



IXM WEB Integration with SIEMENS SiPort

Installation Instructions

V1.0



Table of Contents

1. Introduction	8
Purpose	8
Summary of key features related to this IXM WEB and SSP Integration	8
Description	8
Acronyms	8
Field Mappings	9
2. Compatibility	10
Invixium Readers	10
Software Requirements	10
Other Requirements	11
Compatibility Matrix for IXM WEB & SiPort Integration	11
3. Checklist	12
4. Task List Summary	13
5. Prerequisites for SSP and IXM WEB Integration	14
SiPort API Configuration	14
6. Prerequisites for Installing Invixium IXM WEB Software	15
Acquiring IXM WEB Activation Key	15
Setting Up SQL instance	17
Minor Checklist and Considerations	21
7. Installing IXM WEB	22
Software Install	22
8. Configuring Email Settings using IXM WEB	30
Email Setting Configuration	30
9. Software and Module Activation	35
IXM WEB Activation	35
SiPort Module Activation	38
10. Configuring IXM Link for SIEMENS	41
11. Add and Configure Invixium Readers	47



Adding an Invixium Reader in IXM WEB	47
12. Adding an Invixium Device to a Device Group.....	52
Configuring Wiegand Format to Assign Invixium Readers	53
Assign Wiegand to Invixium Readers	56
Configuring Thermal Settings	59
Thermal Calibration.....	63
Test Calibration Options.....	67
Change Temperature Unit Settings	68
Configuring Mask Authentication Settings	70
13. Enrollment Best Practices	73
Fingerprint Enrollment Best Practices.....	73
Avoid Poor Fingerprint Conditions	73
Fingerprint Image Samples.....	74
Fingerprint Imaging Do's and Don'ts.....	75
Finger Vein Enrollment Best Practices	76
Face Enrollment Best Practices	77
14. Appendix	78
Installing Invixium IXM WEB with Default Installation using SQL Server 2014	78
Pushing Configuration to Multiple Invixium Readers	83
Configuring for OSDP Connection	86
Configuring MIFARE DESFire Custom Cards	92
Wiring and Termination	95
Wiring	96
Wiegand Connection.....	98
Wiegand Connection with Panel Feedback	99
OSDP Connections	100
15. Troubleshooting.....	101
Reader Offline from the IXM WEB Dashboard	101
Logs in IXM WEB Application	104
Unable to connect to the SiPort Server.....	106
16. Support	109
17. Disclaimer and Restrictions	109



List of Figures

Figure 1: IXM WEB Online Request Form.....	15
Figure 2: Sample Email After Submitting Online Request Form	16
Figure 3: SQL New Login.....	18
Figure 4: SQL Login Properties.....	19
Figure 5: SQL Server Roles	20
Figure 6: IXM WEB Installer.....	22
Figure 7: Advanced Options in IXM WEB Installer	23
Figure 8: Invixium Fingerprint Driver Installation Message	24
Figure 9: IXM WEB Installation Progress	24
Figure 10: IXM WEB Installation Completed	25
Figure 11: IXM WEB Icon - Desktop Shortcut	26
Figure 12: IXM WEB Database Configuration	26
Figure 13: IXM WEB Administrator User Configuration	27
Figure 14: IXM WEB Login Page	28
Figure 15: Configure Email	30
Figure 16: IXM WEB - SMTP Settings.....	31
Figure 17: IXM WEB - Save Email Settings	32
Figure 18: IXM WEB - Test Connection	32
Figure 19: IXM WEB - Enter Email ID	33
Figure 20: IXM WEB - Forgot Password	34
Figure 21: IXM WEB - Enter Login Credentials	35
Figure 22: IXM WEB - License Setup.....	36
Figure 23: IXM WEB - Online Activation.....	37
Figure 24: IXM WEB - SIEMENS Link Activation	38
Figure 25: SIEMENS License Key Email.....	39
Figure 26: IXM WEB - Activate SIEMENS Link License	40
Figure 27: IXM WEB - Link Menu.....	41
Figure 28: IXM WEB - Enable SIEMENS Link Module	42
Figure 29: IXM WEB - Map Access Group to User Group.....	43
Figure 30: IXM WEB - Sync Direction	44
Figure 31: IXM WEB - Sync Activities	45
Figure 32: IXM WEB - Devices Tab	47
Figure 33: IXM WEB - Search Device Using IP Address.....	48
Figure 34: IXM WEB - Register Device	49



Figure 35: IXM WEB - Device Registration Complete	50
Figure 36: IXM WEB - Dashboard, Device Status	51
Figure 37: IXM WEB - Assign Device Group	52
Figure 38: IXM WEB - Create Wiegand Format	53
Figure 39: IXM WEB - Create Custom Wiegand Format	54
Figure 40: IXM WEB – Create Wiegand Format.....	54
Figure 41: IXM WEB - Upload Wiegand Format.....	55
Figure 42: IXM WEB - Navigate to Access Control Tab	56
Figure 43: IXM WEB - Wiegand Output.....	57
Figure 44: IXM WEB - Save Output Wiegand.....	58
Figure 45: IXM WEB - Thermal Settings	59
Figure 46: IXM WEB - Save Thermal Settings	62
Figure 47: IXM WEB - Thermal Calibration Settings.....	63
Figure 48: IXM WEB - Save Thermal Calibration Settings.....	64
Figure 49: IXM WEB - Capture Thermal Data	65
Figure 50: IXM WEB - Save Captured Thermal Data	66
Figure 51: IXM WEB - Test Thermal Calibration	67
Figure 52: IXM WEB - Option to Change Temperature Unit	68
Figure 53: IXM WEB - Save Temperature Unit Setting.....	69
Figure 54: IXM WEB - Mask Authentication Settings.....	70
Figure 55: IXM WEB - Save Mask Settings.....	72
Figure 56: Fingerprint Enrollment Best Practices	73
Figure 57: Fingerprint Images Samples	74
Figure 58: Finger Vein Enrollment Best Practices	76
Figure 59: Face Enrollment Best Practices	77
Figure 60: Install IXM WEB	78
Figure 61: Loading SQL Express & Installation Progress.....	79
Figure 62: IXM WEB - Shortcut Icon on Desktop	80
Figure 63: IXM WEB - Configuring IXM WEB Database.....	81
Figure 64: IXM WEB - Select Database Name.....	81
Figure 65: IXM WEB - Server URL format.....	82
Figure 66: IXM WEB - Broadcast Option.....	83
Figure 67: IXM WEB - Wiegand Output Selection in Broadcast	83
Figure 68: IXM WEB - Broadcast Wiegand Output Settings	84
Figure 69: IXM WEB - Broadcast to Devices.....	85
Figure 70: IXM WEB - OSDP Settings	86
Figure 71: IXM WEB - Save OSDP Settings	89



Figure 72: IXM WEB - Edit Device	90
Figure 73: IXM WEB - Edit Device Options	90
Figure 76: IXM WEB - Disable Panel Feedback.....	91
Figure 77: IXM WEB - MIFARE DESFire Configuration	92
Figure 78: IXM WEB - MIFARE DESFire Sample Configuration.....	94
Figure 79: Earth Ground Wiring	95
Figure 80: IXM TITAN – Top & Bottom Connector Wiring	96
Figure 81: Power, Wiegand & OSDP Wires	97
Figure 82: IXM TITAN - Wiegand	98
Figure 83: IXM TITAN - Panel Feedback	99
Figure 84: IXM TITAN - OSDP Connections	100
Figure 85: IXM WEB - Device Communication Settings	101
Figure 86: IXM WEB - Server URL Setting.....	102
Figure 87: IXM WEB - Server URL Setting from General Settings	103
Figure 88: IXM WEB - Enable Device Logs.....	104
Figure 89: Save Device Log File	104
Figure 90: IXM WEB - Licence Module	106
Figure 91: IXM WEB - SiPort Link Module	107
Figure 92: SIEMENS SiPort API	108



List of Tables

Table 1: Compatibility Matrix for IXM WEB & SIEMENS Integration.....	11
Table 2: Task List Summary	13
Table 3: System Related Checklist	21
Table 4: Port Information	21
Table 5: IXM WEB - OSDP Configuration Options	88
Table 6: IXM WEB - OSDP Text Options	89
Table 7: IXM WEB – MIFARE DESFire Configuration Options.....	94
Table 8: Logs Folder Location.....	105

1. Introduction

Purpose

This document outlines the process of configuring the software integration between SIEMENS SiPort (SSP) and Invixium's IXM WEB.

Summary of key features related to this IXM WEB and SSP Integration

- SiPort API to support SiPort integration
- ['Sync All' feature](#) to resynchronize the database from SSP to IXM WEB
- [MIFARE DESFire custom layout](#) to support SIEMENS access card

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 SIEMENS SiPort 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 SiPort by using SIEMENS SiPort API to import cardholders.

Acronyms

Acronym	Description
API	SIEMENS SiPort API
ACPCS	Access Control Panel Configuration Software
SSP	SIEMENS SiPort
IXM	Invixium



Field Mappings

The following are the SSP fields that are mapped to IXM WEB:

SSP Field	IXM Field	Notes
Auto ID	Internal mapping with ACPID	
Person ID	Employee ID	
First name	First Name	First Name is a mandatory field in IXM WEB and not mandatory in SiPort. While importing, if the First Name is null in SiPort, then the Last Name will be considered as First Name in IXM WEB. If the Last Name is also null, then Card Number will be considered as First Name in IXM WEB.
Last name	Last Name	
ValidTo	Employee End Date	The start date in IXM WEB will be the date and time of import.
Gender	Gender	
Status	Suspend	An employee that is "Inactive" in SiPort will be marked as suspended in SiPort.
Cards	Prox ID	Multiple cards will be imported using a card array if exist in SiPort.
Profiles	Employee Group, Device Group, and Sync Group	Setting Map Access Group to YES in configuration will create an employee group, device group, and sync group in IXM WEB. Further employees imported from SSP will be added to this created employee group and will be used for automatic transfer to IXM devices. Refer to separate Feature Description Documents (FDDs) accessible from Invoxium Customer Portal for details on Employee/Device/Sync Groups.



Note: Multiple Cards - SSP can have multiple cards per user, and IXM WEB supports a maximum of 10 cards per user. IXM Link selects the available valid cards.

As SiPort does not maintain the status of the card, IXM Web will consider the card status as "Active".

The API will fetch all the cardholders with cards based on Last Modified Date and Time.



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
SIEMENS SiPort	3.1.4.286
Invixium IXM WEB	2.3.0.0
Operating Systems	Windows 10 (Build 1709+) Professional Version Windows Server 2016 Standard Windows Server 2019 Supported but not recommended: (Legacy) <i>Windows 8.1</i> <i>Windows Server 2012 R2</i> <i>Windows Server 2012</i>
Microsoft .NET Framework	.NET Framework 4.8
Database Engine	SQL Server 2016+ Supported but not recommended: (Legacy) SQL Server 2014 Express Edition (Default Installation)
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 10-15 devices registered with 500 employees or fewer. For large enterprise installation server requirements, contact support@invixium.com.

Compatibility Matrix for IXM WEB & SiPort Integration

IXM WEB version	SiPort version	Compatible
IXM WEB 2.3.0.0	v3.1.4.286	Yes

Table 1: Compatibility Matrix for IXM WEB & SIEMENS Integration



3. Checklist

Item List	Interface
SiPort API Configuration	SIEMENS
IXM WEB Activation ID	Invixium
SQL Instance on SQL Server 2016+	Invixium
Install IXM WEB Application	Invixium
IXM WEB and IXM Link Activation	Invixium
Configure IXM Link to SIEMENS	Invixium
Configure Invixium Reader	Invixium
Face or Finger Enrollment	Invixium

4. Task List Summary

Task	IXM WEB Application Task List using IXM WEB	SIEMENS SiPort Task List using SSP
1	Activate IXM WEB and IXM Link for SSP	Create Cardholder. Assign Card and Access Profile to cardholder
2	Configure IXM Link for SSP	Define Reader and Door in SSP for integration with SiPort Controller on OSDP
3	Register IXM Devices and configure settings as per the requirement	Monitor Events
4	Configure Weigand or OSDP settings in the device for integration with SIEMENS SiPort	
5	Assign a specific Device Group to the device	

Table 2: Task List Summary



5. Prerequisites for SSP and IXM WEB Integration

SiPort API Configuration

SIEMENS has to deploy and configure the SiPort API package at the customer end. The integration between SSP and IXM WEB will be successful only once the API is up and running.

To access SiPort API, IXM Web is required to pass basic authentication which includes username and password. The data will be retrieved only after successful authentication.

On accessing the SiPort API, cardholder information will be fetched by using CardholderWithChild API available on the following path:

<https://{SIPORT-Server}:{port}/API/Cardholderwithchild>

6. Prerequisites for Installing Invixium IXM WEB Software

Acquiring IXM WEB Activation Key

Procedure

STEP 1

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* v	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* v	Postal Code*

< Back
Submit

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 sample of the email that includes instructions on how to download and install IXM WEB along with your Activation ID.

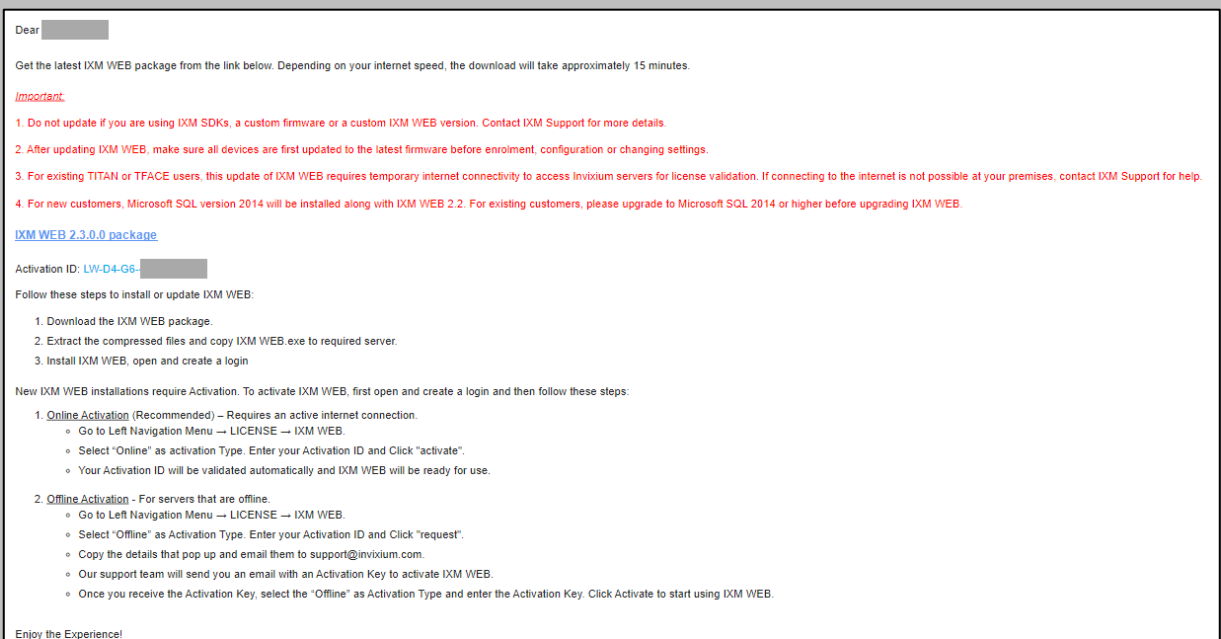



Figure 2: Sample Email After Submitting Online Request Form



Setting Up SQL instance

 Note: The following section describes the setup of a pre-created instance of SQL 2016+. Creating a new instance can be done with the use of SQL Installer within the SiPort installation media kit.

Procedure

STEP 1

Make sure to **Create** a new SQL instance on the server.

STEP 2

Set the instance name as IXM WEB (default) or Invixium.

STEP 3

Select mixed mode: SQL Authentication and Windows Authentication for secure logins. Leave everything else as default.

STEP 4

Install **SQL Management Studio** on the server.

STEP 5

Log into the new instance and create a new user.

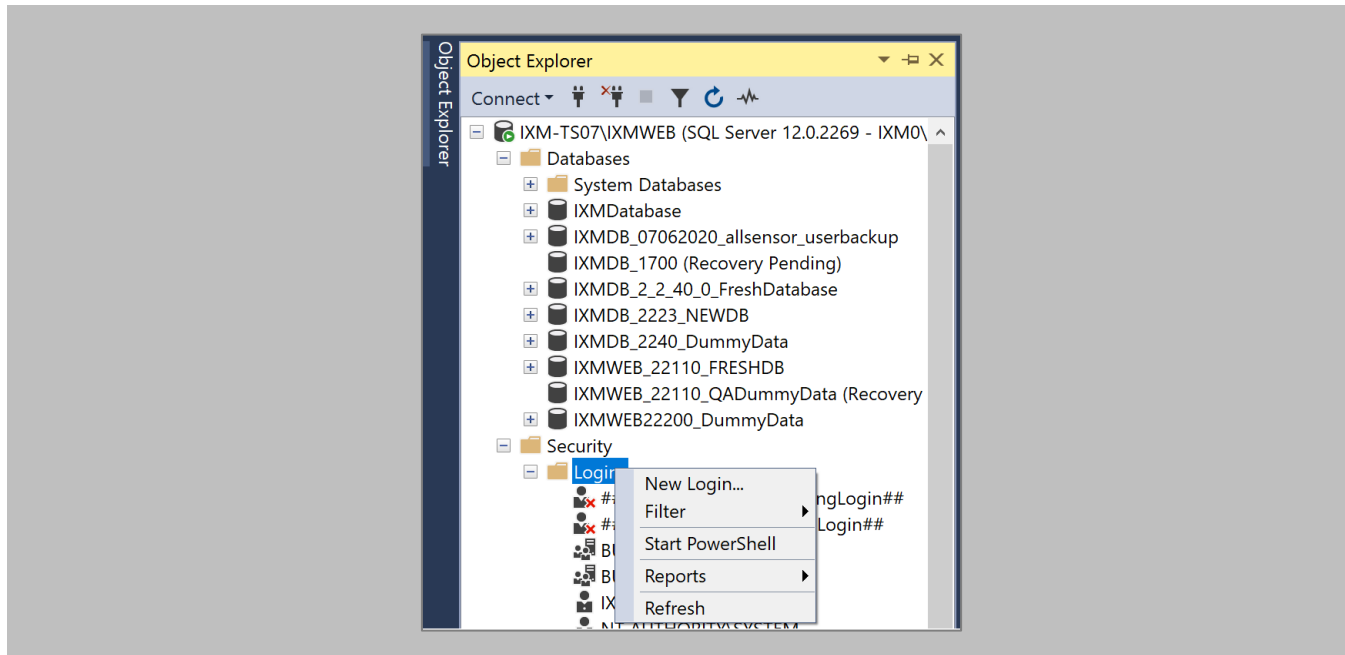



Figure 3: SQL New Login

STEP 6

Select **SQL Server authentication**.

 Note: Make sure to uncheck both 'Enforce password expiration' and 'User must change password at next login'.

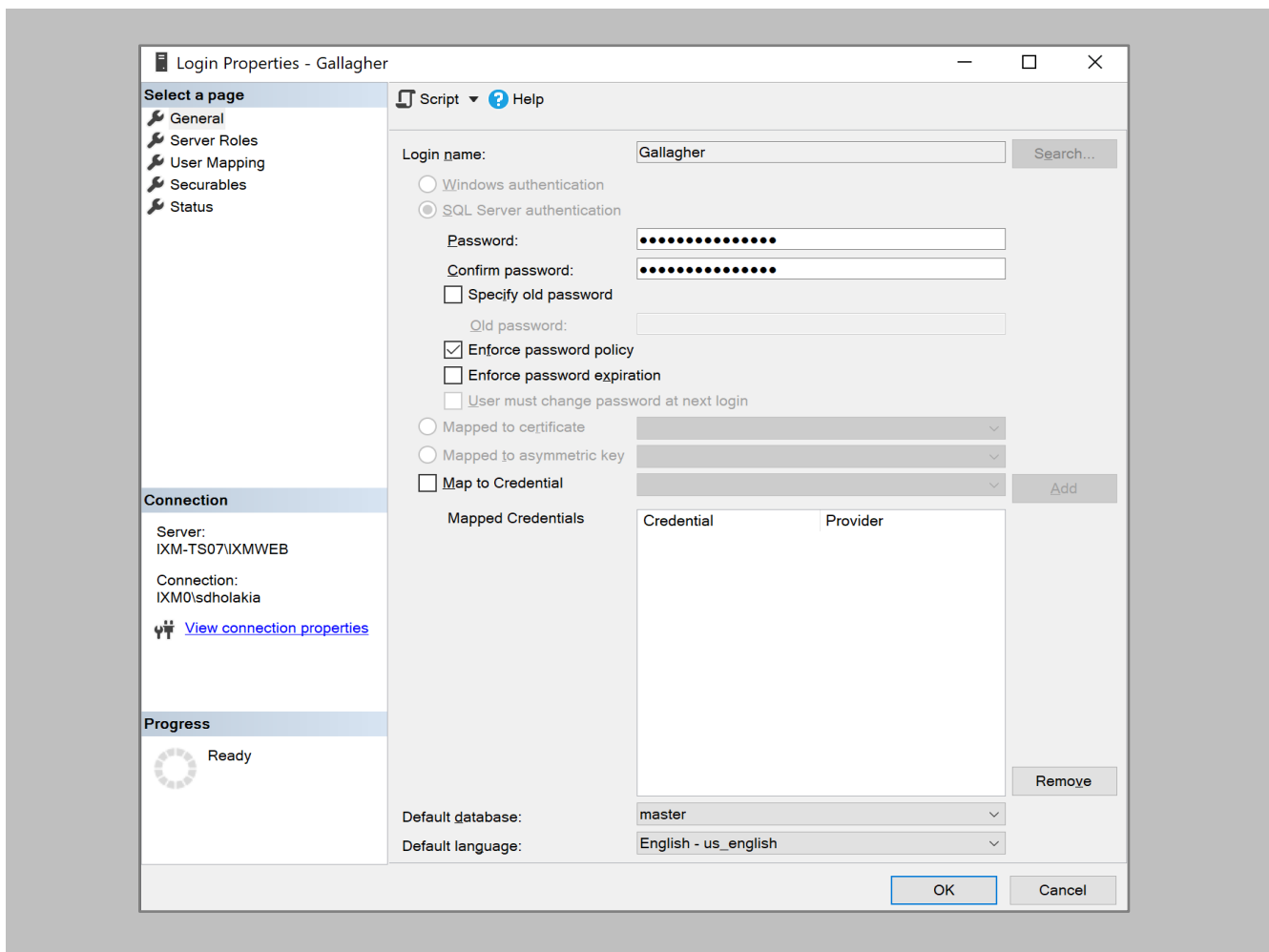


Figure 4: SQL Login Properties

STEP 7

Add this user under **Server Roles**, **dbcreator**, and **sysadmin**.

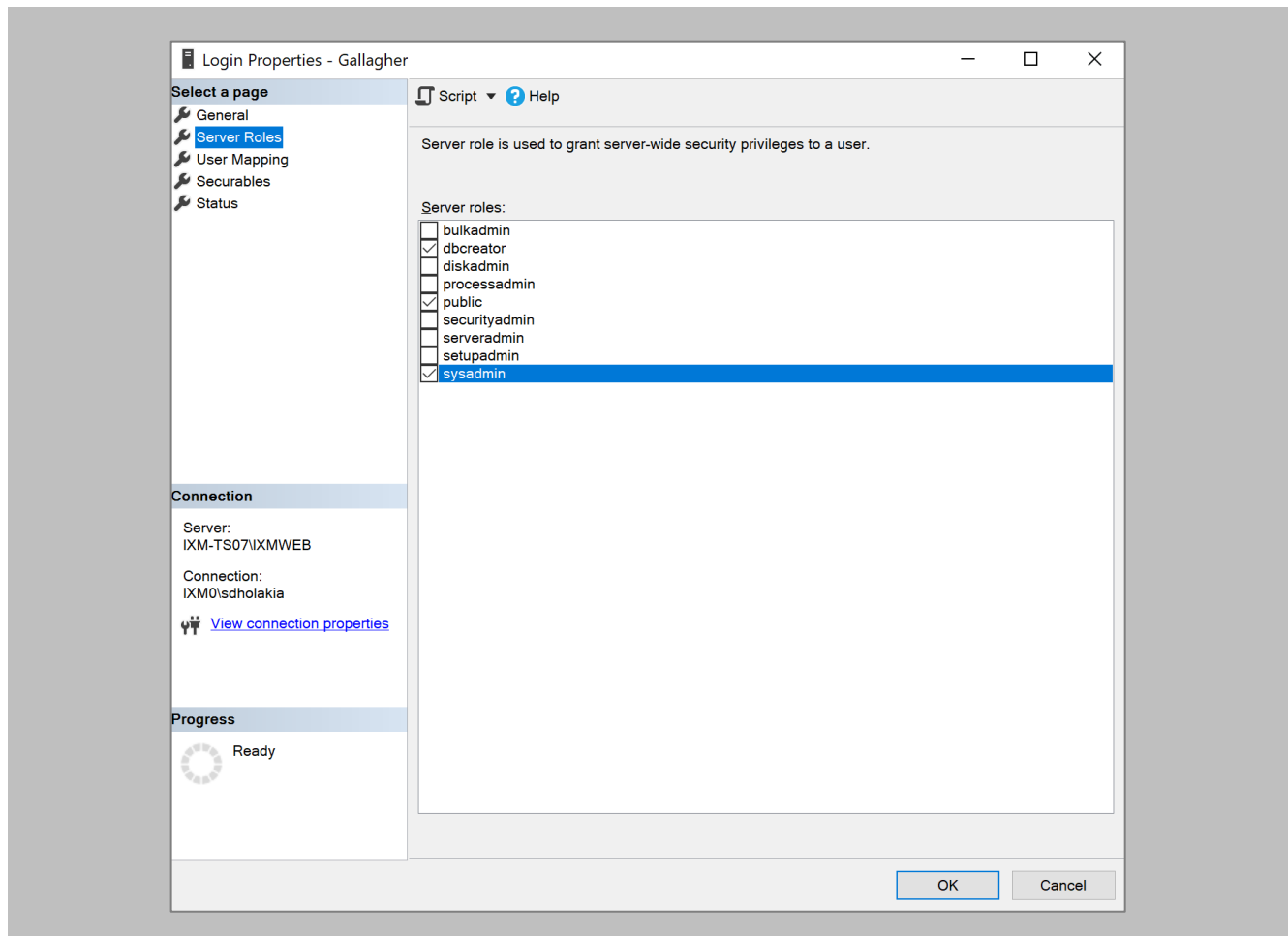


Figure 5: SQL Server Roles

RESULT

These privileges will be used later in the installation process to create the database.

Minor Checklist and Considerations

Use these tables to verify that you have carried out all the required steps.

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

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
SSP API Port	1255

Table 4: Port Information

7. Installing IXM WEB

Software Install

Procedure

STEP 1

Run the IXM WEB installer (Run as administrator).

Select **Advanced**.

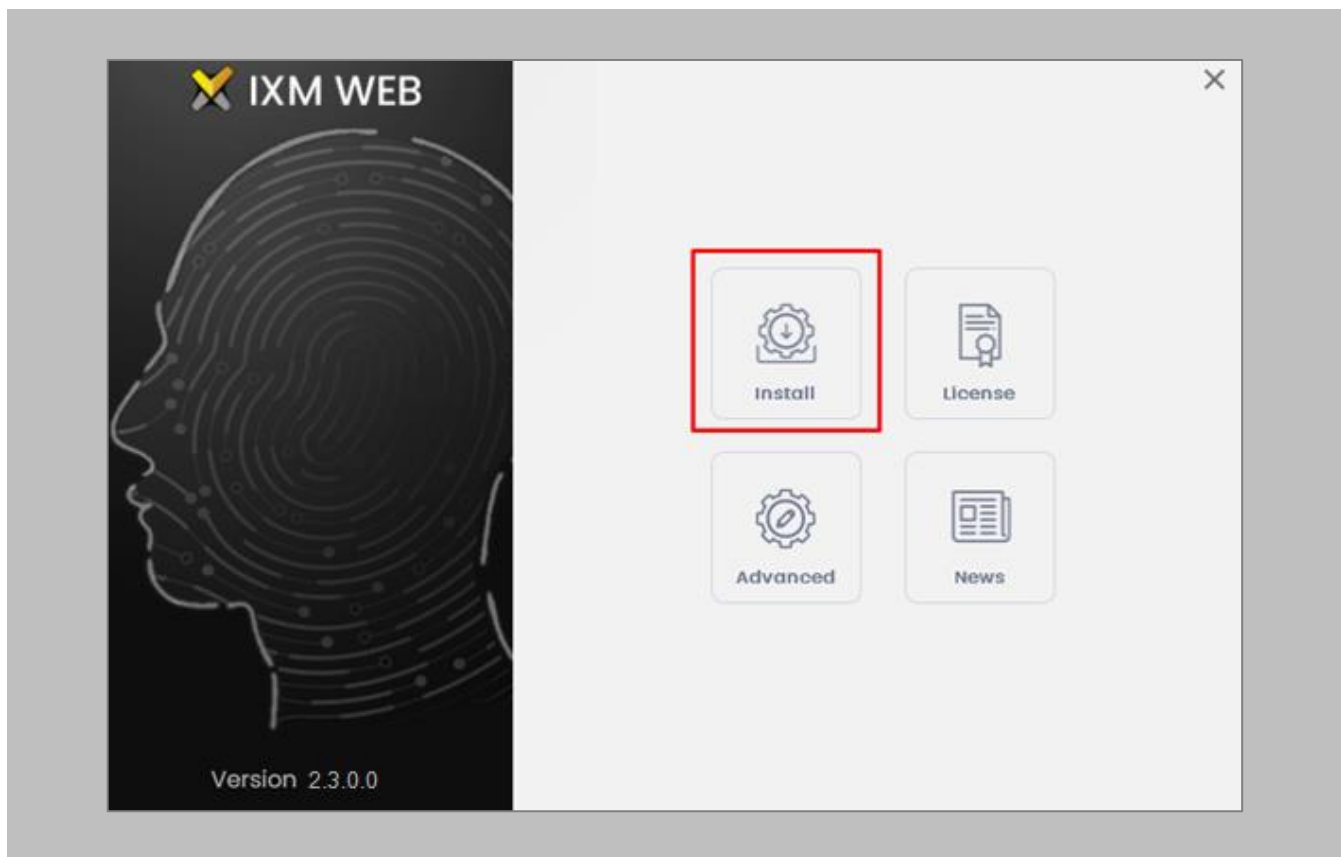


Figure 6: IXM WEB Installer

STEP 2

Deselect **Install SQL Server** and select **Install**.

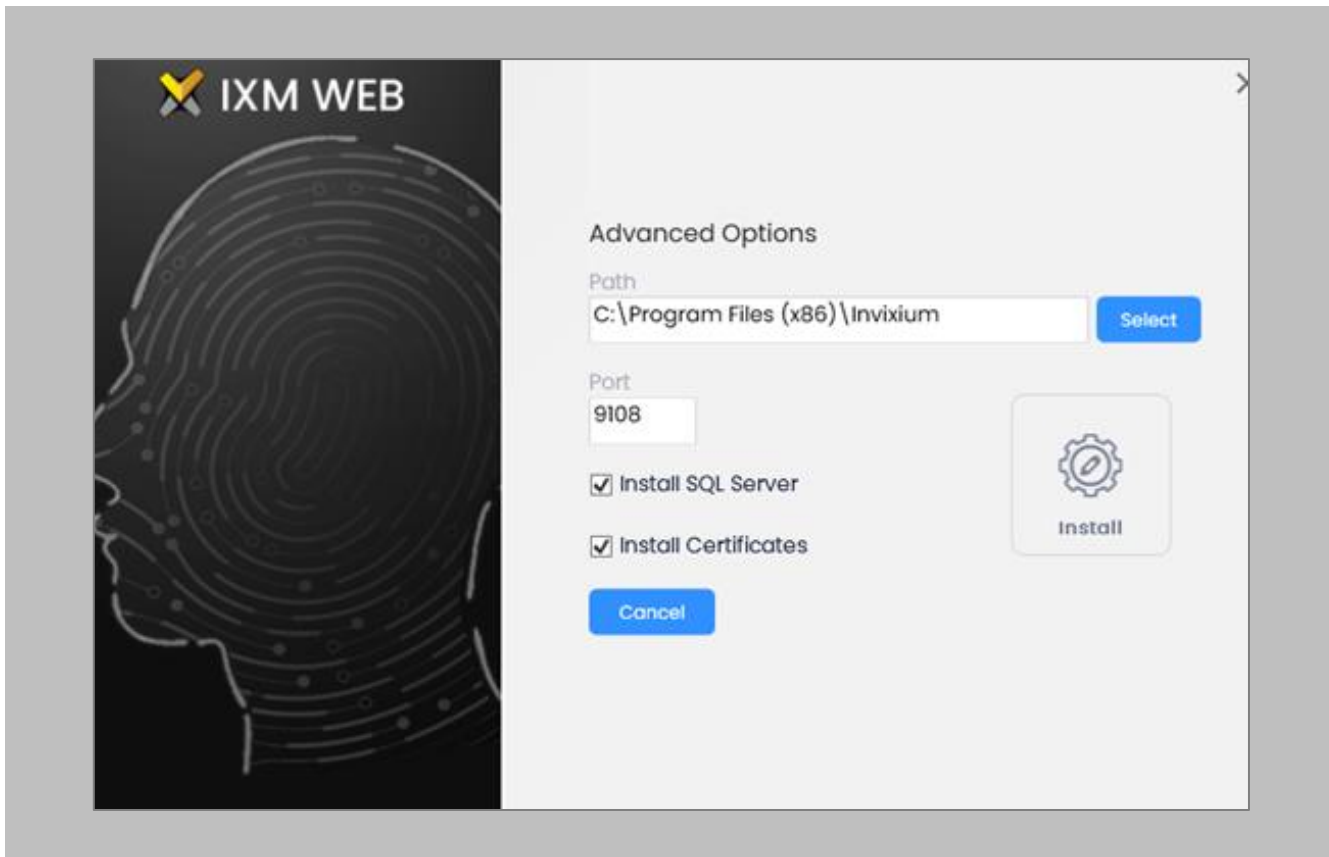


Figure 7: Advanced Options in IXM WEB Installer

STEP 3

During the installation, you may see this message, click **Install**.

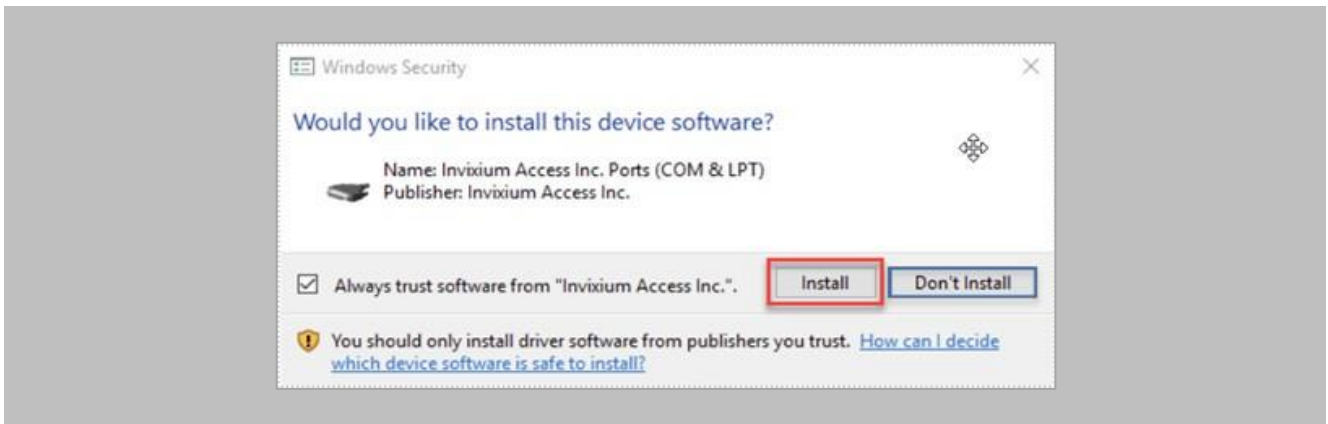


Figure 8: Invidia Fingerprint Driver Installation Message

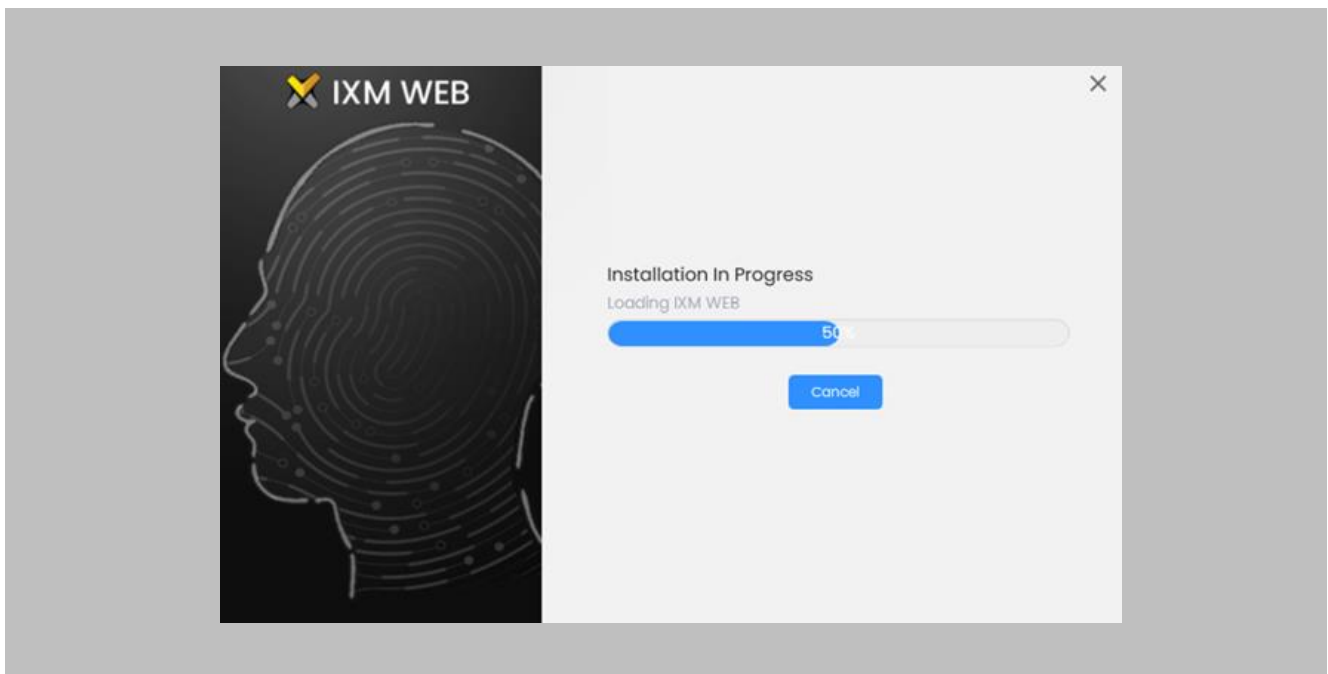


Figure 9: IXM WEB Installation Progress

STEP 4

After the installation completes, you should see the following screen:

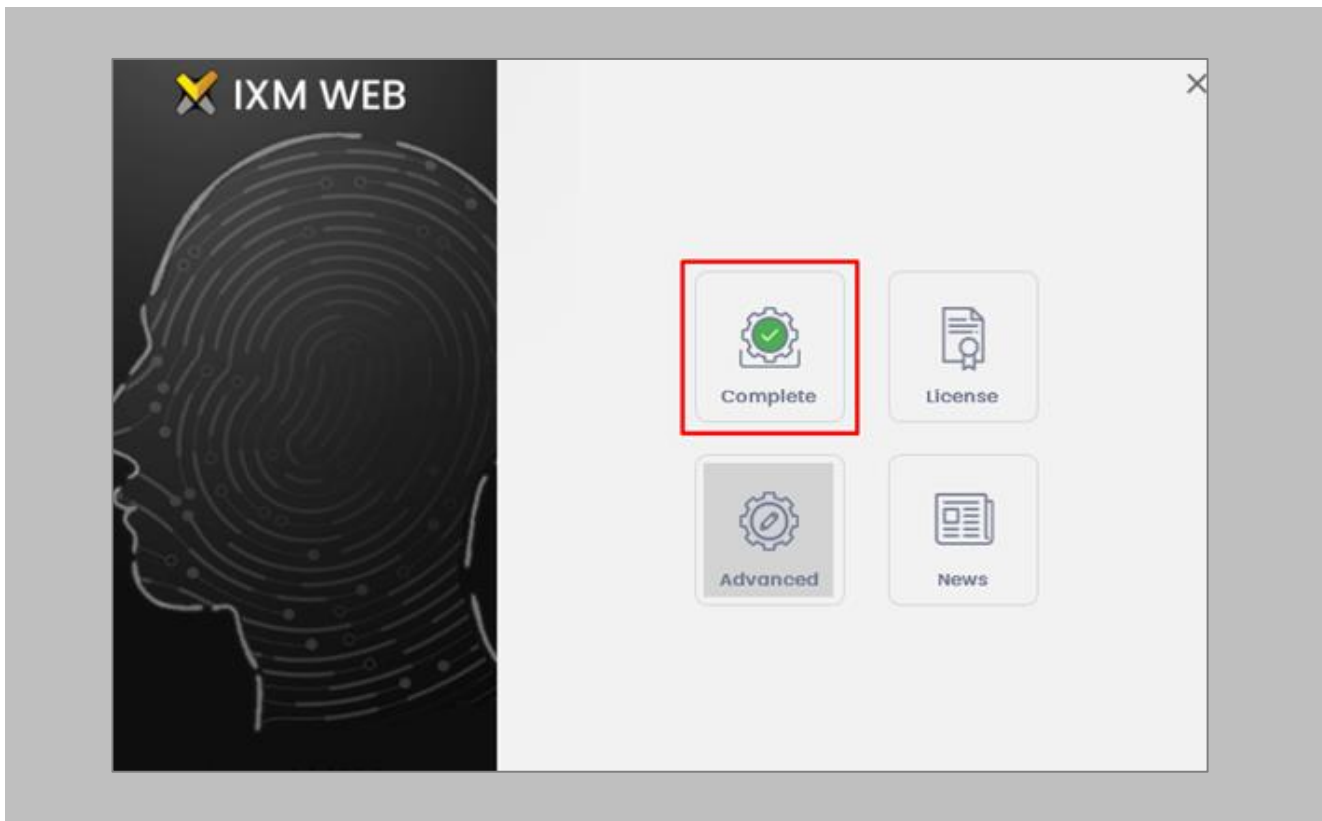


Figure 10: IXM WEB Installation Completed

Click on the **X** in the upper right corner to close.

STEP 5

Double-click on the new **desktop shortcut** to open IXM WEB.

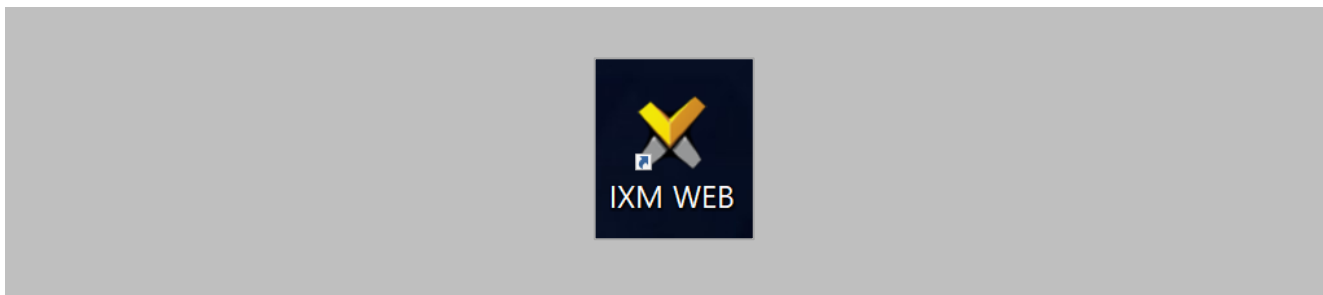


Figure 11: IXM WEB Icon - Desktop Shortcut

IXM WEB will open in your default browser (initial opening may take a few minutes).

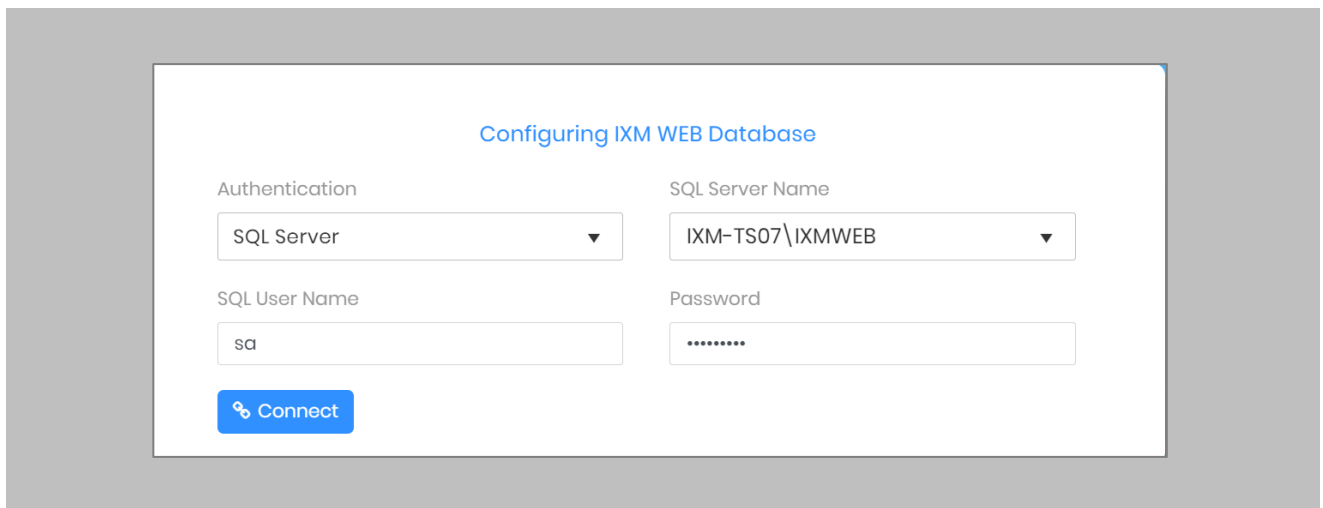


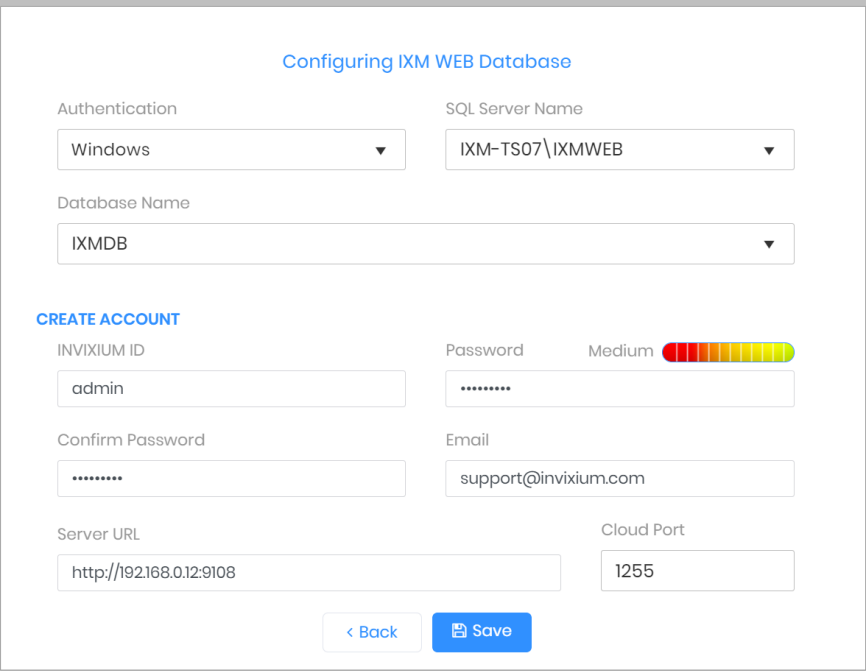
Figure 12: IXM WEB Database Configuration

STEP 6

Select the **SQL Server** authentication and the **Server Name** from the drop-down options. If it does not appear, enter it manually.

STEP 7

Enter the user credentials created above and leave **IXMDB** as the database name.



Configuring IXM WEB Database

Authentication: Windows | SQL Server Name: IXM-TS07\IXMWEB

Database Name: IXMDB

CREATE ACCOUNT

INVIXIUM ID: admin | Password: Medium (strength indicator) | Confirm Password: | Email: support@invixium.com

Server URL: http://192.168.0.12:9108 | Cloud Port: 1255

< Back | Save

Figure 13: IXM WEB Administrator User Configuration

Now comes the step to create the user account for Invixium to access the database itself.

STEP 8

Create a **user account** (this is different from the identity used to connect to the SQL instance at the top of the page). The status bar will indicate the strength of the chosen password.

STEP 9

Change **http://localhost:9108** to **http://[IP address of server]:9108**

For example:

If the IP address of the server is 192.168.1.100, then specify the Server URL as the following:

http://192.168.1.100:9108

STEP 10

Click **Save**. The software will now create the database and continue setup. This could take several minutes.

STEP 11

When IXM WEB is finished installing, you should be prompted with the following screen:

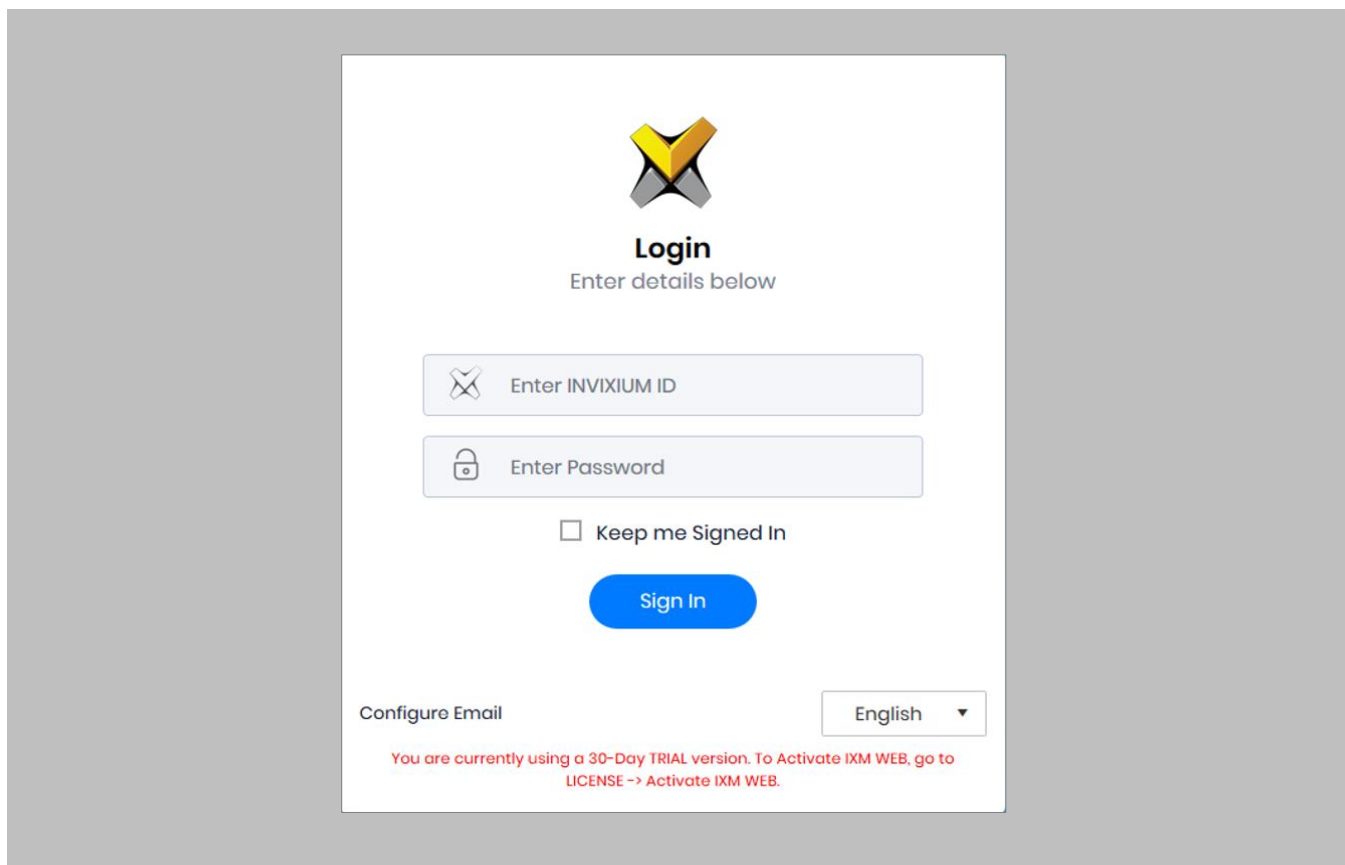



Figure 14: IXM WEB Login Page



 Note: During an upgrade of IXM WEB from any previous release to 2.3.0.0, an internet connection is required for license validation. As this new version includes a face algorithm update, it will automatically convert templates without the need for re-enrollment of faces.

8. Configuring Email Settings using IXM WEB

Configuring Email settings is highly recommended as one of the first steps after installing IXM WEB. Email configuration settings will help the admin retrieve the password for IXM WEB in case it is forgotten. In addition, having email settings configured also 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](#).

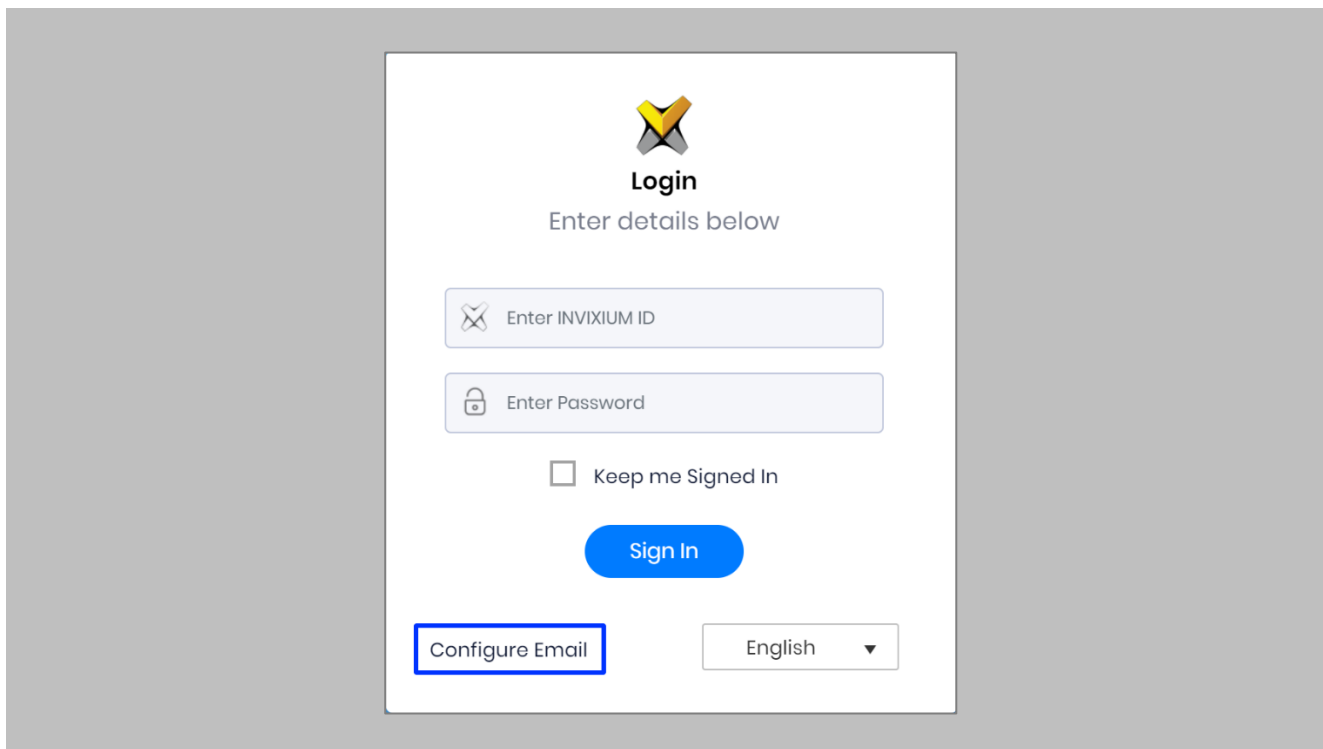


Figure 15: Configure Email

STEP 2

Select “Enable Email Configuration” and enter values for the “SMTP Host”, “SMTP Port”, and “Send email message from” fields.

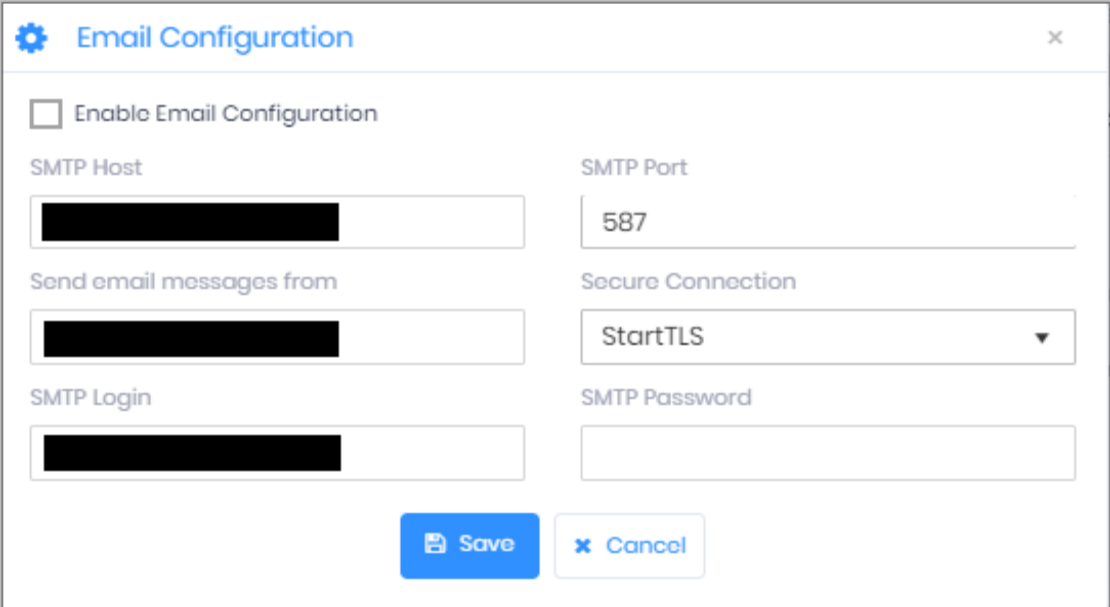



Figure 16: IXM WEB - SMTP Settings

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

STEP 3

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

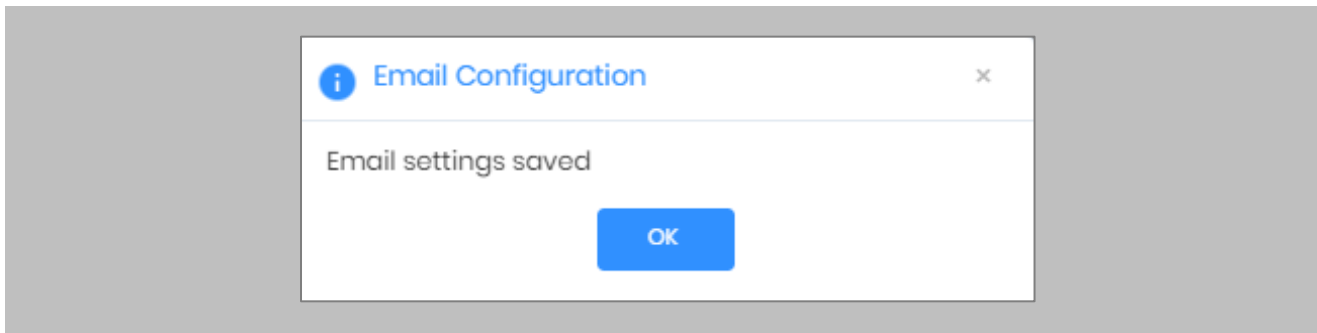


Figure 17: IXM WEB - Save Email Settings

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

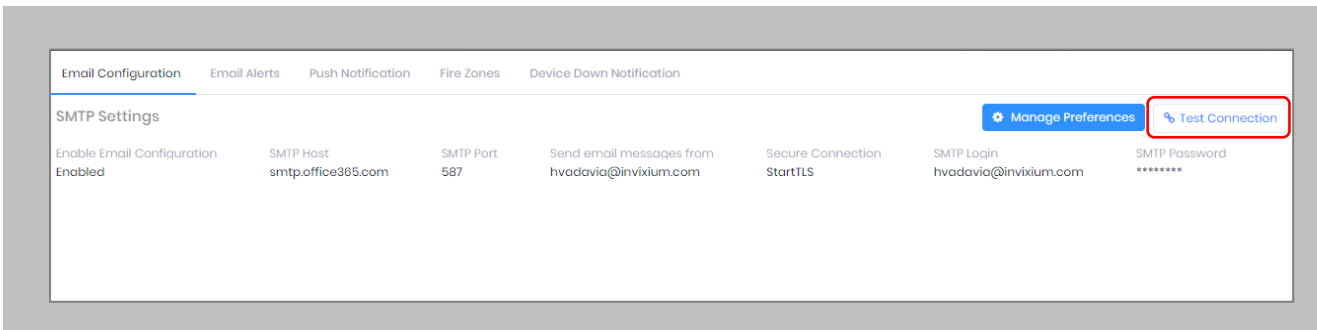


Figure 18: IXM WEB - Test Connection

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

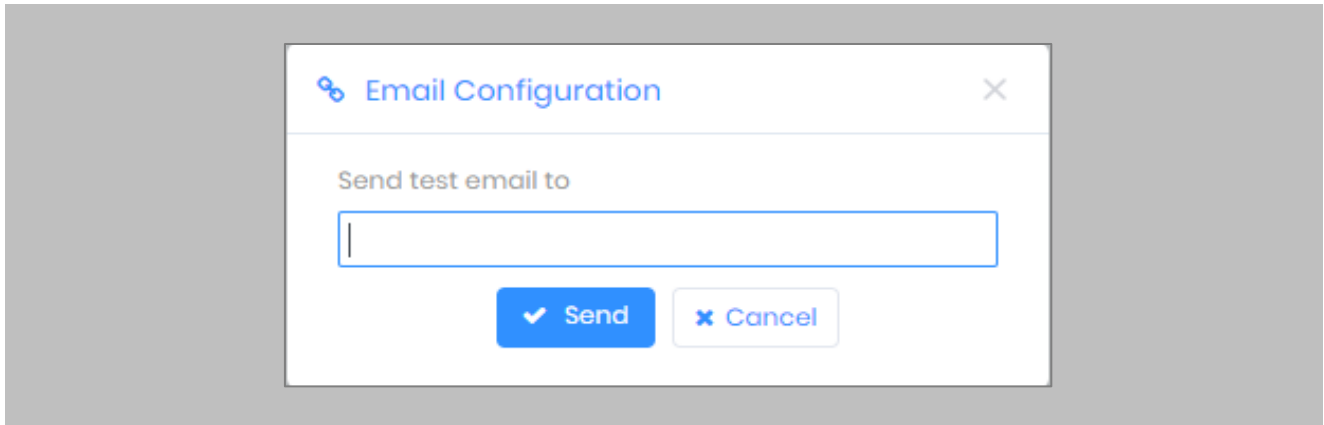
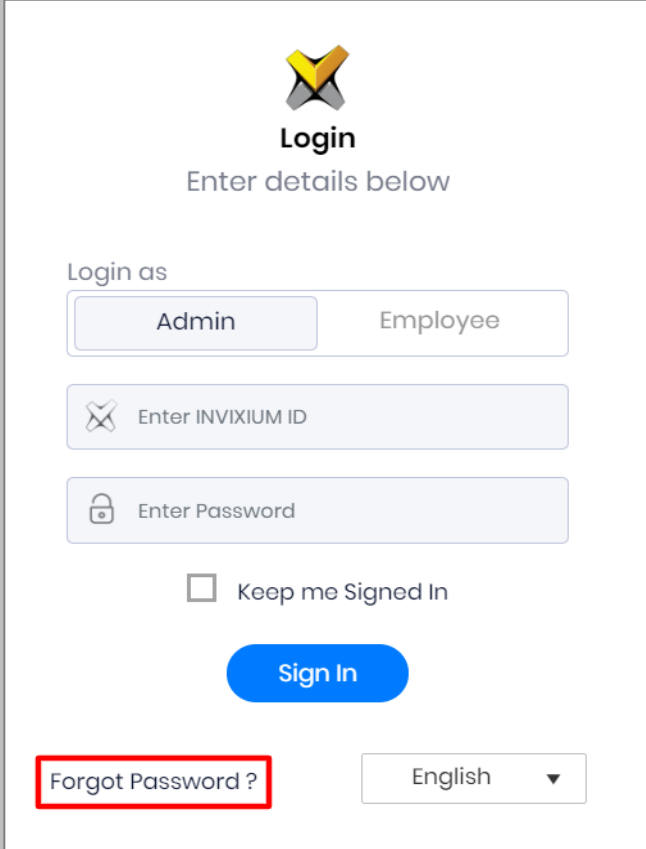


Figure 19: IXM WEB - Enter Email ID

STEP 4

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



The screenshot shows the login interface for the INVIXIUM system. At the top center is the INVIXIUM logo, a stylized 'X' with a yellow and grey gradient. Below the logo, the word "Login" is displayed in bold, followed by the instruction "Enter details below". The login form consists of several elements: a "Login as" section with two buttons labeled "Admin" and "Employee"; a text input field with a key icon and the placeholder text "Enter INVIXIUM ID"; another text input field with a lock icon and the placeholder text "Enter Password"; a checkbox labeled "Keep me Signed In"; a prominent blue "Sign In" button; and at the bottom, a "Forgot Password?" link which is highlighted with a red rectangular border, and a language dropdown menu currently set to "English".

Figure 20: IXM WEB - Forgot Password

9. Software and Module Activation

IXM WEB Activation

Procedure

STEP 1

Log into IXM WEB.

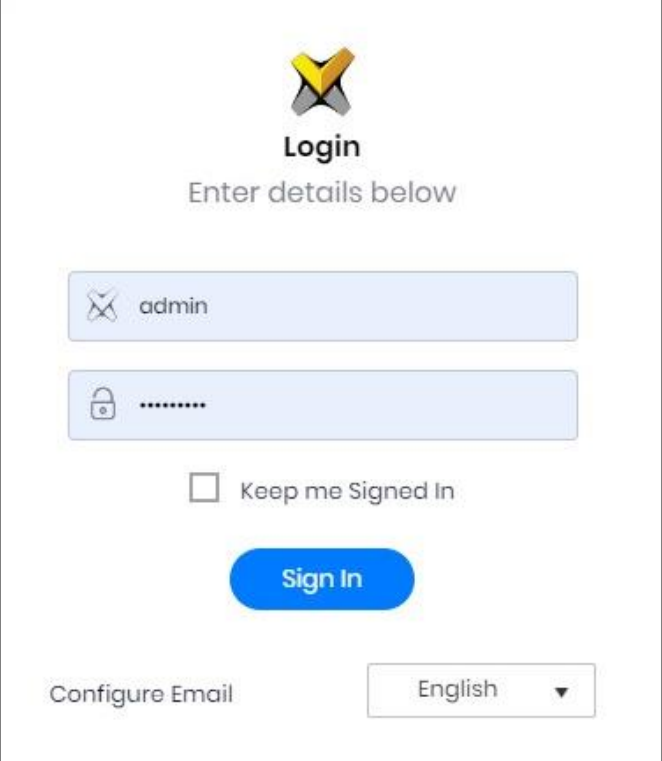


Figure 21: IXM WEB - Enter Login Credentials

STEP 2

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

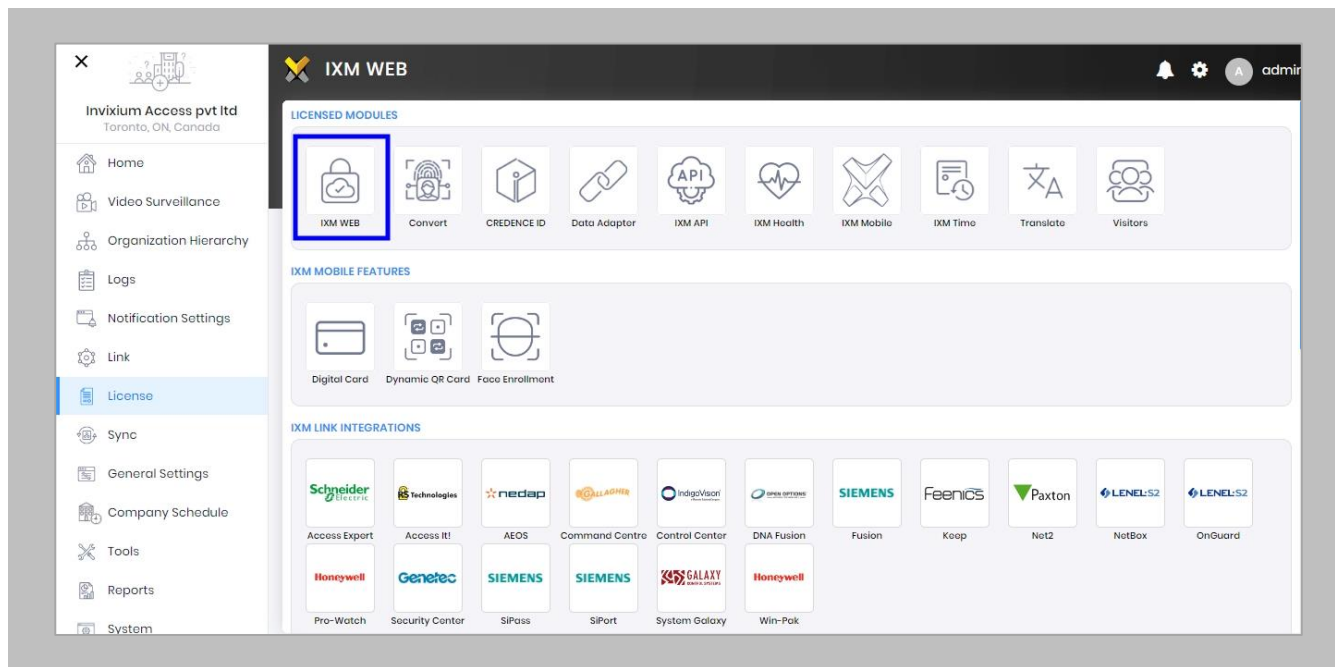



Figure 22: IXM WEB - License Setup

STEP 3

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

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

STEP 4

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

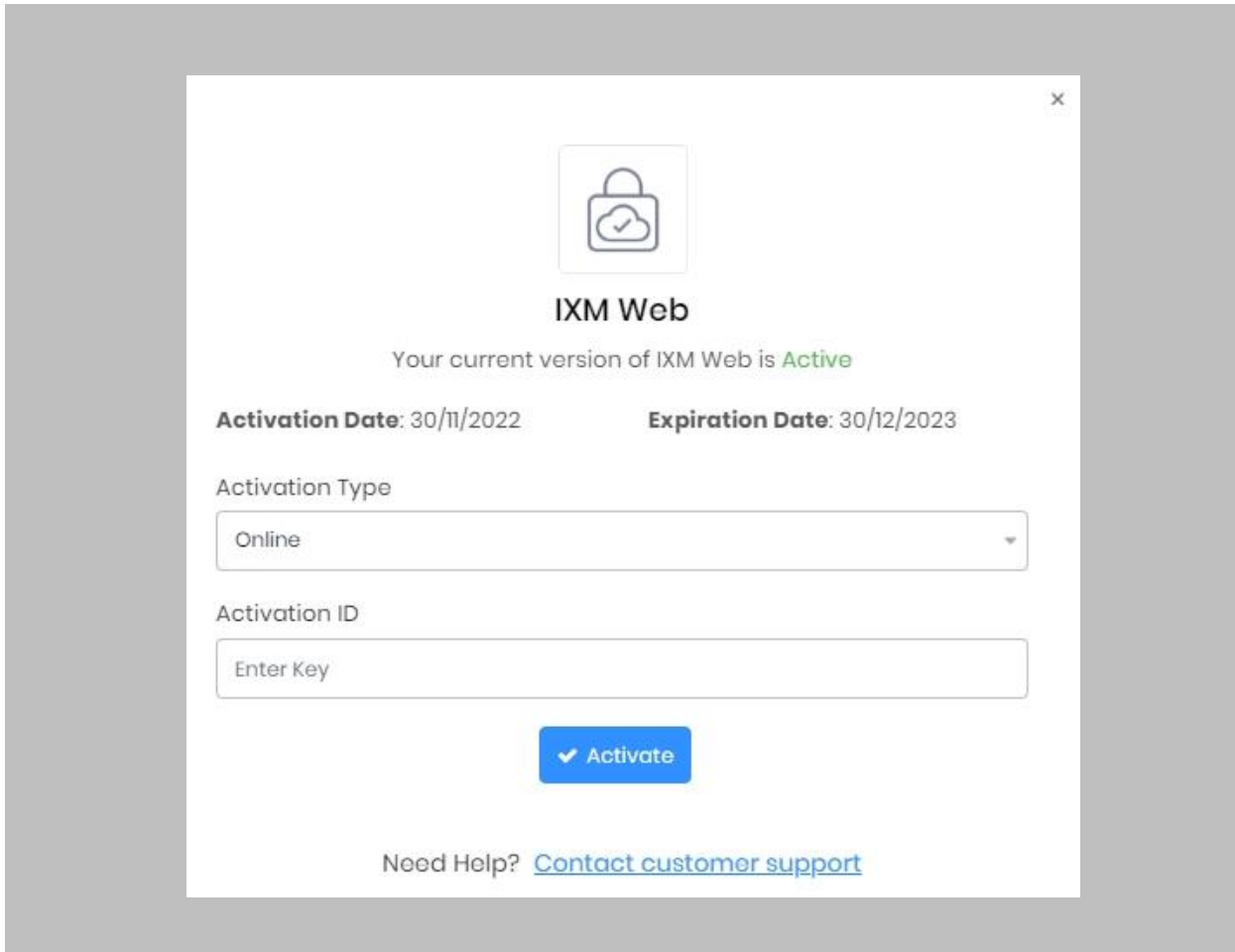


Figure 23: IXM WEB - Online Activation

SiPort Module Activation

The option to activate a SIEMENS SiPort 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 **SiPort (SIEMENS)**.

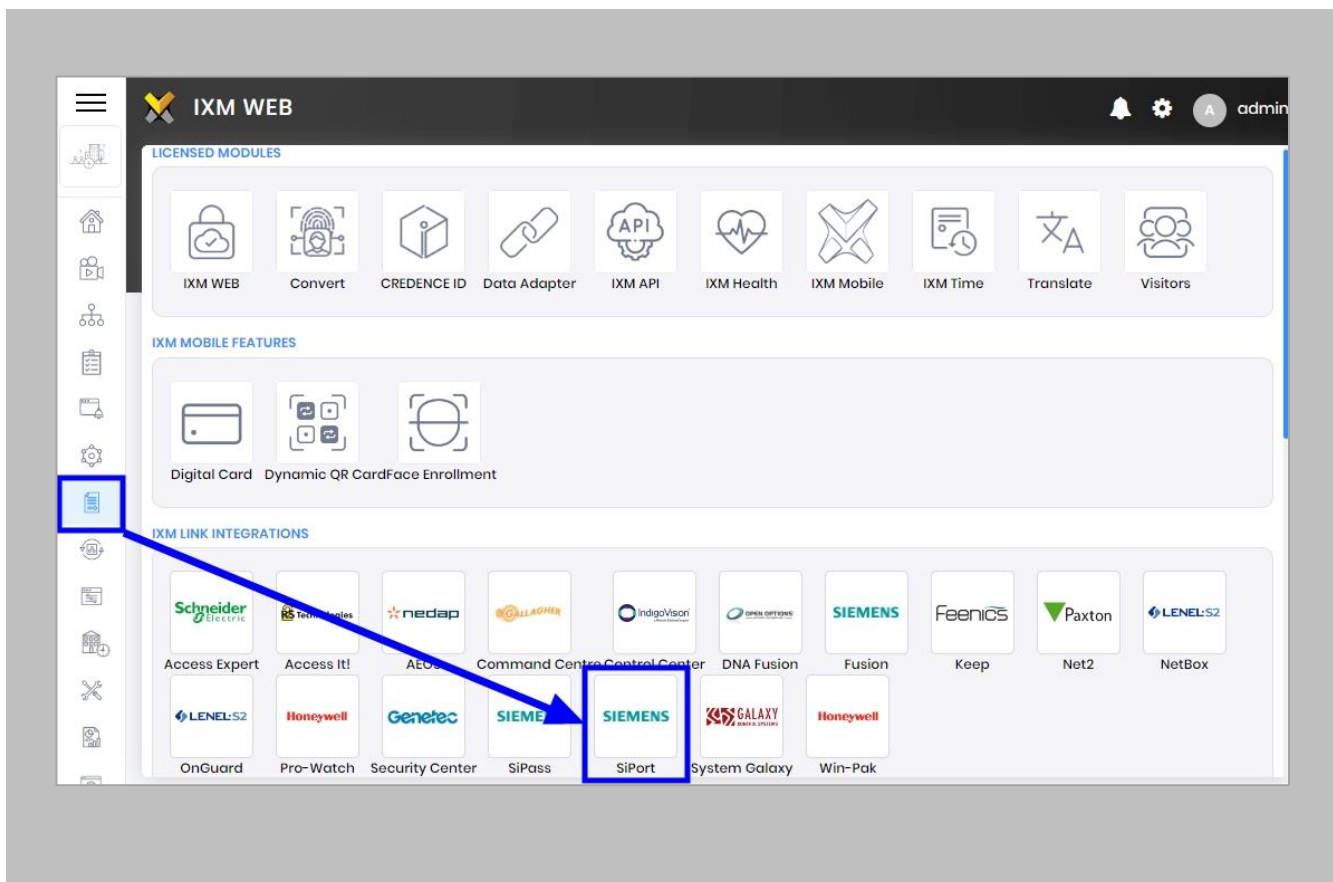


Figure 24: IXM WEB - SIEMENS Link Activation

STEP 3

You will receive an email from Invixium Support containing a license key for the SIEMENS SiPort Activation.

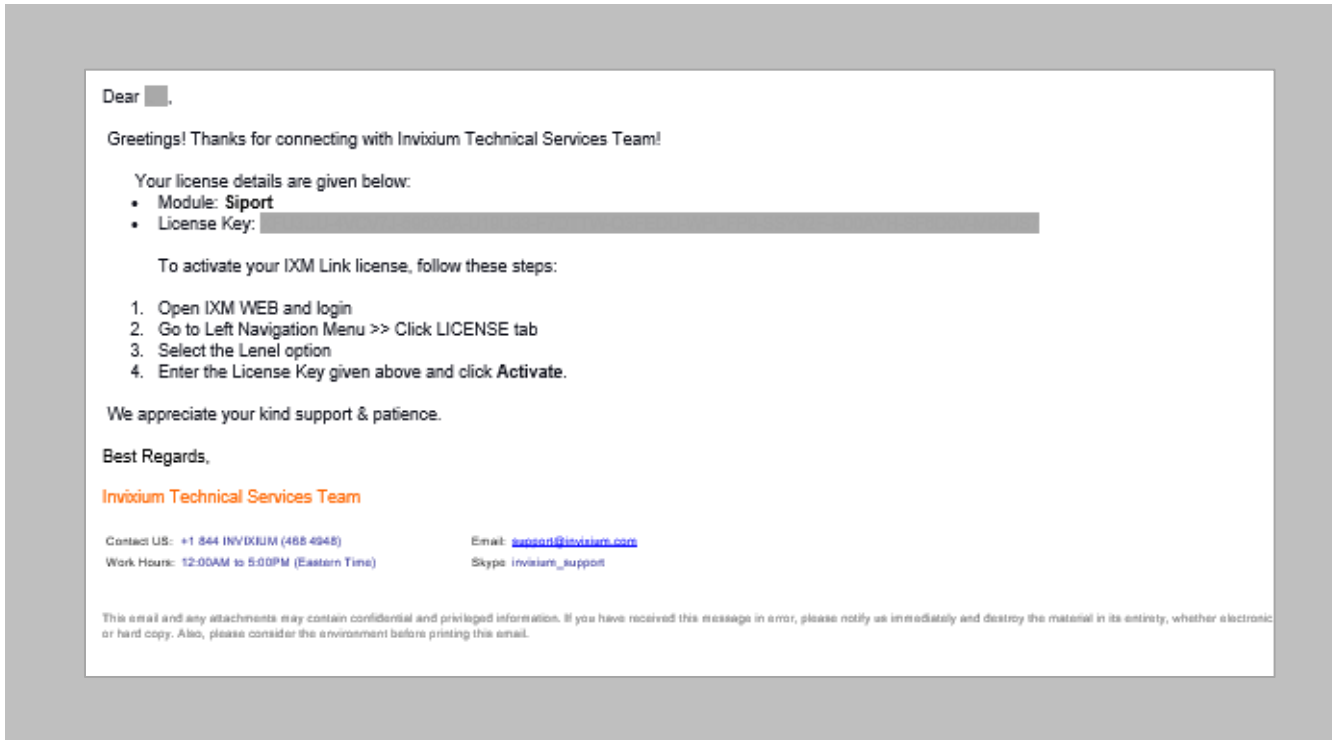


Figure 25: SIEMENS License Key Email

STEP 4

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

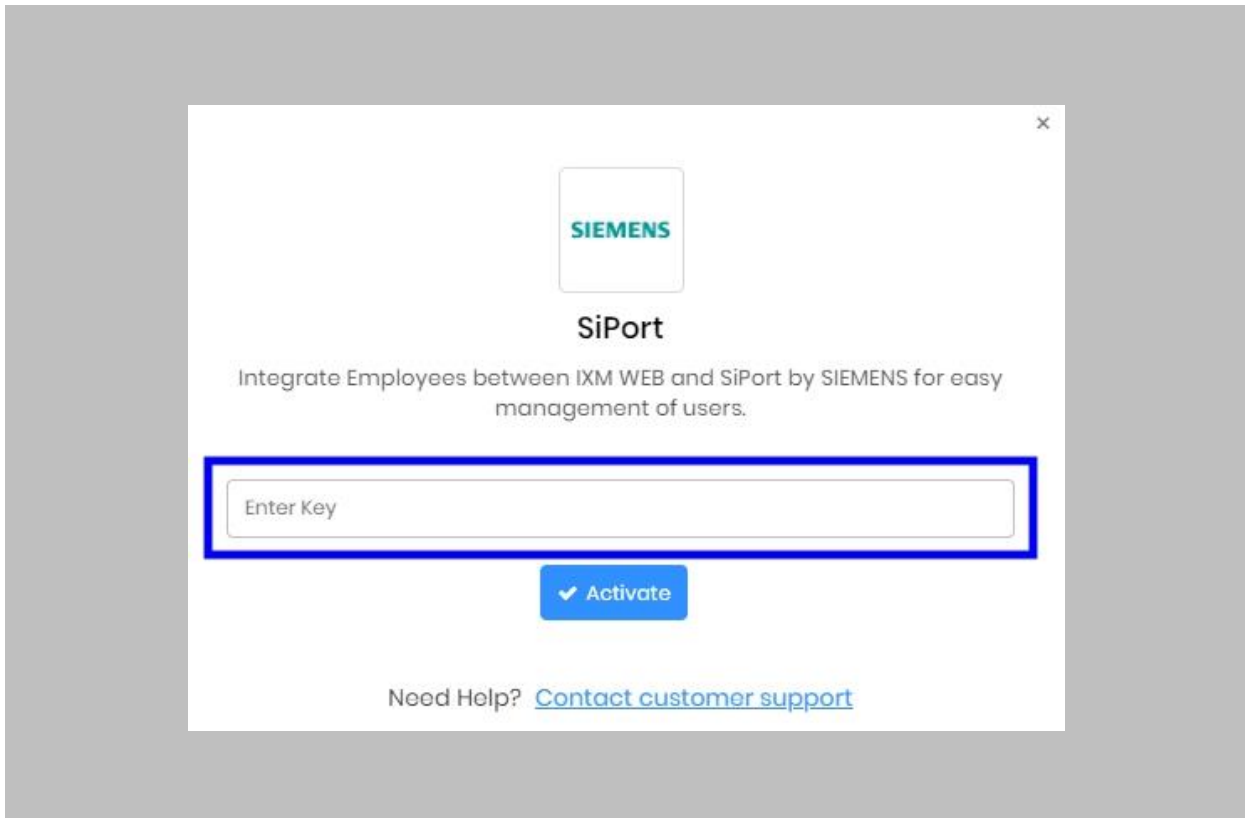


Figure 26: IXM WEB - Activate SIEMENS Link License

RESULT

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

10. Configuring IXM Link for SIEMENS

Procedure

STEP 1

From the **Left Navigation Pane** → **Link** → click the orange **SiPort (SIEMENS)** icon.

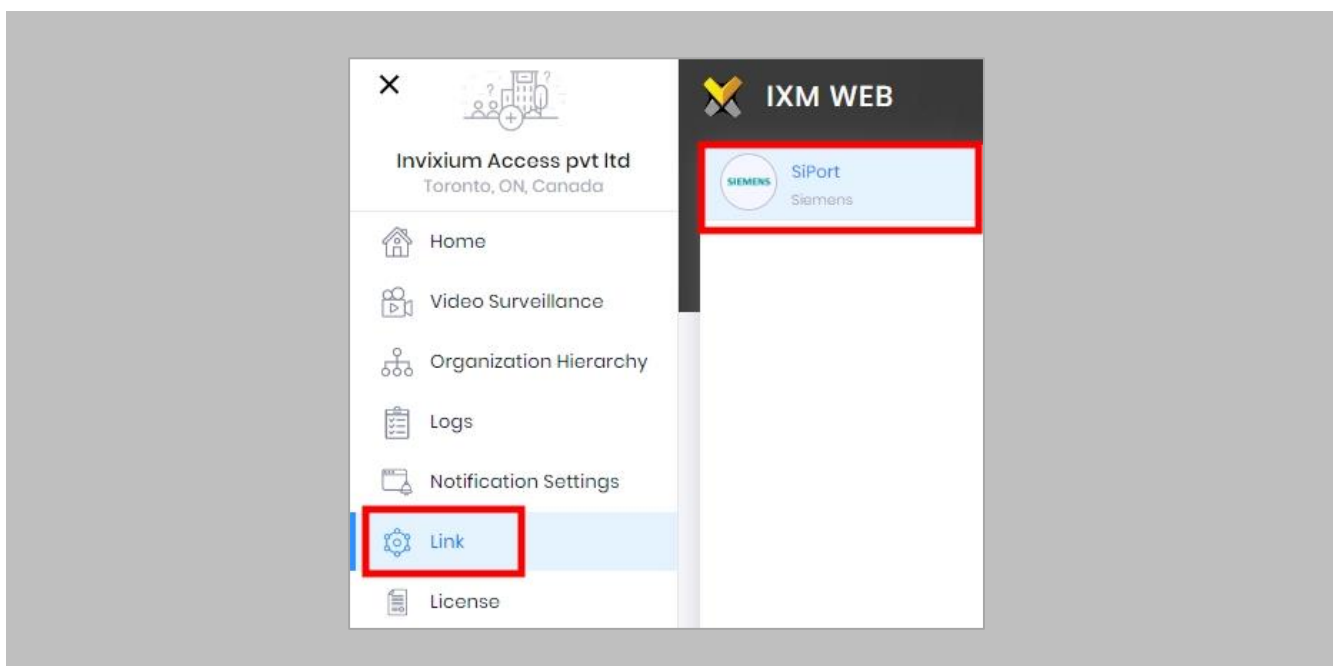
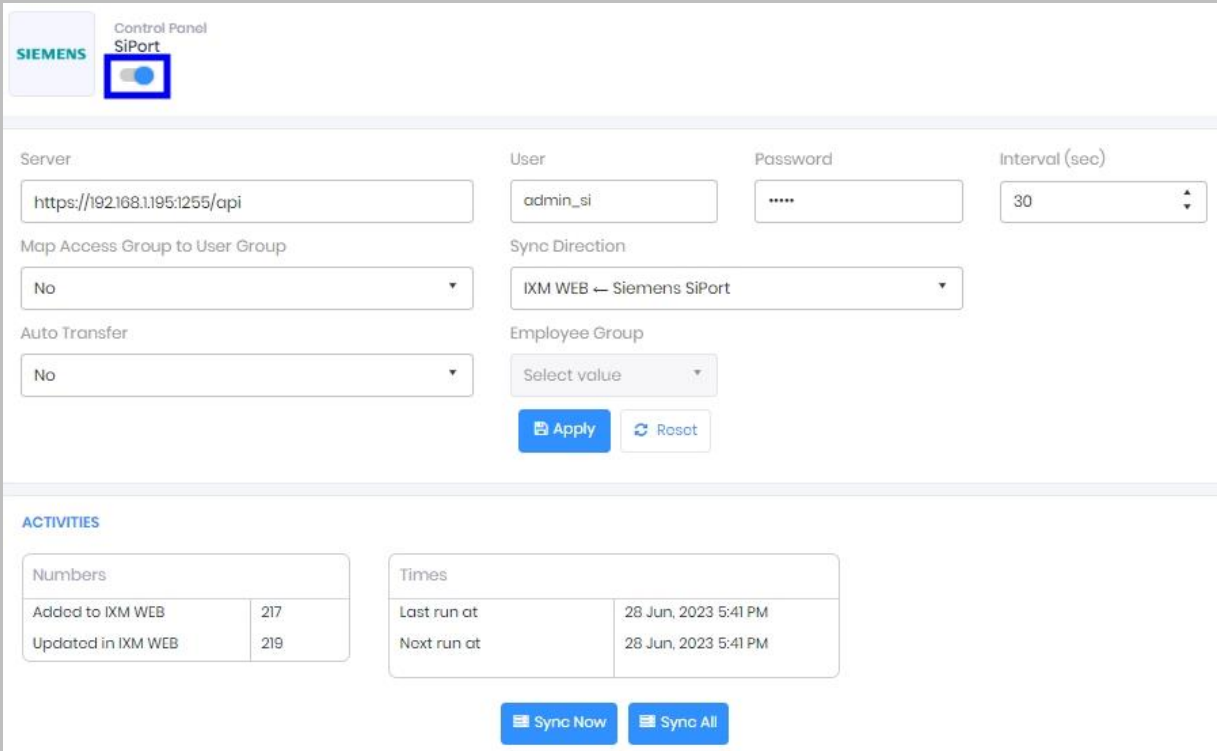


Figure 27: IXM WEB - Link Menu

STEP 2

Toggle the **Status** switch to enable.



Control Panel
SIEMENS SiPort

Server: User: Password: Interval (sec):

Map Access Group to User Group: Sync Direction:

Auto Transfer: Employee Group:

ACTIVITIES

Numbers	
Added to IXM WEB	217
Updated in IXM WEB	219

Times	
Last run at	28 Jun, 2023 5:41 PM
Next run at	28 Jun, 2023 5:41 PM

Figure 28: IXM WEB - Enable SIEMENS Link Module

Server:

Enter the **Server URL**. For example: <http://{{SIPORT-Server IP or hostname}}:{{port}}/API/>

User:

Enter the name of the authorized user to connect to the API of SIEMENS SiPort.

Password:

Enter the Password of the authorized user to connect to the API of SIEMENS SiPort.

Interval (Sec):

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

Map Access Group to User Group:

Select “Yes” or “No” from the dropdown list.

Yes: IXM WEB User Group, Device Group, and Sync Group will be created automatically with one-one mapping of User Group and Device Group.

As per the SIEMENS Access Profile selected by the cardholder, that cardholder will be assigned to the IXM WEB User Group. It will be assigned to the Invixium devices mapped with that particular User Group.

No: Cardholders won't be assigned to any IXM WEB user group.

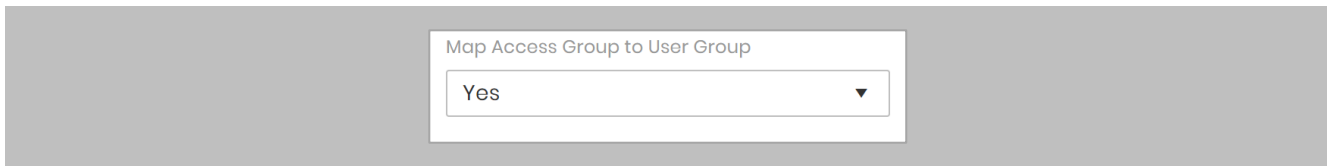


Figure 29: IXM WEB - Map Access Group to User Group

Sync Direction:

Click on the field to select the direction of data transfer. Data can be transferred one way only.

Select one-way sync direction IXM WEB ← SIEMENS SiPort to import cardholders from SIEMENS to IXM WEB. SIEMENS SiPort is considered as the master data in this case and any changes made in IXM WEB data will be overwritten during transfer.

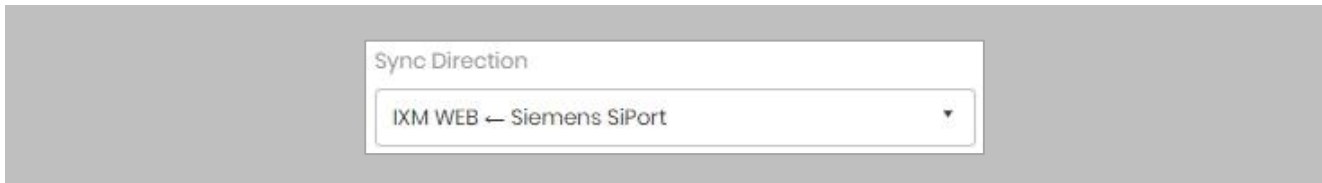


Figure 30: IXM WEB - Sync Direction

Auto Transfer:

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

Click on either 'Yes' or 'No'.

Yes: Selection of User Group is mandatory to use Auto Transfer. Users will be transferred to IXM Devices based on Sync Group configuration for selected Employee Group.

No: Users will not be transferred to the IXM Devices.

Employee Group:

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

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

Click **Apply**. The transfer of data between SIEMENS SiPort and IXM WEB is possible only after a successful connection.

In case of an unsuccessful connection, please refer to the *Troubleshooting* section.

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

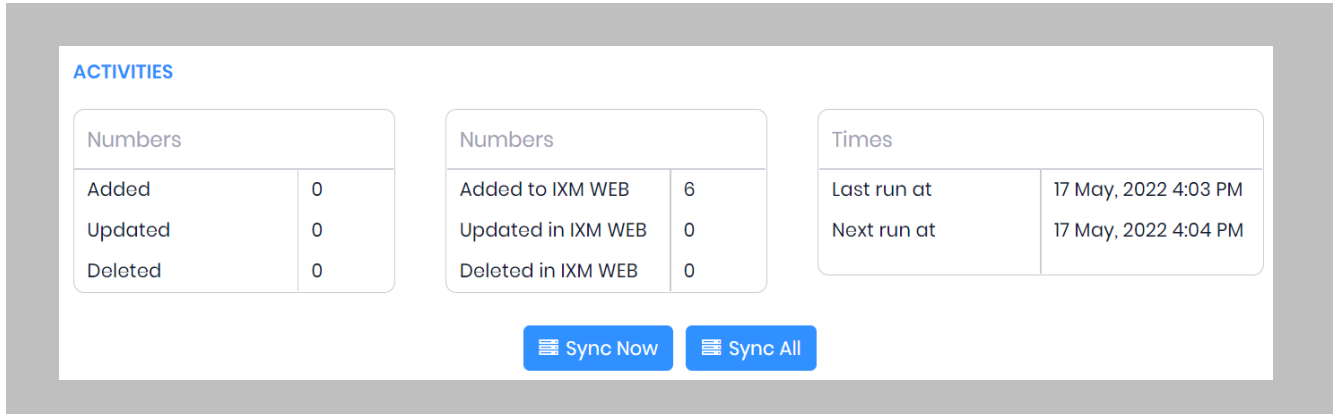


Figure 31: IXM WEB - Sync Activities

Numbers

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

Times

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

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

STEP 3

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

STEP 4

If the sync direction is selected as SIEMENS to IXM WEB (One-way sync), then the **Sync All** button will be visible.

STEP 5

The **Sync All** feature allows a resynchronization of the database from SSP to IXM WEB. This will re-import missing cardholders or updated cardholders from SSP to IXM WEB.

No action will be taken on Employees that have been deleted in SiPort.

RESULT

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

11. Add and Configure Invixium Readers

Adding an Invixium Reader in IXM WEB

Procedure

STEP 1

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

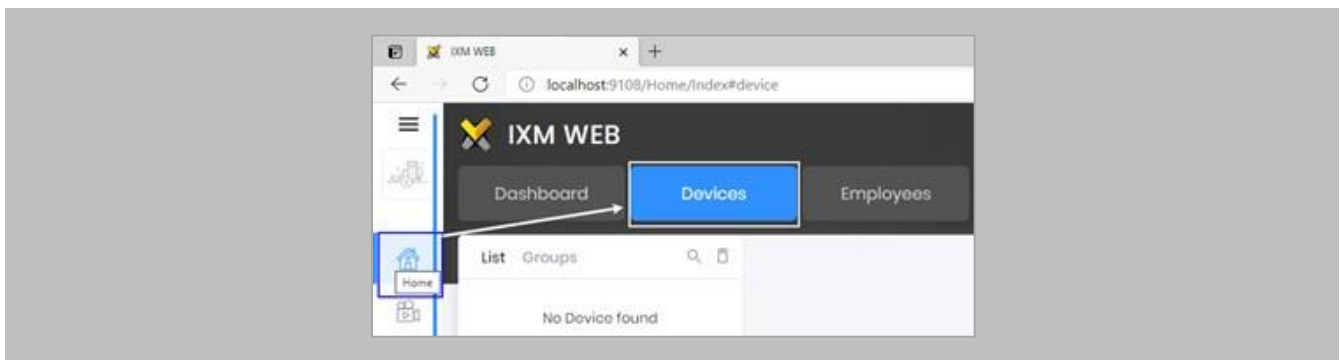


Figure 32: IXM WEB - Devices Tab

STEP 2

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

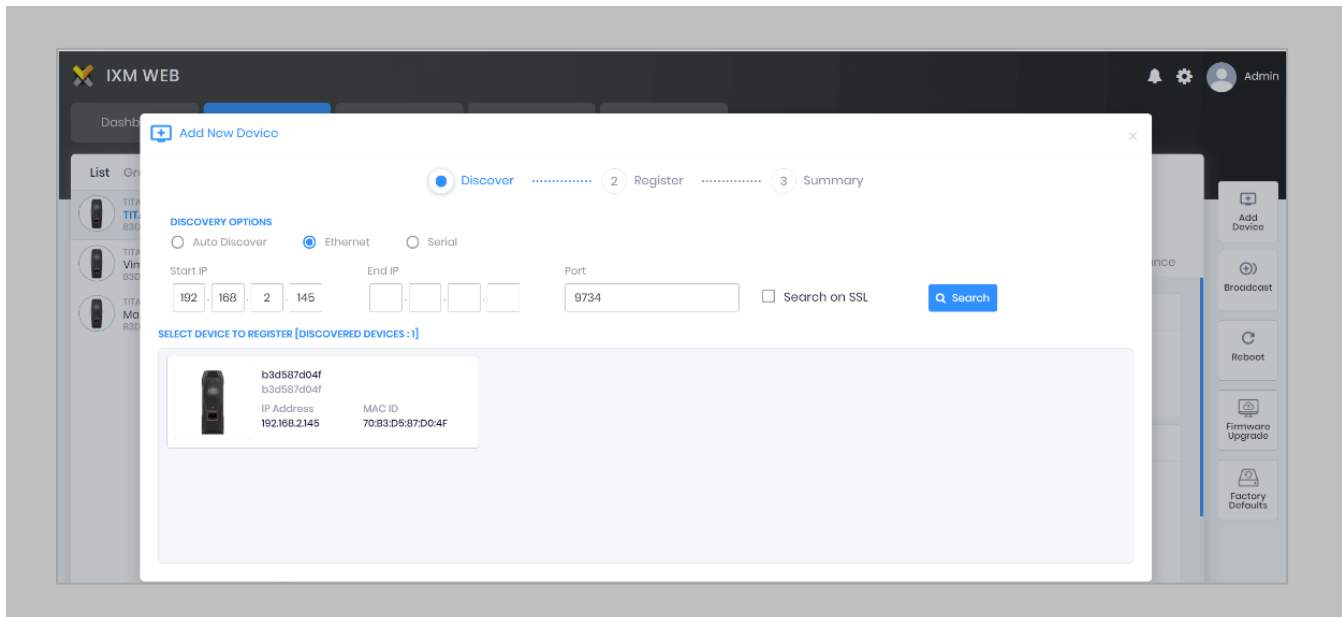
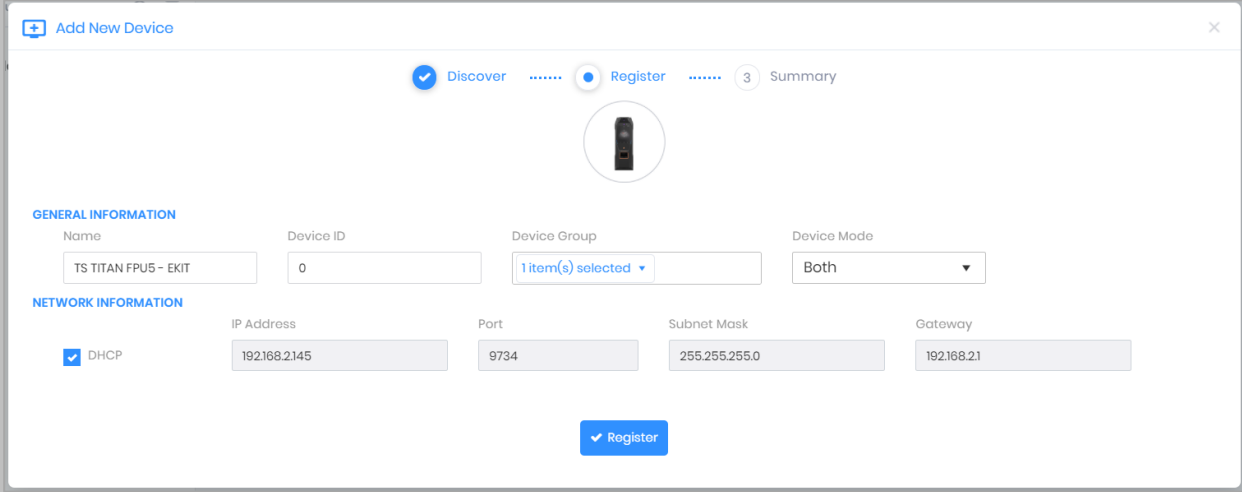


Figure 33: IXM WEB - Search Device Using IP Address

STEP 3

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



The screenshot shows the 'Add New Device' window with the 'Register' step selected. The 'GENERAL INFORMATION' section contains the following fields: Name (TS TITAN FPU5 - EKIT), Device ID (0), Device Group (1 item(s) selected), and Device Mode (Both). The 'NETWORK INFORMATION' section includes a checked DHCP checkbox, IP Address (192.168.2145), Port (9734), Subnet Mask (255.255.255.0), and Gateway (192.168.21). A 'Register' button is located at the bottom center.

Figure 34: IXM WEB - Register Device

STEP 4

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

Device Mode: Select accordingly.

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

STEP 5

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

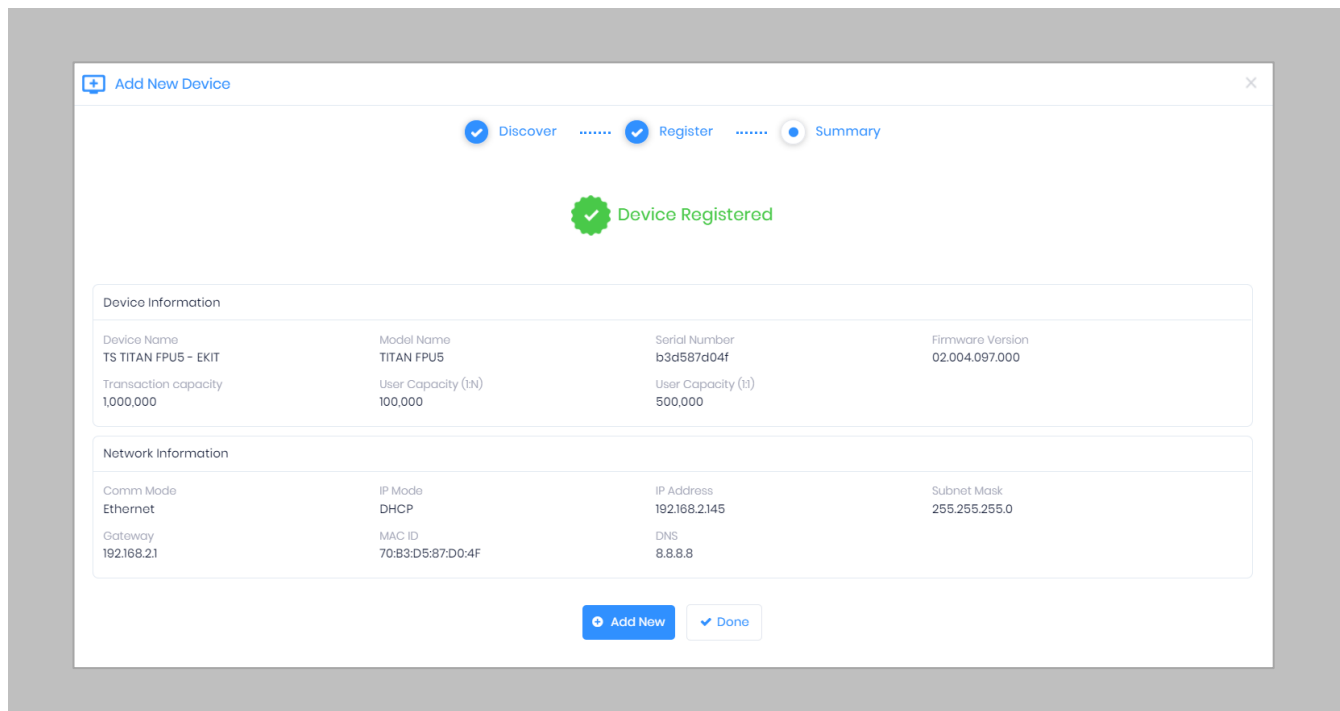


Figure 35: IXM WEB - Device Registration Complete

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

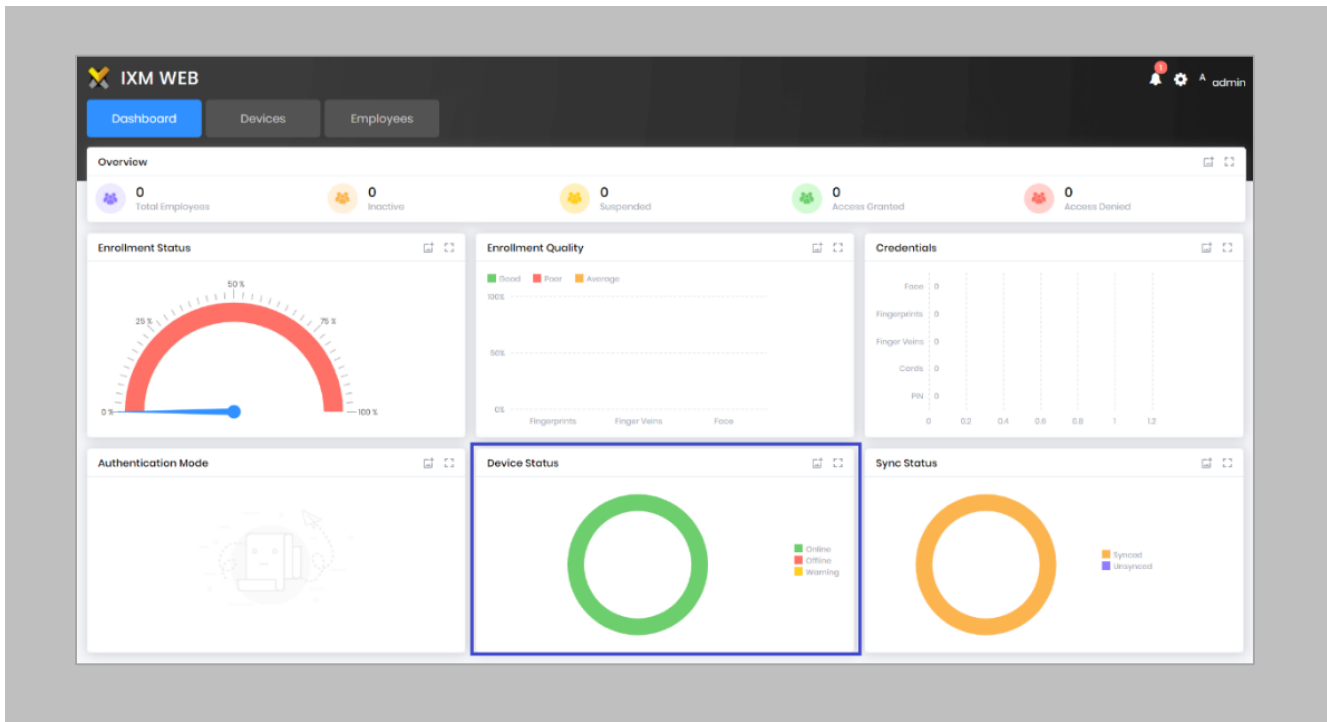


Figure 36: IXM WEB - Dashboard, Device Status

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**.

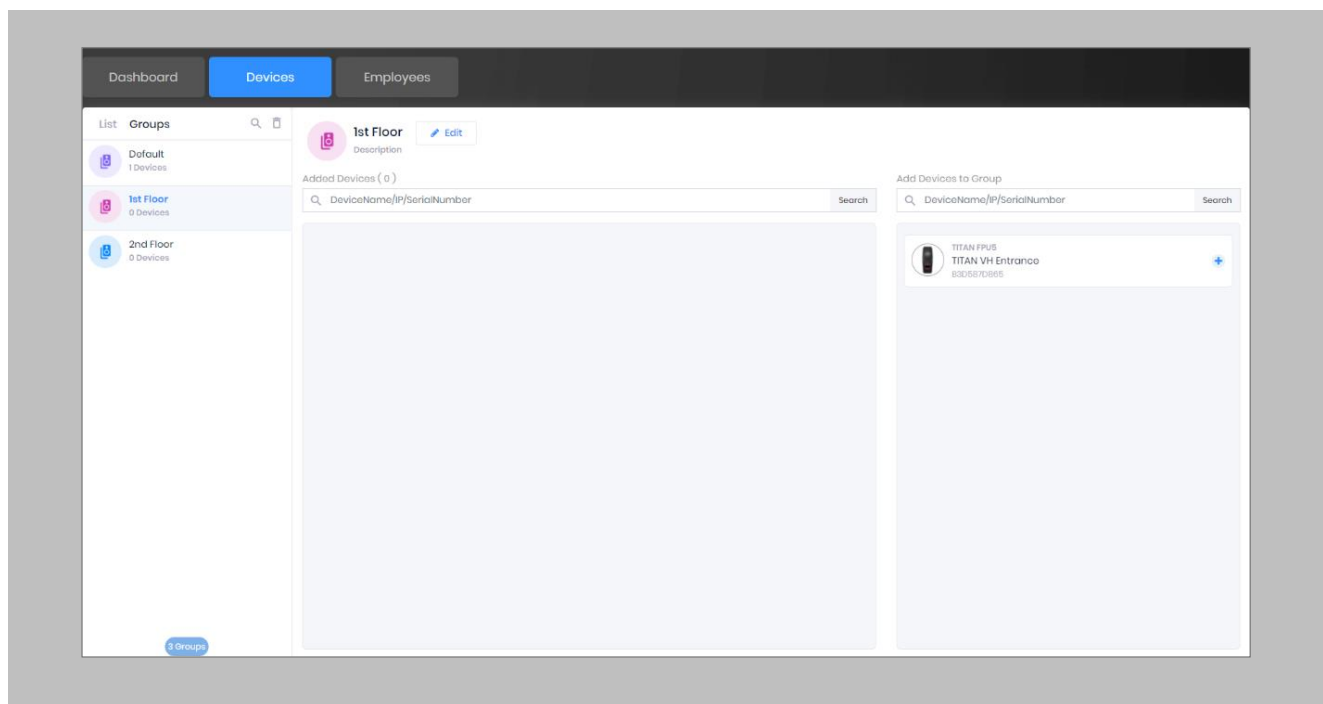



Figure 37: IXM WEB - Assign Device Group

Configuring Wiegand Format to Assign Invixium Readers

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

STEP 1

From Home >> Expand the Left Navigation Pane >> Navigate to the **General Settings** tab >> Click the **Wiegand** tab to open the Wiegand Format settings.

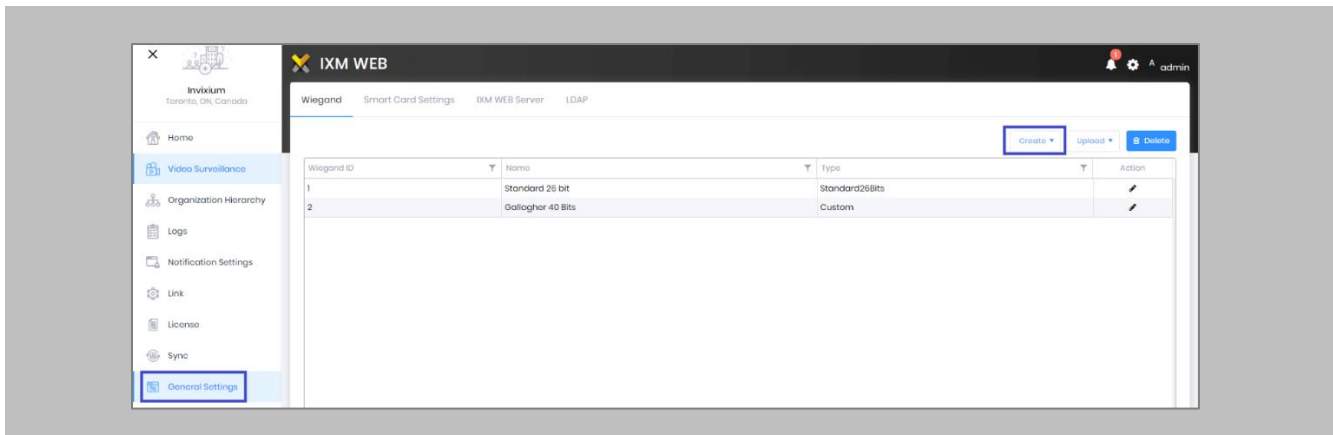


Figure 38: IXM WEB - Create Wiegand Format

STEP 2

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

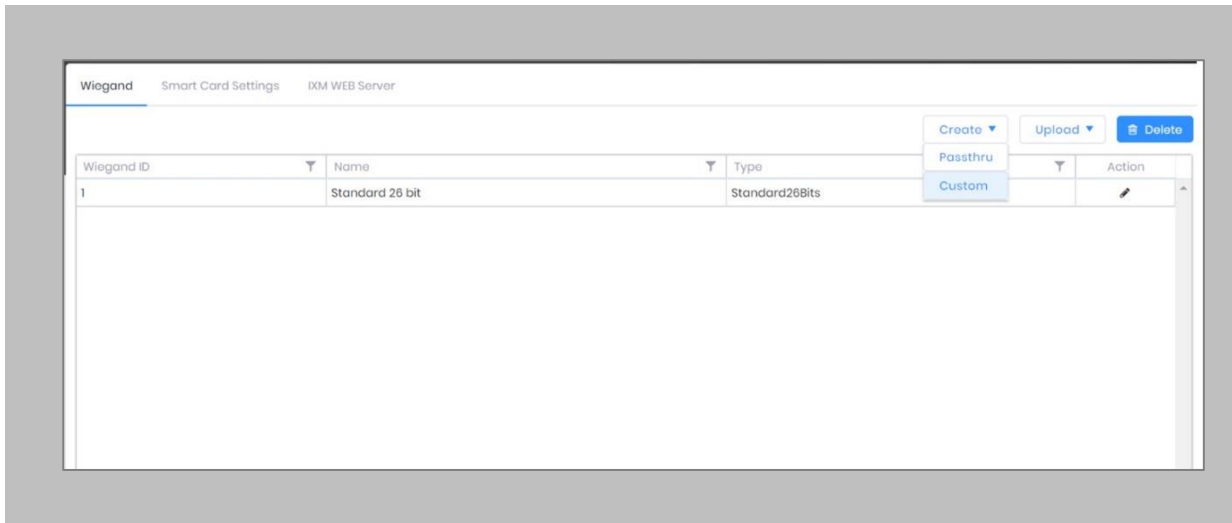


Figure 39: IXM WEB - Create Custom Wiegand Format

STEP 3

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

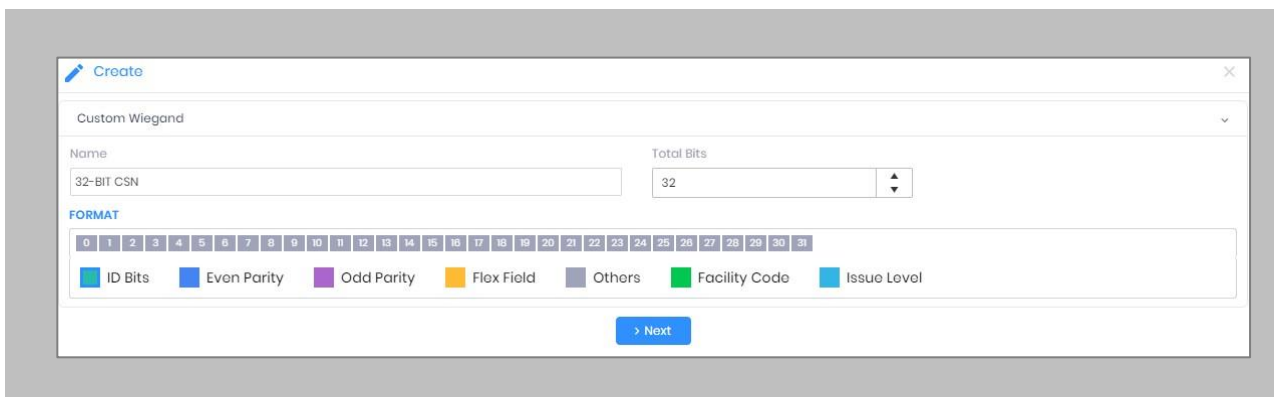


Figure 40: IXM WEB – Create Wiegand Format

STEP 4

Click **Next** and **Save**.

STEP 5

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

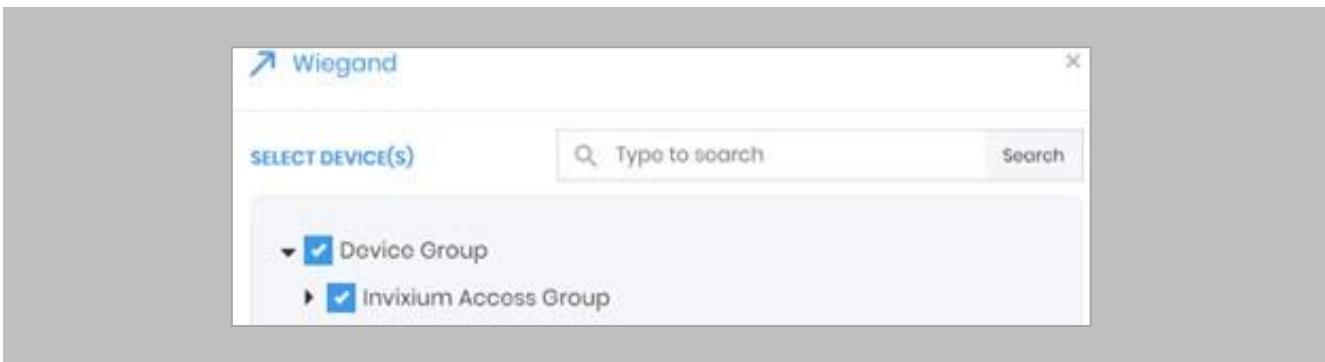



Figure 41: IXM WEB - Upload Wiegand Format

Assign Wiegand to Invixium Readers

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

The created Wiegand will be used to define which output format will be sent to SSP.

STEP 1

From [Home](#) > click the [Devices](#) tab. Select any device.

STEP 2

Navigate to the [Access Control](#) tab.

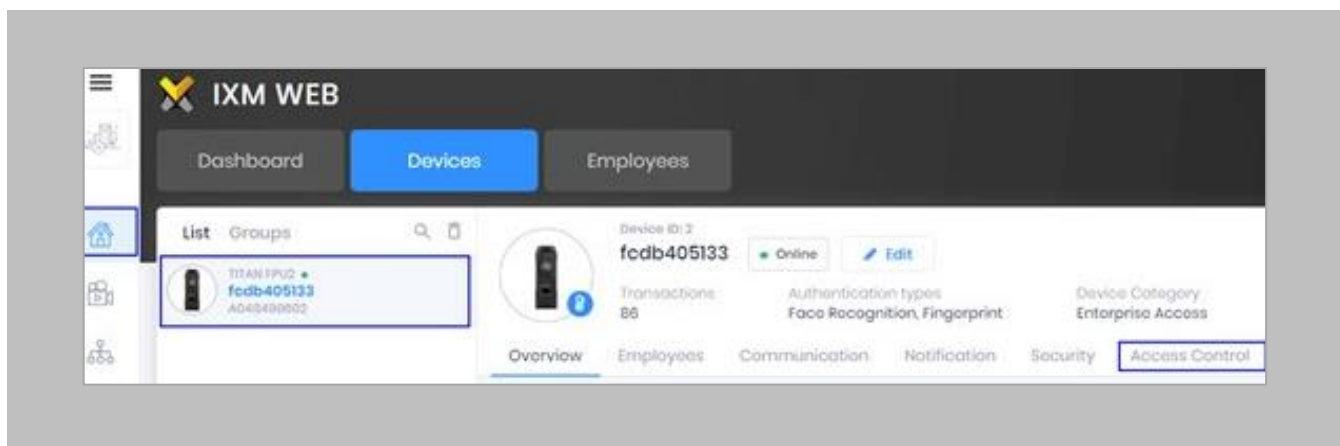


Figure 42: IXM WEB - Navigate to Access Control Tab

STEP 3

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

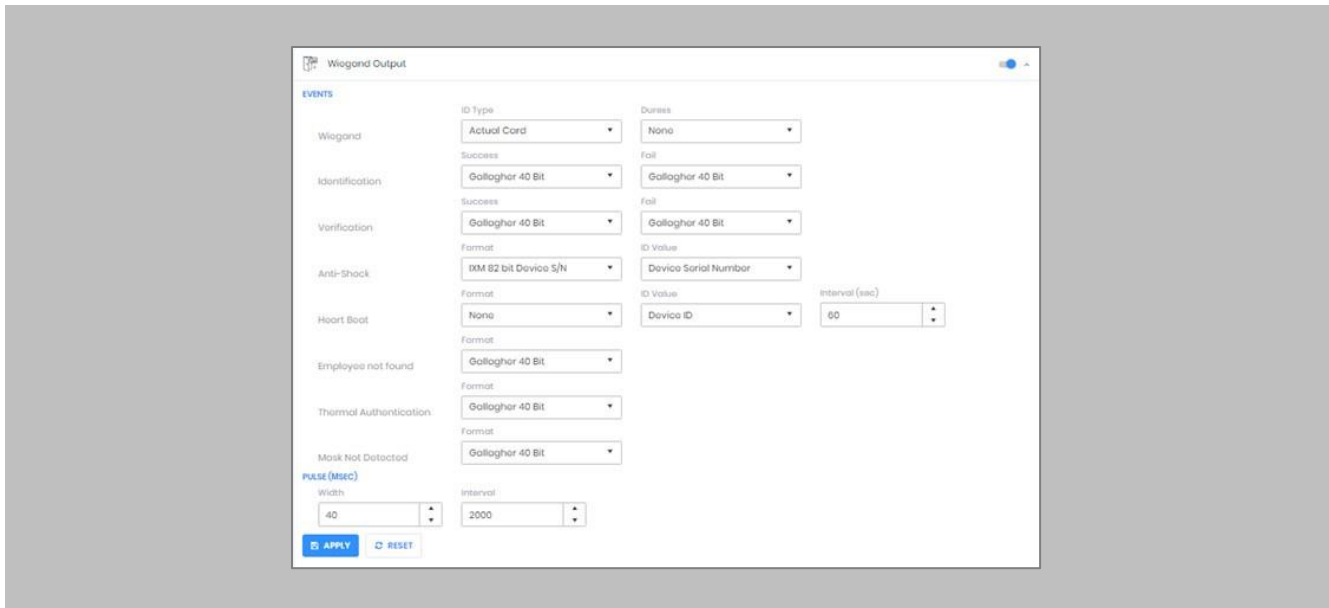


Figure 43: IXM WEB - Wiegand Output

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 SSP, select either Default Card or Actual Card.

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

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

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

STEP 4

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

STEP 5

Click **Apply**.

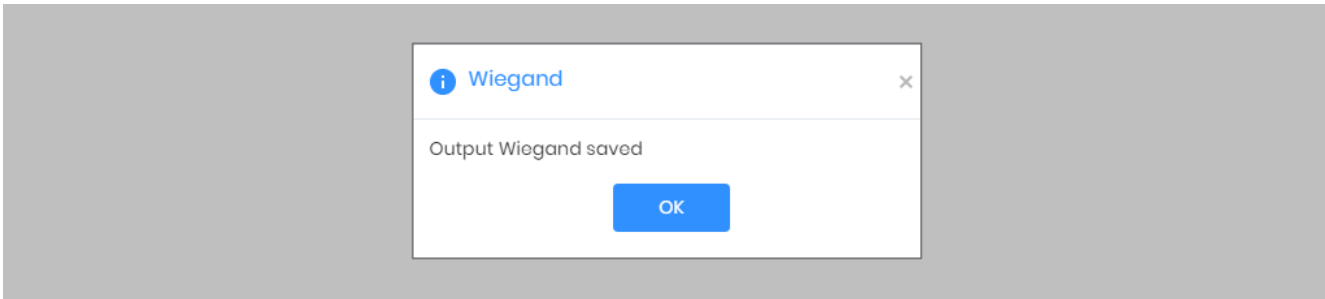


Figure 44: IXM WEB - Save Output Wiegand

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 C for more information.
- If the cardholder was assigned multiple cards, the first assigned card will be the 'default' selected card. The details of the card will be sent as the Wiegand bits input to SIEMENS Controller.
- To make this Wiegand output work on SIEMENS, you will need to create a UCF (Universal Card Format) for use on the controllers talking to the Invixium reader (by Wiegand or OSDP).

Configuring Thermal Settings



Note: confirm your device is capable of temperature screening first.

Procedure

STEP 1

Click the **Devices** tab → Select **Device** → Select **Thermal Settings** → **Thermal Authentication Settings** to view default settings.

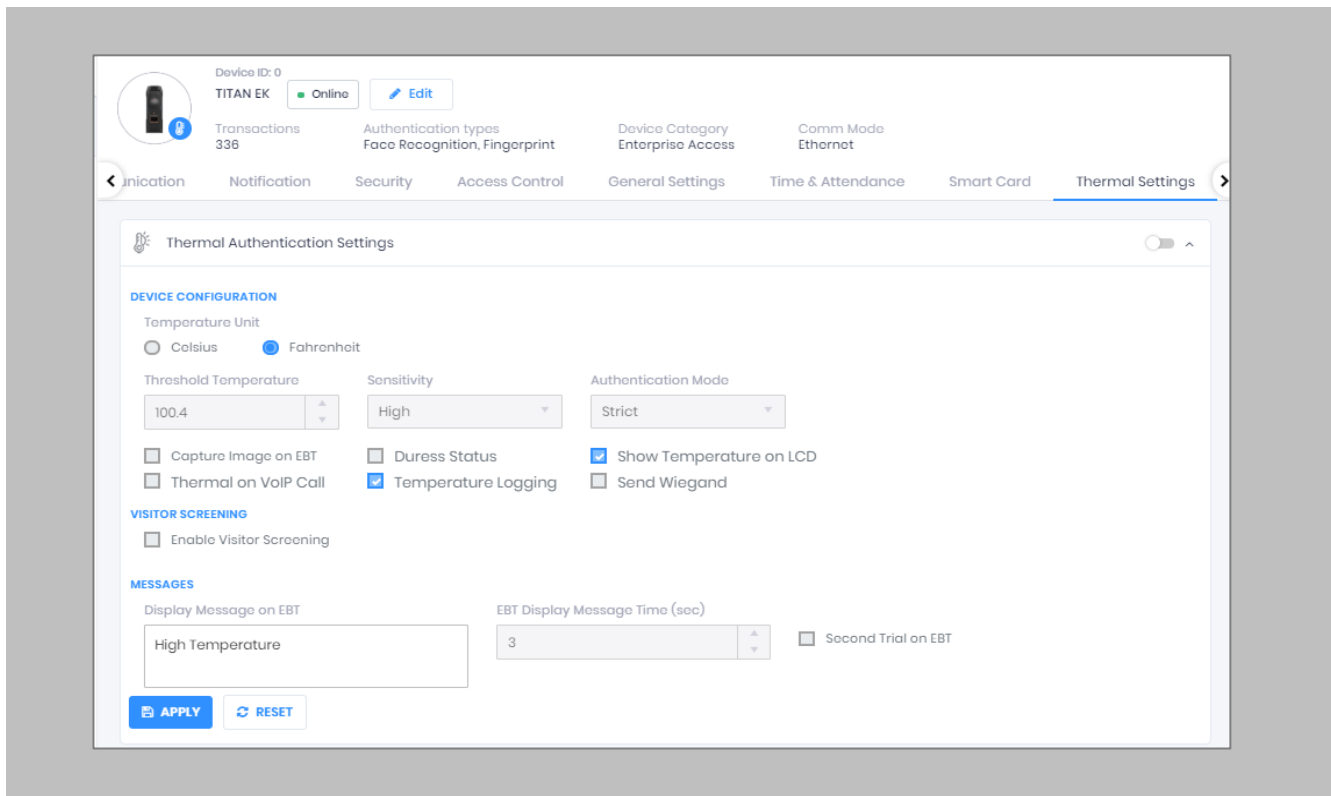


Figure 45: IXM WEB - Thermal Settings

STEP 2

The list of settings along with their functions are:

- **Temperature Unit:** IXM WEB supports Celsius and Fahrenheit temperature units. By default, the selected option will be Fahrenheit.
- **Threshold Temperature:** Users can set a threshold temperature. Elevated Body Temperature (EBT) workflows will trigger when any user whose temperature is above the threshold value. The default threshold temperature is 100.4 degrees Fahrenheit.
- **Sensitivity:** Users can set Thermal Sensitivity to low or high.
- **Authentication Mode:** The user will have two options for the Mode of authentication Soft / Strict, this mode of authentication is used to control the access of the user if fever is detected. The default mode of authentication is Strict.
 - **Soft:** Access will be granted to the End-user even after the fever is detected.
 - **Strict:** Access will be denied if the fever is detected.
- **Send Wiegand:** This setting will be visible only if the user selects the “Strict” Authentication Mode. Enabling this setting will generate Wiegand whenever “High Face Temperature” is detected in the authentication process.
- **Capture Image on EBT:** Enable this setting to capture the image of the user if EBT is detected. By default, this setting will remain disabled. The same image will be used for sending email notifications from IXM WEB.
- **Duress Status:** Enabling this setting will allow access to the user even after detecting EBT if the user authenticates using their pre-programmed duress finger. The default setting is disabled.
- **Show Temperature on LCD:** By enabling this setting, TITAN will display the screened temperature upon authentication. By default, this setting is disabled.



-
- **Display Message on EBT:** Users can set a message to display after detecting EBT. Users can set a message up to a maximum of 50 characters.
 - **EBT Display Message Time (sec):** Users can configure the length of time that the EBT message stays on the screen. The default time is 3 seconds.
 - **Second Trial on EBT:** By enabling this setting, users will get a notification to retry after EBT detection. If this setting is enabled, Display Message for Second Trial, Second Trial Wait Time after EBT (mins), and Display Message Time After Second Trial (sec) fields will be visible.
 - **Display Message for Second Trial:** Users can set a message to display after the second trial if EBT is detected. This message can be a maximum of 50 characters.
 - **Second Trial Display Message Time (sec):** Users can configure the length of time that the second trial message stays on the screen. The default time is 3 seconds.
 - **Enable Visitor Screening:** Enable this setting to start screening temperatures for visitors. By default, this field remains disabled.
 - **Visitor Screening Message:** Users can set a message that will be displayed when a visitor is showing their face. Maximum 50 characters allowed.
 - **Visitor Screening Message on EBT:** Users can set a message that will be displayed when the visitor has an EBT. Maximum 50 characters allowed.
 - **Visitor Message Display Time (sec):** Users can configure the length of time that the visitor screening message stays on the screen. The default time is 3 seconds.
 - **Thermal on VoIP Call:** Enable this setting to start screening temperatures for a user when a VoIP call is going on. By default, this field remains disabled.
 - **Temperature Logging:** This setting keeps logging detected temperature in the Transaction Log. By default, this field remains enabled. Users can disable this feature using IXM WEB only. Enable/Disable this setting is not available in LCD.

STEP 3

Once all the settings have been configured, click **Apply**, then click **OK**.

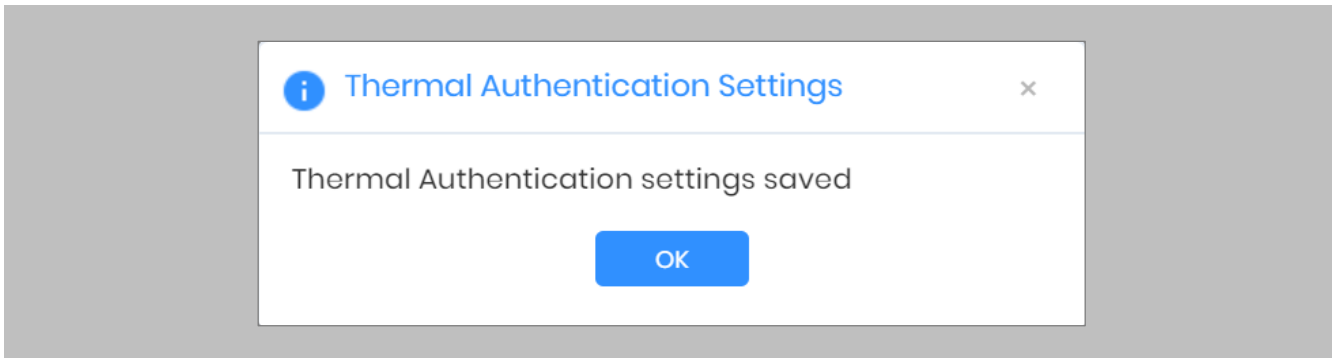


Figure 46: IXM WEB - Save Thermal Settings

Thermal Calibration

STEP 1

Click the **Devices** tab → Select **Device** → Select **Thermal Settings** → **Thermal Calibration** to view default settings.

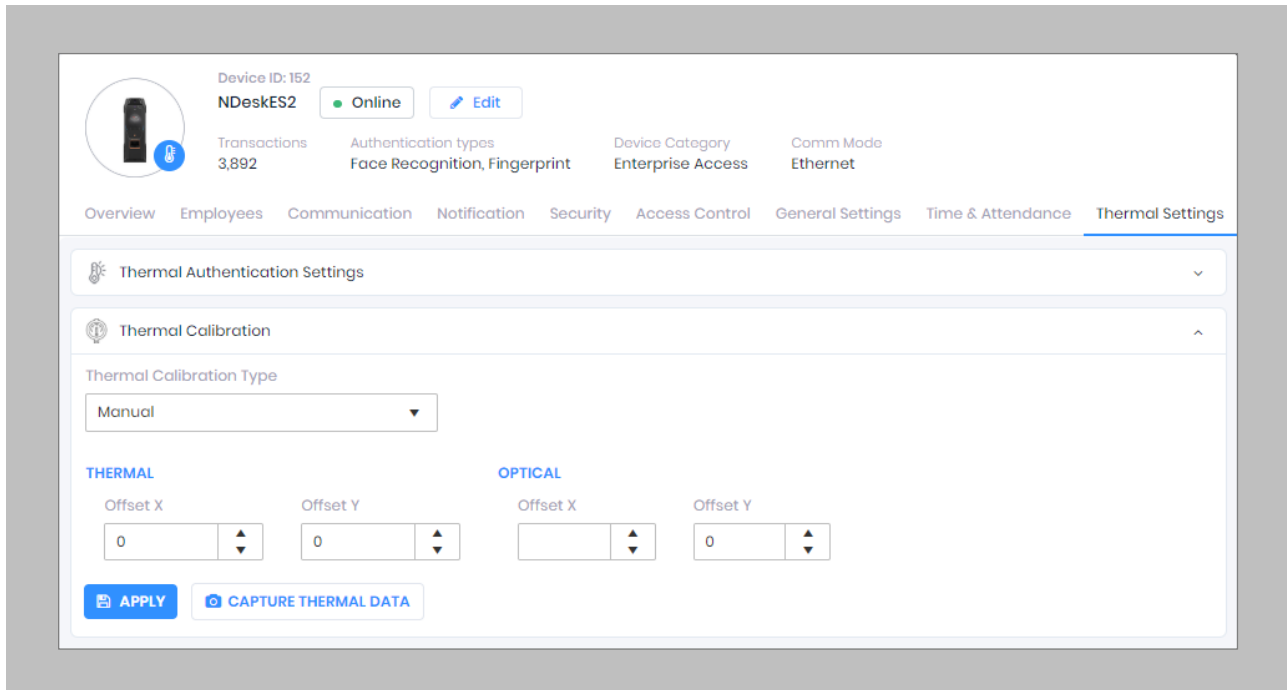


Figure 47: IXM WEB - Thermal Calibration Settings

STEP 2

The settings along with their functions are:

- **Thermal Calibration Type:**
 - Manual
 - Face
 - Black Body

Invizium supports only Manual Thermal Calibration and does not recommend the user select any other option.

- **Offset X (Thermal Section):** Users can set the value for the offset X coordinate of the TIR camera.
- **Offset Y (Thermal Section):** Users can set the value for the offset Y coordinate of the TIR camera.
- **Offset X (Optical Section):** Users can set the value for the offset X coordinate of the TITAN camera.
- **Offset Y (Optical Section):** Users can set the value for the offset Y coordinate of the TITAN camera.

STEP 3

Once all the settings have been configured, click **Apply**, then click **OK**.

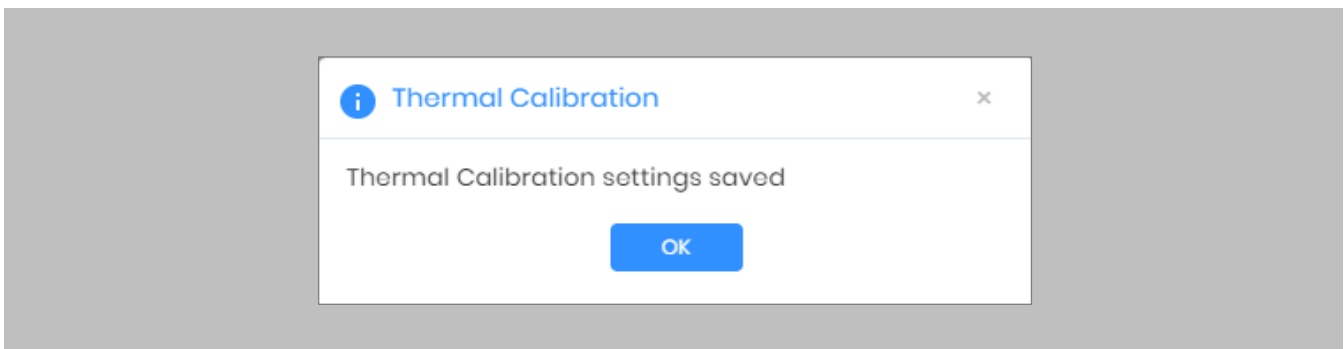


Figure 48: IXM WEB - Save Thermal Calibration Settings

To provide the Thermal Data to the Invixium Technical Services team using IXM WEB, the user needs to click [Capture Thermal Data](#). It will open the popup window and ask the user to show their face 3 times.



Figure 49: IXM WEB - Capture Thermal Data

STEP 4

Once the face is captured 3 times, it will ask the user to save the “.zip” file.

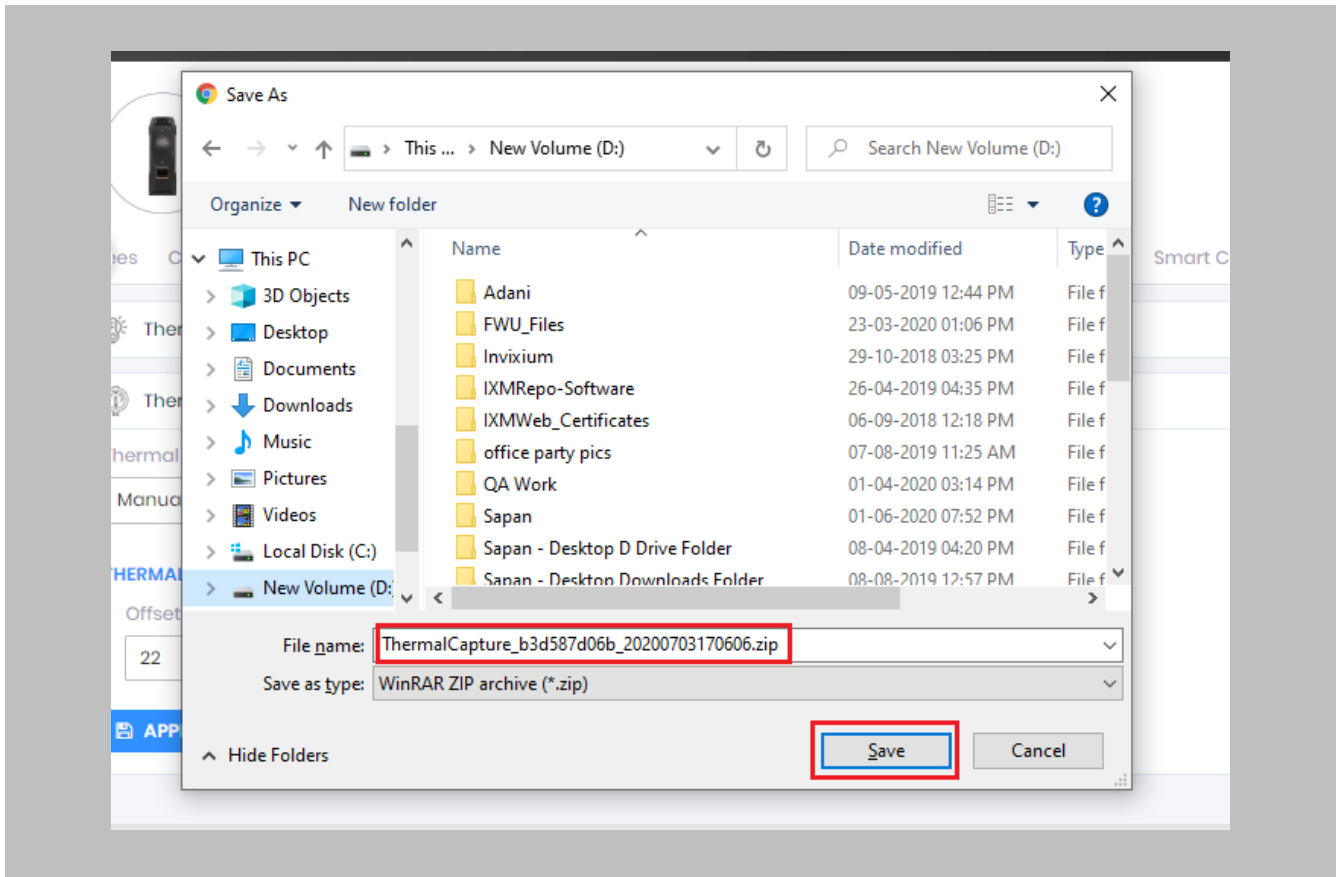



Figure 50: IXM WEB - Save Captured Thermal Data

STEP 5

Click **Save** to store the zip file, then send this file to support@invoxium.com. Invoxium’s Technical Services team will process this file and respond to the user with calibrated values for “X” & “Y” coordinates for the TIR camera and TITAN camera.

 Note: TITAN and the Enhancement kit are factory calibrated when purchased as a bundle. If thermal offset and optical offset values are 0, they capture thermal data.

Test Calibration Options

To test Thermal Calibration, click **Test Calibration**.

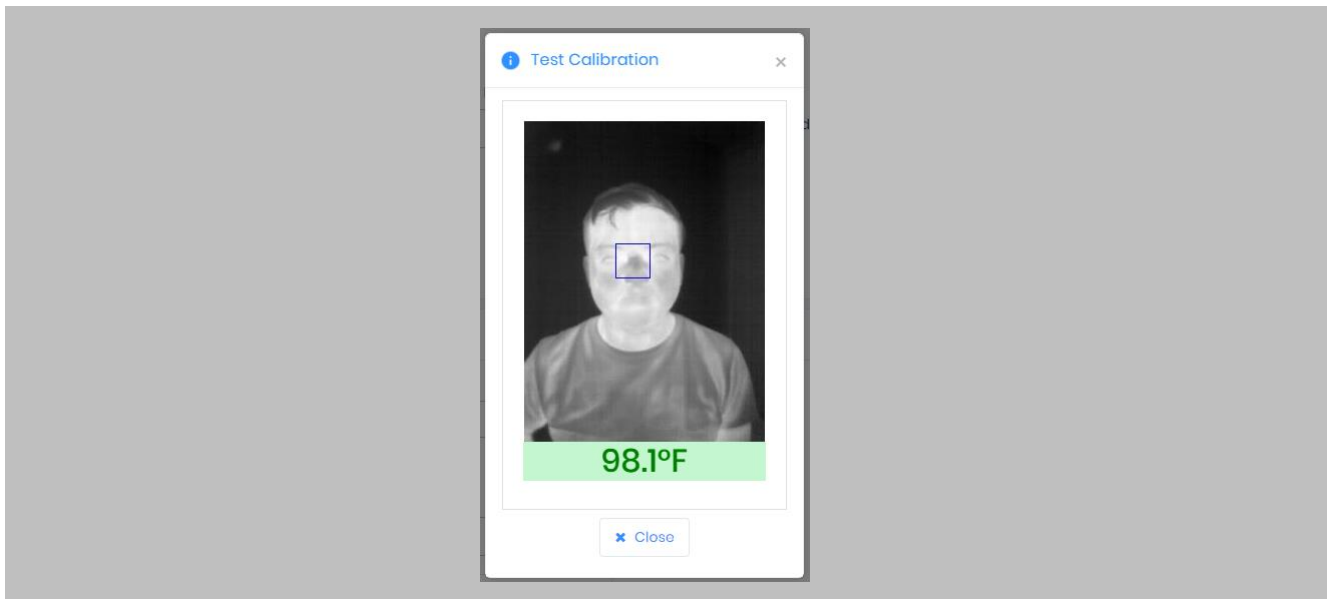



Figure 51: IXM WEB - Test Thermal Calibration

 Note: Square box position should be in the center and cover the tear duct area (Eye Inner Canthus).

Change Temperature Unit Settings

STEP 1

To change the Temperature Unit from Celsius to Fahrenheit and vice-versa, click **Tools** → **Options** → **Manage Preferences**.

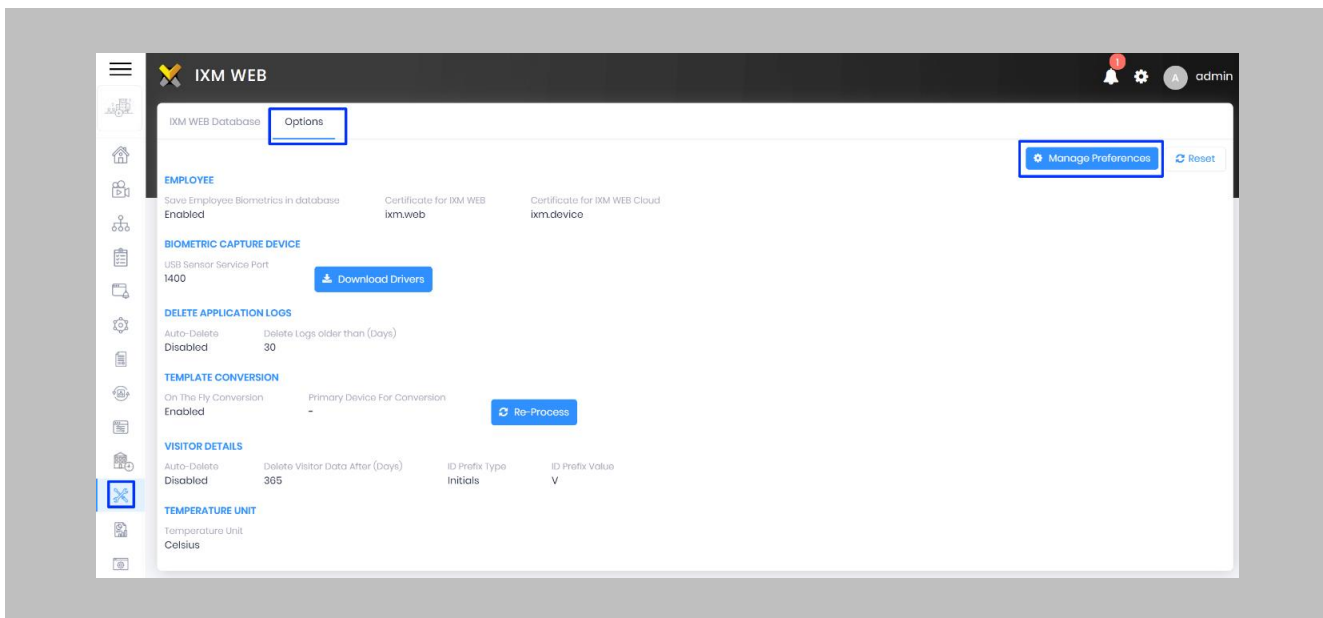



Figure 52: IXM WEB - Option to Change Temperature Unit

STEP 2

Click **Save**.

 Note: Temperature Test failure event in SSP Alarm Viewer will show the Temperature Value as per the Temperature Unit selection.

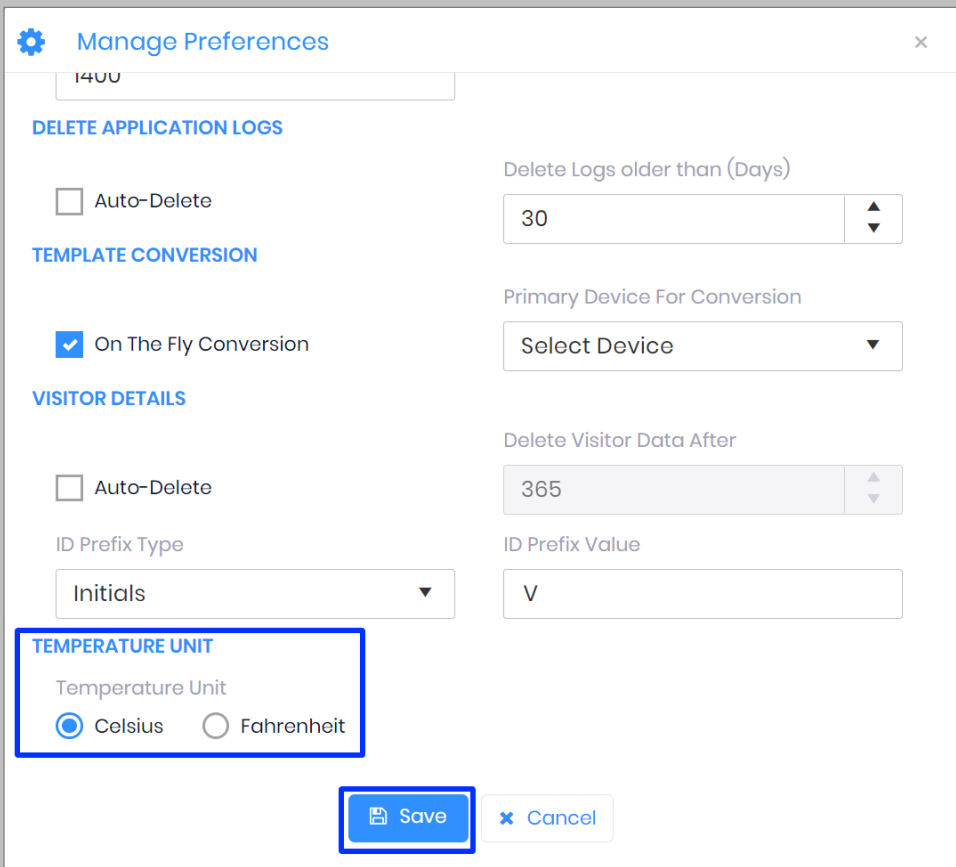


Figure 53: IXM WEB - Save Temperature Unit Setting

Configuring Mask Authentication Settings

STEP 1

Click the **Devices** tab → Select **Device** → Select **General Settings** → **Mask Authentication Settings** to view default settings.

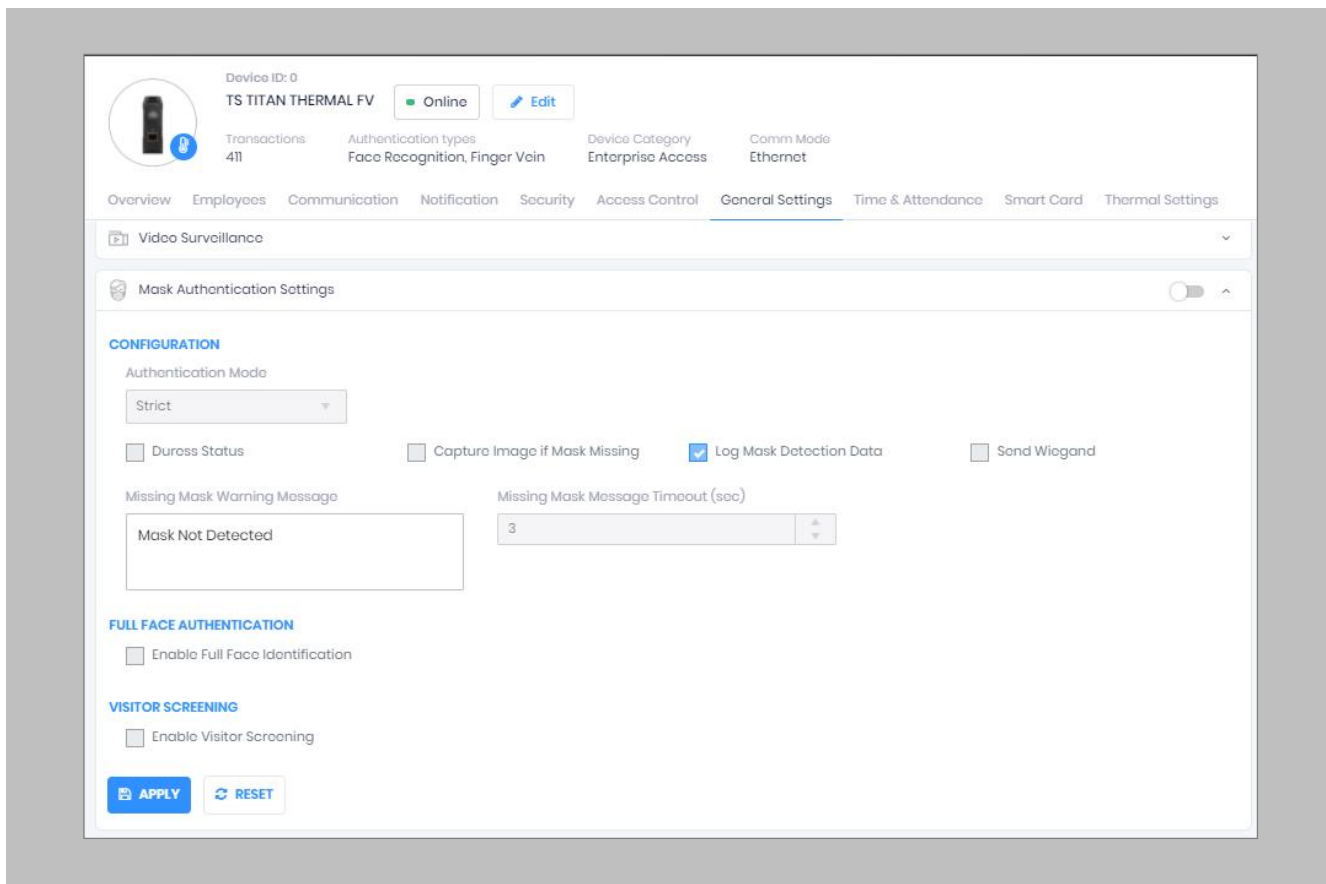


Figure 54: IXM WEB - Mask Authentication Settings

STEP 2

The list of settings is:

- **Authentication Mode:** There are two options for the mode of authentication used to control the access workflow if a mask is not detected. The default mode of authentication is strict.
 - **Soft: Access will be granted to the user even if a mask is not detected.**
 - **Strict: Access will be denied if a mask is not detected.**
- **Duress Status:** Enabling this setting would allow access to the user if a mask was not detected if the user authenticates using their pre-programmed duress finger. The default setting is **disabled**.
- **Capture Image if Mask Missing:** Enable this setting to capture an image of the user if a mask is not detected. By default, this setting is **disabled**. The same image will be used for sending email notifications from IXM WEB.
- **Log Mask Detection Data:** This setting tracks mask detection in the transaction log. By default, this setting is **enabled**. You can disable this feature using IXM WEB only, not on the device's LCD.
- **Send Wiegand:** This setting will be visible only in "Strict" authentication mode. Enabling this setting will generate Wiegand whenever a mask is not detected in the authentication process.
- **Missing Mask Warning Message:** Set a message to display after a mask is not detected. The message can be up to 50 characters.
- **Missing Mask Warning Message Timeout (sec):** Configure the length of time that the mask is not detected message stays on the screen. The default time is 3 seconds.
- **Enable Full Face Identification:** Invixium Periocular algorithms can achieve accurate identification using only the eye and eyebrow regions of the face. Full face identification is used to get more accuracy in authentication and capture a user's face without a mask in the image log. By default, this setting is **disabled**.

- **Remove Mask Display Message:** Set a message to display after a mask is detected when Full Face Identification is enabled. Messages can be up to 50 characters.
- **Remove Mask Display Message Time (sec):** Configure the length of time that the mask is detected message stays on the screen. The default time is 3 seconds.
- **Enable Visitor Screening:** Enable this setting to start screening visitors for masks. By default, this field is **disabled**.
- **Visitor Screening Message:** Set a message that will be displayed when a visitor is showing their face. Messages can be up to 50 characters.
- **Visitor Mask Missing Warning Message:** Set a message that will be displayed when a visitor is screened without a mask. Messages can be up to 50 characters.
- **Visitor Message Display Time(sec):** Configure the length of time that the visitor screening message stays on the screen. The default time is 3 seconds.

STEP 3

Once all the settings have been configured, click **Apply**, then click **OK**.

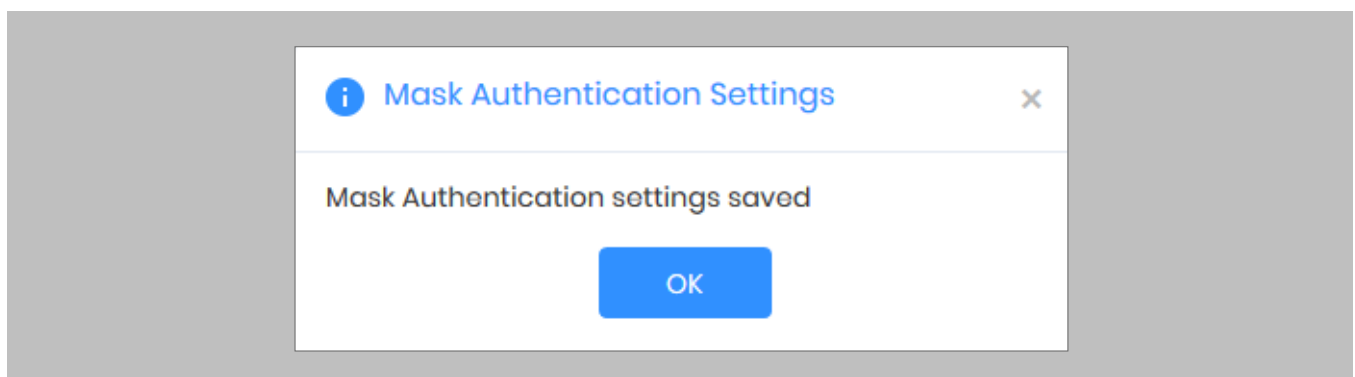


Figure 55: IXM WEB - Save Mask Settings

13. 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 required.

Avoid Poor Fingerprint Conditions

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

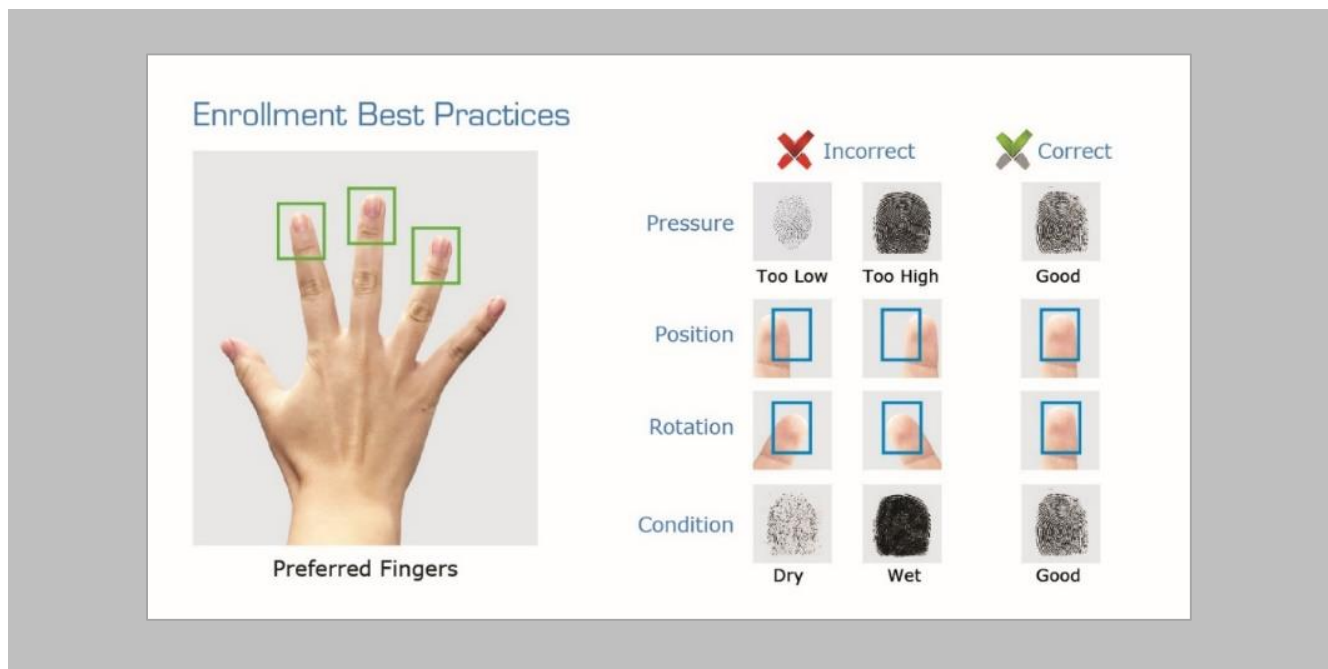


Figure 56: Fingerprint Enrollment Best Practices

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 your finger and re-enroll for better results
	Wet/Sweaty finger	Rub the finger on a clean cotton cloth and re-enroll for better results

Figure 57: 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 with 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.

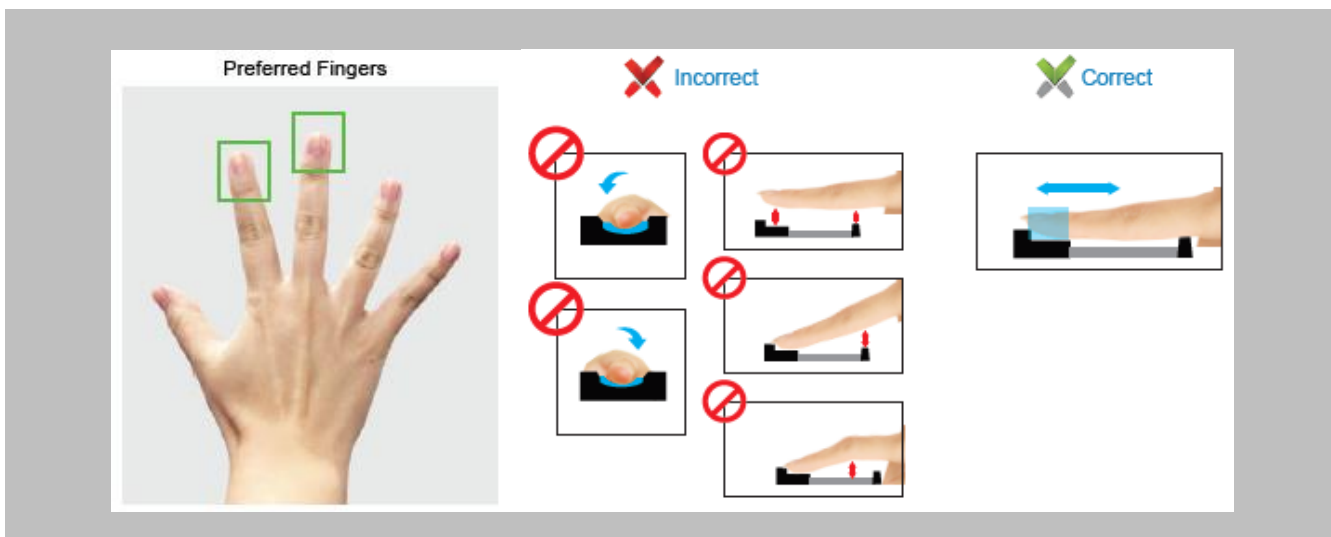


Figure 58: Finger Vein Enrollment Best Practices

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.

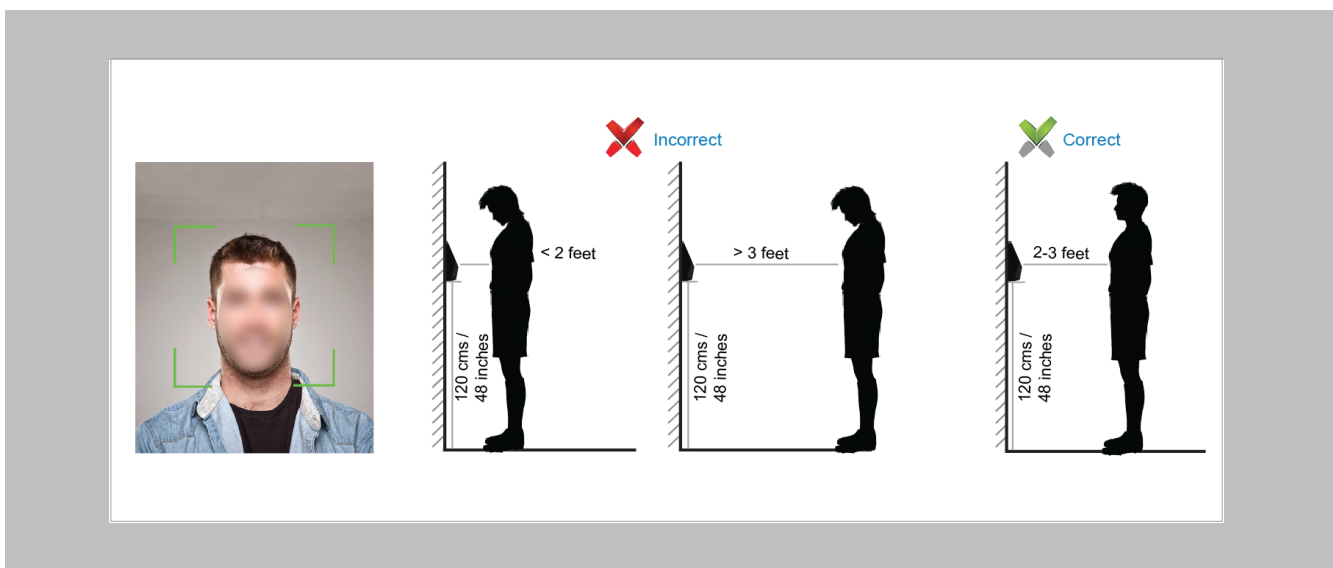


Figure 59: Face Enrollment Best Practices

14. Appendix

Installing Invixium IXM WEB with Default Installation using SQL Server 2014



Note:

- By default, the IXM WEB installer will install SQL Server 2014
- It is highly recommended to use SQL Server 2016 or higher

If it is intended for IXM WEB to use a non-default SQL 2014 installed instance, please refer to Installing SQL Instance.

Procedure

STEP 1

Run the [installer.exe](#)

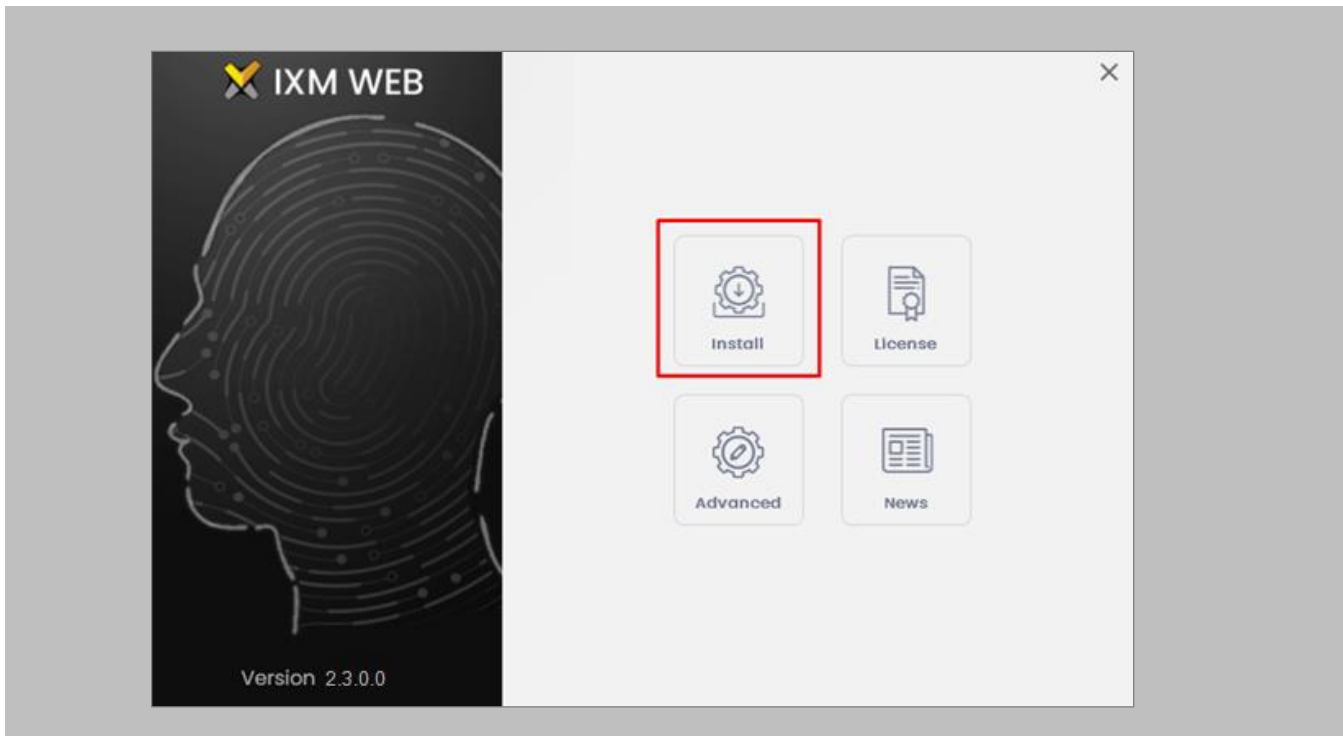


Figure 60: Install IXM WEB



Note: Installs SQL 2014 Express.

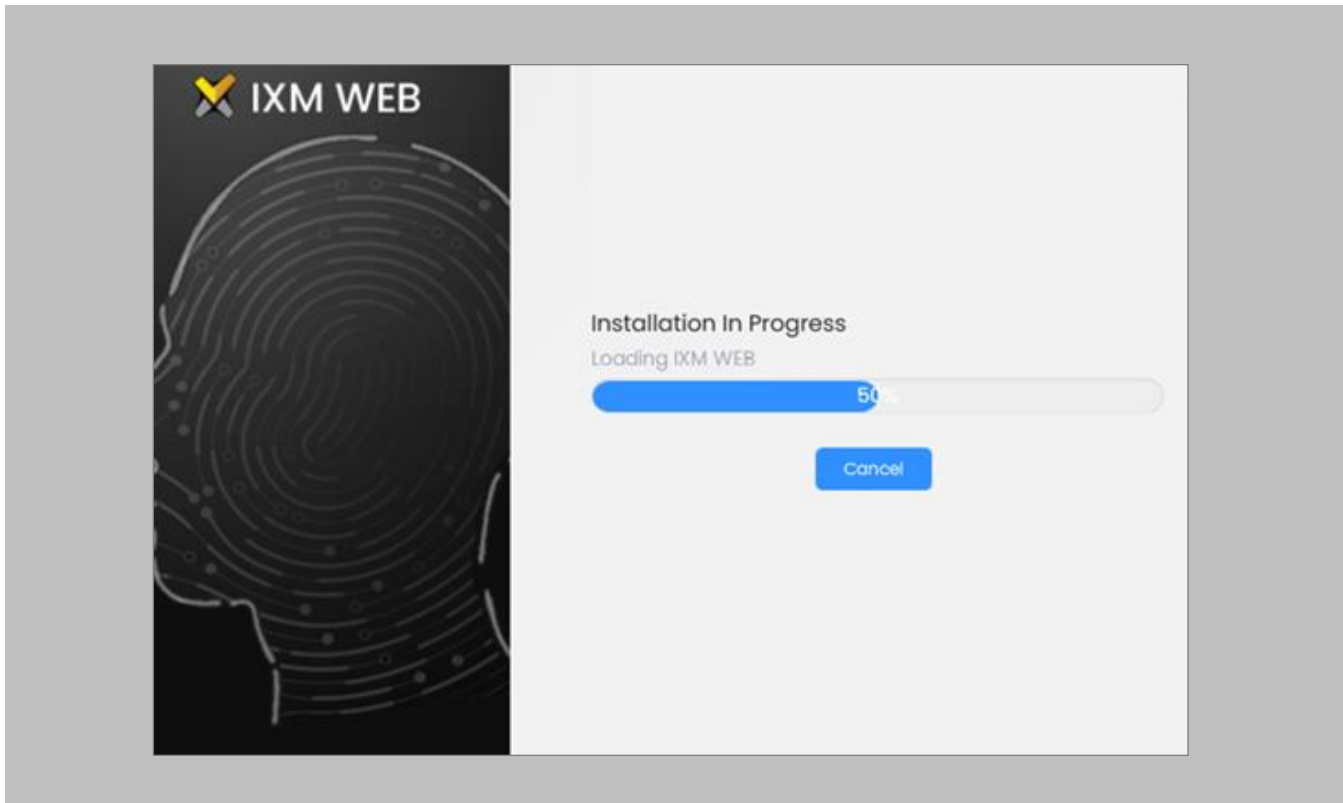


Figure 61: Loading SQL Express & Installation Progress

STEP 2

Once the installation is completed, check these services to make sure they are all running:

- Bonjour
- Invixium Device Discovery
- IXM WEB

STEP 3

Run **IXM WEB** by selecting it from the Windows Start menu on your desktop.

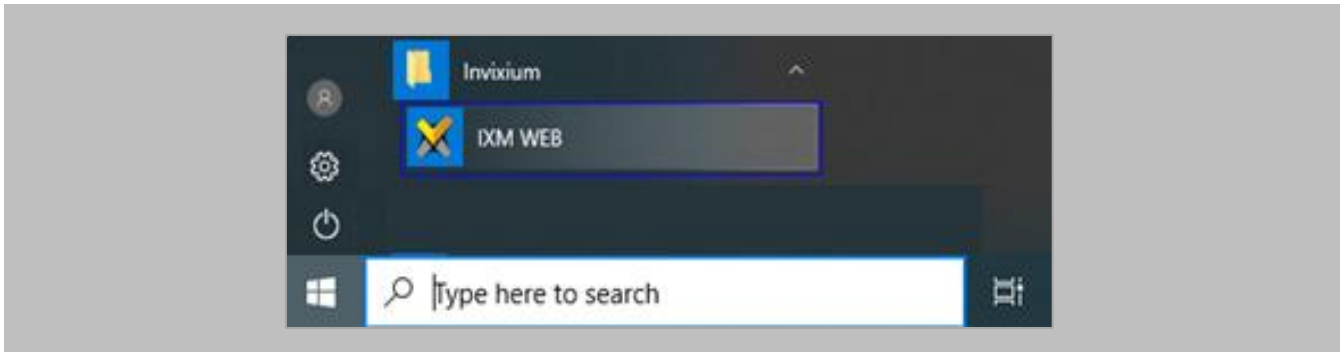


Figure 62: IXM WEB - Shortcut Icon on Desktop

STEP 4

Select **Windows Authentication** and the **SQL Server Name**, then click on **Connect**.

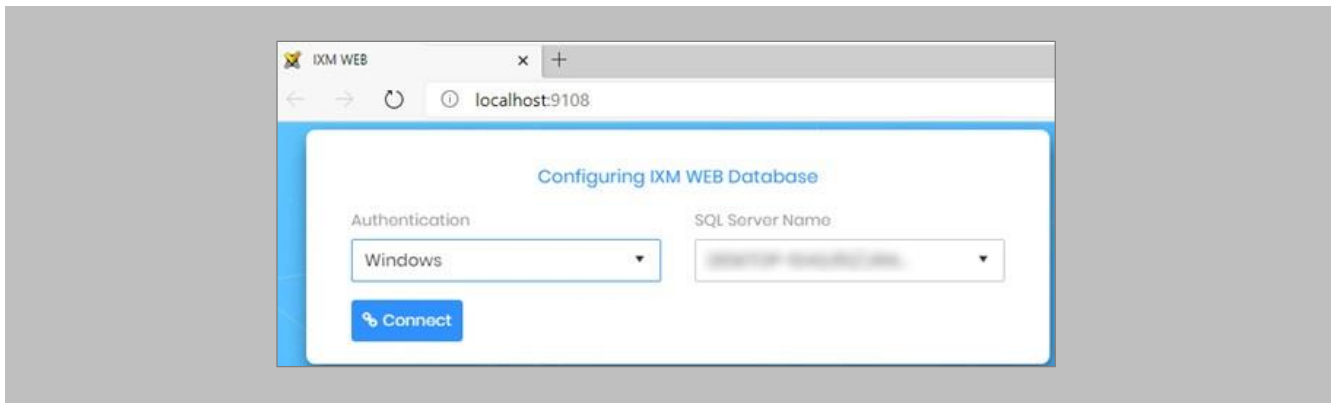


Figure 63: IXM WEB - Configuring IXM WEB Database

STEP 5

Select the **Database Name** and then click **Next**.

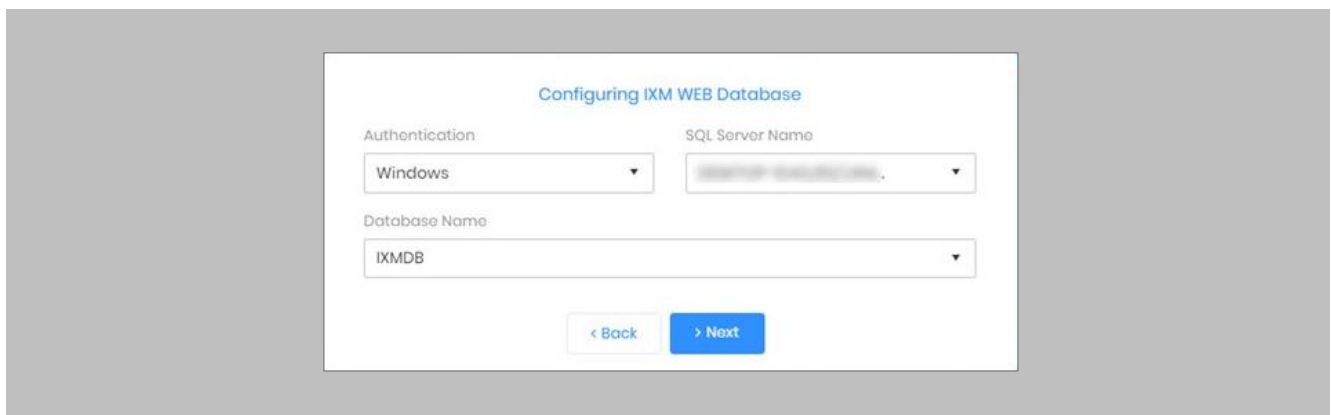


Figure 64: IXM WEB - Select Database Name

STEP 6

Fill in the fields under the **Create Account** section and then select **Save At Server URL**.

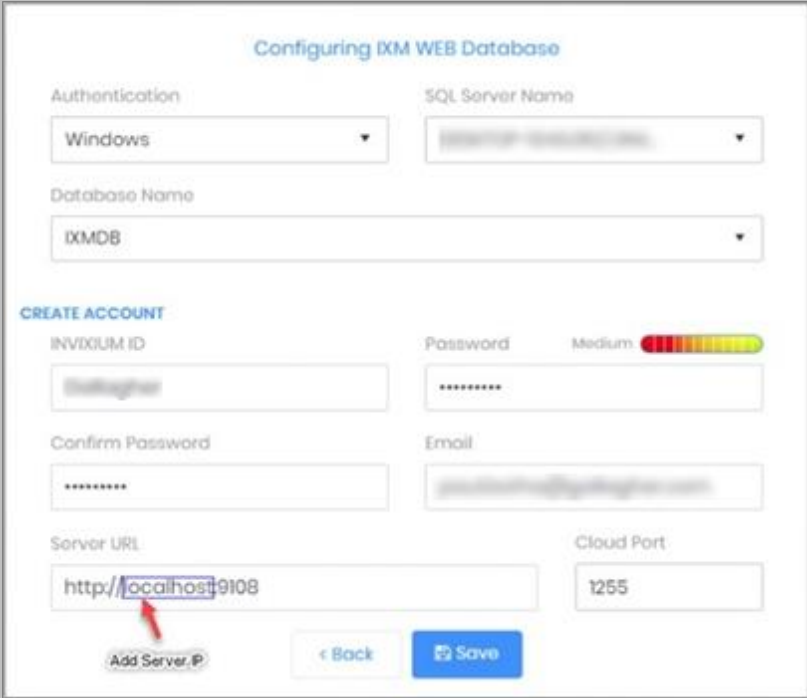


Figure 65: IXM WEB - Server URL format

STEP 7

Use the server machine's **IP Address** which will interface with the Invidium reader.

Pushing Configuration to Multiple Invoxium Readers

Procedure

STEP 1

To push these configurations to other Invoxium readers, while the configured Invoxium device is selected, click the **Broadcast** option on the right-hand side.

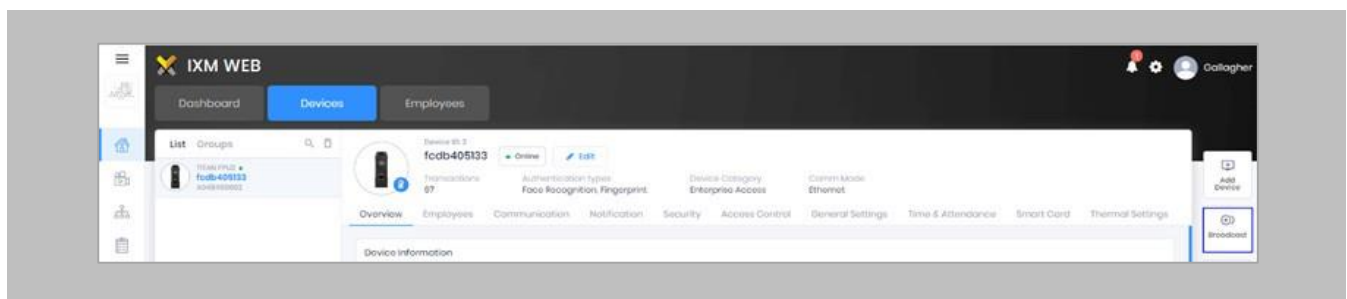


Figure 66: IXM WEB - Broadcast Option

STEP 2

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

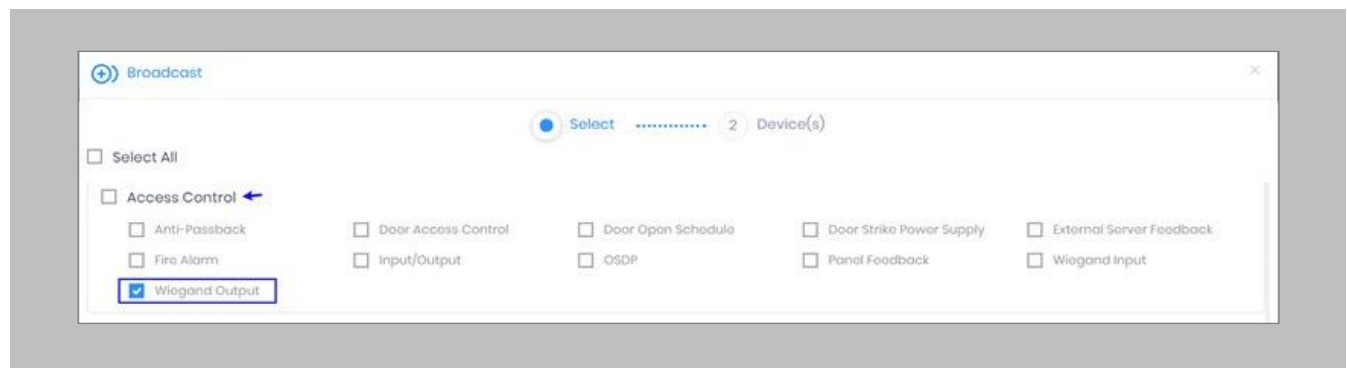


Figure 67: IXM WEB - Wiegand Output Selection in Broadcast

STEP 3

Click **Broadcast**.

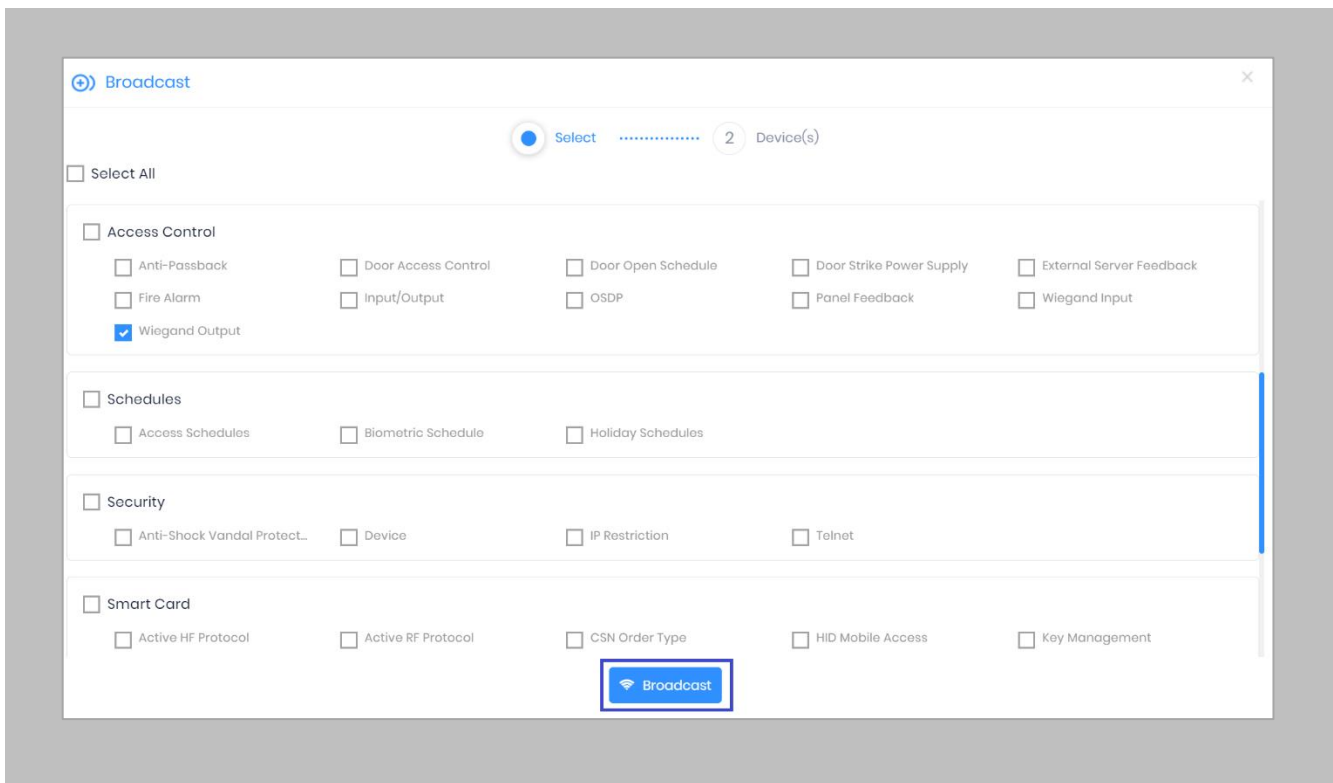


Figure 68: IXM WEB - Broadcast Wiegand Output Settings

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.

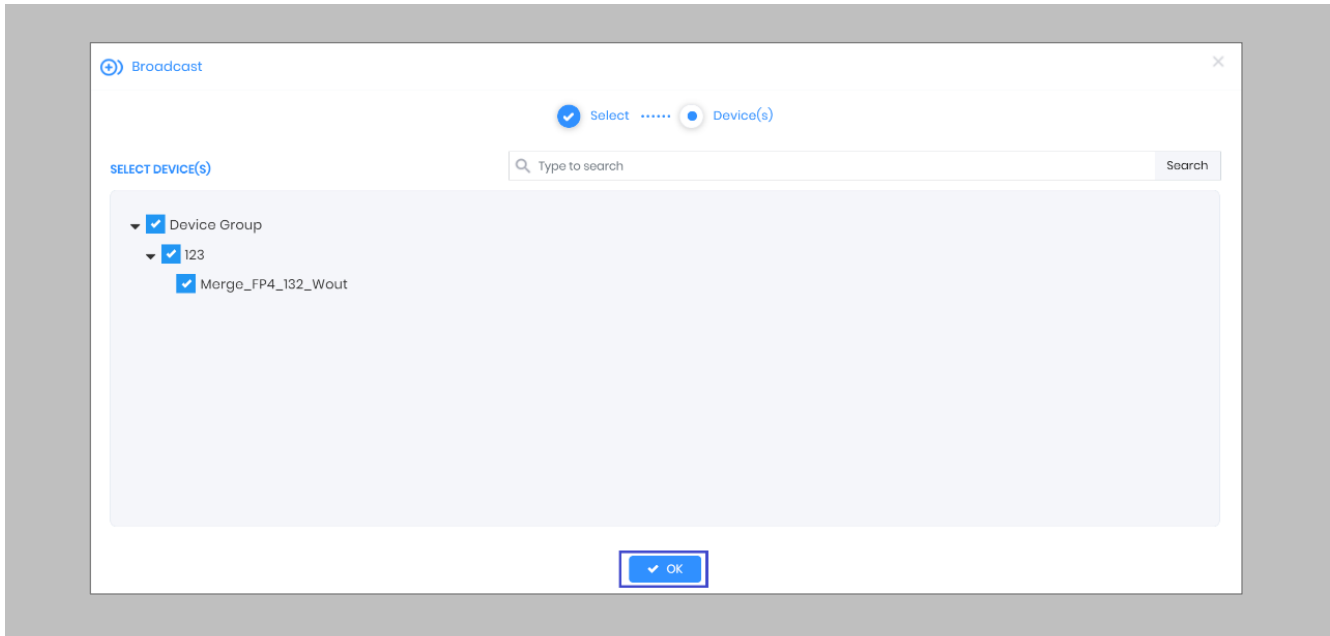


Figure 69: IXM WEB - Broadcast to Devices




STEP 2

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

Baud Rate	The baud rate of serial communication. The value must be the same as the Access Control Panel's value.
Parity Bit	The parity bit of the serial communication. The value must be the same as the Access Control Panel's value.
Stop Bit	The stop bit of the serial communication. The value must be the same as the Access Control Panel's value.
Timeout (msec)	The time duration (500 to 10000 milliseconds) up to which the Device should keep trying to connect to the Access Control Panel. The default timeout duration is 300 milliseconds. On timeout, the Device LCD flashes an "Access Denied" message, and the "Application Logs" window will show a failure message.
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

	<p>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:</p> <ul style="list-style-type: none"> • 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.
<p>On Color/Off Color</p>	<p>The LED color configuration is based on panel events. The value must be the same as the Access Control Panel's value. Options are:</p> <ul style="list-style-type: none"> • Red • Green • Yellow • Blue

Table 5: IXM WEB - OSDP Configuration Options

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

Display OSDP Text	Enables to display OSDP Text.
Display Message	<p>Notification on the device's screen.</p> <p>If enabled: Displays both the unit hardcoded notification and the Access Control Panel notification. IXM notification - Access Granted or Access Denied. Access Control Panel notification – Valid or Invalid.</p> <p>If disabled: Displays only the Access Control Panel notification.</p>

Table 6: IXM WEB - OSDP Text Options

STEP 3

Click **Apply** to save the settings.

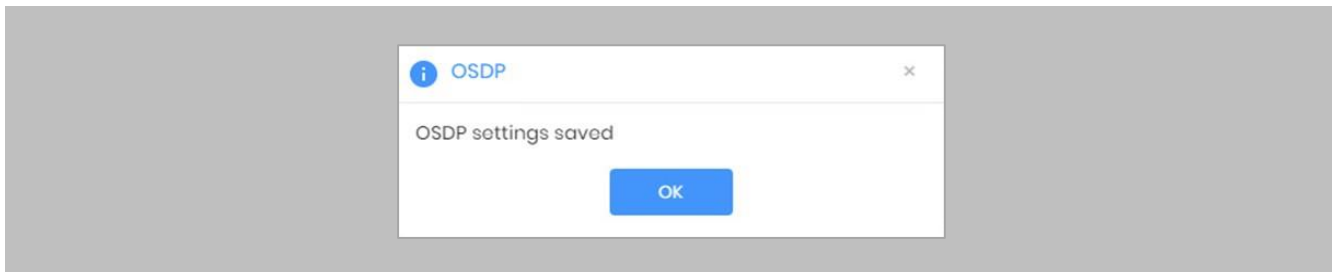


Figure 71: IXM WEB - Save OSDP Settings

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 the SiPort.

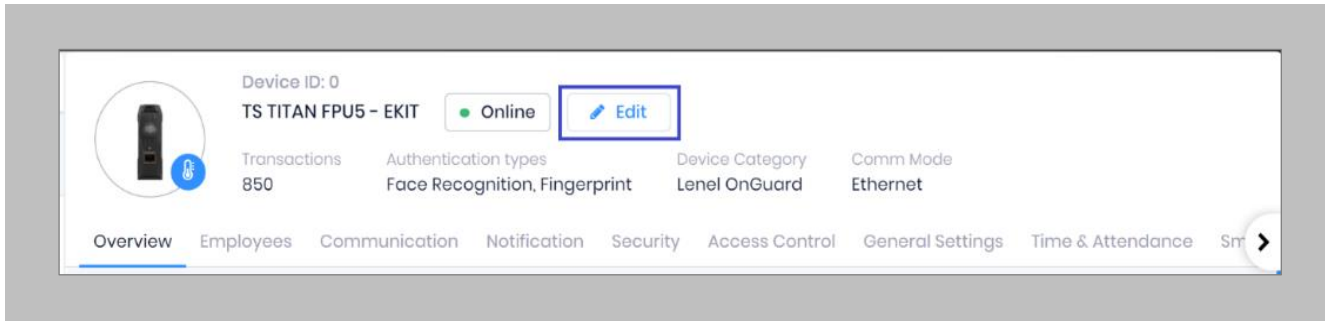


Figure 72: IXM WEB - Edit Device

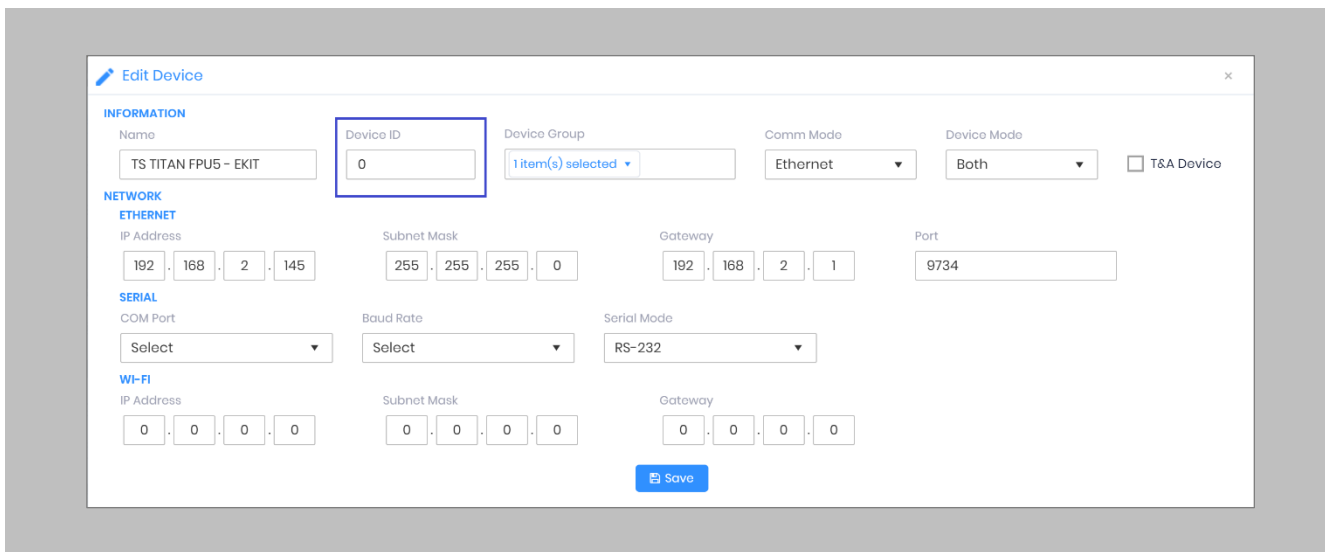


Figure 73: IXM WEB - Edit Device Options

STEP 6

Optional: Enable encryption from within SiPort.

STEP 7

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 8

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

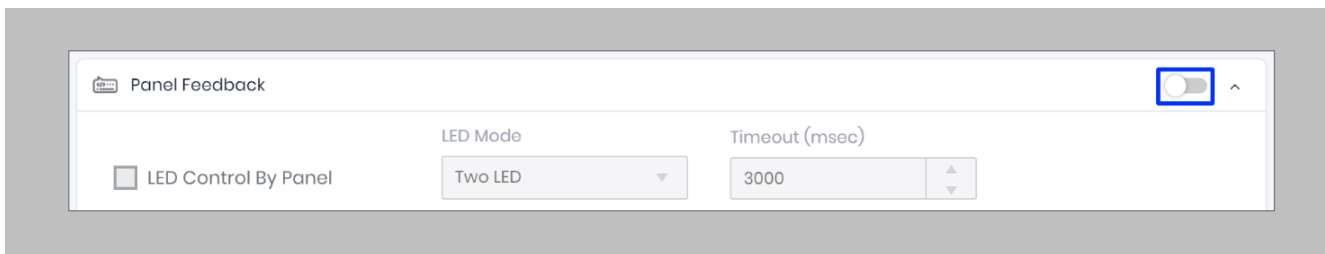


Figure 74: IXM WEB - Disable Panel Feedback

Configuring MIFARE DESFire Custom Cards

STEP 1

From **Home**, click the **Devices** tab. Select the required **Device** and navigate to **Smart Card**. Click **MIFARE DESFire Configuration**.

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

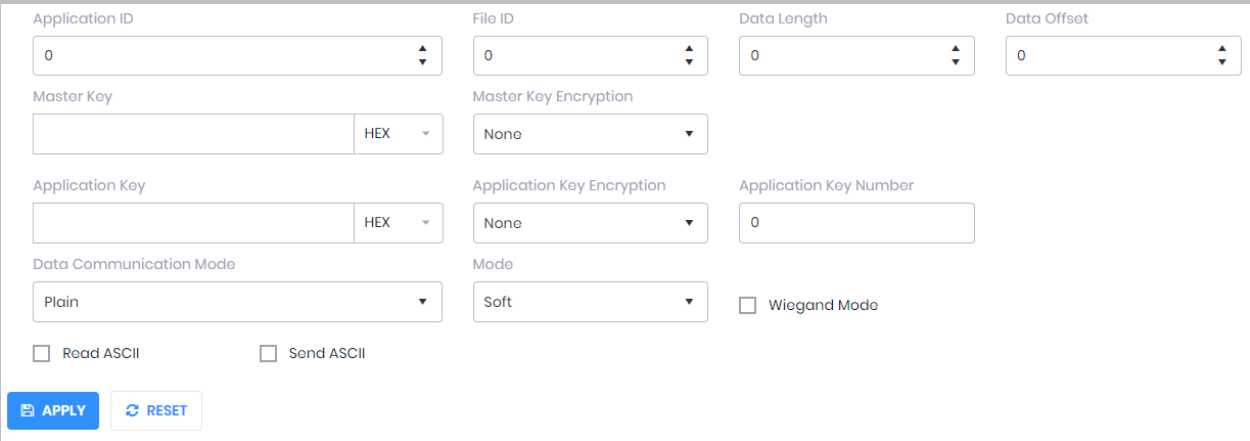


Figure 75: IXM WEB - MIFARE DESFire Configuration

STEP 2

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

Application ID	The application ID of the SIEMENS cards.
File ID	The file ID of the SIEMENS cards.
Data Length	Enter the data length of SIEMENS cards.

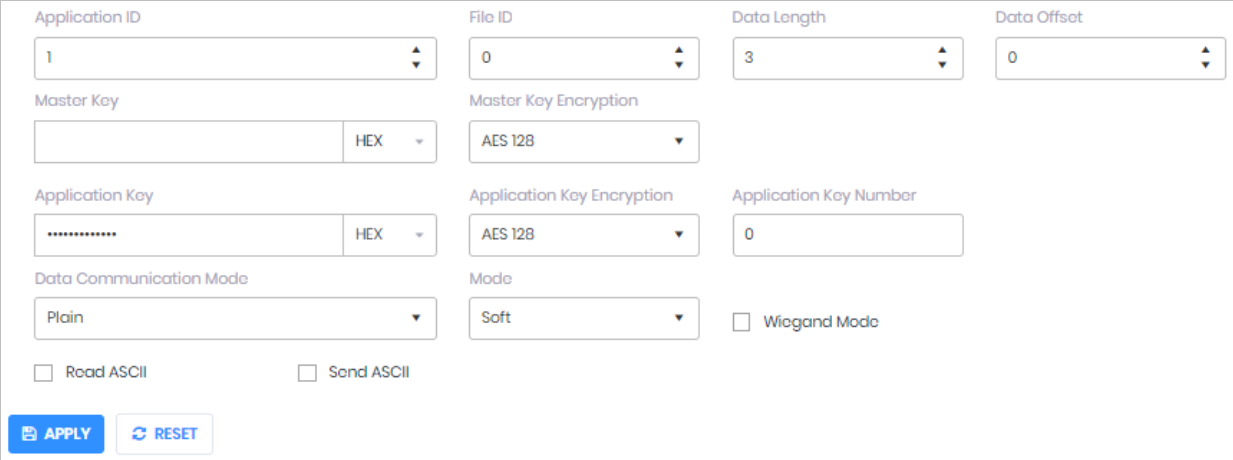
Data Offset	Enter data offset of SIEMENS cards.
Master Key	Enter the Master key of SIEMENS cards.
Master Key Encryption	Select Master Key Encryption from the dropdown as per requirement. Options are: <ul style="list-style-type: none"> • None • 2K 3DES • 3K 3DES • AES 128
Application Key	Enter the Application key of SIEMENS cards.
Application Key Encryption	Select Application Key Encryption from the dropdown as per requirement. Options are: <ul style="list-style-type: none"> • None • 2K 3DES • 3K 3DES • AES 128
Application Key Number	Enter the Application key Number of SIEMENS cards.
Data Communication Mode	Select Data Communication Mode from the dropdown as per requirement. Options are: <ul style="list-style-type: none"> • Plain • MAC • Enciphered
Mode	Select the Mode from the dropdown as per requirement. Options are: <ul style="list-style-type: none"> • Soft • Strict
Wiegand Mode	Enable Wiegand mode if data is encoded in Wiegand format.

Read ASCII	Enable Read ASCII so that the Device can read the ASCII data from the Smart Card as per the configuration.
Send ASCII	Enable Send ASCII so that the Device can send the ASCII raw data.

Table 7: IXM WEB – MIFARE DESFire Configuration Options

STEP 3

The below image shows the configuration for a sample **SIEMENS Card**.



The screenshot shows the configuration interface for a MIFARE DESFire card. The fields are as follows:

- Application ID: 1
- File ID: 0
- Data Length: 3
- Data Offset: 0
- Master Key: (empty)
- Master Key Encryption: AES 128
- Application Key: (masked with dots)
- Application Key Encryption: AES 128
- Application Key Number: 0
- Data Communication Mode: Plain
- Mode: Soft
- Wiegand Mode:
- Read ASCII:
- Send ASCII:

Buttons: APPLY, RESET

Figure 76: IXM WEB - MIFARE DESFire Sample Configuration

Wiring and Termination

Procedure

Earth Ground

For protection against ESD, Invixium recommends the use of a ground connection between each Invixium device to 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 the earth ground wire provided in the install kit box to the **building earth ground**.

STEP 3

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

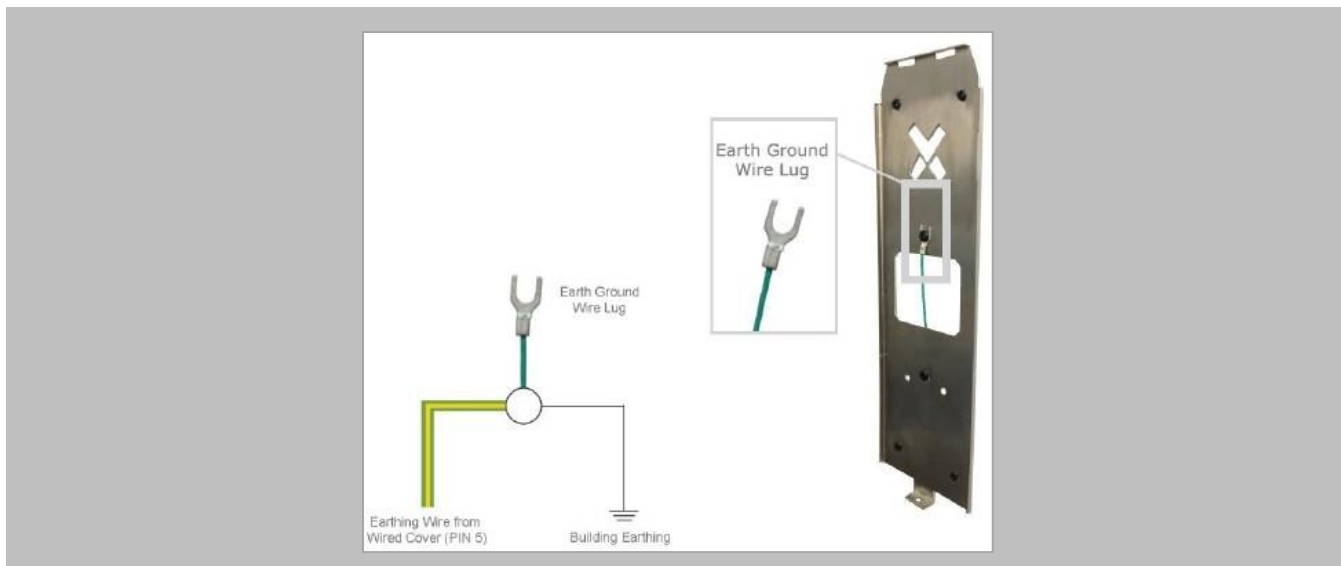


Figure 77: Earth Ground Wiring

Wiring

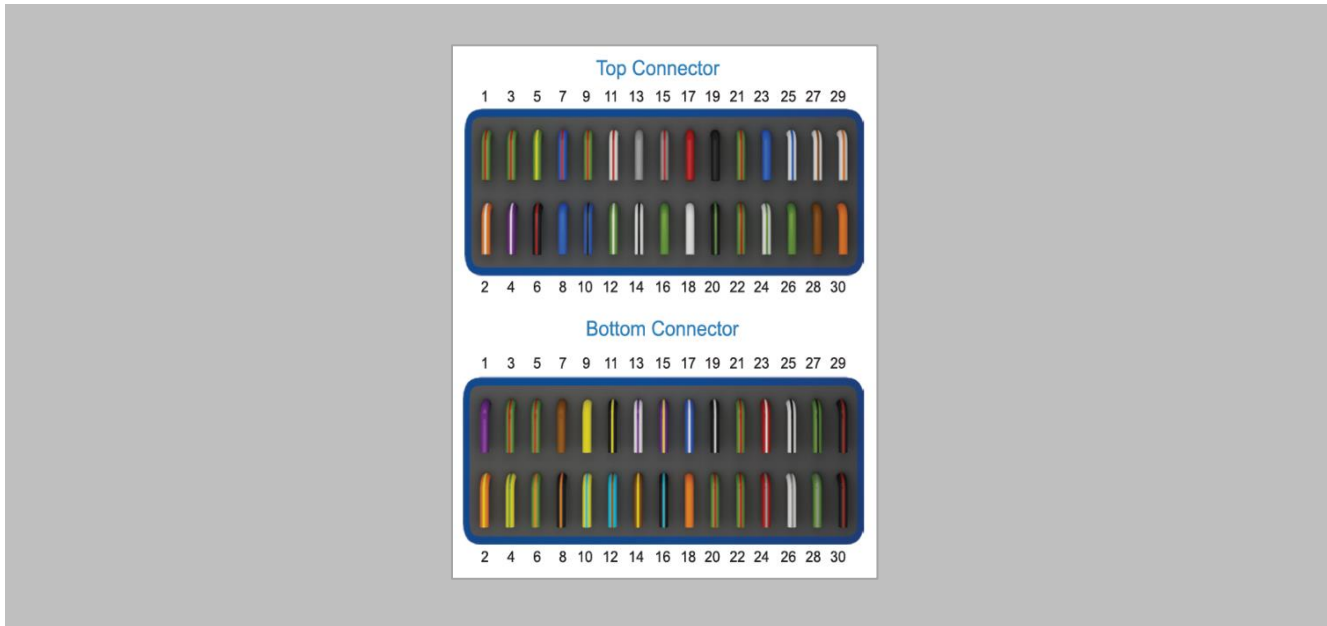


Figure 78: IXM TITAN – Top & Bottom Connector Wiring

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	POWER			
Blue/Black		RS485_D-	10	Wiegand			
White/Red		RLY_NC	11	OSDP			
Green/White		WDATA_IN0	12				
Grey		RLY_COM	13				
White/Black		WDATA_IN1	14				
Grey/Red		RLY_NO	15				

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 79: Power, Wiegand & OSDP Wires

All Invixium devices support Wiegand and OSDP.

Invixium devices can be integrated with SIEMENS Controller on:

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

Wiegand Connection

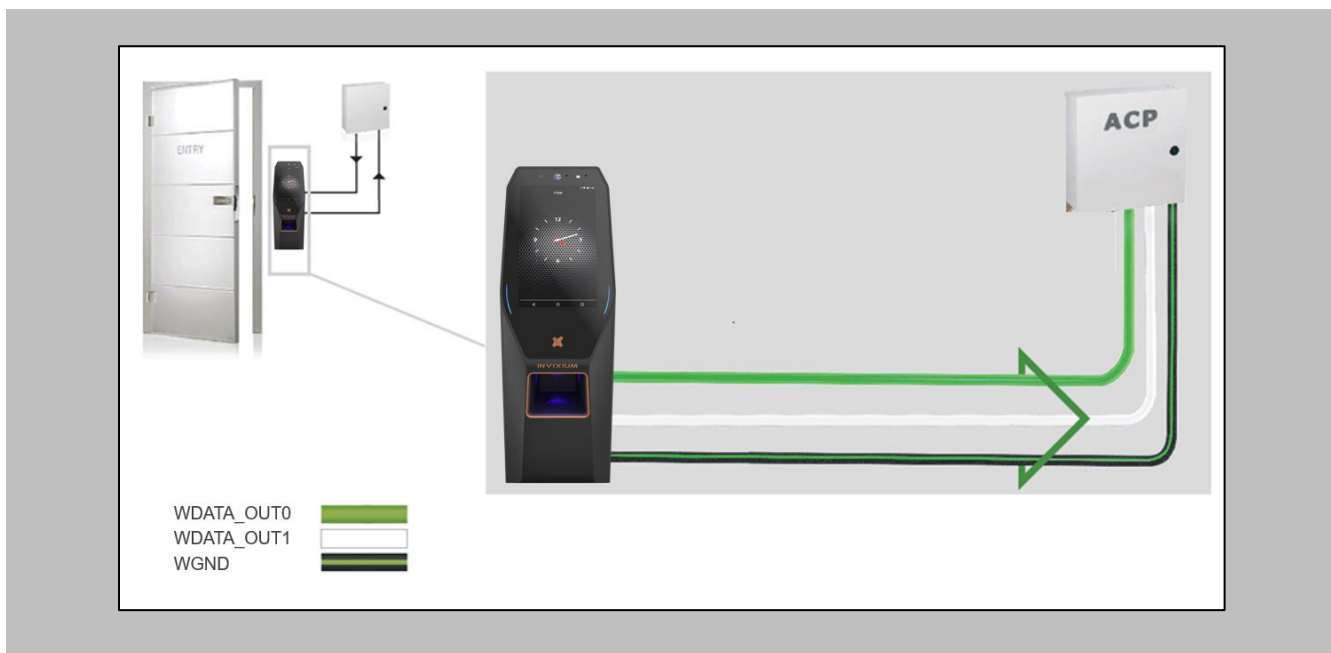



Figure 80: IXM TITAN - Wiegand

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

Wiegand Connection with Panel Feedback

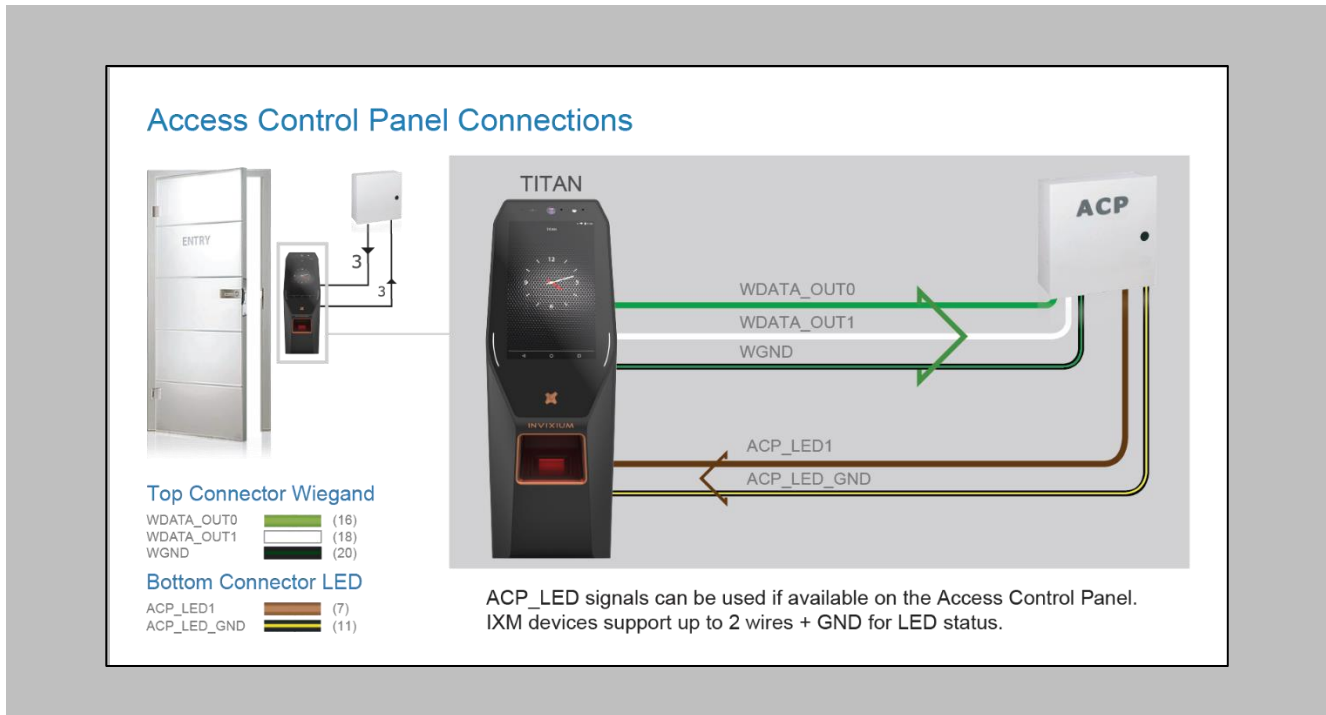



Figure 81: IXM TITAN - Panel Feedback

 Please refer to the INGUIDE document provided for each product on [Invixium.com](https://www.invixium.com) under the **Download** section of the **Products** menu.

OSDP Connections

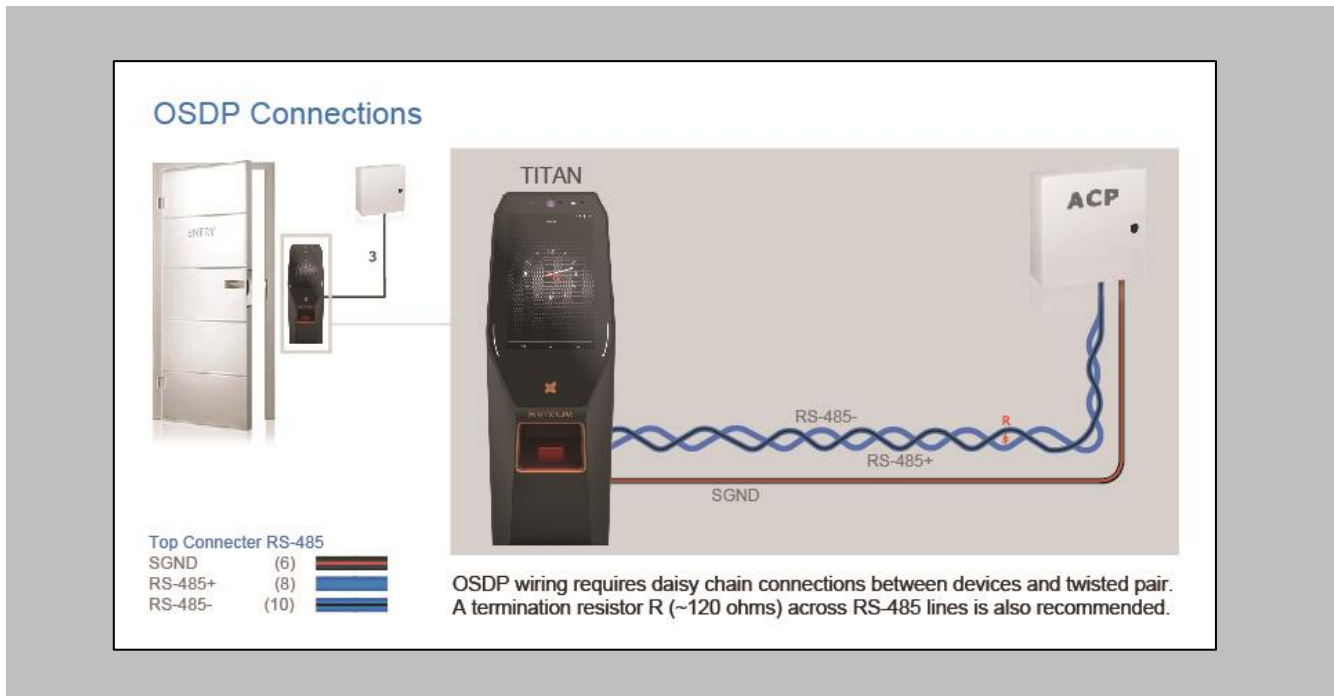




Figure 82: IXM TITAN - OSDP Connections

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

15. Troubleshooting

Reader Offline from the IXM WEB Dashboard

 Note: Confirm communication between the IXM WEB server and the Invixium reader.

Procedure

STEP 1

From [Home](#), click the [Devices](#) tab.

STEP 2

[Select](#) any device.

STEP 3

Navigate to the [Communication](#) tab.

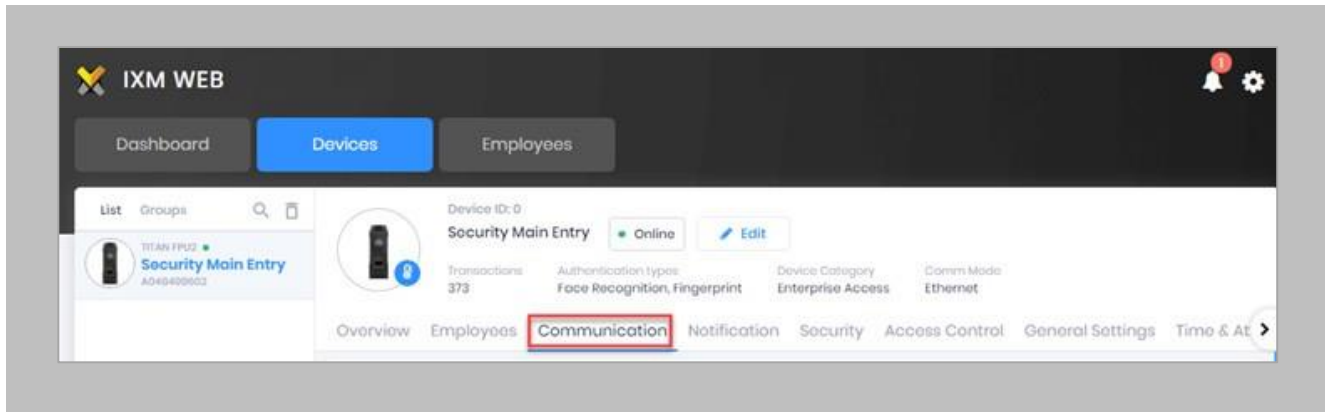


Figure 83: IXM WEB - Device Communication Settings

STEP 4

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

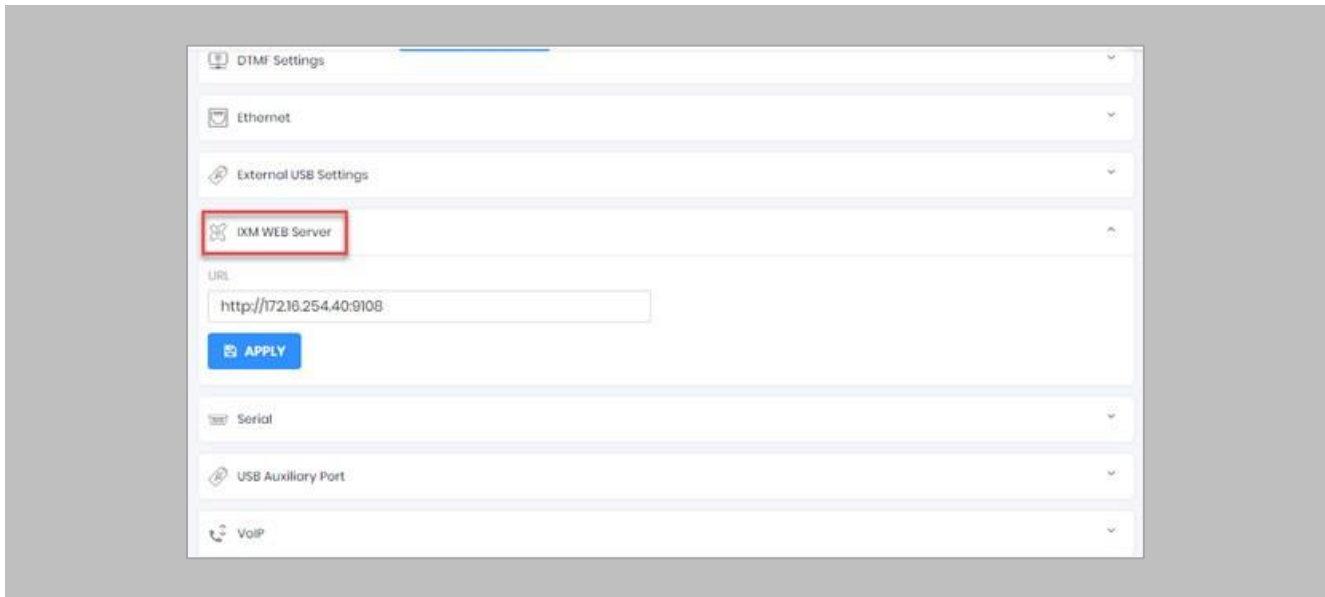


Figure 84: IXM WEB - Server URL Setting

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

STEP 5

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

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

STEP 6

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

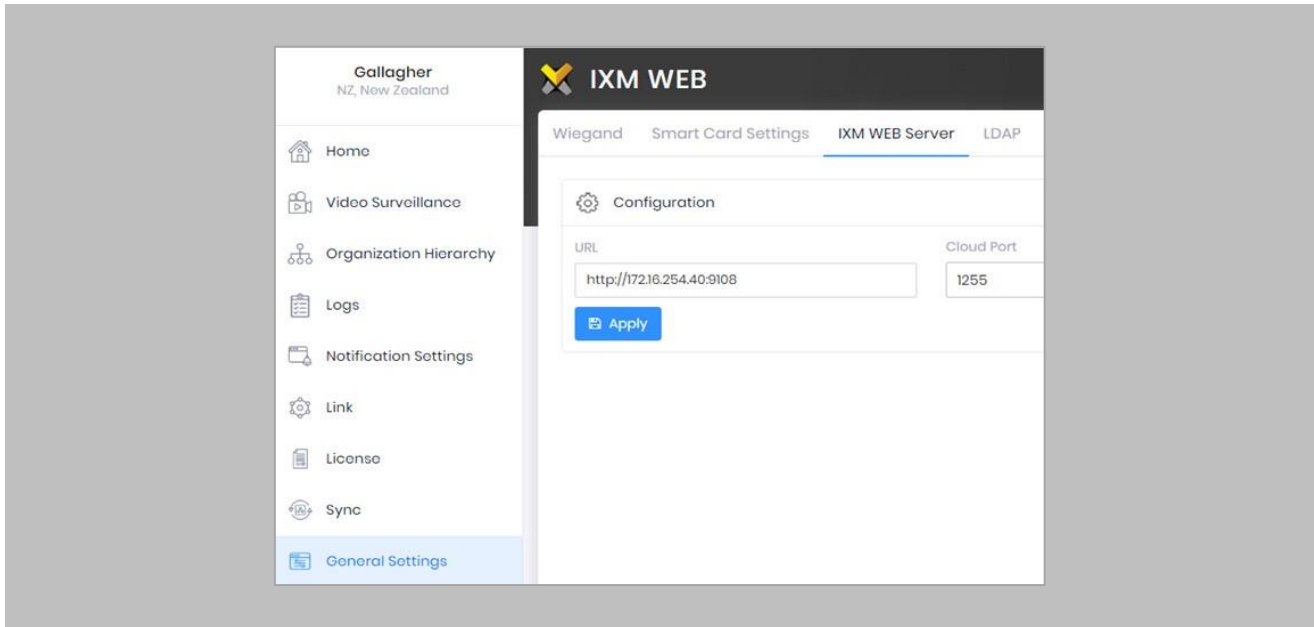


Figure 85: IXM WEB - Server URL Setting from General Settings

Logs in IXM WEB Application

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

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

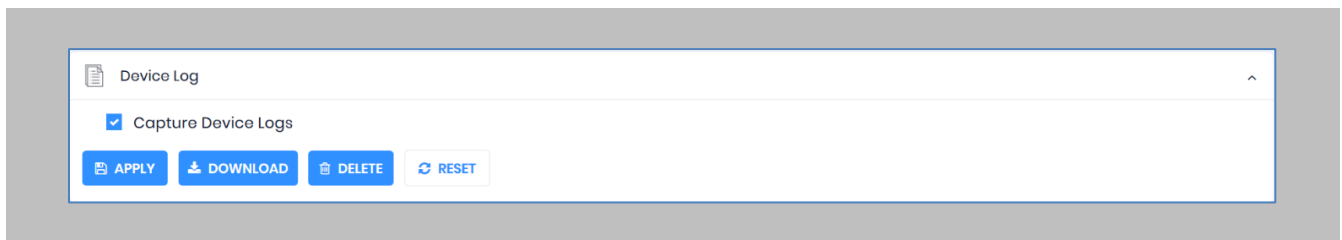


Figure 86: IXM WEB - Enable Device Logs

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

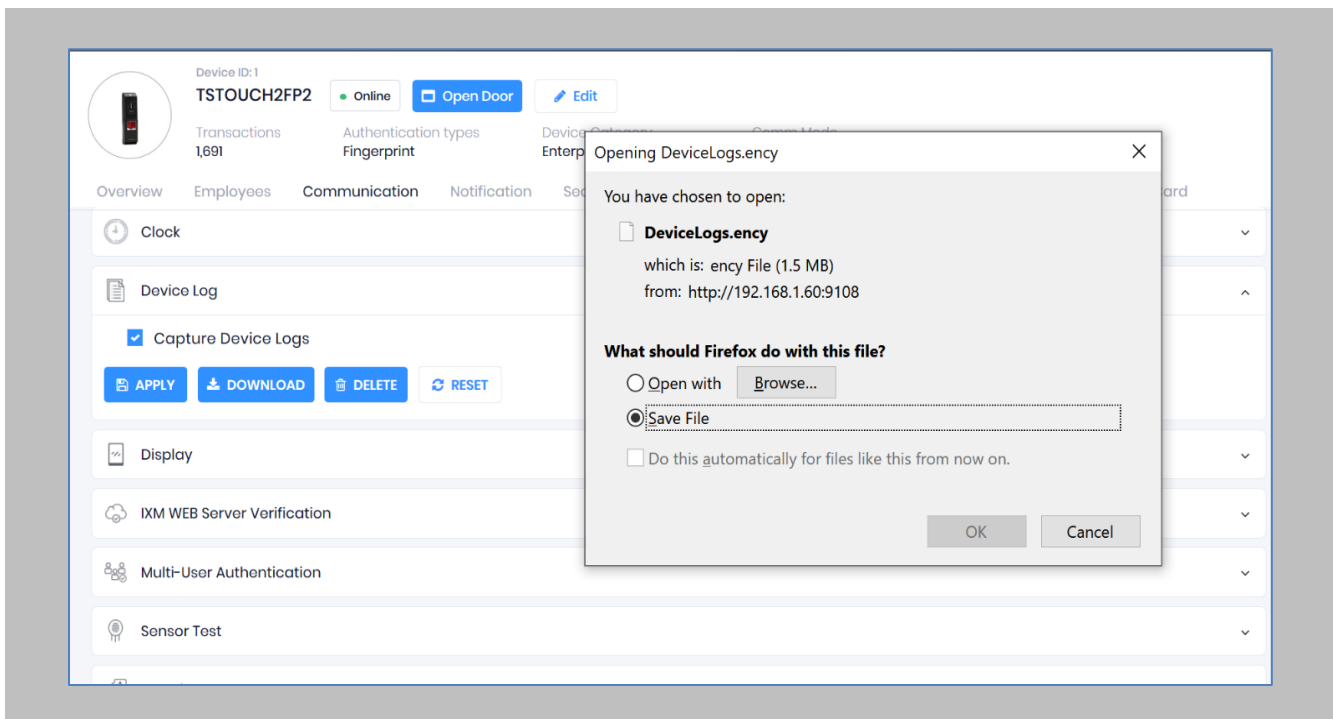


Figure 87: Save Device Log File



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 the Left Navigation pane in IXM WEB and click on Transaction Logs. A filter option is available in the Transaction Logs columns.

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

- Applications 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. The filter option is available in the Application Logs columns.

Logs folder location on IXM WEB Server:


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

Table 8: Logs Folder Location

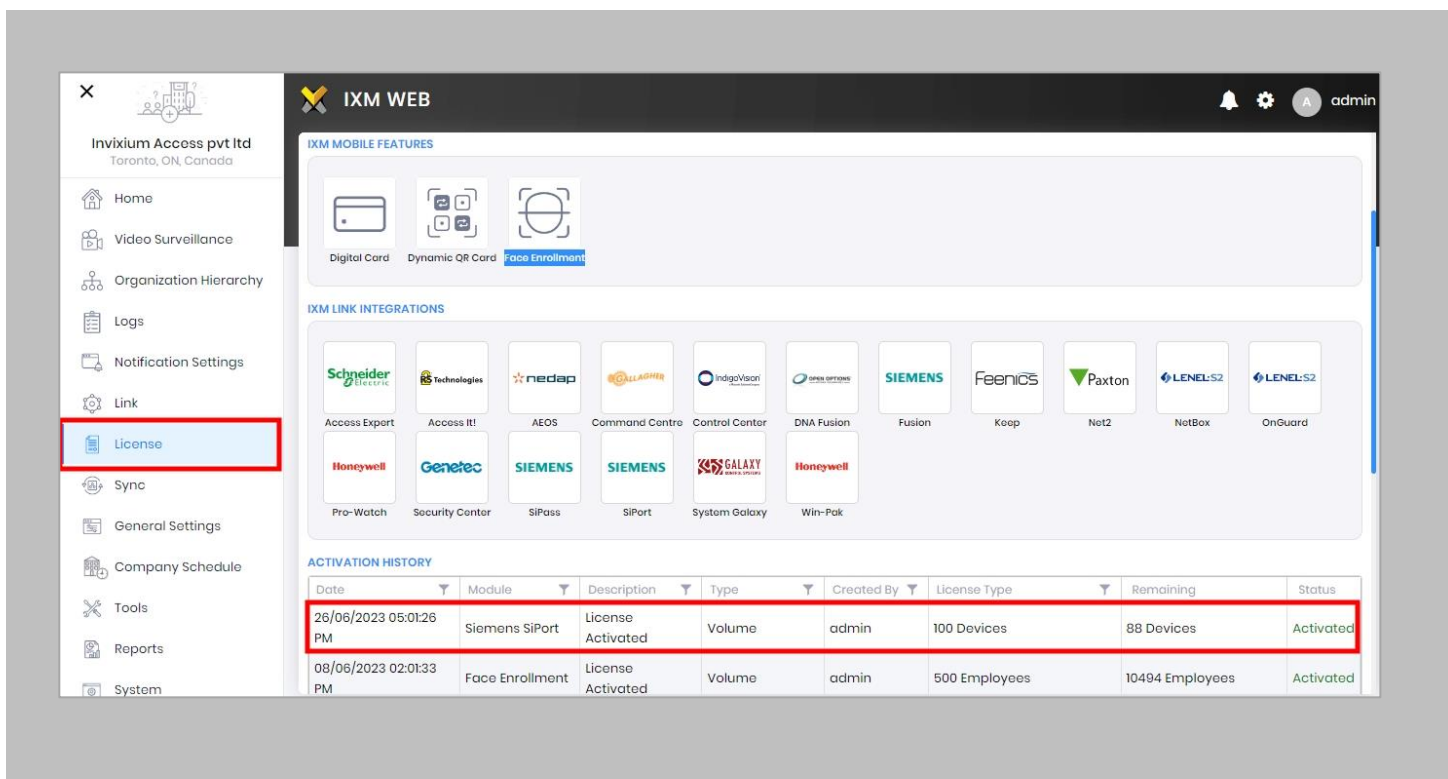
Unable to connect to the SiPort Server

Procedure

STEP 1

 Note: Confirm module activation

Navigate to **Licence**, and check **ACTIVATION HISTORY**. If not there, request a Licence.



The screenshot shows the IXM WEB interface. On the left is a navigation menu with the 'License' option highlighted in a red box. The main content area is divided into three sections: 'IXM MOBILE FEATURES' (Digital Card, Dynamic QR Card, Face Enrollment), 'IXM LINK INTEGRATIONS' (various vendor logos like Schneider Electric, Siemens, etc.), and 'ACTIVATION HISTORY'. The 'ACTIVATION HISTORY' section contains a table with the following data:

Date	Module	Description	Type	Created By	License Type	Remaining	Status
26/06/2023 05:01:26 PM	Siemens SiPort	License Activated	Volume	admin	100 Devices	88 Devices	Activated
08/06/2023 02:01:33 PM	Face Enrollment	License Activated	Volume	admin	500 Employees	10494 Employees	Activated

Figure 88: IXM WEB - Licence Module

STEP 2

 Note: Confirm SiPort API is enabled.

From [Link](#), click the **SiPort** tab. Ensure the correct **URL** of the server is listed. here. If not, **correct** and **apply**.

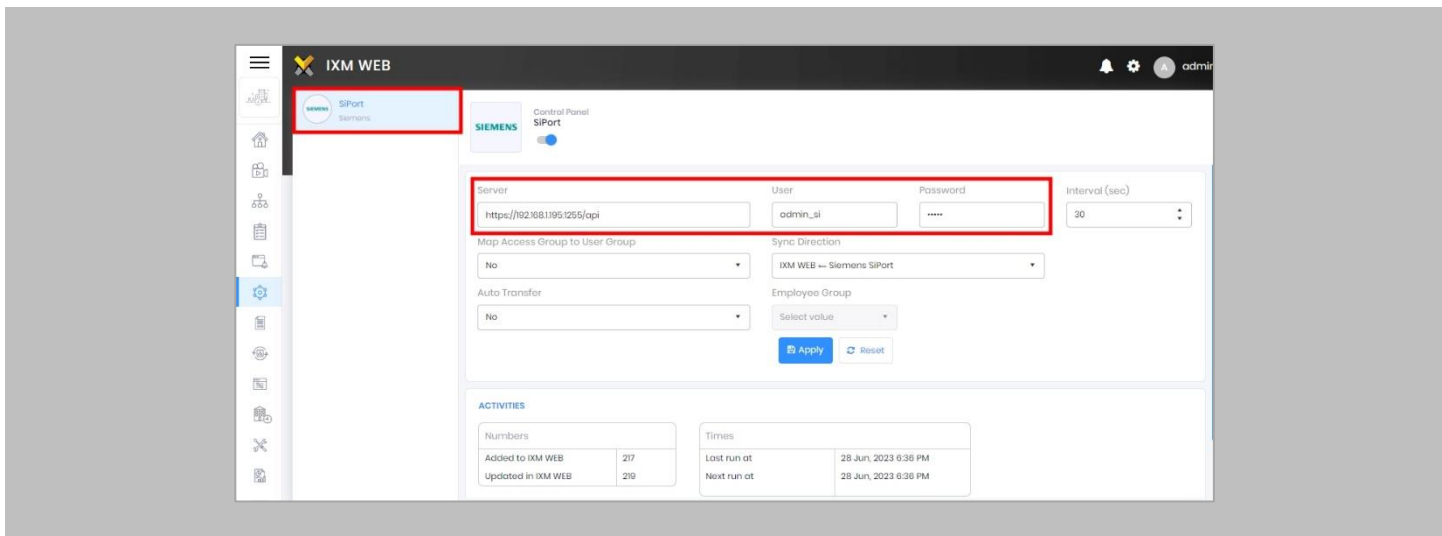




Figure 89: IXM WEB - SiPort Link Module

 Note: Confirm parameters entered to connect to the SiPort server.

Ensure the correct **User** who is authorized to connect to the API of SIEMENS SiPort is listed here. If not, **correct** and **apply**.

Ensure the correct **Password** of the user who is authorized to connect to the API of SIEMENS SiPort is listed here. If not, **correct** and **apply**.

STEP 4

 Note: Confirm SiPort API is up and running using some REST API Client.

This can be checked from Windows Services (Services.msc).

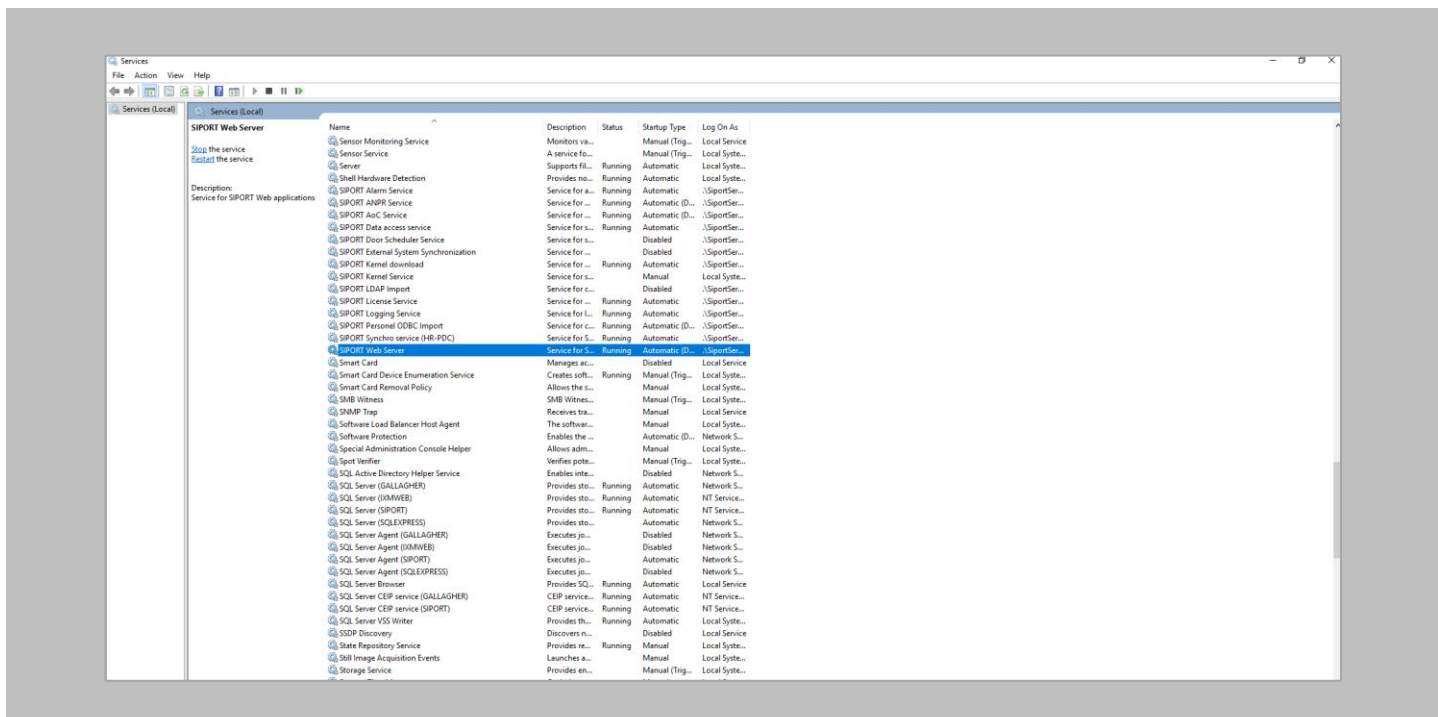



Figure 90: SIEMENS SiPort API

 Note: If you are still facing problems with connection, please email the [logtxt.txt](mailto:support@invixium.com) file to support@invixium.com.

This file is available at the following path:

Program Files (x86)\Invixium\IXM WEB\Log



16. Support

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

17. 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.

Copyright © 2023 Invixium. All rights reserved.