IXM WEB Integration with AEOS by Nedap

Installation Instructions

V3.0

P/N XAD-TPI-004-03G

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	2.3.0.0
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 4.8
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
IXM WEB 2.2.330.0	2021.1	Yes
IXM WEB 2.3.0.0	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	

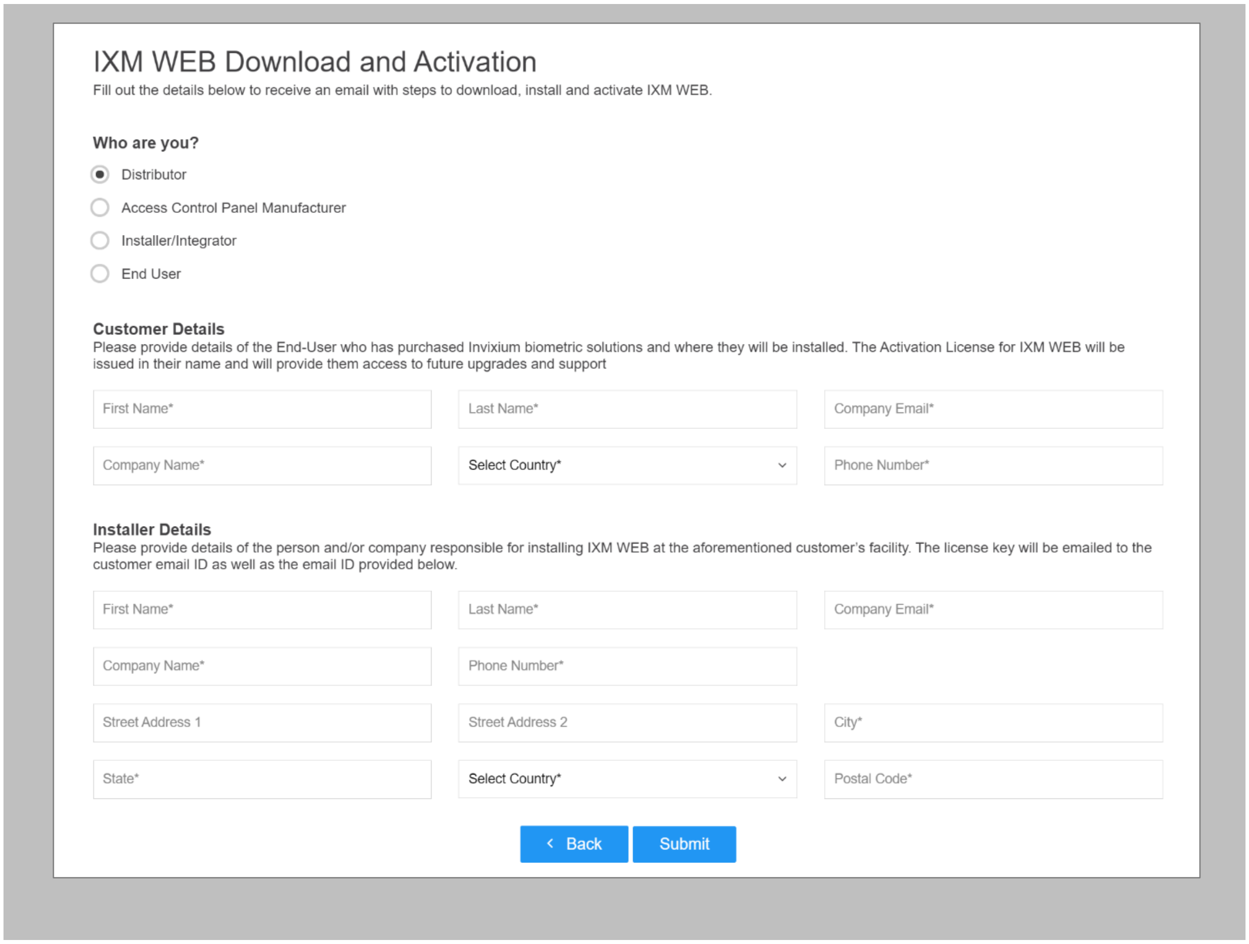
Table 2: Task List Summary

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/



IXM WEB Download and Activation

Fill out the details below to receive an email with steps to download, install and activate IXM WEB.

Who are you?

● Distributor

○ Access Control Panel Manufacturer

○ Installer/Integrator

○ End User

Customer Details

Please provide details of the End-User who has purchased Invixium biometric solutions and where they will be installed. The Activation License for IXM WEB will be issued in their name and will provide them access to future upgrades and support

First Name*	Last Name*	Company Email*
Company Name*	Select Country*	Phone Number*

Installer Details

Please provide details of the person and/or company responsible for installing IXM WEB at the aforementioned customer's facility. The license key will be emailed to the customer email ID as well as the email ID provided below.

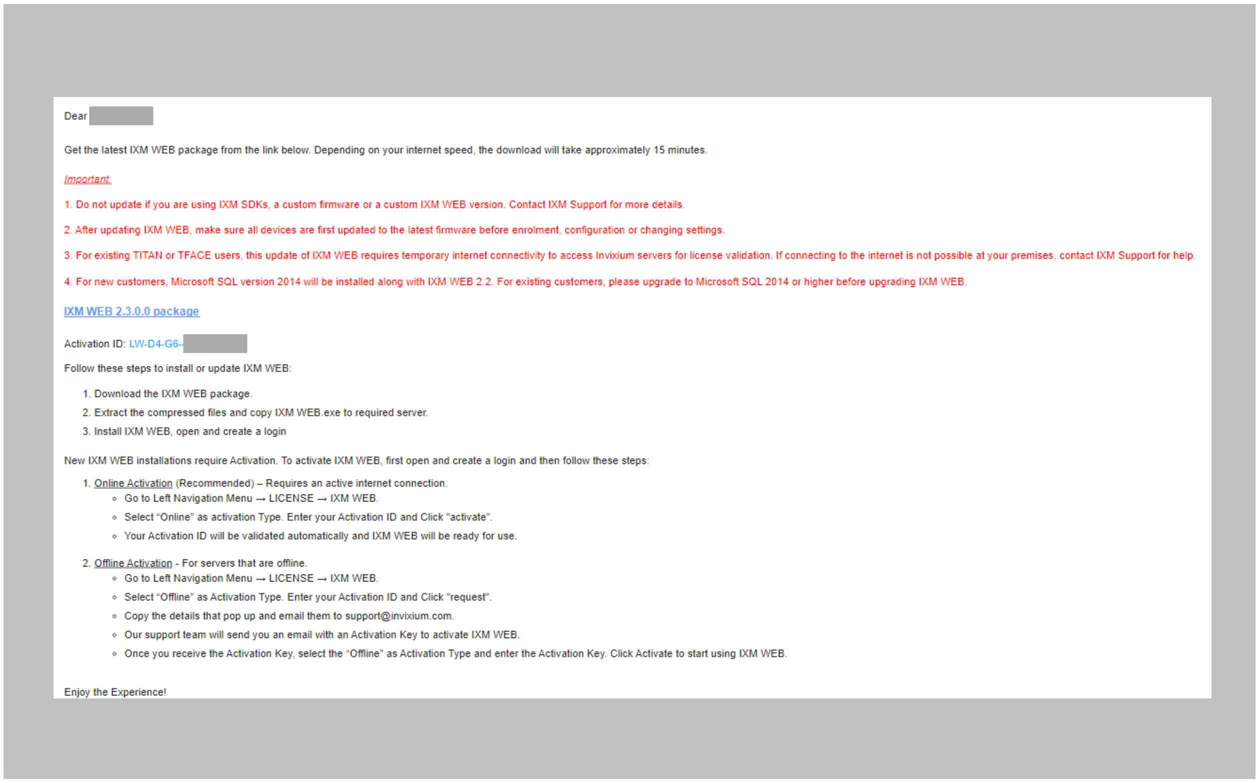
First Name*	Last Name*	Company Email*
Company Name*	Phone Number*	
Street Address 1	Street Address 2	City*
State*	Select Country*	Postal Code*

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.



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 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**.

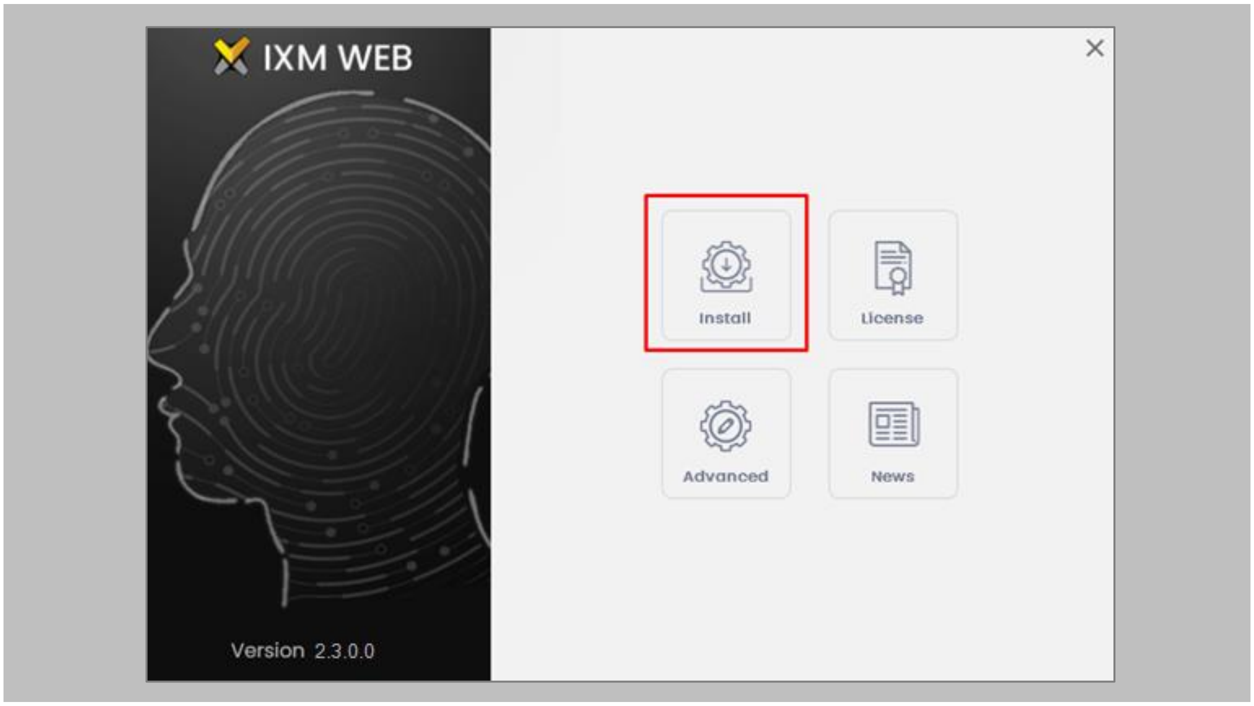


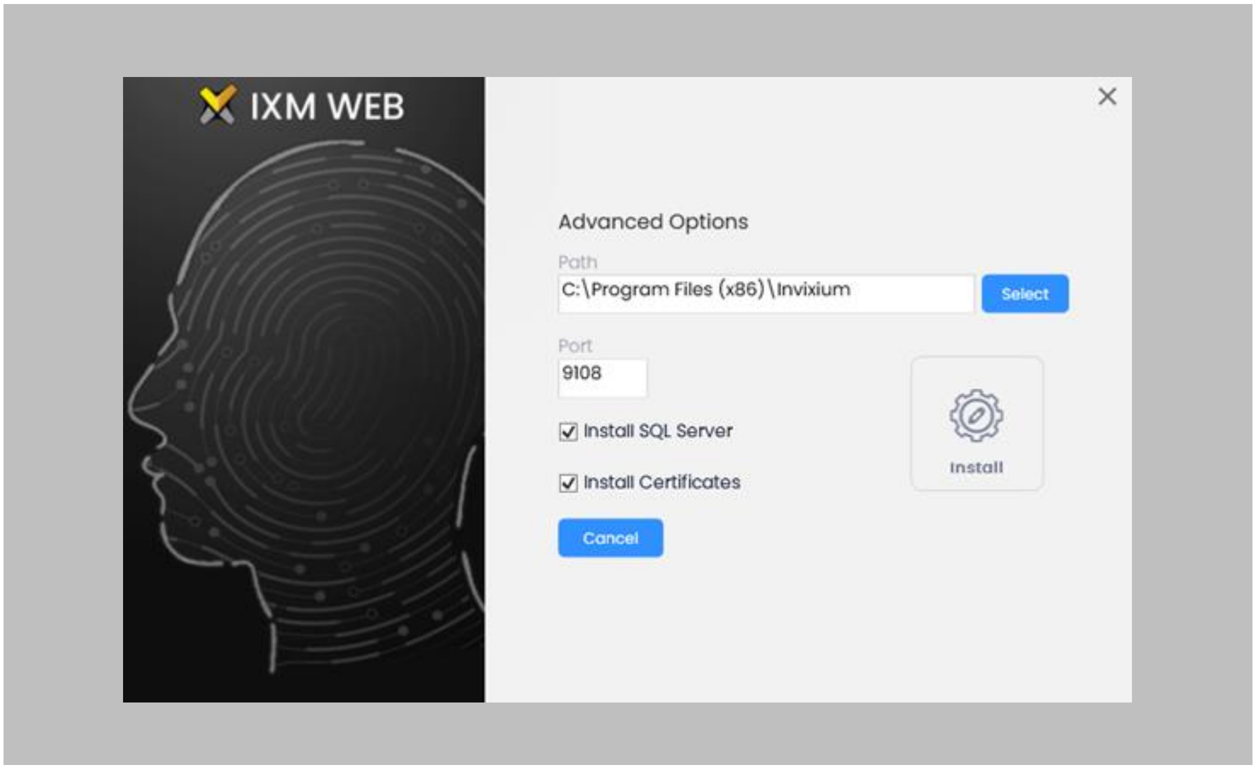
Figure 3: IXM WEB Installer

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**.



Advanced Options

Path: C:\Program Files (x86)\Invixium

Port: 9108

☑ Install SQL Server

☑ Install Certificates

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.

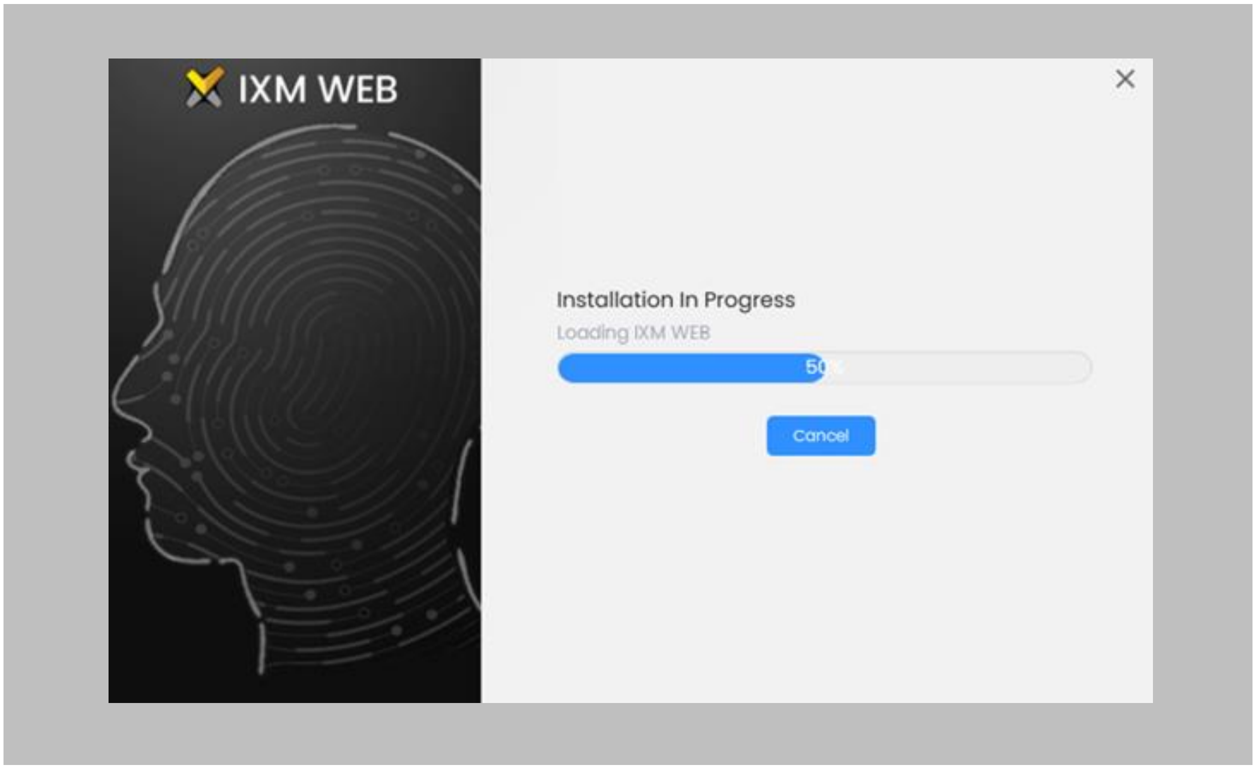


Figure 5: IXM WEB Installation

STEP 6

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

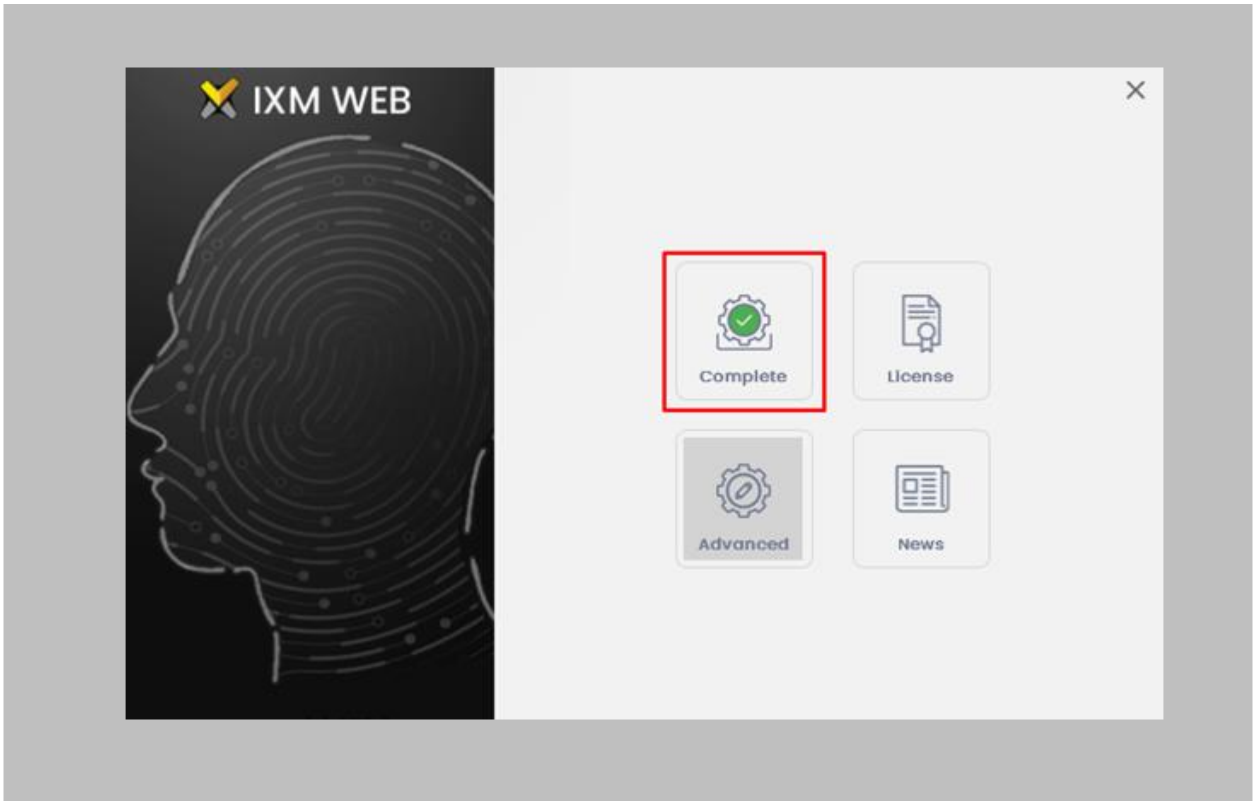


Figure 6: IXM WEB Installation Completed

STEP 7

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

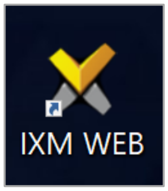
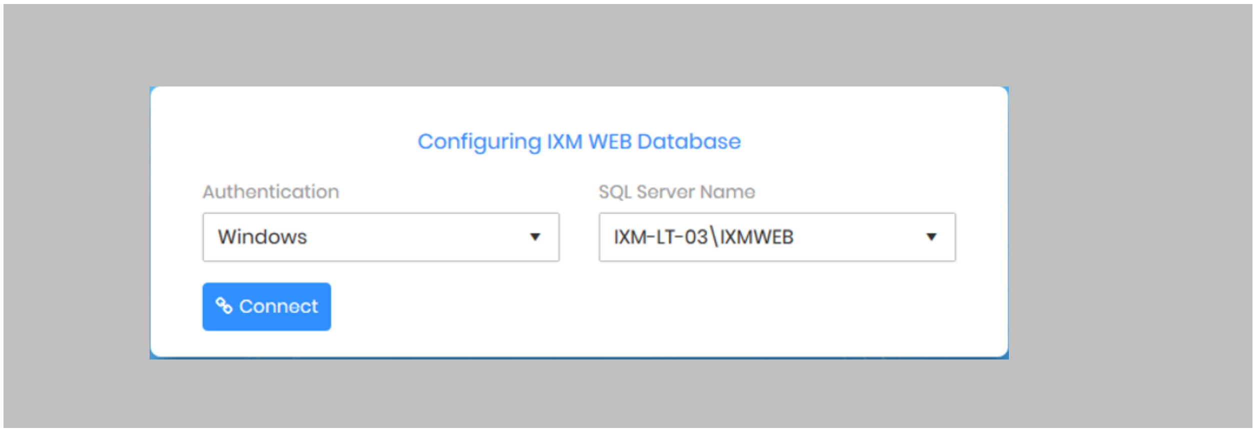


Figure 7: IXM WEB Icon - Desktop Shortcut

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.



Configuring IXM WEB Database

Authentication: Windows

SQL Server Name: IXM-LT-03\IXMWEB

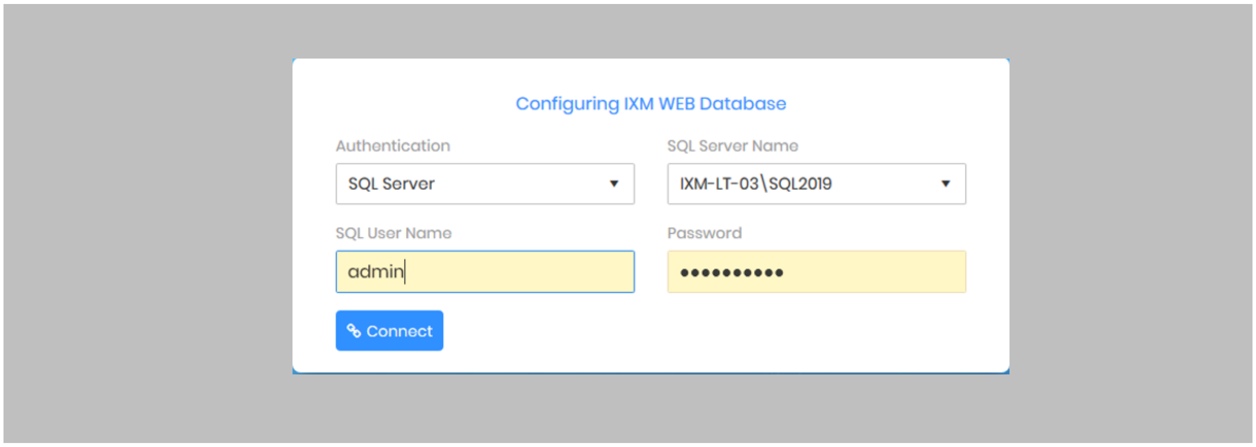
Figure 8: IXM WEB Database Configuration

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.



Configuring IXM WEB Database

Authentication: SQL Server

SQL Server Name: IXM-LT-03\SQL2019

SQL User Name: admin

Password: ●●●●●●●●●●●

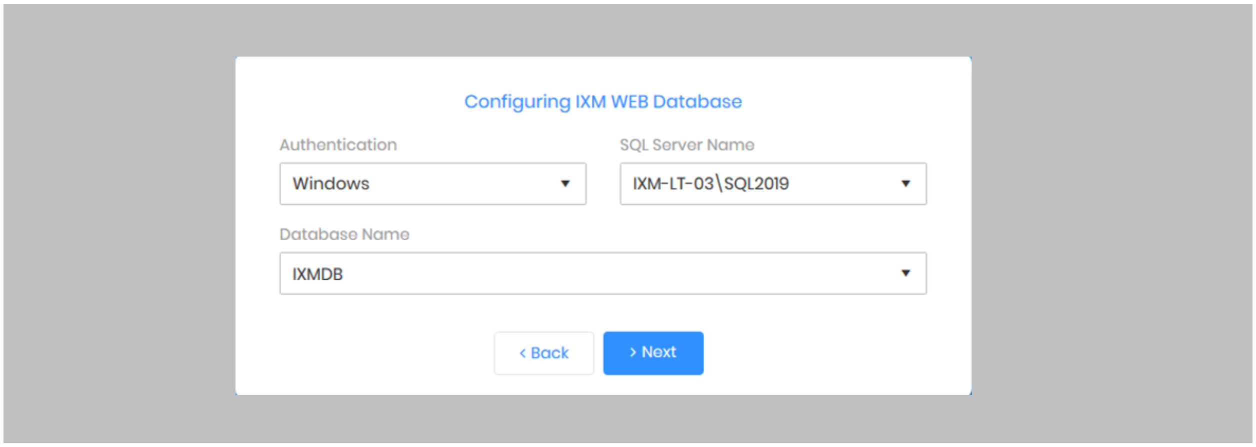
Figure 9: SQL Database Configuration

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.



Configuring IXM WEB Database

Authentication: Windows

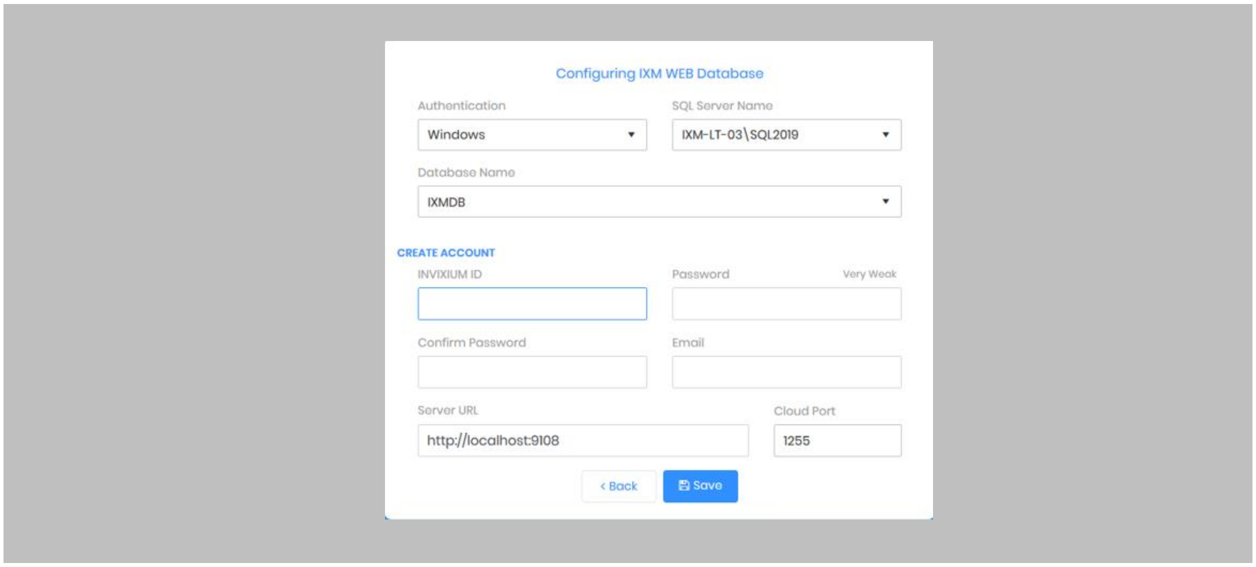
SQL Server Name: IXM-LT-03\SQL2019

Database Name: IXMDB

Figure 10: IXM WEB Database Name

STEP 13

Click **Next**.



Configuring IXM WEB Database

Authentication: Windows

SQL Server Name: IXM-LT-03\SQL2019

Database Name: IXMDB

CREATE ACCOUNT

INVIXIUM ID:

Password: Very Weak

Confirm Password:

Email:

Server URL: http://localhost:9108

Cloud Port: 1255

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.

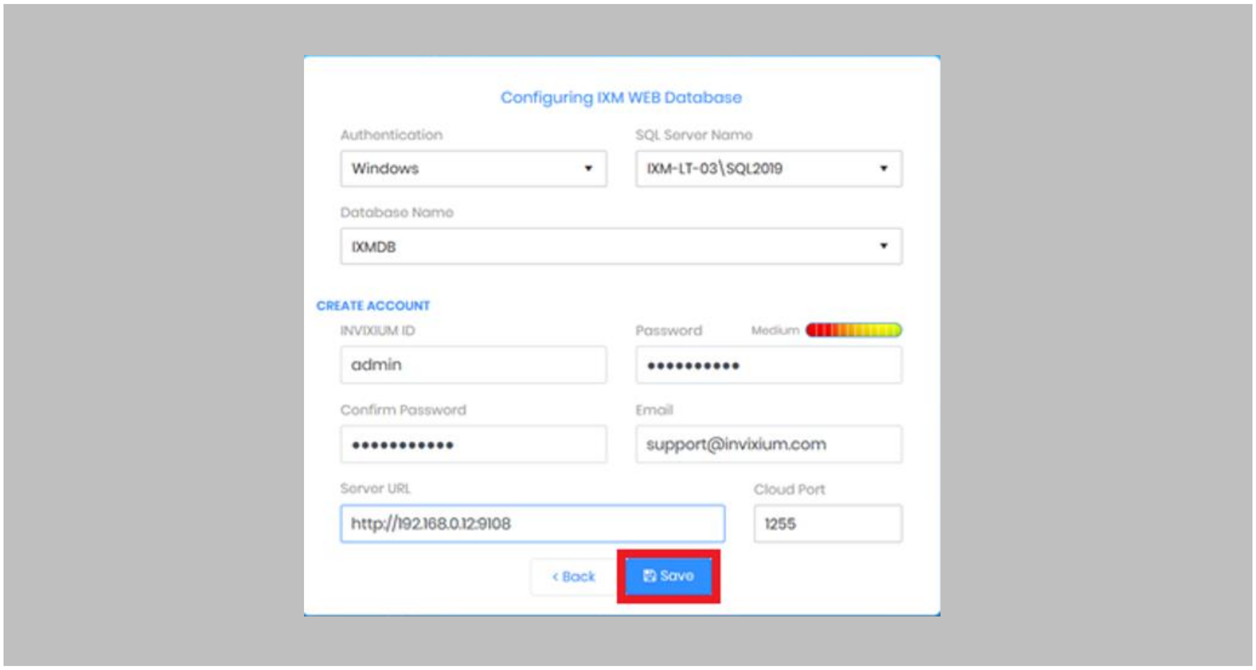
- **Email:** Set an administrator email address. IXM WEB will use this email address in the future in case the password needs to be reset, or any email notification must be sent.

- **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**.



Configuring IXM WEB Database

Authentication: Windows

SQL Server Name: IXM-LT-03\SQL2019

Database Name: IXMDB

CREATE ACCOUNT

INVIXIUM ID: admin

Password: ●●●●●●●●●●● Medium

Confirm Password: ●●●●●●●●●●●●

Email: support@invixium.com

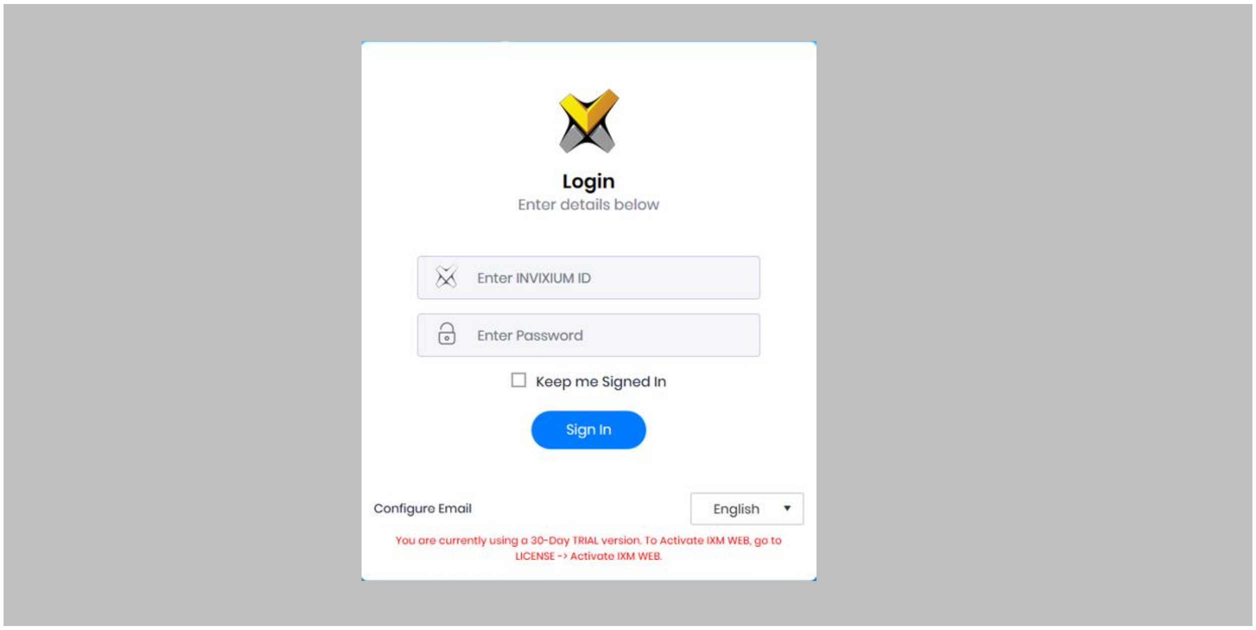
Server URL: http://192.168.0.12:9108

Cloud Port: 1255

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**.



You are currently using a 30-Day TRIAL version. To Activate IXM WEB, go to LICENSE -> Activate IXM WEB.

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**.

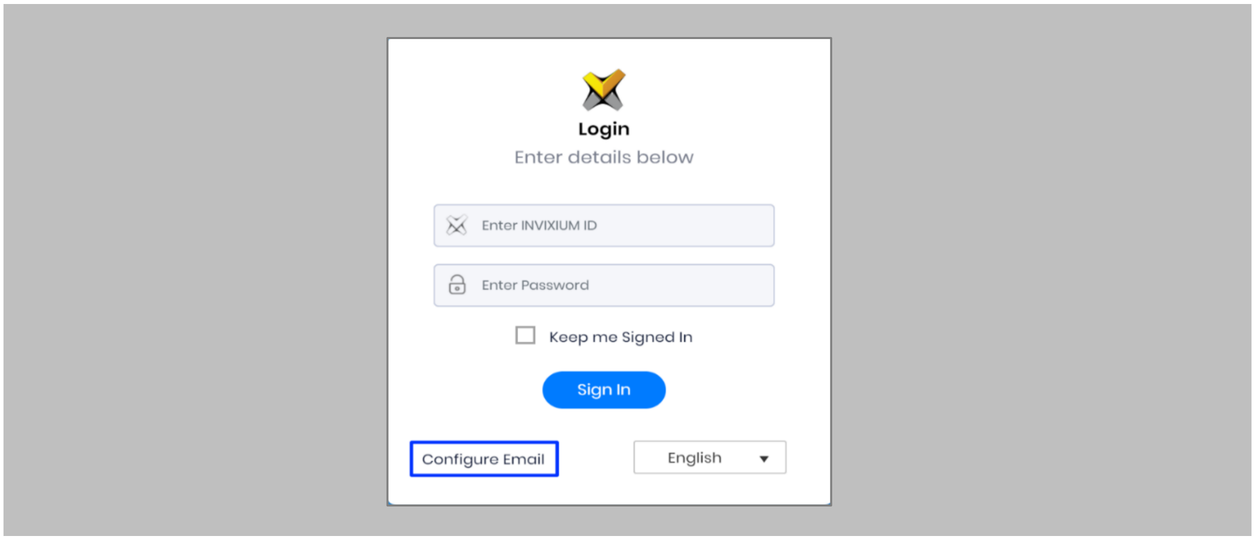
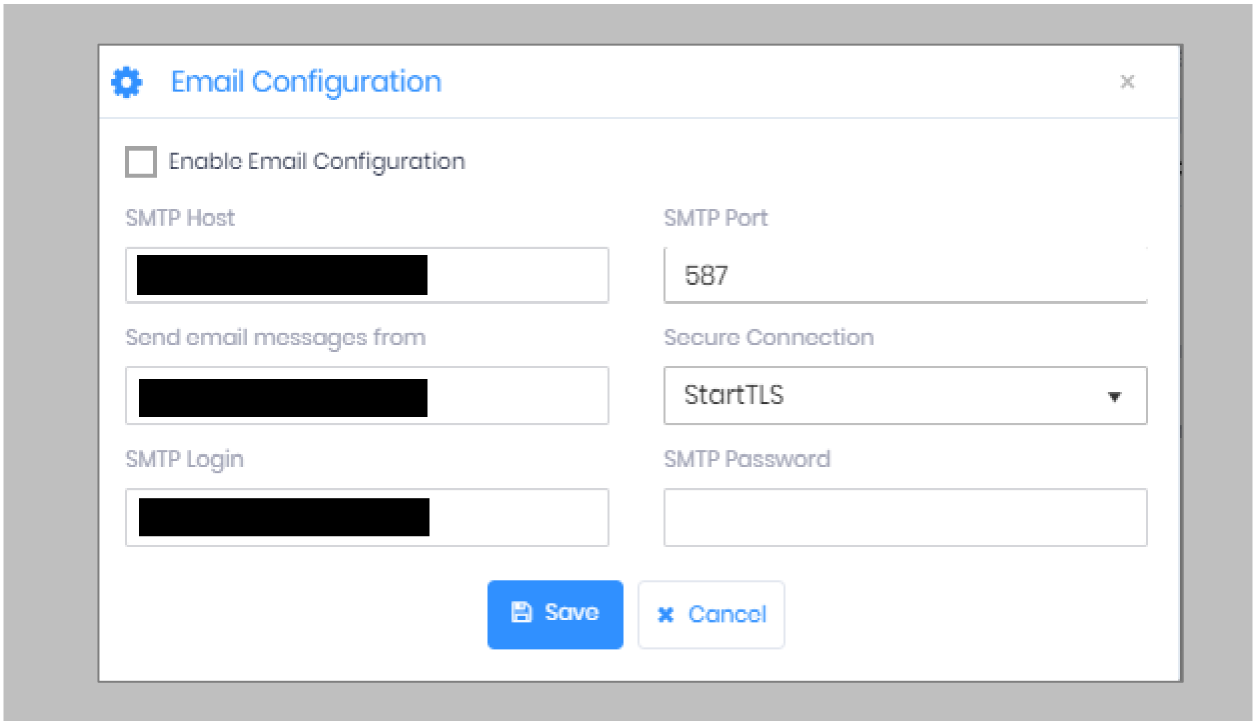


Figure 14: Configure Email

STEP 2

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



Email Configuration

☐ Enable Email Configuration

SMTP Host: [redacted]

SMTP Port: 587

Send email messages from: [redacted]

Secure Connection: StartTLS ▾

SMTP Login: [redacted]

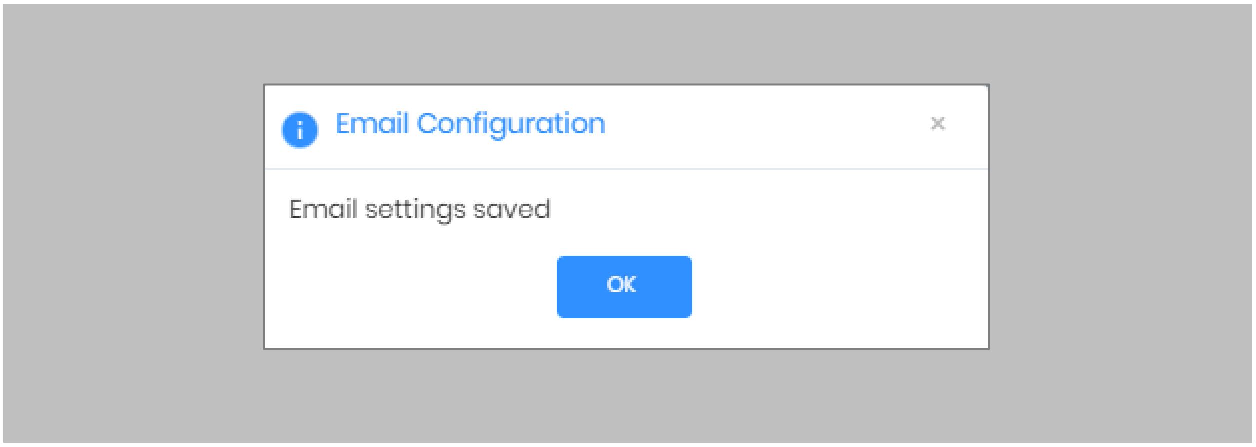
SMTP Password:

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

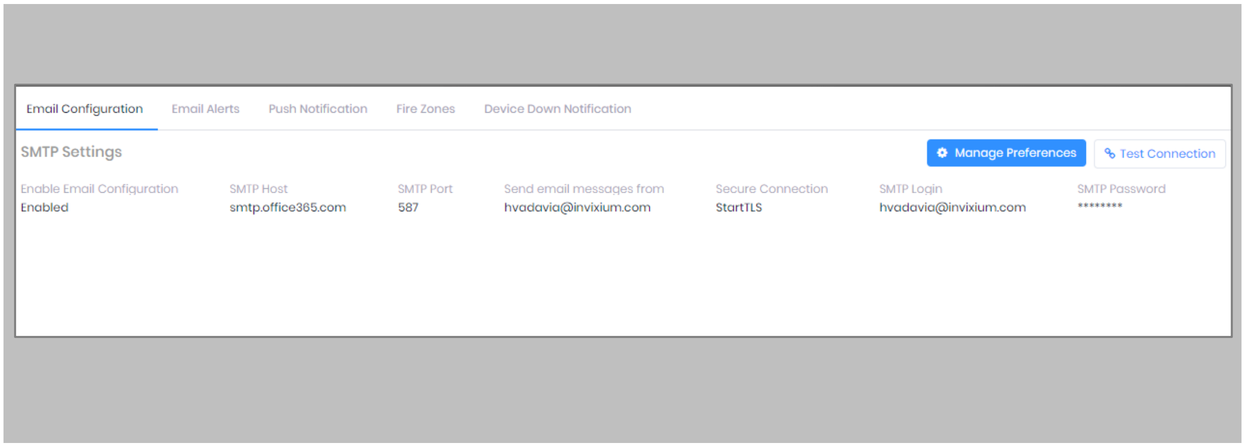
After entering the values, click **Save** to save the SMTP Settings on the IXM WEB Database.



Email settings saved

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.



SMTP Settings

Enable Email Configuration	SMTP Host	SMTP Port	Send email messages from	Secure Connection	SMTP Login	SMTP Password
Enabled	smtp.office365.com	587	hvadavia@invixium.com	StartTLS	hvadavia@invixium.com	********

Figure 17: IXM WEB - Test Connection

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

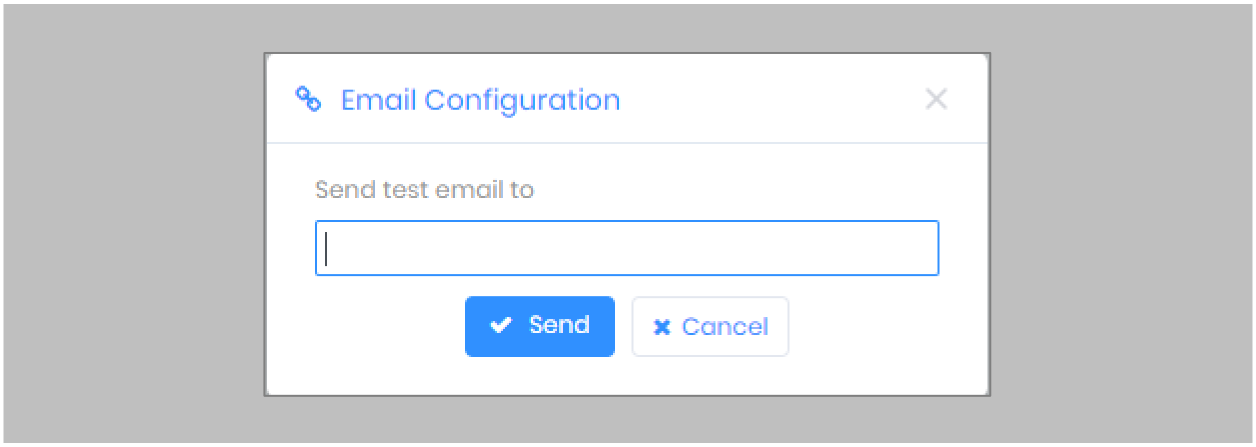


Figure 18: IXM WEB - Enter Email ID

STEP 4

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

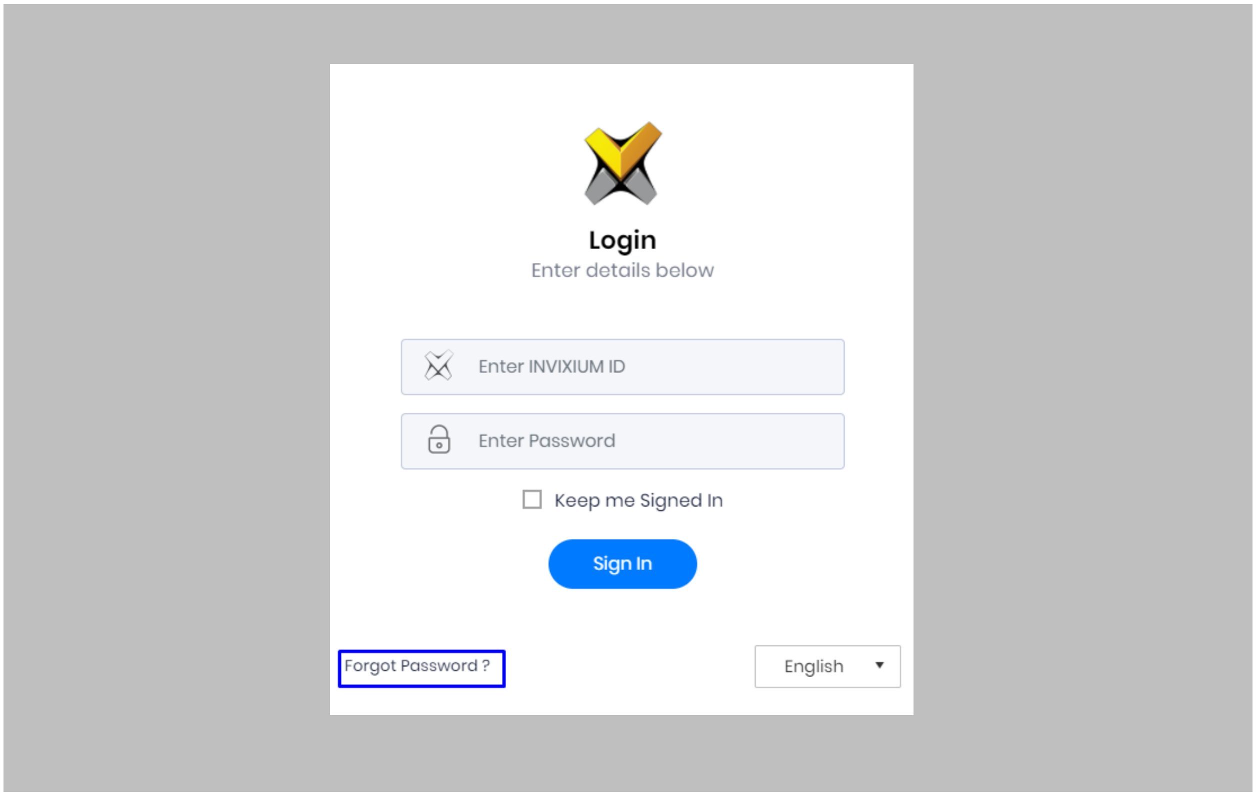


Figure 19: IXM WEB - Forgot Password

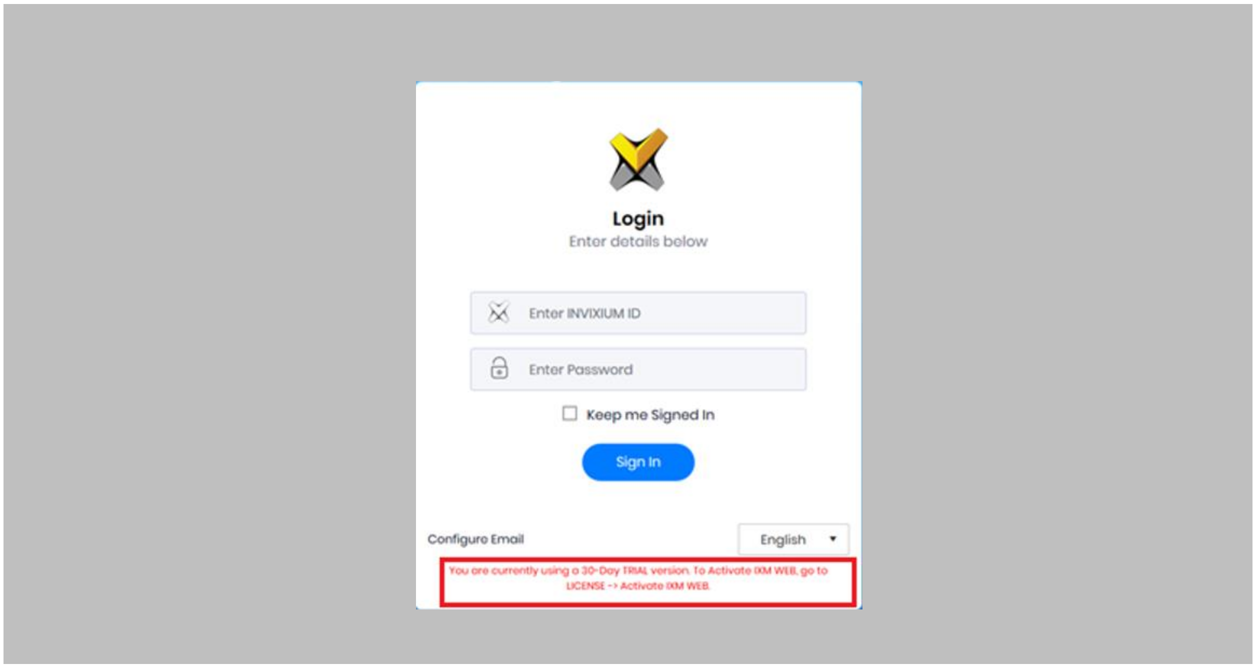
8. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.



You are currently using a 30-Day TRIAL version. To Activate IXM WEB, go to LICENSE -> Activate 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.**

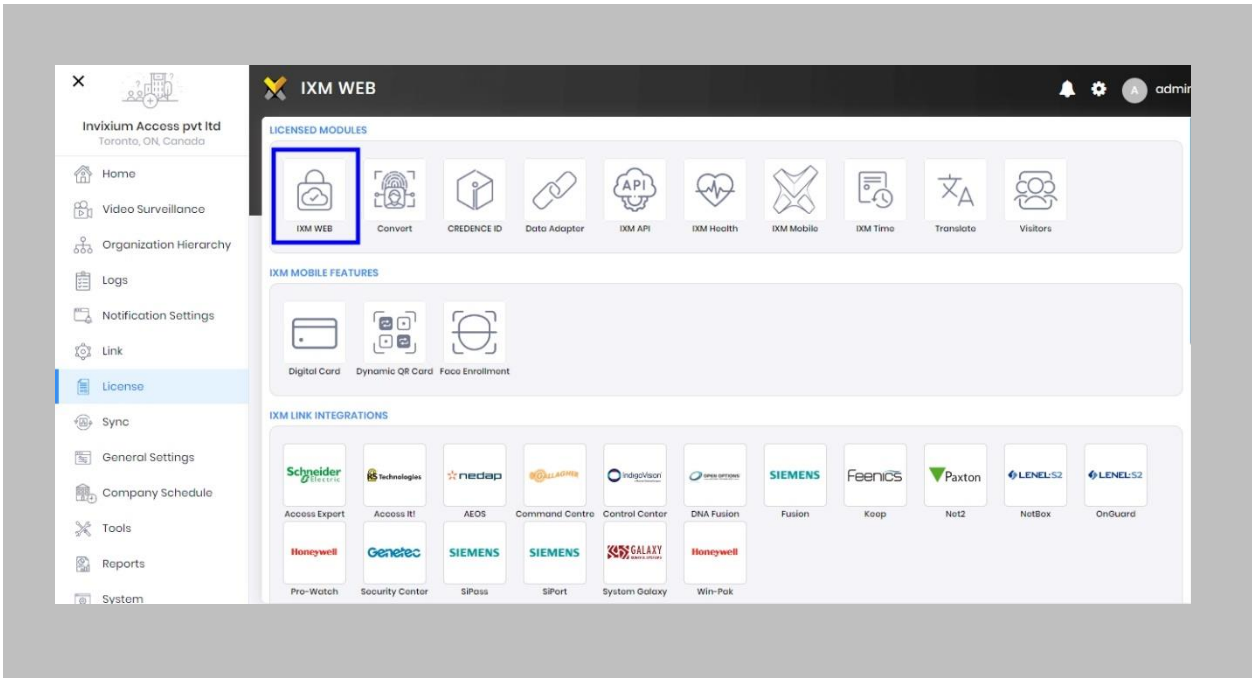


Figure 21: IXM WEB - License Setup

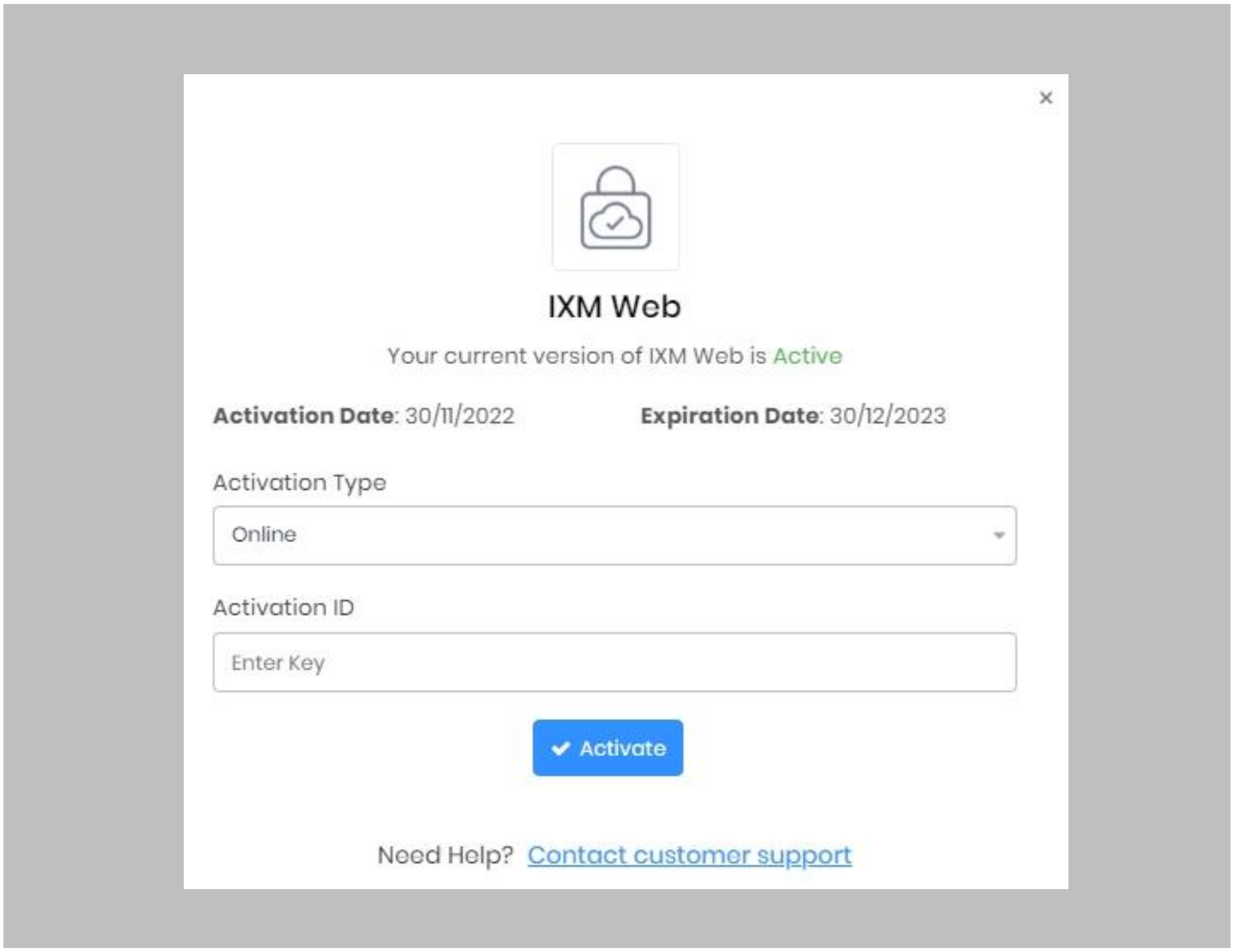
STEP 3

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**.



IXM Web

Your current version of IXM Web is Active

Activation Date: 30/11/2022 **Expiration Date**: 30/12/2023

Activation Type

Online

Activation ID

Enter Key

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**

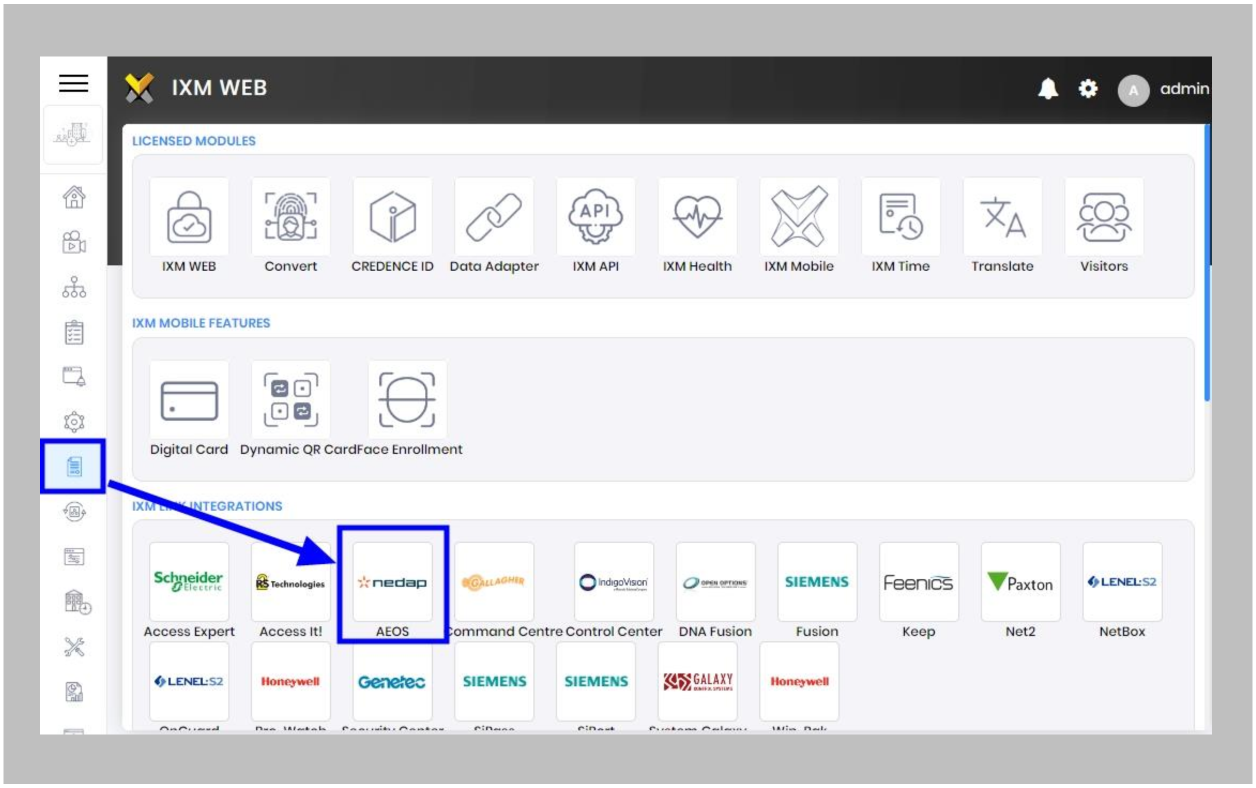
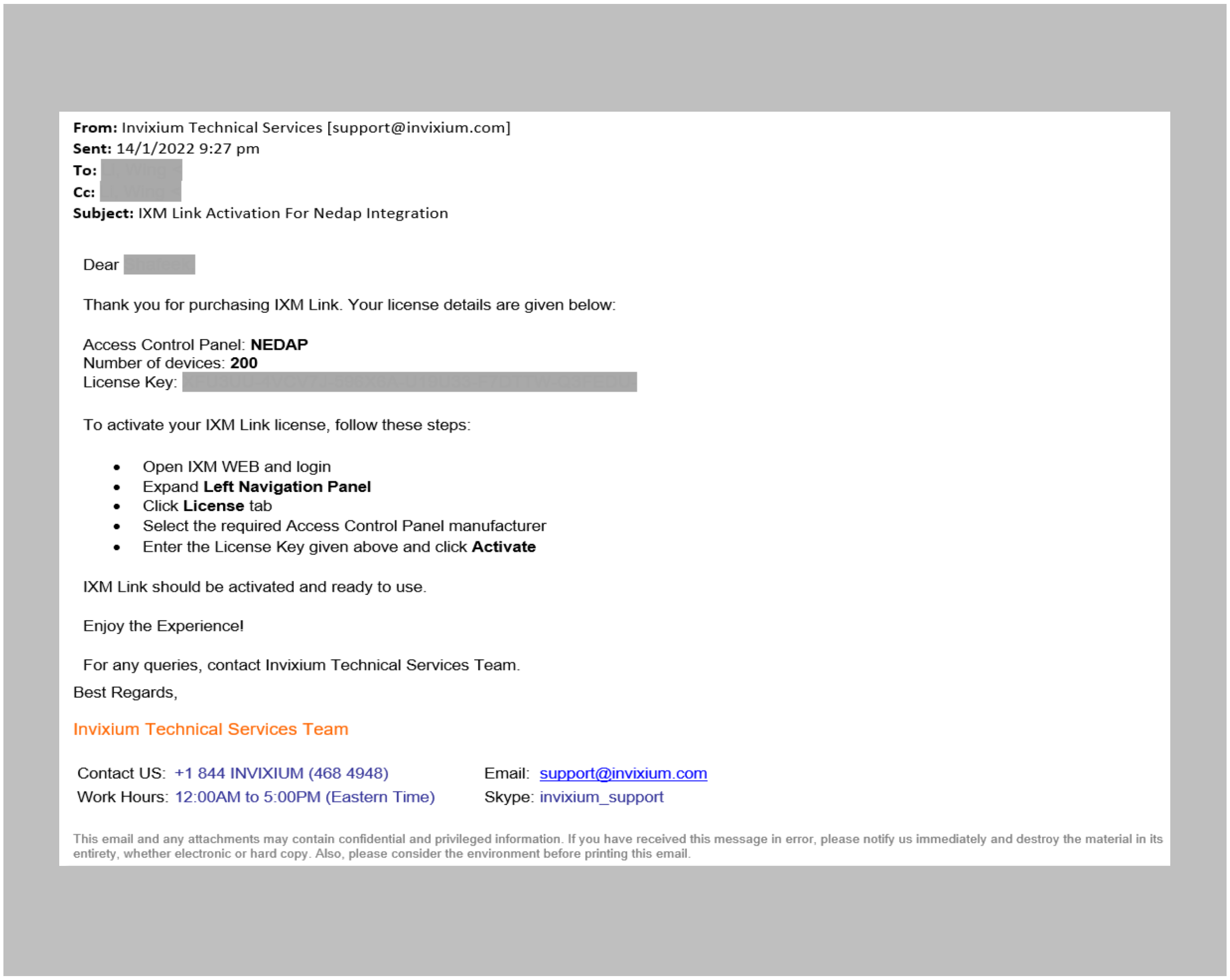


Figure 23: IXM WEB - Nedap Link Activation

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

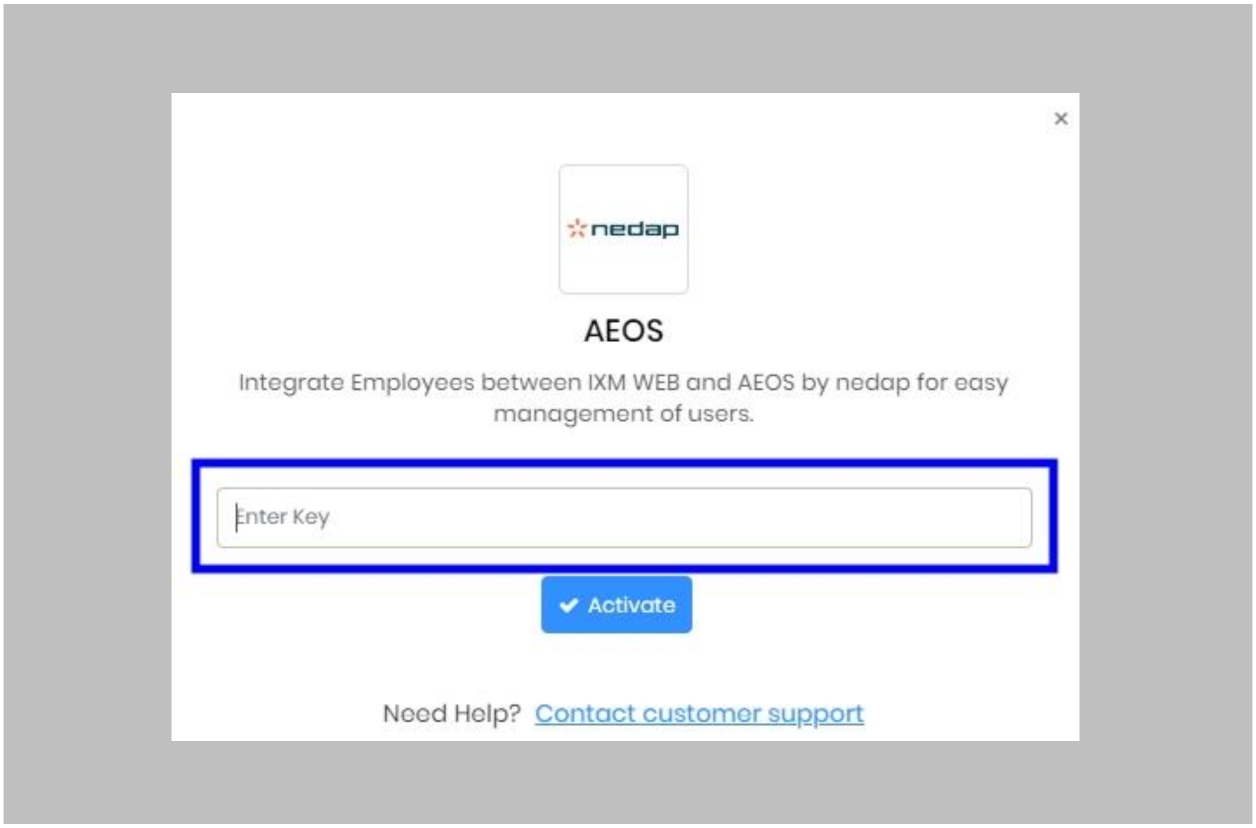
Contact US: +1 844 INVIXIUM (468 4948)
Work Hours: 12:00AM to 5:00PM (Eastern Time)
Email: support@invixium.com
Skype: invixium_support

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**.


AEOS

Integrate Employees between IXM WEB and AEOS by nedap for easy management of users.

Figure 25 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.

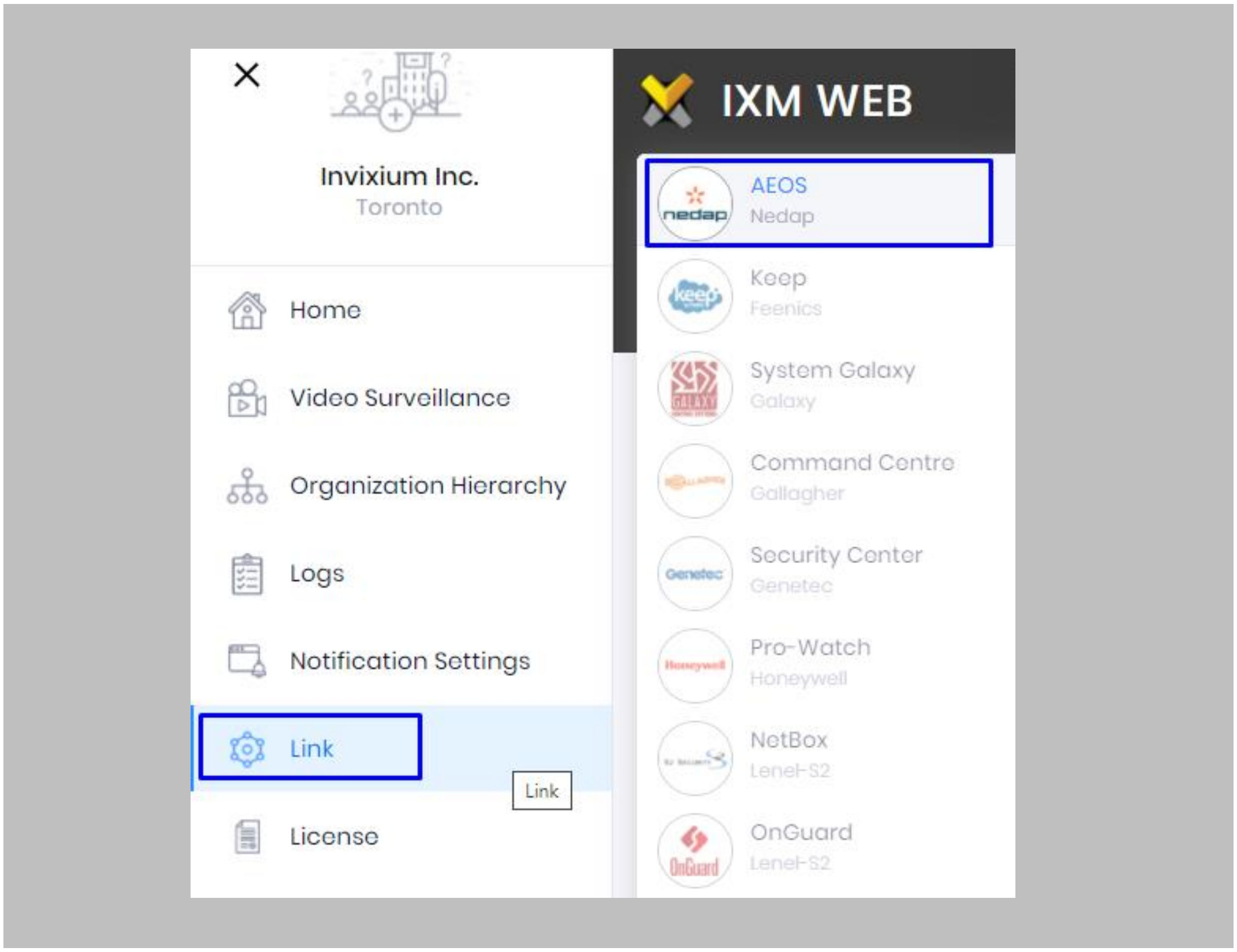
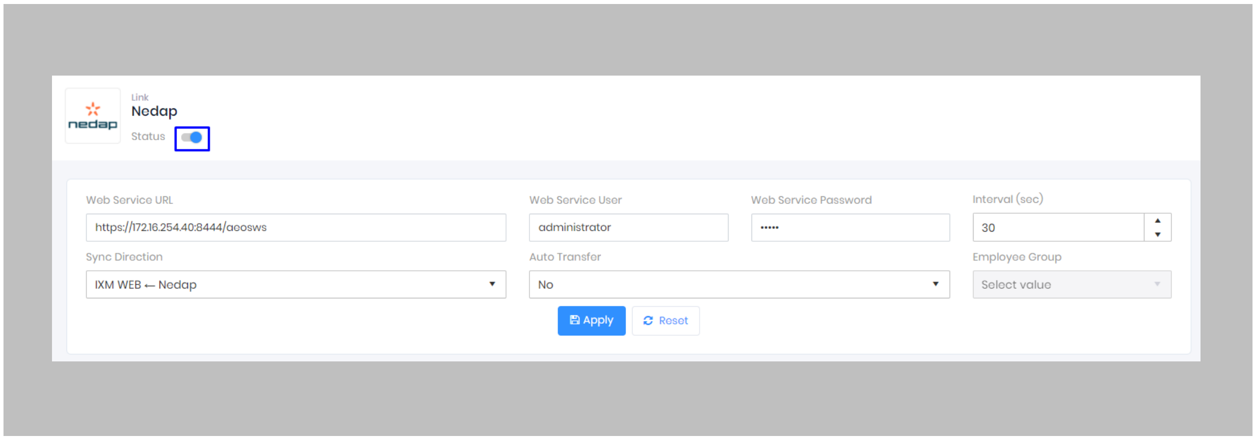


Figure 26: IXM WEB - Link Menu

STEP 2

Toggle the **Status** switch to enable.



Link

Nedap

Status ●

Web Service URL: https://172.16.254.40:8444/aeosws

Web Service User: administrator

Web Service Password: •••••

Interval (sec): 30

Sync Direction: IXM WEB ← Nedap

Auto Transfer: No

Employee Group: Select value

Figure 27: 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.

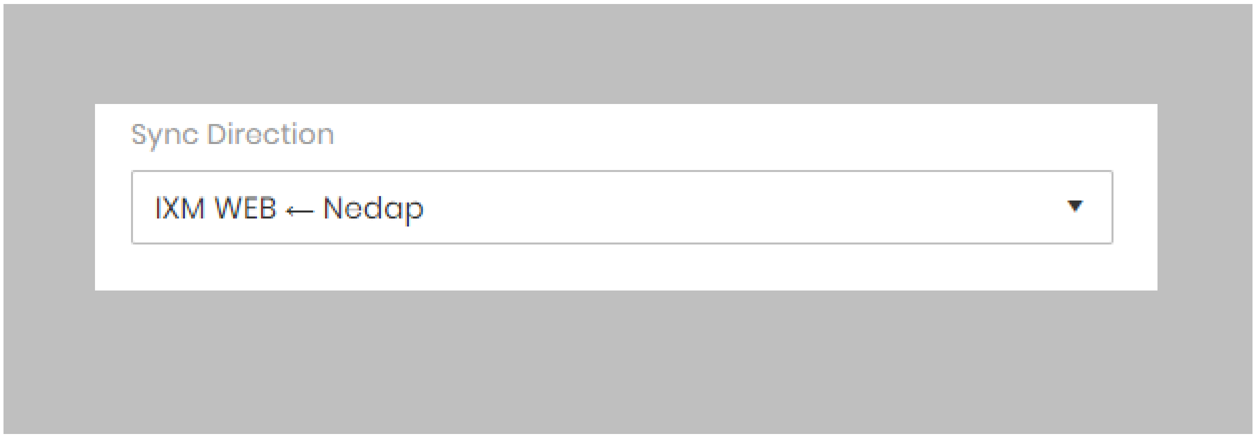
STEP 5

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.



Sync Direction

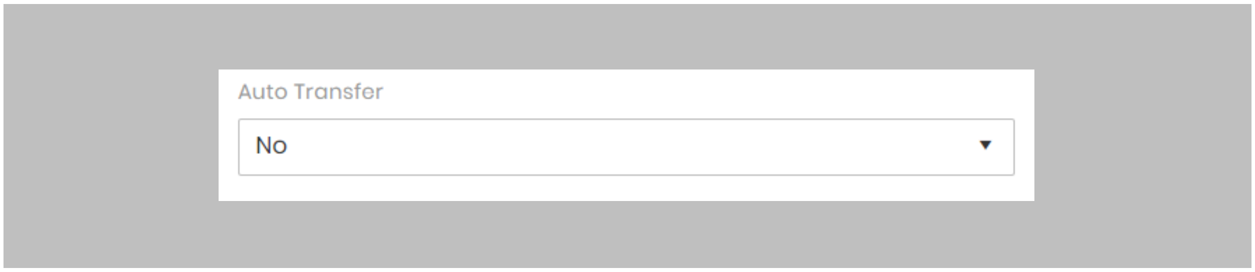
IXM WEB ← Nedap

Figure 28: 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.

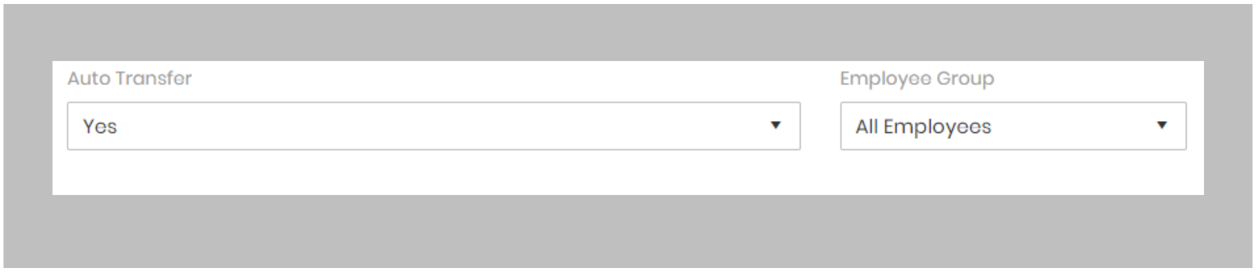


Auto Transfer

No

Figure 29: 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.



Auto Transfer

Yes

Employee Group

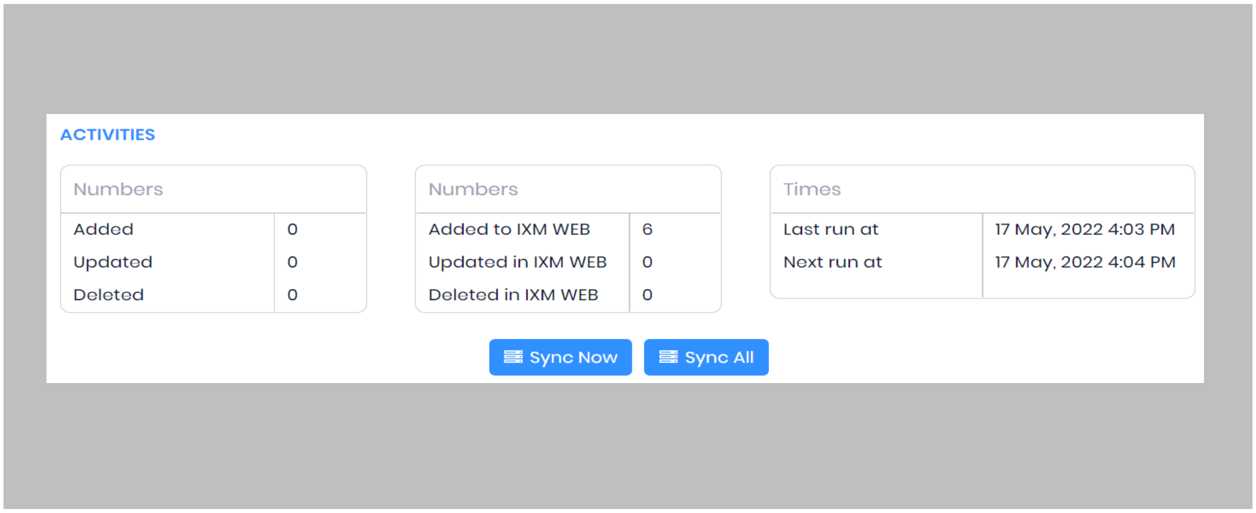
All Employees

Figure 30: IXM WEB - Auto Transfer Yes

STEP 8

Click **Apply**

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



ACTIVITIES

Numbers	
Added	0
Updated	0
Deleted	0

Numbers	
Added to IXM WEB	6
Updated in IXM WEB	0
Deleted in IXM WEB	0

Times	
Last run at	17 May, 2022 4:03 PM
Next run at	17 May, 2022 4:04 PM

Figure 31: 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.

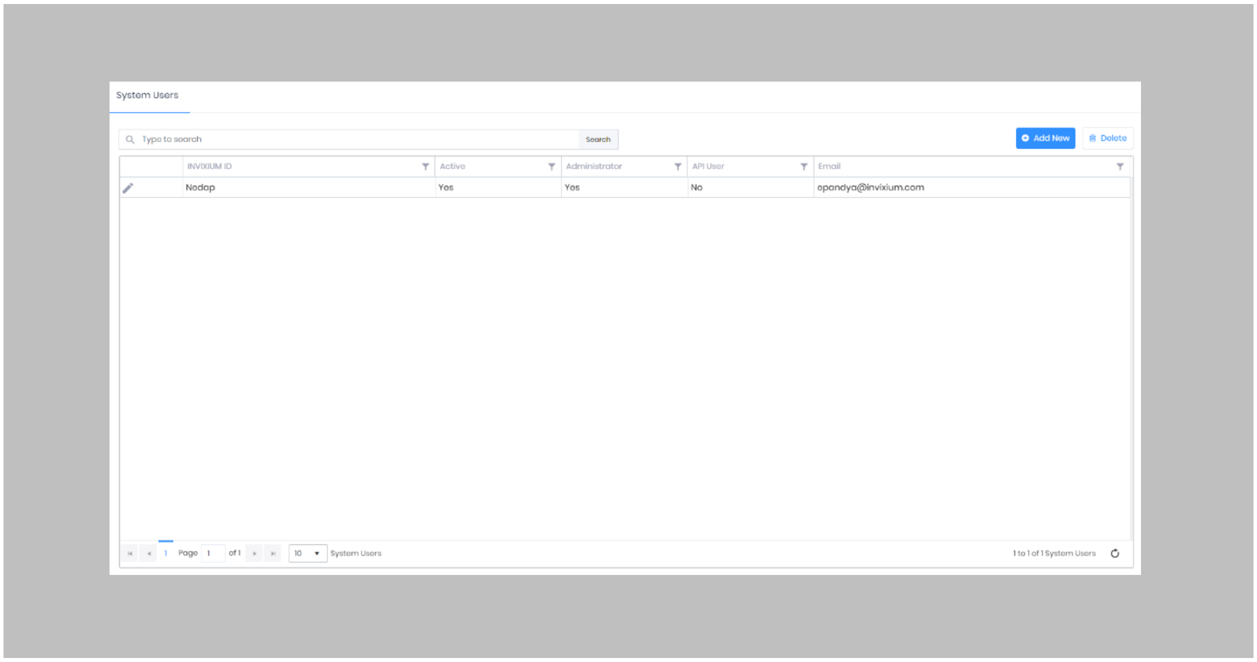
10. Create System User(s) for Biometric Enrollment

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.

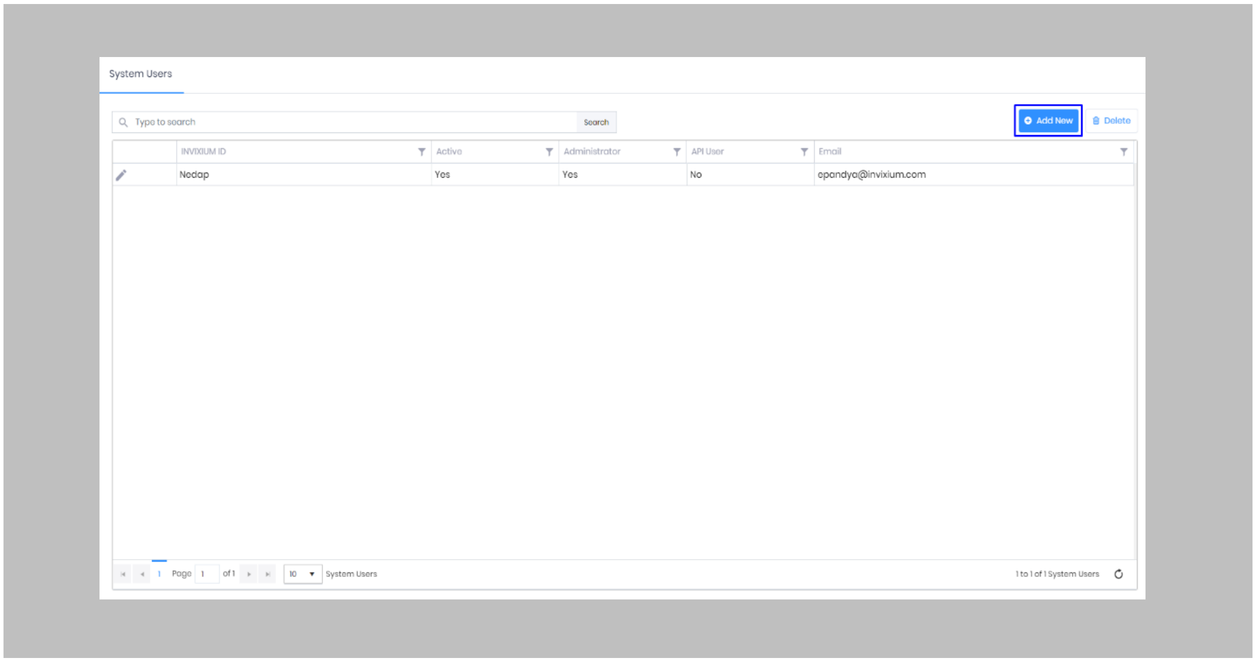


	INVIXIUM ID	Active	Administrator	API User	Email
	Nedap	Yes	Yes	No	epandya@invixium.com

Figure 32: IXM WEB - Create API User

STEP 2

Click **Add New**.



	INVIXIUM ID	Active	Administrator	API User	Email
	Nedap	Yes	Yes	No	epandya@invixium.com

Figure 33: IXM WEB - Add New System User

Creating a system user requires the following details:

- Login Type
    1. Local employee
    2. 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.

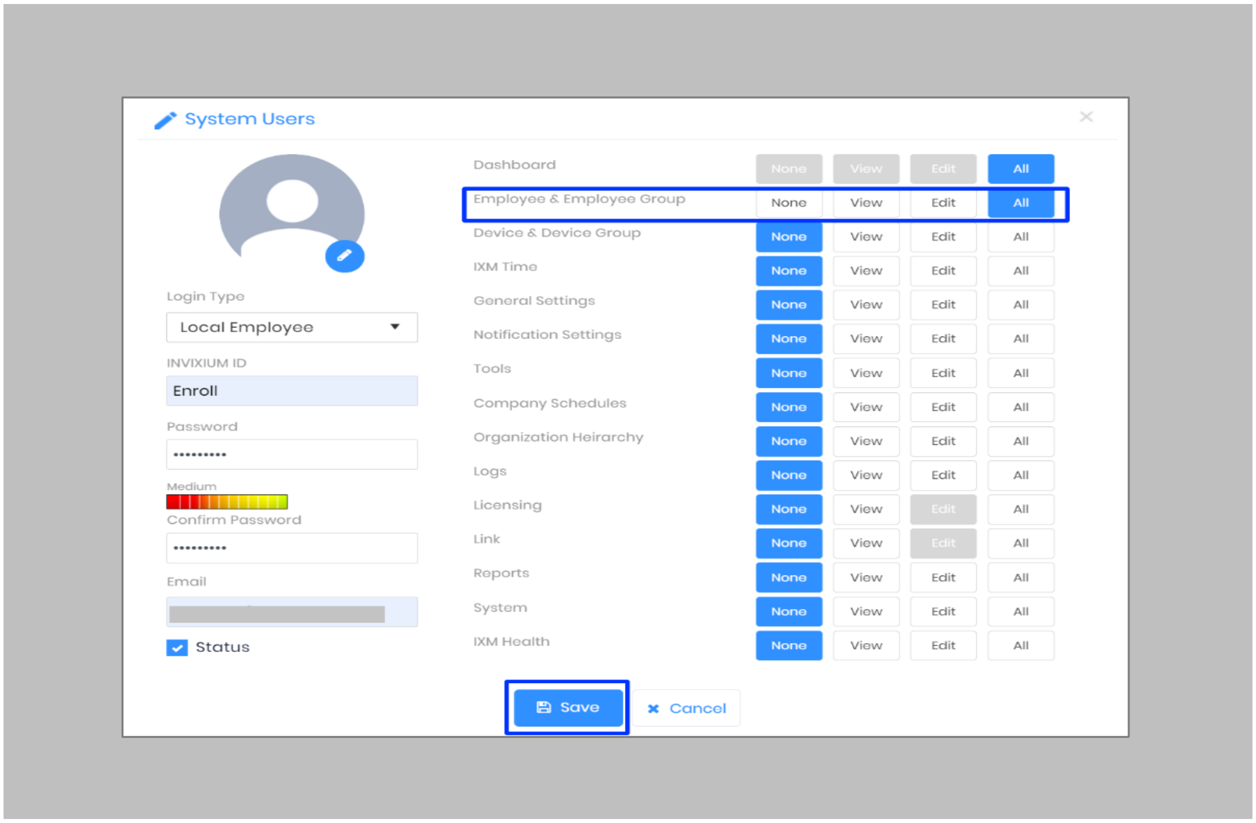
STEP 4

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

STEP 5

Add an email address.

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



System Users

Login Type: Local Employee ▾

INVIXIUM ID: Enroll

Password: •••••••••

Medium

Confirm Password: •••••••••

Email: [redacted]

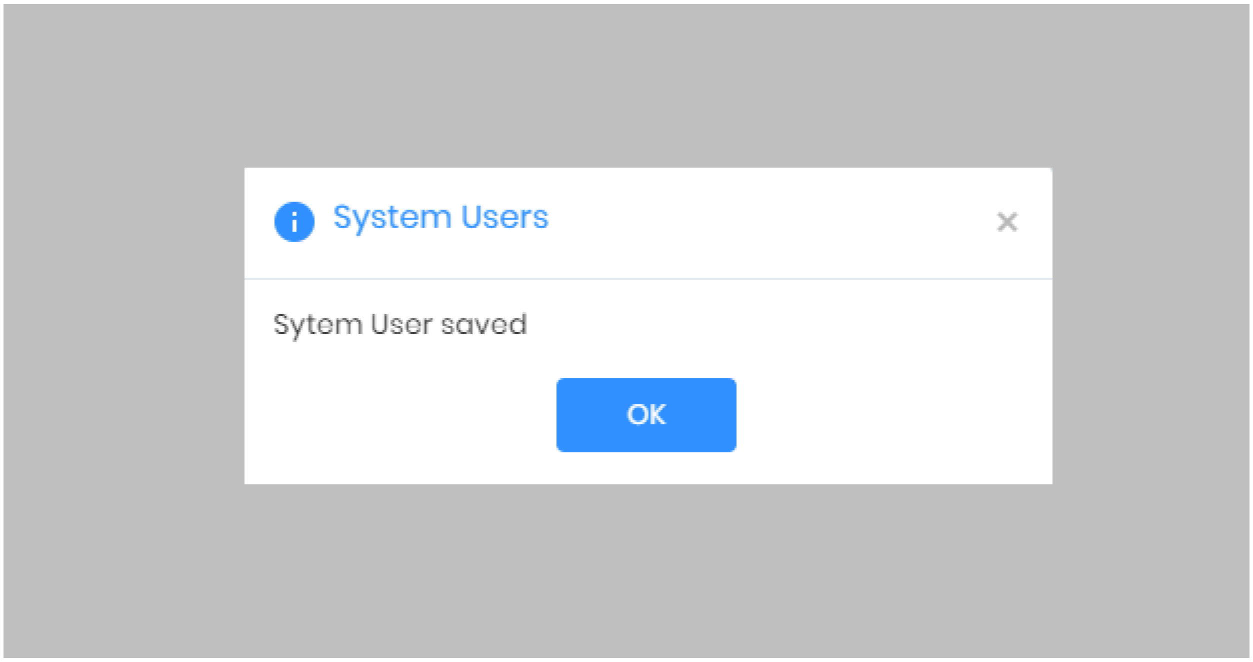
☑ Status

Dashboard	None	View	Edit	[✓ All]
Employee & Employee Group	None	View	Edit	[✓ All]
Device & Device Group	[✓ None]	View	Edit	All
IXM Time	[✓ None]	View	Edit	All
General Settings	[✓ None]	View	Edit	All
Notification Settings	[✓ None]	View	Edit	All
Tools	[✓ None]	View	Edit	All
Company Schedules	[✓ None]	View	Edit	All
Organization Heirarchy	[✓ None]	View	Edit	All
Logs	[✓ None]	View	Edit	All
Licensing	[✓ None]	View	Edit	All
Link	[✓ None]	View	Edit	All
Reports	[✓ None]	View	Edit	All
System	[✓ None]	View	Edit	All
IXM Health	[✓ None]	View	Edit	All

Figure 34: IXM WEB - New System User

STEP 6

Click **Save**.



System Users

Sytem User saved

Figure 35: 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.

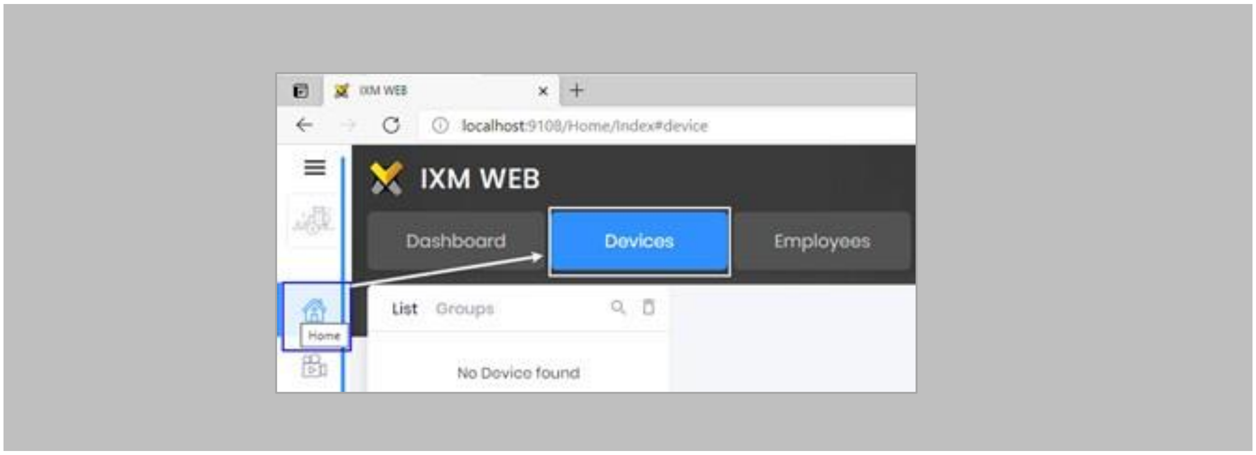
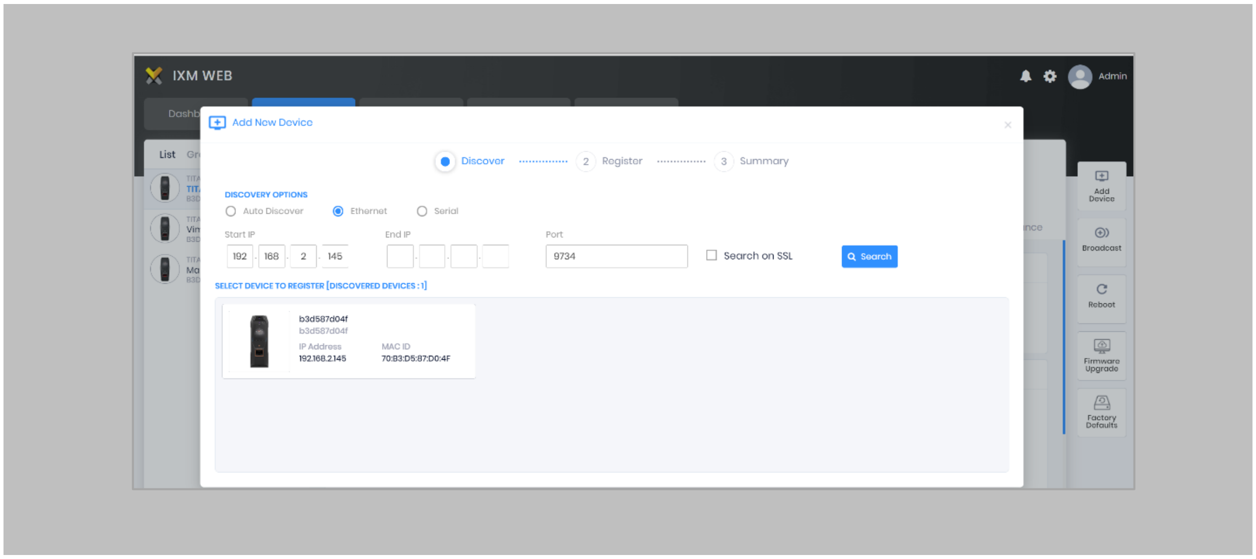


Figure 36: IXM WEB - Devices Tab

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.



DISCOVERY OPTIONS

○ Auto Discover ● Ethernet ○ Serial

Start IP: 192 . 168 . 2 . 145

End IP:

Port: 9734

□ Search on SSL

Search

SELECT DEVICE TO REGISTER [DISCOVERED DEVICES : 1]

b3d587d04f
b3d587d04f

IP Address: 192.168.2.145

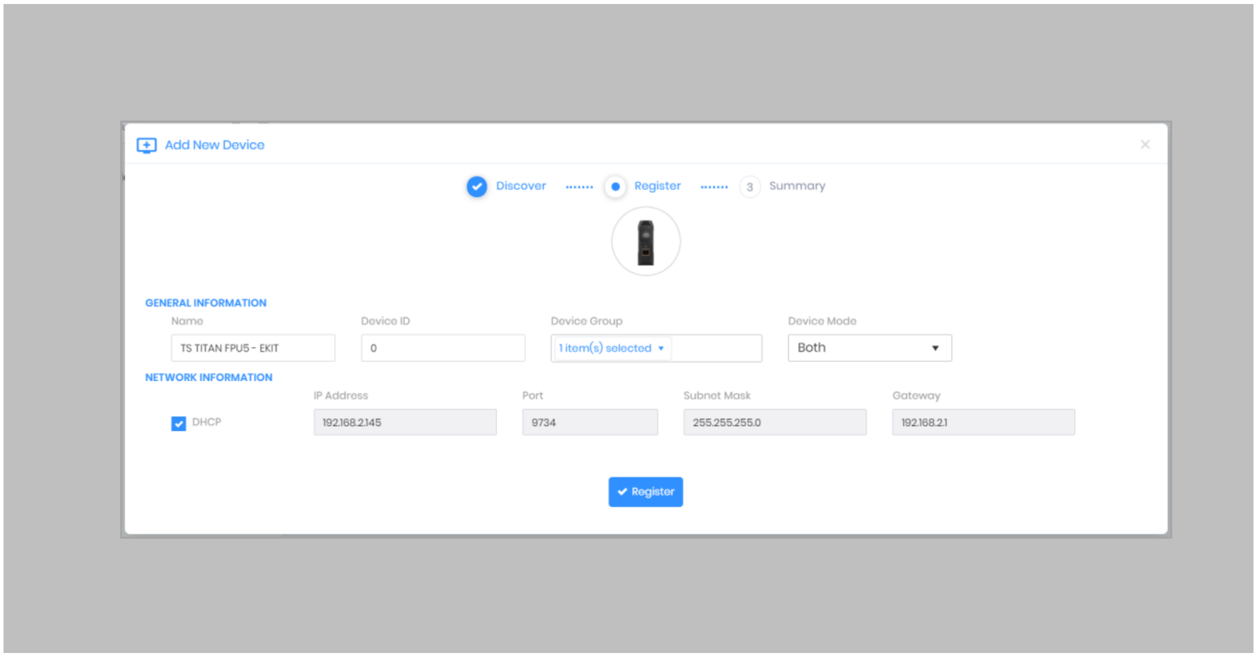
MAC ID: 70:B3:D5:87:D0:4F

Figure 37: 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).



GENERAL INFORMATION

Name	Device ID	Device Group	Device Mode
TS TITAN FPU5 - EKIT	0	1 item(s) selected	Both

NETWORK INFORMATION

	IP Address	Port	Subnet Mask	Gateway
☑ DHCP	192.168.2.145	9734	255.255.255.0	192.168.2.1

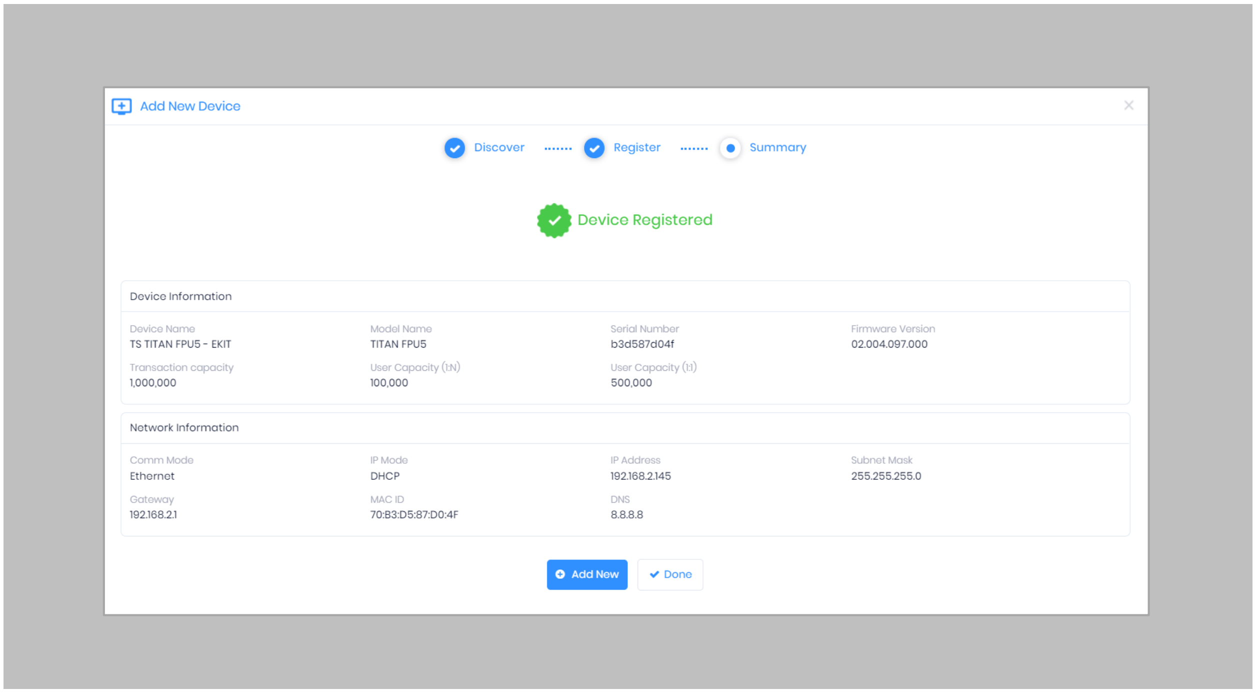
Figure 38: IXM WEB - Register Device

STEP 4

Click **Register**.

STEP 5

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



Device Registered

Device Information

Device Name
TS TITAN FPU5 - EKIT

Model Name
TITAN FPU5

Serial Number
b3d587d04f

Firmware Version
02.004.097.000

Transaction capacity
1,000,000

User Capacity (1:N)
100,000

User Capacity (1:1)
500,000

Network Information

Comm Mode
Ethernet

IP Mode
DHCP

IP Address
192.168.2.145

Subnet Mask
255.255.255.0

Gateway
192.168.2.1

MAC ID
70:B3:D5:87:D0:4F

DNS
8.8.8.8

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).

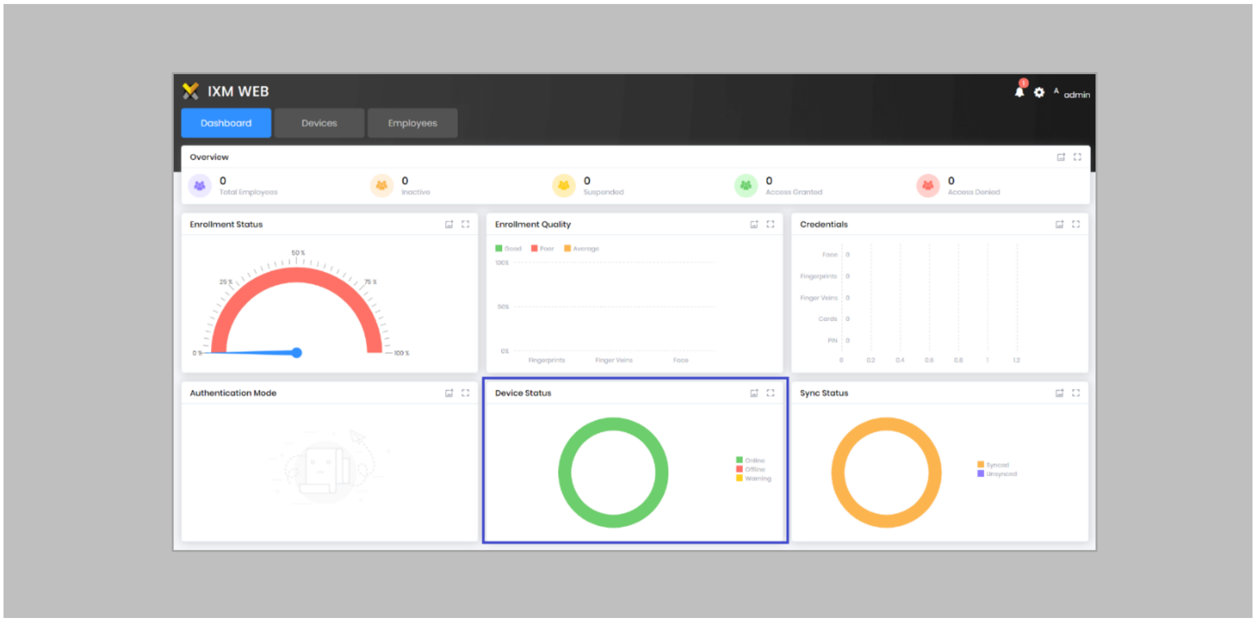


Figure 40: IXM WEB - Dashboard, Device Status

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.**

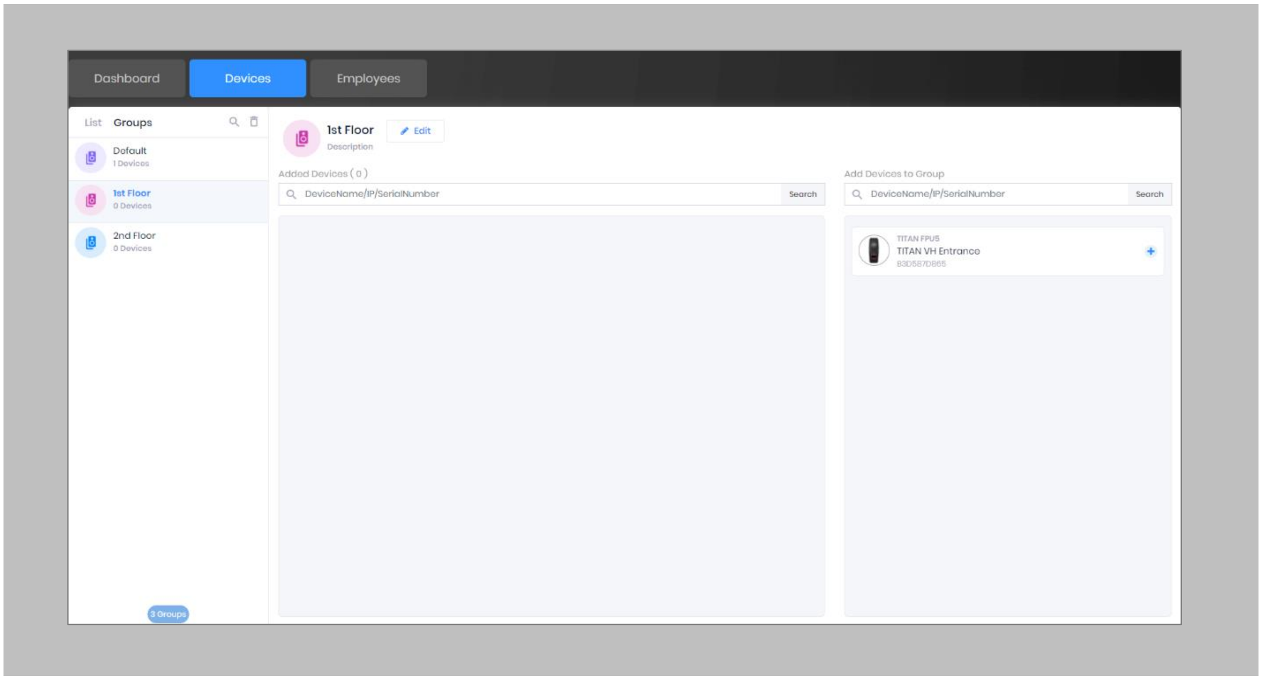


Figure 41: IXM WEB - Assign Device Group

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.

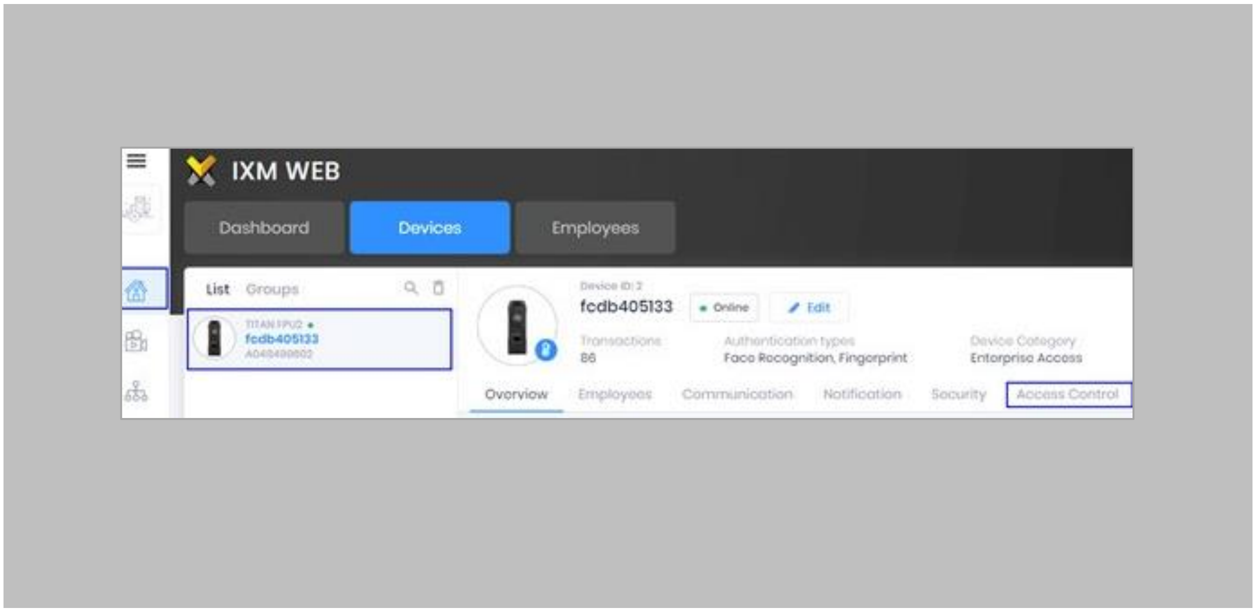
The Standard 26 Bit Wiegand will be used to define which output format will be sent to Nedap AEOS.

STEP 1

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

STEP 2

Navigate to the **Access Control** tab.

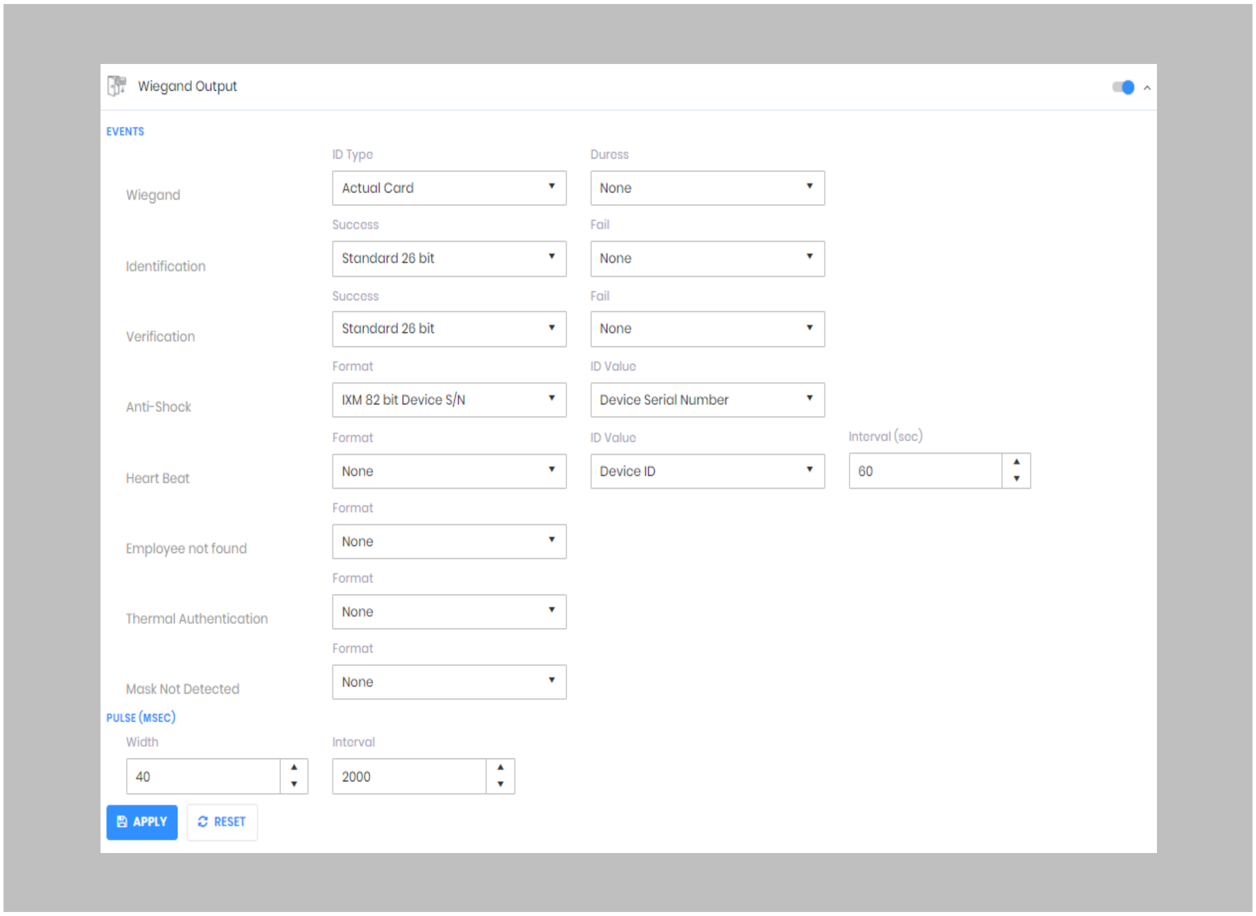


Device ID: 2
fcdb405133
Transactions
86
Authentication types
Face Recognition, Fingerprint
Device Category
Enterprise Access

Figure 42: 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.



Wiegand Output

EVENTS

Wiegand: ID Type: Actual Card; Duress: None

Identification: Success: Standard 26 bit; Fail: None

Verification: Success: Standard 26 bit; Fail: None

Anti-Shock: Format: IXM 82 bit Device S/N; ID Value: Device Serial Number

Heart Beat: Format: None; ID Value: Device ID; Interval (sec): 60

Employee not found: Format: None

Thermal Authentication: Format: None

Mask Not Detected: Format: None

PULSE (MSEC)

Width: 40

Interval: 2000

Figure 43: 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.

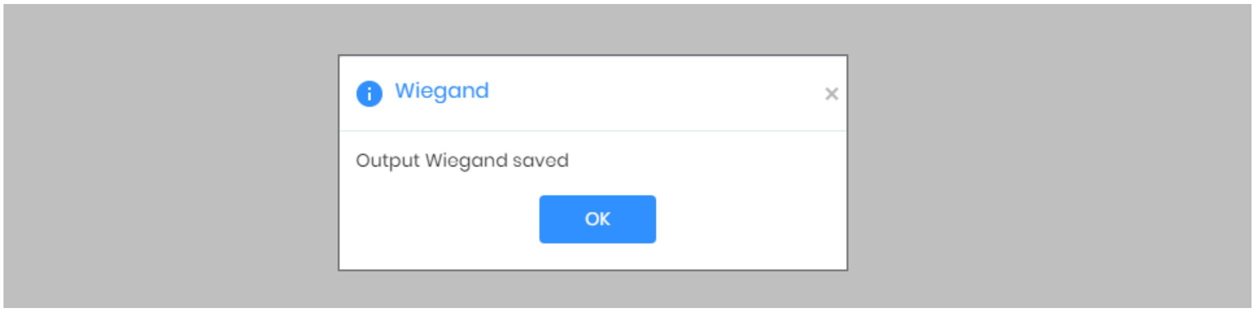
STEP 4

Set the **items**:

Wiegand	Actual Card
Identification	26 - bit
Verification	26 - bit

STEP 5

Click **Apply.**



Wiegand

Output Wiegand saved

Figure 44: 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**.

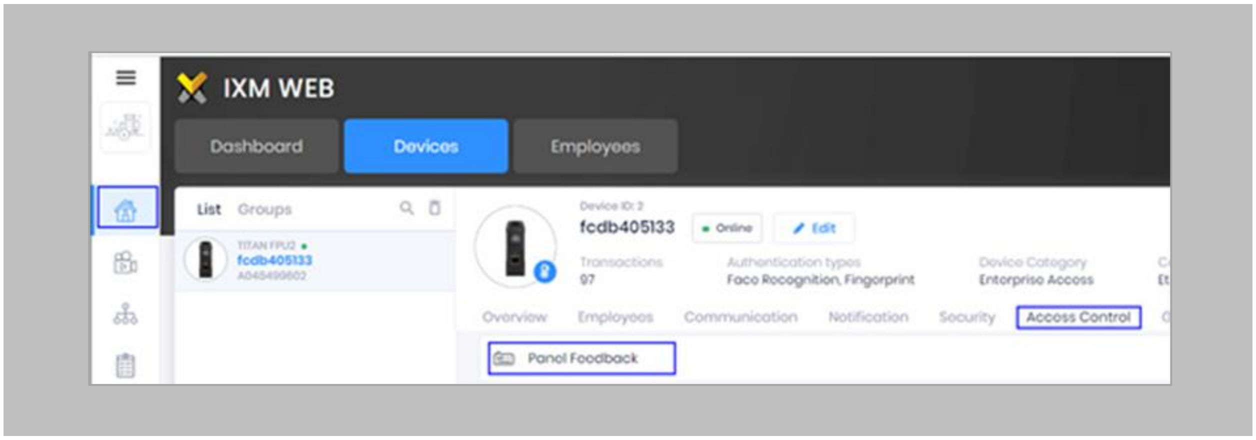
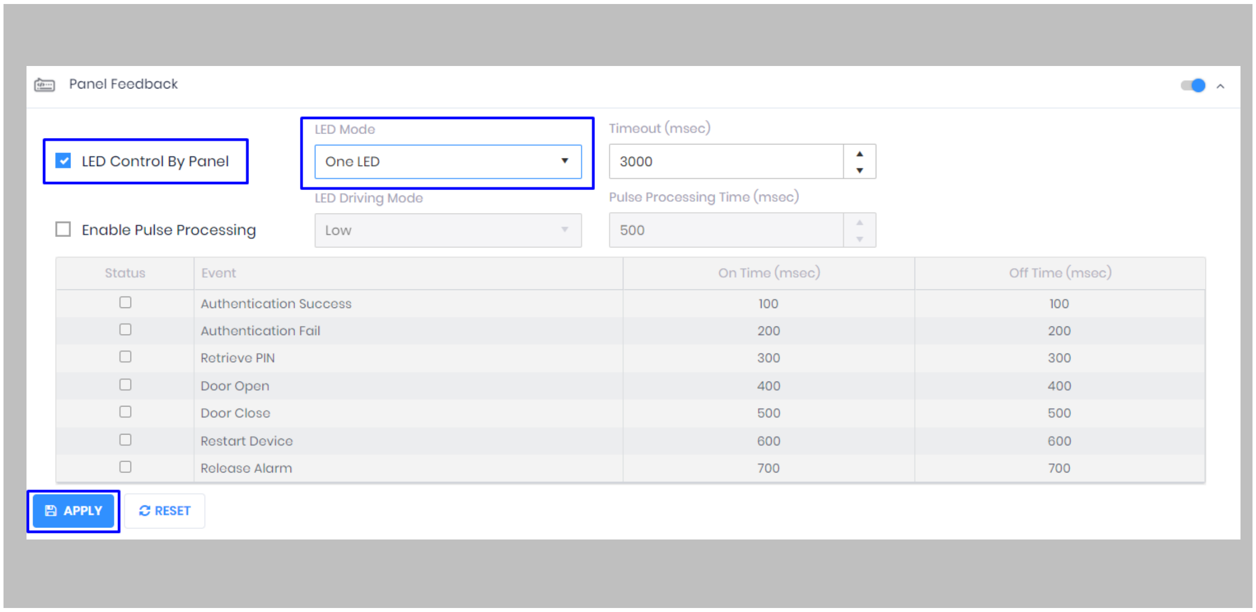


Figure 45: IXM WEB - Panel Feedback

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**.



Panel Feedback

☑ LED Control By Panel

LED Mode: One LED

Timeout (msec): 3000

□ Enable Pulse Processing

LED Driving Mode: Low

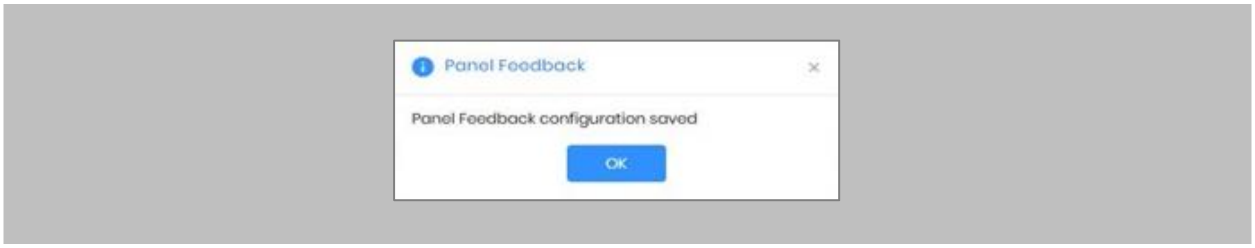
Pulse Processing Time (msec): 500

Status	Event	On Time (msec)	Off Time (msec)
□	Authentication Success	100	100
□	Authentication Fail	200	200
□	Retrieve PIN	300	300
□	Door Open	400	400
□	Door Close	500	500
□	Restart Device	600	600
□	Release Alarm	700	700

Figure 46: IXM WEB - Configuring Panel Feedback in IXM WEB

STEP 5

Click **Apply**.



Panel Feedback

Panel Feedback configuration saved

Figure 47: 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'.**

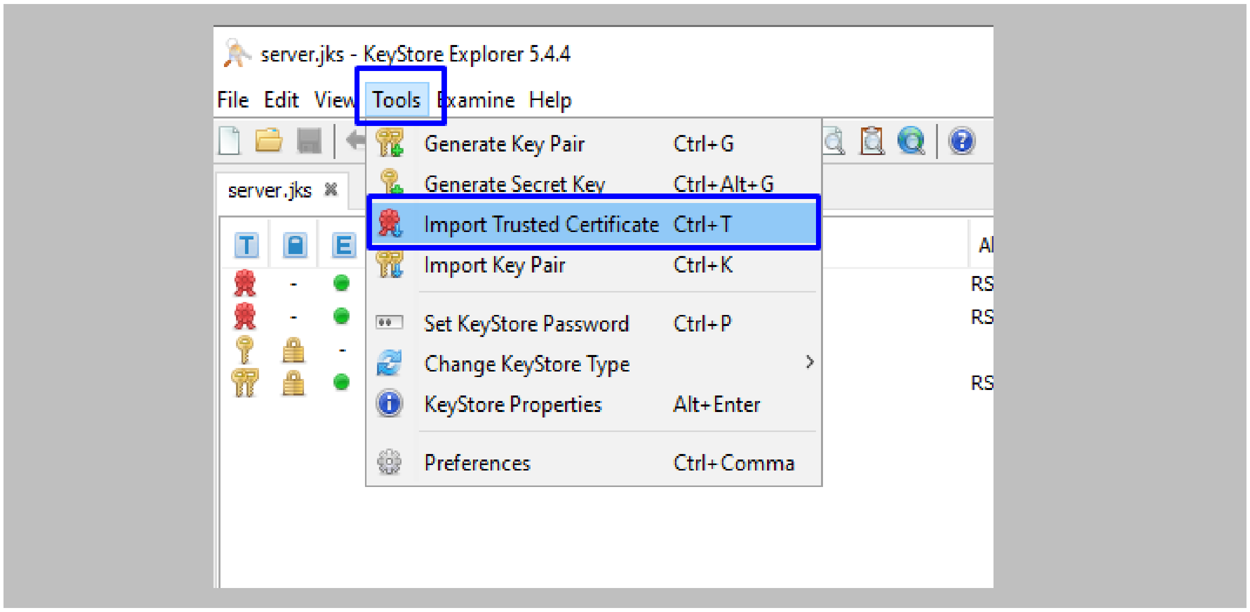

server.jks - KeyStore Explorer 5.4.4
File Edit View Tools Examine Help
server.jks
Generate Key Pair Ctrl+G
Generate Secret Key Ctrl+Alt+G
Import Trusted Certificate Ctrl+T
Import Key Pair Ctrl+K
Set KeyStore Password Ctrl+P
Change KeyStore Type
KeyStore Properties Alt+Enter
Preferences Ctrl+Comma
T
E
Al
RS
RS
RS

Figure 48: 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.**

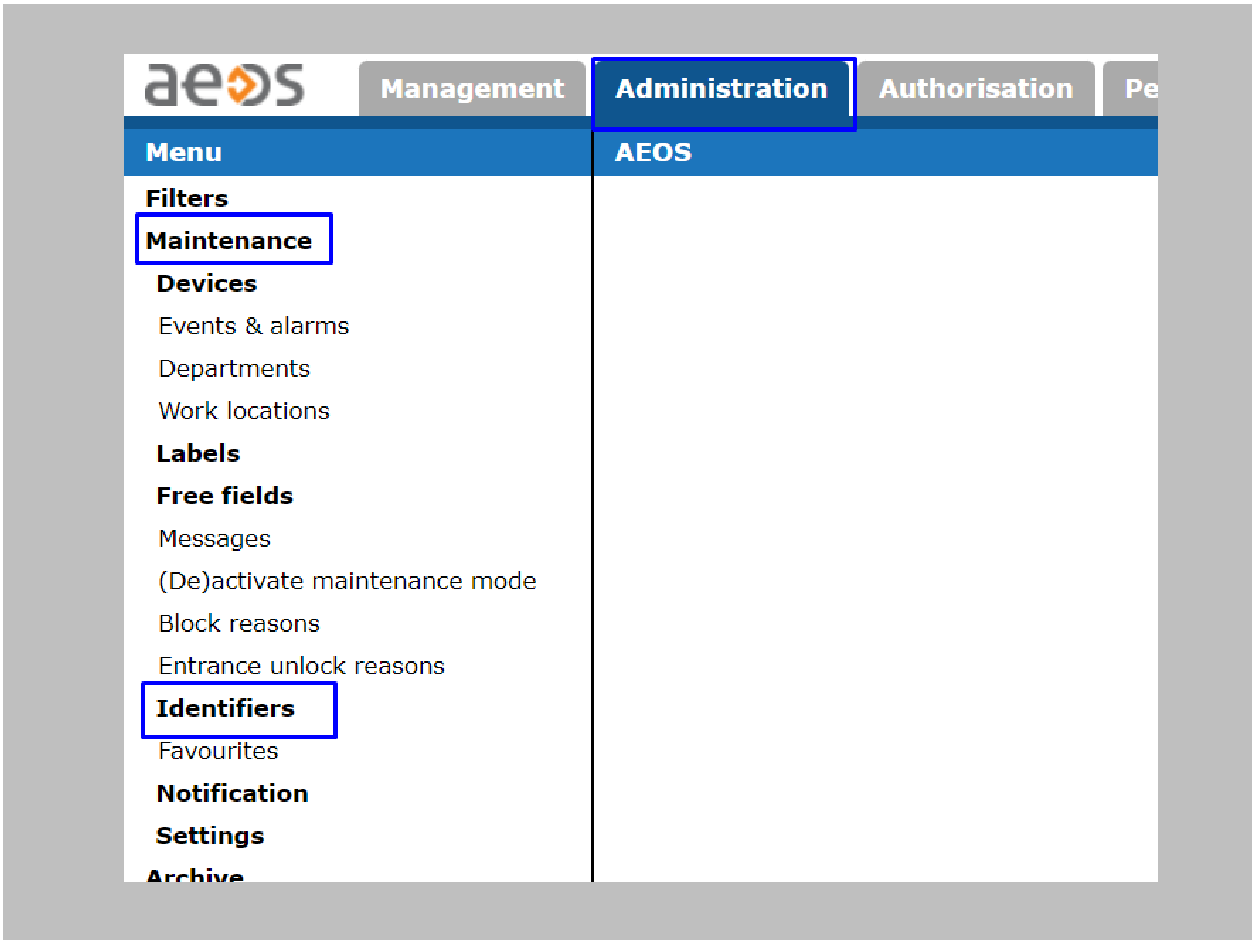


Figure 49: AEOS - Identifiers

STEP 8

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

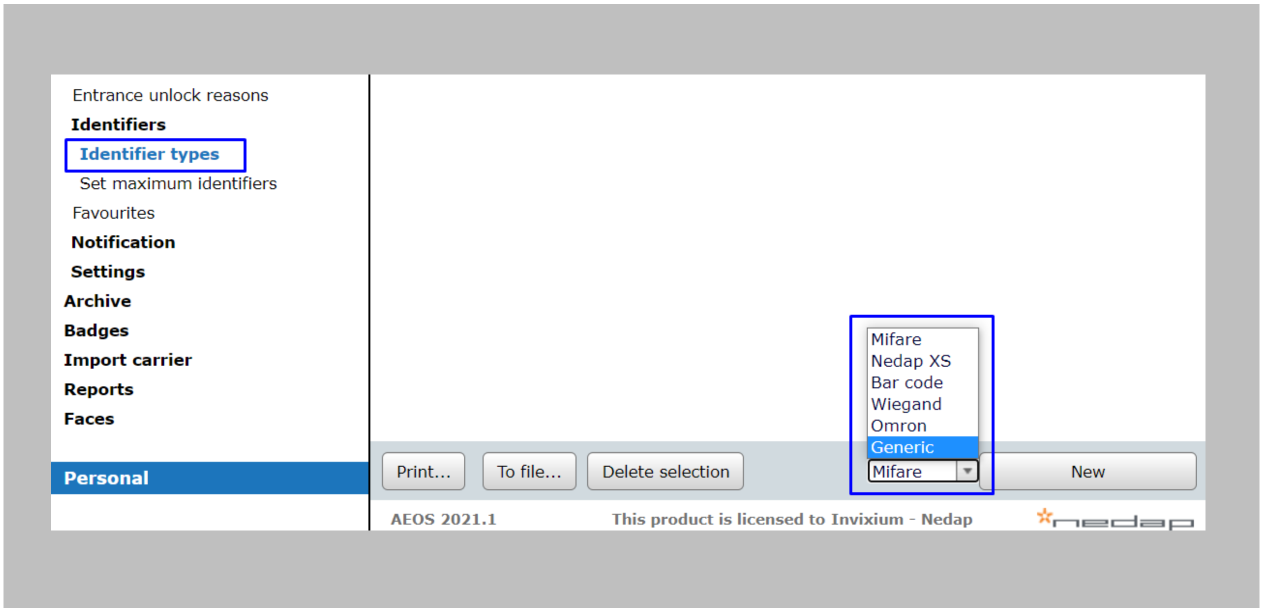


Figure 50: AEOS - Identifier Type Selection

Click on **New.**

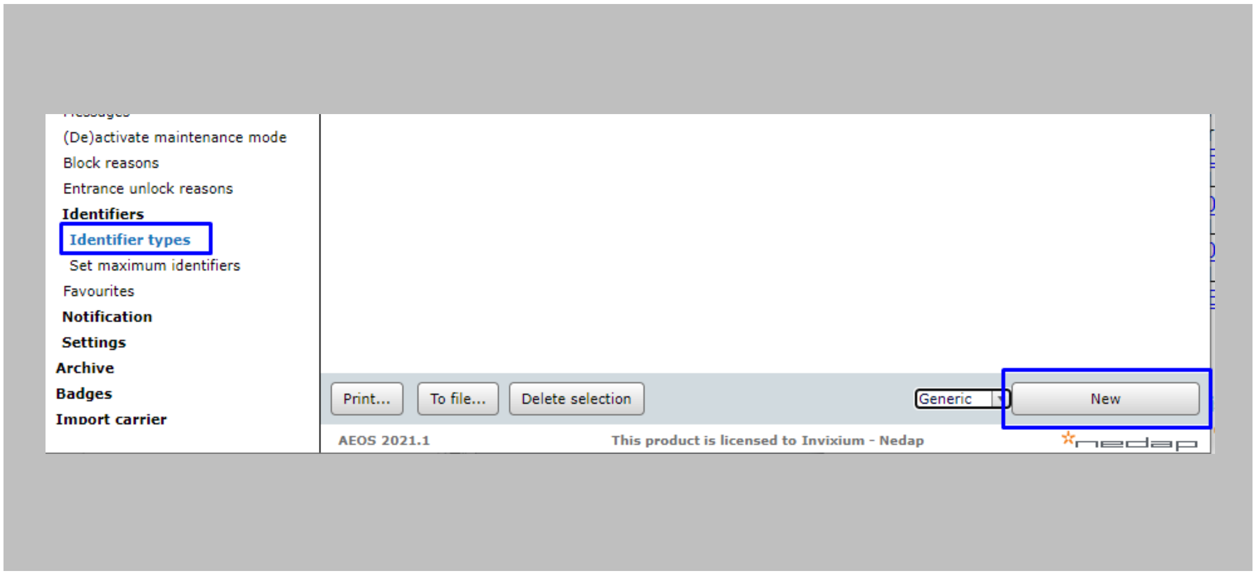


Figure 51: AEOS - Add New Identifier Type

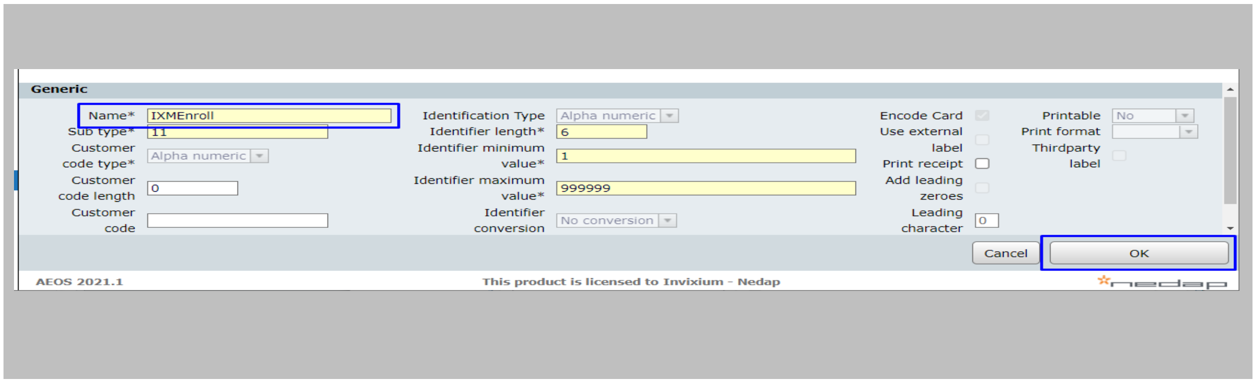
STEP 9

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.**



Generic

Name* IXMEnroll

Sub type* 11

Customer code type* Alpha numeric

Customer code length 0

Customer code

Identification Type Alpha numeric

Identifier length* 6

Identifier minimum value* 1

Identifier maximum value* 999999

Identifier conversion No conversion

Encode Card ☑

Use external label □

Print receipt □

Add leading zeroes □

Leading character 0

Printable No

Print format

Thirdparty label □

Figure 52: AEOS - New Identifier Type

STEP 10

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

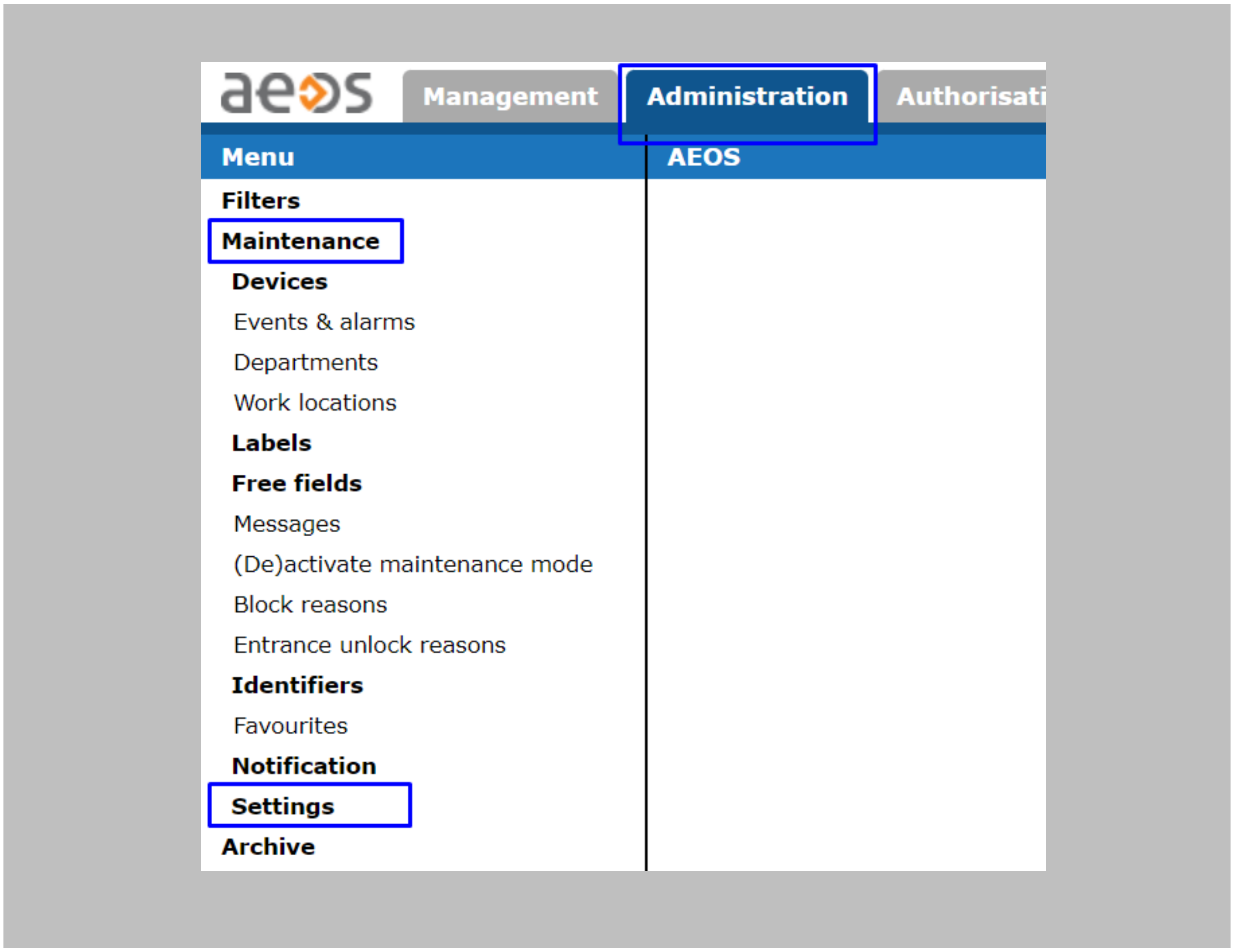


Figure 53: AEOS- Settings

STEP 11

Click on **System Properties.**

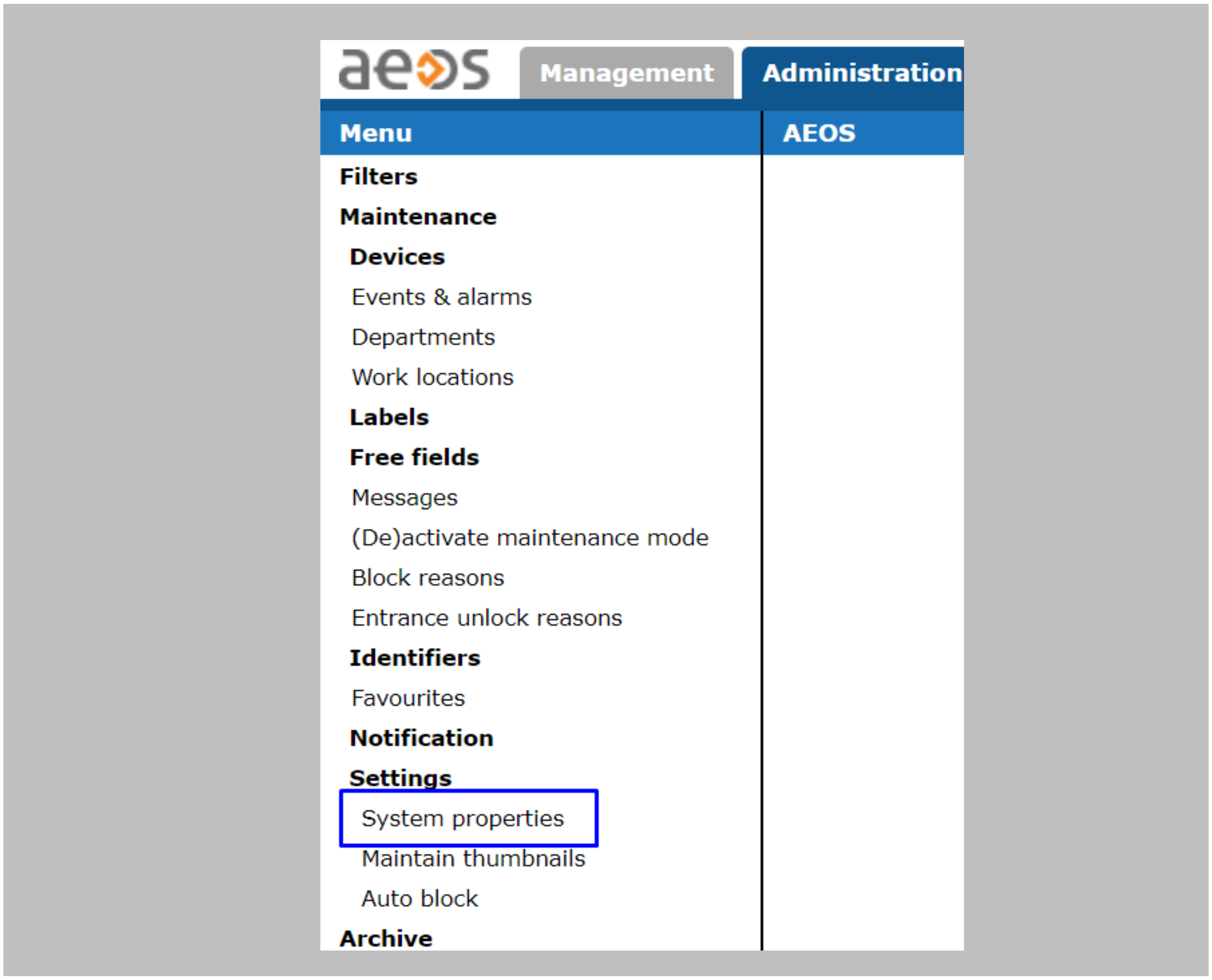
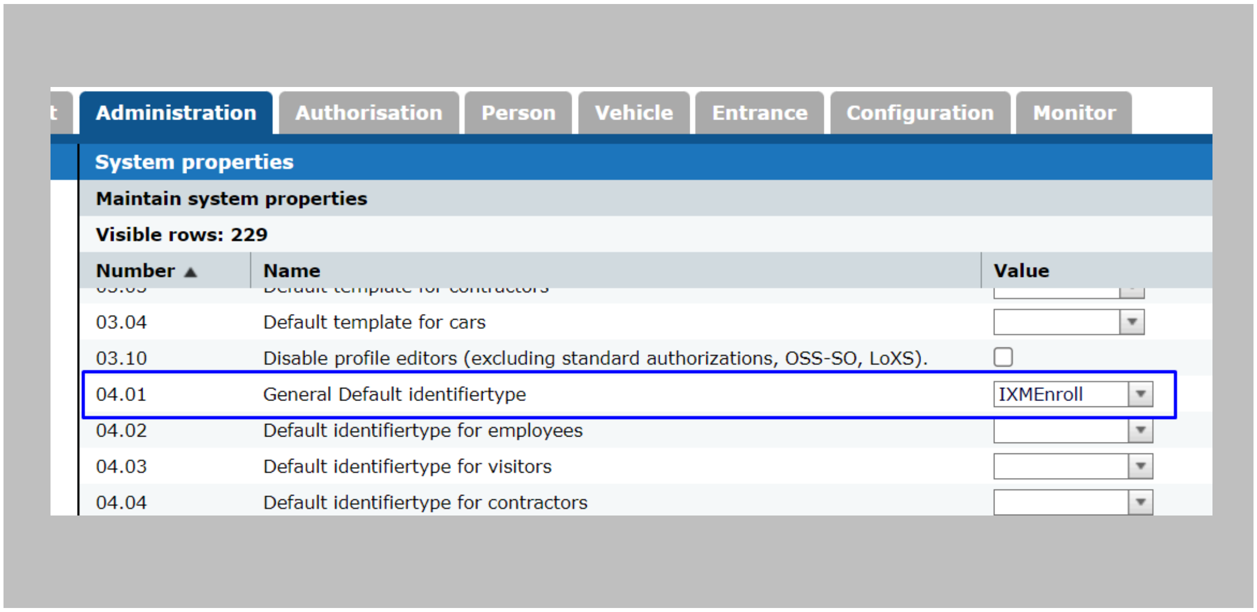


Figure 54: AEOS - System Properties

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’**.



System properties

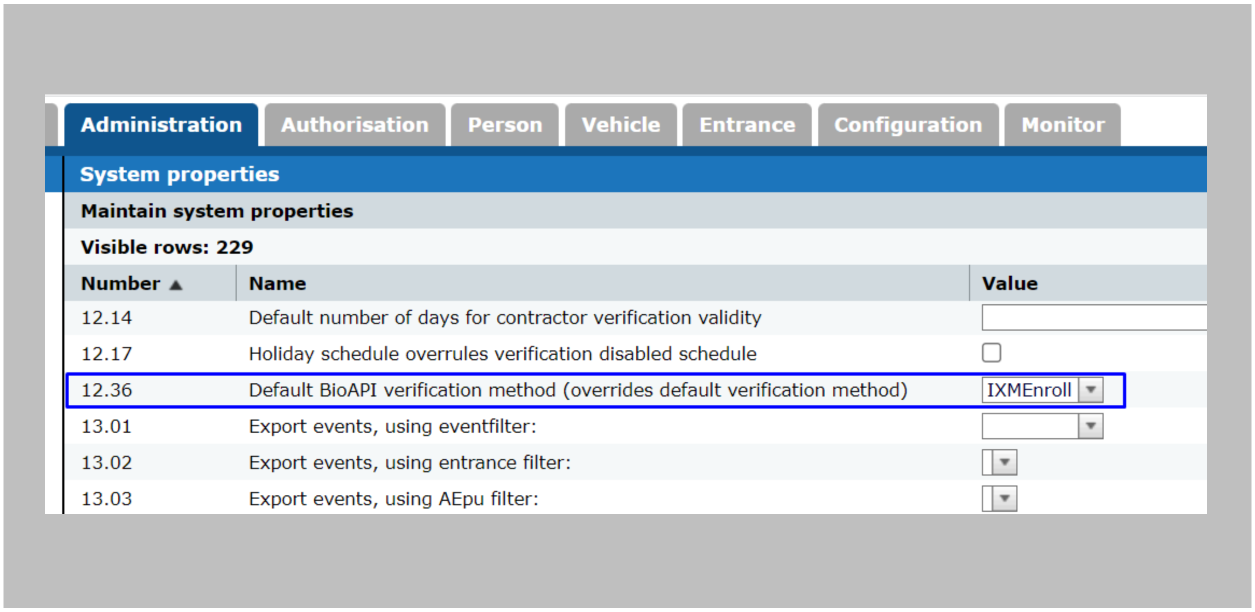
Maintain system properties

Visible rows: 229

Number ▲	Name	Value
03.03	Default template for contractors	
03.04	Default template for cars	
03.10	Disable profile editors (excluding standard authorizations, OSS-SO, LoXS).	□
04.01	General Default identifiertype	IXMEnroll
04.02	Default identifiertype for employees	
04.03	Default identifiertype for visitors	
04.04	Default identifiertype for contractors	

Figure 55: 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'**.



System properties

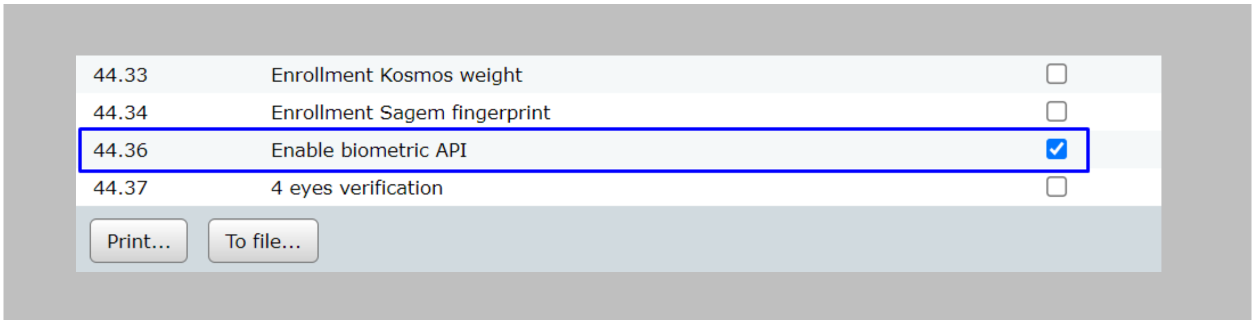
Maintain system properties

Visible rows: 229

Number ▲	Name	Value
12.14	Default number of days for contractor verification validity	
12.17	Holiday schedule overrules verification disabled schedule	□
12.36	Default BioAPI verification method (overrides default verification method)	IXMEnroll ▾
13.01	Export events, using eventfilter:	▾
13.02	Export events, using entrance filter:	▾
13.03	Export events, using AEpu filter:	▾

Figure 56: AEOS - System Properties Default BioAPI Verification

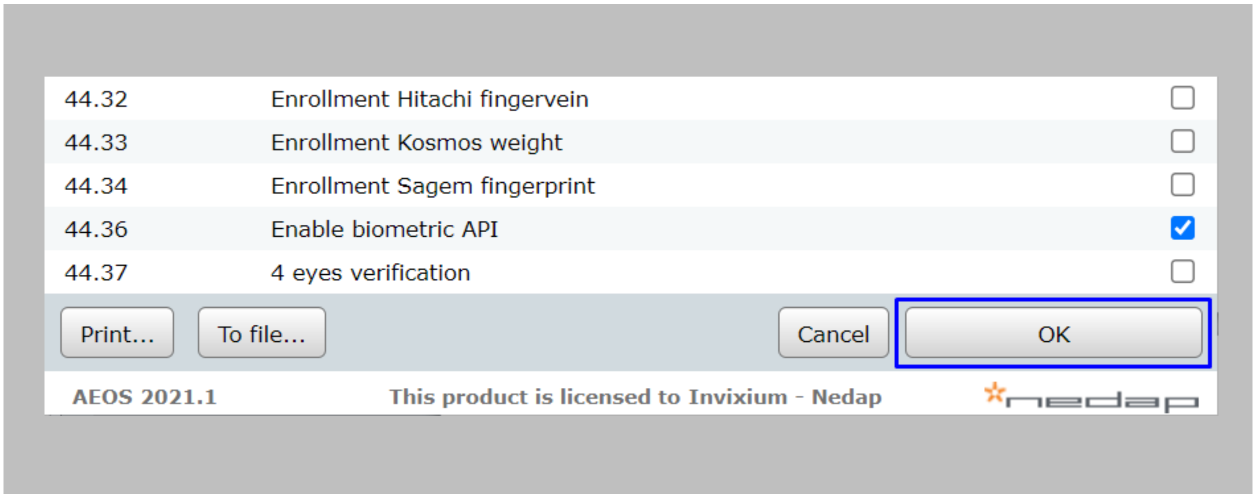
- **44.36 - Enable biometric API:** Select the checkbox to enable **biometric API**.



44.33	Enrollment Kosmos weight	□
44.34	Enrollment Sagem fingerprint	□
44.36	Enable biometric API	☑
44.37	4 eyes verification	□

Figure 57: AEOS - System Properties Enable Biometric API

Click on **OK.**



44.32	Enrollment Hitachi fingervein	□
44.33	Enrollment Kosmos weight	□
44.34	Enrollment Sagem fingerprint	□
44.36	Enable biometric API	☑
44.37	4 eyes verification	□

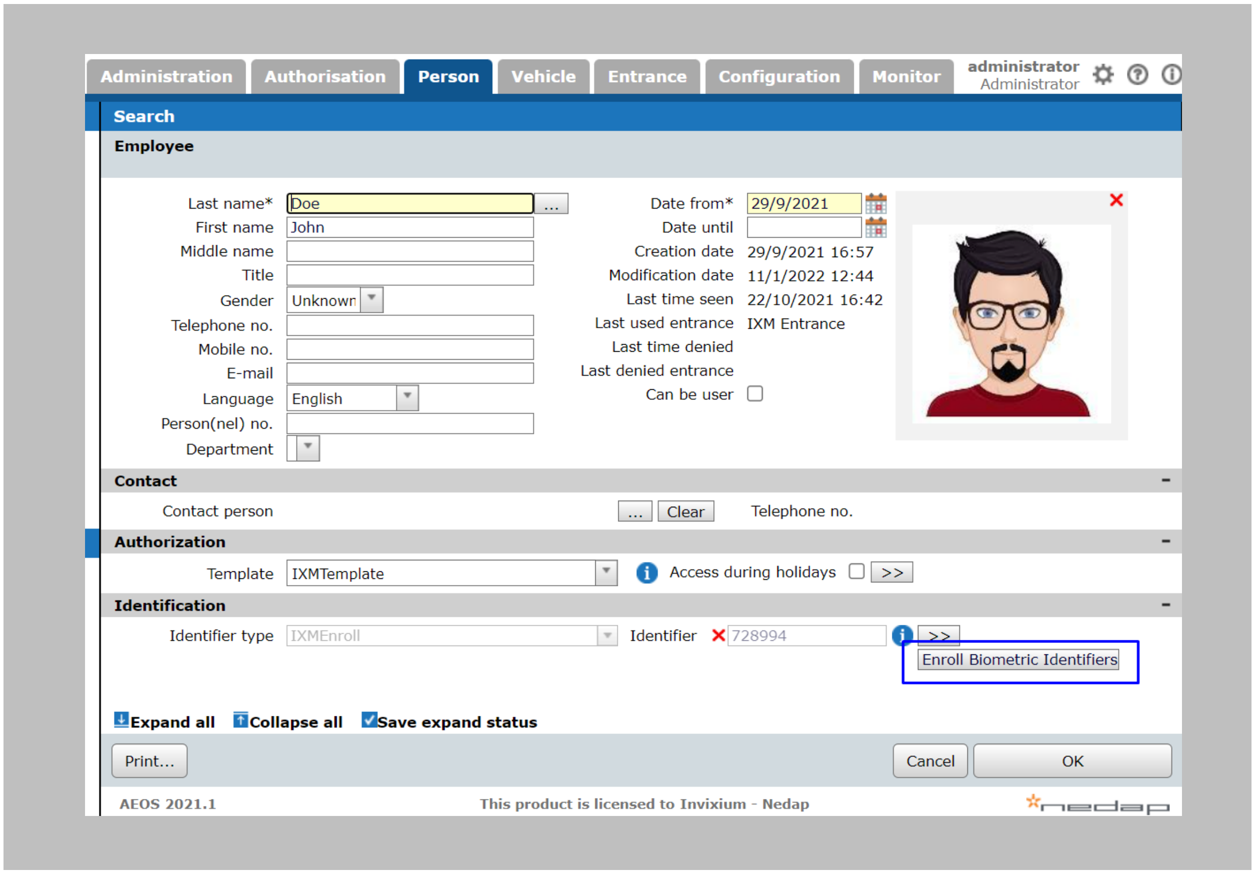
Figure 58: AEOS - Save System Properties

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.



Employee

Last name* Doe

First name John

Middle name

Title

Gender Unknown

Telephone no.

Mobile no.

E-mail

Language English

Person(nel) no.

Department

Date from* 29/9/2021

Date until

Creation date 29/9/2021 16:57

Modification date 11/1/2022 12:44

Last time seen 22/10/2021 16:42

Last used entrance IXM Entrance

Last time denied

Last denied entrance

Can be user □

Contact

Contact person

Telephone no.

Authorization

Template IXMTemplate

Access during holidays □

Identification

Identifier type IXMEnroll

Identifier 728994

☑ Save expand status

AEOS 2021.1

This product is licensed to Invixium - Nedap

Figure 59: AEOS - Enroll Button

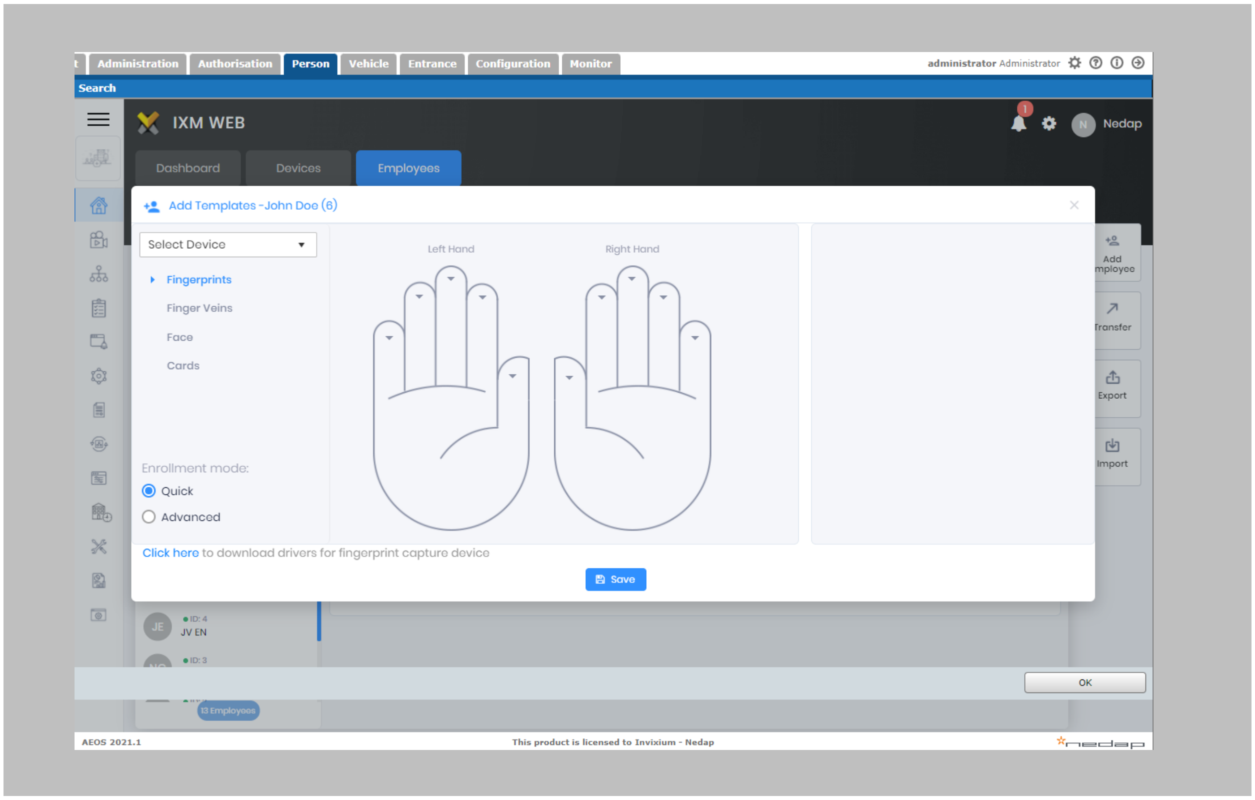
13. Enrollment from Nedap AEOS

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.



Enrollment mode:
● Quick
○ Advanced

Click here to download drivers for fingerprint capture device

This product is licensed to Invixium - Nedap

Figure 60: 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.

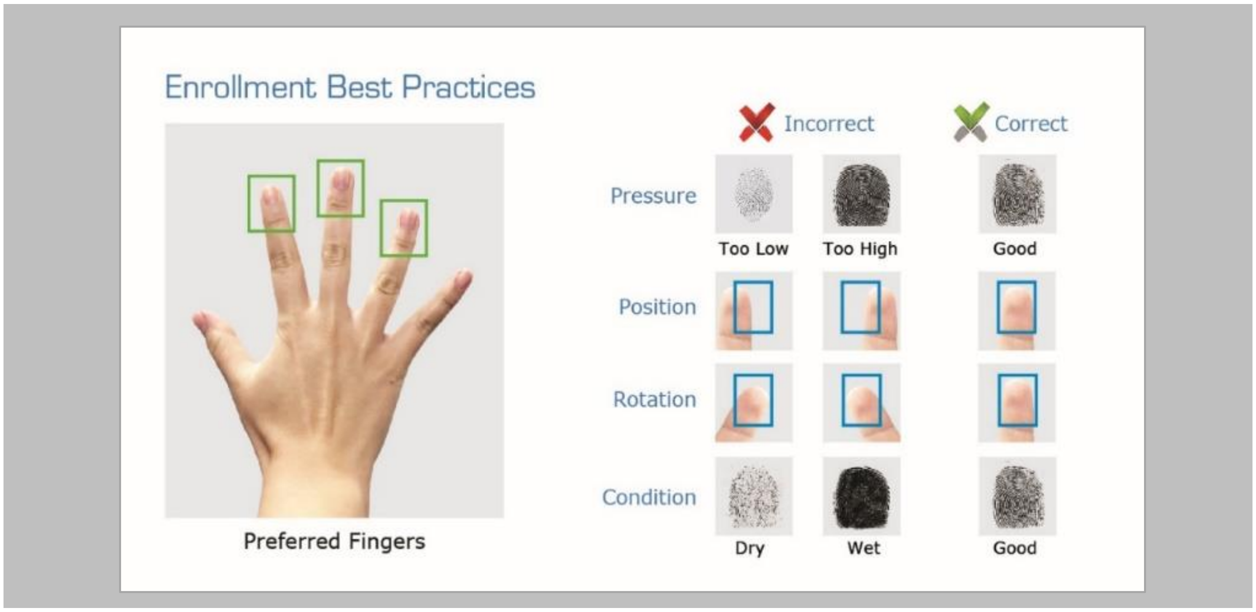


Figure 61: Fingerprint Enrollment Best Practices

Fingerprint Image Samples

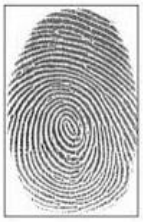
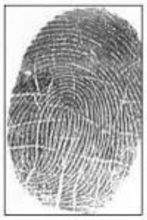
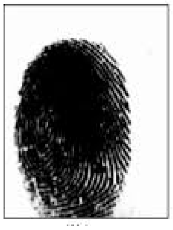
Fingerprint Sample	Result	Recommendation
	Good Fingerprint	Always try and get a good fingerprint like this for a good enrollment score
	Fingerprint with cuts	Invixium recommends using Card + Biometrics or Card + PIN
	Dry finger	Moisten finger and re-enroll for better results
	Wet/Sweaty finger	Rub finger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

Figure 62: 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.

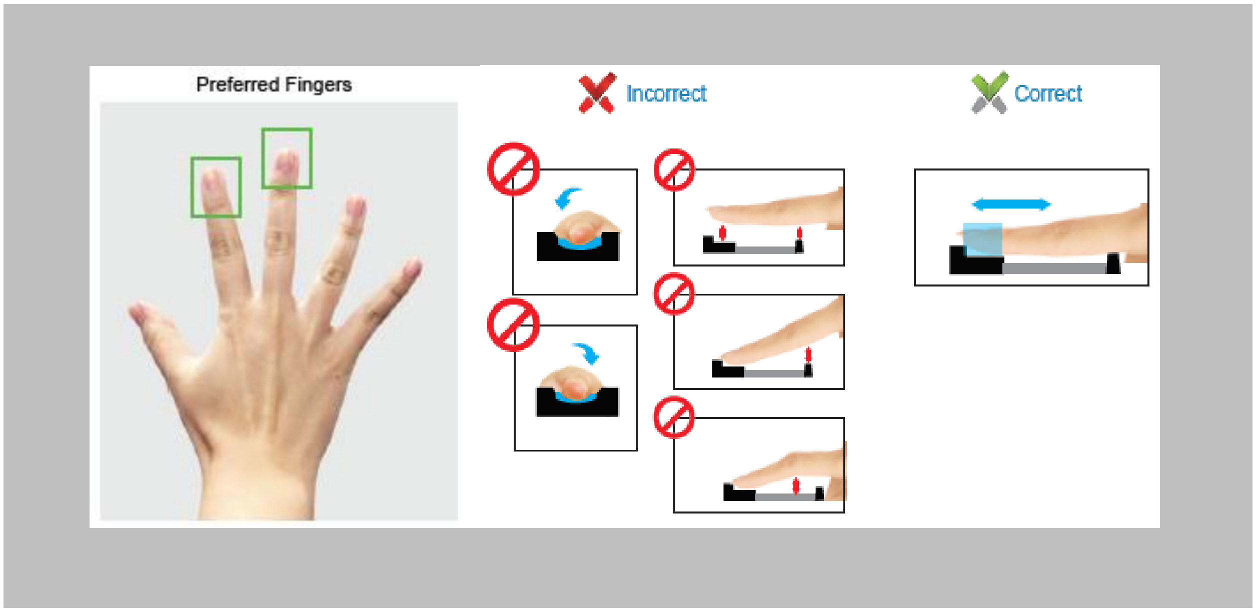


Figure 63: Finger Vein Enrollment Best Practices

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.

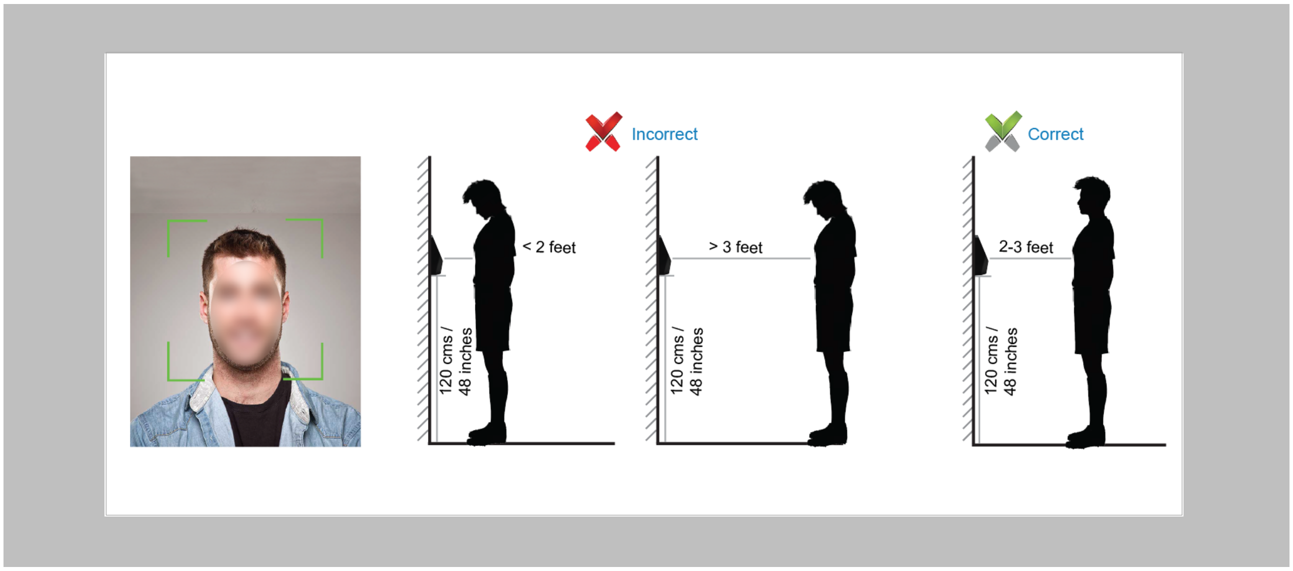


Figure 64: Face Enrollment Best Practices

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.

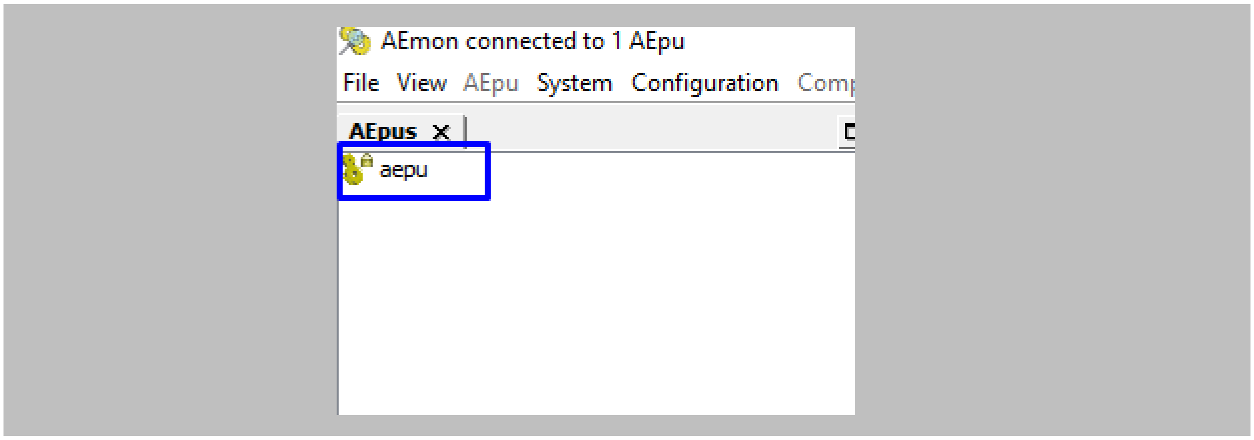

AEmon connected to 1 AEpu
File View AEpu System Configuration Comp
AEpus ✕
aepu

Figure 65: AEmon – Aepu

STEP 2

Go to View → Select Configuration.

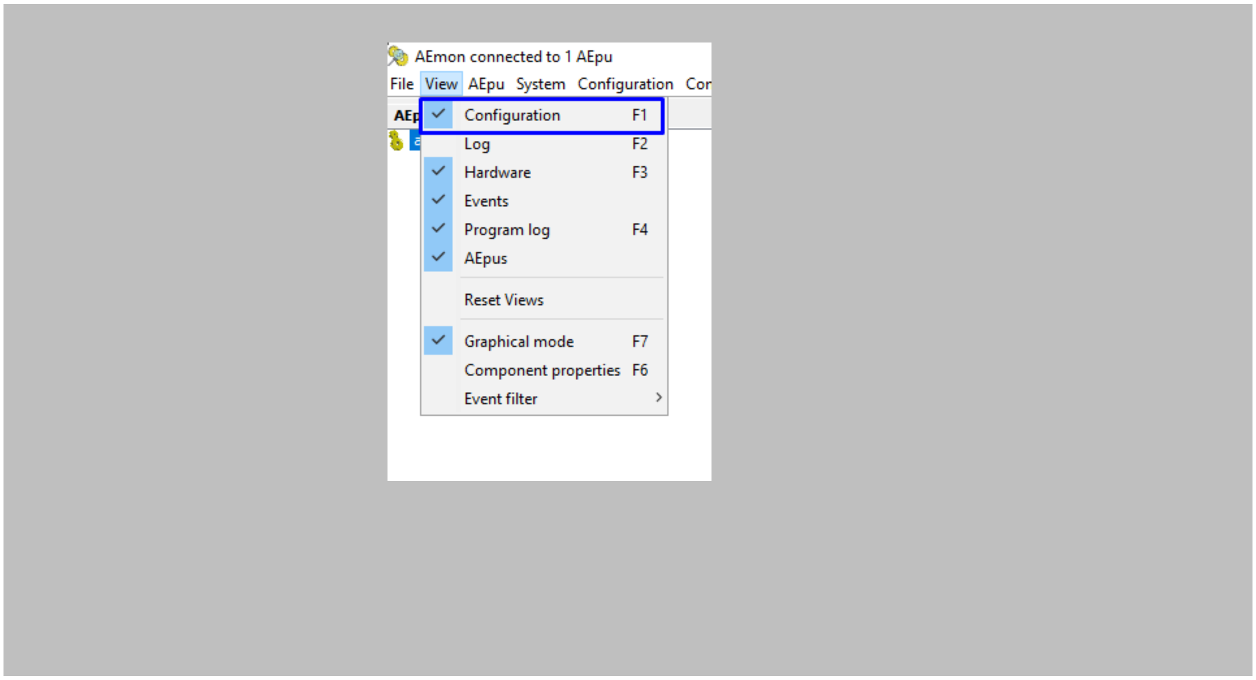
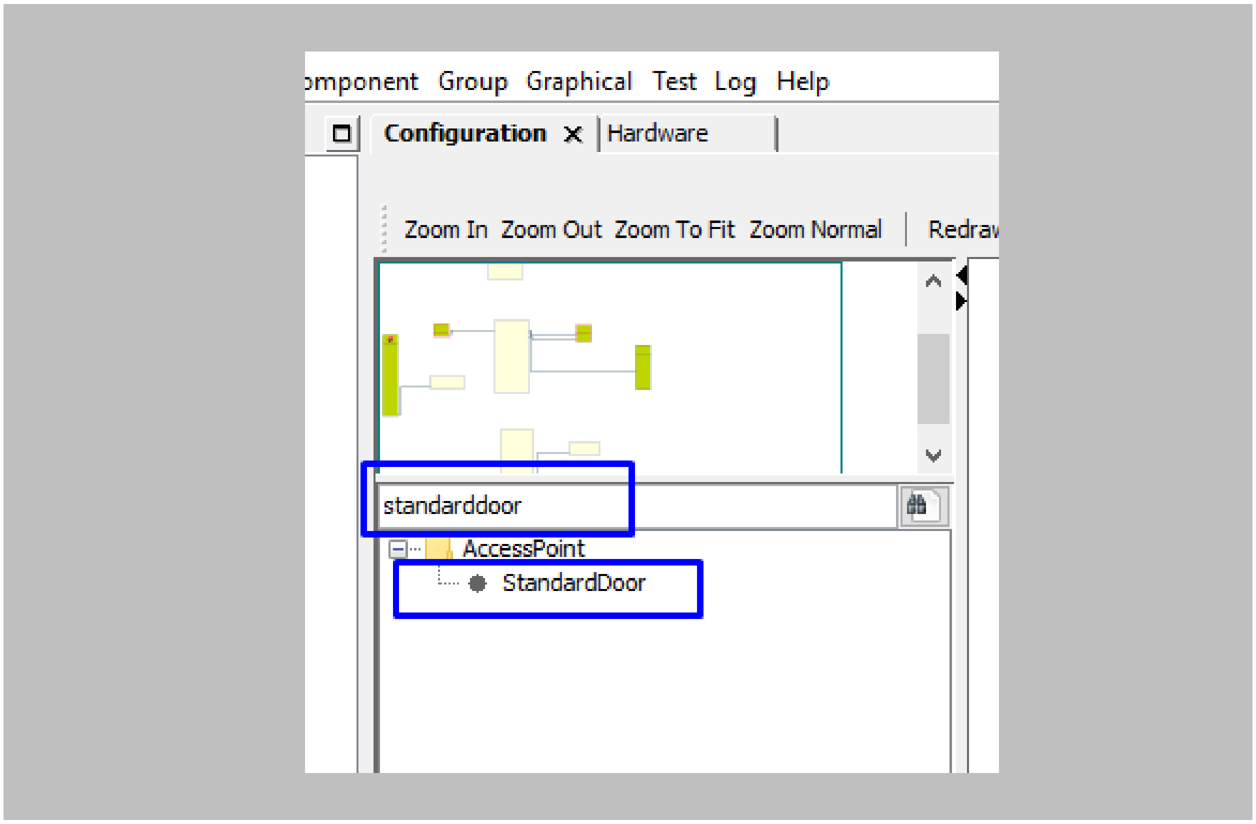


Figure 66: AEmon - AEpu Configuration

STEP 3

On the Configuration window search for StandardDoor → Add StandardDoor.



omponent Group Graphical Test Log Help
Configuration
Hardware
Zoom In Zoom Out Zoom To Fit Zoom Normal
Redraw
AccessPoint
StandardDoor

standarddoor

Figure 67: AEmon - Add Standard Door

STEP 4

Right Click on StandardDoor → Select Rename component.

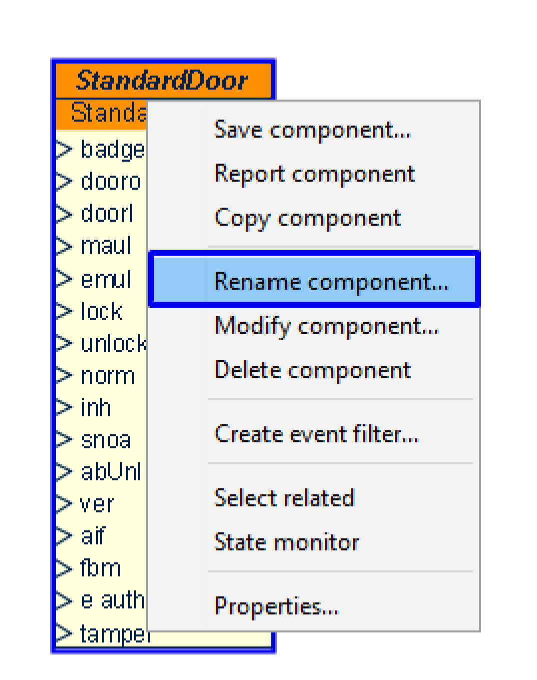


Figure 68: AEmon - Rename Component

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

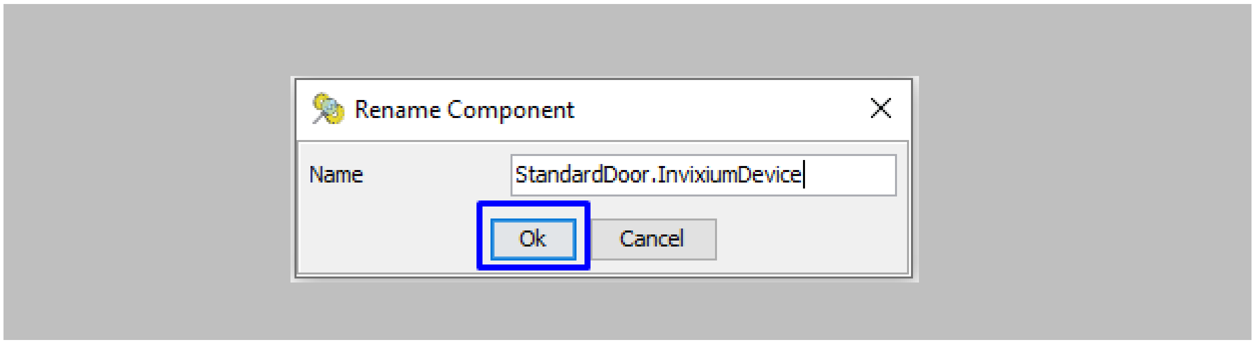


Figure 69: AEmon - Rename Standard Door

STEP 4

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

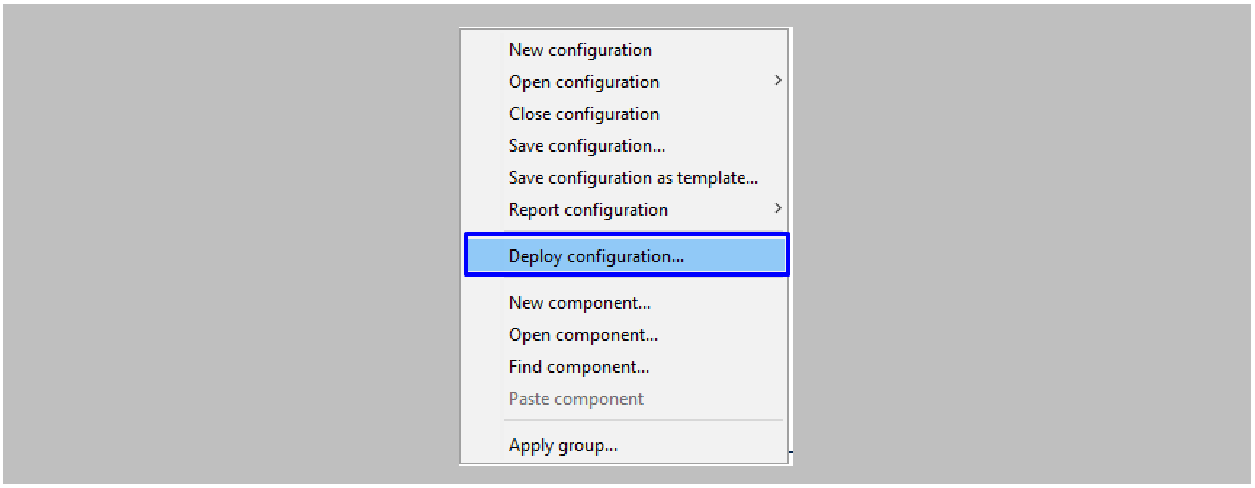


Figure 70: AEmon - Deploy Configuration

STEP 5

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

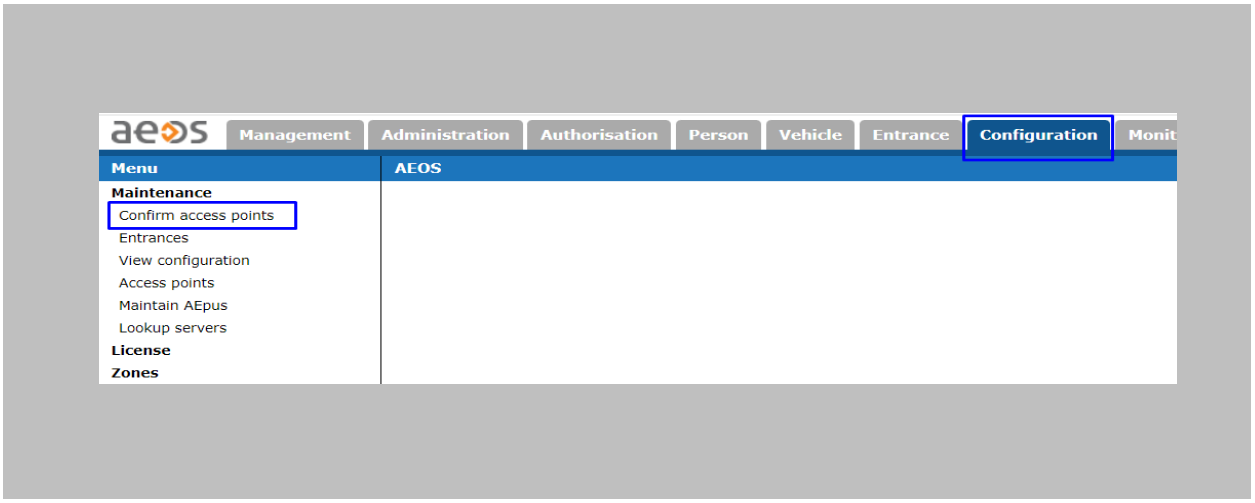
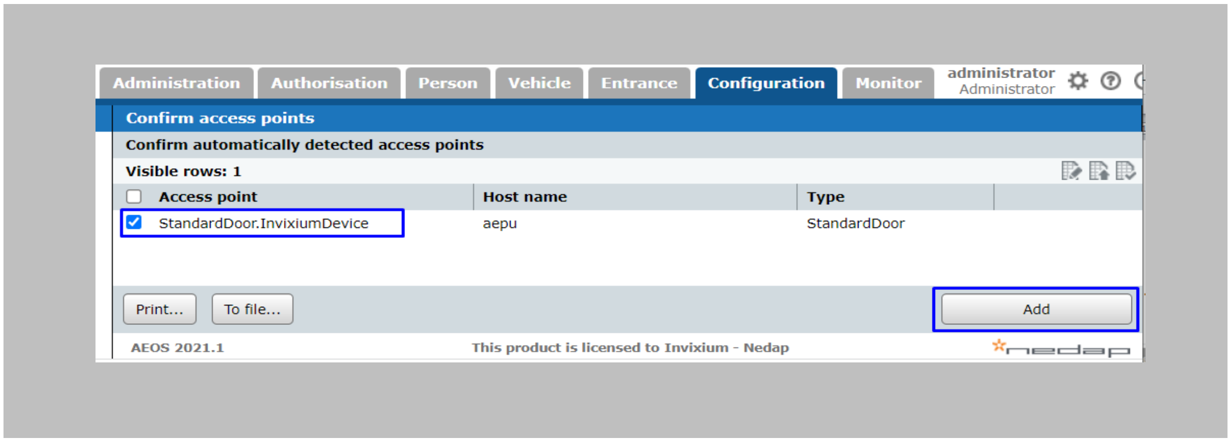


Figure 71: AEOS - Confirm Access Points

STEP 6

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



Confirm access points

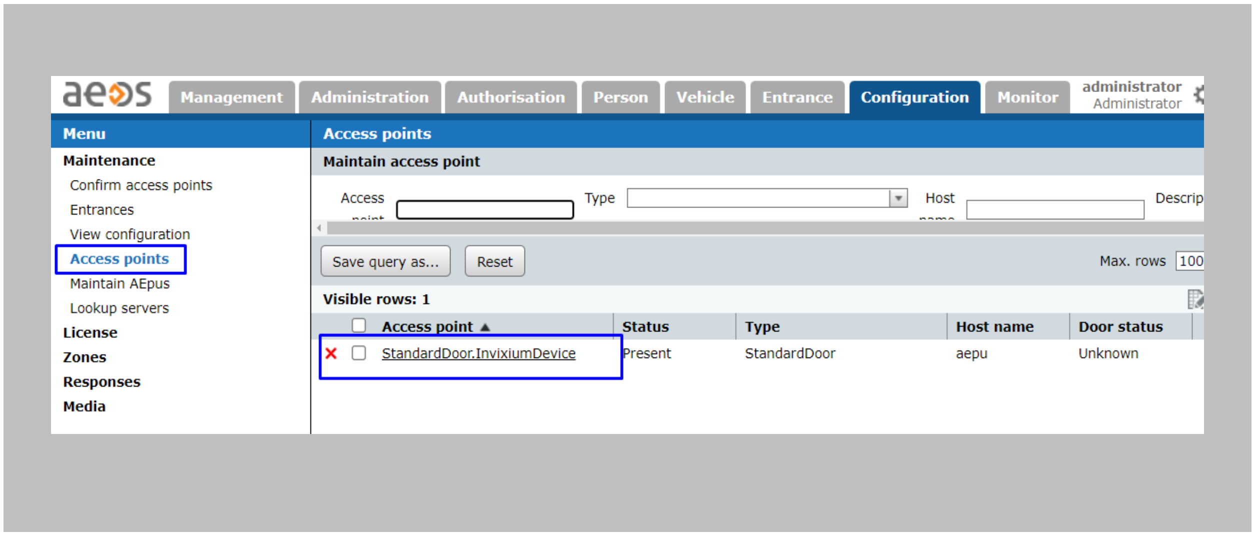
Confirm automatically detected access points

Visible rows: 1

□ Access point	Host name	Type
☑ StandardDoor.InvixiumDevice	aepu	StandardDoor

Figure 72: 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.**



	Access point ▲	Status	Type	Host name	Door status
✕ □	StandardDoor.InvixiumDevice	Present	StandardDoor	aepu	Unknown

Figure 73: AEOS - Access Point

STEP 7

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

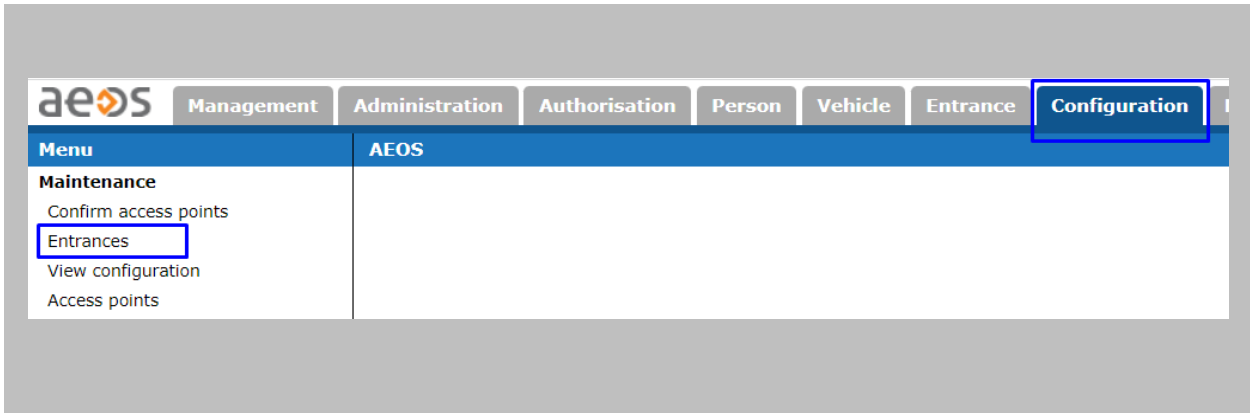
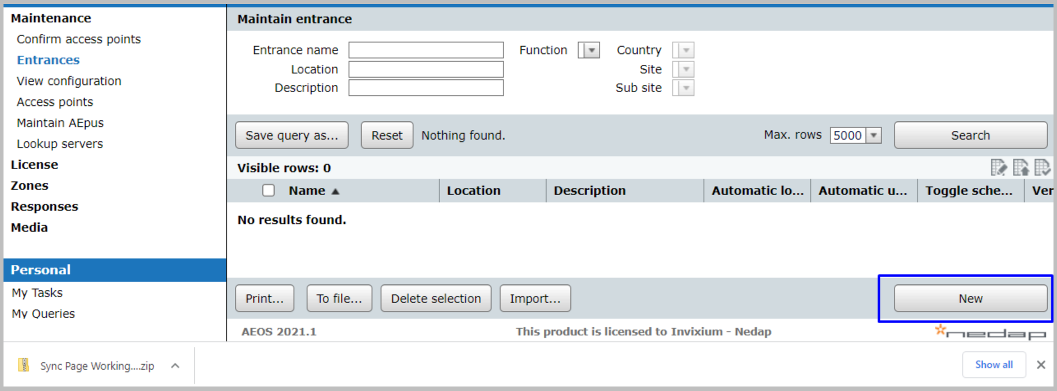


Figure 74: AEOS – Entrances

Click on the **New** button.



Nothing found.

No results found.

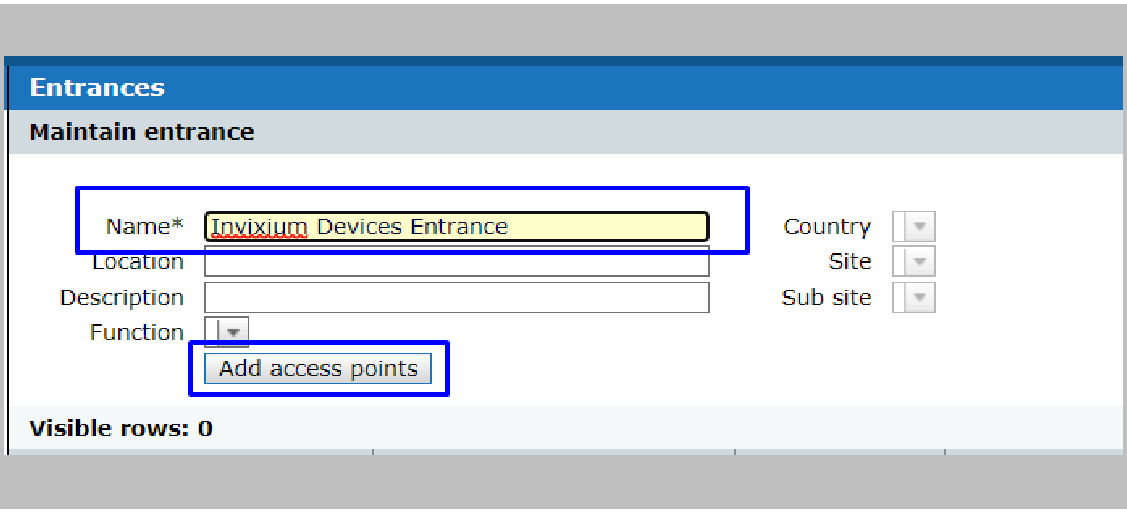
AEOS 2021.1

This product is licensed to Invixium - Nedap

Figure 75: AEOS - New Entrance

STEP 8

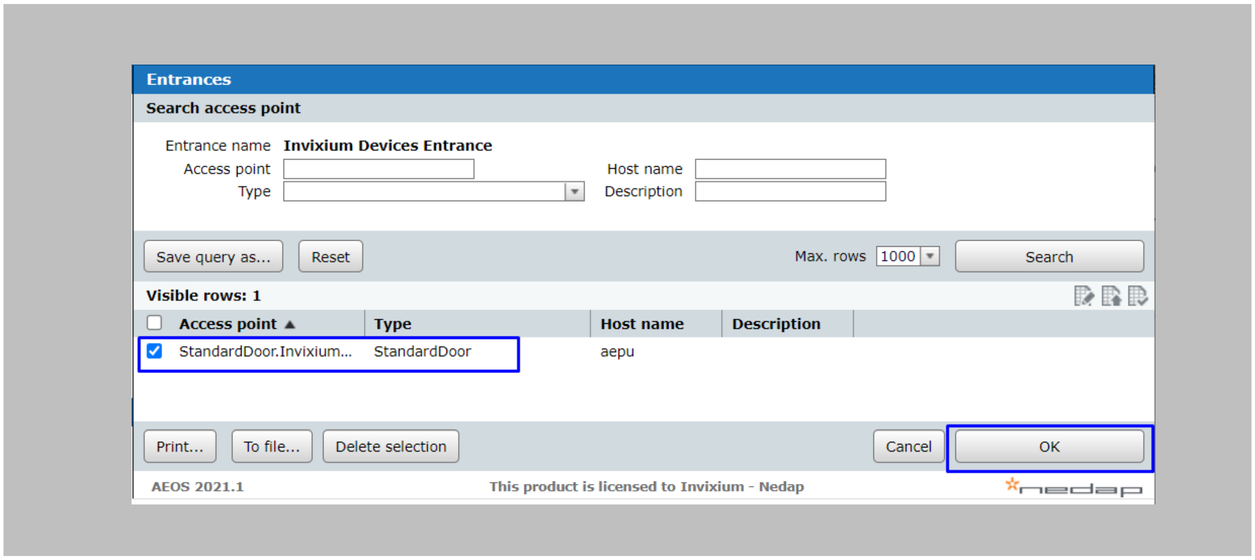
Define **Entrance Name** → Click on **Add Access Points** button.



Name* Invixium Devices Entrance

Figure 76: AEOS - Create New Entrance

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



Entrances

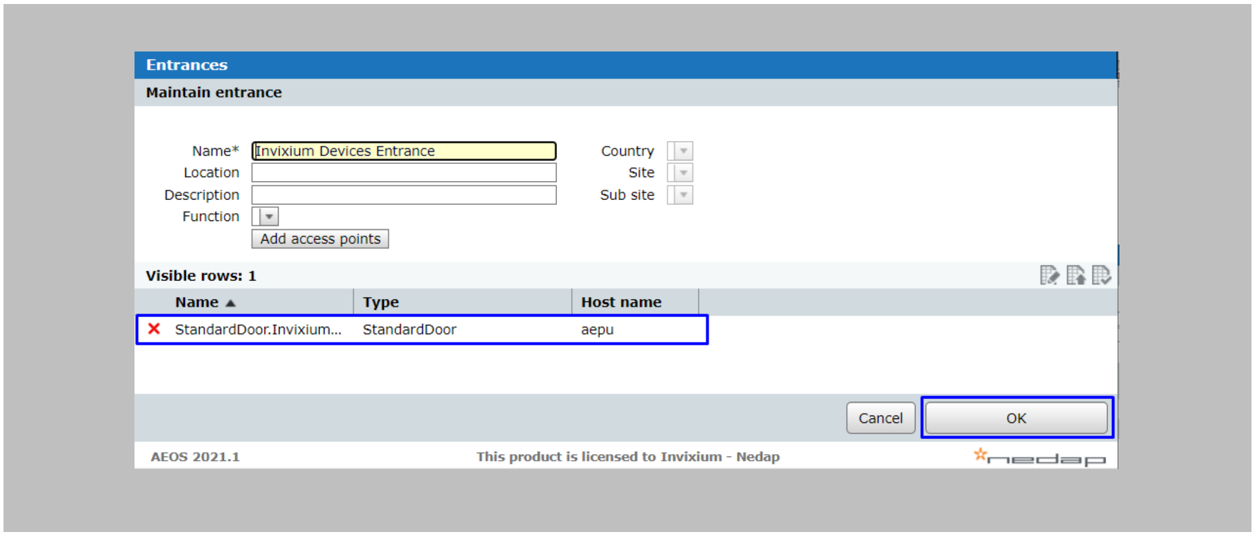
Search access point

Entrance name **Invixium Devices Entrance**

Access point	☑	Type	Host name	Description
StandardDoor.Invixium...	☑	StandardDoor	aepu	

Figure 77: AEOS - Add Access Point in Entrance

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



Entrances

Maintain entrance

Name* Invixium Devices Entrance

Name	Type	Host name
✗ StandardDoor.Invixium...	StandardDoor	aepu

Figure 78: AEOS - Save Entrance

STEP 9

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

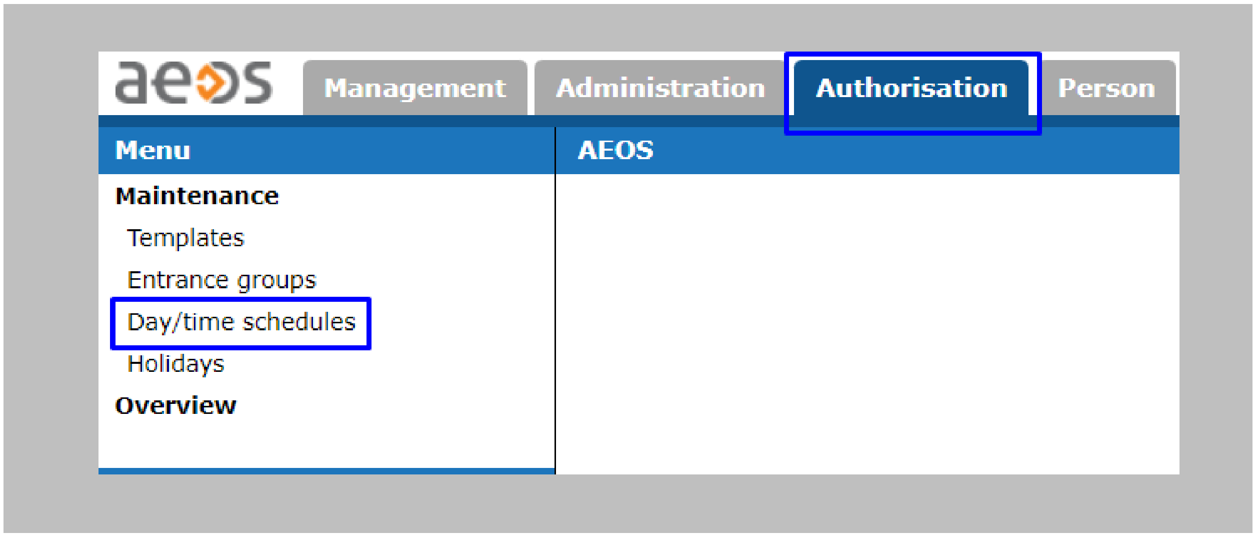
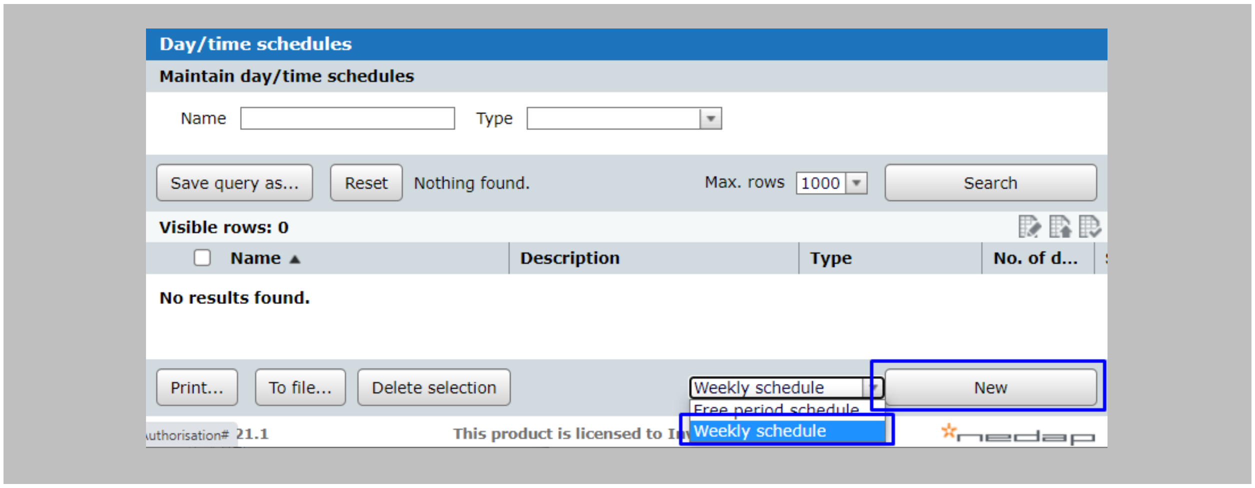


Figure 79: AEOS – DayTimeSchedules

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


Day/time schedules

Maintain day/time schedules

Nothing found.

Max. rows 1000

Visible rows: 0

□ Name ▲	Description	Type	No. of d...

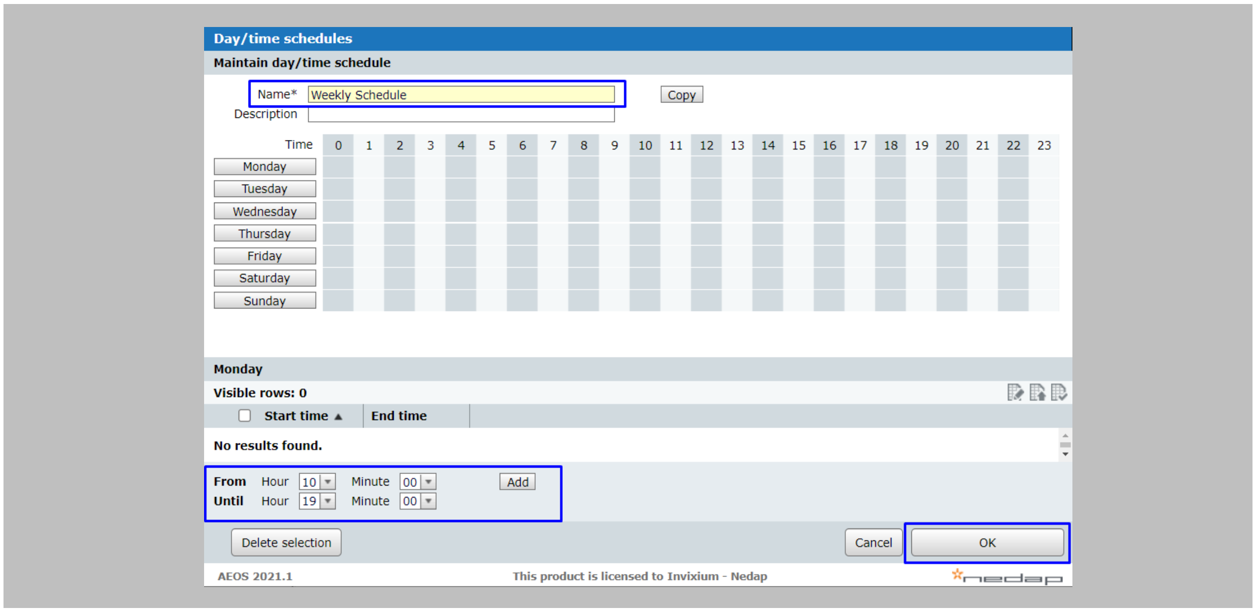
No results found.

Weekly schedule

Figure 80: 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.



Day/time schedules

Maintain day/time schedule

Name* Weekly Schedule

Description

Monday

Visible rows: 0

No results found.

From Hour 10 Minute 00

Until Hour 19 Minute 00

AEOS 2021.1

This product is licensed to Invixium - Nedap

Figure 81: AEOS - Define Weekly Schedule

STEP 11

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

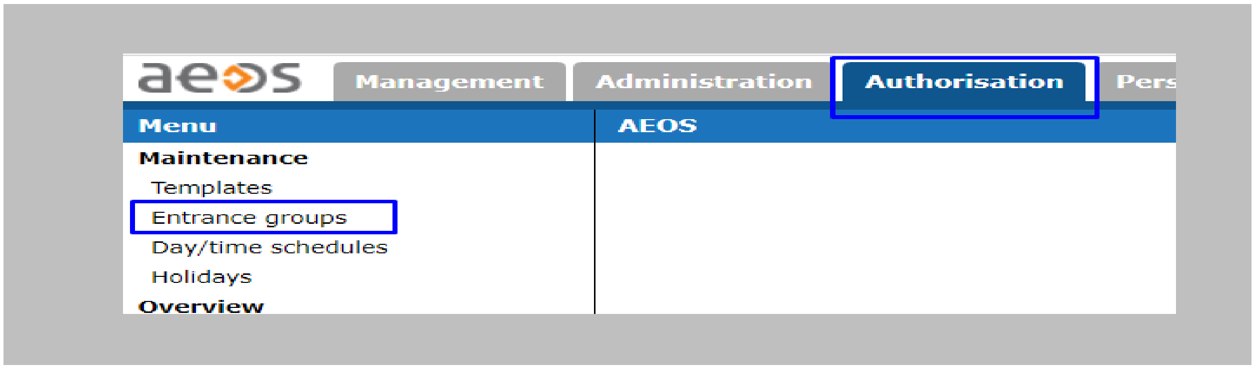
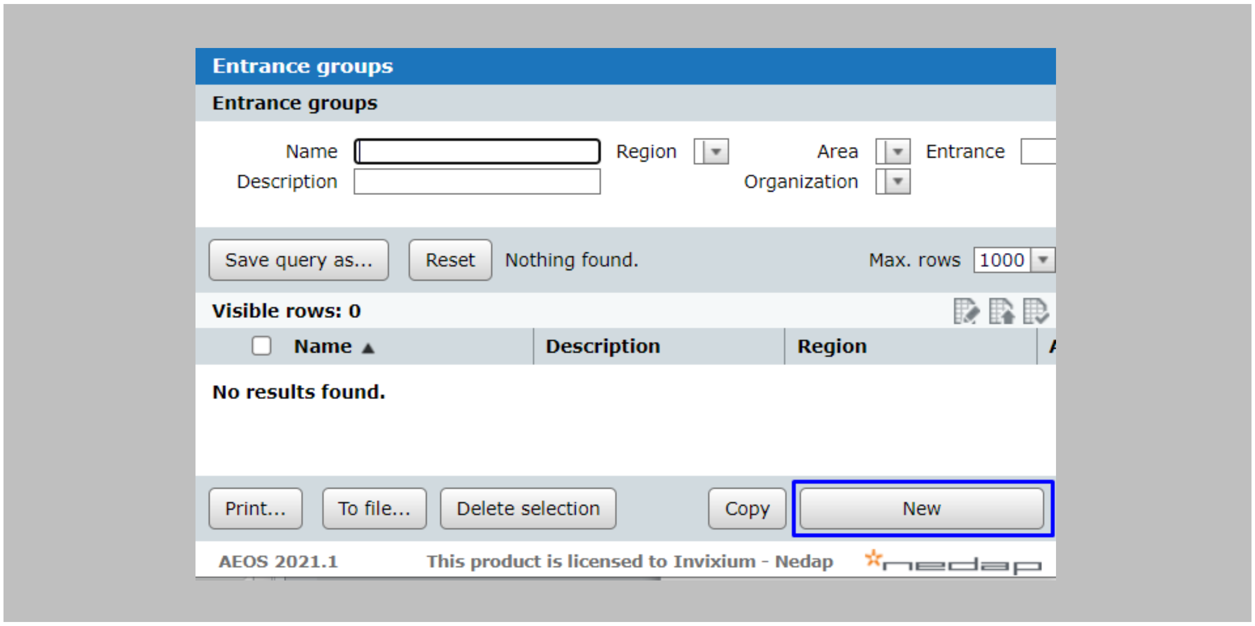


Figure 82: AEOS - Entrance Groups

Click on the **New** button.



Nothing found.

Max. rows 1000

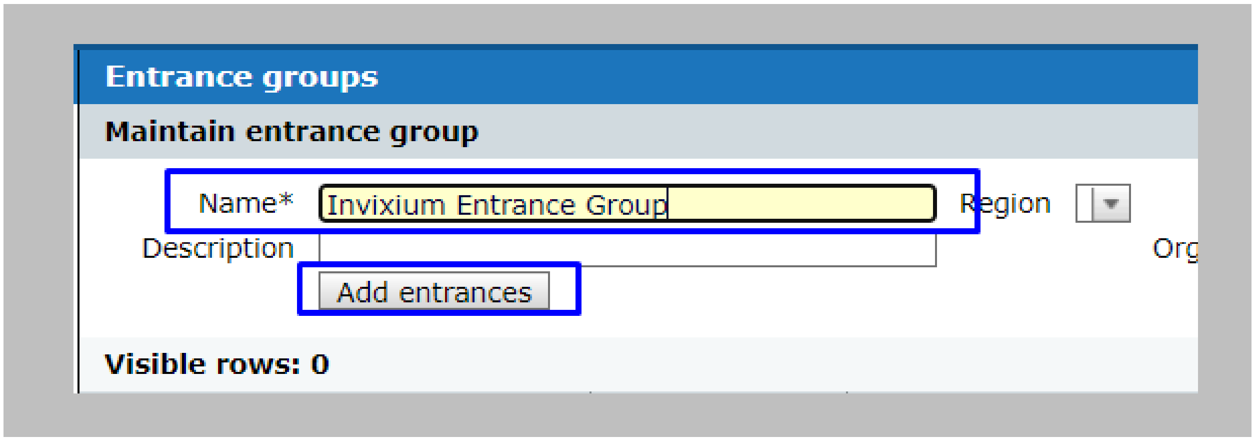
No results found.

AEOS 2021.1 This product is licensed to Invixium - Nedap

Figure 83: AEOS - New Entrance Group

STEP 12

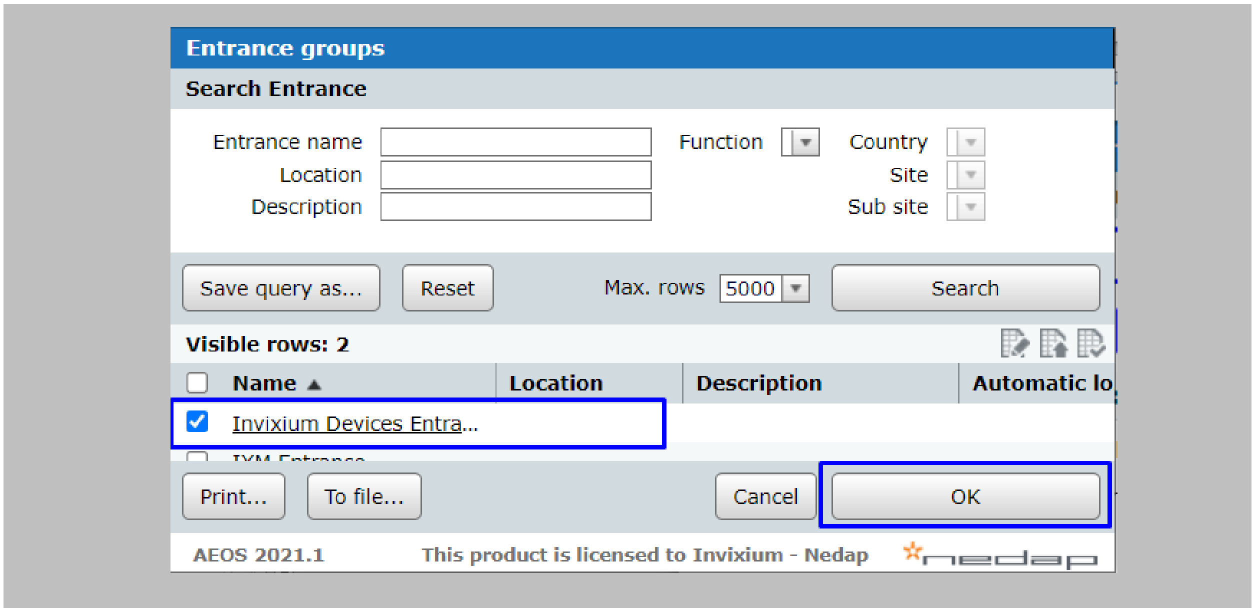
Define **Entrance Group Name** → Click on **Add Entrances** button.



Name* Invixium Entrance Group

Figure 84: AEOS - Add Entrance in Entrance Group

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



Entrance groups

Search Entrance

Entrance name

Location

Description

Function

Country

Site

Sub site

Max. rows 5000

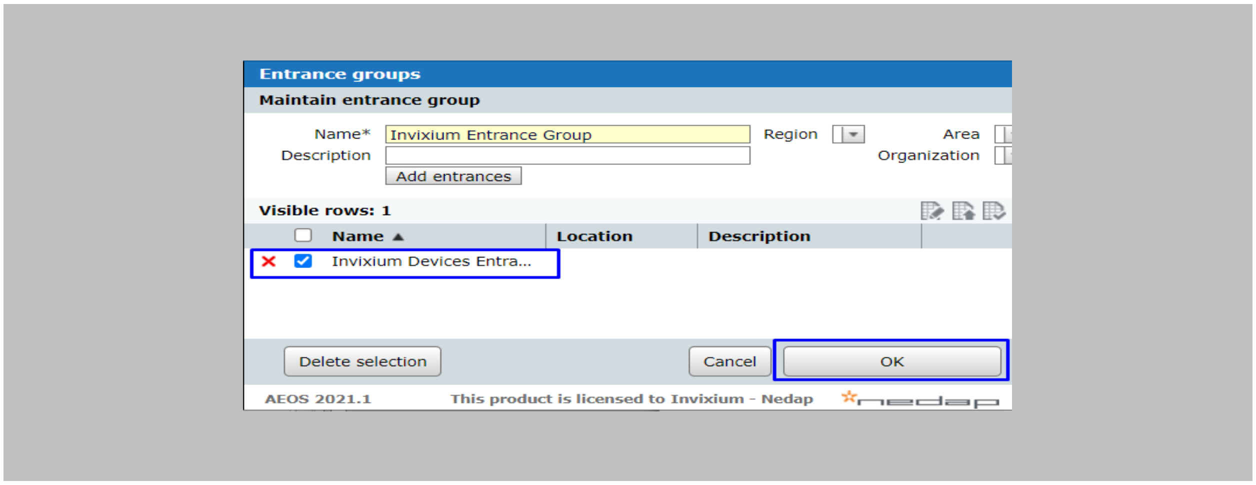
Visible rows: 2

□	Name ▲	Location	Description	Automatic lo
☑	Invixium Devices Entra...			
□	IXM Entrance			

AEOS 2021.1 This product is licensed to Invixium - Nedap

Figure 85: AEOS - Add Entrance Group

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



Entrance groups

Maintain entrance group

Name* Invixium Entrance Group

Description

Region

Area

Organization

Visible rows: 1

	□	Name ▲	Location	Description
✕	☑	Invixium Devices Entra...		

AEOS 2021.1 This product is licensed to Invixium - Nedap

Figure 86: AEOS - Save Entrance Group

STEP 13

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

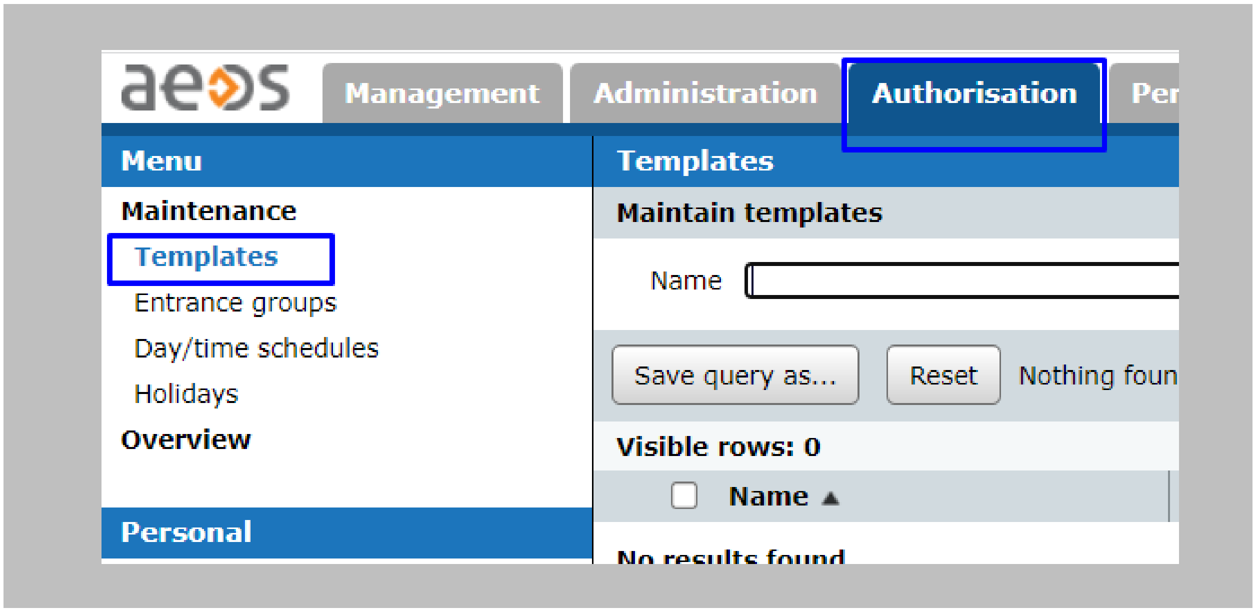


Figure 87: AEOS – Template

Click on the **New** button.

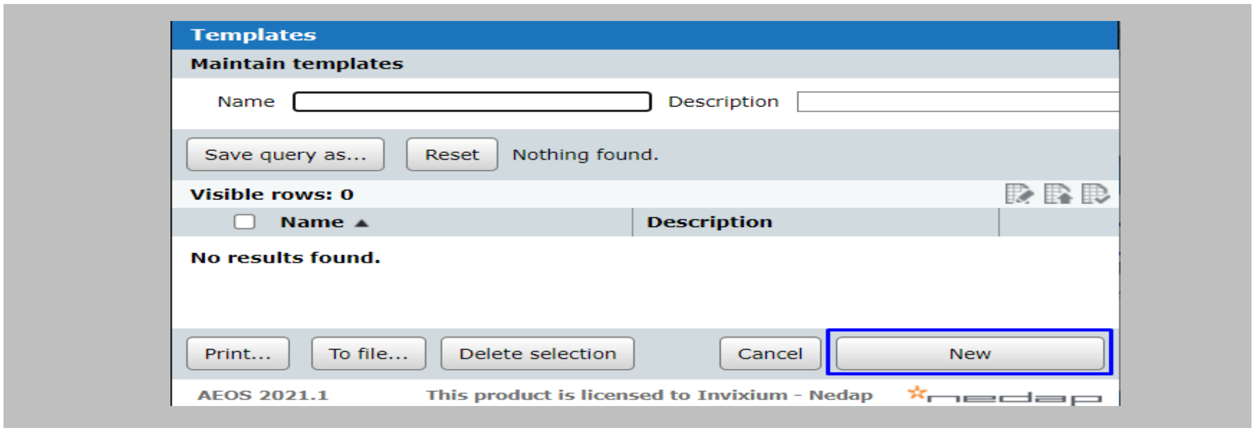
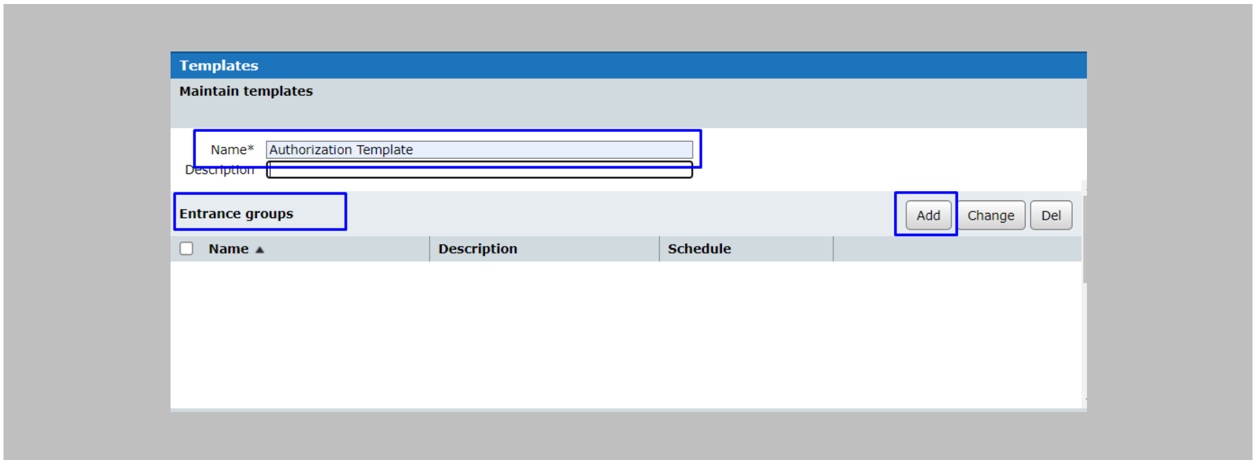


Figure 88: AEOS - New Template

STEP 14

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

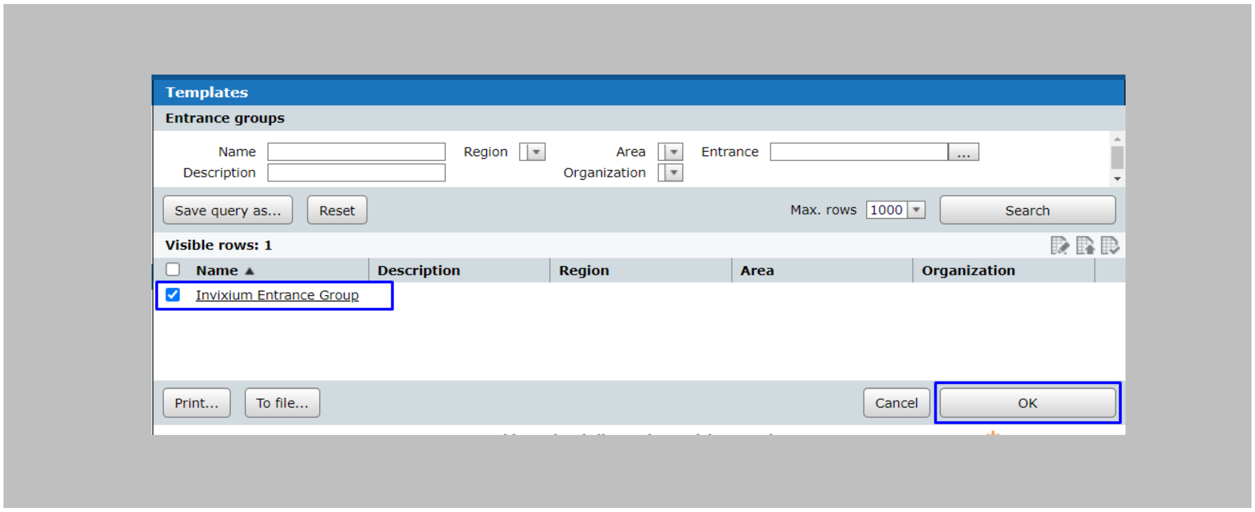


Name* Authorization Template
Description

□ Name ▲	Description	Schedule

Figure 89: AEOS Template - Add Entrance Group

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

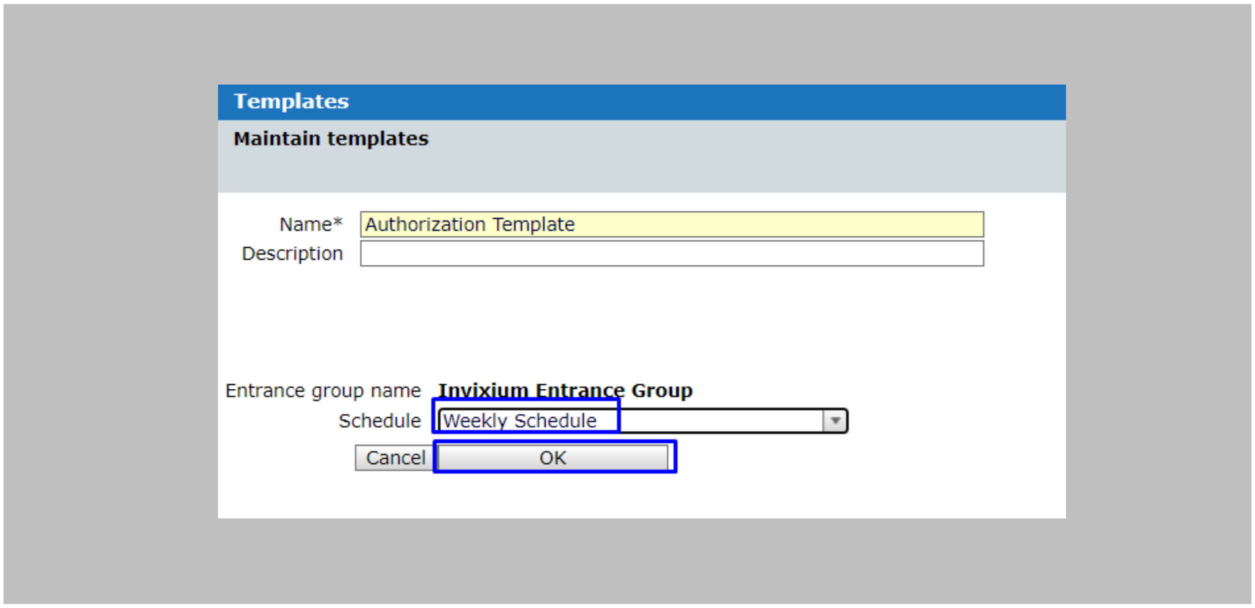


Visible rows: 1

□ Name ▲	Description	Region	Area	Organization
☑ Invixium Entrance Group				

Figure 90: AEOS Template - Add Entrance Group

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



Templates

Maintain templates

Name* Authorization Template

Description

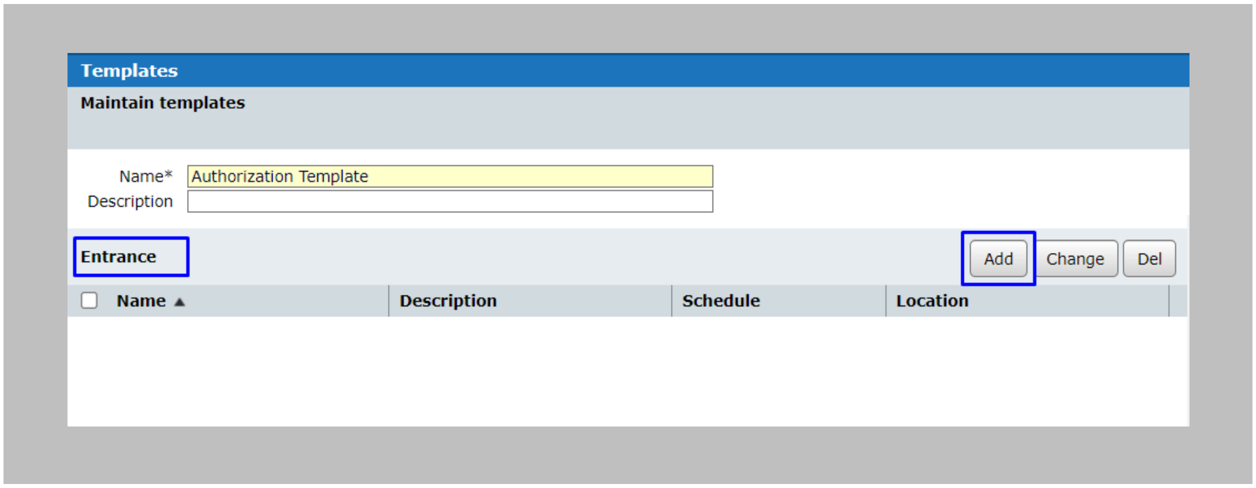
Entrance group name **Invixium Entrance Group**

Schedule Weekly Schedule

Figure 91: AEOS Template - Assign Schedule to Entrance Group

STEP 15

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



Templates

Maintain templates

Name* Authorization Template

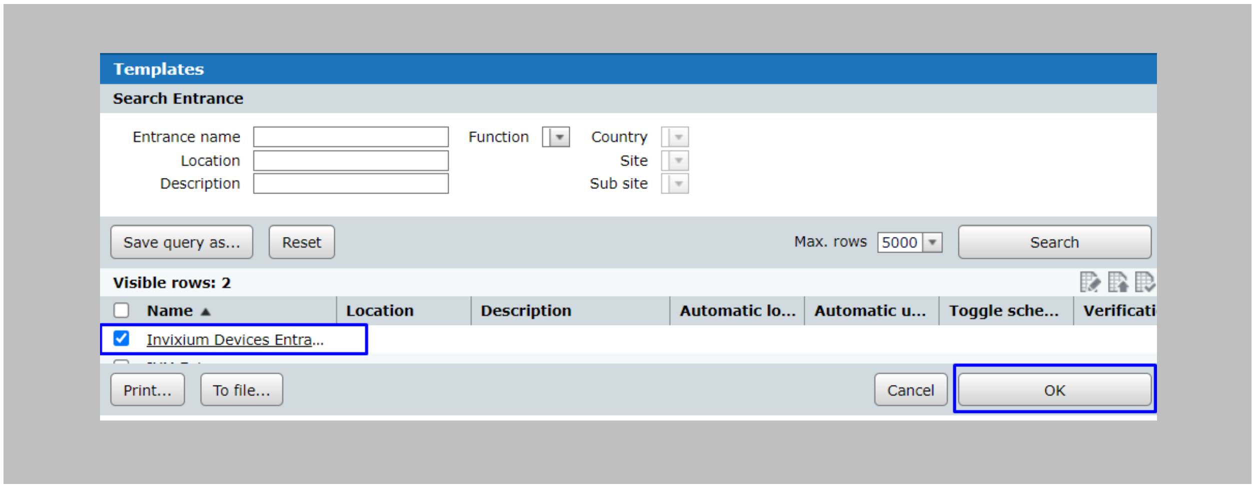
Description

Entrance

☐ Name ▲	Description	Schedule	Location

Figure 92: AEOS Template - Add Entrance

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



Templates

Search Entrance

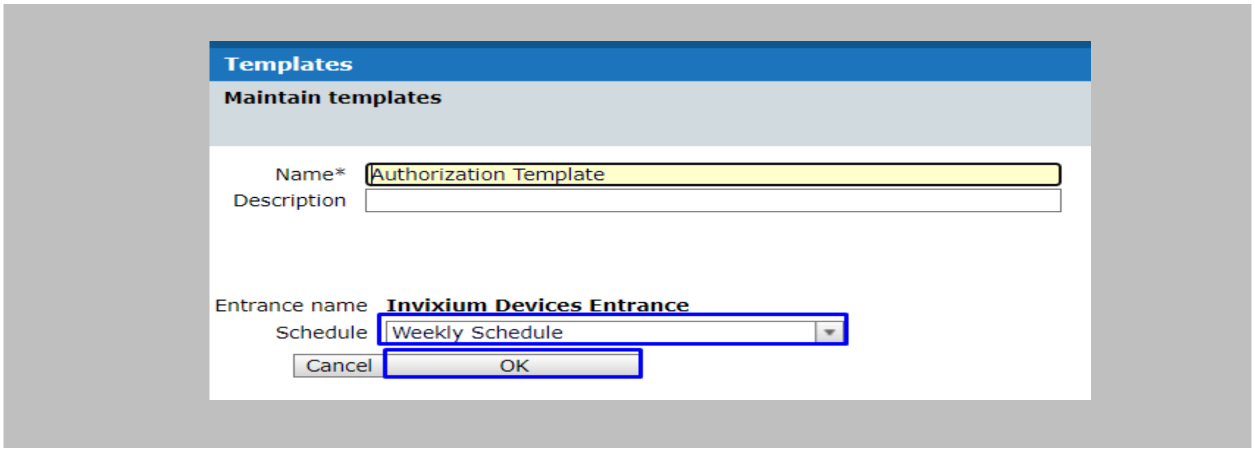
Entrance name
Location
Description
Function
Country
Site
Sub site

Visible rows: 2

□ Name ▲	Location	Description	Automatic lo...	Automatic u...	Toggle sche...	Verificati
☑ Invixium Devices Entra...						

Figure 93: AEOS Template - Save Entrance

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



Templates

Maintain templates

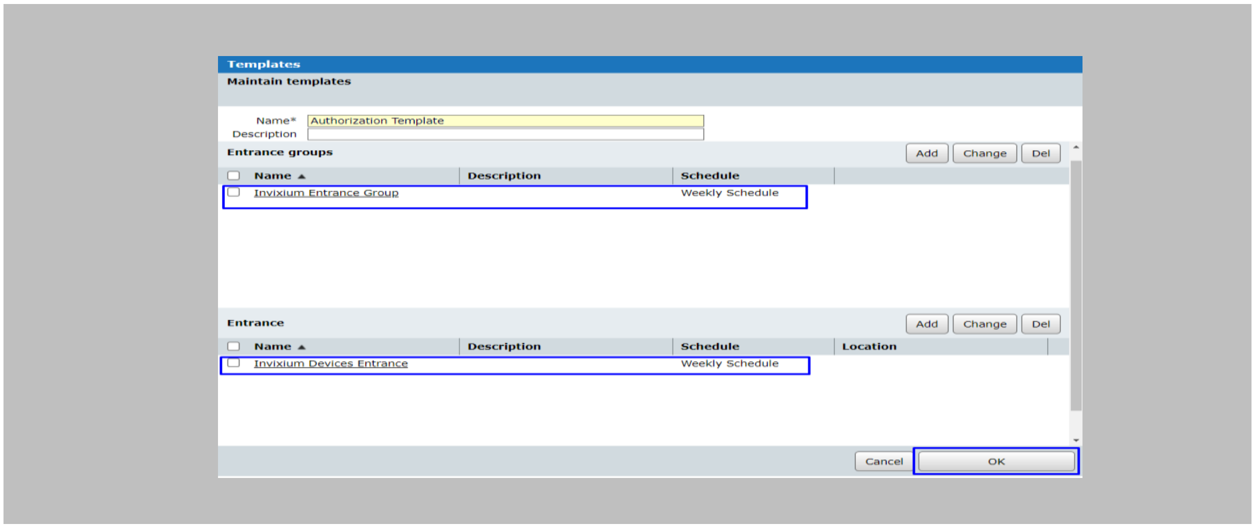
Name* Authorization Template
Description

Entrance name **Invixium Devices Entrance**
Schedule Weekly Schedule

Figure 94: AEOS Template - Assign Schedule to Entrance

STEP 16

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



Templates

Maintain templates

Name* Authorization Template

Description

Entrance groups

☐	Name ▲	Description	Schedule
☐	Invixium Entrance Group		Weekly Schedule

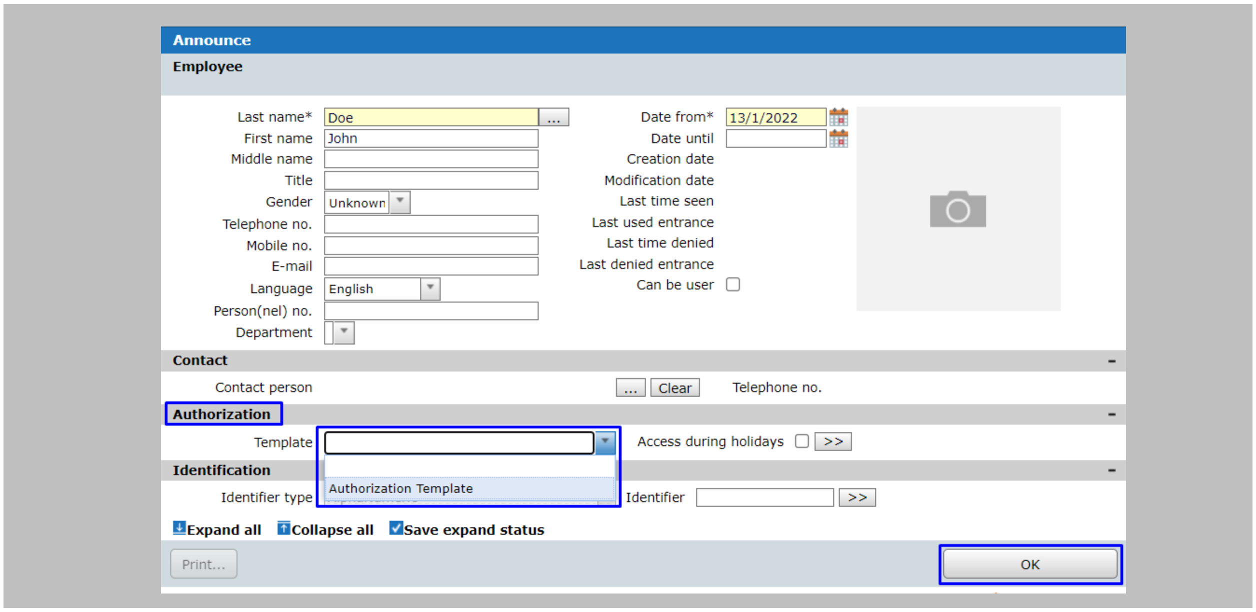
Entrance

☐	Name ▲	Description	Schedule	Location
☐	Invixium Devices Entrance		Weekly Schedule	

Figure 95: 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.



Announce

Employee

Last name*	Doe	Date from*	13/1/2022
First name	John	Date until	
Middle name		Creation date	
Title		Modification date	
Gender	Unknown	Last time seen	
Telephone no.		Last used entrance	
Mobile no.		Last time denied	
E-mail		Last denied entrance	
Language	English	Can be user	□
Person(nel) no.			
Department			

Contact

Contact person ... Clear Telephone no.

Authorization

Template: Authorization Template — Access during holidays □ >>

Identification

Identifier type — Identifier >>

Expand all — Collapse all — ☑ Save expand status

Figure 96: 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:

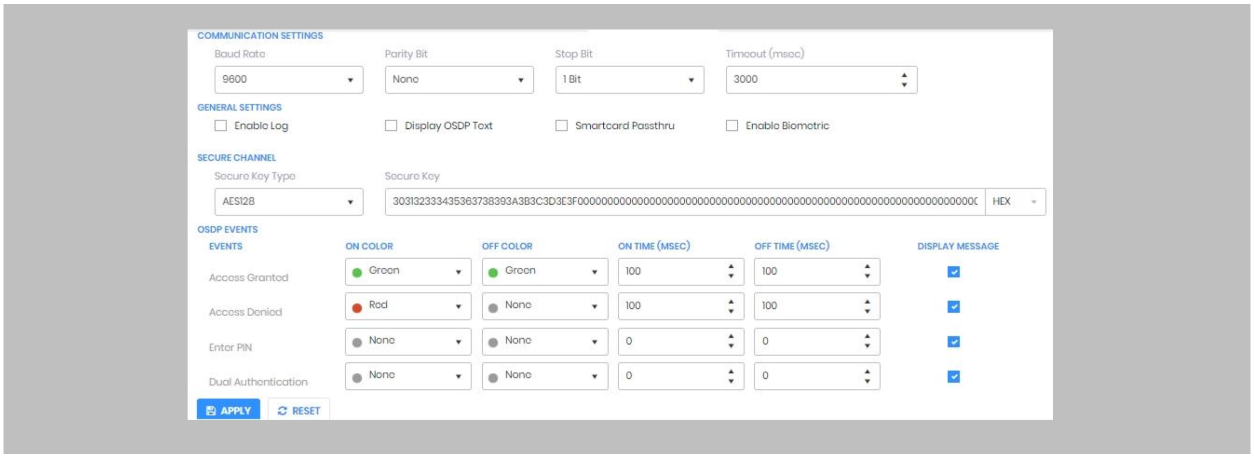
1. The Nedap panel needs OSDP-supported firmware to use OSDP communication with the Invixium device. It can be found at the default location of AEOS i.e., C:\AEOS\AEmon\firmware
2. Wiegand Out should be in the Invixium device (Refer Assign Wiegand to Invixium Readers).
3. Standard Door should be created,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



COMMUNICATION SETTINGS

Baud Rate	Parity Bit	Stop Bit	Timeout (msec)
9600	None	1 Bit	3000

GENERAL SETTINGS

☐ Enable Log ☐ Display OSDP Text ☐ Smartcard Passthru ☐ Enable Biometric

SECURE CHANNEL

Secure Key Type	Secure Key	
AES128	303132333435363738393A3B3C3D3E3F0000000000000000000000000000000000000000000000000000000000000000	HEX

OSDP EVENTS

EVENTS	ON COLOR	OFF COLOR	ON TIME (MSEC)	OFF TIME (MSEC)	DISPLAY MESSAGE
Access Granted	Green	Green	100	100	☑
Access Denied	Red	None	100	100	☑
Enter PIN	None	None	0	0	☑
Dual Authentication	None	None	0	0	☑

Figure 97: 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 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

Table 5: IXM WEB - OSDP Configuration Options

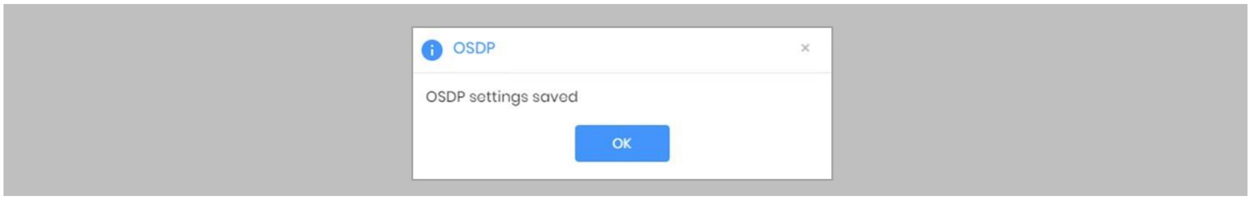
Note: Mismatches between the unit and Access Control Panel LED configuration will cause unrecognized events.

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.



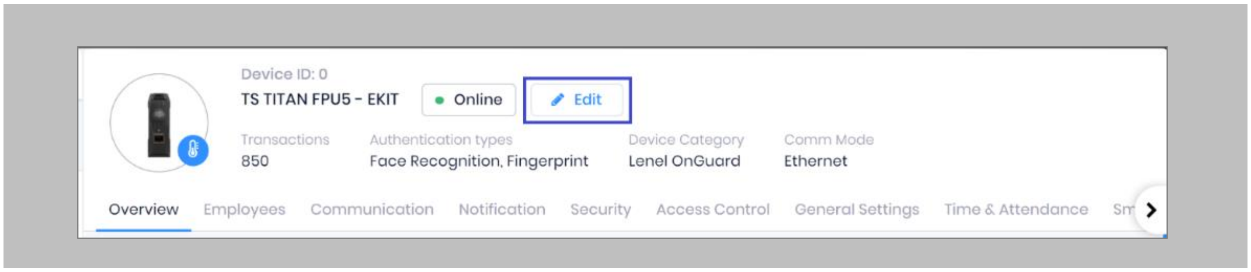
OSDP

OSDP settings saved

Figure 98: 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.



Device ID: 0

TS TITAN FPU5 - EKIT

Online

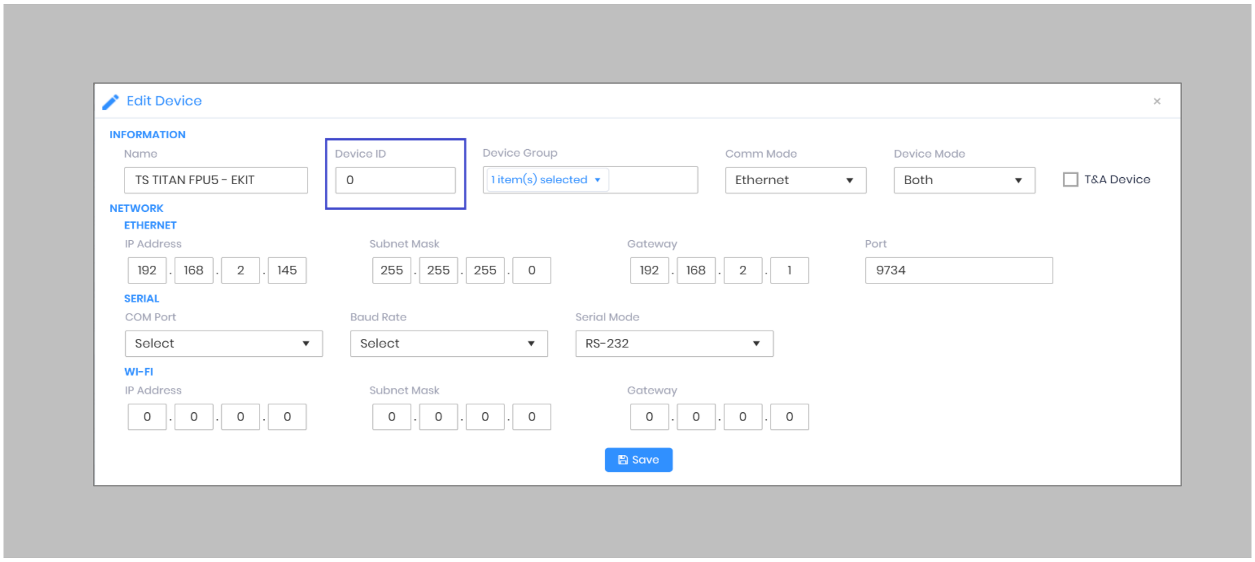
Transactions: 850

Authentication types: Face Recognition, Fingerprint

Device Category: Lenel OnGuard

Comm Mode: Ethernet

Figure 99: IXM WEB - Edit Device



Edit Device

INFORMATION

Name	Device ID	Device Group	Comm Mode	Device Mode	
TS TITAN FPU5 - EKIT	0	1 item(s) selected	Ethernet	Both	□ T&A Device

NETWORK

ETHERNET

IP Address	Subnet Mask	Gateway	Port
192 . 168 . 2 . 145	255 . 255 . 255 . 0	192 . 168 . 2 . 1	9734

SERIAL

COM Port	Baud Rate	Serial Mode
Select	Select	RS-232

WI-FI

IP Address	Subnet Mask	Gateway
0 . 0 . 0 . 0	0 . 0 . 0 . 0	0 . 0 . 0 . 0

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

STEP 5

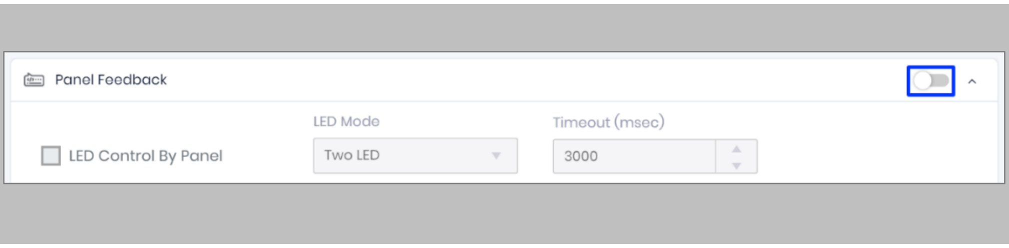
Wiegand input and output also need to be **configured** to allow OSDP communication to work. Create the same settings for Wiegand connections as you did previously.

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.



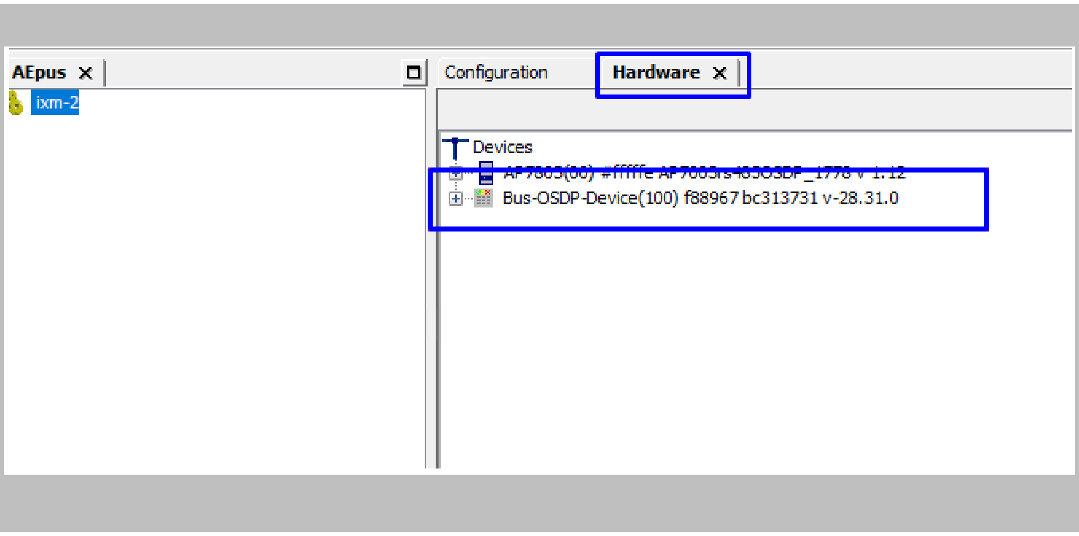
Panel Feedback

□ LED Control By Panel

LED Mode: Two LED

Timeout (msec): 3000

Figure 103: IXM WEB - Disable Panel Feedback



ixm-2

Devices

AP7803(00) #fffffe AP7803rs485OSDP_1778 v 1.12

Bus-OSDP-Device(100) f88967 bc313731 v-28.31.0

Figure 101: AEmon - OSDP Device

STEP 8

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

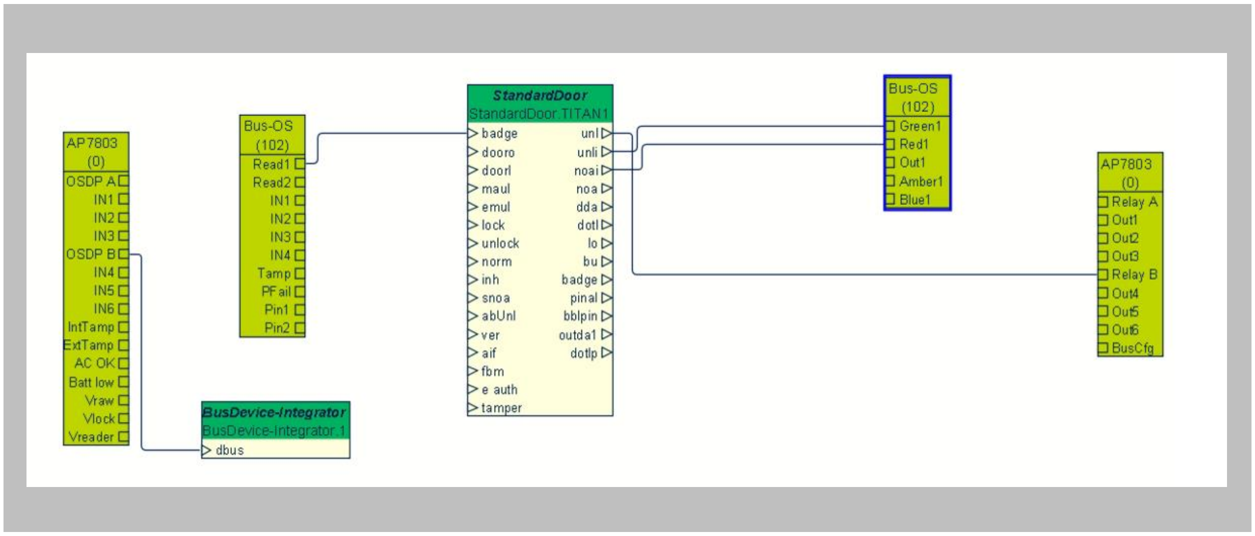


Figure 102:AEmon - OSDP Device Behavior

STEP 9

Right click on Standard Door → Properties.

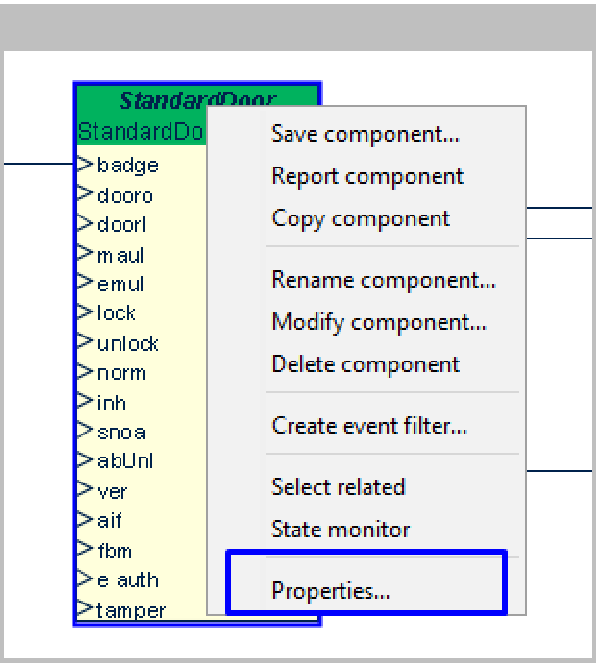
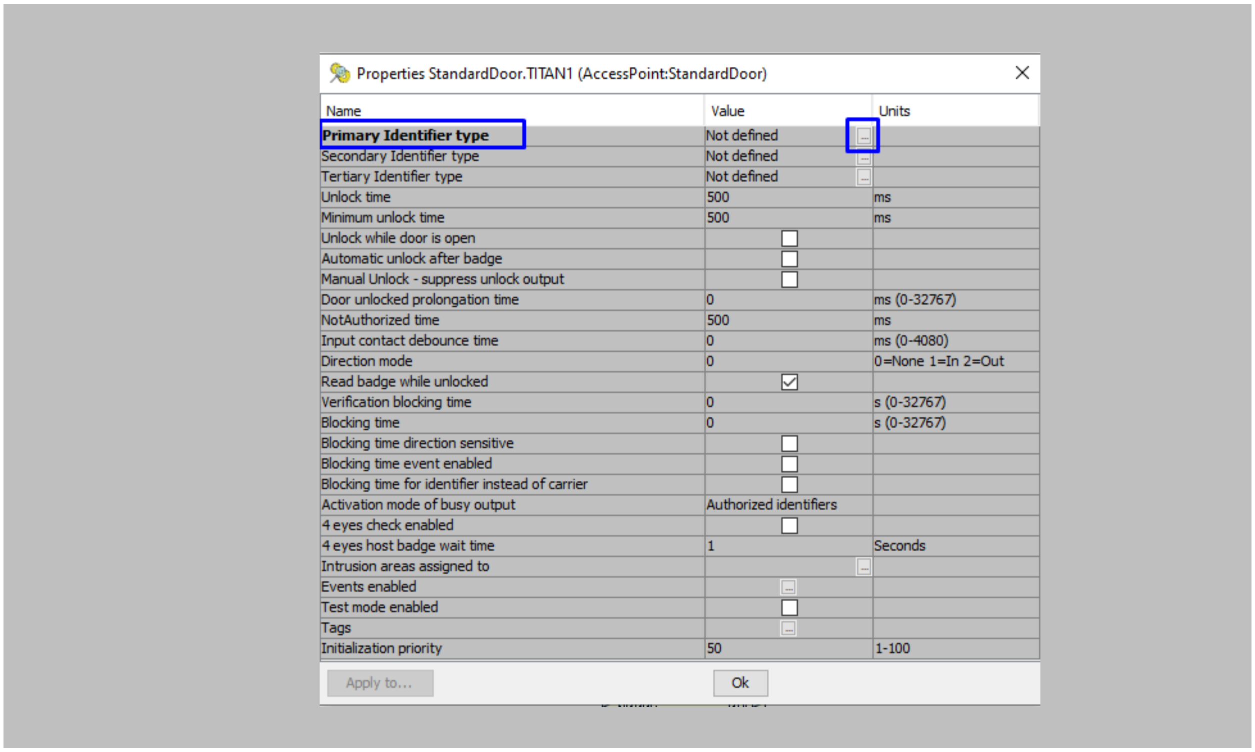


Figure 103: AEmon - Standard Door Property

STEP 10

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

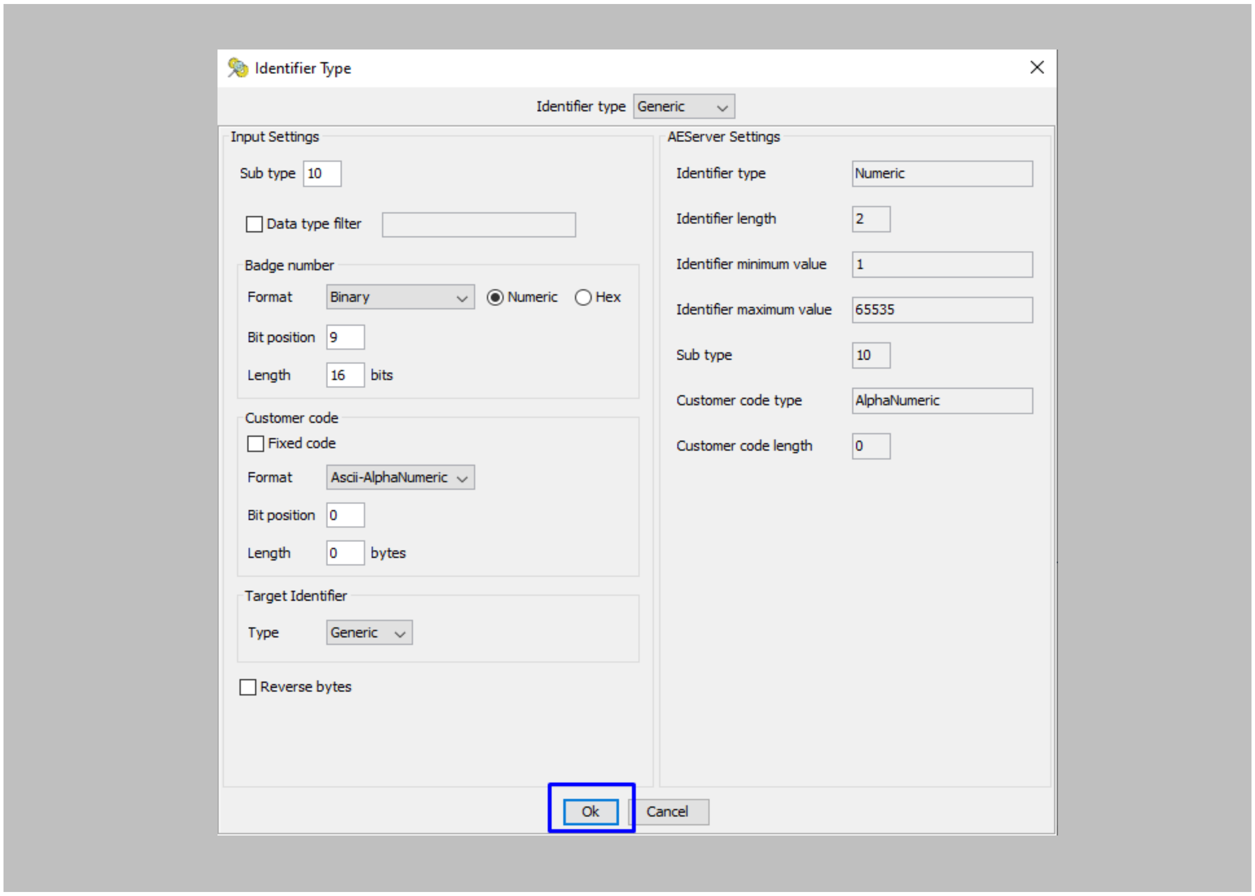


Properties StandardDoor.TITAN1 (AccessPoint:StandardDoor)

Name	Value	Units
Primary Identifier type	Not defined …	
Secondary Identifier type	Not defined …	
Tertiary Identifier type	Not defined …	
Unlock time	500	ms
Minimum unlock time	500	ms
Unlock while door is open	□	
Automatic unlock after badge	□	
Manual Unlock - suppress unlock output	□	
Door unlocked prolongation time	0	ms (0-32767)
NotAuthorized time	500	ms
Input contact debounce time	0	ms (0-4080)
Direction mode	0	0=None 1=In 2=Out
Read badge while unlocked	☑	
Verification blocking time	0	s (0-32767)
Blocking time	0	s (0-32767)
Blocking time direction sensitive	□	
Blocking time event enabled	□	
Blocking time for identifier instead of carrier	□	
Activation mode of busy output	Authorized identifiers	
4 eyes check enabled	□	
4 eyes host badge wait time	1	Seconds
Intrusion areas assigned to	…	
Events enabled	…	
Test mode enabled	□	
Tags	…	
Initialization priority	50	1-100

Figure 104: AEmon - Primary Identifier Type

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



Identifier Type

Identifier type: Generic

Input Settings

Sub type: 10

□ Data type filter

Badge number

Format: Binary ● Numeric ○ Hex

Bit position: 9

Length: 16 bits

Customer code

□ Fixed code

Format: Ascii-AlphaNumeric

Bit position: 0

Length: 0 bytes

Target Identifier

Type: Generic

□ Reverse bytes

AEServer Settings

Identifier type: Numeric

Identifier length: 2

Identifier minimum value: 1

Identifier maximum value: 65535

Sub type: 10

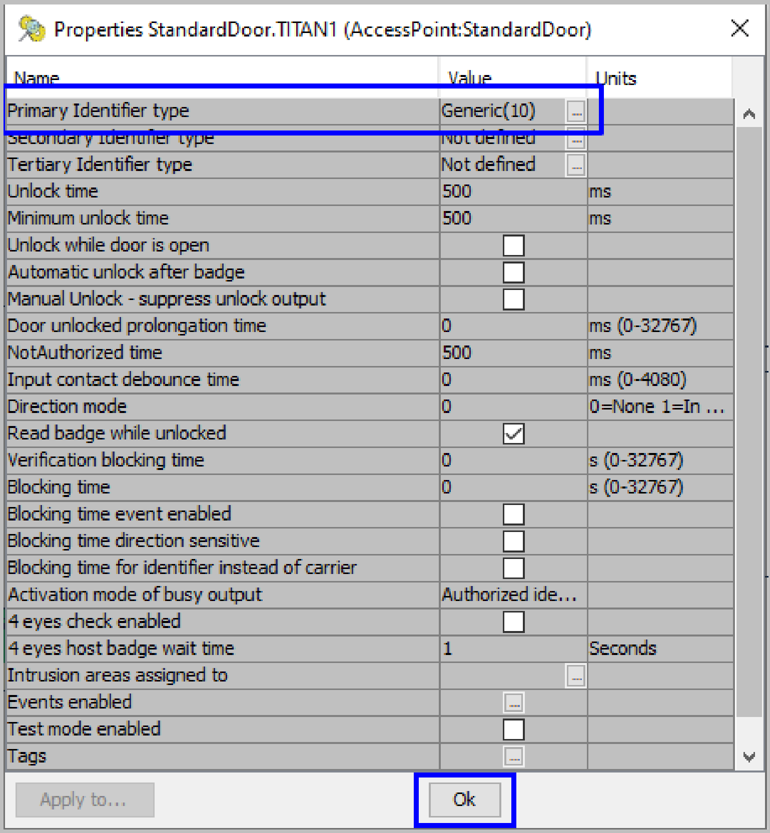
Customer code type: AlphaNumeric

Customer code length: 0

Figure 105: AEmon - Configure Primary Identifier Type

STEP 11

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



Properties StandardDoor.TITAN1 (AccessPoint:StandardDoor)

Name	Value	Units
Primary Identifier type	Generic(10) ...	
Secondary Identifier type	Not defined ...	
Tertiary Identifier type	Not defined ...	
Unlock time	500	ms
Minimum unlock time	500	ms
Unlock while door is open	□	
Automatic unlock after badge	□	
Manual Unlock - suppress unlock output	□	
Door unlocked prolongation time	0	ms (0-32767)
NotAuthorized time	500	ms
Input contact debounce time	0	ms (0-4080)
Direction mode	0	0=None 1=In ...
Read badge while unlocked	☑	
Verification blocking time	0	s (0-32767)
Blocking time	0	s (0-32767)
Blocking time event enabled	□	
Blocking time direction sensitive	□	
Blocking time for identifier instead of carrier	□	
Activation mode of busy output	Authorized ide...	
4 eyes check enabled	□	
4 eyes host badge wait time	1	Seconds
Intrusion areas assigned to	...	
Events enabled	...	
Test mode enabled	□	
Tags	...	

Figure 106: AEmon - Generic Primary Identifier Type

STEP 12

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

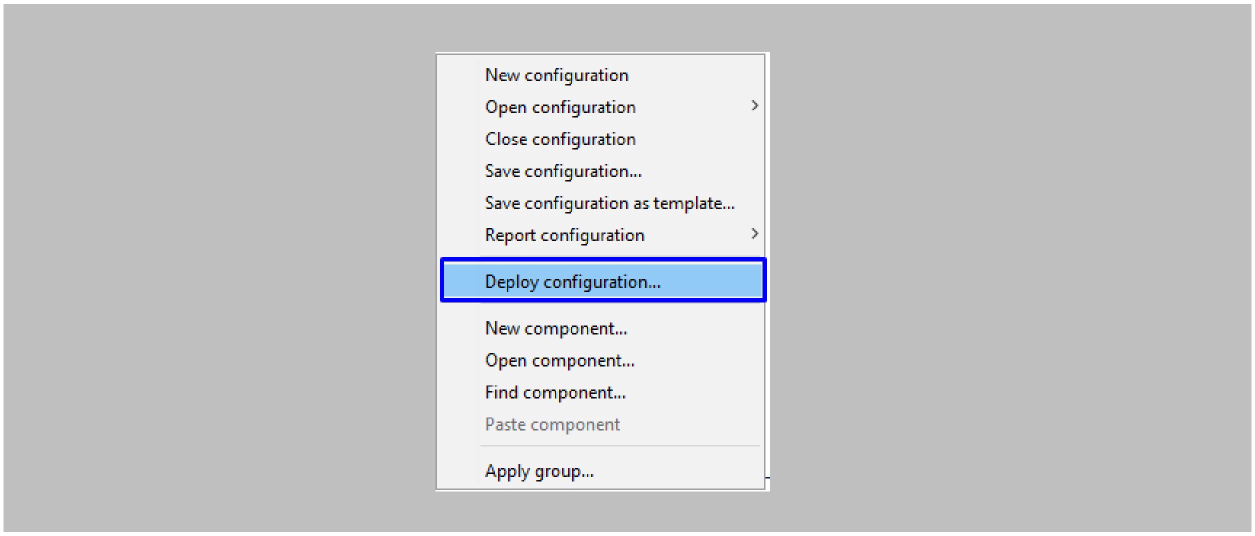


Figure 107: AEmon - Deploy Configuration

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**.

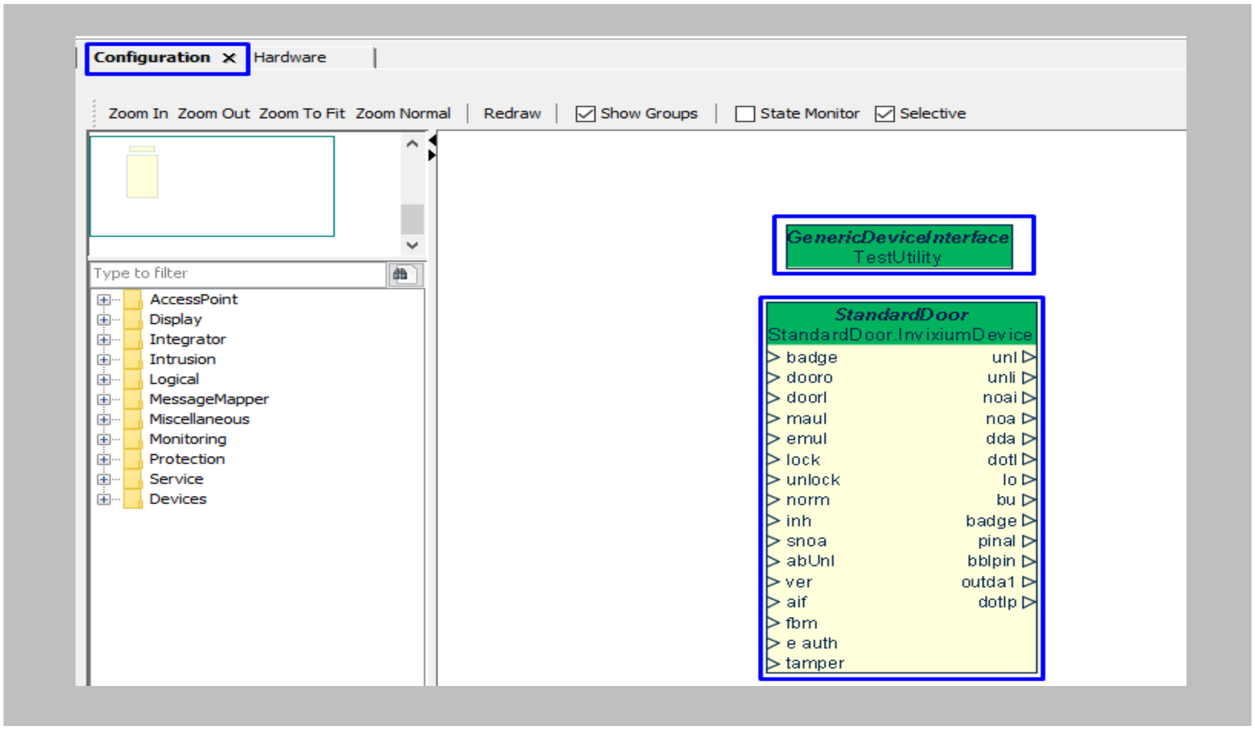
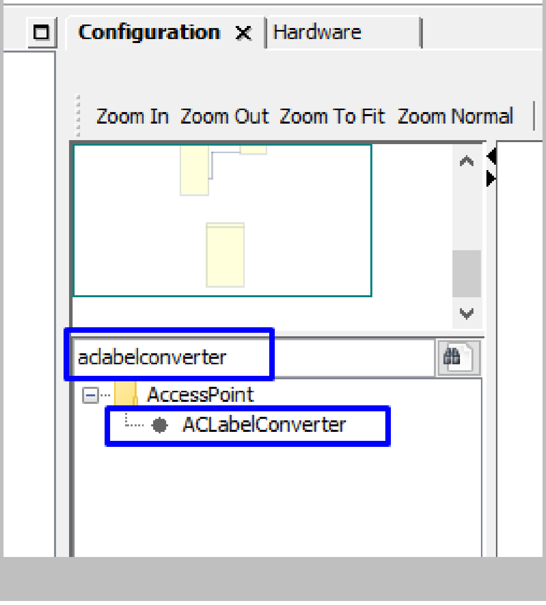


Figure 108: AEmon - Configuration tab

STEP 2

Search for ACLabelConverter → Add ACLabelConverter.



aclabelconverter

Figure 109: AEmon - Add ACLabelConverter

STEP 3

Connect 'Output Data1' of StandardDoor with 'Access Point Status' of ACLabelConverter.

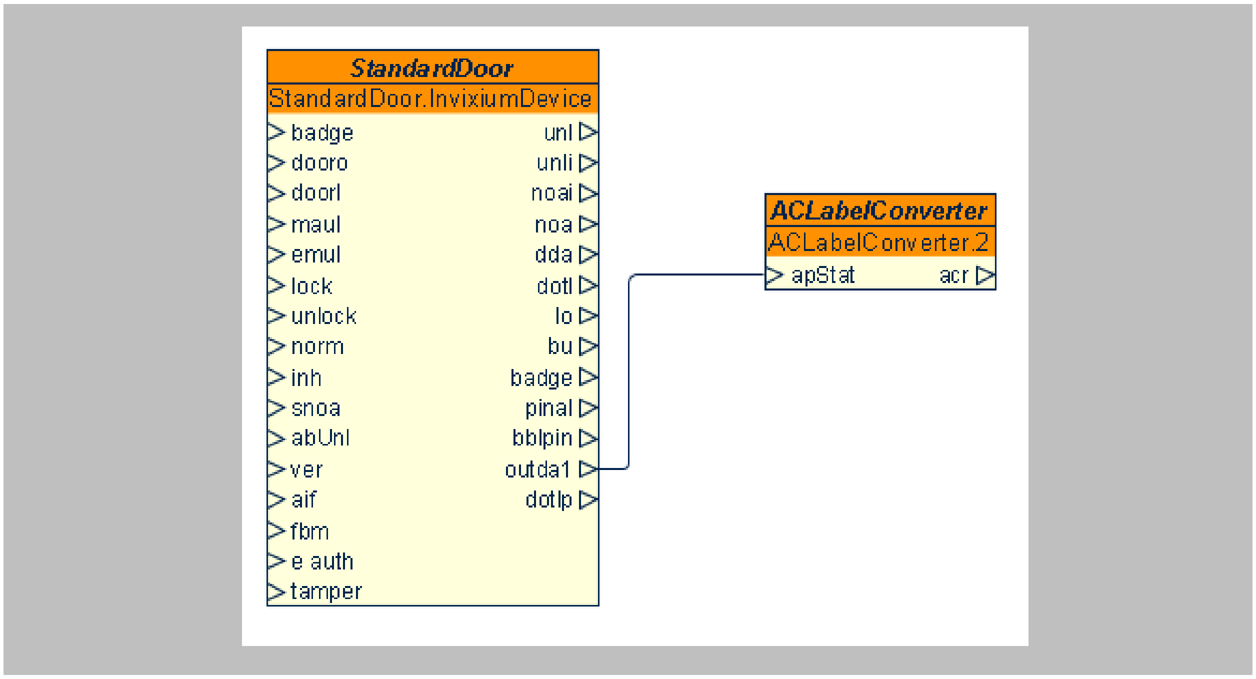


Figure 110: AEmon - StandardDoor and ACLabelConverter Connection

STEP 4

Right click on GenericDeviceInterface → click on Properties.

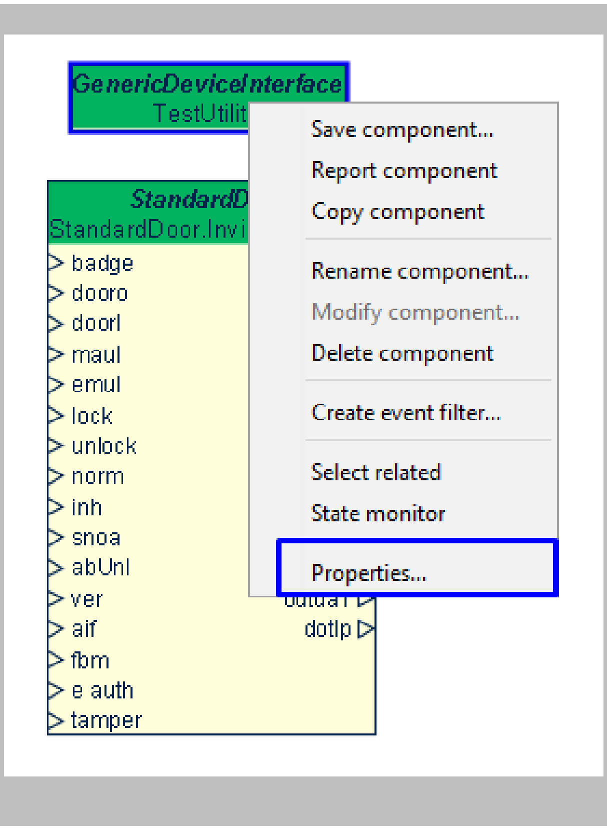
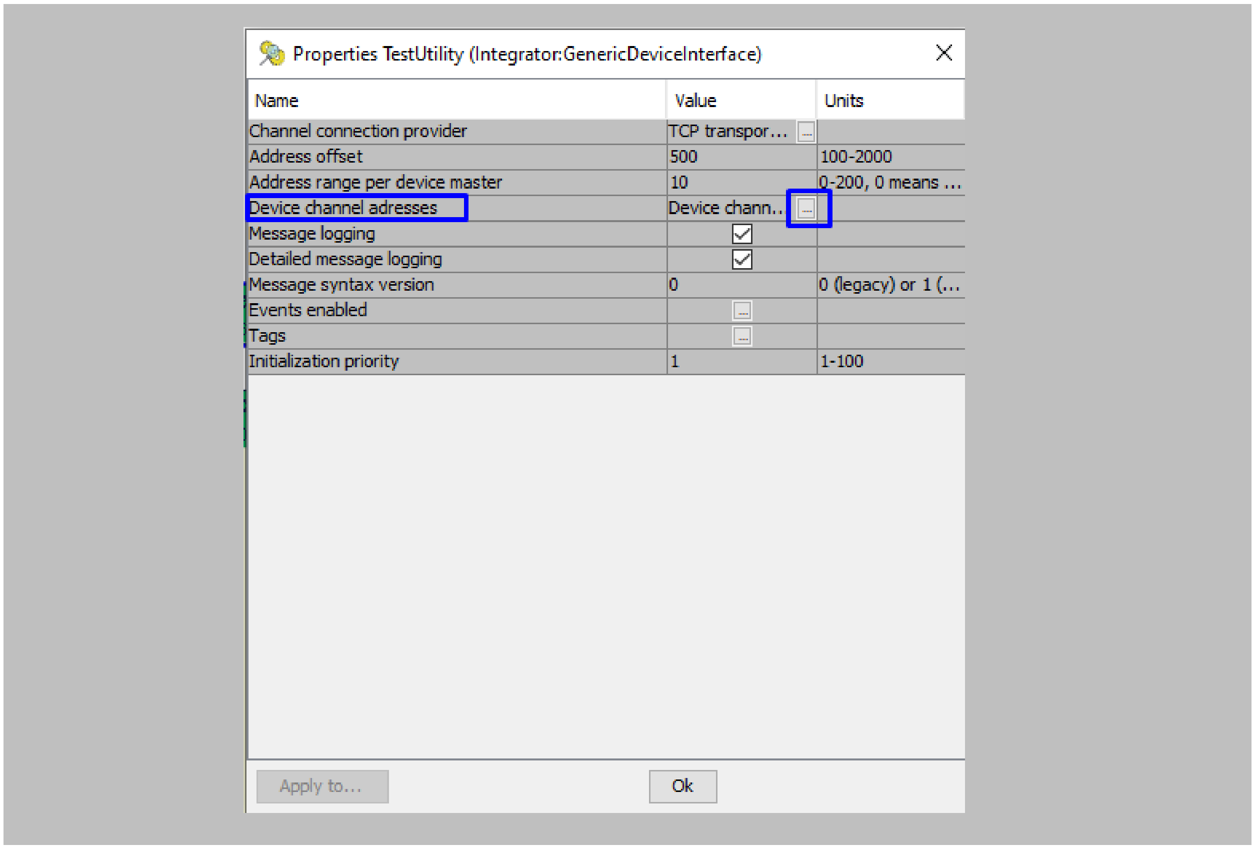


Figure 111: AEmon - GenericDeviceInterface Properties

STEP 5

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



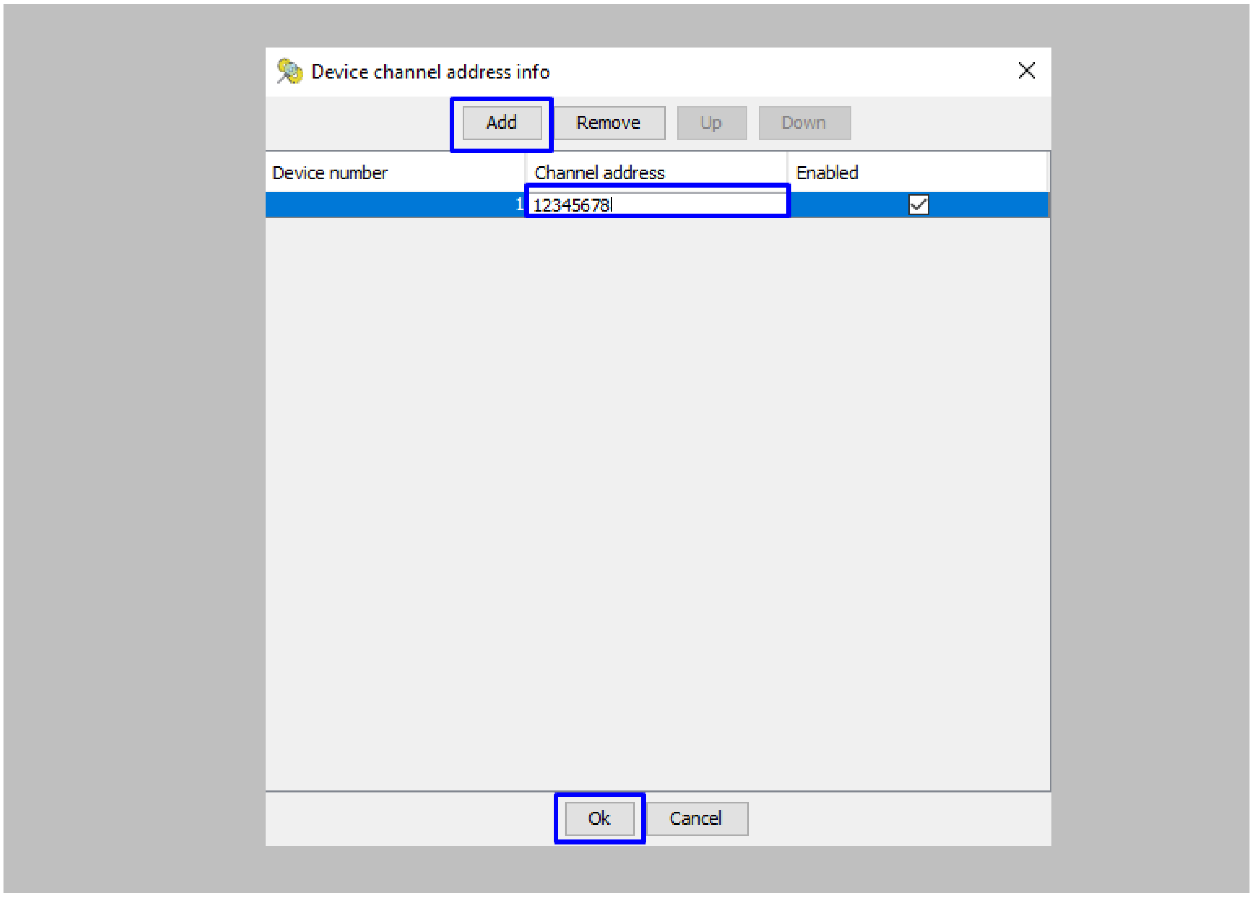
Properties TestUtility (Integrator:GenericDeviceInterface)

Name	Value	Units
Channel connection provider	TCP transpor… ...	
Address offset	500	100-2000
Address range per device master	10	0-200, 0 means …
Device channel adresses	Device chann… ...	
Message logging	☑	
Detailed message logging	☑	
Message syntax version	0	0 (legacy) or 1 (…
Events enabled	...	
Tags	...	
Initialization priority	1	1-100

Figure 112: AEmon - Device Channel Address

STEP 6

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



Device number	Channel address	Enabled
1	12345678	☑

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.**

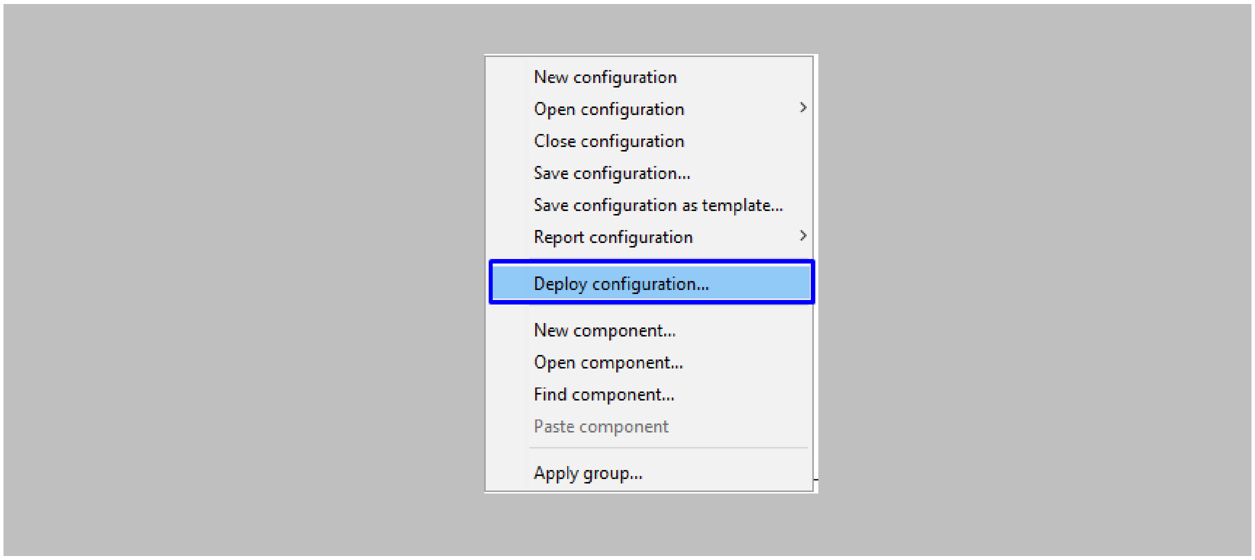
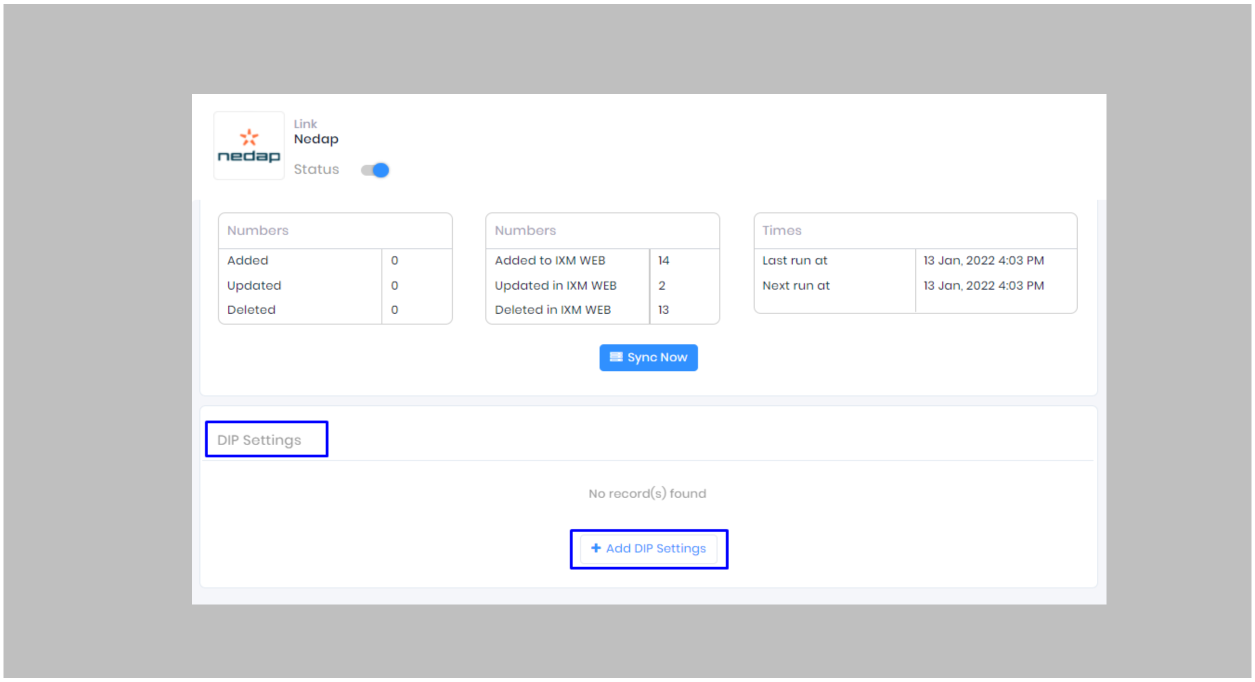


Figure 113: AEmon - Deploy Configuration

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.



Numbers	
Added	0
Updated	0
Deleted	0

Numbers	
Added to IXM WEB	14
Updated in IXM WEB	2
Deleted in IXM WEB	13

Times	
Last run at	13 Jan, 2022 4:03 PM
Next run at	13 Jan, 2022 4:03 PM

No record(s) found

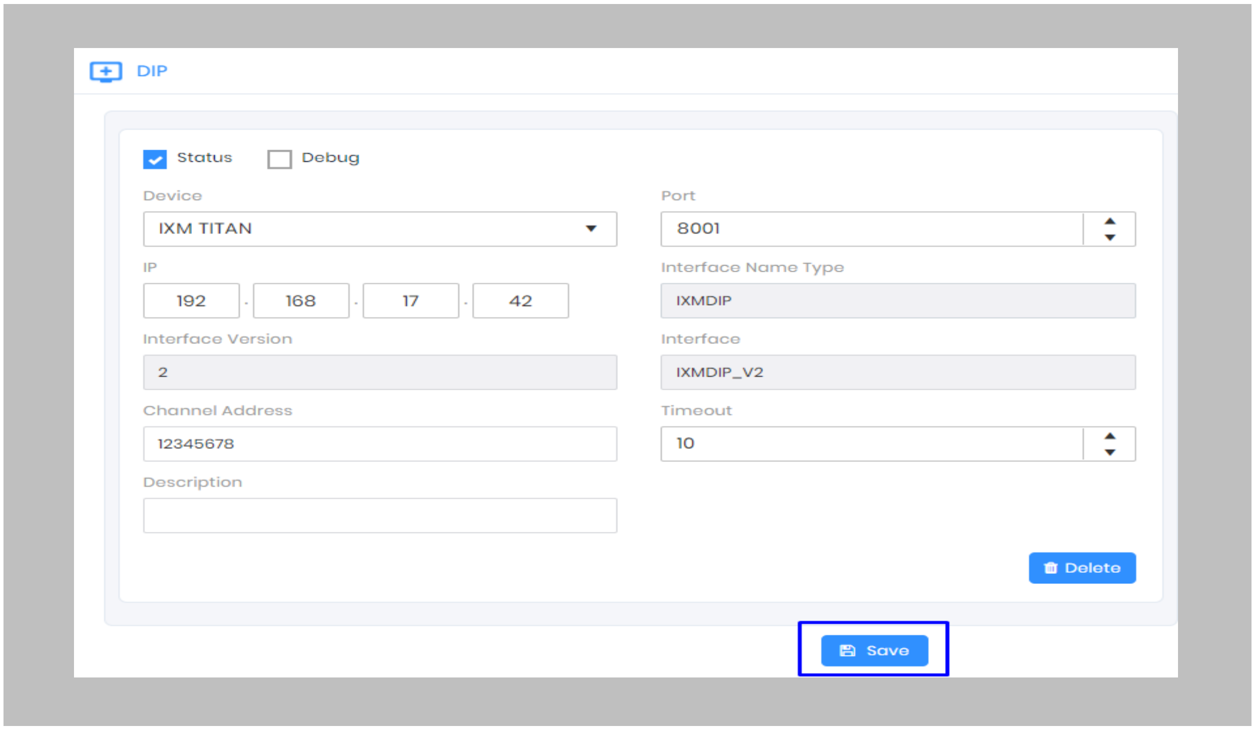
Figure 114: IXM WEB - Add DIP Settings

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.



DIP

☑ Status □ Debug

Device: IXM TITAN

Port: 8001

IP: 192 . 168 . 17 . 42

Interface Name Type: IXMDIP

Interface Version: 2

Interface: IXMDIP_V2

Channel Address: 12345678

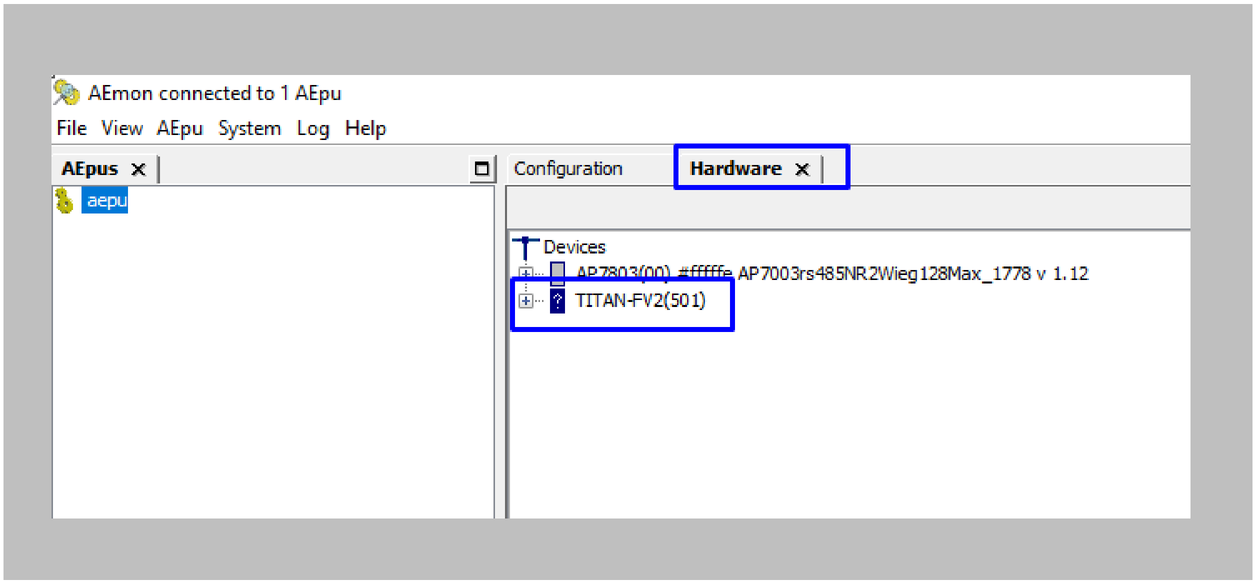
Timeout: 10

Description:

Figure 115: 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.



Devices
AP7803(00) #fffffe AP7003rs485NR2Wieg128Max_1778 v 1.12
TITAN-FV2(501)

Figure 116: AEmon - DIP Device

STEP 11

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

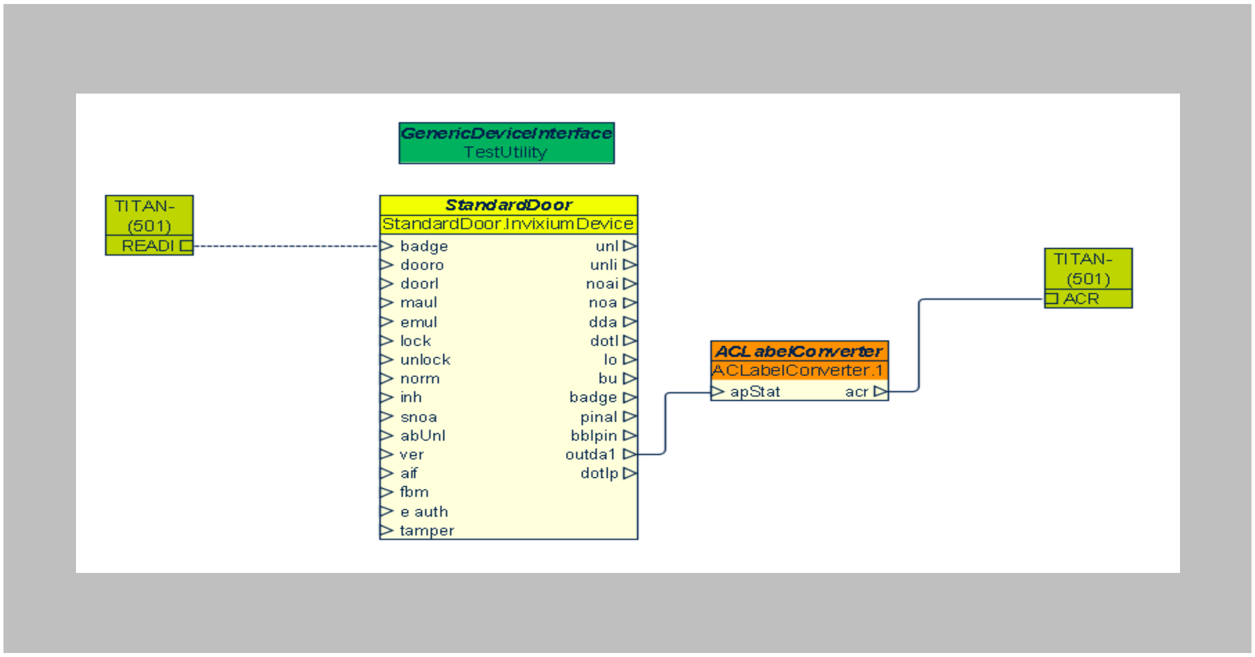


Figure 117: AEmon - DIP Device Behavior

STEP 12

Right click on Standard Door → Properties.

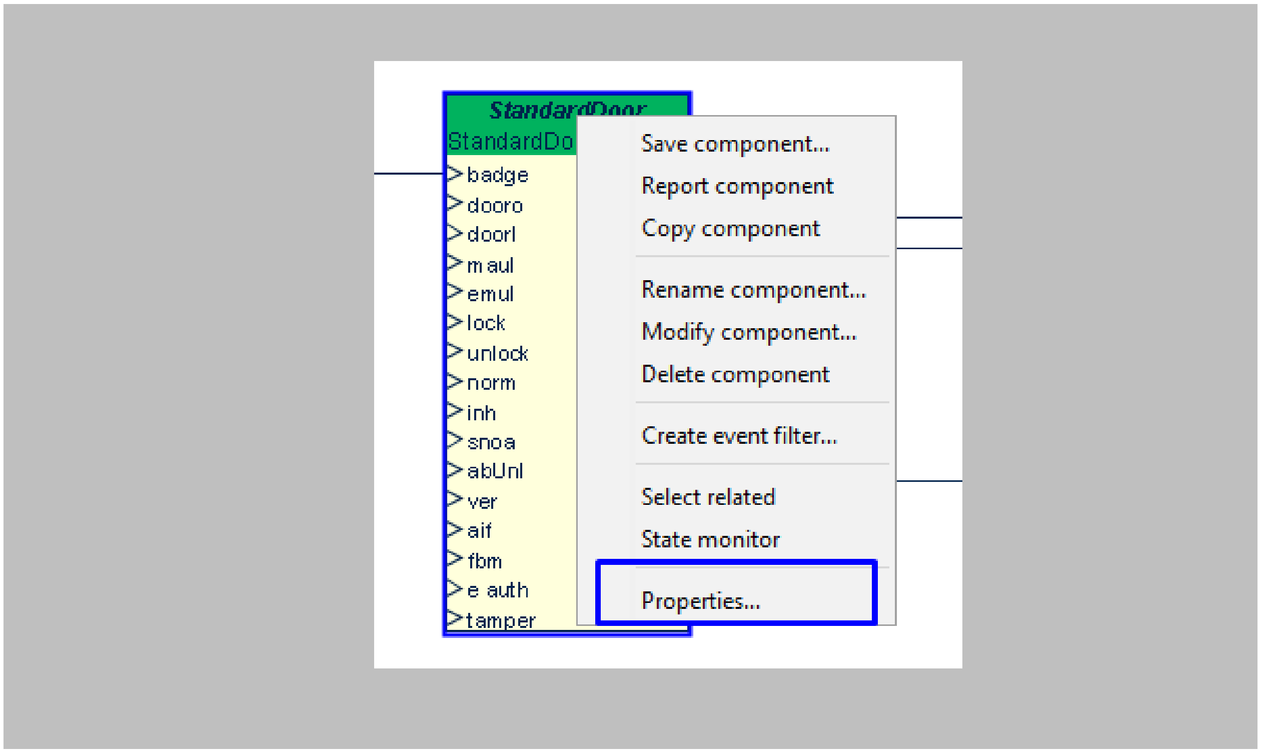
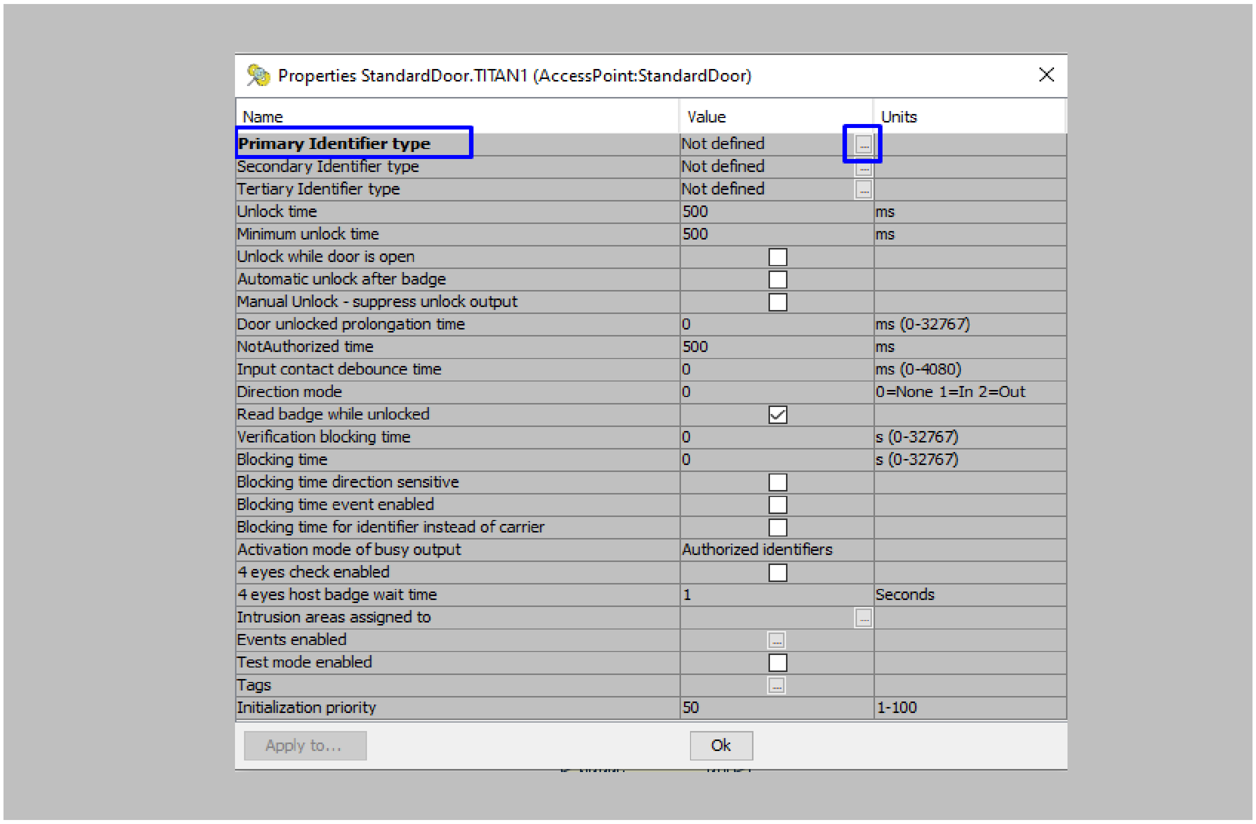


Figure 118: AEmon - Standard Door Property

STEP 13

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

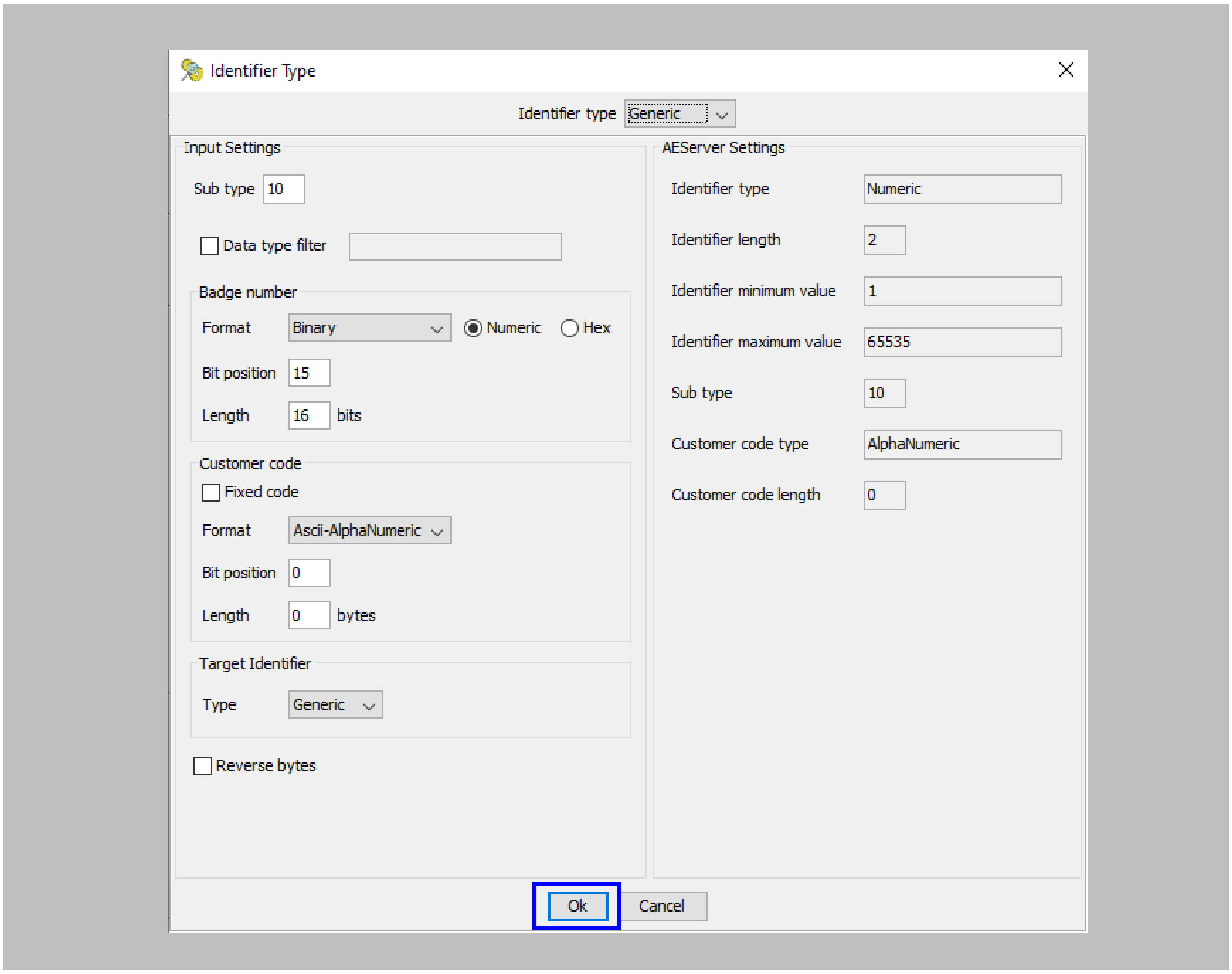


Properties StandardDoor.TITAN1 (AccessPoint:StandardDoor)

Name	Value	Units
Primary Identifier type	Not defined ...	
Secondary Identifier type	Not defined ...	
Tertiary Identifier type	Not defined ...	
Unlock time	500	ms
Minimum unlock time	500	ms
Unlock while door is open	☐	
Automatic unlock after badge	☐	
Manual Unlock - suppress unlock output	☐	
Door unlocked prolongation time	0	ms (0-32767)
NotAuthorized time	500	ms
Input contact debounce time	0	ms (0-4080)
Direction mode	0	0=None 1=In 2=Out
Read badge while unlocked	☑	
Verification blocking time	0	s (0-32767)
Blocking time	0	s (0-32767)
Blocking time direction sensitive	☐	
Blocking time event enabled	☐	
Blocking time for identifier instead of carrier	☐	
Activation mode of busy output	Authorized identifiers	
4 eyes check enabled	☐	
4 eyes host badge wait time	1	Seconds
Intrusion areas assigned to	...	
Events enabled	...	
Test mode enabled	☐	
Tags	...	
Initialization priority	50	1-100

Figure 119: AEmon DIP - Primary Identifier Type

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



Identifier type: Generic

Input Settings

Sub type: 10

□ Data type filter

Badge number

Format: Binary ● Numeric ○ Hex

Bit position: 15

Length: 16 bits

Customer code

□ Fixed code

Format: Ascii-AlphaNumeric

Bit position: 0

Length: 0 bytes

Target Identifier

Type: Generic

□ Reverse bytes

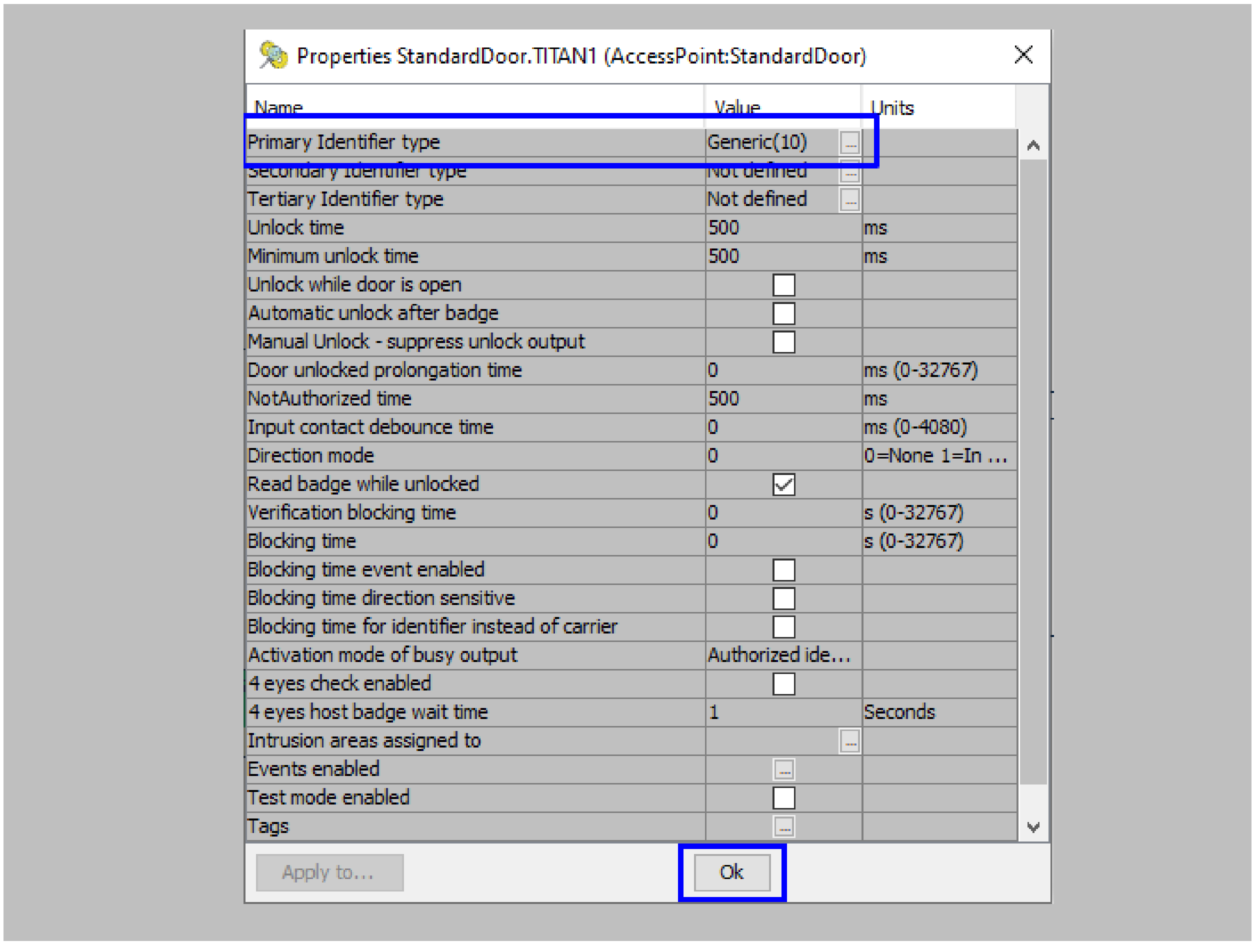
AEServer Settings

Identifier type	Numeric
Identifier length	2
Identifier minimum value	1
Identifier maximum value	65535
Sub type	10
Customer code type	AlphaNumeric
Customer code length	0

Figure 120: AEmon DIP - Primary Identifier Configuration

STEP 14

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



Properties StandardDoor.TITAN1 (AccessPoint:StandardDoor)

Name	Value	Units
Primary Identifier type	Generic(10) ...	
Secondary Identifier type	Not defined ...	
Tertiary Identifier type	Not defined ...	
Unlock time	500	ms
Minimum unlock time	500	ms
Unlock while door is open	□	
Automatic unlock after badge	□	
Manual Unlock - suppress unlock output	□	
Door unlocked prolongation time	0	ms (0-32767)
NotAuthorized time	500	ms
Input contact debounce time	0	ms (0-4080)
Direction mode	0	0=None 1=In ...
Read badge while unlocked	☑	
Verification blocking time	0	s (0-32767)
Blocking time	0	s (0-32767)
Blocking time event enabled	□	
Blocking time direction sensitive	□	
Blocking time for identifier instead of carrier	□	
Activation mode of busy output	Authorized ide...	
4 eyes check enabled	□	
4 eyes host badge wait time	1	Seconds
Intrusion areas assigned to	...	
Events enabled	...	
Test mode enabled	□	
Tags	...	

Figure 121: 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.**

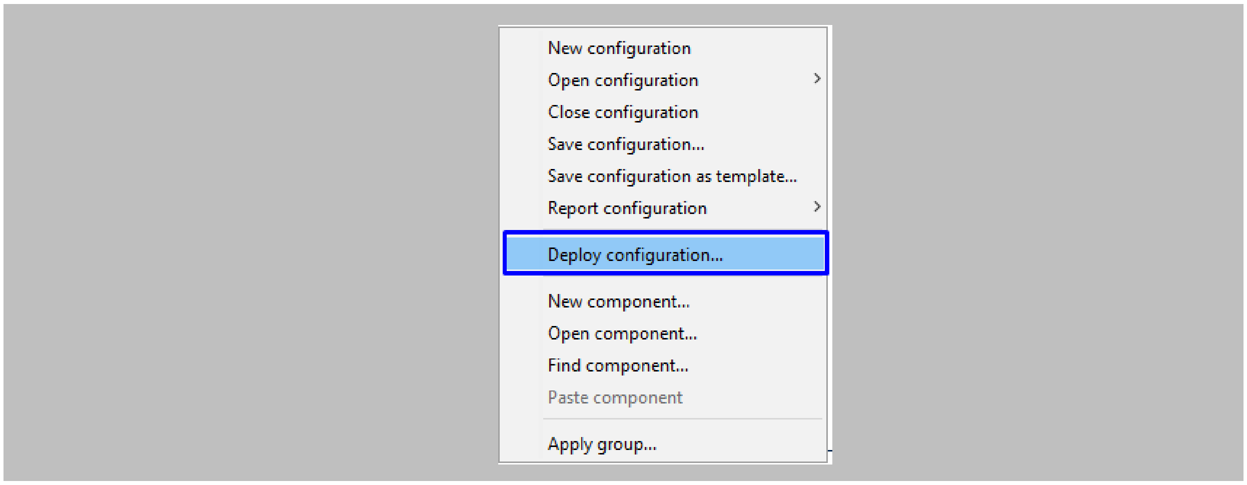


Figure 122: AEmon - Deploy Configuration

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.

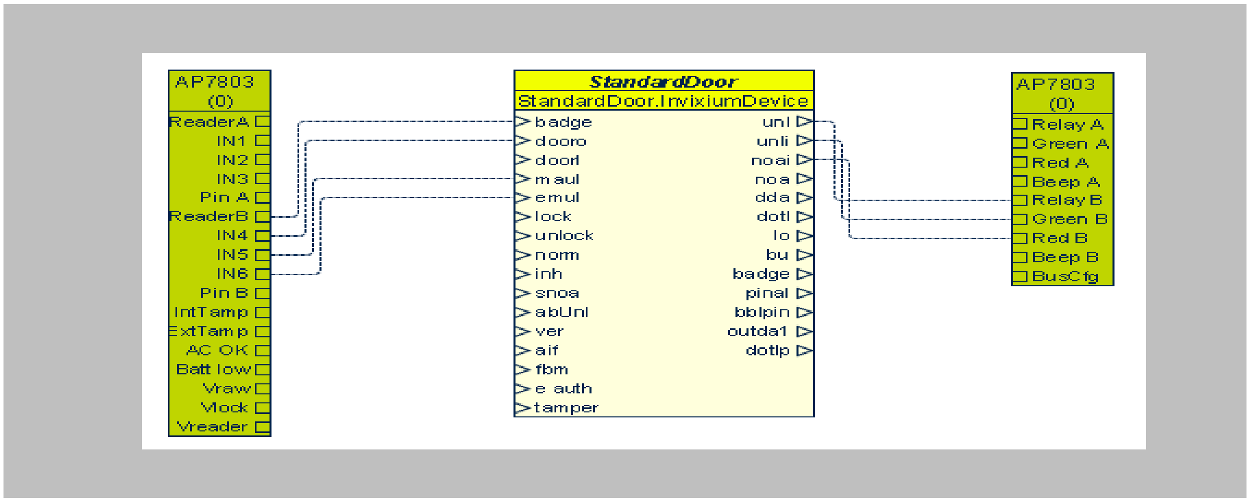


Figure 123: AEmon - Wiegand Device Behavior

STEP 3

Right Click on Standard Door → Properties.

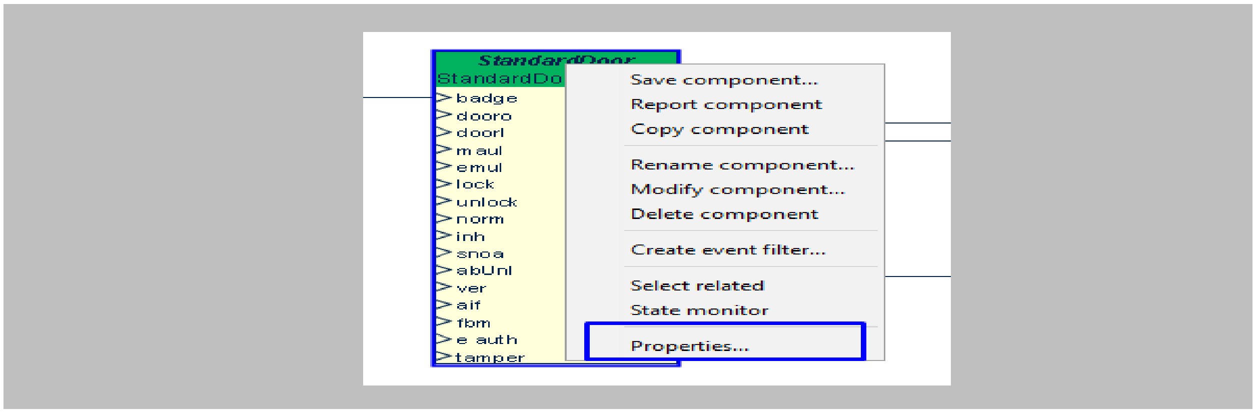
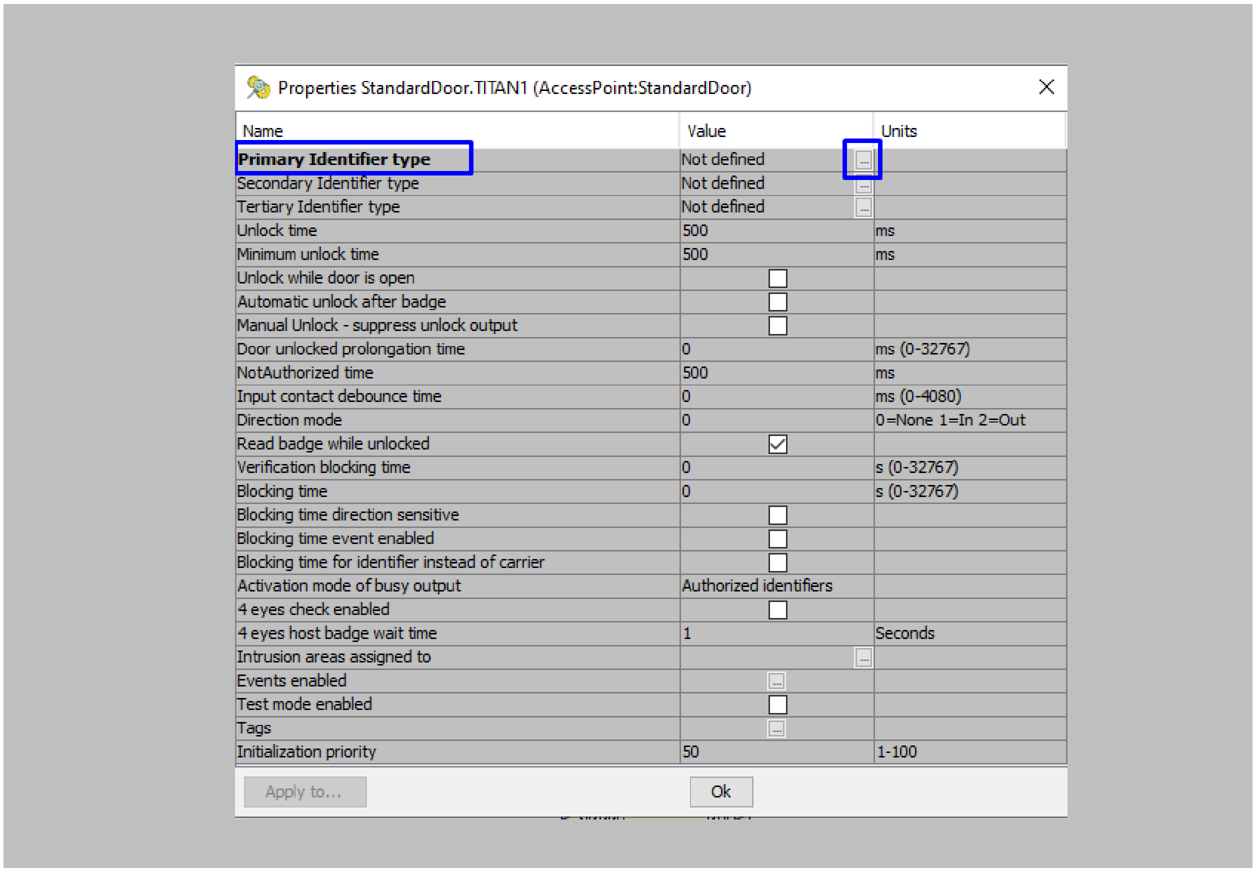


Figure 124: AEmon - Standard Door Property

STEP 4

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

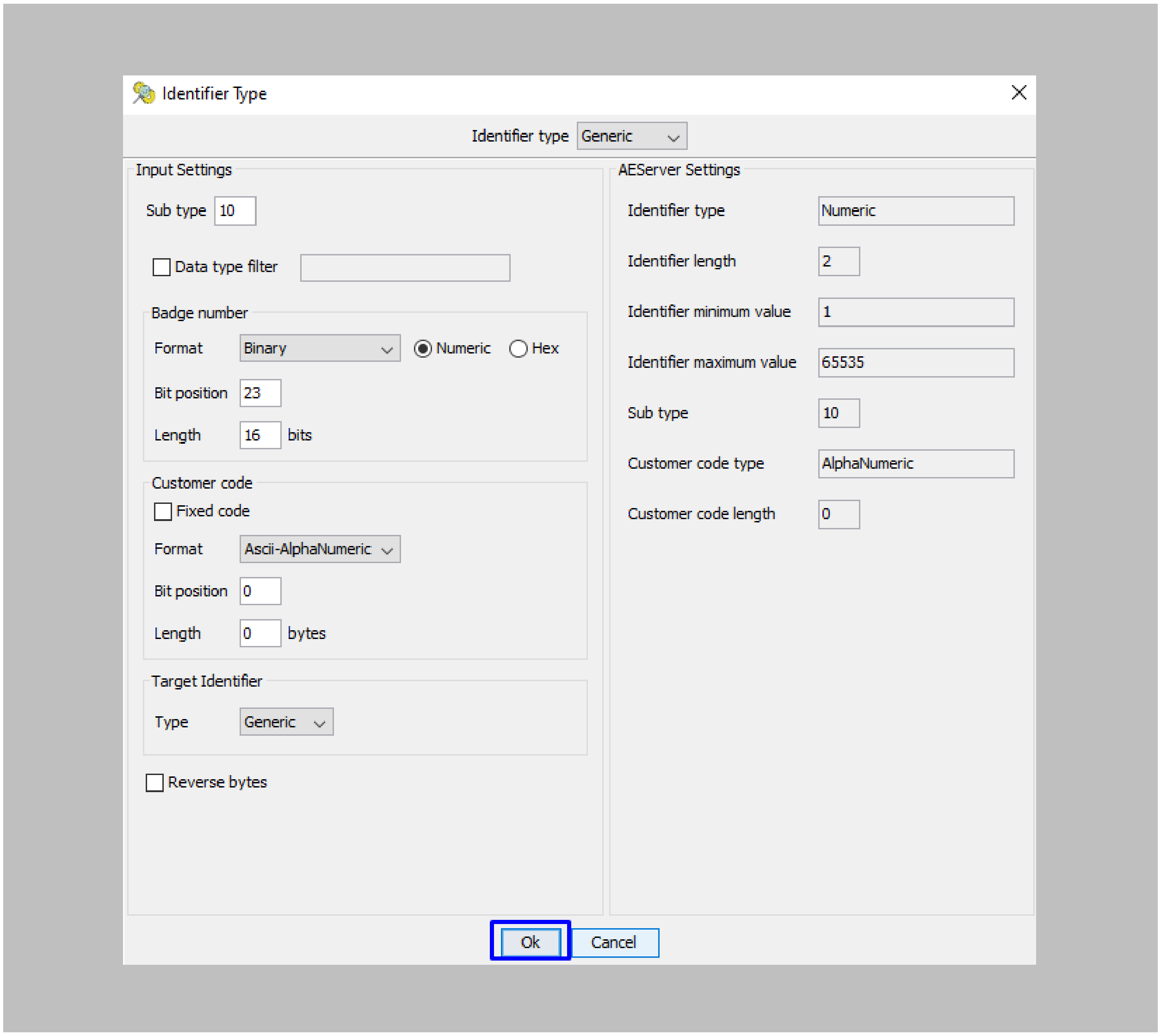


Properties StandardDoor.TITAN1 (AccessPoint:StandardDoor)

Name	Value	Units
Primary Identifier type	Not defined …	
Secondary Identifier type	Not defined …	
Tertiary Identifier type	Not defined …	
Unlock time	500	ms
Minimum unlock time	500	ms
Unlock while door is open	□	
Automatic unlock after badge	□	
Manual Unlock - suppress unlock output	□	
Door unlocked prolongation time	0	ms (0-32767)
NotAuthorized time	500	ms
Input contact debounce time	0	ms (0-4080)
Direction mode	0	0=None 1=In 2=Out
Read badge while unlocked	☑	
Verification blocking time	0	s (0-32767)
Blocking time	0	s (0-32767)
Blocking time direction sensitive	□	
Blocking time event enabled	□	
Blocking time for identifier instead of carrier	□	
Activation mode of busy output	Authorized identifiers	
4 eyes check enabled	□	
4 eyes host badge wait time	1	Seconds
Intrusion areas assigned to	…	
Events enabled	…	
Test mode enabled	□	
Tags	…	
Initialization priority	50	1-100

Figure 125: AEmon Wiegand – Primary Identifier Type

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



Identifier Type

Identifier type: Generic

Input Settings

Sub type: 10

□ Data type filter

Badge number

Format: Binary ● Numeric ○ Hex

Bit position: 23

Length: 16 bits

Customer code

□ Fixed code

Format: Ascii-AlphaNumeric

Bit position: 0

Length: 0 bytes

Target Identifier

Type: Generic

□ Reverse bytes

AEServer Settings

Identifier type: Numeric

Identifier length: 2

Identifier minimum value: 1

Identifier maximum value: 65535

Sub type: 10

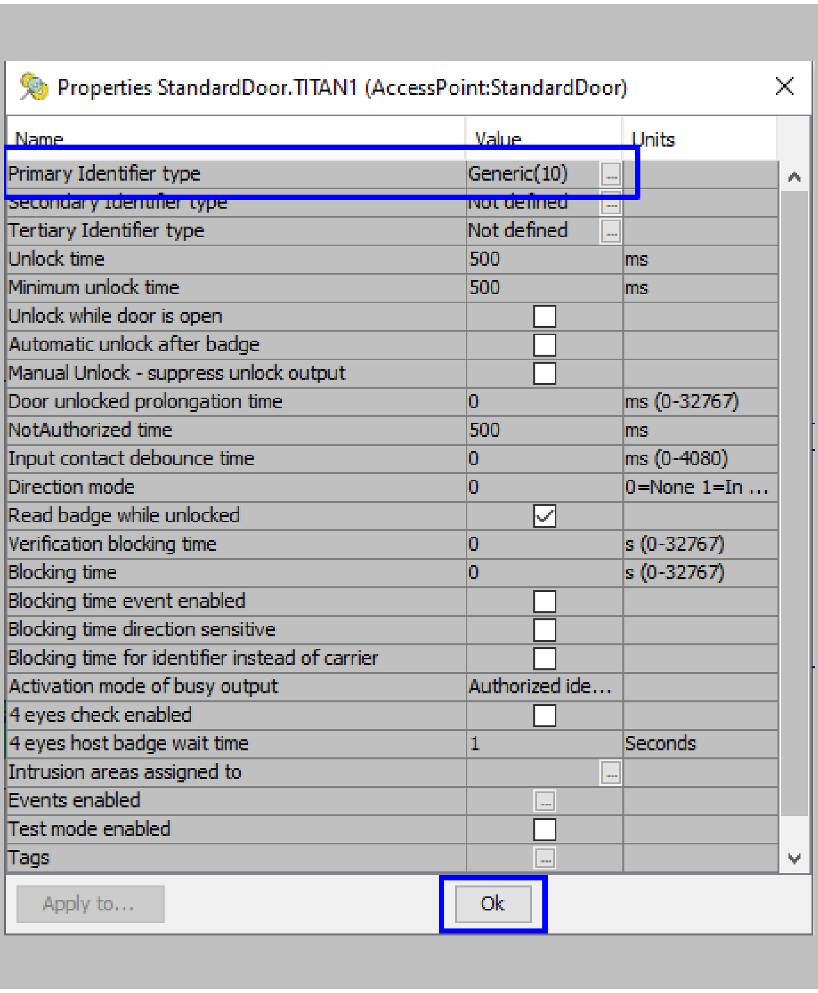
Customer code type: AlphaNumeric

Customer code length: 0

Figure 126: AEmon Wiegand - Configure Primary Identifier Type

STEP 5

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



Properties StandardDoor.TITAN1 (AccessPoint:StandardDoor)

Name	Value	Units
Primary Identifier type	Generic(10)	
Secondary Identifier type	Not defined	
Tertiary Identifier type	Not defined	
Unlock time	500	ms
Minimum unlock time	500	ms
Unlock while door is open	□	
Automatic unlock after badge	□	
Manual Unlock - suppress unlock output	□	
Door unlocked prolongation time	0	ms (0-32767)
NotAuthorized time	500	ms
Input contact debounce time	0	ms (0-4080)
Direction mode	0	0=None 1=In ...
Read badge while unlocked	☑	
Verification blocking time	0	s (0-32767)
Blocking time	0	s (0-32767)
Blocking time event enabled	□	
Blocking time direction sensitive	□	
Blocking time for identifier instead of carrier	□	
Activation mode of busy output	Authorized ide...	
4 eyes check enabled	□	
4 eyes host badge wait time	1	Seconds
Intrusion areas assigned to		
Events enabled		
Test mode enabled	□	
Tags		

Figure 127: 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.**

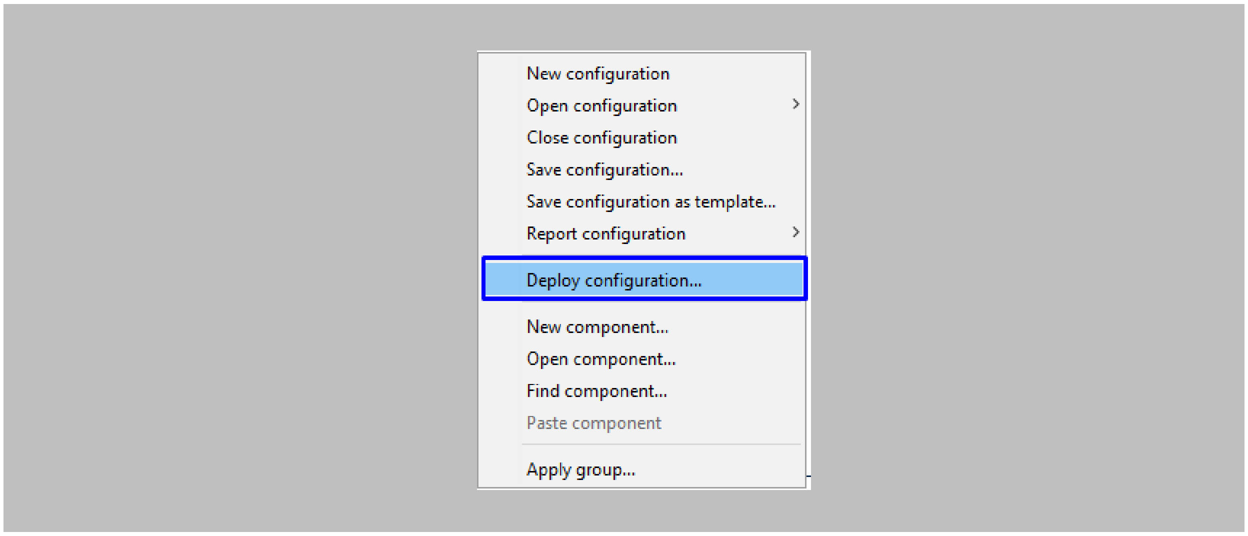


Figure 128: AEmon Wiegand- Deploy Configuration

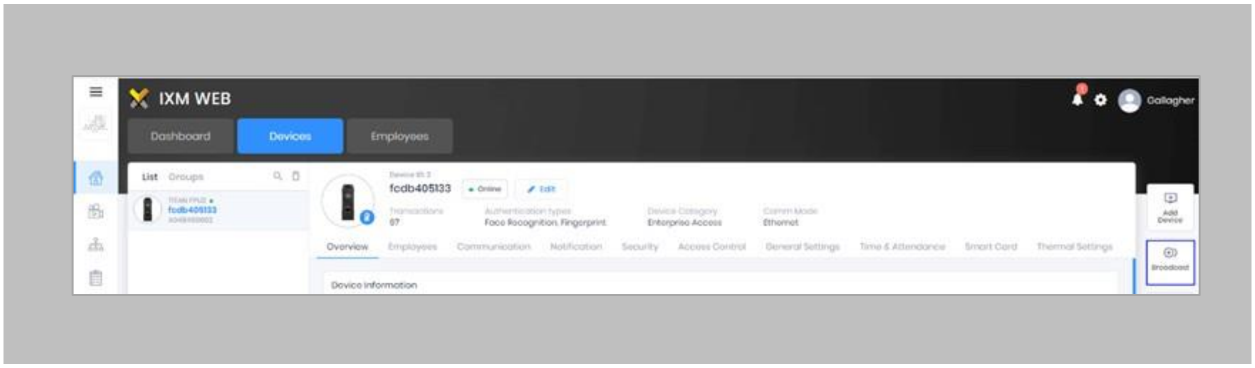
Appendix

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.



fcdb405133 • Online Edit

Transactions: 07

Authentication types: Face Recognition, Fingerprint

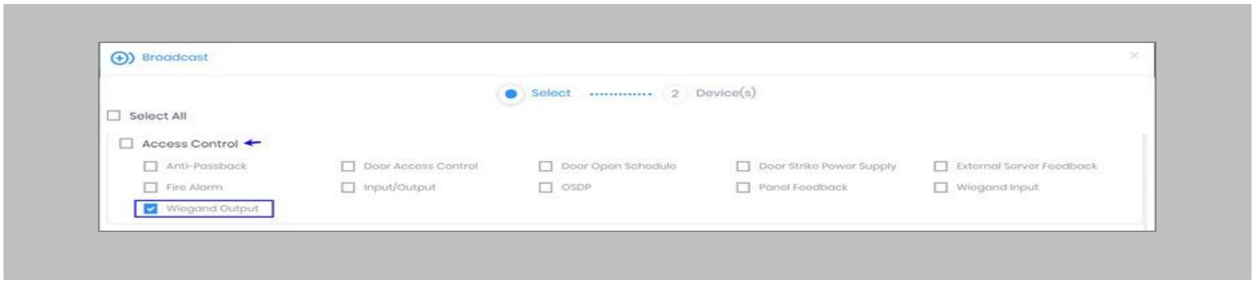
Device Category: Enterprise Access

Comm Mode: Ethernet

Figure 129: IXM WEB - Broadcast Option

STEP 2

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



□ Select All

□ Access Control

□ Anti-Passback □ Door Access Control □ Door Open Schedule □ Door Strike Power Supply □ External Server Feedback

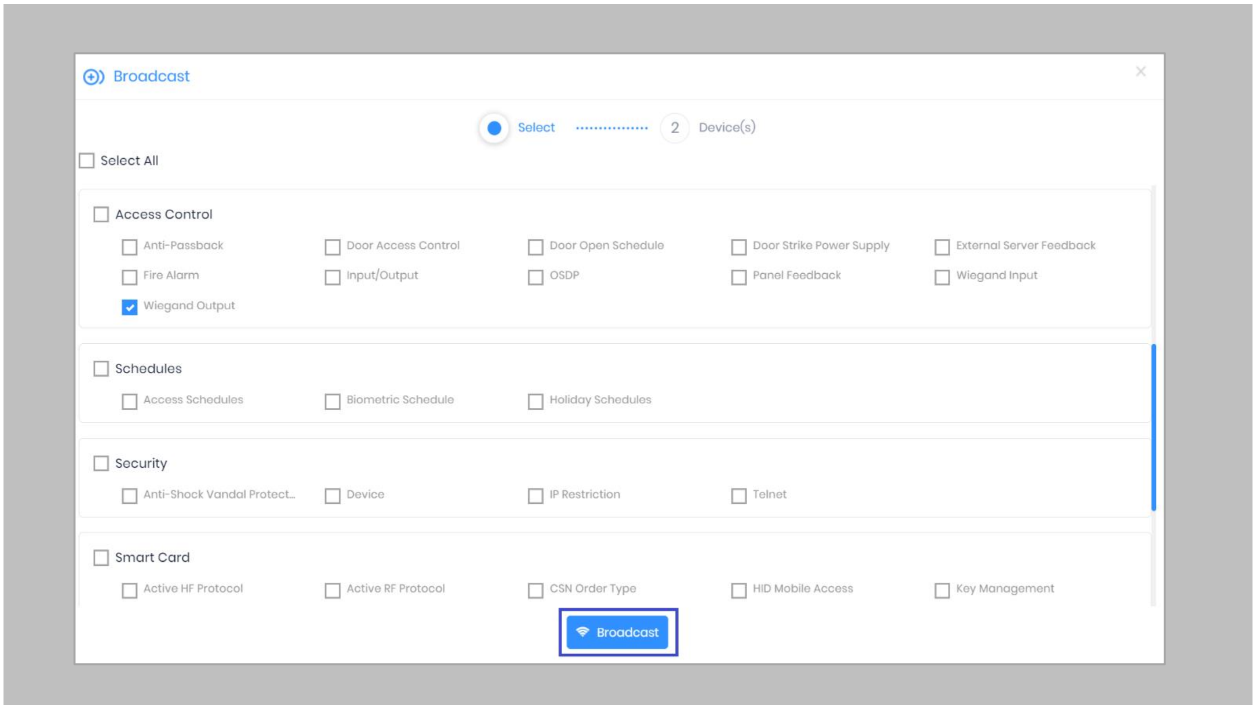
□ Fire Alarm □ Input/Output □ OSDP □ Panel Feedback □ Wiegand Input

☑ Wiegand Output

Figure 130: IXM WEB - Wiegand Output Selection in Broadcast

STEP 3

Click **Broadcast.**



Broadcast

● Select ·················· 2 Device(s)

□ Select All

□ Access Control

□ Anti-Passback □ Door Access Control □ Door Open Schedule □ Door Strike Power Supply □ External Server Feedback

□ Fire Alarm □ Input/Output □ OSDP □ Panel Feedback □ Wiegand Input

☑ Wiegand Output

□ Schedules

□ Access Schedules □ Biometric Schedule □ Holiday Schedules

□ Security

□ Anti-Shock Vandal Protect... □ Device □ IP Restriction □ Telnet

□ Smart Card

□ Active HF Protocol □ Active RF Protocol □ CSN Order Type □ HID Mobile Access □ Key Management

Figure 131: 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.

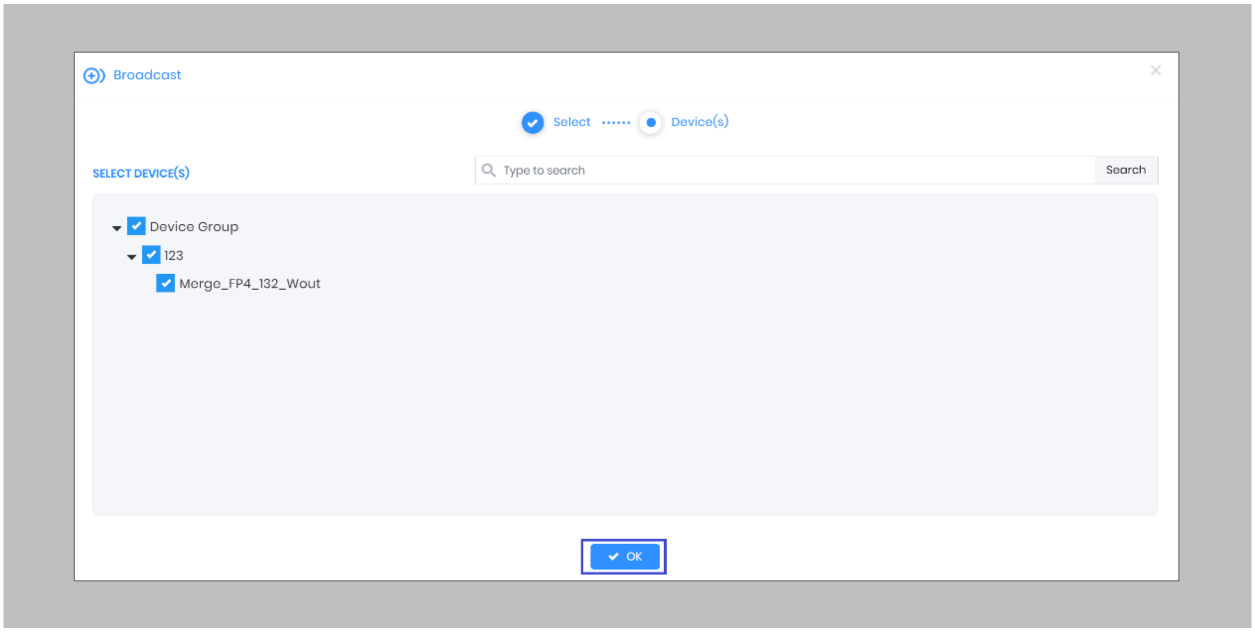


Figure 132: IXM WEB - Broadcast to Devices

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.

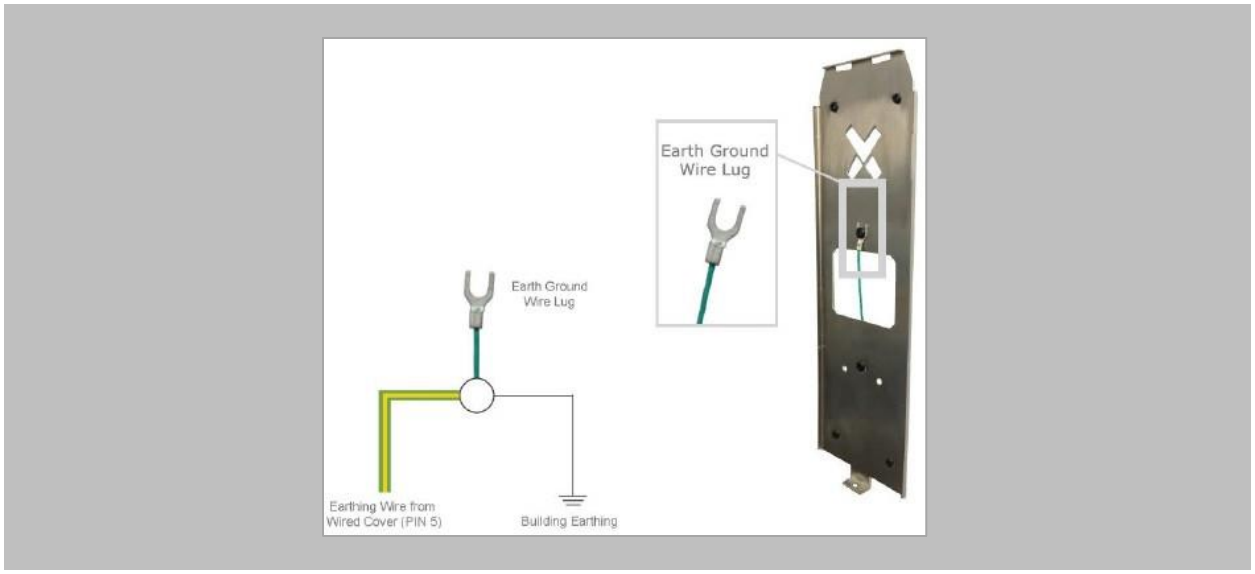


Figure 133: Earth Ground Wiring

WIRING

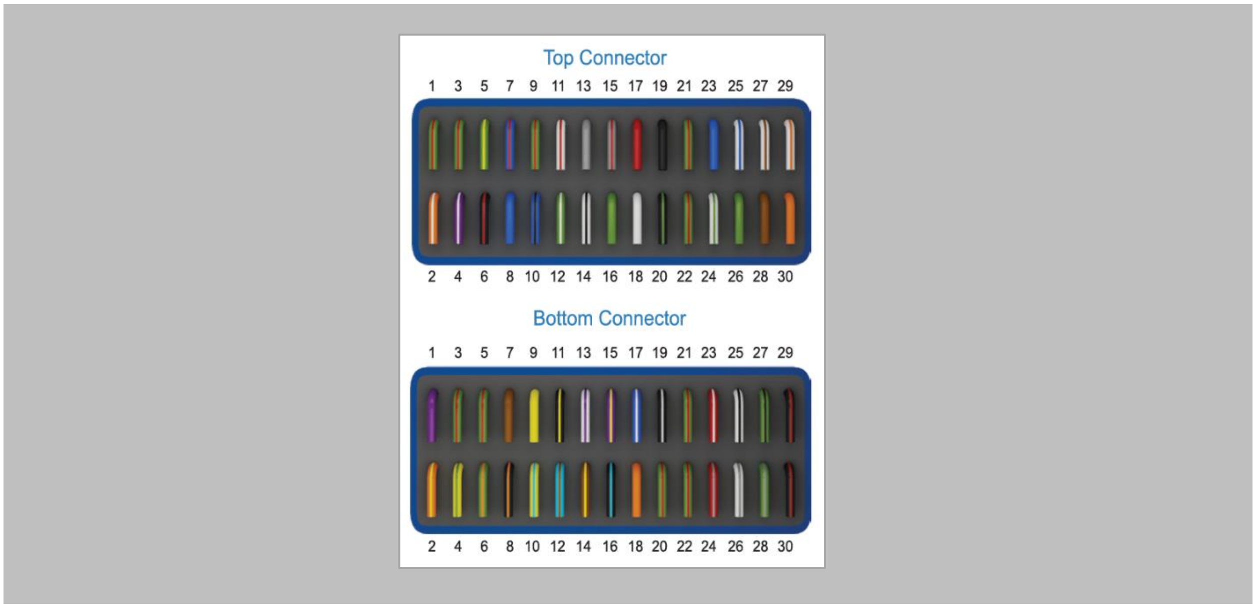
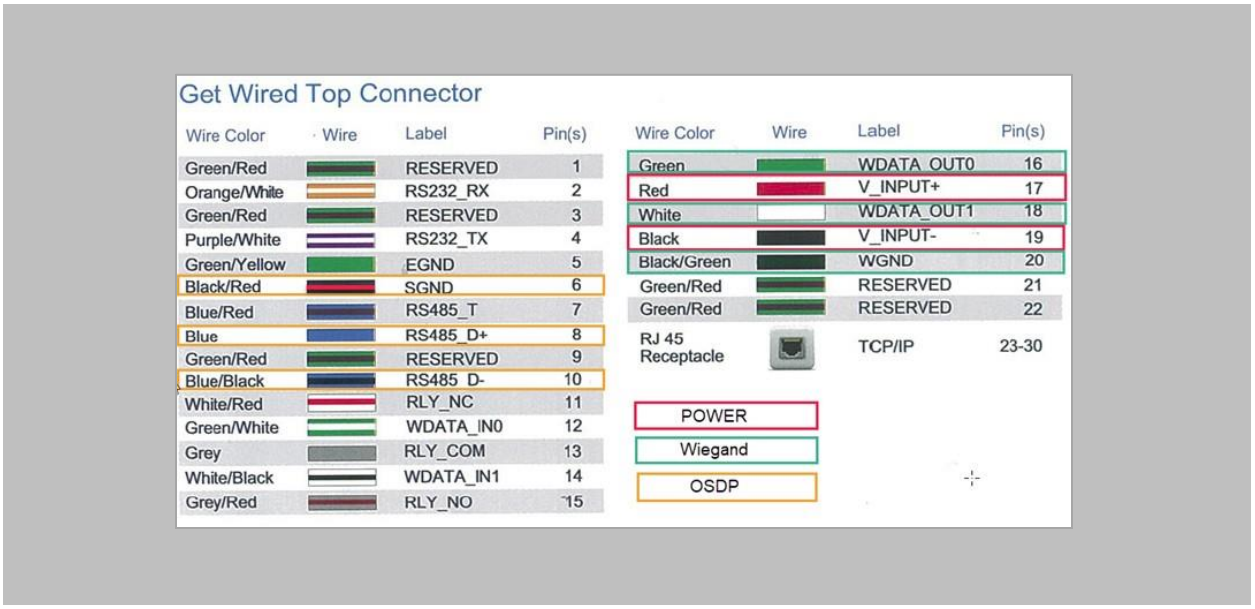


Figure 134: IXM TITAN – Top & Bottom Connector Wiring



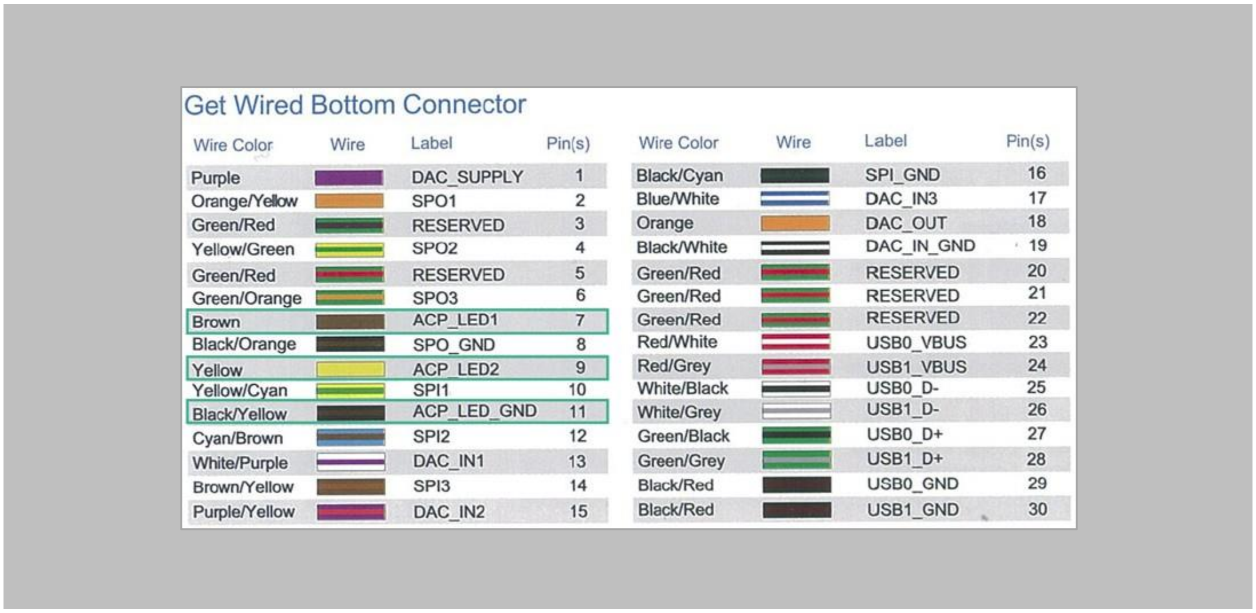
Get Wired Top Connector

Wire Color	Wire	Label	Pin(s)	Wire Color	Wire	Label	Pin(s)
Green/Red	🟩🟥	RESERVED	1	Green	🟩	WDATA_OUT0	16
Orange/White	🟧⬜	RS232_RX	2	Red	🟥	V_INPUT+	17
Green/Red	🟩🟥	RESERVED	3	White	⬜	WDATA_OUT1	18
Purple/White	🟪⬜	RS232_TX	4	Black	⬛	V_INPUT-	19
Green/Yellow	🟩🟨	EGND	5	Black/Green	⬛🟩	WGND	20
Black/Red	⬛🟥	SGND	6	Green/Red	🟩🟥	RESERVED	21
Blue/Red	🟦🟥	RS485_T	7	Green/Red	🟩🟥	RESERVED	22
Blue	🟦	RS485_D+	8	RJ 45 Receptacle	☎	TCP/IP	23-30
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				

POWER

Wiegand

OSDP



Get Wired Bottom Connector

Wire Color	Wire	Label	Pin(s)	Wire Color	Wire	Label	Pin(s)
Purple	🟪	DAC_SUPPLY	1	Black/Cyan	⬛🟦	SPI_GND	16
Orange/Yellow	🟧🟨	SPO1	2	Blue/White	🟦⬜	DAC_IN3	17
Green/Red	🟩🟥	RESERVED	3	Orange	🟧	DAC_OUT	18
Yellow/Green	🟨🟩	SPO2	4	Black/White	⬛⬜	DAC_IN_GND	19
Green/Red	🟩🟥	RESERVED	5	Green/Red	🟩🟥	RESERVED	20
Green/Orange	🟩🟧	SPO3	6	Green/Red	🟩🟥	RESERVED	21
Brown	🟫	ACP_LED1	7	Green/Red	🟩🟥	RESERVED	22
Black/Orange	⬛🟧	SPO_GND	8	Red/White	🟥⬜	USB0_VBUS	23
Yellow	🟨	ACP_LED2	9	Red/Grey	🟥▨	USB1_VBUS	24
Yellow/Cyan	🟨🟦	SPI1	10	White/Black	⬜⬛	USB0_D-	25
Black/Yellow	⬛🟨	ACP_LED_GND	11	White/Grey	⬜▨	USB1_D-	26
Cyan/Brown	🟦🟫	SPI2	12	Green/Black	🟩⬛	USB0_D+	27
White/Purple	⬜🟪	DAC_IN1	13	Green/Grey	🟩▨	USB1_D+	28
Brown/Yellow	🟫🟨	SPI3	14	Black/Red	⬛🟥	USB0_GND	29
Purple/Yellow	🟪🟨	DAC_IN2	15	Black/Red	⬛🟥	USB1_GND	30

Figure 135: 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

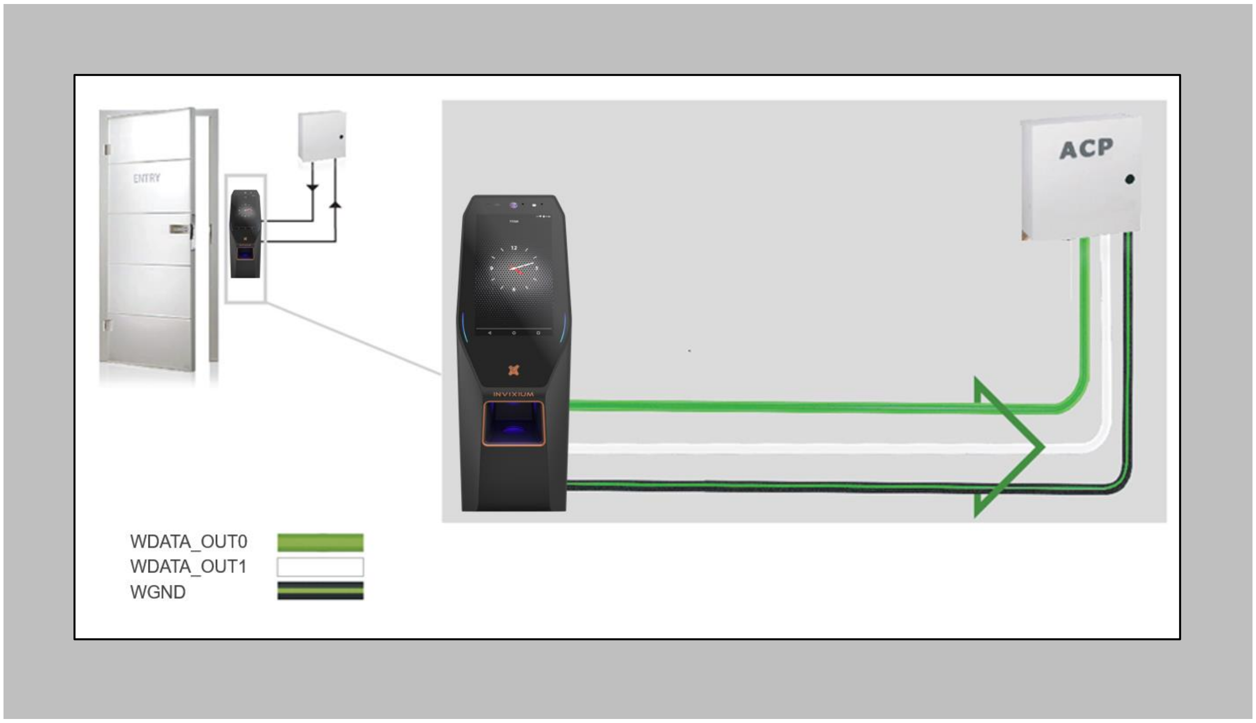
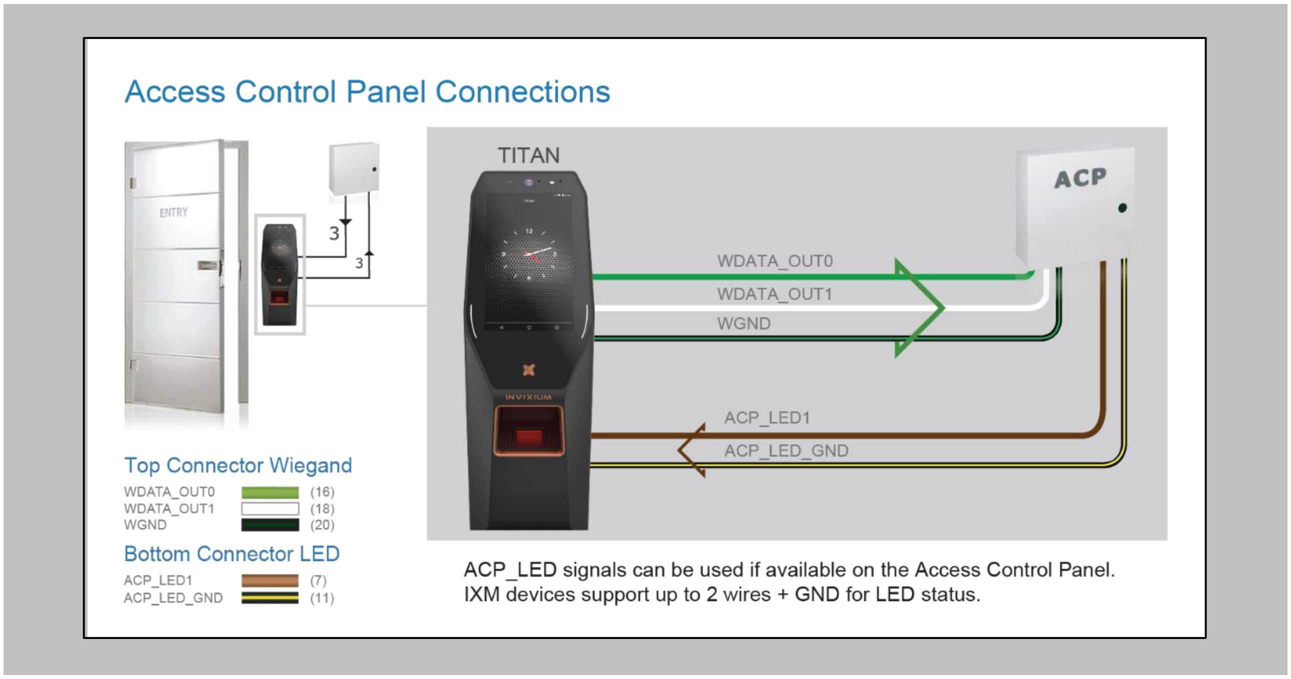


Figure 136: IXM TITAN - Wiegand

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



Access Control Panel Connections

Top Connector Wiegand

WDATA_OUT0	🟩	(16)
WDATA_OUT1	⬜	(18)
WGND	⬛	(20)

Bottom Connector LED

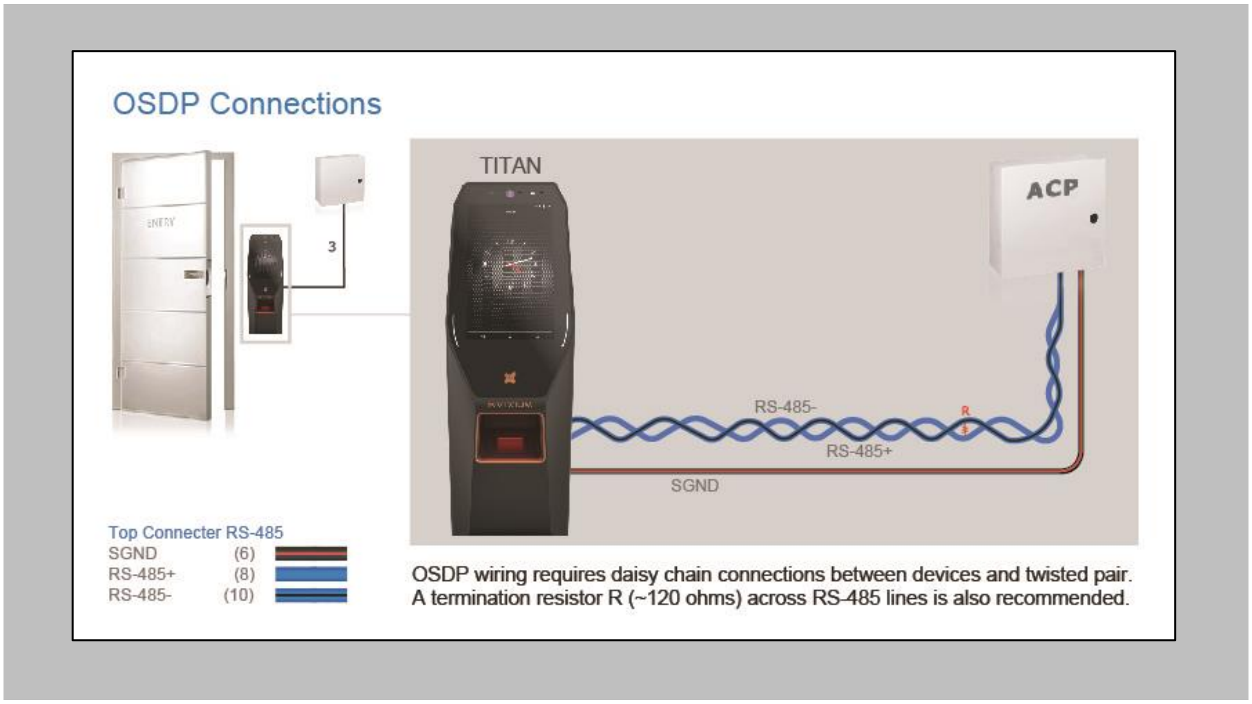
ACP_LED1	🟫	(7)
ACP_LED_GND	▨	(11)

ACP_LED signals can be used if available on the Access Control Panel.
IXM devices support up to 2 wires + GND for LED status.

Figure 137: 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



Top Connecter RS-485

SGND	(6)	▬
RS-485+	(8)	▬
RS-485-	(10)	▬

OSDP wiring requires daisy chain connections between devices and twisted pair. A termination resistor R (~120 ohms) across RS-485 lines is also recommended.

Figure 138: 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.

19. Troubleshooting

Reader Offline from IXM WEB Dashboard

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

Procedure

STEP 1

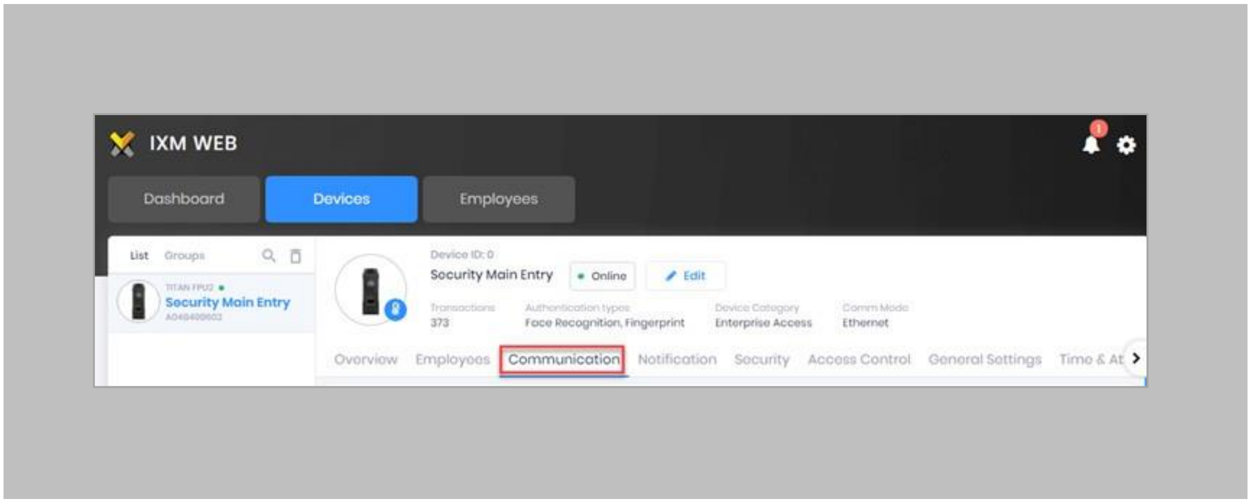
From **Home**, click the **Devices** tab.

STEP 2

Select any device.

STEP 3

Navigate to the **Communication** tab.



Device ID: 0

Security Main Entry

Transactions: 373

Authentication types: Face Recognition, Fingerprint

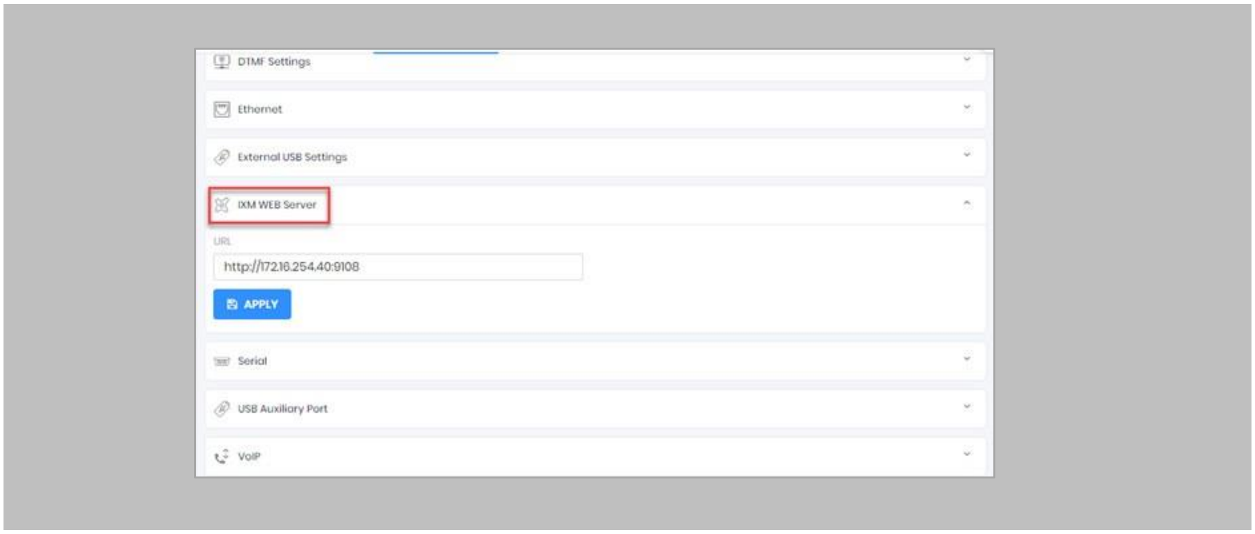
Device Category: Enterprise Access

Comm Mode: Ethernet

Figure 139: IXM WEB - Device Communication Settings

STEP 4

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



URL

http://172.16.254.40:9108

Figure 140: IXM WEB - Server URL Setting

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

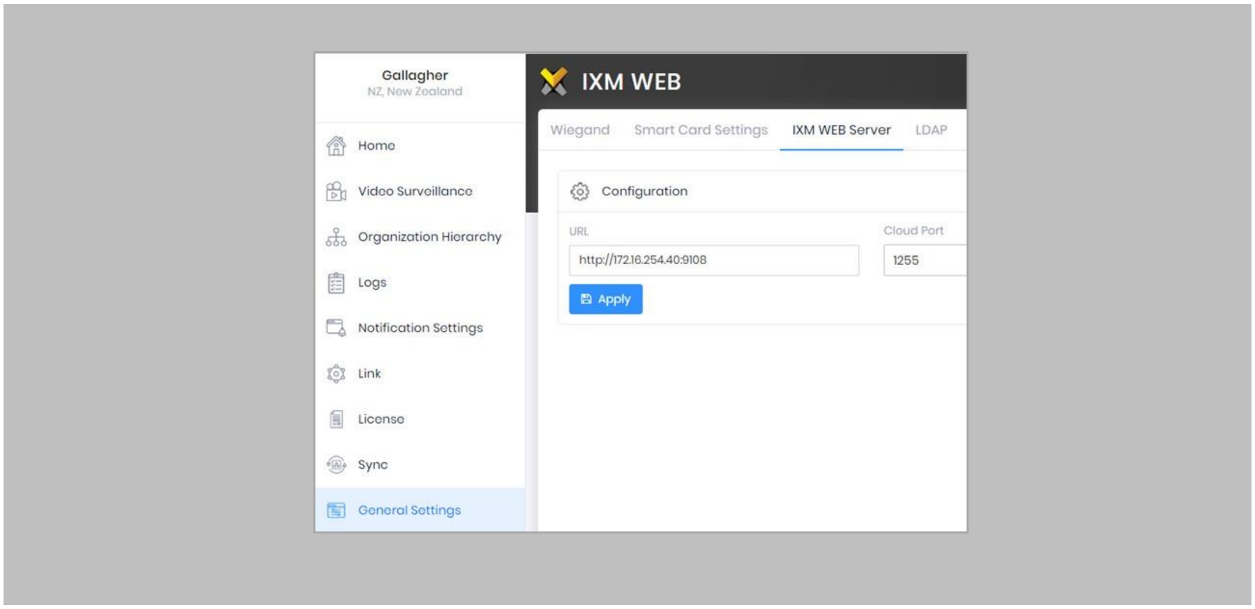
STEP 5

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.



URL: http://172.16.254.40:9108

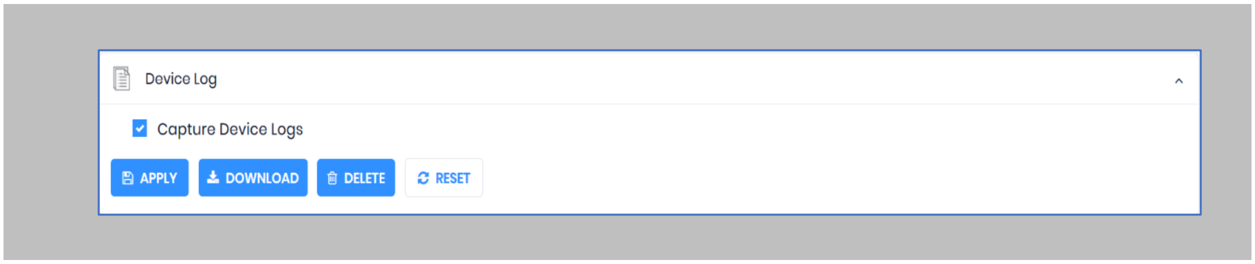
Cloud Port: 1255

Figure 141: IXM WEB - Server URL Setting from General Setting

Logs in IXM WEB Application

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

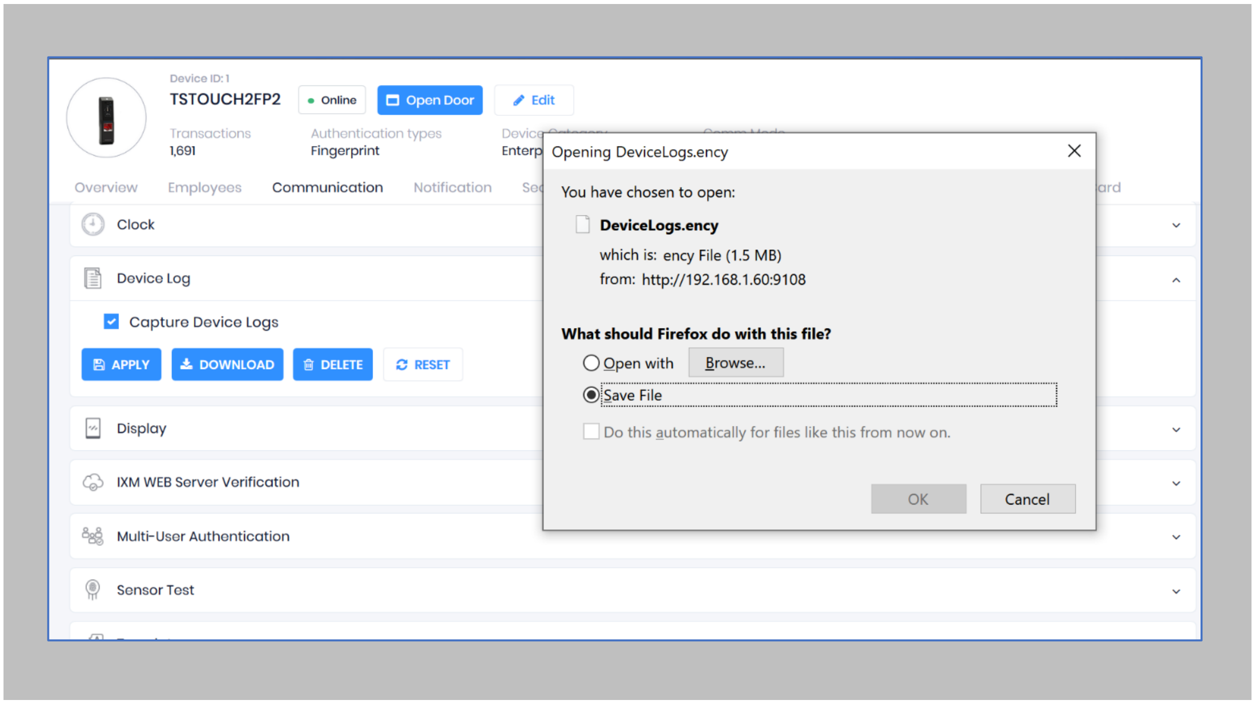
From **Home** → Click the **Devices** tab on the top → Select the required **Device** → Navigate to the General Settings tab for the device → Click on Device Log → Enable Capture Device Logs.


Device Log

☑ Capture Device Logs

Figure 142: IXM WEB - Enable Device Logs

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


Device ID: 1
TSTOUCH2FP2
● Online
Transactions 1,691
Authentication types Fingerprint

☑ Capture Device Logs

Opening DeviceLogs.ency

You have chosen to open:

DeviceLogs.ency
which is: ency File (1.5 MB)
from: http://192.168.1.60:9108

What should Firefox do with this file?

○ Open with Browse...
● Save File
□ Do this automatically for files like this from now on.

Figure 143: 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.