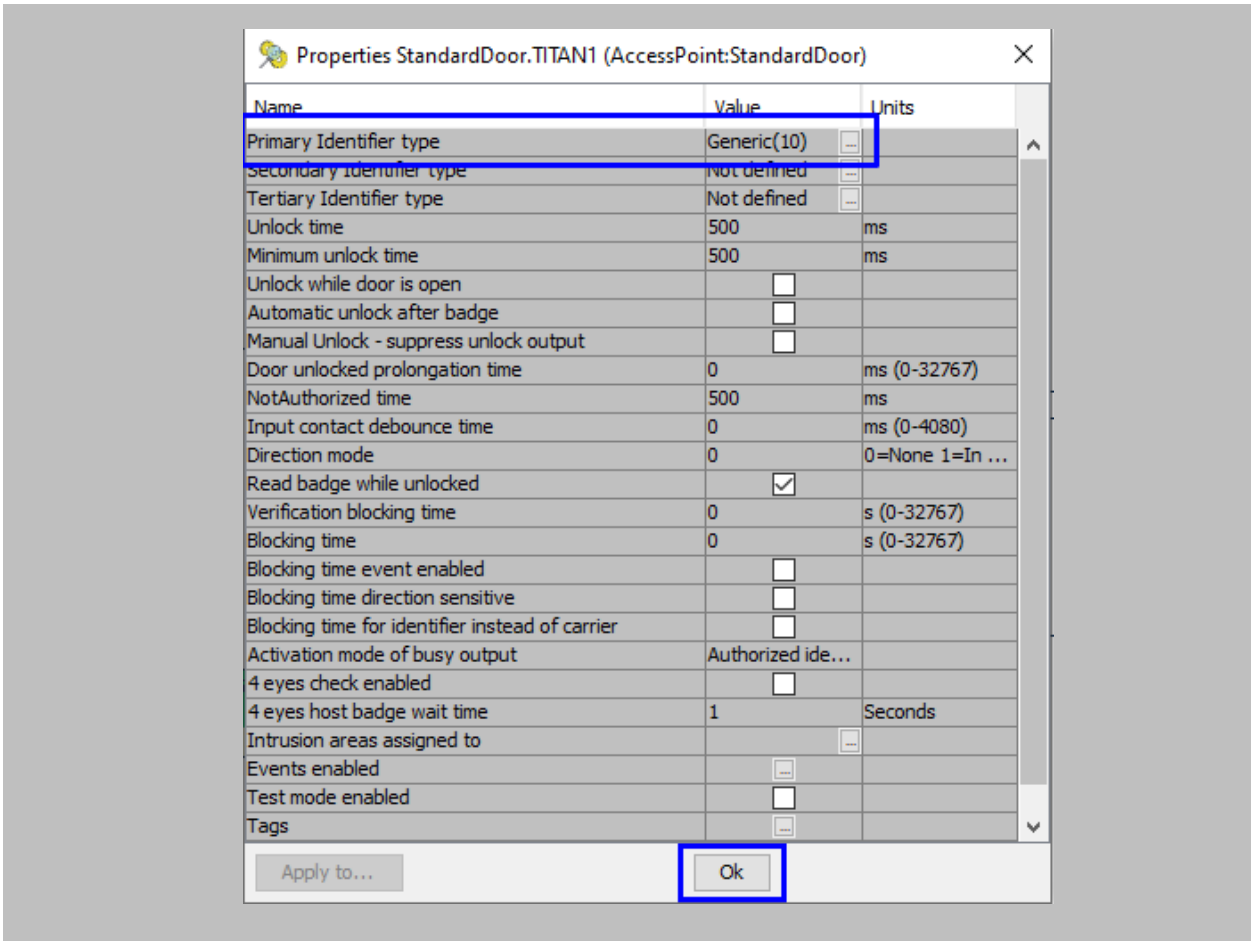


Figure 123: AEmon DIP - Generic Primary Identifier Type

STEP 15

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

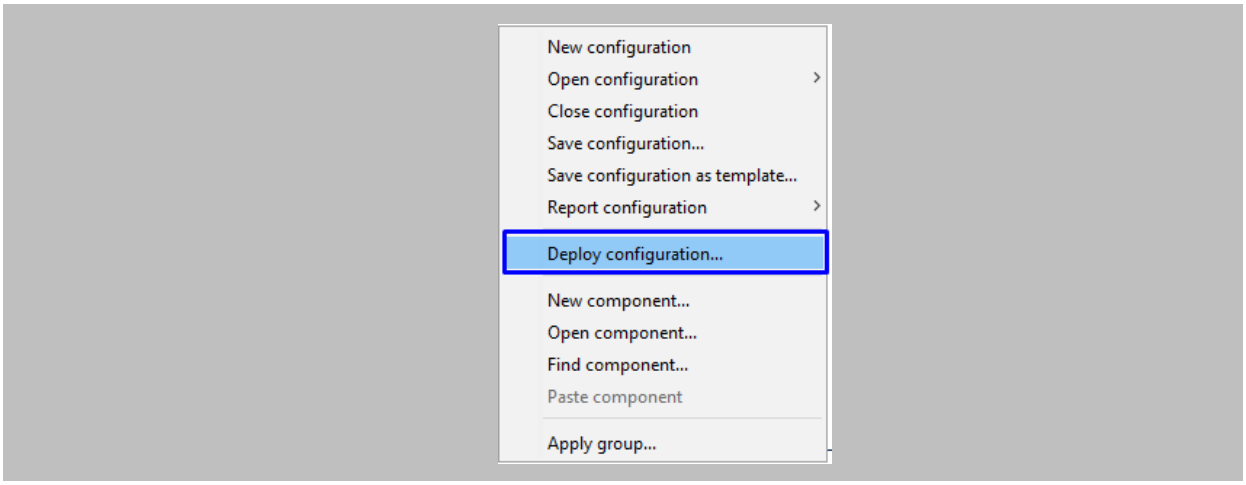


Figure 124: AEmon - Deploy Configuration

18. 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.

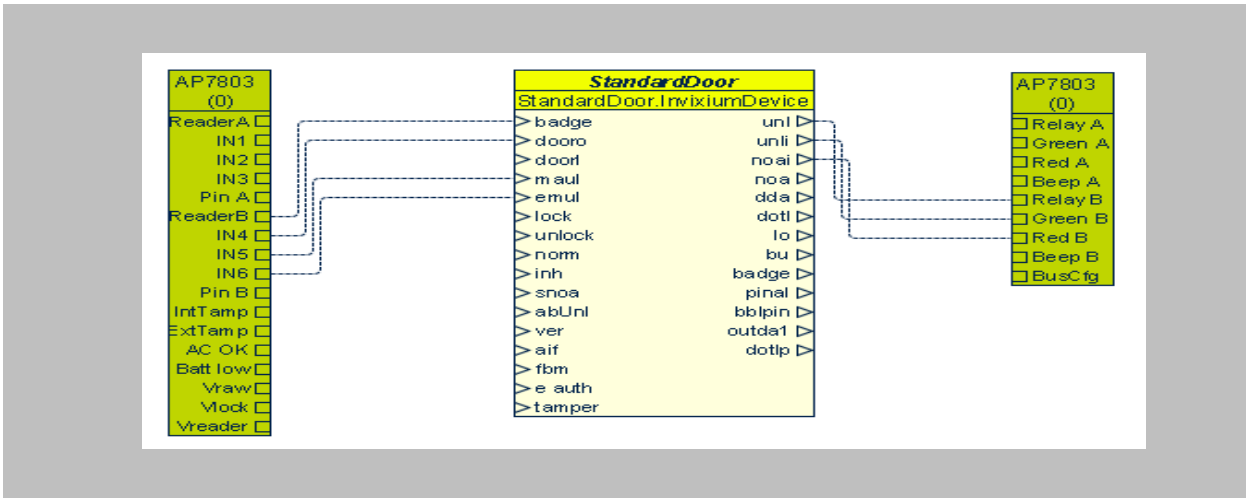


Figure 125: AEmon - Wiegand Device Behavior

STEP 3

Right Click on Standard Door → Properties.

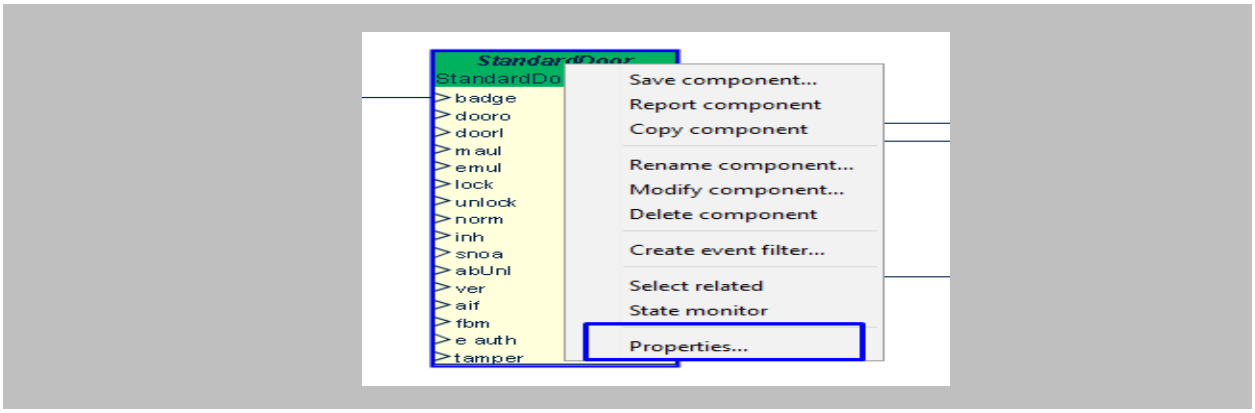


Figure 126: AEmon - Standard Door Property

STEP 4

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

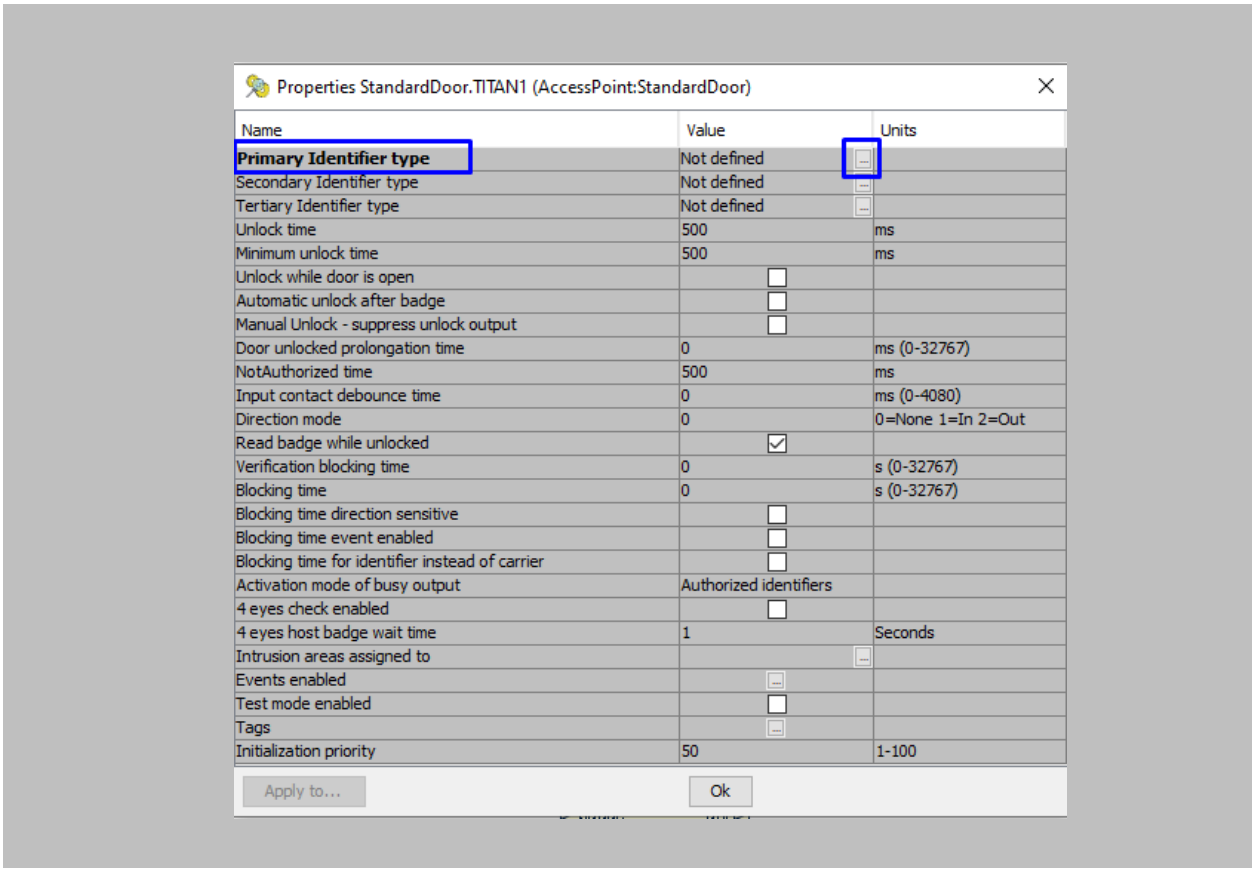


Figure 127: AEmon Wiegand – Primary Identifier Type

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

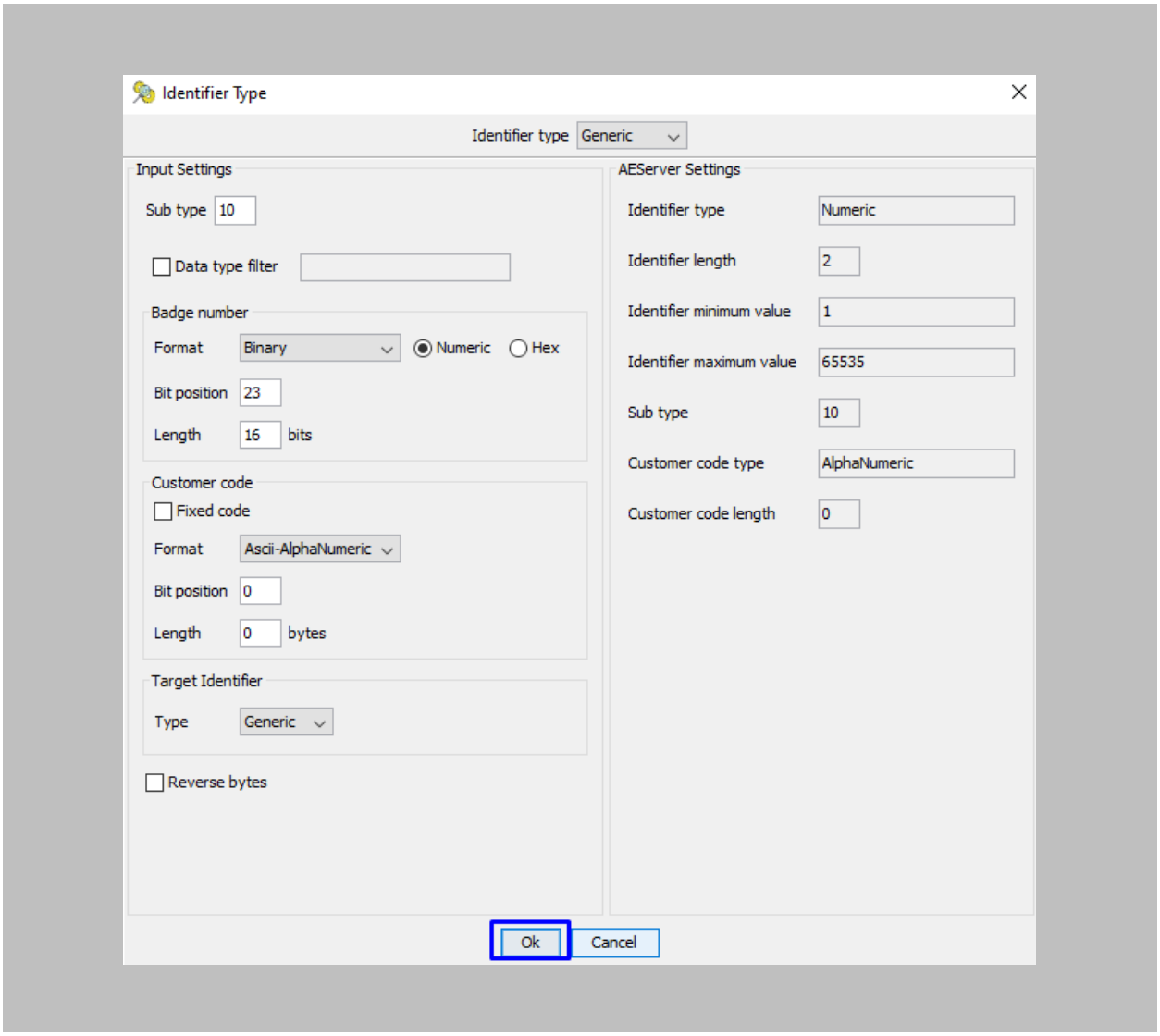


Figure 128: AEmon Wiegand - Configure Primary Identifier Type

STEP 5

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

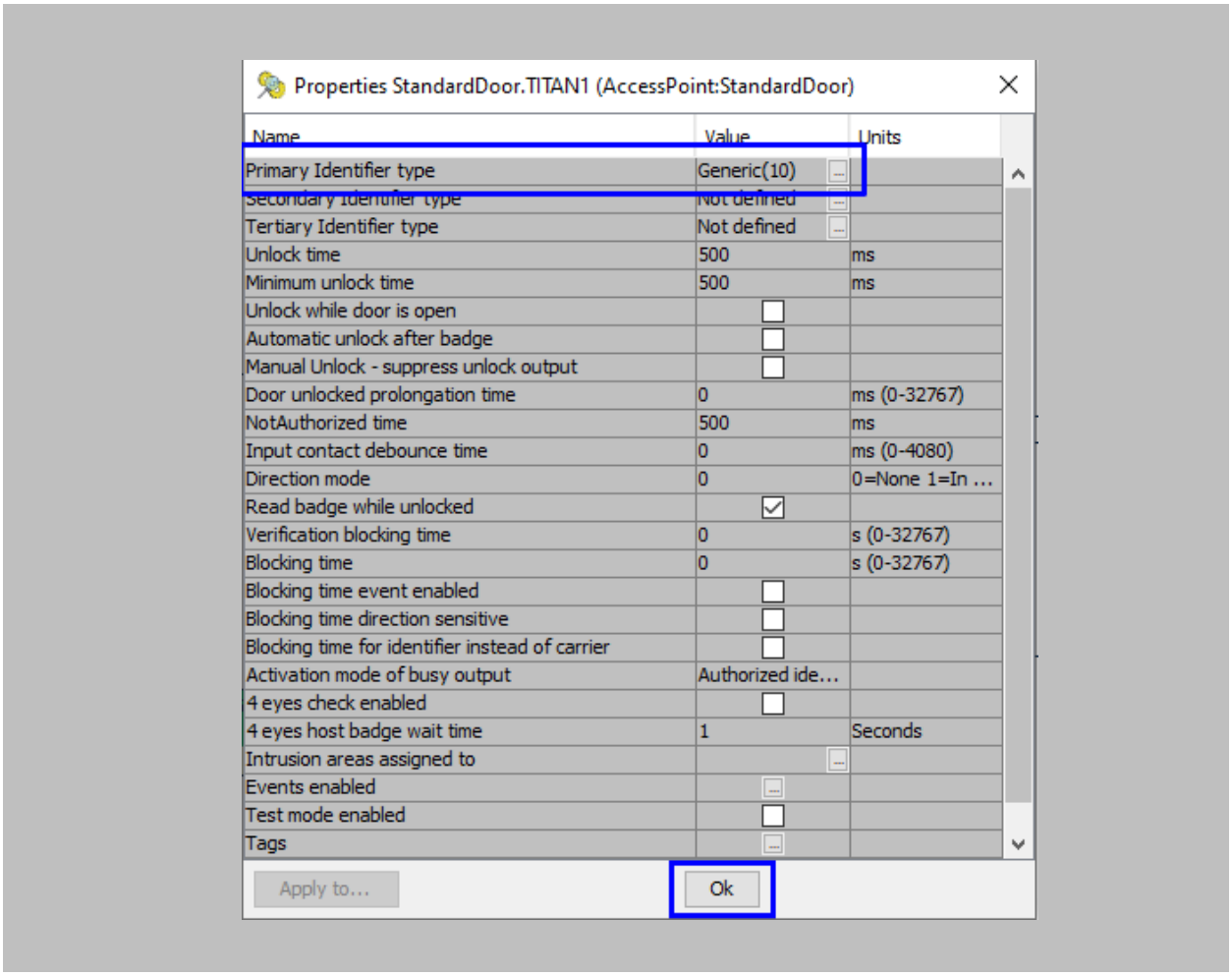


Figure 129: AEmon Wiegand- Generic Primary Identifier Type

STEP 6

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

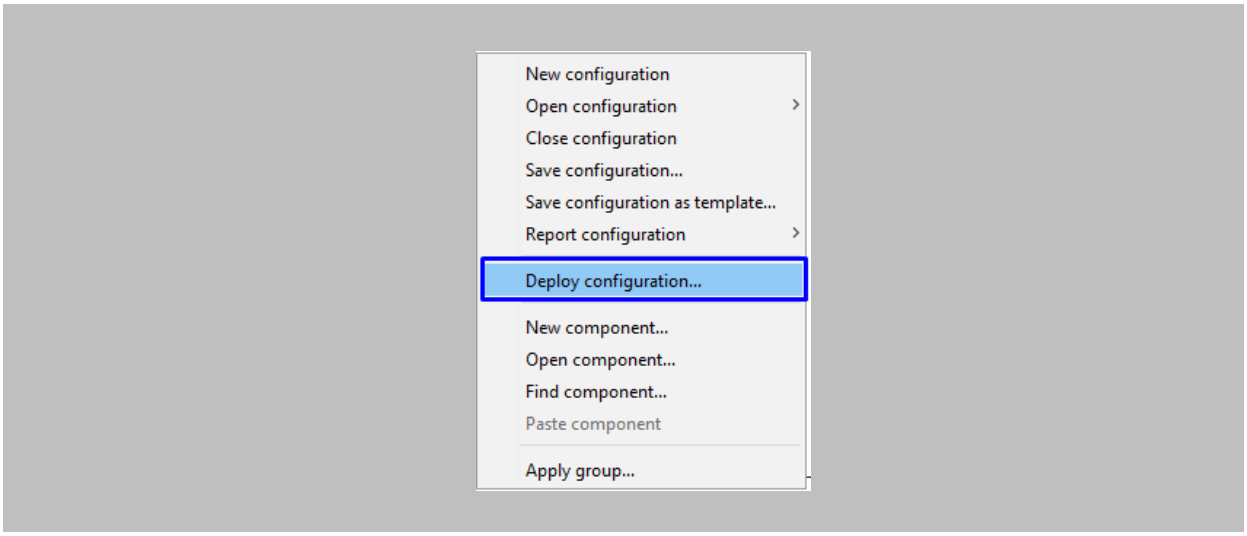


Figure 130: AEmon Wiegand- Deploy Configuration

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 on the right-hand side.

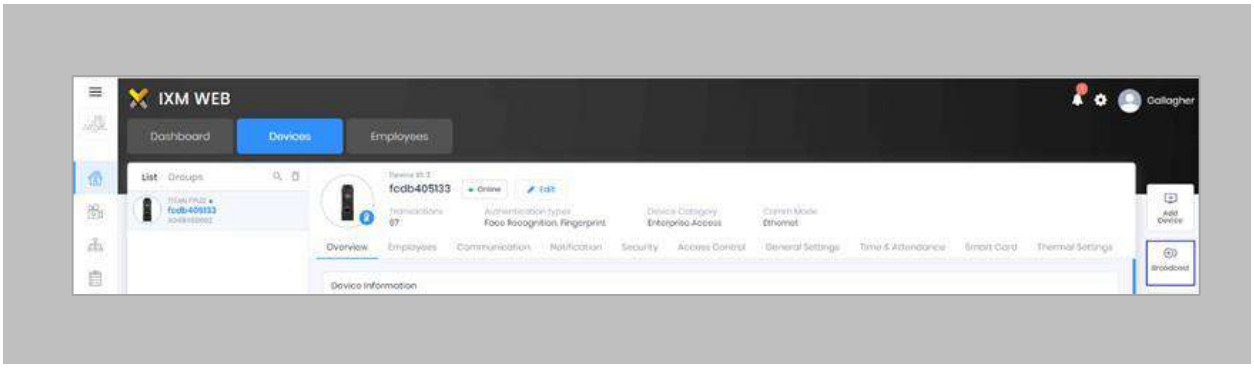


Figure 131: IXM WEB - Broadcast Option

STEP 2

Scroll down to the **Access Control** section and check the **Wiegand Output** option.

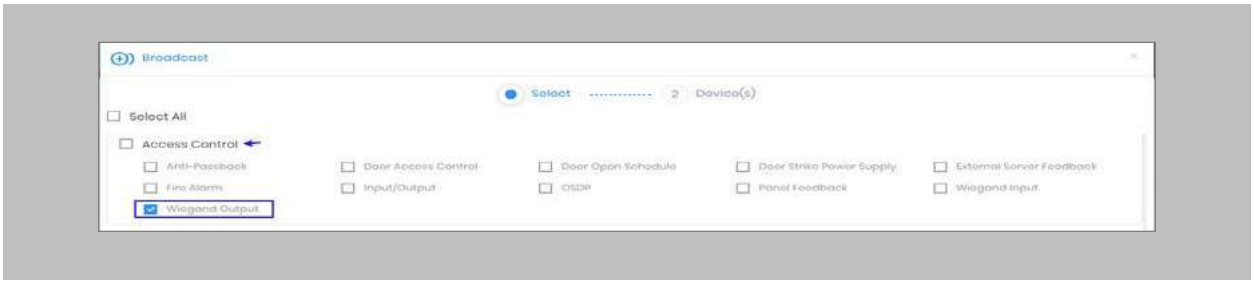


Figure 132: IXM WEB - Wiegand Output Selection in Broadcast

STEP 3

Click **Broadcast.**

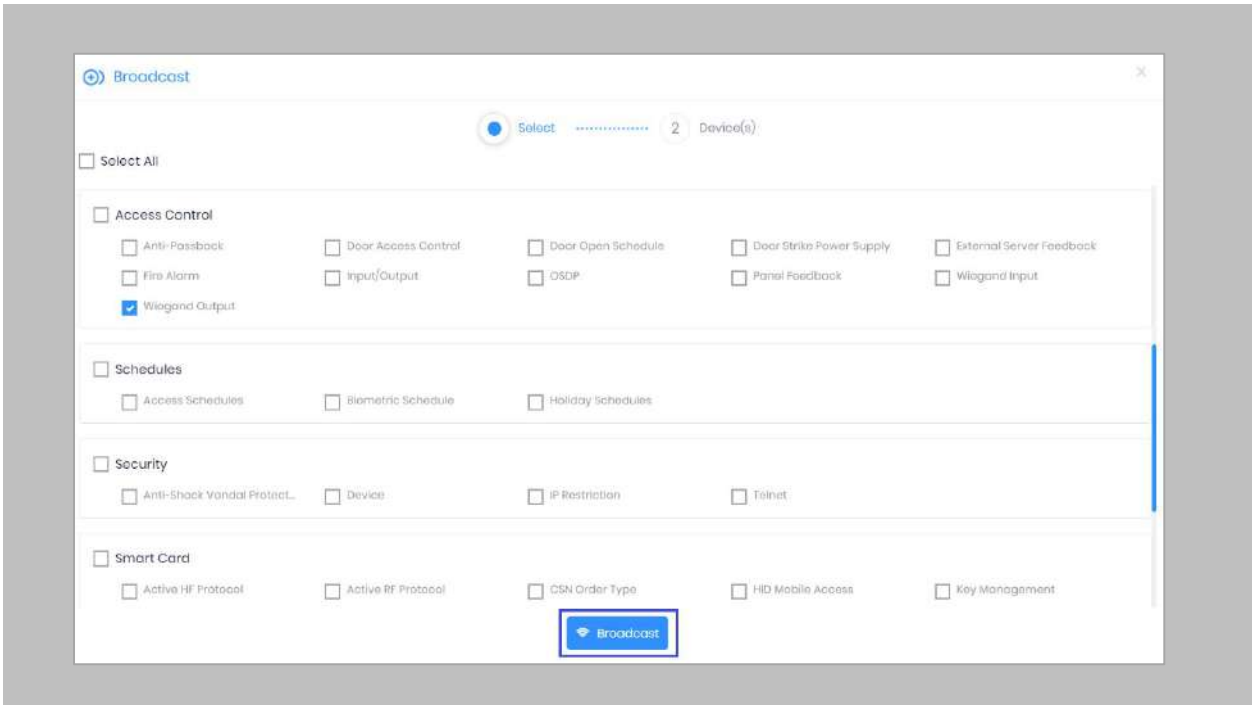


Figure 133: IXM WEB - Broadcast Wiegand Output Settings

STEP 4

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.

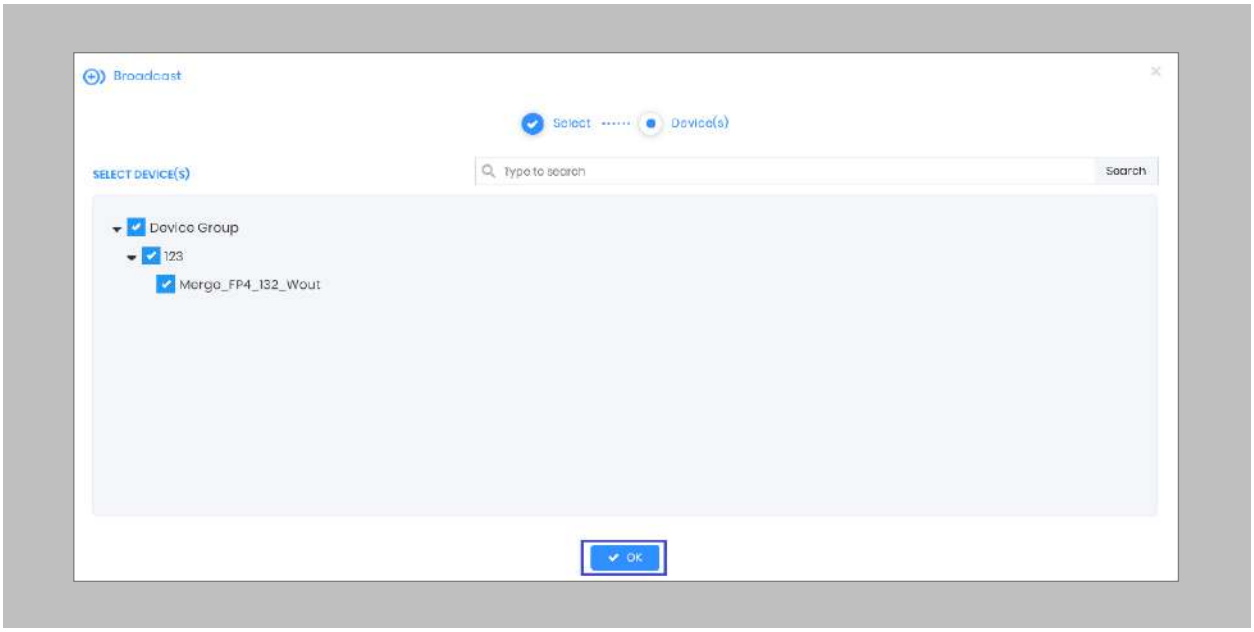


Figure 134: IXM WEB - Broadcast to Devices

Note: Popup will display devices of the same category only.

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.

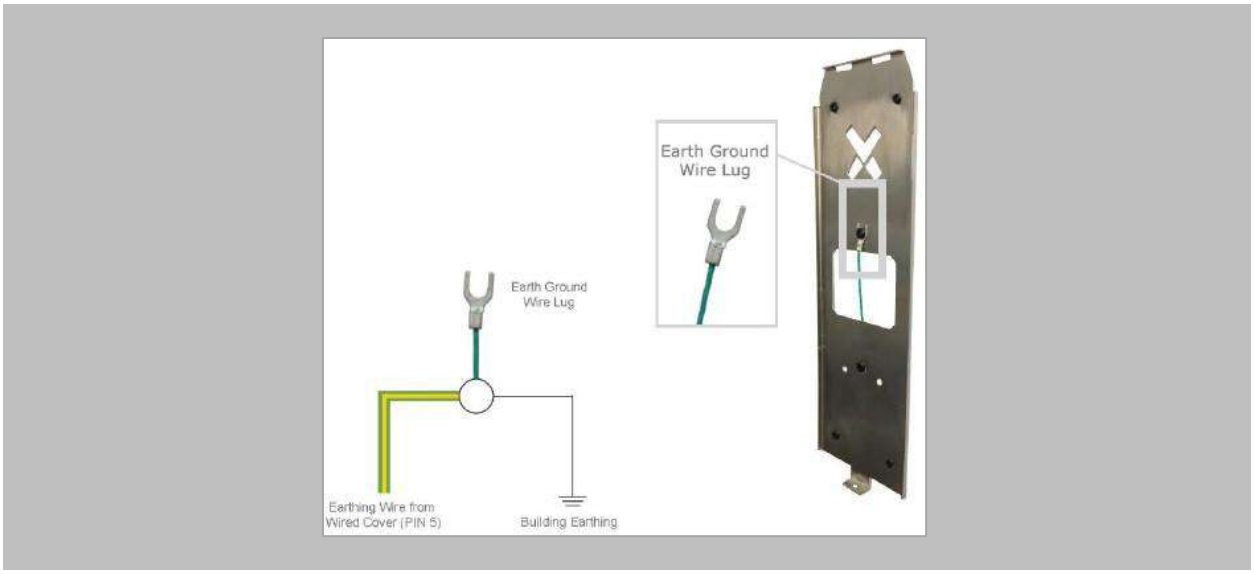
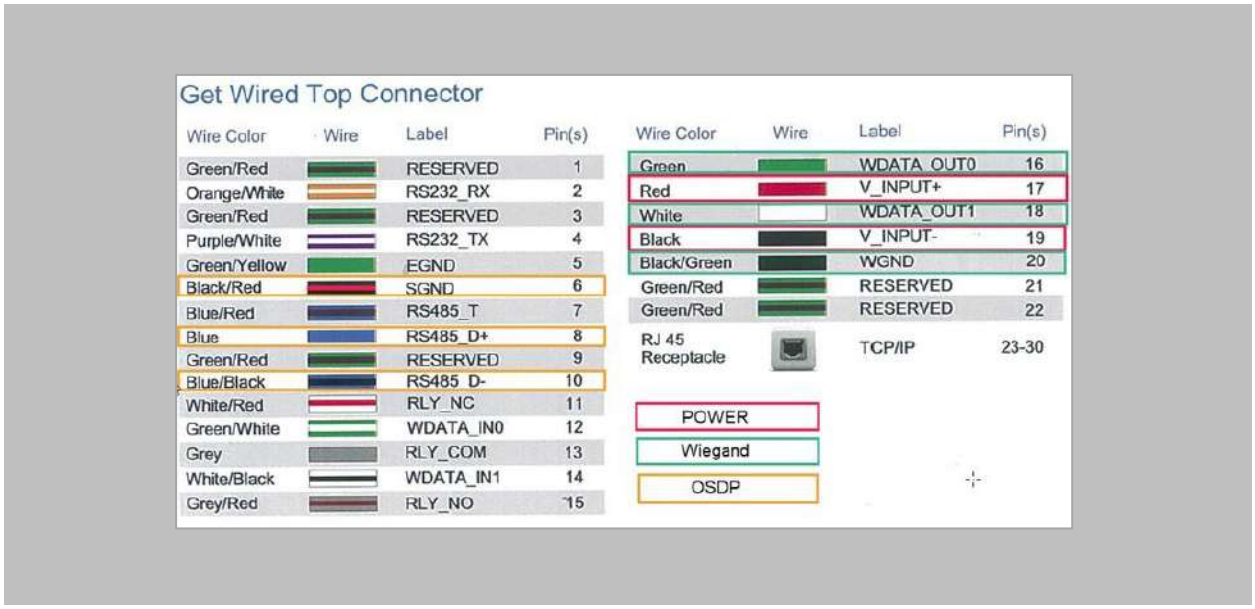


Figure 135: Earth Ground Wiring

WIRING

Figure 136: IXM TITAN – Top & Bottom Connector Wiring



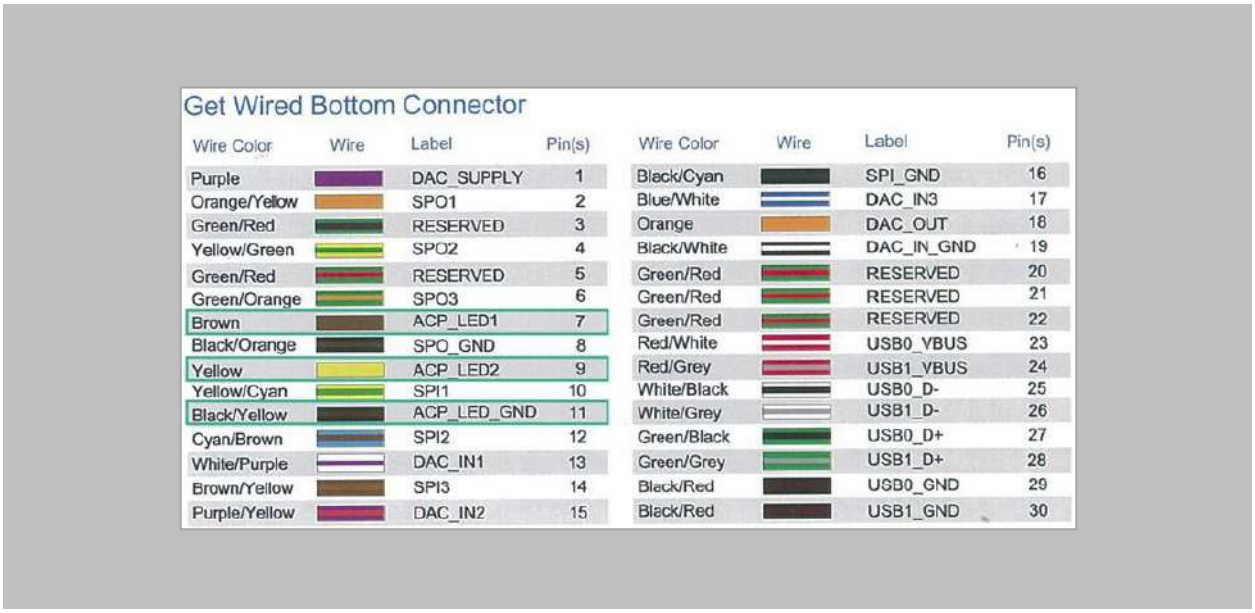


Figure 137: Power, Wiegand & OSDP Wires

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

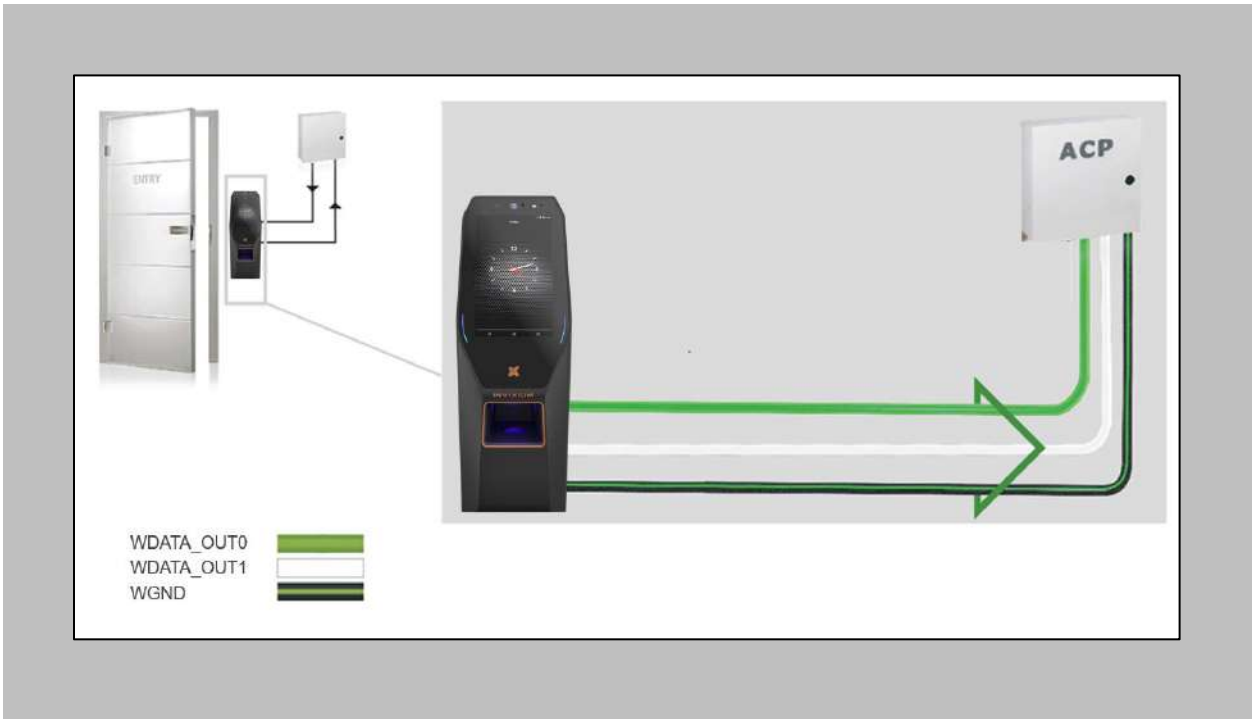


Figure 138: IXM TITAN - Wiegand

Wiegand Connection with Panel Feedback

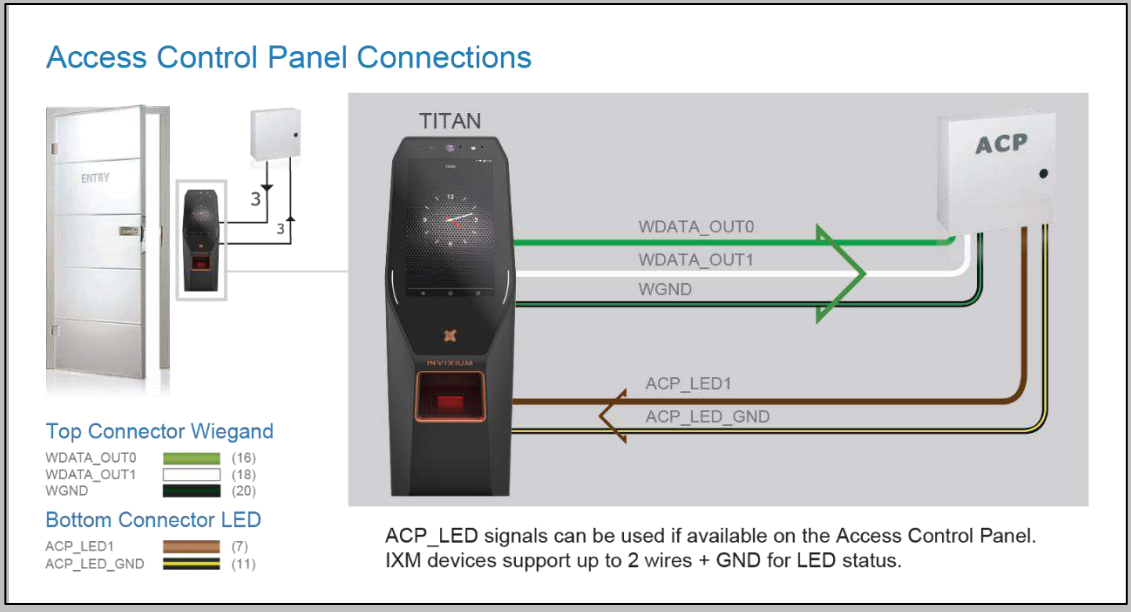


Figure 139: IXM TITAN - Panel Feedback

OSDP Connections

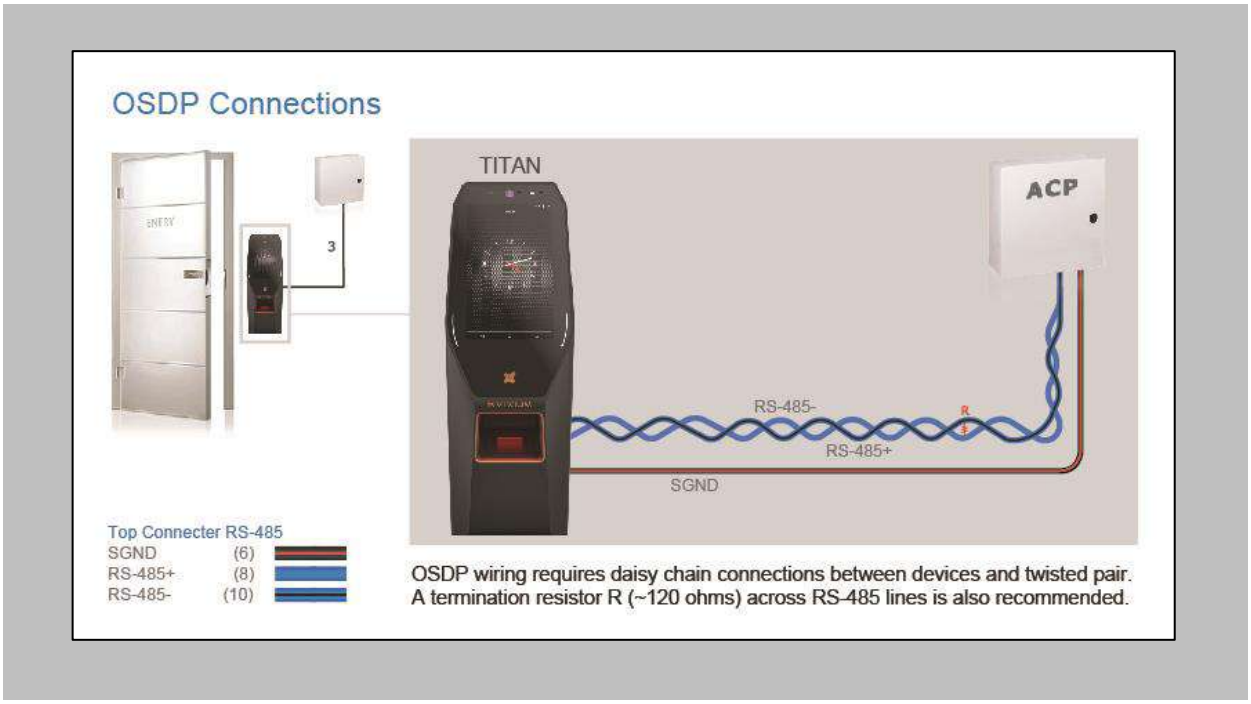


Figure 140: IXM TITAN - OSDP Connections

19. 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.

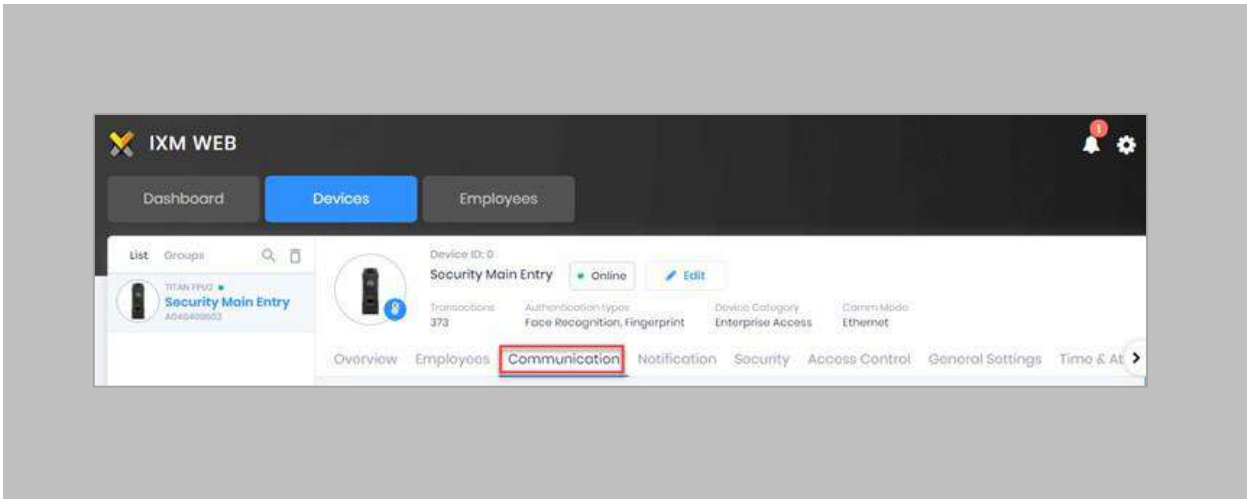


Figure 141: IXM WEB - Device Communication Settings

STEP 4

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

Figure 142: 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.

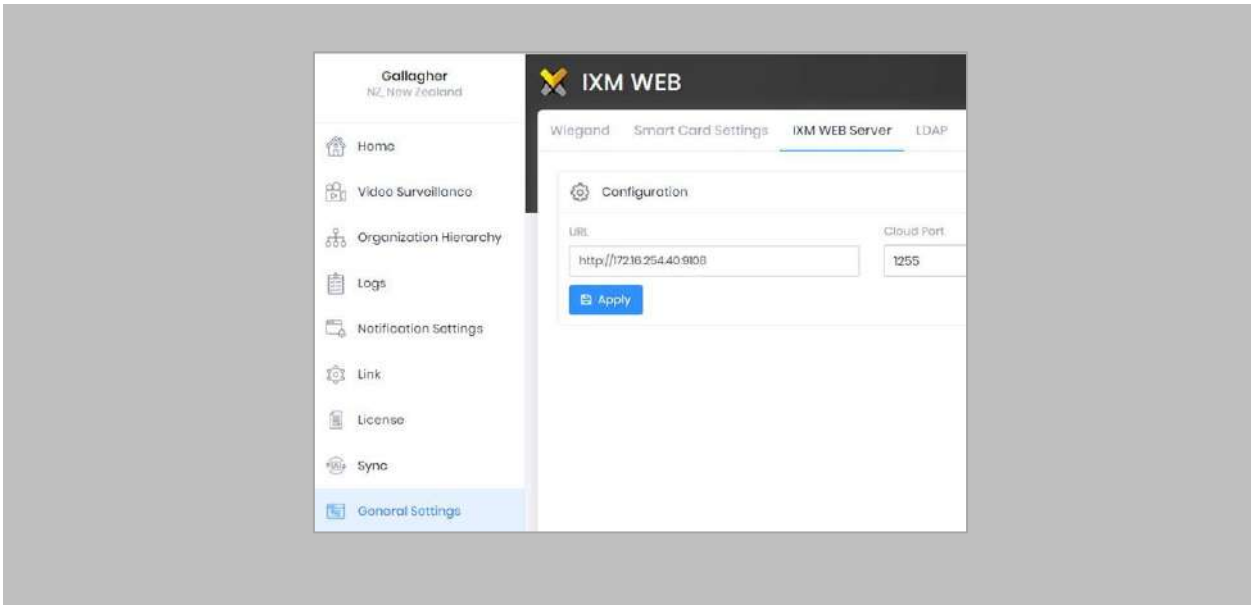


Figure 143: IXM WEB - Server URL Setting from General Setting

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.

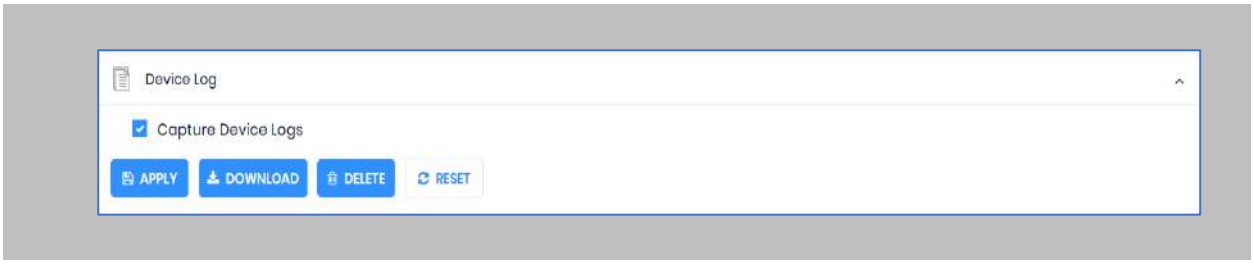


Figure 144: IXM WEB - Enable Device Logs

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

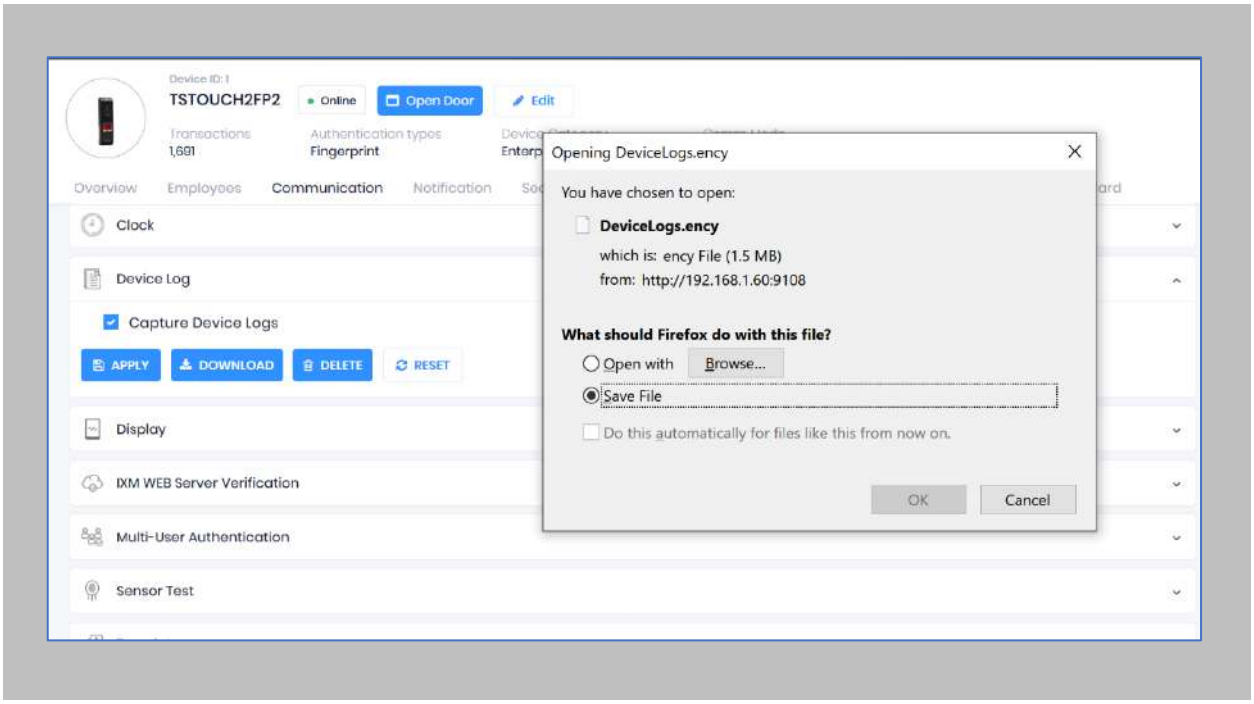


Figure 145: Save Device Log File

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 7: Logs Folder Location

20. Support

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

21. 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.